UNIVERZITET SINGIDUNUM



Gojko Grubor

PROJEKTOVANJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

BEOGRAD, 2012.

UNIVERZITET SINGIDUNUM

Gojko Grubor

PROJEKTOVANJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

Prvo izdanje

Beograd, 2012.

PROJEKTOVANJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

Autor:
Doc. dr Gojko Grubor

Recenzenti:
Prof. dr Milovan Stanišić
Prof. dr Branko Kovačević

Izdavač:
UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32
www.singidunum.ac.rs

Za izdavača:
Prof. dr Milovan Stanišić

Priprema za štampu:
Novak Njeguš

Dizajn korica:
Aleksandar Mihajlović

Lektor:
Snježana Krstić

Godina izdanja:
2012.

Tiraž:
300 primeraka

Štampa:
Mladost Grup
Loznica

ISBN 978-87-7912-398-5

Copyright:
© 2012 Univerzitet Singidunum
Izdavač zadržava sva prava.
Reprodukcija pojedinih delova ili celine ove publikacije nije dozvoljeno.



PREDGOVOR

Sistem inženjerski (SE) i procesni pristup, strukturno i objektno orijentisano modelovanje (OOM) pokazuju najbolje rezultate u projektovanju, razvoju i praksi kompleksnih IKT sistema i sistema zaštite informacija. Procesi zaštite, koji transformišu ulazne veličine u očekivano povećane izlazne vrednosti, integrišu ključne atribute svakog posla – procedure, alate i ljude, fundamentalni su blokovi za izgradnju sistema zaštite. Kako je zaštita *proces*, a ne *odredište*, procese zaštite treba neprekidno poboljšavati. Da bi se procesi zaštite kvalitetno upravljali, potrebno ih je meriti. Metrike i merenja u oblasti zaštite omogućavaju projektovanje menadžment sistema bezbednosti informacija (ISMS-a). Poboljšanje procesa zaštite zahteva evaluaciju tekućeg stanja formalno opisanih i definisanih procesa zaštite. Primenjeni PDCA model procesa ISMS-a obezbeđuje smernice za planiranje, implementaciju, održavanje i poboljšanje procesa. Za evaluaciju kvaliteta i merenje progresivnog sazrevanja i poboljšanja procesa, razvijeni su procesno orijentisani standardi i modeli (ISO/IEC 27001, ISO/IEC 21827). Komparativna analiza komplementarnosti standarda i modela razvijenih na bazi sistem inženjerskog (SE) pristupa, ukazuje na mogućnost uspostavljanja više okvira za evaluaciju usaglašenosti i poboljšanje procesa zaštite. Modeli koji integrišu procese (SSE CMM, CMMI) obezbeđuju integrisani i jedinstven okvir za evaluaciju i poboljšanje različitih tipova procesa. Za evaluaciju procesa zaštite na bazi SSE CMM modela specifično je razvijen SSAM metod verifikacione evaluacije, a za evaluaciju integrisanih procesa na bazi CMMI modela, razvijen je SCAMPI metod evaluacije.

U izradi ovog udžbenika uloženi su napor i vreme za koje je uskraćena moja porodica. Zato se u prvom redu zahvaljujem supruzi *Mileni* i kćerkama *Mariji* i *Jeleni* za opštu podršku i razmevanje koje su mi pružili. Posebno se zahvaljujem *prof. dr Milenku Heleti*, na inicijativi, punoj podršci, datim sugestijama i ukupnom pozitivnom pristupu i ličnom doprinosu u definisanju forme i sadržaja rada u pripremi i realizaciji. Izuzetno se zahvaljujem recenzentima ovog udžbenika, *prof. dr Milovanu Stanišiću*, rektoru Univerziteta Singidunum na razumevanju potrebe, odobravanju sadržaja predmeta i stvaranju opštih uslova za realizaciju udžbenika i *prof. dr Branislavu Kovačeviću*, rektoru Beogradskog univerziteta, na iznetim sugestijama i velikom doprinosu da udžbenik dobije formu i kvalitet na zahtevanom nivou.

Za tehničku obradu rada i iznete sugestije o dizajnu i grafičkim prilozima, zahvaljujem se Novaku Njegušu i Aleksandru Mihajloviću.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM



SADRŽAJ

PREDGOVOR III
UVOD 1

1. KONCEPTI *BEZBEDNOSTI* I *ZAŠTITE* INFORMACIJA 5
   1.1 UVOD 5
   1.2 INFORMACIJE I INFORMACIONA IMOVINA 6
   1.3 INFORMACIONA IMOVINA KAO OBJEKAT ZAŠTITE 7
   1.4 BEZBEDNOST I ZAŠTITA INFORMACIJA 8
   1.5 FAKTORI UTICAJA NA BEZBEDNOST INFORMACIJA 10
   1.6 OPŠTA DEFINICIJA SISTEMA ZAŠTITE 13
   1.7 OSNOVNE FUNKCIONALNOSTI SISTEMA ZAŠTITE 14
      1.7.1 Servisi zaštite 15
      1.7.2 Mehanizmi i protokoli zaštite 15
      1.7.3 Kontrole zaštite informacija 18
   1.8 GENERIČKI, FUNKCIONALNI MODEL SISTEMA ZAŠTITE 25
   1.9 DEFINISANJE *OPTIMALNOG SISTEMA ZAŠTITE* 26
   1.10 ARHITEKTURA SISTEMA ZAŠTITE INFORMACIJA 27
   1.11 NOVA PARADIGMA ZAŠTITE INFORMACIJA 28
   1.12 REZIME 30
   1.13 PITANJA ZA PONAVLJANJE 31

2. SISTEMSKI I PROCESNI PRISTUP ZAŠTITI INFORMACIJA **33**
2.1 UVOD 33
2.2 SISTEMSKA ANALIZA 34
2.2.1 Sistemsko mišljenje 34
2.3 SISTEMSKI PRISTUP ZAŠTITI INFORMACIJA 36
2.3.1 Modelovanje sistema zaštite informacija 38
2.3.1.1 Strukturno modelovanje sistema zaštite 38
2.3.2.2 Objektno orijentisano modelovanje sistema zaštite informacija 40
2.4 PROCESNI PRISTUP ZAŠTITI INFORMACIJA 42
2.4.1 Definicija, struktura i kontrola *„procesa"* 42
2.4.2. Menadžment sistem procesa 44
2.4.3. Tipovi kvaliteta procesa 48
2.4.3.1 Proces najbolje prakse 49
2.4.4. Modeli procesa zaštite 51
2.5 REZIME 55
2.6 PITANJA ZA PONAVLJANJE 56

3. GENERIČKI METODI POBOLJŠAVANJA PROCESA ZAŠTITE **59**
3.1 UVOD 59
3.2 KONCEPTI POBOLJŠAVANJA PROCESA ZAŠTITE 60
3.2.1 Neformalni metod poboljšanja stabilnosti procesa zaštite 60
3.2.1.1 Poboljšanje produktivnosti 60
3.2.1.2 Poboljšanje adaptivnosti procesa 62
3.2.1.3 Poboljšanje korisničke prihvatljivosti 64
3.2.2 Formalni, struktuirani pristup za poboljšavanje procesa 65
3.2.2.1 Evaluacija procesa zaštite 71
3.2.2.2 Standardi za poboljšavanje proizvoda i procesa zaštite informacija 71
3.3 OSNOVNI PARAMETRI POTPUNE KOMUNIKACIJE 74
3.3.1 Značaj potpune komunikacije za poboljšavanje procesa zaštite 77
3.4. REZIME 78
3.5. PITANJA ZA PONAVLJANJE 79

4. EVOLUCIJA STANDARDA KVALITETA ZAŠTITE INFORMACIJA **81**
4.1 UVOD 81
4.2. MEĐUNARODNA TELA ZA STANDARDIZACIJU ZAŠTITE INFORMACIJE 82
4.3 STANDARDI I MODELI KVALITETA PROIZVODA I PROCESA ZAŠTITE 83
4.3.1 Generički standardi procesa i proizvoda zaštite 83
4.3.2 Standard za evaluaciju kriptografskih algoritama i modula 84
4.3.3 Komparativna analiza izvornih standarda zaštite 85
4.4. RAZVOJ STANDARDA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA 85

4.4.1. Razvoj standarda *najbolje prakse* zaštite informacija 85
4.4.2 Razvoj modela sazrevanja procesa 87
4.4.3 Model sazrevanja procesa zaštite (SSE-CMM) 91
4.4.4. Ostali relevantni standardi i regulative zaštite informacija 92
4.4.4.1 ISO/IEC 13335-1 (IT Security Managament) 92
4.4.4.2 Standard za zaštitu podataka industrije platnih kartica (PCI) 92
4.4.4.3 COBIT 92
4.4.4.4 ISO/IEC 20000 serija standarda (ITIL) 93
4.4.4.5 Zakoni i regulative zaštite 93
4.5 KOMPLEMENTARNOST I KOMPATIBILNOST STANDARDA ZAŠTITE 94
4.6 REZIME 99
4.7 PITANJA ZA PONAVLJANJE 100

5. EVOLUCIJA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA 101
5.1 UVOD 101
5.2 RAZVOJ METODOLOGIJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA 102
5.2.1 Principi menadžment sistema zaštite informacija 103
5.2.2 Razvoj uloga i odgovornosti u ISMS 103
5.2.3 Generički procesi menadžment sistema 104
5.3 RAZVOJ STANDARDA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA 104
5.3.1 Uvod u standard ISO/IEC 27001 (ISMS) 106
5.3.2 Uvod u standard ISO/IEC 27002 110
5.3.3 Komplementarnost ISMS standarda sa drugim ISO standardima 112
5.4 PDCA PROCESNI PRISTUP ZA USPOSTAVLJANJE ISMS-a 113
5.4.1 Drugi pristupi za uspostavljanje ISMS-a 116
5.4.2 Razvoj metrika za evaluaciju ISMS-a 117
5.5 REZIME 121
5.6 PITANJA ZA PONAVLJANJE 122

6. MENADŽMENT SISTEM ZAŠTITE INFORMACIJA (ISMS) 125
6.1 UVOD 125
6.2 USPOSTAVLJANJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA 126
6.2.1 Principi i model menadžment sistema zaštite informacija 126
6.2.2 Procesni pristup u ISMS standardu 131
6.2.3 Obim i primena ISMS-a 132
6.2.4 Zahtevi ISMS standarda 133
6.2.4.1 Implementacija i rad ISMS (4.2.2 standarda) 135
6.2.4.2 Monitoring i provera ISMS-a (poglavlje 4 i 5 standarda) 136
6.2.4.3 Održavanje i poboljšanje ISMS-a (6 i 7 standarda) 136

6.2.4.4 Zahtevi ISMS standarda za dokumentaciju i zapise 137
6.2.4.5 Odgovornosti menadžmenta u ISMS-u (5.0 standarda) 138
6.2.4.6 Upravljanje resursima (5.2 standarda) 138
6.2.4.7 Obuka, svest o potrebi i kompetencije zaposlenih (5.2.2 standarda) 138
6.2.4.8 Interna provera ISMS-a (6.0 standarda) 139
6.2.4.9 Menadžerska revizija ISMS-a (7.0 standarda) 139
6.2.4.10 Poboljšavanje ISMS-a (8.0 standarda) 140
6.3 OTVORENI PROBLEMI MENADŽMENTA ZAŠTITE INFORMACIJA 141
6.4 PREPORUKE ZA MENADŽMENT SISTEM ZAŠTITE INFORMACIJA 142
6.5 REZIME 143
6.6 PITANJA ZA PONAVLJANJE 144

7. PLANIRANJE ISMS-a I MENADŽMENT RIZIKA 147
7.1 UVOD 147
7.2 PRIMENA PDCA MODELA PROCESA U ISMS-u 148
7.3 PDCA FAZA *PLANIRANJA I USPOSTAVLJANJA ISMS*-a 148
7.3.1 Definisanje obima ISMS-a 149
7.3.2 Definisanje politike zaštite informacija 149
7.3.2.1 IMS politika zaštite 149
7.3.2.2 *Sveobuhvatna politika zaštite informacija* 150
7.3.3 Menadžment bezbednosnog rizika organizacije 156
7.3.4 Priprema izjave o primenljivosti (SoA) 173
7.4 REZIME 173
7.5 PITANJA ZA PONAVLJANJE 174

8. IMPLEMENTACIJA, PROVERA I POBOLJŠANJE ISMS-a 177
8.1 UVOD 177
8.2 IMPLEMENTACIJA ISMS-a (*Do phase*) 178
8.2.1 Implementacija plana tretmana rizika 178
8.2.2 Pisanje politike i procedura komponenti zaštite 178
8.2.3 Izbor metrike i merenja ISMS-a 180
8.2.4 Selekcija i implementacija kontrola zaštite 184
8.2.5 Razvoj svesti o potrebi, obuka i obrazovanje u zaštiti 184
8.2.6 Menadžment operativne primene ISMS-a i sistema zaštite 185
8.2.7 Menadžment bezbednosnog incidenta 185
8.2.8 Povratak investicija u zaštitu informacija (ROSI) 188
8.3 PROVERA IMPLEMENTIRANOG ISMS-a 189
8.3.1 Izvršavanje operativnog plana 190

8.3.2 Provera nivoa preostalog rizika 192
8.3.3 Interna provera ISMS-a 192
8.3.4 Regularna menadžerska revizija ISMS-a 196
8.4 POBOLJŠAVANJE ISMS-a (*Act Phase*) 196
8.5 REZIME 198
8.5 PITANJA ZA PONAVLJANJE 200

9. SERTIFIKACIJA, AKREDITACIJA I USAGLAŠAVANJE ISMS-a 203
9.1 UVOD 203
9.2 ORGANIZACIJA PROCESA SERTIFIKACIJE I AKREDITACIJE 204
9.2.1 Uloge i odgovornosti u procesu sertifikacije i akreditacije 204
9.2.2 Proces sertifikacije 205
9.2.3 Sertifikacija usaglašenosti sa ISMS standardom 210
9.2.4 Akreditacija ISMS-a 212
9.3 USPOSTAVLJANJE USAGLAŠENOSTI SA STANDARDIMA 213
9.3.1 Organizaciona struktura menadžment sistema usaglašenosti 213
9.3.2 Uspostavljanje usaglašenosti sa standardima 215
9.3.3 Program menadžment sistema usaglašenosti ISMS-a 216
9.3.3.1.Sistem inženjerski zahtevi za menadžment usaglašenosti 217
9.3.3.2 Metodologija menadžmenta bezbednosne usaglašenosti 223
9.3.3.3 Alati za menadžment sistem usaglašenosti 226
9.3.3.4 Metrika procesa menadžment sistema usaglašenosti 227
9.4 REZIME 231
9.5 PITANJA ZA PONAVLJANJE 232

10. MODEL SAZREVANJA PROCESA ZAŠTITE 235
10.1 UVOD 235
10.2 RAZVOJ I STRUKTURA GENERIČKOG MODELA SAZREVANJA PROCESA 236
10.3 MODEL I METOD SAZREVANJA PROCESA ZAŠTITE 237
10.3.1 Dimenzija primene SSE CMM modela 239
10.3.2 Dimenzija sazrevanja kapaciteta procesa 243
10.4 PRIMENA SSE CMM MODELA ZA RAZVOJ PROGRAMA ZAŠTITE 249
10.4.1 Razvoja optimalnog programa zaštite 250
10.4.2 Primene SSE CMM za profilisanje procesa organizacija u zaštiti 250
10.4.3 Obezbeđivanje argumenata garantovane bezbednosti 250
10.4.4 Profilisanje kompetencija zaposlenih u oblasti zaštite (P-CMM) 252
10.4.5 Razvoj bezbednosnih zahteva 255
10.4.6 Primene metrike sazrevanja kapaciteta procesa zaštite 257
10.4.7 Implementacija CMM praksi i procesa 262

10.4.8 Prednosti i nedostaci SSE CMM modela 263
10.5 REZIME 264
10.6 PITANJA ZA PONAVLJANJE 264

11. METOD EVALUACIJE I POBOLJŠANJA PROCESA ZAŠTITE 267
11.1. UVOD 267
11.2 CILJEVI I IZLAZNI REZULTATI EVALUACIJE 268
11.3 METOD EVALUACIJE SAZREVANJA PROCESA ZAŠTITE 269
11.3.1 Uloge i odgovornosti učesnika SSAM procesa evaluacije 270
11.3.2 Tipovi SSAM procesa evaluacije 272
11.3.3 Promenljivi parametri procesa evaluacije 273
11.3.4 Rezultati i izveštavanje SSAM evaluacije 275
11.4 STUDIJA SLUČAJA: *Asistirana SSAM evaluacija „CAXY"* 275
11.4.1 Izbor željenog profila procesa 275
11.4.2 Analiza rezultata SSAM evaluacije tekućih procesa CAXY 277
11.4.2.1 Analiza i konsolidacija dokaza 279
11.4.2.2 Analiza glavnih nalaza SSAM evaluacije tekućih procesa CAXY 281
11.4.2.3 Komparativna analiza referentnog i tekućeg profila OP CAXY 284
11.4.3 Poboljšanje tekućih procesa CAXY 284
11.4.3.1 Poboljšanje procesa na bazi CMM modela 284
11.4.3.2 Uloge i odgovornosti u projektu poboljšanja procesa 286
11.4.3.3. Tipična infrastruktura procesa za poboljšanje procesa 286
11.4.3.4 Akcioni planovi za poboljšanje tekućih procesa CAXY 287
11.5 ANALIZA ISKUSTAVA IZ SSAM PROCESA EVALUACIJE 288
11.5.1 Dopuštena odstupanja od SSE CMM modela 288
11.5.2. Odstupanja od procesa SSAM metoda evaluacije 289
11.5.3 Iskustva iz sprovođenja *plana evaluacije tekućih procesa CAXY* 290
11.5.4 Iskustva iz vođenja intervijua 291
11.5.5 Sugestije za sponzora 291
11.6. REZIME 292
11.7 PITANJA ZA PONAVLJANJE 293

12. OBRASCI I MODELI PROCEDURA ZAŠTITE 295
12.1. UZORAK OBRASCA ZA DOKUMENTOVANJE PROCEDURE 295
12.2 GENERIČKA STRUKTURA PROCEDURE ZA IZRADU *PLANA ZAŠTITE (NIST)* 296
12.3 PROCEDURA KONTROLE PRISTUPA 303
12.4 PROCEDURA INTERNE PROVERE ISMS-a 308

13. PRILOZI **315**
Prilog 6.1: Projektna dokumentacija implementacije ISMS 315
Prilog 7.1: Nacrt plana faze planiranja 320
Prilog 7.2: Obrazac sadržaja za ISMS politiku 321
Prilog 7.3: Prioritetizacija incidenta (P = UT + UR) 325
Prilog 7.4: Uzorak obrasca za izradu politike zaštite 326
Prilog 7.5: Primer upitnika za vrednovanje informacione imovine 330
Prilog 7.6: Tipični parovi ranjivost/pretnja (V/T) 331
Prilog 7.7: Uzorak izveštaja o proceni rizika (NIST *template*) 334
Prilog 7.8: Obrazac plana tretmana rizika 335
Prilog 7.9: Uzorak *Izjave o primenljivosti* (SoA) 336
Prilog 8.1: Inicijalna priprema implementacije ISMS-a 337
Prilog 8.2: Projekat poboljšanja procesa 339
Prilog 10.1: SSE CMM v.3.0 model: dimenzija nivoa kapaciteta (CL) 342
Prilog 10.2: SSE CMM kriterijumi za razvoj optimalnog programa zaštite 343
Prilog 10.3: Razvoj referentnog profila op standardnog CA 346
Prilog 10.4: Primer *plana im*plementacije poboljšanja procesa 348
Prilog 11.1: Primer *UPITNIKA* za SSAM evaluaciju 349
Prilog 11.2: Kontrolna lista za pripremu aktivnosti faze evaluacije na terenu 352
Prilog 11.3: Radna tabela za praćenje podataka (DTS) 353
Prilog 11.4: Radni dokumenti za praćenje kretanja dokaza 356
Prilog 11.5: Scenario komunikacija u procesu SSAM evaluacije 357
Prilog 11.6: Projekat za razvoj i poboljšavanje *OP18 SSE CMM* 360
Prilog 11.7: Uzorak: Akcioni plan projektnog tima za poboljšanje procesa 361

REČNIK TERMINA ISMS-A **363**
LITERATURA **371**

PREGLED TABELA

Tabela 1.1 Definicije pojma informacija u funkciji izvora i cilja
Tabela 1.2 Klasifikacija informacione imovine
Tabela 1.3 Relevantni aspekti zaštite IKT sistema
Tabela 1.4 Mrežni protokoli sa poznatim ranjivostima
Tabela 1.5 Klase, familije i identifikatori kontrola zaštite
Tabela 1.6 Dimenzije kontrola zaštite
Tabela 1.7 Primer matrice praćenja bezbednosnih zahteva
Tabela 1.8 Metodi za procenu efektivnosti kontrola zaštite za različite uticaje rizika
Tabela 1.9 SABSA okvir i model arhitekture sistema zaštite
Tabela 2.1 Uzorak kriterijuma za definisanje procesa
Tabela 3.1 Uzorak kriterijuma za definisanje procesa
Tabela 3.2 Uzorak *kratke verzije opisa procesa*
Tabela 3.3 Uzorak *duge verzije opisa procesa*
Tabela 3.4 Uzorak za *opis procedure*
Tabela 4.1 Relevantna međunarodna tela za standardizaciju u oblasti zaštite
Tabela 4.2 Kriterijumi indikatora kriptografskih nivoa bezbednosti (L)
Tabela 4.3 Indikatori nivoa bezbednosti standarda TCSEC, ITSEC, CC i FIPS-140-2
Tabela 4.4 Osnovne karakteristike standarda ISO/IEC 17799:2000
Tabela 4.5 Objavljeni modeli sazrevanja procesa zaštite
Tabela 4.6 Pregled relevantnih parametara primenjivanih standarda zaštite
Tabela 4.7 Kompatibilnost ISO/IEC 21827 i ISO/IEC 15504
Tabela 4.8 Uporedni pregled SSE CMM i drugih standarda i modela IKT zaštite
Tabela 4.9 Komplementarnost SSE CMM, ISO/IEC 17799, ISO/IEC 13335 i NIST
Tabela 5.1 Razvoj ISMS standarda zaštite informacija
Tabela 5.2 Familija standarda ISO/IEC 27000
Tabela 5.3 Uzorak SMF okvira i smernice za interpretaciju politike zaštite
Tabela 5.4 Struktura *kontrole zaštite* u standardu ISO/IEC 27002
Tabela 5.5 Kratak opis faza PDCA modela procesa
Tabela 5.6 Koraci faza PDCA modela procesnog pristupa
Tabela 6.1 Komplementarnost OECD principa i PDCA modela
Tabela 6.2 Opšte prihvaćeni (GAISP) principi zaštite
Tabela 6.3 Komplementarnost ISO 9001:2000, ISO 14001:2004 i ISO/IEC 27001:2005
Tabela 6.4 Komplementarnost PDCA procesnog pristupa i ISMS standarda
Tabela 7.1 Nacrt sadržaja politike zaštite
Tabela 7.2 Pristupi proceni rizika
Tabela 7.3 Proces menadžmenta rizika
Tabela 7.4 Uzorak sadržaja liste informacione imovine organizacije

Tabela 7.5 Primer kriterijuma za kategorizaciju informacione imovine
Tabela 7.6 Obrazac za evaluaciju i vrednovanje rizika
Tabela 7.7 Primer dokumentovanja ranjivosti
Tabela 7.8 Primeri pretnji
Tabela 7.9 Naziv imovine <naziv>
Tabela 7.10 Smernica za procenu pojave pretnje i štete za organizaciju
Tabela 7.11 Primer kvalitativne procene da će pretnja/e iskoristiti ranjivost
Tabela 7.12 Primeri kontrola fizičke zaštite
Tabela 7.13 Tehničke kontrole sistema zaštite
Tabela 7.14 Personalna zaštita
Tabela 7.15 Primeri procedura zaštite
Tabela 7.16 Vrednovanje metoda implementiranog sistema zaštite
Tabela 7.17 Matrica za vrednovanje verovatnoće faktora rizika
Tabela 7.18 Smernica za utvrđivanje vrednosti uticaja rizika
Tabela 7.19 Matrica za određivanje faktora rizika
Tabela 7.20 Nacrt sadržaja plana tretmana rizika
Tabela 7.21 Primer nacrta *plana tretmana rizika*
Tabela 7.22 Primer sažetka izabranih kontrola (S oC) iz ISO/IEC 27001
Tabela 7.23 Uzorak obrasca za opis imovine
Tabela 7.24 Primer izjave o primenljivosti (SoA)
Tabela 8.1 Izvor smernica za razvoj metrika i merenja za politiku zaštite
Tabela 8.2 Definicije faktora za implementaciju *metrike politike zaštite*
Tabela 8.3 Kriterijumi za proveru efektivnosti kontrola zaštite
Tabela 8.4 Primer čekliste za praćenje provera ISMS-a
Tabela 8.5 Smernice za proračun ciljeva godišnjeg rada (*uptim)* IKT sistema
Tabela 8.6 Smernice za proračun tolerisanog vremena prekida rada IKT sistema
Tabela 8.7 Obrazac za internu proveru ISMS-a
Tabela 8.8 Primer strukture *upitnika za internu proveru ISMS*-a (*Audit Checklist*)
Tabela 9.1 Spisak dokumenata i aktivnosti za pripremu procesa sertifikacije
Tabela 9.2 Koraci faze provere u procesu sertifikacije
Tabela 9.3 Izveštaj o pregledu dokumenata posle faze 1
Tabela 9.4 Izveštaji provere posle treće faze
Tabela 9.5. Struktura menadžmenta usaglašenosti u kontekstu PDCA
Tabela 9.6 Prošireni okvir za menadžment zahteva za usaglašenost sa standardima
Tabela 9.7 Matrica za praćenje zahteva za usaglašenost
Tabela 9.8 Matrica za praćenje zahteva za usaglašenost – *Izvod iz* FSG *smernica*
Tabela 9.9 Obrazac matrice za praćenje PSP-a
Tabela 9.10 Obrazac matrice za praćenje zahteva za usaglašenost
Tabela 9.11 Matrica za praćenje zahteva – *Poslovni pokretači* (*Business Drivers* – BD)
Tabela 9.12 Matrica dokumenata zahteva za usaglašavanje (CRDM)

Tabela 9.13 Matrica za praćenje zahteva na bazi SMF
Tabela 9.14 Opšti WBS za razvoj ISMS-a na bazi ISO/IEC 27001 standarda
Tabela 9.15 Primer skale ponderisanja težinskih faktora
Tabela 9.16 Uzorak obrasca za definisanje usaglašenosti ISMS programa
Tabela 10.1 CMM modeli, reprezentacije i oblasti primene
Tabela 10.2 Razvoj SSE CMM modela
Tabela 10.3 Nivoi kapaciteta — CL i zrelosti — ML procesa SSE CMM modela
Tabela 10.4 Oblasti procesa u tri opšte kategorije SSE CMM
Tabela 10.5 Međuzavisnosti OP i GP SSE CMM modela procesa
Tabela 10.6 Broj BP po OP u SSE CMM modelu
Tabela 10.7 Zajedničke karakteristike (CF) po nivoima kapaciteta (CL)
Tabela 10.8 Raspored CF po CL SSE CMM modela
Tabela 10.9 Principi sazrevanja procesa zaštite u SSE CMM modelu
Tabela 10.10 OP P-CMM modela po nivoima zrelosti
Tabela 10.11 Međuzavisnosti kategorije OP-a i nivoa zrelosti u P-CMM modelu
Tabela 11.1 Uporedna analiza atributa metoda evaluacije
Tabela 11.2 Faze procesa SSAM metoda evaluacije
Tabela 11.3 Kvalifikacije i odgovornosti primarnih učesnika u procesu evaluacije
Tabela 11.4 Zahtevi za radno angažovanje u SSAM procesu evaluacije
Tabela 11.5 Neki kriterijumi za izbor projekata za evaluaciju
Tabela 11.6 Atributi DTS tabele za skupljanje i praćenje dokaza

PREGLED SLIKA I GRAFIKONA

Slika 1.1. Primer odnosa podataka i informacije
Slika 1.2 Nivo ukupne bezbednosti u funkciji komponenti bezbednosti
Slika 1.3 Nivo ukupne bezbednosti IKTS u funkciji pretnji
Slika 1.4 Lokacija SSL protokola u višeslojnoj arhitekturi računarske mreže
Slika 1.5 Generički model i međusobni odnosi komponenti sistema zaštite
Slika 1.6 Optimalni sistem zaštite informacija
Slika 1.7 Model SABSA® slojeva arhitekture sistema zaštite

Slika 2.1. Tri nivoa sistemskog inženjerstva
Slika 2.2. Izlaz strukturnog modelovanja sistema osnovne zaštite IKT sistema
Slika 2.3 Proces lavine
Slika 2.4 Uticaji na proces
Slika 2.5 Statističko upravljanje procesa
Slika 2.6 Interpretacija statističke kontrole procesa
Slika 2.7 Rentabilnost poslovanja
Slika 2.8 Inkrementalna i inovativna poboljšanja procesa

Slika 2.9 Model menadžment sistema kvaliteta zasnovanog na procesima
Slika 2.10 Generički proces sistema zaštite
Slika 2.11 Proces zaštite kao transformator ulaznih parametara u izlazne
Slika 2.12 Proces kao integrator ljudi, metoda i tehnologije
Slika 2.13 Troškovi, prednosti i nedostaci uvođenja modela procesa

Slika 3.1 Programi za poboljšanje procesa
Slika 3.2 Zatvorena petlja komunikacije
Slika 3.3 Interakcija za razmenu poruka
Slika 3.4 Kompletirana komunikaciona petlja
Slika 3.5 Konteksti komunikacione petlje

Slika 4.1 Organizaciona šema Tehničkog komiteta ISO/IEC JTC 1SC 27
Slika 4.2 Razvoj ISO/IEC standarda zaštite informacija
Slika 4.3 Pregled istorije razvoja CMM modela procesa
Slika 4.4 Korelacija ISO/IEC 21827 i ISO/IEC 17799:2000 standarda

Slika 5.1 Generički proces ISMS-a (a) i usaglašenosti sa ISBS (b)
Slika 5.2 Okvir menadžment sistema zaštite (SMF)
Slika 5.3 Kategorije kontrola zaštite u standardu ISO/IEC 27002
Slika 5.4 PDCA procesni model
Slika 5.5 Funkcionalni model PDCA procesa

Slika 6.1 Tok procesa uspostavljanja ISMS-a
Slika 6.2 PDCA model ISMS procesa
Slika 6.3 Struktura relevantnih sekcija ISMS-a

Slika 7.1 Dokumentacija i proizvodi rada faze planiranje
Slika 7.2 Hijerarhija politike organizacije
Slika 7.3 Organizacija menadžment sistema zaštite
Slika 7.4 Model menadžmenta bezbednosnog rizika
Slika 7.5 Međuzavisnosti komponenti bezbednosnog rizika
Slika 7.6 Pojednostavljeni odnosi i tok podataka u procesu menadžmenta rizika u IKT
Slika 7.7 Struktura procesa menadžmenta rizika

Slika 8.1 Proces PDCA faze primene
Slika 8.2 PDCA faza provere implementiranog ISMS-a
Slika 8.3 Međuzavisnost sistema zaštite i rizika (13335-1.204)
Slika 8.4 PDCA faza poboljšanja procesa (Act phse)

Slika 9.1 Organizaciona struktura procesa nezavisne ISMS serifikacije
Slika 9.2 Proces implementacije i sertifikacije ISMS-a
Slika 9.3 Okvir menadžment sistema zahteva za usaglašenost sa standardima
Slika 9.4 Matrice praćenja bezbednosnog usaglašavanja: pregled

Slika 10.1. Struktura SSE CMM modela sazrevanja procesa zaštite
Slika 10.2 SSE CMM kategorije procesa
Slika 10.3 Međusobni odnosi bezbednosno orijentisanih OP
Slika 10.4 Nivoi kapaciteta procesa zaštite u kontinualnoj reprezentaciji
Slika 10.5 Put sazrevanje procesa (ML) SSE CMM modela
Slika 10.6 Sazrevanje kapaciteta OP u SSE CMM modelu
Slika 10.7 Implementacija SSE CMM nivoa zrelosti SSE procesa
Slika 10.8 Odnosi metoda obezbeđivanja garantovane bezbednosti i redukovanog modela životnog ciklusa
Slika 10.9 Nivoi i atributi CL OP P-CMM modela
Slika 10.10 Sazrevanje nivoa i atributi OP P-CMM modela
Slika 10.11 Okvir za razvoj profila zaštite PKI sistema
Slika 10.12 Menadžment proces web aplikacija primenom metodologije S-vektora
Slika 10.13 Razvoj metrike zaštite
Slika 10.14 Odnosi SSE CMM metrike procesa i metrike zaštite
Slika 10.15 SSE CMM merljivi atributi procesa
Slika 10.16 SSE CMM merljivi atributi sistema zaštite
Slika 10.17 Primena SSE CMM metrika procesa i sistema zaštite
Slika 10.18 Dijagram razvoja metrika zaštite
Slika 10.19 Moguće metrike servisa kontrole pristupa
Slika 10.20 Odnosi SSE CMM OP u modelu metrike za OP upravljanja rizikom
Slika 10.21 Model IDEAL za implementaciju CMMI i SSE CMM procesa
Slika 10.22 Dijagram rasta CL procesa u funkciji porasta troškova (izvor: Merie Whatley, Texas Instruments. Inc.)

Slika 11.1 Model faza i koraka procesa SSAM evaluacije
Slika 11.2 Kriterijumi za dostizanje nivoa kapaciteta OP SSE CMM modela
Slika 11.3 Referentni profil OP standardnog CA
Slika 11.4 Profil nivoa zrelosti kapaciteta tekućih procesa CAXY
Slika 11.5 Nivoi dekompozicije programa za razvoj procesa

PREGLED SKRAĆENICA

ARC (*Appraisal Requirements for CMMI)* — zahtevi za CMMI evaluaciju

ASE (*Assurance Security Evaluation*) — klasa za evaluaciju bezbednosne garancije u CC standardu

AVP — antivirusni program

BAR — brza analiza rizika

BP (*Basic Practices*) — bazične prakse u CMM i SSE CMM modelima

BS (British standard) — Britanski standard (BS 7799 standard zaštite uključen u ISO/IEC 127799)

BSI (*Bundesamt für Sicherheit in der Informationstechnik*) — Nemačka agencija za zaštitu informacija

CA (*Certification Authority*) — sertifikaciono telo u sistemu infrastrukture sa javnim ključem.

CBA-IPI (*CMM Based Appraisal for Internal Process Improvement*) — evaluacija internih procesa na bazi CMM modela

CC *(Common Criteria)* — standard opštih kriterijuma, odnosno, *ISO 15408* standard za evaluaciju proizvoda i sistema zaštite

CCB *(Configuration Control Board)* — telo za kontrolu konfiguracije i upravljanje dokumentacijom

CEM (*CC Evaluation Methodology*) — metodologija CC evaluacije

CF (*Common Features*) — opšte karakteristike u CMM i SSE CMM modelima

CIRT (*Computer Incident Response Team*) — interventni tim za odgovore na kompjuterski incident

CL (*Capability Levels*) — nivoi kapaciteta procesa u CMM i SSE CMM modelima

CMM (*Capability Maturity Model*) — model (generički) sazrevanja procesa.

CMMI (*Capability Maturity Model Integration*) — integracioni model sazrevanja procesa za proizvodnju, snabdevanje i servise

CMP (*Compliance Managament Programm*) — program menadžmenta usaglašenosti

CoBIT(*Control Objectives for Information and Related Technology*) — kontrolni ciljevi za informacione i odnosne tehnologije

COBRA (*Risk Assessment Methodology*) — metodologija za procenu rizika

CP *(Certificate Policy)* — politika sertifikacije

CPS *(Certification Practice Statement)* — izjava o praksi sertifikacije; elemenat politike zaštite PKI

CTCPEC (*Canadian Trusted Computer Product Evaluation Criteria)* — kanadski kriterijumi za evaluaciju proizvoda poverljivih računarskih sistema

DAC (*Discret Access Control*) — diskreciona kontrola pristupa sa dodelom prava pristupa na bazi odluke vlasnika sistema; digitalni sertifikat (DS)

DoD *(Department of Defence)* —– Ministarstvo odbrane SAD

DTS *(Data Tracking Sheet)* — radna *Excel* tabela za praćenje podataka o implementaciji i institucionalizaciji BP, GP i OP i generisanje profila nivoa kapaciteta evaluiranih procesa (OP) u SSAM metodu evaluacije

EAL (*Evaluation Assurance Level*) — bezbednosni nivo evaluacije u CC standardu

EPG *(Engineering Process Group)* — SE tim za implementaciju procesa

ETVX (*Entry Criteria, Tasks, Verification, and eXit Criteria)* — IBM, SEI ***ETVX*** format za opis procesa

FIPS (*Federal Information Processing Standards*) — standardi procesiranja federalnog IKT sistema SAD

GAISP (*Generaly Accepted Information Security Principles*) — opšte prihvaćeni principi zaštite

GG (*Generic Goal)* — generički cilj u CMMI modelu procesa (kao CL u SSE CMM modelu)

GP (*Generic Practices*) — *generičke prakse* u CMM, SSE CMM i CMMI modelima

HasS *(Hardware as Service)* — ponuda hardvera kao servisa u *Cloud Copmuting*-u

HIPAA (*The Health Insurance Portability And Accountability Act)* — zakon o računovodstvu i prenosivosti zdravstvenog osiguranja

IA CMP (*Information Assurance CMP*) — program menadžmenta usaglašenosti bezbednosti informacija

IAP (*Information Assurance Program*) — program bezbednosti informacija

IasS — ponuda infrastrukture kao servisa u *Cloud Copmuting*-u

iCMM (*Integrated Capability Maturity Model*) — integrisani model sazrevanja procesa

IDEAL (*Initiating, Diagnosing, Establishing, Acting and Learning*) — model *SEI* instituta za implementaciju SSE CMM i CMMI procesa.

IDPS (*Intrusion Detection and Protection System*) — sistem za detekciju i sprečavanje upada

IDWG (*Intrusion Detection Working Group)* — radna grupa za detekciju upada

IEC *(International Electronig Committee)* —– Međunarodno standardizaciono telo

IEC (*International Electrotechnical Commission*) — Međunarodno standardizaciono telo

IEEE (*Institute of Electrical and Electronics Engineers*) — Institut inženjera elektrotehnike i elektronike, međunardona asocijacija od 150.000 članova

IETF (*International Engineering Task Force)* — Međunarodna inženjerska

IKT — Informaciono **K**omunikacione **T**ehnologije

IPSec protocol (*Internet Protocol Security*) — Internet protokol zaštite

ISBS (*Information Security Benchmark System)* — sistem indikatora progresa zaštite informacija

ISF (*International Security Forum*) — Međunarodni forum za bezbednost i zaštitu

ISMS (*Information Security Management System*) — menadžment sistem zaštite informacija

ISO *(International Standardization Organization)* — Međunarodna organizacija za standardizaciju

ISSEA (*International Systems Security Engineering Association*) — Međunarodna asocijacija za sistemsko inženjerstvo zaštite informacija

ITGI *(IT Governance Institute*) — Institut za davanje smernica u IT-u

ITSEC (*Information Technology Security Evaluation Criteria*) — kriterijumi za evaluaciju zaštite IKT sistema

ITSEM (*Information Technology Security Evaluation Manual*) — uputstvo za evaluaciju zaštite informacija

ITU (*International telecommuniccation Union*) — Međunardno standardizaciono telo u oblasti komunikacija

KEMZ — kompromitujuće elektromagnetno zračenje

MDD (*Method Description Document*) — dokument za opisivanje SCAMPI metoda

ML (*Maturity level*) — nivo zrelosti procesa u CMM modelima procesa

N/A (*Non Applicable*) — nije primenljivo

NDA (*Non Disclouse Agreement*) — ugovor o neotkrivanju informacija

NIDPS (*Network Intrusion Detection and Protection System*) — mrežni sistem za detekciju i sprečavanje upada

NIST (*National Institute of Standards and Technology*,) — Nacionalni institut za standarde i tehnologiju (SAD)

NOC (*Network Operation Center*) — Centar za mrežne operacije

OCTAVE (*Operationally Critical Threat, Assets and Vulnerability Evaluation*) — metod analize rizika i evaluacije ranjivosti od operativno kritičnih pretnji za imovinu organizacije

OECD (*Organisation for Economic Co-operation i Development*) — Evropska organizacija za ekonomsku saradnju i razvoj

OOM (*Object Oriented Modeling*) — objektno-orijentisano modelovanje

OP (*Proces Area*) — oblast procesa u CMM modelima

PC /Personnal Computer) — lični računar

PCI (*The Payment Card Industry*) — industrija platnih kartica

P-CMM *(Personal Capability Maturity Model)* — model sazrevanja procesa ljudskih kapaciteta

PDCA (*Plan, Do, Check, Act)* — model procesa

PII *(Practice Implementation Indicator*) — indikator implementacije praksi u SCAMPI metodu evaluacije procesa

PIID *(PII Description)* — opis PII u SCAMPI metodu evaluacije

PIP (*Process Improvement Program*) — program za poboljšavanje procesa

PKI (*Public Key Infrastructure*) — infrastruktura sa javnim ključem; sistem asimetrične kriptografije.

PM *(Project Manager)* — menadžer projekta

PP (*Protection Profile*) — profil zaštite u CC standadu

PT (*Poject Team*) — projektni tim

QA *(Quality Assurance)* — predstavnik sistema kvaliteta

RFC (*Request for Comment*) — zahtev za komentar

RFP (*Request for proposal*) — zahtev za predlog, ponudu, klasa u CC standardu

ROSI (*Return on Security Investment*) — povratak investicija u zaštitu informacija

RTM (*Requirements Traceability Matrix*) — matrice za praćenja bezbednosnih zahteva

SA — sistemska analiza

SABSA (Sherwood Applied Business Security Architecture) — framework

SasS (*Software as Service) — Cloud Compiting* ponuda softvera kao servisa

SBC (*Security By Consensus*) — model sistema zaštite sa konsenzusom

SCAMPI (*Standard CMMI Appraisal Method for Process Improvement*) — metod za evaluaciju procesa na bazi CMMI referentnog modela

SCE (*Software Capability Evaluation*) — evaluacija kapaciteta za razvoj softvera

SDLC (*System Development Life Cycle*) — metodologija životnog ciklusa za razvoj sistema

SE (*System Engineering*) — sistemski inženjering ili sistemski pristup

SE CMM (*System Engineering Capability Maturity Model*) — model sazrevanja sistem inženjerskih procesa

SEI (*Software Engineering Institute)* — Institut za inženjerstvo softvera, *Carnegy Mellon* Univerziteta u SAD

SG (*Specific Goals)* — specifični cilj u CMMI modelu procesa

SLA (*Seciruty Level Agreement*) — sporazum o nivou servisa (zaštite)

SLC (Security *Level Sertification*) – bezbednosni nivoi sertifikacije (NIST standarda)

SM *(Senior Manager)* — stariji menadžer

SMF (*Security Menagament Framework*) — okvir menadžmenta zaštite informacija

SMP (*Security Management Program*) — program menadžmenta zaštite informacija

SoA (*Statement of Aplicability*) — izjava o primenljivosti kontrola zaštite u proceni rizika

SOC (*Security Operation Center*) — Centar za bezbednosne operacije

SoC (*Select of Controls*) — izbor kontrola zaštite u tretmanu rizika

SOW (*Statement of Work*) — izjava o radu

SP (*Specific Practice)* — specifična praksa u CMMI modelu procesa (kao BP u SSE CMM modelu)

SQA (*Solution Quality Assurance*) — garantovani kvalitet rešenja

SSAM (*System Security Appraisal Method*) — metod za evaluaciju i poboljšanje procesa na bazi SSE CMM modela sazrevanja procesa zaštite

SSAM PIID — opis PII u SSAM metodu evaluacije

SSE *(System Security Engineering)* — sistemsko inženjerstvo u oblasti zaštite informacija

SSE CMM (*System Security Engineering Capability Maturity Model)* — model i metod sazrevanja procesa zaštite

SSH (*Secure Socket Shell*) — protokol zaštite

ST (*Security Target*) — bezbednosni cilj u CC standardu

S-vektor (*Security Vector*) — vektor zaštite

SW CMM (*Capability Maturity Model for Software Developement*) — model sazrevanja procesa za razvoj softvera

SWG (*Security Working Groop*) — tim za zaštitu informacija

TBD (*to be done*) — treba da se uradi

TCB (*Trusted Computing Base*) — baza poverljivog računarskog sistema

TCMM (*Trusted CMM*) — poverljivi CMM

TCP — protokol na transportnom nivou OSI modela računarskih mreža

TCSEC (*Trusted Computer System Evaluation Criteria*) — kriterijumi za evaluaciju poverljivog računarskog sistema (SAD standard, tzv. „*Orange book*")

TE (E*valuation team*) — tim za evaluaciju u procesima SSAM i SCAMPI metoda evaluacije

TELNET — Internet servis za udaljeni pristup

TEMPEST (*Transient Electro — Magnetic Pulse Surveillance Technology*) — tehnologija za snimanje tranzijentnih elektro-magnetnih (kompromitujućih) impulsa

TLS (*Transport Layer Security)* — protokol zaštite na transportnom nivou

TM *(Technology Managament)* — menadžment tehnologije

TOE (*Target of Evaluation*) — cilj (objekat) evaluacije u CC standardu

TQM (*Tortal Quality Managament*) — menadžment totalnog kvaliteta

TSF *(Target Security Function)* — bezbednosna funkcija objekta evaluacije u CC standadu

TSM (*Trusted Software Methodology*) — metodologija poverljivog softvera

TSP *(Target Security Policy)* — politika zaštite objekta evaluacije u CC standadu

TTPS (*Trusted Third Party Service*) — servis poverljivog provajdera (zaštite)

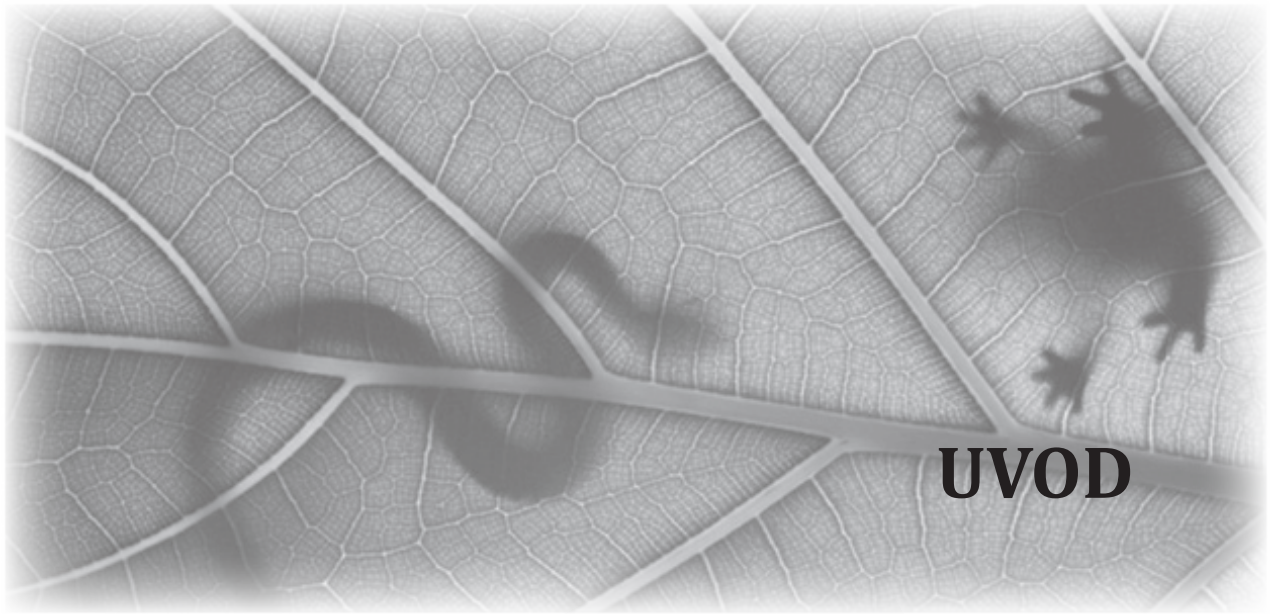
UPSS (*Unbrakable Power Suply System*) — sistem za neprekidno napajanje

VARF (*Vulnerability Assesment Report Format*) — format za izveštavanje procene ranjivosti

VM (*Virtual Machine*) — virtuelna mašina

VMI *(Virtual Machine Introspection)* — virtuelna mašinska introspekcija (forenzički alat)

WBS *(Work Breakdown Structure)* — detaljna struktura rada



UVOD

Bezbednosne potrebe savremenih poslovnih sistema informaciono-komunikacionih tehnologija (IKT sistema), određene su njihovim osnovnim karakteristikama: *globalnim umrežavanjem, velikom složenosti i distribucijom, virtuelizacijom, izdavanjem beta verzija sistemskih, aplikativnih i uslužnih programa i evolutivnim razvojem funkcionalnih i bezbednosnih tehnologija.*

Globalno umrežavanje nebezbednih komponenti i mreža povećava rizik od napada spolja i iznutra, a kompleksnost savremenih poslovnih IKT sistema dodatno povećavaju složeni sistemi zaštite, što otežava razumevanje, modelovanje i projektovanje tih sistema. Trend virtuelizacije klijentske i serverske strane i razvoj distribuiranog Internet računarstva (*Cloud Computing*) zahtevaju novu paradigmu zaštite informacija i IKT sistema. Zbog toga, čak i kada se primeni adekvatan sistem zaštite, efektivnost zaštite obično ostaje nepoznata. Proizvodi i sistemi IKT i zaštite dolaze na tržište posle dugotrajnog i skupog razvoja, *sa evaluacijom ili bez evaluacije*, a jedna od posledica je da korisnici postavljaju nerealne bezbednosne zahteve i definišu neadekvatne bezbednosne ciljeve. Samim tim, koncepti zaštite i tehnička rešenja arhitekture sistema zaštite ne odgovaraju stvarnom stanju bezbednosnog rizika i bitno otežavaju menadžment sistem zaštite informacija.

U skladu sa *procesnim pristupom*, sistem zaštite informacija se može modelovati procesom koji *transformiše* ulazne veličine u očekivano veće (bolje) izlazne veličine. Procesi zaštite *integrišu* i konzistentno disciplinuju relevantne atribute svakog posla u zaštiti informacija – *dobro osposobljene i motivisane ljude, tehnike i alate zaštite* i *metode* za izvršavanje procedura i zadataka zaštite. U *objektno-orijentisanom pristupu* zaštiti informacija, od brojnih atributa informacija (*tačnost, integritet, blagovremenost, trajnost, raspoloživost, poverljivost* itd.), kvalitet informacija u potpunosti zavisi od skupa relativno nezavisnih atributa: *poverljivosti* – da informacije nisu otkrivene neovlašćenim korisnicima; *integriteta* – da informacije nisu neovlašćeno izmenjene i *raspoloživosti* – da su informacije dostupne

legitimnim korisnicima kad god je to potrebno. *Kvalitet informacija*, procesiranih, skladištenih i prenošenih u savremenim, visoko distribuiranim i umreženim IKT sistemima Internet tipa, u potpunosti zavisi od funkcionalne i tehničke pouzdanosti i bezbednosti IKT sistema i njegovog okruženja, odnosno, od implementiranog sistema zaštite. Na taj način, pored zahteva za kvalitet *hardvera* i *softvera, bezbednost* IKT sistema, tj. *kvalitet sistema zaštite* postaje treći gradivni blok sistema kvaliteta poslovnih IKT sistema i poslovnih sistema u celini. Produktivnost savremenih poslovnih sistema u najvećoj meri zavisi od brzine donošenja odluka koja u potpunosti zavisi od *kvaliteta informacija*, koje procesiraju, skladište i prenose umreženi poslovni IKT sistemi.

U ovom udžbeniku, umesto uobičajenih skraćenica **IS** (informacioni sistem) ili **IT** (informacione tehnologije) koristi se termin **IKT[1] sistem** (*sistem informaciono komunikacionih tehnologija*), koji generički uključuje sve atribute i aspekte zaštite informacija: *sistemski, procesni* i *objektno orijentisani* pristup i *informacionu imovinu — čistu* (informacije, podatke, programe), *hardversku* (mrežne, informacione, komunikacione i tehnologije zaštite) i *humanu* (ljude – korisnike i druge relevantne učenike). Termin *„zaštita informacija"* u svakom kontekstu implicira *zaštitu celokupne informacione imovine, uključujući objekte IKT sistema* u celini. Zato se termini *"zaštita informacija" i „zaštita informacione imovine"* u udžbeniku koriste ravnopravno, a u kontekstu se ističe fokus na neposrednu zaštitu informacija ili objekata IKT sistema, sa krajnjim ciljem zaštite informacija koje oni procesiraju, skladište i prenose. Takođe, ravnopravno se koriste termini *„upravljanje"* i *„menadžment"*. Upotreba termina *menadžment* usvojena je u cilju harmonizacije sa standardnom ISO terminologijom u svim *menadžment sistemima* kvaliteta.

Udžbenik je primarno namenjen studentima osnovnih studija, ali i master studentima, korisnicima i menadžerima, koji prvi put ulaze u problematiku upravljanja zaštitom informacija. Mogu ga koristiti i profesionalci u zaštiti i sistemima kvaliteta koji žele sistematizovati i upotpuniti svoja znanja iz ove široke, multidisciplinarne oblasti.

Glavni cilj pisanja ovog udžbenika je da se raznovrsna i obimna teorija, dostupna u brojnoj stranoj literaturi, stručnim časopisima, preporukama, uputstvima, standardima i autorskim radovima na Internetu, sistematizuje, terminološki ujednači i definiše i što više približi korisnicima i menadžerima sistema zaštite koji po pravilu ne moraju biti tehnički obrazovani. Smanjenje kompleksnosti terminologije jedan je od strateških ciljeva teorije i prakse menadžment sistema zaštite informacija, čime se postiže veća razumljivost i korisnička prihvatljivost.

Međunarodna organizacija za standardizaciju (ISO) i Međunarodna komisija za elektrotehniku (IEC) zajedno čine svetski specijalizovani sistem za standardizaciju. Državna tela koja su članovi ISO ili IEC učestvuju u razvoju međunarodnih standarda, posredstvom određenih organizacija koje formiraju tehničke odbore za određene oblasti tehničkih aktivnosti. Tehnički odbori organizacija ISO i IEC sarađuju u domenima od zajedničkog interesa, a deo posla preuzimaju ostale međunarodne, vladine ili nevladine organizacije povezane sa ISO i IEC. Međunarodni standardi formulisani su u saglasnosti sa propozicijama datim u *ISO/IEC Directives, Part 2.*

1 ICT (*Information and Communiccation Technologies*) —zahtev standarda ISO/IEC 13335-2:2002.

U domenu informacionih tehnologija, ISO i IEC imaju formiran udruženi odbor za tehniku — ISO/IEC JTC 1, čiji je glavni zadatak priprema međunarodnih standarda. Kada udruženi tehnički odbor usvoji predlog međunarodnog standarda, daje se državnim telima na usvajanje putem glasanja. Publikovanje međunarodnog standarda zahteva odobrenje od minimalno 75% učesnika (državnih tela). Standard *menadžment sistema zaštite informacija* (ISO/IEC 27001) — ISMS pripremio je ISO/IEC JTC1 potkomitet za tehničke sisteme zaštite — SC 27, odnosno, njegova peta radna grupa (WG5). ISO i IEC upozoravaju da neki od elemenata ovog standard mogu biti autorska dela (patenti), pa se odriču od odgovornosti za bilo koja identifikovana autorska prava.

Metodološki, udžbenik je koncipiran u dvanaest poglavlja. Svako poglavlje sadrži uvod, funkcionalnu razradu, rezime lekcije i pitanja za ponavljanje. U *prvom poglavlju* opisani su osnovni koncepti bezbednosti i zaštite informacija. Metodologija sistemskog inženjerstva i procesi zaštite definisani su u *drugom poglavlju*, a generički metodi poboljšanja procesa – *u trećem*. U *četvrtom poglavlju* data je skraćena istorija razvoja relevantnih standarda kvaliteta proizvoda i sistema zaštite. Sažeta evolucija menadžment sistema zaštite informacija opisana je u *petom poglavlju*. Metodološki zahtevi i zahtevi za *kontrole zaštite* ISMS standarda, definisani su u *šestom poglavlju*, uključujući procesni model PDCA za planiranje, implementaciju, održavanje i poboljšanje ISMS procesa. U *sedmom poglavlju* detaljno su opisane PDCA faza planiranja implementacije ISMS-a i menadžment rizika. Faze PDCA implementacije, provere i poboljšanja procesa ISMS-a, analizirane su u *osmom poglavlju*. Generički okvir programa *menadžment sistema usaglašenosti* (CMP) i programa *menadžment sistema usaglašenosti bezbednosti informacija* (IA CMP), sa komponentom sertifikacije i akreditacije sistema zaštite i ISMS-a, opisani su u *devetom* poglavlju. U poglavljima *deset* i *jedanaest* opisani su funkcionalni model i struktura sazrevanja procesa zaštite (SSE CMM) sa metodom evaluacije (SSAM). Uzorci za izradu relevantnih procedura zaštite dati su u *dvanaestom poglavlju*. Na kraju su dati *prilozi* kao dopuna teorijskoj analizi, spisak ključnih reči i spisak korišćene i šire literature iz oblasti teorije, prakse i standardizacije zaštite informacija.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM



1. KONCEPTI BEZBEDNOSTI I ZAŠTITE INFORMACIJA

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Značaj usvajanja terminologije zaštite
- ☑ Semantičko značenje termina „bezbednost“ i „zaštita“
- ☑ Funkcionalnu zavisnosti „bezbednost -zaštita“ i „bezbednost-pretnje“
- ☑ Definicije „sistema zaštite» i „optimalnog sistema zaštite“
- ☑ Opšti funkcionalni model sistema zaštite
- ☑ Ključne faktore bezbednosnog stanja IKT sistema
- ☑ Neke koncepte nove paradigme zaštite u savremenom web okruženju

1.1. UVOD

Informaciona imovina, koja uključuje čistu *informacionu imovinu, hardversku i humanu imovinu* [56], od suštinskog je značaja za poslovanje organizacije, pa je potrebno da bude odgovarajuće zaštićena i upravljana. Informacija je najznačajniji deo *informacione imovine*. Informacije mogu imati razne oblike i forme. One mogu biti štampane ili pisane na papiru, uskladištene u elektronskom obliku, prenesene putem pošte ili elektronskih sredstava, prikazane na filmu ili videu, ili izgovorene. Informacije u bilo kojem obliku, uskladištene, procesirane ili prenošene, moraju uvek biti odgovarajuće zaštitićene, jer predstavljaju ključni resurs svakog poslovnog sistema.

U ovom udžbeniku termin *bezbednost informacija koristi se u značenju bezbednosti informacione imovine*, gde god to nije eksplicitno navedeno. *Bezbednost informacija* se uspostavlja i održava implementacijom sistema zaštite. Sistem zaštite štiti informacionu imovinu od širokog opsega pretnji, odnosno, od rizika da pretnje iskoriste brojne *ranjivosti* (softvera, hardvera, konfiguracije, ljudi) *IKT sistema*[1] i nanesu štetu samim sistemima i poslovnim procesima, koje ovi sistemi podržavaju. *Misija sistema zaštite* je smanjenje i održavanje rizika poslovanja na minimalnom, prihvatljivom nivou, održavanje kontinuiteta poslovanja i osiguranje maksimuma prihoda od investicija i povoljnih poslovnih prilika.

Bezbednost/sigurnost informacija se postiže implementacijom skupa upravljačkih, organizacionih i tehničkih kontrola zaštite. Menadžment sistem bezbednosti informacija, u okviru totalnog menadžment sistema – TQM (*Tortal Quality Managament*), zahteva da se kontrole zaštite uspostave, implementiraju, nadgledaju, proveravaju i poboljšavaju, da bi se osiguralo ispunjavanje specifičnih bezbednosnih i poslovnih ciljeva i misije organizacije.

1.2 INFORMACIJE I INFORMACIONA IMOVINA

Informacija čini ključni gradivni blok IKT sistema i informacione imovine. Kako ne postoji jedinstvena definicija pojma *informacija*, koja bi zadovoljila sve zahteve, izbor definicije najčešće zavisi od izvora i cilja definicije (tabela 1.1). U kontekstu ovog udžbenika usvojena je definicija: „*Informacija je skup podataka koji korisniku donosi novo saznanje u datom kontekstu*".

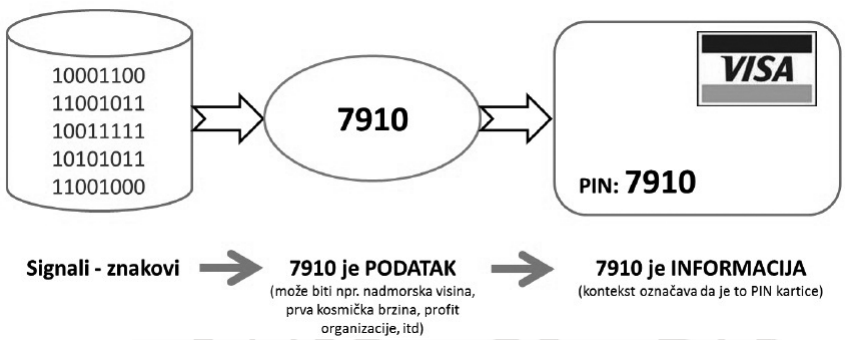
Tabela 1.1 *Definicije pojma informacija u funkciji izvora i cilja*

Izvor/cilj	Definicija informacije
Statistika	Zbir podataka iz kojih se može izvući zaključak.
Teorija komunikacija	Numerička mera nesigurnosti ishoda prenosa signala od 1000 bita.
Tehnika	Uređeni niz simbola, reprezent činjenice (poruke) za primaoca.
Nauka	Rezultat izlaza procesa, samog procesa i ulaza u proces.
Šenonov model	Vrednost izlaza bilo kojeg procesa u hijerarhiji procesa.
Zaštita	Informaciona imovina *koja ima vrednost za* organizaciju.

Informacije su usko povezane s pojmovima: *ograničenja, komunikacije, kontrole, formata, instrukcije, znanja, značenja, mentalnog podražaja, uzorka, percepcije i zastupljenosti.* Informacije mogu imati brojne atribute, kao što su: *vrednost, funkcija, argument, proces, reverzibilnost, poruka, kanal, inverzne funkcije, reprezentacija, percepcija, verovanje, znanje, tačnost, blagovremenost, integritet, raspoloživost, poverljivost, gubitak, pogodnost, nepotpunost i dezinformacije.*

1 Sistem **IKT** (**I**nformaciono **K**omunikacionih **T**ehnologija) – Prema standardu ISO/IEC 13355 iz 2002.

Definicija *informacije* usvojena u oblasti zaštite, znači da je skup podataka stavljen u neki kontekst, dok su sami podaci izvan konteksta, odnosno, podatak je beskoristan sve dok ne prenosi neku informaciju korisniku. Informacija je primljena i shvaćena poruka, koja je rezultat procesiranja, manipulacije i organizovanja podataka koji donose novo saznanje korisniku. Na slici 1.1 je prikazan odnos podataka i informacije.



Slika 1.1. Primer odnosa podataka i informacije [2]

Informacioni ili IKT sistem je uređen, dokumentovan skup *resursa*, *pravila* i *mernih metoda*, koji zadovoljava ulazne zahteve za manipulaciju sa podacima i dobijanje traženih izlaznih informacija, odnosno, zadovoljenja ulaznih zahteva. *Informacije,* procesi za podršku, računarski sistemi i mreže i ljudi koji ih koriste, predstavljaju najvažniju imovinu organizacije. Procesi definisanja, implementacije, održavanja i poboljšavanja *bezbednosti informacija*, mogu imati presudan značaj za održavanje konkurentnosti na tržištu, finansijsku zaštitu, rentabilnosti rada i ugled organizacije.

1.3 INFORMACIONA IMOVINA KAO OBJEKAT ZAŠTITE

Osnovna *strukturna obeležja* savremenih IKT sistema sa (pod)sistemom zaštite su visoka kompleksnost i teritorijalna distribucija računarskih mreža u intenzivnoj zaštićenoj komunikaciji sa računarskim sistemima. U *objektno orijentisanom pristupu* smanjenje kompleksnosti postiže se uvođenjem dve *grane objekata* [22]:

- *informacione imovine***:** *poverljivosti (**C**), integriteta (**I**) i raspoloživosti (**A**) ili **CIA**,* čime se struktuiraju *bezbednosni ciljevi,* tj. objekti koje treba štititi i
- *mera i sredstava zaštite*: *proceduralne* (upravljačke i operativne) i *tehničke kontrole* zaštite, čime se struktuiraju mehanizmi i protokoli zaštite.

U objektno orijentisanom pristupu pod *zaštitom informacija* podrazumeva se zaštita *informacione imovine*: *čiste, fizičke* i *humane* (tabela 1.2) [56, 57].

2 Adelsberger Z., *Značaj ocjene rizika kod umreženih informacijskih sistema,* doktorski rad u pripremi, Univerzitet Singidunum, 2010.

Tabela 1.2 *Klasifikacija informacione imovine*

Čista informaciona imovina	
Digitalni podaci i informacije	personalne, finansijske, zakonske, istraživačke i razvojne, strateške i komercijalne, e-pošte, *voice*-mail, baze podataka, lični i deljeni folder, *backup* mediji – trake/CD/DVD i digitalna arhiva, šifarski ključevi, lozinke...
Opipljiva informaciona imovina	personalna, finansijska, zakonska, istraživanje i razvoj, strateške i komercijalne, poštanske pošiljke, faksovi, mikrofiš i drugi bekap/arhivirani materijali, ključevi skladišta medija, žurnala, magacina, knjiga ...
Neopipljiva inf. imovina	znanje, poslovni odnosi, trgovačke tajne, licence, patenti, iskustva, brend, reputacija, poverenje, konkurentnost, etika, produktivnost,
Aplikativni program	razvijeni u organizaciji/kastomizovani, klijentski, komercijalni, *midleware,* uslužni i programi za e-poslovanje, ERP sistemi, baze podataka ...
Sistemski programi	za servere, desktop i *mainframe* računare, mrežne uređaje, priručne i ugrađene računare (uključujući BIOS ROM i druge *firmware),*
Fizička informaciona imovina	
Infrastruktura za podršku IKT sistema	zgrada za smeštaj, sobe i sefovi za čuvanje EM i optičkih diskova, uređaji za identifikaciju i autentifikaciju (kartični sistemi za pristup, tokeni, smart kartice itd.), uređaji za tehničku zaštitu (CCTV, protivprovalni sistemi itd.),
Kontrole okruženja IKT sistema	protivpožarni alarmi/sistemi za gašenje požara/protivpožarni aparati, jedinice za neprekidno napajanje (UPSS), mrežno napajanje, mrežni transformatori/ atenuatori, klima uređaji, alarmni sistemi za poplavu itd.
Hardver IKT sistema	serveri, računari (PC, radne stanice, laptop, *mainframes*...), modemi i linijski terminatori, komunikacioni uređaji, printeri/kopir/fax mašine itd.
Imovina IKT sistema	autentifikacioni servisi i administrativni procesi za korisničke naloge, pretraživači, *firewalls*, mrežni i web servisi, antivirusni programi, e–mail itd.
Humana informaciona imovina	
Zaposleni	zaposleni, menadžment, dizajneri/programeri/evaluatori programa, menadžer i administrator zaštite, operateri, korisnici sa privilegijama itd
Nezaposleni	privremeno zaposleni, konsultanti, specijalisti po ugovoru, partneri itd.

1.4 BEZBEDNOST I ZAŠTITA INFORMACIJA

Termini *bezbednost informacija ili informaciona bezbednost,* podrazumevaju primarno bezbednost informacija i podataka u IKT sistemu, a sekundarno — *bezbednost informacione imovine*, čime se posredno štite informacije, kao njen najvredniji deo. Ovakav pristup implicira da je krajnji cilj bezbednosti informacione imovine – *zaštita informacija i podataka*, koja se

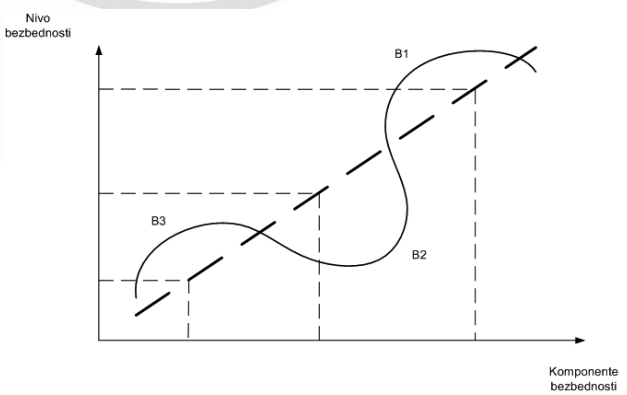
direktno ili posredno postiže zaštitom svih komponenti *informacione imovine*. U stranoj literaturi se koriste različiti termini (eng. *information security*; rus. *безопасност информации;* nem. *Informations–sicherheit),* a u ovom udžbeniku se ravnopravno koriste termini *bezbednost informacija i informaciona bezbednost*, koji *uvek* impliciraju bezbednost *informacione imovine* u celini.

Bezbednosti informacija u praksi zaštite ima više definicija, zavisno od nivoa apstrakcije. Na nivou države to je *stanje zaštićenosti nacionalnih interesa u informacionoj sferi, određenih skupom ličnih, poslovnih i državnih interesa* ili *zaštićenost informacija od slučajnih ili namernih aktivnosti prirodnog ili veštačkog karaktera, koje mogu naneti neprihvatljivu štetu informacionoj imovini organizacije*. *Bezbednost informacija* je *objektivna mera stanja rizika ili stanja bezbednog, pouzdanog i neometanog funkcionisanja IKT sistema, u odnosu na samog sebe i svoje okruženje* [30]. Dakle, sistem se smatra bezbednim, ako je *zaštićen* od uticaja rizika.

Sigurnost informacija je sinonim *bezbednosti informacija*, a semantički predstavlja *subjektivnu meru poverenja* ili osećaja sigurnosti da je sistem bezbedan. Oba termina – *bezbednost* i *sigurnost*, zasnivaju se na mehanizmu ljudske percepcije *poverenja*. Informaciona imovina se smatra objektivno *bezbednom,* ako je *do određenog stepena pouzdano poznato* da zaista poseduje neka bezbednosno relevantna svojstva, koja nominalno poseduje, a *sigurnom* — ako se *do određenog stepena veruje* da ima neka bezbednosno-relevantna svojstva koja nominalno poseduje. U oba slučaja termin *do određenog stepena* indicira relativnost definicija ovih pojmova. *Garantovana bezbednost* semantički najbliže odgovara značenju engl. termina *Security Assurance.*

Generalno, ukupna bezbednost nekog složenog sistema obuhvata neki skup *komponenti bezbednosti (B1, B2...Bn)*. Nivo ukupne bezbednosti sistema – **Bu** raste sa porastom nivoa bezbednosti njenih *relativno nezavisnih* komponenti, čiji se skupovi uticaja negde presecaju, ali približno aditivno doprinose porastu ukupne bezbednosti. U idealnom slučaju, da je bezbednost deterministička veličina, ova bi zavisnost bila linearna funkcija, ali je uvek *nelinearna*, zbog stohastičke prirode kombinovanih, dinamički promenljivih pretnji i neodređenosti faktora rizika, koji utiču na bezbednost (slika 1.2) [30].

Najveći uticaj na Bu, npr. države, imaju najosetljivije komponente – *državna, vojna, ekonomska i informaciona* bezbednost. Kako se razvija informatičko društvo, u toj meri raste značaj *informacione bezbednosti kiber prostora*. Uobičajeno se *bezbednost* IKT sistema poistovećuje sa *bezbednošću informacija ili informacione imovine*. Osnovna razlika je u pristupu i metodologiji zaštite. U objektno orijentisanom pristupu, bezbednost



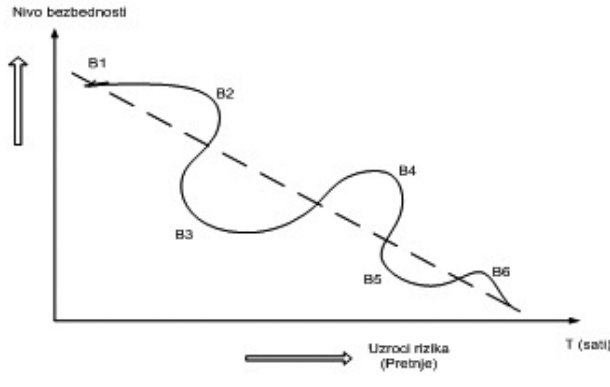
Slika. 1.1. Nivo ukupne bezbednosti u funkciji komponenti bezbednosti

informacija se odnosi na zaštitu ključnih, relativno nezavisnih atributa informacija: *poverljivosti, integriteta i raspoloživosti* – **CIA** (*Confidenciality, Integrity, Avialability*), bez obzira na formu u kojoj se informacija nalazi, dok se bezbednost IKT sistema odnosi na zaštitu **CIA** informacija koje se skladište, obrađuju ili prenose u IKT sistemu [38].

Bezbednost informacija je kritičan faktor za kontinuitet poslovanja; smanjuje potencijalnu štetu, obezbeđuje povratak investicije i unapređuje ukupno poslovanje organizacije. U tom smislu se bezbednost informacija može definisati kao *odsustvo rizika za CIA informacija* ili *zaštićenost informacija od neovlašćenog otkrivanja, izmene ili nedostupnosti* [10]. U praksi se bezbednost informacija najčešće manifestuje u bezbednom radu bez otkaza, malicioznih programa i prisluškivanja u bezbednoj komunikaciji, kupovini i plaćanju preko Interneta sa zaštitom privatnosti. Dakle, bezbednost informacija nije odredište, nego *ciklično ponovljiv proces* stalnog održavanja zaštićenosti informacija, kojeg je potrebno *planirati, implementirati, izvršavati, održavati i poboljšavati,* kroz uspostavljen *menadžment sistem bezbednosti informacija* – ISMS (*Information Security Management System*) [52].

1.5 FAKTORI UTICAJA NA BEZBEDNOST INFORMACIJA

Informaciona imovina organizacije je izložena brojnim bezbednosnim pretnjama iz širokog opsega izvora, uključujući maliciozne zloupotrebe računara, špijunažu, sabotažu, vandalizam, požar, poplavu i druge vanredne događaje. Zlonamerni napadi hakera, malicioznih programa i odbijanja servisa (DoS/DDoS) sve su češći, intenzivniji i sofosticiraniji. *Agenti* potencijalnih pretnji su izvršioci *napada* i uzroci nastanka faktora rizika. *Rizik* je procenjena mera uticaja pretnje na informacionu imovinu i osnovna kategorija analize bezbednosti informacija, a može se definisati i kao *verovatnoća da će agent pretnje iskoristiti neku ranjivost sistema i izazvati negativne posledice (štetu) za informacionu imovinu organizacije*. Kako apsolutna bezbednosti praktično ne postoji[3], menadžment bezbednosti informacija najbolje se objašnjava procesom *menadžmenta rizika*. U realnim uslovima, sa porastom pretnji povećavaju se rizici, a nivo ukupne bezbednosti nelinearno opada, zbog stepena neodređenosti uticaja faktora rizika (slika 1.3) [30].



Slika 1.3. Nivo ukupne bezbednosti informacija u funkciji pretnji

Bezbednost informacija je dinamičko stanje, proces i specifično — situacioni

3 Apsolutna bezbednost u praksi postoji ako su na raspolaganju **neograničeni resursi** za zaštitu, što je praktično neizvodljivo.

problem realnog okruženja, pa ne postoji univerzalno i nepromenljivo stanje bezbednosti. Bezbednost informacija podjednako je važna za zaštitu kritičnih infrastruktura i poslovanje u javnom i u privatnom sektoru, gde funkcioniše kao mehanizam koji omogućuje, npr. uspostavljanje elektronske uprave ili elektronskog poslovanja, a da se izbegnu ili umanje odgovarajući rizici. Povezivanje javnih i privatnih mreža i zahtevi za zajedničko korišćenje informacionih resursa, otežavaju ostvarivanje logičke kontrole pristupa. Takođe, trend distribuiranog rada i virtuelizacije računara (npr. *Cloud Computing* — CC) slabi efikasnost centralizovanog menadžment sistema i specijalističke kontrole sistema zaštite.

Na bezbednost informacija utiču brojni, manje očigledni faktori, od kojih su najznačajniji: *funkcionalni zahtevi poslovnih sistema* (npr. e-poslovanje, CC), *organizaciona struktura* (npr. promena prava pristupa, zbog promene posla), *tehnološki razvoj* (npr. problem zaštite u CC okruženju), *politika zaštite* (npr. nedostatak *menadžment okvira zaštite* — SMF[4]), *svest o potrebi zaštite* (npr. implementacija tehnologije zaštite bez procene rizika*), kompleksnost i skalabilnost sistema* koja otežava postizanje koherentnog sistema zaštite, *poverljivost i privatnost* (npr. problem prenosa poverenja u IKT okruženju) i drugi faktori [86, 22].

U poslovnom sistemu za podršku odlučivanja, potrebne su k*valitetne i integrisane informacije* koje postaju najznačajniji resurs svake organizacije i kritični objekat zaštite. Izvršni menadžeri rangiraju zaštitu informacija sa 7,5 od 10, po značaju za funkcionisanje IKT sistema [25]. Na *kvalitet informacije* utiče niz njenih atributa, koji pojedinačno mogu biti od relativnog značaja za različite poslovne sisteme. Zato se ukupan kvalitet poslovnih IKT sistema često ilustruje trouglom stabilnosti — *hardvera, softvera i bezbednosti***.** Sa porastom informatizacije svih sfera života raste značaj *kvalitetnih informacija*, koje u velikoj meri obezbeđuje *sistem kontrola zaštite*.

Činjenica da je vrednost informacija funkcija vremena (tj. informacija značajna danas ne mora biti značajna i sutra), presudno utiče na način zaštite informacija. Na primer: informacije, koje obezbeđuju komparativnu prednost za duži vremenski period, treba štititi jakim kriptološkim mehanizmima zaštite. Otuda i potreba za razvoj realnih metoda za procenu rizika, kompatibilnih sa dinamikom savremenog e-poslovanja.

Zbog čestih *organizacionih* promena, pod uticajem brojnih ekonomskih i tehnoloških faktora, osnovni problem je kako obezbediti specijaliste zaštite sa potrebnim znanjima i veštinama i izvršne menadžere, koji najbolje poznaju poslovne procese, identifikuju faktore rizika, određuju prava pristupa, upravljaju sistemom zaštite itd.

Tehnološki razvoj pomera težište sa automatizacije poslovanja na *integraciju tehničkih* i *menadžment sistema* kompleksnih procesa, što otežava administraciju zaštite informacija, koju je vrlo teško potpuno automatizovati i integrisati. Zato uloga čoveka u sistemu bezbednosti informacija, ostaje nezamenljiv i kritičan faktor.

Kompleksnost savremenih, heterogenih, visoko distribuiranih IKT sistema, glavni je problem za planiranje arhitekture sistema zaštite, zbog teškoća identifikovanja i korekcije ranjivosti. Razvojem *web* servisa i aplikacija[5], IKT i Internet umrežavanja, generisani su sasvim novi tipovi pretnji, koje zahtevaju razvoj novih *modela, procesa* i *kontrola* zaštite.

U većini organizacija procesi zaštite su nedovoljno razvijeni i stabilni i aksiomatski zavise od predefinisane *politike zaštite* i procene stepena izloženosti faktorima rizika na bazi

4 Engl.: SMF – *Security Menagament Framework.*

5 SOA, mrežno računarstvo (*Greed Computing*), distribuirano Internet računarstvo (*Cloud Computing*).

statičkog okvira ISMS standarda[6] za menadžment sistem zaštite, operativnih uputstava i tehničkih kontrola zaštite. Relevantni standardi zaštite identifikuju sva ograničenja sistema zaštite, projektovanog na bazi predefinisane *politike zaštite* i sugeriše regularnu *procenu rizika,* koja se uzima kao primarni alat za donošenje odluka, što ne umanjuje značaj *menadžment okvira* (SMF) na bazi politike zaštite [51, 53, 54, 86]. Naprotiv, SMF treba redovno koristiti, ali samo češće kontrolisati njegovu relevantnost u realnom kontekstu i na bazi procene rizika.

Veći problem je nedostatak svesti menadžera o potrebi procene rizika, koji češće implementiraju tehnologije zaštite bez procene rizika, kao i krajnjih korisnika koji nedovoljno shvataju potrebu kontrole i posledice uticaja rizika na dnevne aktivnosti. Forsiranje primene tehničkih rešenja zaštite, može stvoriti iluzija da se rizik uspešno kontroliše i da bezbednost zavisi od primene sve novijih alata. Iako u zaštiti informacija dominiraju tehnički fenomeni, treba izbegavati projektovanje arhitekture sistema zaštite samo na bazi tehnologije i standarda najbolje prakse zaštite. Racionalan pristup obezbeđuje samo razumevanje *realnog rizika* i njegovog relativnog značaja za organizaciju.

Na praksu zaštite informacija, glavni uticaj imaju: *kompleksnost, skalabilnost, poverljivost i privatnost*. *Kompleksnost* zahteva duboko razumevanje principa funkcionisanja IKT sistema, da bi se implementirao koherentan sistem zaštite. *Zahtev za skalabilnost* (nadogradivost) raste uporedo sa porastom kompleksnosti, distribuiranosti i umrežavanja IKT sistema, što automatski zahteva analizu modularnosti i mogućnosti integracije. *Poverljivost i privatnost* su dva ključna pitanja koja dramatično rastu sa povećavanjem broja umreženih aplikacija i primene IKT sistema, servisa i aplikacija. Modeli autentifikacije (verifikacije identiteta) postali su tehnički najkompleksnija oblast zaštite savremenih IKT sistema u Internet okruženju, pošto su jedini mehanizmi koji mogu rešiti istovremeno probleme uzajamnog poverenja i zaštite privatnosti korisnika. Zahtevi za zaštitom privatnosti i poverljivosti ličnih podataka rastu uporedo sa lakoćom sa kojom se elektronske informacije mogu skladištiti, prenositi, menjati i distribuirati. U većini zemalja u svetu doneti su zakoni za zaštitu privatnosti ličnih podataka u elektronskom okruženju[7], dok se pristup ovom problemu bitno razlikuje od zemlje do zemlje [78, 93]. U sekciji *Osam izveštaja privremenog komiteta evropskog parlamenta* navodi se da: „*Svaki akt koji uključuje intercepciju komunikacija i čak snimanje podataka od strane obaveštajnih službi za obaveštajne namene, predstavlja ozbiljno kršenje lične privatnosti*". Međutim, porast terorizma u svetu i kompjuterskog kriminala nameću potrebu, da se izbalansiraju prava zaštite privatnosti i potrebe država da imaju pristup svim informacijama.

Generalno, pored uticaja navedenih inherentnih faktora, bezbednost informacija ugrožavaju brojne interne i eksterne pretnje i vanredni događaji.

Primer: u prvom kvartalu 2011. godine hakeri su dnevno na Internetu generisali 73.000 novih, sofisticiranih maliciozni programa, od koji oko 40% promeni svoju definiciju u prva 24 časa[8].

Bezbednost realnog IKT sistema zavisi od toga *šta sistem treba da radi* (specifikacija/politika), *kako to radi* (implementacija/mehanizmi zaštite), *da li stvarno to radi* (tačnost/garantovana bezbednost) i *može li sistem preživeti sofosticirane napadače* (ljudska priroda)[9].

6 Standard ISO/IEC 27001:2005
7 Engl.: *Top Ten Gudelines to Workplace privacy,* SAD, *2001.*
8 Engl.: *The Help Net Security News*, 17. maj 2011.
9 Engl.: Stamp, M., *Information Security: Principles and Practice,* JohnWiley & Sons, Inc. 2006.

Održavanje stanja bezbednosti IKT sistema, u nebezbednom Internet okruženju, treba da bude *stabilan (zreo) proces*.

1.6 OPŠTA DEFINICIJA SISTEMA ZAŠTITE

Bezbednost informacija u nebezbednom Internet okruženju, omogućava *sistem zaštite*. Rentabilan sistem zaštite se dobro opisuje i definiše *strukturnim i objektno orijentisanim* modelom. Fokus menadžment sistema zaštite je na *menadžment rizika* i izbor *kontrola zaštite* za ublažavanje tog rizika. Kako je za svaku organizaciju *profil rizika* specifičan, primena *standarda najbolje prakse zaštite informacija* ne daje uvek najbolje rezultate, jer ne uzima u obzir specifičnosti rizika organizacija. Dakle, *optimalni sistem* zaštite informacija znači *rentabilan* i *adekvatan* sistem zaštite za dato poslovno okruženje, specifičan profil rizika i prihvatljive troškove zaštite.

U objektno-orijentisanom pristupu, sistem zaštite se može definisati kao *organizovan i koherentan skup upravljačkih* **(U),** *operativnih* **(O) i** *tehničkih* **(T)** *kontrola zaštite i njihovih veza i ograničenja, primenjenih na IKT sistem, da bi se zaštitila raspoloživost, poverljivost i integritet, procesiranih, uskladištenih i prenošenih podataka i informacija i održao ili povećao nivo bezbednosti i pouzdanosti funkcionisanja IKT sistema u izvršavanju poslovnih ciljeva i misije organizacije* [OZI]. Ova definicija nedvosmisleno implicira da sistem zaštite informacija nije sam po sebi cilj, nego da je u funkciji pouzdanog funkcionisanja IKT sistema u izvršavanju poslovnih ciljeva i misije organizacije. Međutim, brojni IKT sistemi nisu projektovani tako da budu bezbedni. Bezbednost koja se može ostvariti *tehničkim* sredstvima je ograničena i treba je podržti odgovarajućim proceduralnim (**U, O**) kontrolama zaštite. Identifikovanje i izbor kontrola zaštite za implementaciju, zahteva pažljivo i detaljno planiranje. Za menadžment sistem zaštite informacija u organizaciji, zahteva se učešće svih zaposlenih, ali i isporučioca, poverljivih provajdera servisa zaštite (TTPS[10]), korisnika ili drugih spoljnih saradnika.

Suština je da organizacija identifikuje svoje *bezbednosne zahteve* iz *procene operativnog rizika, socijalno-kulturnog okruženja, zakona i ugovora i posebnog skupa principa, ciljeva i poslovnih zahteva za obradu informacija*. Na bazi bezbednosnih zahteva definišu se *bezbednosni ciljevi*. Procenu rizika potrebno je ponavljati periodično kako bi se uključile izmene koje bi mogle uticati na povećanje rizika. Troškovi *kontrola* zaštite za smanjenje rizika treba da su proporcionalni šteti, koja bi mogla nastati kao rezultat otkaza sistema zaštite.

Za analizu i razvoj *sistema zaštite* najbolje rezultate daje metodologija *sistem inženjerske analize* (SA), *objektno-orijentisanog modelovanja* (OOM) i *procesnog pristupa*, čija je glavna prednost smanjivanje kompleksnosti [22]. Definisanje modela IKT sistema i određivanje objekata koje treba štititi na bazi procene rizika, prva je faza razvoja sistema zaštite za životni ciklus IKT sistema.

Osnovni bezbednosni zahtevi za sistem zaštite informacija su sprečavanje: *ugrožavanja bezbednosti ličnosti, organizacija i države; krađe, pronevere, gubitaka i izmene informacija; neovlašćenih aktivnosti u IKT sistemu; povreda intelektualne svojine, privatnosti i poverljivosti ličnih i poslovnih podataka*.

10 Engl.: TTPS – *Trusted Third Party Service.*

Sistem zaštite informacija je *podsistem* IKT sistema i postaje najvažnija komponenta razvoja savremenih IKT sistema, svih tipova i namena; integriše se u IKT sisteme kroz opšte funkcionalne komponente sistema ili dodatne komponente i posebne kanale, koji spajaju elemente jednog sistema sa drugim. Normalno, IKT sistemi se uglavnom zasnivaju na standardnim hardversko–softverskim proizvodima. Mehanizmi i protokoli zaštite, koji za svoj rad koriste funkcije IKT sistema, u velikoj meri zasnivaju se na tehničkoj pouzdanosti IKT sistema. Standardi zaštite preporučuju da se sistem zaštite projektuje paralelno i u toku razvoja prve faze životnog ciklusa IKT sistema, a implementira u fazi implementacije samog sistema za sve faze životnog ciklusa.

U procesima definisanja bezbednosnih ciljeva, planiranja i projektovanja sistema zaštite, u prvom koraku treba razmatrati bezbednosno relevantne komponente IKT sistema: *mrežnu arhitekturu, topologiju, infrastrukturu*, *protokole*, *servise*, *kvalitet servisa, platforme* i *aplikativne programe* (tabela 1.3) [22].

Tabela 1.3 *Relevantni aspekti zaštite IKT sistema*

Aspekti zaštite	Objekti zaštite za analizu
Ključne karakteristike IKT sistema	vrsta komunikacionih veza i uređaja i procesi upravljanja, kompleksnost formalnog opisa IKTS, raznorodnost i prostorna distribucija komponenti IKTS, vrste prezentacije servisa, upravljanje procesima i umrežavanje;
Servisi IKT sistema	uspostavljanje veze, predaja podataka, obrada podataka udaljenim pristupom, prenos datoteka, e-pošta, pristup distribuiranim bazama i dr.
Kvalitet servisa IKT sistema	*ukupan broj veza* – potencijalna sposobnost uspostavljanja međusobnih veza korisnika i distribuiranih objekata sistema;
	vremenska karakteristika – brzina isporuke servisa korisnicima na bazi srednjeg vremena pristupa (zavisi od veličine, udaljenosti i opterećenja);
	srednje vreme isporuke servisa – vreme utrošeno na obradu zahteva korisnika u nekom režimu rada sistema;
	pouzdanost servisa – verovatnoća rada sistema bez otkaza;
	vernost prenosa, pohranjivanja i integriteta informacija, određena brojem sistemskih grešaka i pristupnih tačaka informacijama i podacima.

1.7 OSNOVNE FUNKCIONALNOSTI SISTEMA ZAŠTITE

Osnovne funkcionalnosti sistema zaštite izvršavaju se kroz *servise, mehanizme, kontrole* i *funkcije zaštite*. U praksi zaštite stanje bezbednosti IKT sistema se održava na prihvatljivom nivou rizika sa implementiranim U, O i T kontrolama zaštite [12]. Funkcije zaštite se izvršavaju kontrolama (*mehanizmima* i *protokolima*) zaštite, koje u logičkom smislu predstavljaju način realizacije *servisa zaštite* [105, 82].

1.7.1 Servisi zaštite

Servisi zaštite su logičke aplikacione jedinice, koje se izvršavaju kroz različite akcije, kao što su *metodi za implementaciju operacija kontrola zaštite*, *funkcionisanje ili transformisanje bezbednosnih funkcija*, *implementacija skupa politika zaštite, rukovanje mehanizmima zaštite, ažuriranje, dodavanje, modifikacija sa novim rešenjima zaštite itd.* Servis zaštite je proces ili neprekidna, ponovljiva aktivnost, izvršena funkcijama mehanizama i protokola zaštite. Korisnike ne zanima kako su servisi zaštite implementirani, već da li mogu da izvrše željenu akciju [105].

Primer: *zaštita tajnosti informacija* u komunikacionom kanalu je servis zaštite u IKT sistemu, a algoritamska *kriptografska transformacija* sadržaja informacija (npr. IPSec) je mehanizam za realizaciju tog servisa zaštite.

1.7.2 Mehanizmi i protokoli zaštite

Mehanizmi i protokoli zaštite su individualni algoritmi, hardversko-softverski moduli ili metodi za izvršavanje bezbednosnih funkcija. Neki mehanizmi zaštite su za jedan, a neki za više različitih servisa (npr. *kriptografski* mehanizmi). *Za* realizaciju mehanizma zaštite, potrebno je obezbediti određene *kontrolne strukture*, koje mogu biti *upravljačke, operativne i tehničke,* a uobičajeno se nazivaju *kontrole zaštite*.

Primeri mehanizama zaštite računarskih sistema i mreža su, za logičku kontrolu pristupa: antivirusni programi, skeneri, logičke barijere (*firewalls),* IDPS (sistemi za detekciju i sprečavanje upada u računarski sistem/mrežu), simetrični/asimetrični kriptološki mehanizmi itd. [30].

Standardni mrežni protokoli obezbeđuju dobru funkcionalnost, ali pokazuju i određene ranjivosti (tabela 1.4).

Tabela 1.4 *Mrežni protokoli sa poznatim ranjivostima*

Protokol	Osnovne ranjivosti
FTP	Nema kriptozaštitu, izlaže korisničko ime, lozinke i podatke u OT.
TELNET	Ranjiv na preplavljivanje bafera, povratni odgovor i *spoofing* za dobijanje privilegija i otkrivanje lozinke.
HTTP	Više ranjivosti u raznim implementacijama; slaba konfiguracija HTTP servera omogućava eskalaciju privilegija.
LDAP i MS *Directory Services*	Neke implementacije su podložne preplavljivanju bafera i DoS napadima sa mogućnošću izmene privilegija.
SNMP	Mogući DoS napadi i preplavljivanje bafera, ako ostane ime organizacije i dr. podaci u predefinisanoj konfiguraciji; može omogućiti eskalaciju privilegija i kompromitaciju.
SSH (*Secure Socket Shell*)	Kada protokol radi pod nalogom ruta, mogući su DoS napadi, eskalacija privilegija i kompromitacija.
DNS	Više bezbednosnih ranjivosti u raznim implementacijama.

Zaštita mrežne infrastrukture deo je rešenja ovog problema, ali ne obuhvata mogućnost da neovlašćeni korisnik može koristiti svoju opremu za pristup mreži i aktivirati *snifer* (skener prisluškivač) ili sličan alat za kontrolu saobraćaja u računarskoj mreži. Takođe, ne može se, u bežičnim (WLAN) mrežama ili na Internetu, verovati u mehanizme zaštite drugih korisnika. Zato je neophodno ugraditi mehanizme zaštite u sam proces razmene podataka i elektronskih transakcija. Uobičajen način, da se ovo uradi, je korišćenje standardnih *autentifikacionih protokola,* koji čine posebnu oblast mrežnih protokola [14, 86].

Autentifikacioni protokoli se, uglavnom, zasnivaju na konceptu *upita – odgovora* ili razmene *digitalnih sertifikata*, npr. *NeedhamSchroeder* protokol u *Kerberos* sistemu, *Windows NT 4.0* i kasnijih *OS*. Osnovna ideja je da sistem zahteva dokaz o identitetu, a korisnici inicijalno koriste neki drugi mehanizam za razmenu kriptografskih ključeva. Kada korisnik zahteva pristup, identifikuje se sistemu, koji odgovara sa slučajnim upitom (*chalange*). Korisnik šifruje ovaj upit, koristeći svoj tajni ključ i šalje nazad sistemu, koji koristi matematički par istog ključa (javni ključ korisnika) za dešifrovanje originalne informacije. Ako je korisnik jedina osoba, koja poseduje tajni ključ, neophodan za šifrovanje slučajnog upita sistema, ovo je verifikacija identiteta. Ako upit nije slučajna vrednost, zlonamerni korisnik ga može presresti, lažno se predstaviti i izdati novu vrednost upita korisniku, primiti transformisani odgovor i obezbediti pristup ciljnom sistemu. Treba uočiti da autentifikacija nije isto što i uspostavljanje bezbedne sesije i da svaka konekcija, koja ne koristi dodatne mere zaštite, kao što su mehanizmi za šifrovanje ili zaštitu integriteta, može biti kompromitovana. U jednostavnom slučaju, proces autentifikacije korisnika uključuje unošenje lozinke preko uspostavljene bezbedne sesije, pomoću **SSL** (*Secure Socket Layer*) protokola u višeslojnoj arhitekturi računarske mreže (slika 1.4).



Slika 1.4 Lokacija SSL protokola u višeslojnoj arhitekturi računarske mreže

Ovaj metod autentifikacije često se koristi za pristup *web* aplikacijama na Internetu. SSL je osnovni protokol za zaštićen prenos lozinke, a obezbeđuje autentifikaciju servera klijentu, klijenta serveru i uspostavu bezbedne, kriptološki zaštićene, sesije između klijenta i servera. Osnovni element za dokazivanje autentičnosti kod SSL protokola je *digitalni sertifikat,* koji izdaje sertifikaciono telo – CA (*Certification Authority*). Digitalni sertifikati, između ostalog, sadrže javne ključeve entiteta, koji ih razmenjuju. Programska podrška za upravljanje SSL protokolom na računaru klijenta/servera (npr. *MS Outlook*) proverava valjanost digitalnog sertifikata datog servera/klijenta. Svi podaci koji se razmenjuju između klijenta i servera se šifruju na računaru pošiljaoca, a dešifruju na računaru primaoca, čime se vrši zaštita poverljivosti sesije. Podaci se pre slanja digitalno potpisuju i na taj način se postiže zaštita integriteta podataka sesije [107].

SSL protokol koristi dva potprotokola: (1) *SSL protokol zapisa poruka* (*SSL record protocol*), koji definiše formate poruka za prenos podataka i (2) *SSL protokol dogovaranja parametara sesije* (*SSL handshake protocol*), koji se koristi za razmenu poruka, sastavljenih prema prvom potprotokolu, između SSL klijenta i SSL servera, kada se prvi put uspostavlja veza. SSL protokol podržava više kriptografskih algoritama za autentifikaciju klijenta i servera, razmenu digitalnih sertifikata i uspostavu tajnih simetričnih ključeva (tj. ključeva sesije) kao što su: *DES, DSA, KEA, MD5, RC2 i RC4, RSA, RSA key exchange, SHA–512, Triple–DES*. Algoritmi za razmenu ključeva, *KEA* i *RSA key exchange*, određuju način na koji klijent i server dogovaraju simetrični ključ, koji će koristiti u SSL sesiji. U najvećem broju slučajeva koristi se *RSA key exchange* algoritam. Tokom uspostavljanja SSL sesije, odnosno u fazi dogovaranja kriptografskih parametara, klijent i server biraju najjači skup kriptografskih algoritama, koji oba istovremeno podržavaju i koriste tokom SSL sesije. SSL sesija između klijenta i servera uvek započinje razmenom poruka SSL protokola dogovaranja parametara sesije, koji omogućava korisniku da izvrši autentifikaciju servera, primenom PKI metoda, a klijentu i serveru da zajedno učestvuju u generisanju i izboru simetričnog tajnog ključa sesije, koji se koristi za šifrovanje, dešifrovanje i digitalno potpisivanje poruka tokom SSL sesije. Ako server to zahteva, SSL protokol dogovara parametre sesije i omogućava da i server izvrši autentifikaciju klijenta.

Autentifikacioni SSL protokoli dopuštaju napad ubacivanjem čoveka u sredinu i uticaj na većinu servera na Internetu. Ranjivost omogućava da se napadač ubaci u SSL protokol na komunikacionom putu. Pri tome ni *web* server ni *web* pretraživač ne mogu otkriti da je sesija oteta. Ranjivost dolazi u standardu protokola, formalno poznatog kao TLS — (*Transport Layer Security*). Većina SSL implementacija je ranjiva na neki način. Scenario napada uključuje korisnika koji plaća *online* račune, banku koja koristi protokole zasnovane na *web* servisima i druge aplikacije kao što su *mail* serveri, serveri baza podataka itd. Sve biblioteke SSL treba bezbednosno popraviti.

Autentifikacioni uređaji (*smart kartica, biometrijski uređaj, token)* obezbeđuju korisniku neki fizički identifikator, koji se zahteva za kompletiranje autentifikacije.

Protokoli zaštite na prenosnom putu podrazumevaju kriptološke mehanizme zaštite. *IPSec protokol* (*Internet Protocol Security*) je najpoznatiji protokol zaštite tajnosti prenošenih informacija na mrežnom nivou [30]. Standardni IP *skup* protokola za usmeravanje paketa podataka kroz mrežu od izvorišta do odredišta, pokazuje dobra komunikacijska svojstva, skalabilnost, prilagodljivost i otvorenost prema različitim arhitekturama i mrežnoj opremi, ali ne obezbeđuje zaštitu **CIA** prenošenih podataka. Prenos osetljivih podataka u IP mrežama potrebno je, takođe, obezbediti i na transportnom i aplikativnom sloju. Primer bezbednosnog mehanizma, koji deluje između aplikativnog i transportnog sloja je SSL protokol. Problem je, što postoji veliki broj različitih protokola sa aplikativnog sloja, za koje je potrebno posebno razvijati mehanizme zaštite.

Mrežni sloj koristi funkcionalnosti fizičkog i sloja veze podataka, dok za usmeravanje paketa koristi vlastitu logiku. U IP mrežama ovaj sloj se naziva IP sloj, a usmeravanje paketa kroz mrežu se obavlja prema IP protokolu. Značajno svojstvo IP mreža je potpuna homogenost mrežnog, odnosno IP sloja, dok u ostalim slojevima postoji određen stepen raznovrsnosti. IP sloj koristi jedinstveni IP protokol. Svojstvo homogenosti IP sloja bitno pojednostavljuje uvođenje jedinstvenog bezbednosnog mehanizma u IP mreži. Zaštitom

komunikacije na nivou IP protokola štiti se celokupna mrežna komunikacija. Protokol za zaštitu komunikacije u mrežnom, odnosno IP sloju, naziva se IPSec protokol–. IPSec protokol je deo mrežnog sloja, čiji je zadatak prikupljanje podataka o stanju mreže i usmeravanje paketa podataka između mrežnih čvorova.

IPSec protokol zadržava kompatibilnost s postojećim IP protokolom, što omogućava transparentnost mrežne opreme, zasnovane na IP protokolu, odnosno, samo dva krajnja učesnika u komunikaciji, moraju imati podršku za komunikaciju IPSec-om, dok mrežna čvorišta i ruteri ne moraju imati ovu podršku. Fizički sloj i sloj veze podataka koriste *Ethernet* zaglavlje i *Ethernet* zaštitu. Za pravilan rad mrežnog sloja i IP protokola bitno je IP zaglavlje, u kojem su, između ostalog, upisane izvorišna i odredišna adresa IP paketa, koje su potrebne za usmeravanje paketa kroz mrežu. Ostali delovi TCP/IP paketa, pripadaju višim slojevima i za IP sloj predstavljaju obične podatke koje je potrebno preneti kroz mrežu. Da bi se zadržala kompatibilnost IPSec sa IP protokolom, potrebno je, da u strukturi IPSec paketa podataka, ostane očuvano IP zaglavlje. *IPSec protokol stoga obavlja kriptografske akcije nad zaglavljima i podacima viših slojeva*. Polje sa IPSec zaglavljem i podacima uključuje, u šifrovanom obliku, TCP zaglavlje, kao i sva ostala zaglavlja i podatke viših slojeva.

1.7.3 Kontrole zaštite informacija

Kontrola zaštite informacija je konačna klasifikacija mehanizama zaštite i interfejs između mehanizma i čoveka, a može biti *tehnička* funkcija arhitekture sistema zaštite (npr. alarmni signal generisan na izlazu IDPS), *organizaciono-operativna mera* (npr. barijere za fizički pristup) i *upravljačko–administrativna mera* (npr. primenjen standard). Termin *kontrola zaštite,* takođe, implicira suštinsku potrebu neprekidnog nadzora i *kontrolisanja* sistema zaštite [77].

Kvalitet *kontrole zaštite* određen je funkcionalnim karakteristikama: *robusnost* (otpornost na napade), *adaptivnost* (*fleksibilnost* — mogućnost zamenljivosti i *skalabilnost* – mogućnost proširivanja), *organizacija* i *struktura* u procesu zaštite. Kvalitet kontrole zaštite osnov je za evaluaciju *kvaliteta procesa zaštite* i garantovane bezbednosti informacija u procesima interne i nezavisne provere (*audit*), sertifikacije i akreditacije [89,117].

Robusnost kontrole definiše intenzitet funkcije zaštite (garantovane bezbednosti). Zavisno od efektivnosti implementacije, omogućava definisanje kontrole sa različitim stepenom zaštite. Robusnost je određena sa *intenzitetom funkcije* zaštite ili relativnom merom potrebnog rada/troškova za proboj implementirane kontrole i *nivoom* poverenja u njenu efektivnost – *osnovnim* (**o**), *poboljšanim* (***p***)) i *visokim* (**v**).

Adaptivnost omogućava nadgradnju, poboljšanje i izbor skupa kontrola, adekvatnih za politiku zaštite i potrebe organizacije. *Skalabilnost* implicira modularnu nadgradnju kontrola, a *fleksibilnost* elastičnu primenu poznatih formi zaštite (npr. bekapovanje se može vršiti sedmično, mesečno, dnevno).

Struktura kontrole zaštite ima standardnu formu, koja se može neznatno razlikovati u različitim standardima najbolje prakse zaštite [57, 77, 51]. Postoje brojni tipovi različitih kontrola zaštite, koje se mogu iskoristiti u konkretnom sistemu. Kontrole se dinamički razvijaju i menjaju u zavisnosti od promena u menadžment sistemu, operativnom okruženju, pretnjama i tehnologijama zaštite. U NIST standardu [77] struktura dokumentovanih

kontrola zaštite sadrži sekcije: (1) *cilja* za **o**, **p** i **v** zaštitu, (2) *opisa* specifičnih zahteva i detalja za **o**, **p** i **v** zaštitu i (3) *mapiranja* sa zahtevima za zaštitu, da se izbegne dupliranje kontrola. Kontrole zaštite su organizovane u *klase, familije u klasi* i *kontrole* u *familiji* (ukupno **198**). U ISMS standardu (Aneks A) i ISO/IEC 27002 kontrole zaštite (ukupno **13**4) su struktuirane u sekcije sa *ciljem i obrazloženjem* kontrole.

U NIST standardu, u skladu sa objektno orijentisanim modelom, postoje *klase upravljačkih* (**U***), operativnih* (**O**) *i tehničkih* (**T**) *kontrola zaštite*. Klasa **U** *kontrola zaštite* odnosi se na menadžment sistem zaštite i rizika i sadrži **pet** *familija*. Klasa **O** *kontrola* sadrži **devet** *familija*, koje podržavaju **U** i **T** kontrole. Ove kontrole primarno izvršavaju ljudi. Klasa T kontrola sadrži **četiri** *familije*, uključuje hardversko-softverske mehanizme i protokole zaštite, a primarno ih izvršava sistem. Kontrole familije *Menadžment programa* zaštite – PM (*Program Managament*) mogu se smatrati opštim kontrolama zaštite na nivou organizacije (uvedene su u reviziji 3). Tipično pokrivaju više IKT sistema i obično se specifikuju u *planu zaštite*, umesto u katalogu kontrola. U tabeli 1.5 prikazane su klase, pripadajuće familije i jedinstveni identifikatori familija za srpsku i (*englesku*) konvenciju kodiranja [30].

Tabela 1.5 Klase, familije i identifikatori kontrola zaštite

Identifikator	Klasa	Familija kontrola
UP (*PM*)	Upravljačka	menadžment programa
BA (*CA*)		sertifikacija i akreditacija sistema zaštite
PS (*PL*)		planiranje sistema zaštite
PR (*RA*)		procena rizika
AS (*SA*)		akvizicija sistema i servisa zaštite
SO (*AT*)	Organizaciono–operativna	svest o potrebi i obuka u zaštiti
UK (*CM*)		upravljanje konfiguracijom
PP (*CP*)		planiranje kontinuiteta poslovanja
UI (*IR*)		upravljanje incidentom
IS (*SI*)		integritet sistema i informacija
OS (*MA*)		održavanje sistema zaštite
ZM (*MP*)		zaštita medija
FZ (*PE*)		fizička i zaštita okruženja
PZ (*PS*)		personalna zaštita
RO (*AU*)	Tehnička	revizija i odgovornosti
KP (*AC*)		kontrola pristupa
IA (*IA*)		identifikacija i autentifikacija
ZS (*SC*)		zaštita sistema i komunikacija

Svaka kontrola je jedinstveno kodirana, primenom standardizovane konvencije, i to: *klasa*, numeričkom oznakom (1, 2, 3...), *familija* sa dva velika slova koja jednoznačno definišu ime familije, *nivo robusnosti* sa **o**, **p** i **v,** *kontrola* sa brojem ispred ovog identifikatora, koji određuje redosled kontrole u okviru familije prema prioritetu bezbednosnog značaja.

Primer: **PZ–4.o** jedinstveno označava četvrtu kontrolu zaštite sa *osnovnim* nivoom robusnosti u familiji *personalna zaštita* (videti tabelu 1.5).

Dimenzije kontrola zaštite — životni ciklus, forma, namena, kategorija, karakteristike i parametri implementacije, određuju njihov kvalitet (tabela 1.6).

Tabela 1.6 *Dimenzije kontrola zaštite*

Dimenzija kontrole zaštite	Opis atributa
Životni ciklus	*dizajn, implementacija, održavanje, odlaganje*
Forma	*politika, procesi, tehnologija*
Namena	*prevencija, odvraćanje, detekcija, redukcija, oporavak, korekcija, monitoring, razvoj svesti*
Kategorija događaja	*kontrola gubitaka, kontrola pretnji, kontrola ranjivosti*
Karakteristike	*robusnost, fleksibilnost*
Parametri implementacije	*cena, benefiti, prioriteti*

Izbor skupa kontrola za sistem osnovne zaštite ispunjava specifične zahteve za zaštitu i demonstrira stvarnu odlučnost organizacije za zaštitu CIA informacija [51]. Minimalan *skup kontrola za sistem osnovne zaštite,* koji preporučuje NIST standard za tipičan IKT sistem, obezbeđuje održavanje ukupnog preostalog rizika na prihvatljivom nivou. Rentabilne kontrole zaštite određuju se i biraju na bazi *bezbednosne klasifikacije* i *kategorizacije* informacione imovine i *procene rizika*.

Bezbednosna klasifikacija i kategorizacija informacione imovine, uzima informacije o sistemu (obim, granice, dekompoziciju, kritičnost i izloženost napadima itd.) iz *plana zaštite*, a na osnovu bezbednosnih zahteva i ciljeva [3,94,71]. U sistemu zaštite pojam klasifikacije se odnosi na klasifikaciju bezbednosnih nivoa informacija (npr. *interne, poverljive, strogo poverljive, državna tajna* itd.). Informacije se svrstavaju u kategorije u odnosu na tip (*privatna, vojna, zdravstvena, finansijska, naučno–istraživačka, poslovna, diplomatska, obaveštajna* itd.), koje definišu zakoni, uredbe, regulative, organizacije ili politika zaštite [7]. Pod *bezbednosnom kategorizacijom* se podrazumeva klasifikacija svih objekata informacione imovine u bezbednosne kategorije, na koje se mogu primeniti svi generički kriterijumi klasifikacije [30].

ISO/IEC 27001:2005 (Anex A)
A.7.2.1 Informacije treba da budu klasifikovane u odnosu na njihovu vrednost, legalne zahteve, osetljivost i kritičnost za organizaciju.
A.7.2.2 Treba razviti i implementirati odgovarajući set procedura za označavanje i rukovanje informacijama, u skladu sa usvojenom šemom klasifikacije.

Standardni proces *kategorizacije* uspostavlja bezbednosne kategorije za određivanje vrednosti informacione imovine (A), koje se zasnivaju na kriterijumu *maksimalnog uticaja* faktora rizika na *misiju organizacije, zaštitu imovine, funkcionalnost, ispunjavanje obaveza i zaštitu prava zaposlenih*. Bezbednosne kategorije se definišu u odnosu na ranjivosti sistema i pretnje u proceni rizika za ciljeve zaštite CIA informacija [7]. *Potencijalni uticaj* na informacionu imovinu realizuje neki agent pretnje, probojem sistema zaštite, tj. nekim gubitkom CIA. Prihvatljiva kvalitativna mera uticaja rizika na informacionu imovine može biti: *nizak (*N*), srednji (*S*), visok (*V*). Bezbednosnu kategoriju* (**BK)** informacione imovine, određuje potencijalni uticaj gubitka ***CIA*** koji ima *najveću vrednost*, tj. *uzima se najgori slučaj* [30]:

$$\mathbf{BK} = (\text{uticaj na } \mathbf{C}), (\text{uticaj na } \mathbf{I}), (\text{uticaj na } \mathbf{R}) = \mathbf{uticaj}_{max}$$

gde se vrednost potencijalnog uticaja pretnji uobičajeno rangira sa: N, S i V.

Primer: Neka je u određivanju bezbednosne kategorije procesa *akvizicije IKTS opreme* (**BKao)** uticaj pretnji na CIA procenjen sa – (C) = **S,** (I) = **V,** a (A) = **N,** biće:

$$\mathbf{BKao} = (C, \mathbf{S}), (I, \underline{\mathbf{V}}), (A, \mathbf{N}) = \mathbf{(S), (\underline{V}), (N)} = \mathbf{uticaj}_{max} = \underline{\mathbf{V}}$$

Izbor minimalnog skupa kontrola za osnovnu zaštitu, uzima se iz skupa kontrola *osnovne zaštite*, a kontrola iz skupa za *poboljšani* ili *viši nivo* zaštite **—** na osnovu povećanih bezbednosnih zahteva i ciljeva [77].

Primer: ako je najveći potencijalni uticaj **N**, izaberu se osnovne kontrole zaštite za nizak (*N)* uticaj pretnji, ako je **S** – izaberu se osnovne kontrole zaštite za *S* i *N* uticaj pretnji, a ako je **V** – biraju se osnovne kontrole za *N, S* i *V* uticaj pretnji. U gornjem primeru maksimalni uticaj je **V**, pa se biraju kontrole za *N, S* i *V* uticaj pretnji iz skupa osnovnih kontrola zaštite.

Za efektivnu zaštitu treba koristiti standardne kontrole zaštite i prilagoditi ih specifičnostima organizacije u formi internog standarda (*kataloga)* [57,77]. Lista kontrola za osnovnu zaštitu obezbeđuje minimum zaštite za odgovarajuću bezbednosnu kategoriju. Kontrole zaštite, u svakom od tri osnovna skupa, sadrže kombinaciju *akumuliranih* kontrola sa sva tri nivoa robusnosti.

Primer: za *N nivo* osnovne zaštite katalog sadrži kontrole zaštite sa osnovnim nivoom robusnosti **o**; za *S nivo* osnovne zaštite – kombinaciju kontrola zaštite sa **o** i **p** nivoima robusnosti; za *V nivo* osnovne zaštite – kombinaciju kontrola zaštite sa **o, p** i **v** nivoima robusnosti. Pri tome ne postoji direktna korelacija između tri nivoa robusnosti kontrola zaštite (**o, p, v**) i tri nivoa osnovnih skupova kontrola zaštite (*N,S,V*).

Odgovarajuće kontrole zaštite biraju se za odgovarajuće nivoe osnovne zaštite. Na primer, neka kontrola zaštite sa **o** nivoom robusnosti, može se prvo pojaviti na *V* nivou osnovne zaštite ili se nikada ne pojavljuje, već je samo na raspolaganju kao opcija organizaciji za dopunu skupa kontrola zaštite. Neke *kompenzujuće* ili *univerzalne* kontrole zaštite, mogu se primenjivati u sva tri osnovna skupa kontrola zaštite i za sve nivoe robusnosti. Skup kontrola za osnovnu zaštitu namenjen je za ublažavanje glavnih faktora rizika, a za *N* uticaj faktora rizika sadrži ukupno **198** (**U = 42 , O = 78 i T =78**) kontrola sa **o** *nivoom robusnosti* [77].

Mapiranje odgovarajućih kontrola sa specifičnim zahtevima za zaštitu vrši se pomoću *matrice za praćenja bezbednosnih zahteva* – **RTM** (*Requirements Traceability Matrix*), koja se konstruiše identifikovanjem usaglašenih, specifičnih *bezbednosnih zahteva* i odgovarajućih *kontrola zaštite* iz izabranih skupova kontrola za osnovnu zaštitu, koje te zahteve ispunjavaju. Mapiranje može biti:

1:1, jedan zahtev rešava se sa jednom kontrolom zaštite,
1:N, jedan zahtev rešava se sa više kontrola zaštite,
N:1, više zahteva rešava se sa jednom kontrolom zaštite i
N:M, više zahteva rešava se sa više kontrola zaštite.

U tabeli 1.7 ilustrovan je primer dela **RTM** matrice za hipotetičke zahteve za zaštitom i standardizovan skup kontrola iz kataloga kontrola zaštite.

Tabela 1.7 *Primer matrice praćenja bezbednosnih zahteva*

Zahtevi zaštite	Mapiranje	Kontrole zaštite
Zahtev br. 1	1:1	PS–1o
Zahtev br. 2	1:N	PE–2o, PE–3o, PE– 6s, PE–7o
Zahtev br. 3, Zahtev br. 4	N:1	CM–2s
Zahtev br. 5, Zahtev br. 6	N:M	IA–1s, IA–2s, IA–4o

Kontrole zaštite nisu statičke kategorije i mogu se revidirati na osnovu *promena prakse, zahteva i tehnologija zaštite.* Modifikacija kontrola zaštite zahteva rigoroznu raspravu, reviziju i konsenzus svih zainteresovanih strana u organizaciji. Za izbor adekvatne kontrole zaštite

za osnovnu zaštitu treba izvršiti analizu i procenu rizika u ranoj fazi razvoja IKT sistema. Ako je pokrivanja pretnji neadekvatno, kontrola za osnovnu zaštitu se može poboljšati povećanjem robusnosti ili dodavanjem nove.

Prilagođavanje rezultatima procene rizika izabranog minimalnog skupa kontrola osnovne zaštite, zahteva dokumentovanje modifikovanih i novih kontrola zaštite [77]. U izboru *optimalnih* U, O i T *kontrola zaštite* za ublažavanje rizika na prihvatljiv nivo, prva aktivnost je opis faktora rizika sa liste prioritetnih rizika. Da bi se razumeli vrsta i intenzitet pokrivanja pretnji/rizika primenjenim kontrolama zaštite, potrebno je odrediti koji se faktori rizika i sa kojim kontrolama zaštite ublažavaju, ne ublažavaju, zaobilaze ili su postali prihvatljivi preostali rizik. Za to su korisne dostupne taksonomije potencijalnih pretnji i ranjivosti IKT sistema [58].

Prema ISMS standardu i*zbor kontrola zaštite* vrši se kada su identifikovani bezbednosni zahtevi i rizici i donete odluke o tretmanu rizika na prihvatljiv nivo. Kontrole se mogu birati na osnovu ISMS ili drugih standarda, a mogu se projektovati potpuno nove kontrole za specifične potrebe organizacije. Izbor kontrola zaštite zavisi od odluke menadžera, na bazi kriterijuma prihvatljivosti rizika, opcija tretmana rizika, pristupa menadžmentu rizika, odgovarajućih zakona ili uredbi. Više informacija o izboru kontrola i opcija za tretman rizika mogu se naći u ISMS standardu, u sekciji 4.2 "*Tretman rizika za bezbednost informacija* ".

Neke od kontrola iz ISMS standarda mogu se smatrati primenljivim u većini organizacija. Veći deo kontrola može se smatrati dobrom polaznom tačkom za implementaciju sistema zaštite informacija, a sve se zasnivaju na pravnim zahtevima ili se smatraju za uobičajenu praksu u zaštiti informacija. Sa aspekta primenljivih zakona, za svaku organizaciju su *relevantne sledeće ISMS kontrole za*:

a) *zaštitu podataka i tajnost informacija o ličnosti* (videti 15.1.4 ISMS),
b) *zaštitu zapisa organizacije* (videti 15.1.3 ISMS) i
c) *zaštitu prava na intelektualnu svojinu* (videti 15.1.2 ISMS).

Kontrole koje se smatraju uobičajenom praksom u zaštiti informacija, u većini organizacija i okruženja, obuhvataju:

a) *dokument o politici zaštite informacija* (videti 5.1.1 ISMS);
b) *pripisivanje odgovornosti za zaštitu informacija* (videti 6.1.3 ISMS);
c) *razvoj svesti, obuka i obrazovanje u zaštiti informacija* (videti 8.2.2 ISMS);
d) *ispravno procesiranje u aplikacijama* (videti 12.2 ISMS);
e) *menadžment tehničkih ranjivosti* (videti 12.6 ISMS);
f) *upravljanje kontinuitetom poslovanja* (videti 14 ISMS);
g) upravljanje kompjuterskim incidentom (videti 13.2 ISMS).

Iako su sve kontrole zaštite iz ISMS standarda važne i treba ih uzeti u obzir, relevantnost svake kontrole treba utvrditi u odnosu na specifični rizik organizacije. Zato navedeni pristup ne može zameniti izbor kontrola zaštite na bazi procene rizika, iako je dobra polazna tačka u implementaciji menadžment sistema zaštite (ISMS). Kontrole zaštite treba identifikovati i

implementirati tako da ublažavaju specifične faktore rizika za poslovne procese. Svaka kontrola ima svoju cenu, koja se mora uključiti u proces implementacije. Za procenu efektivnosti kontrola razvijeno je više metoda uključujući *intervjue i testiranja* na proboj (tabela 1.8).

Tabela 1.8 *Metodi za procenu efektivnosti kontrola zaštite za različite uticaje rizika*

Metodi procene: intervju, testiranje		**Nivo uticaja rizika na IKT sistem**		
Atribut	Vrednost	Nizak	Srednji	**Visok**
Dubina (samo intervju i testiranje)	skraćen	√	–	–
	značajan	–	√	–
	sveobuhvatan	–	–	√
Obim (samo metod testiranja)	funkcionalnost (crna kutija)	√	√	√
	proboj	–	√	√
	strukturni (siva i bela kutija)	–	–	√
Pokrivanje (svi metodi)	broj i tip objekata za procenu određen u saradnji sa evaluatorom	√	√	√

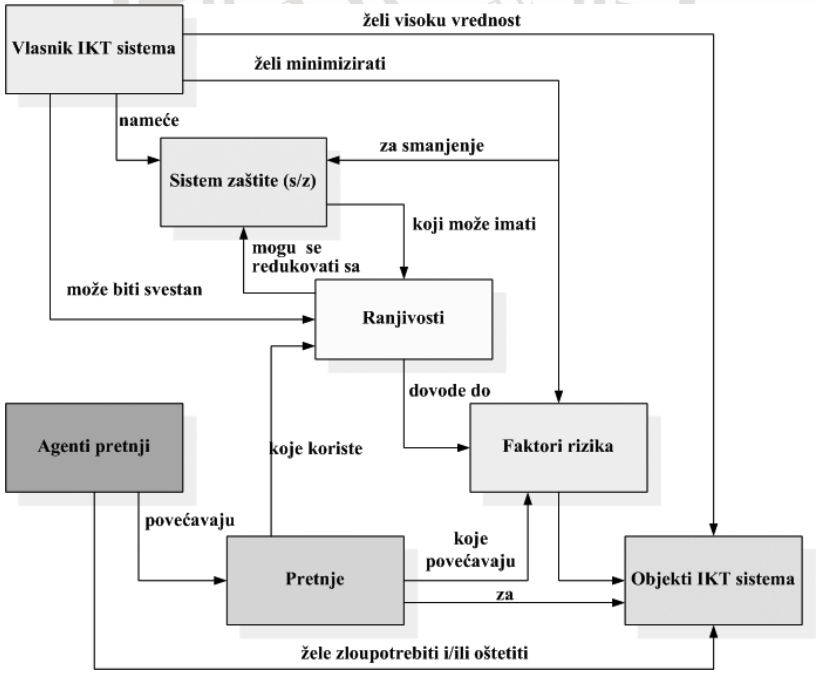
U praksi zaštite treba prepoznati uslove u kojima određeni metod za procenu efektivnosti kontrola zaštite daje najbolje rezultate i ima najveću vrednost. *Kritični faktori uspeha* implementacije kontrola zaštite informacija u nekoj organizaciji su:

1. *politika zaštite informacija* — aktivnosti i ciljevi u zaštiti koji odražavaju poslovne ciljeve,
2. *pristup i okvir implementacije* — održavanje, nadzor i poboljšanje, kultura rada,
3. *eksplicitna podrška menadžmenta* — obavezujuća za menadžere na svim nivoima,
4. *dobro razumevanje bezbednosnih zahteva* — procena i upravljanje rizikom,
5. *razvoj svesti o potrebi zaštite* — promocija kod svih relevantnih učesnika,
6. *distribucija smernica za zaštitu informacija* — svim relevantnim učesnicima,
7. *obezbeđenje sredstava* za menadžment zaštite informacija,
8. *obezbeđivanje odgovarajuće obuke i obrazovanja u zaštiti*,
9. *uspostavljanje efikasnog procesa upravljanja kompjuterskim incidentom*,
10. *implementacija metrika sistema zaštite* — za vrednovanje i poboljšanje performansi ISMS.

Dokumentovanje kontrola zaštite vrši se u planu tretmana rizika (ili *planu zaštite*). Dokumentuju se rezultati izbora skupa kontrola zaštite, ali i planirane, implementirane i na bazi procene rizika, korigovane kontrole zaštite. Konačni skup kontrola dokumentuje se sa svim obrazloženjima i *glavnim razlozima* za izbor, sa indikatorima koji ukazuju na prateću dokumentaciju i koji objašnjavaju zašto izabrane kontrole ispunjavaju bezbednosne zahteve organizacije. *Plan zaštite* je osnova za sertifikaciju i akreditaciju sistema, čiji su rezultati presudni za donošenje odluke o povezivanju IKT sistema sa drugim sistemima izvan granica akreditacije.

1.8 GENERIČKI, FUNKCIONALNI MODEL SISTEMA ZAŠTITE

Za razumevanje mesta i uloge sistema zaštite u IKT sistemu, od velike koristi je *generički model sistema zaštite* (slika 1.5). *Vlasnik* IKT sistema uspostavlja vrednosti informacione imovine i odgovoran je za njenu zaštitu. *Agent pretnje* je izvršilac potencijalne pretnje i uvek radi protiv interesa vlasnika. *Sistem zaštite* štiti objekte informacione imovine od *pretnji*, koje ugrožavaju *CIA* informacione imovine. Vlasnik *procenom rizika* analizira moguće pretnje primenljive u okruženju, ranjivosti sistema, iskoristivost tih ranjivosti sa jednom ili više pretnji i verovatnoću uticaja na poslovanje. Rezultati analize su rizici, uključujući izbor *kontrola zaštite* za ublažavanje faktora rizika na prihvatljiv nivo, smanjenjem *ranjivosti* i *izloženosti* u skladu sa zahtevima *politike zaštite* vlasnika. Posle implementacije kontrola zaštite, agenti pretnji mogu iskoristiti preostale ranjivosti, što predstavlja *preostali rizik na prihvatljivom nivou*, kojeg vlasnik u neprekidnom (cikličnom) procesu zaštite uvek nastoji smanjiti svim raspoloživim kontrolama zaštite. Vlasnik mora biti uveren da su primenjene kontrole zaštite adekvatne za ublažavanje faktora rizika, pre nego što dozvoli izlaganje IKT sistema – identifikovanim pretnjama. U tom cilju, vlasnik može tražiti *evaluaciju* – internu i spoljnu proveru (*audit*) ili *sertifikaciju* i *akreditaciju* (testiranje i odobrenje za rad) sistema zaštite. Izlaz procesa evaluacije je izjava o *akreditaciji* (na bazi rezultata *sertifikacije*) da će zaštitne mere smanjiti faktore rizika na prihvatljiv nivo. Na osnovu rezultata evaluacije vlasnik odlučuje da li će prihvatiti preostali rizik ili ne, što dokazuje potpisivanjem dokumenta SoA (*Statement of Applicability*) [56].



Slika 1.5 Generički model i međusobni odnosi komponenti sistema zaštite

1.9 DEFINISANJE *OPTIMALNOG SISTEMA ZAŠTITE*

Namena *programa zaštite* informacija je da identifikuje bezbednosne ciljeve i razvije, implementira i održava *optimalan* (ekonomski rentabilan i funkcionalno efektivan) sistem zaštite. IKT sistem je *optimalno zaštićen,* ako ima izbalansirane *efektivnosti* kontrola zaštite i *troškove* njihove akvizicije/razvoja, odnosno, kada su troškovi kontrola zaštite potpuno izjednačeni sa procenjenim gubicima, koji bi mogli nastati da zaštite nema [11].

Za sintezu optimalnog sistema zaštite treba imati gotova rešenja za *arhitekturu sistema zaštite i ocenu kvaliteta njenog funkcionisanja, ocenu osetljivosti modela razvoja u odnosu na apriorne podatke i fizičku realizaciju sistema zaštite integrisanog u IKT sistem*. U zavisnosti od odnosa strategije zaštite i postavljenih bezbednosnih ciljeva, moguća su dva pristupa sintezi *optimalnog sistema zaštite* [11]:

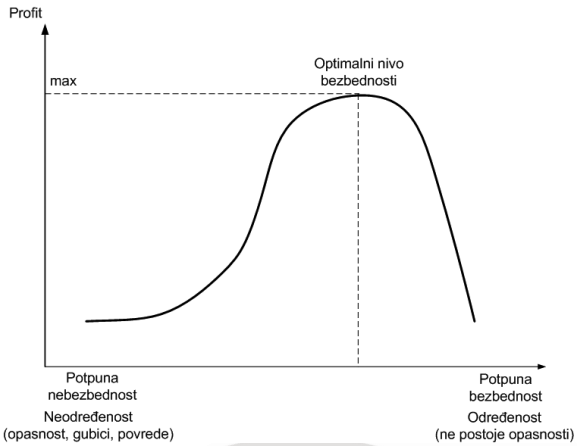
Primarni: za dati nivo troškova zaštite – **Trz** obezbediti maksimalno mogući intenzitet vektora zaštite – $\mathbf{I(s) => I_{max}}$, gde je **s** – izabrana strategija zaštite;

Sekundarni: obezbediti željene rezultate intenziteta vektora zaštite $\mathbf{I(s) > I_{dopušteni}}$, pri minimalno mogućim troškovima zaštite – $\mathbf{T_{trmin.}}$

Pod *efektivnošću kontrole zaštite* informacija podrazumeva se efikasnost i efektivnost u aktivnoj zaštiti poverljivosti, integriteta i raspoloživosti informacija u operacijama obrade, skladištenja i prenosa. Ocena efektivnosti procesa zaštite odnosi se na sposobnost kontrole zaštite da reši zadatak zaštite. Izbor vektora *efektivnosti kontrole zaštite* – **I(s)** zavisi i od izbora *strategije zaštite* – **s**, koja se određuje iz skupa strategija zaštite – **S**. U opštem slučaju ta zavisnost se izražava relacijom transformacije – **Y** skupa mogućih strategija – **S** u skup *indikatora efektivnosti* – **I** [11]:

$$Y : S \rightarrow I$$

Uvođenje indikatora efektivnosti – **I** zahteva takvo određivanje kriterijuma efektivnosti, koji omogućavaju izbor strategije iz skupa dostupnih. Međutim, teoretske osnove za formiranje optimalnog sistema zaštite nisu dovoljno usavršene, a osim nedostatka dovoljno tačne opšte teorije za formiranje *metodoloških osnova* za fenomene sa faktorima neodređenosti, nije primenljiva ni klasična statistička teorija. Pod *metodologijom optimizacije* sistema zaštite informacija podrazumeva se razvijena teorija zaštite, koja povezuje strukturu sistema zaštite, logičku organizaciju i kontrole zaštite u cilju formiranja bezbednosnih funkcija za izbor i izdvajanje podskupa najboljih strategija zaštite. *Optimalno rešenje zaštite je ono, koje u datim uslovima na najbolji način zadovoljava sve uslove razmatranog zadatka, a postiže se putem najracionalnije raspodele resursa utrošenih na rešavanje zadataka zaštite* [11]. U procesu uspostavljanja optimalnog sistema zaštite potrebno je vršiti korekciju zahteva, zbog faktora neodređenosti *ponašanja, funkcionalnosti ili ciljeva zaštite*. Generalno, optimalni sistem zaštite dobije se u tački između potpune bezbednosti i nebezbednosti, uz ostvarivanje maksimalnog profita (slika 1.6) [30].



Slika 1.6 Optimalni sistem zaštite informacija

Sa porastom troškova akvizicije/razvoja sistema zaštite, raste i nivo bezbednosti IKT sistema, ali opada potencijalni profit organizacije zbog troškova sistema zaštite. Zato ne treba težiti sve većem i većem nivou zaštite po svaku cenu. Osnovni nedostaci optimizacije sistema zaštite odnose se na *matematičku složenost rešavanja optimalnog sistema zaštite, težinu programiranja algoritma optimizacije, neprihvatljivo veliko vreme automatske optimizacije i zavisnost kvaliteta optimalnog sistema od tačnosti izvornih ovlašćenja i karaktera promena upravljanog objekta zaštite*.

1.10 ARHITEKTURA SISTEMA ZAŠTITE INFORMACIJA

Arhitektura sistema je set pravila i konvencija, koji usmerava procese projektovanja i održavanja sistema zaštite, odražava potencijalna ograničenja okruženja, resursa, veština zaposlenih i tehnologija i sredstvo za menadžment kompleksnosti sistema i primenu principa sistemskog inženjerstva za postizanje poslovnih ciljeva. Takođe, obezbeđuje okvir procedura, tehnologija i procesa, kao i koherentnu, konzistentnu i rentabilnu implementaciju, upotrebu i održavanje sistema zaštite, sa ciljem da:

- minimizira raznovrsnost tehnologija;
- obezbedi konzistentnu funkcionalnost sistema zaštite informacione imovine;
- integriše servise i mehanizme zaštite u sistem zaštite;
- deli sistem zaštite na različite domene i kontroliše tok informacija između njih i
- primenjuje konzistentne metode, tehnike i konvencije u sistemu zaštite.

Arhitektura sistema zaštite informacija organizacije treba da bude slojevita, gde svaki sloj predstavlja različitu perspektivu zaštite i angažuje različite uloge, a gornji sloj usmerava i upravlja donjim slojem zaštite. Arhitektura se razvija prema modelu *odozgo – nadole*, a dobar pristup je SABSA®[11] okvir i model koji obezbeđuje definisanje arhitekture sistema zaštite informacija, a slojeve zaštite definiše kroz poglede i uloge relevantnih učesnika (tabela 1.9).

11 Engl.: SABSA (*Sherwood Applied Business Security Architecture*) framework, by John A. Zachman.

Tabela 1.9 *SABSA okvir i model arhitekture sistema zaštite*

Sloj arhitekture sistema zaštite	Nivo implementacije sistem zaštite
pogled sa nivoa poslovanja	kontekstualna arhitektura zaštite
pogled arhitekte sistema zaštite	koncept arhitekture zaštite
pogled projektanta sistema zaštite	logička arhitektura zaštite
pogled programera sistema zaštite	fizička arhitektura zaštite
pogled snabdevača	komponente arhitekture zaštite
pogled menadžera	operativna arhitektura zaštite

Na svakom apstraktnom sloju zaštite SABSA® model zahteva odgovore na pitanja *šta, zašto, kako, ko, gde i kada*, a operativna arhitektura sistema zaštite informacija u organizaciji uključuje sve slojeve (slika 1.7).



Slika 1.7 Model SABSA® slojeva arhitekture sistema zaštite

Smernice modela se odnose na faze i korake PDCA modela procesa za uspostavljanje i implementaciju ISMS na ovim slojevima.

1.11 NOVA PARADIGMA ZAŠTITE INFORMACIJA

U zaštiti informacija ključna su dva principa — *slojevita zaštita po dubini* i *primarna zaštita najvrednije imovine*. Ova dva principa su tradicionalno grafički prikazivana sa *prstenovima zaštite* ili tzv. *slojevima luka*, koji višekratno preklapaju *jezgro*. Savremeni razvoj SOA[12] *web* aplikacija, virtuelizacija klijentske i serverske strane i razvoj *distribuiranog Internet računarstva* – **CC** (*Cloud Computing*), kao i neki drugi faktori, zahtevaju promenu klasične paradigme zaštite, bazirane na ova dva principa.

Savremene organizacije sve više diverzifikuju lanac vrednosti, u kojem učestvuju različite organizacije, koje igraju jednako značajne uloge. Sa aspekta zaštite IKT sistema, to znači da

12 Engl.: SOA (*Service Oriented Application*) – servisno orijentisane web aplikacije.

će neki slojevi zaštite biti efektivni, samo ako se implementiraju u svim organizacijama koje učestvuju u distribuiranom lancu vrednosti. Ekonomske i finansijske krize su uzrok velikog broja nezaposlenih i čestih promena posla širom sveta, pa nezadovoljni, vešti profesionalci sa administrativnim privilegijama i slabim etičkim principima, mogu predstavljati ozbiljne pretnje za savremene IKT sisteme. Gubitak granica organizacije i ozbiljne interne pretnje, menjaju paradigmu zaštite od *slojeva luka* na *prsten slojeva luka* ili distribuiranu slojevitu zaštitu po dubini. U ovim uslovima organizacije moraju implementirati takav sistem zaštite, koji je otporan na interne pretnje i obezbeđuje poslovanje, čak i kada je sistem probijen.

Virtualizacija klijentske i serverske strane smanjuje vreme i resurse, potrebne za uvođenje novih sistema u organizaciju. Sa aspekta bezbednosti, otvoreno je novo polje za istraživanje adekvatnih mehanizama zaštite *hipervizora* u konfiguraciji virtuelne mašinske introspekcije (VMI), koji bi sprečili nedozvoljenu komunikaciju između virtuelnih mašina (VM). Veoma brzo, zaštita informacija u virtuelnom okruženju **CC** postaće sve značajnija oblast za istraživanje i razvoj. Za iznajmljivanje softvera (**SasS**), hardvera (**HasS**) ili infrastrukture (**IasS**) kao **CC** servisa, potrebno je samo da se klijent, preko Interneta, poveže sa poslovnom aplikacijom provajdera **CC** usluga. Rad u **CC** nudi brojne prednosti za organizaciju, ali nosi i nove probleme zaštite, kao što su[13], kako zaštititi podatke organizacije u **CC** i koje servise za zaštitu CIA informacija treba da obezbede klijenti, a koje provajderi **CC** itd.

Evolucija mobilnih telefona, od prostog telefona do uređaja, koji je po funkcionalnosti bliži personalnom računaru nego telefonu, unela je dodatnu kompleksnost u oblast zaštite, jer zahteva slične mehanizme zaštite, kao za računare.

Međutim, paralelno sa ovim razvojem, raste i kompjuterski kriminal. Kada se dogodi glavni kompjuterski incident, organizacija u prvom koraku pokušava utvrditi prirodu incidenta i veličinu štete, svojim kapacitetima za upravljanje kompjuterskim incidentom. Kad slučaj prevazilazi nadležnosti organizacije, incident se prijavljuje zvaničnim organima istrage. U oba slučaja počinje istraga kompjuterskog incidenta/kriminala, koja uključuje ispitivanje digitalnih dokaza. Profesionalci, specijalizovani za digitalnu forenzičku istragu su nezamenljivi u ovom poslu. Kako se povećava broj digitalnih uređaja, sve više raste značaj *forenzičke analize* dnevnika rada (*log* datoteka) tih uređaja, zbog potrebe proaktivnog praćenja forenzički relevantnih bezbednosnih događaja[14]. Za pregled i reviziju obimnih podataka neophodna je automatizovana analiza log datoteka, centralizovano skupljenih u *log serveru*. *Aktivna, selektivna analiza forenzički relevantnih bezbednosnih događaja u log serveru, na bazi specifičnog poznavanja realnih pretnji, koje pogađaju kritične poslovne procese, postaje ključ za ranu detekciju incidenta*.

U novom e-okruženju, organizacije moraju generičku metodologiju za upravljanje rizikom dopuniti sa agilnijim tehnikama, zasnovanim na *mikro analizi rizika,* umesto scenarija rizika na *makro* planu. Menadžment rizika mora postati obavezan deo poslovnog odlučivanja, na bazi realnih pretnji, ranjivosti i uticaja na poslovanje. U toku je razvoj novih alata, kao što su: *kriptografske tehnike, tehnologije višeslojne mrežne zaštite*, IDPS, distribuirani sistemi za monitoring i kontrolu saobraćaja, sistemi za centralno upravljanje zaštitom, *proaktivni sistemi zaštite*, *programi* zaštite na heterogenim platformama, mehanizam *kolonije digitalnih mrava* itd. Za zaštitu korisničkih informacija u CC okruženju, pored implementacije tradi-

13 Grubor, G., Njeguš, A., *Paradigma zaštite distribuiranog računarstva*, Naučni skup Singergija 10, 2010.
14 Ova oblast digitalne forenzika naziva se *proaktivna digitalna forenzika*.

cionalnih mehanizama zaštite, potrebno ih je ugrađivati u distribuirane hardverske uređaje i softver u fazi njihovog razvoja i proizvodnje.

1.12 REZIME

Informacija je imovina od suštinskog značaja za poslovanje organizacije, pa je potrebno da bude odgovarajuće zaštićena. U savremenim uslovima poslovanja informacije su izložene velikom broju različitih pretnji i ranjivosti. Informacije mogu imati razne oblike i forme, ali uvek treba da budu odgovarajuće zaštićene.

Bezbednost informacija, sinonim za *bezbednost informacione imovine*, je *objektivna mera/ocena* stanja rizika ili stanja sigurnog, pouzdanog i neometanog funkcionisanja *informacionog sistema*. *Sigurnost sistema* je sinonim *bezbednosti*, *subjektivna mera* uverenja korisnika da je sistem bezbedan. Sistem se smatra bezbednim, ako je *zaštićen* od uticaja faktora rizika. *Nivo bezbednosnog stanja* određen je nivoom preostalog prihvatljivog rizika. Ukupna bezbednost proporcionalna je skupu bezbednosnih stanja relativno nezavisnih komponenti, koje neravnomerno, aditivno utiču na ukupnu bezbednost, a najveći uticaj imaju najosetljivije komponente sistema bezbednosti.

Bezbednost informacija predstavlja zaštitu od širokog opsega pretnji kako bi se osigurao kontinuitet poslovanja, na minimum sveo rizik u poslovanju i na maksimum povisio prihod od investicija i povoljnih poslovnih prilika.

Bezbednost informacija se postiže implementacijom pogodnog skupa *kontrola, zaštite*, koje treba uspostaviti, implementirati, nadgledati, preispitivati i poboljšavati, da bi se osiguralo ispunjavanje bezbednosnih i poslovnih ciljeva.

Bezbednost informacija je situacioni problem stanja sistema i realnog okruženja, a nivo ukupne bezbednosti nelinearno opada, zbog stohastičke prirode pretnji. *Održavanje stanja bezbednosti* informacija, na prihvatljivom nivou rizika, obezbeđuje implementirani *sistem zaštite* poverljivosti, integriteta i raspoloživosti informacija. Osnovnu funkcionalnost sistema zaštite čine *servisi zaštite, mehanizmi i protokoli* zaštite. Za upravljanje mehanizmima zaštite obezbeđene su određene kontrolne strukture ili *kontrole zaštite.* Sa aspekta zaštite, osnovni zahtev je *smanjenje kompleksnosti,* što se postiže sistem-inženjerskim, *objektno-orijentisanim i procesnim pristupom* u svim fazama razvoja IKT sistema. U generičkom modelu, sistem zaštite štiti informacionu imovinu od pretnji, malicioznih i namernih napada. Cilj svakog programa zaštite informacija je da razvije *optimalan sistem* zaštite, koji u datim uslovima na najbolji način zadovoljava sve uslove.

Savremeni *web* servisi (*web* aplikacije, SOA, *Cloud Computing* i dr.) i e-poslovanje zahtevaju promenu paradigme klasične zaštite IKT sistema, sa prstenovima slojeva zaštite i rešenjima *distribuiranih* mehanizama zaštite, koji se ne samo implementiraju, nego i *ugrađuju* u hardverske i softverske komponente u toku njihovog razvoja.

1.13 PITANJA ZA PONAVLJANJE

1. Čista informaciona imovina uključuje:
   a. digitalne podatke, informacije, opipljivu i neopipljivu informacionu imovinu, aplikativne i sistemske programe
   b. infrastrukturu za podršku, kontrole okruženja, hardver i imovinu IKT sistema
   c. aplikativne i sistemske programe, infrastrukturu za podršku IKT sistema
   d. zaposlene, nezaposlene, spoljne saradnike, poslovne partnere.
2. Fizička imovina obuhvata:
   a. digitalne podatke, informacije, opipljivu i neopipljivu informacionu imovinu, aplikativne i sistemske programe
   b. infrastrukturu za podršku, kontrole okruženja, hardver i imovinu IKT sistema
   c. aplikativne i sistemske programe, infrastrukturu za podršku IKT sistema
   d. zaposlene, nezaposlene, spoljne saradnike, poslovne partnere.
3. Humana imovina obuhvata:
   a. digitalne podatke, informacije, opipljivu i neopipljivu informacionu imovinu, aplikativne i sistemske programe
   b. infrastrukturu za podršku, kontrole okruženja, hardver i imovinu IKT sistema
   c. aplikativne i sistemske programe, infrastrukturu za podršku IKT sistema
   d. zaposlene, nezaposlene, spoljne saradnike, poslovne partnere.
4. Bezbednost IKT sistema je::
   a. objektivna mera/ocena stanja rizika IKT sistema
   b. subjektivna ocena stanja zaštićenosti IKT sistema
   c. funkcionalna komponenta IKT sistema
   d. nijedan od navedenih odgovora.
5. Nivo ukupne bezbednosti složenog sistema (Bu) raste:
   a. približno linearno i aditivno sa porastom nivoa bezbednosti komponenti
   b. približno nelinearno i multiplikativno sa porastom bezbednosti komponenti
   c. približno nelinearno i aditivno sa porastom nivoa bezbednosti komponenti.
6. Funkcija zavisnosti komponenti bezbednosti IKT sistema – Bi od faktora rizika – Ri je:
   a. linearno opadajuća
   b. linearno rastuća
   c. nelinearno opadajuća
   d. eksponencijalno opadajuća.
7. Održavanje bezbednosti IKT sistema na određenom nivou, najtačnije obezbeđuje:
   a. tim specijalista za zaštitu
   b. sistem servisa i kontrola osnovne zaštite
   c. održavanje rizika na prihvatljivom nivou
   d. tim za zaštitu i implementirani sistem za zaštitu.
8. Na bezbednosno stanje IKT sistema utiču sledeći ključni faktori:
   a. korisnički zahtevi, politika zaštite, razvoj standarda i normativa zaštite
   b. funkcionalni zahtevi i organizaciona struktura IKT sistema
   c. kadrovska struktura i ugled organizacije
   d. razvoj tehnologija i malicioznih programa
   e. kompleksnost IKT sistema i terminologije zaštite.
9. Sa aspekta kvaliteta, nužno je i dovoljno obezbediti sledeća svojstva informacija:
   a. blagovremenost, tačnost, korisnost
   b. poverljivost, integritet, raspoloživost
   c. blagovremenost, tačnost, integritet
   d. poverljivost, tačnost, integritet, raspoloživost
   e. blagovremenost, integritet, raspoloživost.

10. Sistem zaštite najbolje objašnjava izraz:
    a. aditivna funkcija intenziteta vektora zaštite
    b. skup funkcija zaštite sa kojim se izvršavaju određeni bezbednosni zadaci
    c. multiplikativna funkcija intenziteta vektora zaštite
    d. organizovan i koherentan skup upravljačkih, organizaciono–operativnih i tehničkih kontrola zaštite.
11. Optimalni sistem zaštite je sistem, koji u datim uslovima:
    a. na najbolji način zadovoljava sve bezbednosne zahteve, sa racionalnim resursima za akviziciju, implementaciju i održavanje sistema zaštite
    b. ne zadovoljava sve bezbednosne zahteve, ali se postiže se neznatnim resursima za akviziciju, implementaciju i održavanje sistema zaštite
    c. zadovoljava sve bezbednosne zahteve, ali se postiže se značajnim resursima za akviziciju, implementaciju i održavanje sistema zaštite.
12. Servis zaštite je:
    a. logička aplikaciona jedinica, koja se izvršava kroz različite akcije, izvršavanjem *mehanizama* i *protokola zaštite*
    b. neprekidna aktivnost, koju vrše bezbednosne funkcije mehanizama zaštite
    c. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    d. konačna klasifikacija mehanizama zaštite i interfejs prema korisniku.
13. Mehanizam zaštite je:
    a. neprekidna aktivnost, koju vrše bezbednosne funkcije mehanizama zaštite
    b. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    c. interfejs prema korisniku servisa zaštite.
14. Kontrola zaštite je:
    a. neprekidna aktivnost, koju vrše bezbednosne funkcije mehanizama zaštite
    b. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    c. konačna klasifikacija mehanizama zaštite i interfejs prema korisniku.
15. Relevantni aspekti zaštite IKT sistema kao objekte zaštite, obuhvataju:
    a. ključne karakteristike pretnji, servisi i kvalitet servisa IKT sistema
    b. ključne karakteristike, servisi i kvalitet servisa IKT sistema
    c. ključne karakteristike IKT sistema, servisi zaštite i kvalitet servisa IKT sistema
    d. ključne karakteristike i servisi IKT sistema i kvalitet servisa zaštite.
16. Generički model sistema zaštite IKT sistema obuhvata sledeće objekte:
    a. vlasnika, agente pretnji, sistem zaštite, pretnje, faktore rizika i objekte IKT sistema
    b. politiku zaštite, preostali i prihvatljivi rizik, evaluaciju, sertifikacija i akreditacija
    c. administratora IKT sistema, preostali rizik, evaluacija, sertifikacija i akreditacija
    d. vlasnika IKT sistema, servise zaštite, pretnje, topologiju RM, procenu rizika.
17. U zaštiti savremenih IKT sistema bazična je primena sledeća dva principa:
    a. virtuelizacija i prstenovi *slojeva luka*
    b. digitalni mravi i prstenovi *slojeva luka*
    c. slojevita odbrana po dubini i primarna zaštita najvrednije imovine
    d. odbrana po dubini i prstenovi zaštite.
18. U zaštiti savremenih IKT sistema nova paradigma zaštite obuhvata tehnologije:
    a. odbrane po dubini i primarne zaštita najvrednije informacione imovine
    b. odbrane po dubini i prstenova zaštite
    c. virtuelizacije, prstenova *slojeva luka,* proaktivna zaštita
    d. digitalnih mrava, prstenova *slojeva luka,* IDPS-a, proaktivne zaštita.



2. SISTEMSKI I PROCESNI PRISTUP ZAŠTITI INFORMACIJA

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Definicije i značaj „sistemskog inženjerstvo " (SE) i „SE zaštite " (SSE)
- ☑ Definicije i značaj intelektualnih alata - SA i sistemskog mišljenja
- ☑ Strukturno i objektno orijenisono modelovanje sistema zaštite
- ☑ Definicije, karakteristike i kontrole „procesa" i „modela procesa"
- ☑ Ulogu menadžmenta i kvaliteta procesa u poslovanju
- ☑ Modele procesa najbolje prakse zaštite informacija

2.1 UVOD

Sistem se na meta-nivou može definisati kao „*skup elemenata koji je* nešto *više nego zbir svih njenih delova*" (*Aristotel*) ili „*skup čiji su elementi uzročno-posledično povezani pa se njihova svojstva razlikuju od svojstava skupa*". U tehničkoj praksi sistem se može definisati kao: „*skup svrsishodno povezanih objekata (komponenti) sa njihovim međusobnim dinamičkim vezama, odnosima i uticajima i interakcijom sa relativnim okruženjem, radi izvršavanja zajedničkog cilja i svrhe postojanja", ili „kompleksna matrica sastavnih objekata u interakciji, koja ima definisane strukture cilja, organizacije, funkcionalnosti, informacija, komunikacija i menadžmenta*" [6,9].

U formi *sistema* mogu se struktuirati sva stanja funkcionisanja materijalnih, energetskih, informacionih, vrednosnih ili kombinovanih tokova, uključujući kompleksne uticaje kombinacije brojnih faktora. Sistemi se razlikuju od drugih istraživačkih objekata po kompleksnosti fenomena u različitim disciplinama, uključujući i multidisciplinarnu oblast *zaštite informacija*. Kompleksnost sistema zaštite podrazumeva da se sistem sastoji od mnogo *objekata* i njihovih međusobnih inter-sistemskih i ekstra-sistemskih veza. Prema teoriji kompleksnosti, sistemi čiji su objekti delimično i slabo povezani najbolje se prilagođavaju promenama okruženja, previše veza i zavisnosti objekata blokira tokove sistema, a premalo — dovodi do raspada sistema.

Za proučavanje sistema razvijena je metodologija – *opšta teorija sistema*, gde *teorija* znači konceptualni alat ili metod u sistemu naučnog znanja. *Sistemska analiza* (SA) je sveobuhvatan pristup problemima i njihovom rešavanju. Opšta teorija sistema dovela je do stvaranja *sistemskog inženjerstva* (SE) ili tzv. *sistemskog pristupa*, kojeg karakteriše posmatranje objekata i pojava u dinamičkom odnosu prema sebi i okruženju. Primena SE metoda i principa implicira *procesni pristup*. Za analizu i definisanje procesa koriste se *modeli procesa* — struktuiran skup aktivnosti (praksi) koje opisuju karakteristike, iskustveno potvrđenih, efektivnih procesa.

2.2 SISTEMSKA ANALIZA

Sistemska analiza (SA) predstavlja sveobuhvatan pristup problemima i njihovom rešavanju. Metodologija SA obezbeđuje: *konzistentan i ponovljiv pristup primenljiv na sve projekte, smanjenje rizika od grešaka, kompletnu i konzistentnu dokumentaciju za tekuće i nove projekte i da novi tim koji nastavlja rad svojih prethodnika, brzo i lako shvati način i rezultate rada*. Metodologijom SA utvrđuju se performanse sistema, ograničenja, zahtevi za resursima i interakcije sa okruženjem. Osnovne faze sistemske analize su: *definisanje problema; prepoznavanje, definisanje i kvantizacija ciljeva; definisanje i prepoznavanje granica; analiza potreba korisnika; merenje efektivnosti; analiza funkcionisanja; određivanje ograničenja; određivanje i izbor realnih alternativnih rešenja* [6].

Za razvoj i implementaciju sistema zaštite ključni koncepti su *metodologija, tehnologija, praksa* i *odgovornosti* u zaštiti. U kompleksnim sistemima *metodologije i okviri* se koriste na bazi *internih i industrijskih* standarda, od kojih su oba podjednako značajna. Metodologije i okviri se grupišu zajedno, *dodajući strukturu* procesima menadžment sistema i primene tehnologije. Klasične metodologije za razvoj životnog ciklusa IKT sistema – ***SDLC*** (*System Development Life Cycle*), *vodopada, brzog odziva* itd., preuzete kao formalne metodologije i za razvoj sistema zaštite, ne mogu se lako preneti u *web* okruženje sa enormnim porastom rizika [71]. Savremeni sistemi za e-–poslovanje, koji se razlikuju od klasičnih po brzini promena okruženja i tehnologija i distribuciji servisa, zahtevaju nove pristupe procesima projektovanja i razvoja. U praksi zaštite malo je verovatno da će se primenjena metodologija podudariti sa bilo kojom poznatom. Dobar pristup je da projektant izabere metodologiju koja najviše odgovara, a onda *kreira sopstvenu*, kombinujući različite aspekte poznatih metodologija. Za zaštitu *web* aplikacija od presudnog značaja je pouzdani menadžment sistem *kvaliteta* zaštite *web* aplikacija gde je primenljiva, na primer, *metodologija vektora zaštite*, koja kombinuje standarde *ISO/IEC 15408, ISO/IEC 27001 i ISO/IEC 21827* [53, 56, 104].

2.2.1 Sistemsko mišljenje

Sistemsko mišljenje je eksplicitan naučni alat za istraživanje i dekomponovanje kompleksnih fenomena i rešavanje realnih problema sistemske analize. Dopunjuje analitičko mišljenje i fokusira pažnju na modelovanje, evaluaciju i poboljšavanje *procesa*, kao i na *dinamičke strukture*, što podrazumeva da planirane sisteme treba projektovati, a ne samo planirati.

Ako se u razvoju i upravljanju proizvodnjom ne primenjuju konzistentno SE discipline, ne uočavaju se problemi u inicijalnoj fazi, već se javljaju kada organizacija pokušava da razvije i implementira akcioni plan. Sistemsko mišljenje je: *okvir za razumevanje međuzavisnosti objekata sistema i ponovljivosti; sposobnost uočavanja obrasca promena; disciplina koja obezbeđuje viđenje celine sistema, umesto statičkih i izolovanih objekata sistema i značajan faktor za uspešan razvoj proizvoda i poboljšavanje procesa*. Može se reći da je sistemsko mišljenje *peta* disciplina za učenje organizacije pored četiri tradicionalne: *(1) menadžment ljudskih resursa, (2) mentalni model opšteg tržišta i konkurentskog odnosa, (3) opšta vizija za budućnost organizacije i (4) osposobljavanje timskog rada*. U koncept SE mišljenja ugrađena su brojna iskustva, kao što su: *kratkoročna poboljšavanja često dovode do dugoročnih problema; laka rešenja, generalno, mogu biti nikakva rešenja; brza rešenja, posebno na nivou simptoma, često dovode do još većih problema; uzroci i posledice nisu nužno blisko povezani ni u vremenu ni u prostoru, pa rešenja implementirana lako i na brzinu mogu kasnije imati negativan uticaj; ceo sistem organizacije i okruženja moraju se razmatrati zajedno* itd.

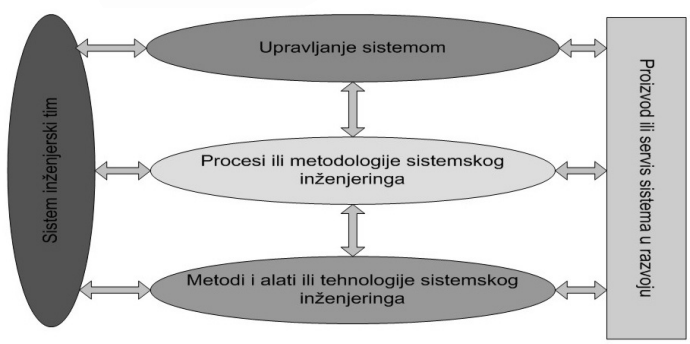
Pravila sistemskog mišljenja primenljiva na svakodnevne poslove u životnom ciklusu sistema zaštite, mogu se sabrati u sledeća:

1. *U razvoju zahteva*, u *svim fazama projekta i životnog ciklusa sistema*, uzimati u obzir viziju, ciljeve i zadatke organizacije, zahteve, probleme i potrebe korisnika.
2. U *razvoju zahteva i tehničkih rešenja* sagledati celinu i interakciju između elemenata sistema i okruženja i razmišljati iterativno i rekurzivno.
3. U *fazama tehničkog rešenja i integracije proizvoda zaštite*, sinergijski koristiti relativnu prednost integracije podsistema zaštite u IKT sistem.
4. U *razvoju sistema* uzimati u obzir ekonomske troškove, zahtev za višekratno korišćenje, organizacione, upravljačke, političke i personalne faktore.
5. U *razvoju sistema* razmatrati sistem sa što je više moguće različitih aspekata.
6. U *razvoju zahteva i tehničkih rešenja*, uvek analizirati električna i mehanička rešenja, uticaj okruženja, garanciju kvaliteta, korisničku prihvatljivost, pouzdanost, rentabilnost, mogućnost održavanja i testiranja itd.
7. *Planirati logističke zahteve za sve faze razvoja sistema* — zahteva i tehničkih rešenja, nabavku rezervnih delova, infrastrukturu za podršku, logističku podršku, servise, nivo održavanja i tehničku dokumentaciju.
11. Procese koji daju slabe i postepene rezultate poboljšavati kroz razvoj i inovacije organizacije.
12. Za rešavanje tekućeg problema treba razmatrati rizik, zavisnosti i ograničenja svakog raspoloživog rešenje.
13. Rizik projekta razvoja proizvoda/sistema zaštite razmatrati kroz ceo ciklus razvoja, primenom procesa planiranja projekta i menadžmenta rizika.
14. Svaki projekat zaštite planirati i uspostaviti menadžment sistem, kontrolu konfiguracije i kontrolne tačke (*milestones*) za merenje progresa projekta.
15. U razvoju zahteva i planiranju projekta krajnje korisnike smatrati glavnim delom sistema zaštite.

16. Za menadžment integrisanog projekta i razvoj integrisanog procesa, proizvoda i tima, integrisati rad, ekspertska znanja i veštine iz više disciplina i ispitivati sa više aspekata.
17. U izboru partnera i podugovarača zahtevati jednaku podelu rizika, uspeha i profita.
18. Kod nabavke komercijalnih proizvoda zaštite, ograničiti odgovornosti spoljnih faktora koji povećavaju zavisnost , kroz sporazum sa snabdevačima.
19. Kod izbora i zahteva za proizvodnju komponente zaštite, uzeti u obzir vreme od trenutka proizvodnje do nabavke.
20. Kada se definišu specifikacija sistema, ciljevi projekta, troškovi i performanse, uključivati verovatnoću i statistiku, kroz proces analize odluka i rešenja.

2.3 SISTEMSKI PRISTUP ZAŠTITI INFORMACIJA

Sistemski pristup ili *sistemsko inženjerstvo* (SE) je logički pristup struktuiranom modelovanju kompleksnih fenomena. SE je konceptualni alat za analizu i istraživanje koji obezbeđuje efikasnost i efektivnost primene IKT u poslovnim sistemima, a može se definisati kao: „*Selektivna aplikacija naučno-inženjerskih aktivnosti, koja transformiše neke operativne potrebe u opisni model konfiguracije sistema i koji, u skladu sa indikatorima merenja efektivnosti, najbolje zadovoljava te operativne potrebe*“ [6]. SE kompleksnog IKT sistem sa (pod) sistemom zaštite, integriše sve parametre na koje se odnosi i obezbeđuje optimalnu kompatibilnost svih interfejsa sistema; takođe, integriše aktivnosti svih inženjerskih disciplina i drugih specijalnosti u ukupnu inženjersku aktivnost, ističući ulogu multidisciplinarnosti i značaj liderstva, pa se može definisati i kao *menadžment tehnologije (TM)*, koji kontroliše ceo evolutivni proces životnog ciklusa sistema, a rezultira sa *definisanjem*, *razvojem* i *implementacijom* visoko kvalitetnog, rentabilnog i na vreme završenog sistema, tako da zadovoljava sve potrebe korisnika (slika 2.1).



Slika 2.1. Tri nivoa sistemskog inženjerstva

SE pokriva razvoj celog sistema, koji može, a ne mora uključivati softver. Pošto se razmatra u okviru inženjeringa sistema, SE uključuje: *menadžment sistem*, *procese* i *SE metode, alate i tehnologije*. Dekompozicijom TM na sastavne komponente može se doći do jasne predstave i razumevanja sistemskog inženjerstva.

Sistemsko inženjerstvo se primenjuje u brojnim oblastima, kao što su**:** *inženjerski menadžment***,** *upravljanje projektima, industrijski inženjering, upravljanje kvalitetom, bezbednost informacija, inženjering kompatibilnosti, kompjuterski inženjering itd.*

Koncept *sistemskog inženjerstva bezbednosti informacija* — SSE (*Security System Engineering*) definiše i uspostavlja izbalansiran skup bezbednosnih ciljeva; transformiše bezbednosne ciljeve i potrebe u dokumenta i uputstva za zaštitu; uspostavlja poverenje u tačnost i efektivnost implementiranih *tehničkih kontrola zaštite*; procenjuje prihvatljivost uticaja preostalog rizika na poslovanje i integriše sve aspekte sistema zaštite u koherentan skup kome se može verovati. Iako precizna definicija **SSE** još uvek ne postoji, jedna od mogućih definicija je:

> „*SSE je oblast SE koja primenjuje naučne i inženjerske principe za identifikaciju bezbednosne ranjivosti informacione imovine i smanjenje ili ublažavanje faktora rizika koji prate te ranjivosti. Generalno, osnovu SE i SSE čine sistemsko mišljenje* i *sistemska analiza*“ [60].

Međutim, namena i ciljevi SSE dobro su poznati — *razumeti bezbednosni rizik, uspostaviti bezbednosne zahteve, razviti uputstva i instrukcije za zaštitu, odrediti prihvatljivi nivo rizika i uspostaviti garantovanu bezbednost*. SSE aktivnosti i procese mogu koristiti i primenjivati brojni subjekti u zaštiti: *razvojni inženjeri, proizvođači, integratori sistema, proveravači, administratori, konsultanti, poverljivi provajderi - TTP servisa zaštite* itd. [90, 108]. SSE procesi i aktivnosti se mogu primenjivati u svim fazama životnog ciklusa i obuhvataju brojne komponente sistema zaštite: *zaštitu raspoloživosti servisa i aplikacija IKT sistema, zaštitu informacija, zaštitu računarskih sistema i mreža, fizičku i personalnu zaštitu, zaštitu od KEMZ-a (kompromitujućeg elektro magnetskog zračenja)* [73] *itd.* U SSE praksi zaštite, identifikovana su tri osnovna problema:

- nema dobro *definisanih procesa* zaštite, integrisanih u razvoju IKT sistema;
- proizvođači više koriste agilne metode za proizvodnju alata za zaštitu, umesto adekvatnih mehanizama za evaluaciju i poboljšanje SSE kapaciteta;
- u procesu evaluacije razvojnih projekata zaštite pogrešno se prenaglašavaju konačni rezultati, umesto procene *procesa* sa kojima se postižu ti rezultati.

Ove problemi su, međutim, doveli do SSE razvoja modela sazrevanja kapaciteta — CMM (*Capability Maturity Model*) procesa za proizvodnju i razvoj mehanizama, komponenti i sistema zaštite [101].

2.3.1 Modelovanje sistema zaštite informacija

U sistemskoj analizi eksperimentiše se i radi sa *modelima* realnog sistema, koji mogu imati četiri generička tipa: *realni fizički*, *narativni*, *grafički* i *matematički* model. *Fizički modeli* se koriste najčešće u proizvodnji i građevinarstvu, *narativni* (govorni i tekstualni, uključujući i tzv. *funkcionalne* i *konceptualne logičke* modele) — u svim naučnim disciplinama, a g*rafički* — u modelovanju tehničkih sistema. *Matematički* model je „*formalan opis sistema pomoću matematičkih simbola, relacija, operacija, dijagrama, dinamičkih i statičkih osobina sistema, nezavisno od početnih uslova, vrednosti ulaznih i izlaznih veličina i karaktera njihovih promena*" [22]; precizan je i koriste se za modelovanje i simulaciju kritičnih i skupih procesa.

U modelovanju IKT i sistema zaštite koriste se narativni, grafički. U kategoriji narativnih modela najviše su zastupljeni *funkcionalni modeli*. Grafički modeli u modelovanju tehničkih sistema su brojni. Primena matematičkih modela za kompleksne sisteme (IKT i zaštite) neracionalna je, teško izvodljiva, nekoherentna i ne daje najbolje praktične rezultate [86]. U SSE pristupu dobre rezultate daju *strukturno i objektno orijentisano modelovanje* [22].

2.3.1.1 Strukturno modelovanje sistema zaštite

Strukturna analiza, jedna od najstarijih tehnika sistemske analize, orijentisana je na procese i *modele procesa. K*oristi se za modelovanje poslovnih zahteva za sistem, gde su modeli struktuirane slike procesa, ulaza, izlaza i skladišta podataka.

Strukturni model posmatra sistem kao *proces* koji transformiše neke ulazne veličine u neke izlazne veličine, pri čemu se struktura realnog sistema dekomponuje i sa različitim nivoima apstrakcije prikazuju detalji sistema koji su samo relevantni za dati nivo posmatranja (apstrakcije). U ovoj interpretaciji sistem se posmatra kao koherentna celina tri ključna elementa: (1) ulaznih veličina, (2) procesa i (3) izlaznih veličina, čije se interakcije odvijaju u realnom kontekstu, koji nameće ograničenja.

Strukturni model bezbednog IKT sistema sadrži tri glavne komponente [22]:

- *skup objekata*, pasivnih i aktivnih, kojima se pristupa na kontrolisan način;
- *skup subjekata*, aktivnih komponenti koje koriste i pristupaju objektima i
- *skup pravila*, na osnovu kojih subjekti koriste i pristupaju objektima.

Strukturni modeli dekomponuju IKT sistem na objekte koje klasifikuju u kategorije skupova objekata, prema definisanim kriterijumima — jedinstvenim bezbednosnim ciljevima, jedinstvenim funkcijama itd., a odbacuju nebitne komponente i tako smanjuju kompleksnost sistema [22].

U visoko distribuiranom računarskom sistemu OSI modela sa integrisanim sistemom zaštite, *strukturni model* obuhvata sledeće bezbednosno relevantne objekte, koji se sa svoje strane mogu po potrebi dalje dekomponovati: *lokalna mreža, kanali i sredstva veze, komutacioni uređaji, centar za upravljanje i obradu, legalni i udaljeni legalni korisnici, nelegalni korisnici, nosioci informacija (magnetski, optički i dr.), izdvojene radne stanice i sistemi za bekapovanje* [22].

Primeri strukturnog modelovanja u praksi zaštite su modelovanje: *mrežne IKT arhitekture* i *mehanizma logičke kontrole pristupa* [30].

Primer: strukturno modelovanje mrežne IKT arhitekture obezbeđuje smanjenje kompleksnosti IKT sistema i projektovanog sistema zaštite u četiri koraka:

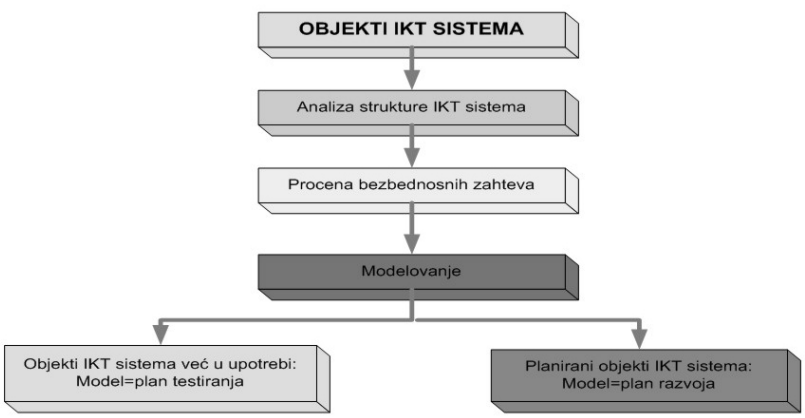
1.korak*:* analiza mrežnog plana i uklanjanje svake informacije koja nije neophodna za izradu koncepta *sistema osnovne zaštite (security baseline);*

2. korak*:* ažuriranje mrežnog plana ili delova plana (ako je podeljen u sekcije) sa stvarnim stanjem topologije mreže;

3. korak*:* definisanje *kategorija bezbednosnih zahteva* i određivanje *bezbednosnih zahteva* za svaku grupu;

4. korak: grupisanje kategorija bezbednosnih zahteva sa istim ili sličnim bezbednosni ciljevima u jedinstvene *zone bezbednosti*.

Osnovni problemi i nedostaci strukturnog modelovanja i klasičnog objektnog pristupa, nastaju iz najmanje dva razloga — podele na aktivne (*subjekte*) i pasivne (*objekte*) i složene realizacije *objekta*, koja je posledica ispunjavanja direktnog ili po pravilu indirektnog zahteva korisnika za određenim informacionim ili bezbednosnim servisom, od nekog objekta IKT/sistema zaštite. Primer izlaza *strukturnog modela* sistema osnovne IKT zaštite prikazan je na slici 2.2 [30].



Slika 2.2. Izlaz strukturnog modelovanja sistema osnovne zaštite IKT sistema

Strukturni model, takođe, ne podržava algoritamsku dekompoziciju sistema, kojom se sistem deli na funkcionalne objekte i prikazuje *funkcionalnim modelom*, pošto nije primenljiv u ranoj fazi analize i modelovanja predmetne oblasti, dok algoritam i funkcije dekompozicije još nisu poznati [22]. Zato je nužno uvesti model „šireg spektra" koji nema takve konceptualne razlike sa realnim sistemima i koji se može primenjivati u svim fazama razvoja i realizacije kompleksnih sistema. Takve zahteve zadovoljava *objektno-orijentisani pristup* [22,30].

2.3.2.2 Objektno orijentisano modelovanje sistema zaštite informacija

U oblasti zaštite informacija još uvek se slabo koriste znanja i iskustva iz *objektno-–orijentisanog modelovanja* (OOM) IKT sistema, isprobanog metoda za smanjivanje kompleksnosti, na kojem se zasniva projektovanje savremenih IKT sistema. Kao i svaki racionalan metod za smanjivanje kompleksnosti, OOM primenjuje princip dekompozicije strukture sistema, tj. ponašanje sistema opisuje se terminima međusobnih dejstava objekata. Princip dekompozicije podrazumeva da se kompleksni sistem na najvišem nivou može dekomponovati u manji broj sastavnih i relativno *disjunktnih* (nezavisnih) objekata sa minimalnim brojem međusobnih veza. U narednim fazama dekompozicija se vrši i na nižim nivoima apstrakcije. U OOM nema pasivnih objekata i smatra se da su svi objekti istovremeno aktivni i da po potrebi izazivaju načine (*metode*) ponašanja jedan drugoga. Detalji realizacije tih ponašanja skriveni su (*inkapsulirani*), a povezivanje objekata dostupno je samo interfejsu [30]. Za razumevanje pojma *objekta* zahteva se razumevanje *klasifikacije i kategorizacije* objekata i uvođenje pojma *klase objekata*. Generički, *klasifikacija* bilo kojih objekata mora da ima sledeće atribute [30]:

- *međusobnu isključivost* – sprečava preklapanja klasa objekata u jednu kategoriju;
- *potpunost* – unija svih kategorija obuhvata sve moguće klasifikacije;
- *nedvosmislenost* – svaka klasifikacija mora biti jasna i precizna;
- *ponovljivost* – svaki proces klasifikacije mora biti ponovljiv i imati isti rezultat;
- *prihvatljivost* – svaka klasifikacija mora biti logična i intuitivna;
- *primenljivost* – klasifikacija mora biti primenljiva u različitim istraživanjima.

U sistemu zaštite *bezbednosna klasifikacija* se odnosi na bezbednosne nivoe klasa *informacija* (npr. *interne, poverljive, strogo poverljive, državna tajna).* Pod *kategorizacijom* podrazumeva se klasifikacija svih objekata informacione imovine u kategorije na koje se mogu primeniti generički atributi klasifikacije i koje imaju jedinstvene bezbednosne ciljeve.

Klasa je apstrakcija skupa stvarnih karakteristika realnog sveta, objedinjenih istom *opštom strukturom i ponašanjem*. *Objekat* je aktivni elemenat klase, ima unutrašnju strukturu i način ponašanja koji se opisuje tzv. *metodom objekta* [22].

Primer: u sistemu zaštite može se odrediti *klasa „korisnika*", koja označava opšti pojam korisnika sa opštim korisničkim podacima i metodama ponašanja, a zatim *objekat* — „*korisnik XY*" sa odgovarajućim konkretnim podacima i potencijalno različitim načinom ponašanja.

Objekti sistema zaštite poseduju svojstva *inkapsulacije, nasleđivanje i polimorfizma. Inkapsulacija* je osnovni instrument smanjenja kompleksnosti sistema, skraćivanjem unutrašnje strukture objekta, detalja realizacije i načina ponašanja i održavanjem vidljivim samo značajnih interfejsa na datom nivou. *Nasleđivanje* označava formiranje nove klase objekata na osnovu postojeće sa mogućnošću dodavanja podataka i načina ponašanja; dopušta razvoj komponenti u ranoj fazi razvoja sistema, ne narušavajući integritet složenog objekta; važan je faktor smanjenja multiplikativnih elemenata realnog sistema, gde se opšta informacija

ne duplira, nego samo ukazuje na postojeće promene, a klasa-potomak postaje koren nove klase-naslednika. *Polimorfizam* je sposobnost objekta da se svrsta u više od jedne klase, što zavisi od aspekta i kriterijuma posmatranja objekta; omogućava grupisanje objekata sa sličnim karakteristikama. Nasleđivanje i polimorfizam zajedno daju OOM-u sposobnost skalabilnosti (modularne nadogradnje), što je poželjan zahtev za sisteme zaštite, koji se konstantno modifikuju, zbog čestih promena okruženja (tehnologija IKT sistema, pretnji itd.) i relativno skupih tehnologija zaštite.

Grane objekata i *nivoi dekompozicije* još su dve bitne karakteristike objekata u OOM. Realni objekti po pravilu poseduju nekoliko relativno nezavisnih karakteristika, koje se u modelu objekta nazivaju *grane objekta*.

Primer: U OOM sistema zaštite za razvoj *integrisanog* sistema zaštite informacija i smanjenje kompleksnosti uvode se dva skupa grana objekata [22, 30]:

1. **skup grana objekata informacione imovine** za strukturiranje bezbednosnog cilja sistema zaštite: *raspoloživost, integritet i poverljivost informacija,* i
2. **skup grana objekata sistema zaštite** za struktuiranje sredstava za zaštitu: *upravljačke, organizaciono-operativne* i *tehničke kontrole zaštite*.

Obe grane objekata omogućavaju raznolikost aspekata posmatranja i apstrakcije objekata, bolje od *polimorfizma*, a u modelovanju i projektovanju sistema zaštite razmatraju se sa različitim nivoima detalja.

Na ove relativno nezavisne grane primenjuje se i princip *inkapsulacije*, što suštinski označava da je svaka grana „relativno nezavisna". Osim toga, ova dva skupa grana možemo nazvati *ortogonalnim*, pošto za fiksnu granu u jednom skupu (na primer, *raspoloživost*) treba razmatrati sve elemente iz drugog skupa grana (*upravljačke, operativne* i *tehničke kontrole zaštite*). Smanjenjem broja ortogonalnih skupova, smanjuje se kompleksnost sistema. Kako ortogonalnih skupova nema mnogo — dva skupa sa brojem elemenata od 3, daje 2^3=8 kombinacija ortogonalnih skupova, što je još uvek prihvatljiv nivo kompleksnosti [22].

Zakoni, drugi normativni akti i standardi usmereni su na subjekte u informacionom okruženju, bez obzira na organizacione nadležnosti (pravna ili fizička lica), dok se administrativne mere odnose na sve subjekte u organizaciji. Proceduralne mere odnose se na pojedince ili grupe korisnika — ljudi u okviru IKT sistema, a hardversko– –softverske – na tehničke mehanizme i protokole zaštite. Na taj način, prelaskom sa jednog na drugi nivo zaštite primenjuje se karakteristika *nasleđivanja* – svaki sledeći nivo se ne menja, nego dopunjuje sa prethodnim nivoom zaštite, što omogućava primenu *slojevitog koncepta zaštite*, kao i *polimorfizma* – na primer, subjekti — ljudi nastupaju u različitim ulogama, kao donosioci administrativnih mera, faktori upravljanja sistemom zaštite i obični korisnici tih mera zaštite.

Pojam *nivoa dekompozicije* važan je ne samo za vizuelizaciju, nego i za sistemsku analizu složenih objekata, predstavljenu u hijerarhijskoj formi. Sama po sebi ova karakteristika je trivijalna: ako se tekući nivo hijerarhije razmatra sa nivoom detalja — $n > 0$, sledeći se razmatra sa nivoom detalja $(n-1)$, pa $(n-2)$ itd. Objekat sa nivoom detalja $n = 0$ smatra se da je atomizovan (nedeljiv). Nivoi dekompozicije variraju kako za objekte tako i za grane objekta.

Korisna konkretizacija dekompozicije u OOM-u su *komponente objekta i kontejner*. *Komponenta objekta* se može definisati kao višestruko korišćeni sastavni elemenat objekta, a *kontejner* sadrži više komponenti i formira opšti kontekst međudejstava sa drugim komponentama i okruženjem. Jedan kontejner može imati ulogu komponente drugog kontejnera. Pojmovima *komponente* i *kontejnera* mogu se na suštinski način predstaviti istovremeno *sistem zaštite* informacija i objekti *informacione imovine* koji se štite. Takođe, pojam *kontejnera* može odrediti granice zone zaštite (perimetra ili domena zaštite). Komponente objekta raspolažu sa svim karakteristikama OOM-a: *inkapsulacija*, *nasleđivanje* i *polimorfizam komponenti objekta* [22].

2.4 PROCESNI PRISTUP ZAŠTITI INFORMACIJA

2.4.1 Definicija, struktura i kontrola *„procesa"*

Primena SSE metoda i principa implicira *procesni pristup* koji podrazumeva da se u svim fazama životnog ciklusa sistema zaštite primenjuje sistemska analiza sa dekompozicijom procesa do atomizovanih aktivnosti. Procesi zaštite zahtevaju menadžment sistem, samo dobro definisani i mereni procesi se mogu upravljati. *Statističko upravljanje procesa,* jedna od najmoćnijih metoda menadžment sistema procesa, zahteva primenu metrika i merenja performansi procesa. Karakteristike, iskustveno potvrđenih, efektivnih procesa opisuju *modeli procesa* koji struktuiraju skup aktivnosti (praksi). Generalno, organizacije sa SSE pristupom i primenom modela procesa, rentabilno zatvaraju proizvodni ciklus i ostvaruju znatan povraćaj investicija.

Reč „*proces*" potiče od latinske reči „*procedere*", što znači *kretati se* ili *ići napred,* odnosno, od imenice „*processus*" — proces. Dakle, *proces* je sve oko nas i u nama — od vožnje automobila, kuvanja, studiranja, turističkog putovanja, do projektovanja sistema, dizajniranja proizvoda itd. Proces NIJE jednostavan dijagram toka na najvišem nivou apstrakcije, niti životni ciklus sistema, alat ili tehnologija. Postoji nekoliko definicija procesa od kojih svaka usmerava pažnju na određeni aspekt funkcionalnosti i značaja procesa.

Prema IEEE: Proces je sekvencijalno izvršavanje aktivnosti po utvrđenom redosledu, uključujući definisanje, ograničenja, resurse i predefinisane ulazno/izlazne parametre aktivnosti.

U teoriji zaštite informacija [86]: Proces zaštite je transformator ulaznih veličina u očekivano poboljšane (veće) izlazne veličine.

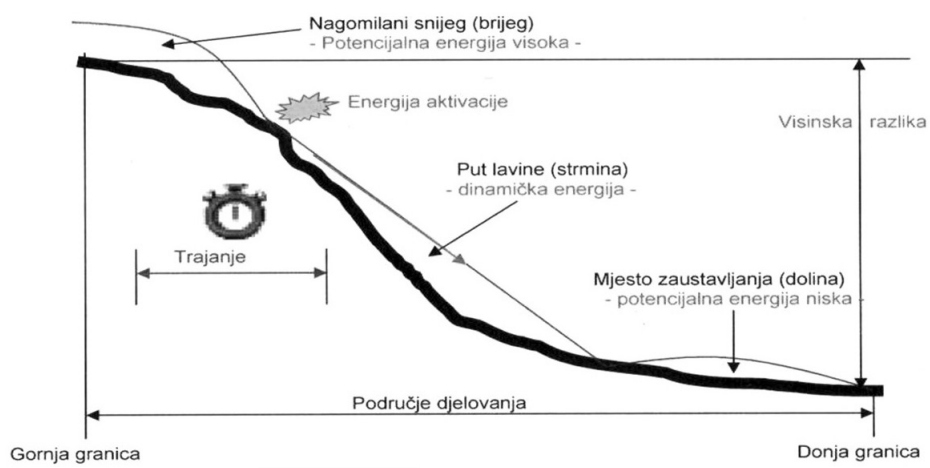
U modelima sazrevanja procesa [9, 18]: Proces je integrator ključnih atributa posla – osposobljenih ljudi, tehnika i alata i metoda i procedura za izvršavanje zadataka.

Integralna definicija procesa [30]: Proces je sekvencijalno izvršavanje aktivnosti koje transformišu ulazne veličine u očekivano veće/bolje izlazne veličine, integrišući rad ljudi, tehnologija i metodologija, koristeći iste resurse za postizanja zajedničkog cilja i obezbeđujući konstruktivan, visoko-produktivan fokus na poslove.

Definisan proces uključuje uloge i odgovornosti ljudi, odgovarajuće alate i tehnike, sekvencijalne korake —šta raditi, i procedure i metode —kako izvršavati zadatke, kao i njihove međusobne odnose.

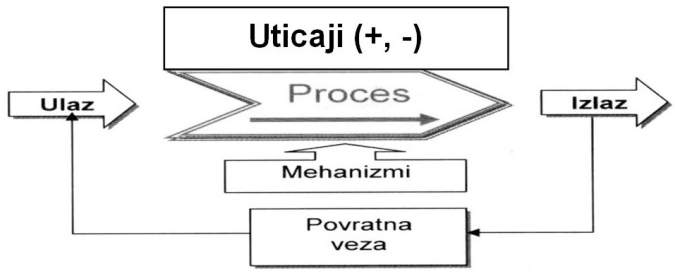
Osnovne komponente svakog procesa čine: struktura i granice, ulazni materijalni i energetski resursi, energija aktivacije, vrsta i oblik transformacije, trajanje, izlazni materijalni i energetski resursi i oblici. Komponente i tok procesa mogu se sagledati na sledećem primeru (slika 2.3):

Primer procesa snežne lavine: Na brdu se skuplja sneg, stvara kritična masa i obezbeđuju potrebni ulazni resursi i potencijalna energija za početak procesa lavine. Topljenjem snega i pomeranjem pokreće se proces lavine, a potencijalna energija se transformiše u dinamičku (početak procesa). Kretanjem niz padinu sneg dobija dodatnu kinetičku energiju (tok procesa). U dolini lavina uništava područje zaustavljanja (rezultat procesa). Dinamička energija se ponovo pretvara u potencijalnu (dolina je na nekoj nadmorskoj visini), što predstavlja benefit procesa. U ovom primeru trajanje procesa je onoliko koliko postojeći resursi (količina snega) to omogućavaju, od pokretanja do smirivanja lavine (ograničeni resursi procesa) [46].



Slika 2.3 Proces lavine [46]

Na svaki proces deluju pozitivni uticaji, koji pojačavaju elemente procesa (efekte i dobit) i negativni uticaji koji slabe efektivnost procesa, u svakom smislu (slika 2.4).



Slika 2.4 Uticaji na proces [46]

Parametri ili karakteristike procesa, mesta gdje se odvijaju događaji bitni za dalje ponašanje i kontrolu procesa, uključuju: vlasnika, obim i granice (humane, vremenske, finansijske), produktivnost (efektivnost i efikasnost), adaptivnost (fleksibilnost i skalabilnost), merljivost (mogućnost korekcije grešaka i prevencija), dokumentovanost, uticaj na okolinu i obradu rezultata (kontrola, provera, verifikacija i validacija). Karakteristike procesa određuju kvalitet procesa i zadovoljenje svih ciljeva realizacije procesa. Od parametara procesa zavise i njegove funkcije koje moraju biti, definisane, pregledne i transparentne. Bitne funkcije procesa su:

- granične vrednosti: ulazne i izlazne veličine i njihove granice;
- tip transformacije: materijalni, energetski, informacioni, finansijski, prostorni;
- povratne veze (+,-): informacione, komunikacione, energetske, materijalne itd;
- stabilnost i upravljivost: distribucija, otklon od srednje vrednosti;
- ponovljivost: vremenska i finansijska komponenta realizacije kvantiteta, kvaliteta, provere, verifikacije i validacije.

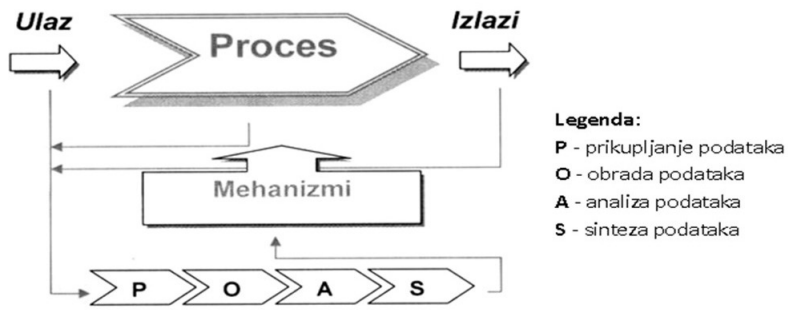
2.4.2. Menadžment sistem procesa

Menadžment sistem procesa uključuje *razvoj, dizajn, implementaciju, održavanje, nadzor, kontrolu i poboljšavanje procesa*. Optimalni rezultati menadžment sistema procesa su maksimalan profit i iskoristivost resursa uz minimalno ulaganje.

Ključne *uloge i odgovornosti* za efektivni menadžment sistem procesa uključuju *sponzora, vlasnika, menadžera i izvršioca* procesa [46]. *Sponzor* je iskusan menadžer, koji obezbeđuje smernice i resurse za poboljšavanje procesa. *Vlasnik* se obično nalazi izvan procesa, ali je direktno odgovoran za ceo proces i pokretanje inicijative za poboljšavanje procesa. *Menadžer* procesa radi u procesu i odgovoran je za: *diskretne delove procesa, dnevne proizvodne performanse, direktno upravljanje zaposlenim u procesu, odnose sa snabdevačima, obezbeđenje metrike procesa, obezbeđenje izveštaja o performansama i ideja za poboljšavanje procesa*. *Izvršilac procesa* radi u procesu, a menadžeru procesa isporučuje rezultate procesa, u skladu sa standardima i obezbeđuje metriku procesa, izveštaje o performansama i ideje za poboljšavanje.

Optimalni menadžment sistem procesa obezbeđuje maksimalno mogući višak vrednosti za dati proces u datom kontekstu, sa minimalnim utroškom resursa, što postaje uslov preživljavanja na tržištu i osnova za dalji razvoj savremene organizacije.

Statističko upravljanje procesa, jedna od najmoćnijih metoda menadžment sistema procesa, obuhvata prikupljanje, obradu, prezentacije i analizu podataka i omogućava uvid u ponašanje, optimalni menadžment i poboljšanje procesa. Statističko upravljanje procesa obezbeđuje (slika 2.5) uspostavljanje i održavanje *kvantitativnog* razumevanja performansi standardnih procesa organizacije, podršku sistemu kvaliteta i podatke o performansama procesa, osnovnom sistemu i modelima za *kvantitativno upravljanje projektima* organizacije.



Slika 2.5 Statističko upravljanje procesa [46]

Za statističko upravljanje procesa neophodno je obezbediti merenje performansi procesa, tj. rada, vremenskog ciklusa, efikasnosti uklanjanja defekata procesa itd. Merenje performansi procesa omogućava identifikovanje procesa koji su konzistentni, predvidljivi, očekivano se najbolje izvršavaju ili pokazuju neobično ponašanje. Merenje performansi procesa takođe obezbeđuje identifikovanje oblasti procesa za poboljšanje i za merenje i analizu efekata poboljšanja procesa.

Primer: Merenja performansi procesa za proizvodnju softvera su: trajanje, rad, veličina, broj otkrivenih defekata, broj unesenih defekata, neusklađenost, kašnjenje itd.

Za predviđanje performansi i procenu efekata promene procesa koriste se modeli performansi procesa. Model performansi procesa je reprezentacija procesa sa podacima o istoriji performansi, a može se uspostaviti na bazi osnovnog sistema performansi, *jedinstvene karakteristike procesa, procenjenih efekata promena procesa i tekućih performansi procesa.* Jednostavan model performansi procesa je procena, za svaku fazu životnog ciklusa procesa: trajanja, rada, veličine, unesenih defekata i detektovanih defekata.

*Osnovni sistem merenja performansi procesa j*e sistem indikatora progresa (benchmark) rezultata procesa za poređenje performansi aktuelnih procesa prema očekivanim performansama procesa. Primer jednostavnog osnovnog sistema merenja performansi procesa po fazama procesa (1, 2, 3, 4) prikazan je u tabeli 2.1.

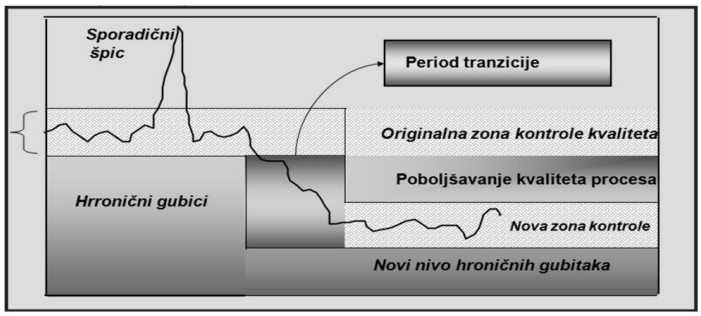
Tabela 2.1 Jednostavan model performansi procesa

Merenje	Faza 1	Faza 2	Faza 3	Faza 4	Total
P1 – velika brzina, vreme izbacivanje na tržište					
Trajanje	3	8	8	6	25
Rad	200	300	300	200	1000
Ubačeni defekti	30	15	20	5	70
Detektovani defekti	15	10	20	15	60
P2 – visok kvalitet, kritičan za misiju					
Trajanje	6	16	16	12	50
Rad	400	600	600	400	2000
Ubačeni defekti	30	15	20	5	70
Detektovani defekti	28	14	20	7	69

Aktivnosti za menadžment performansi procesa zaštite uključuju:

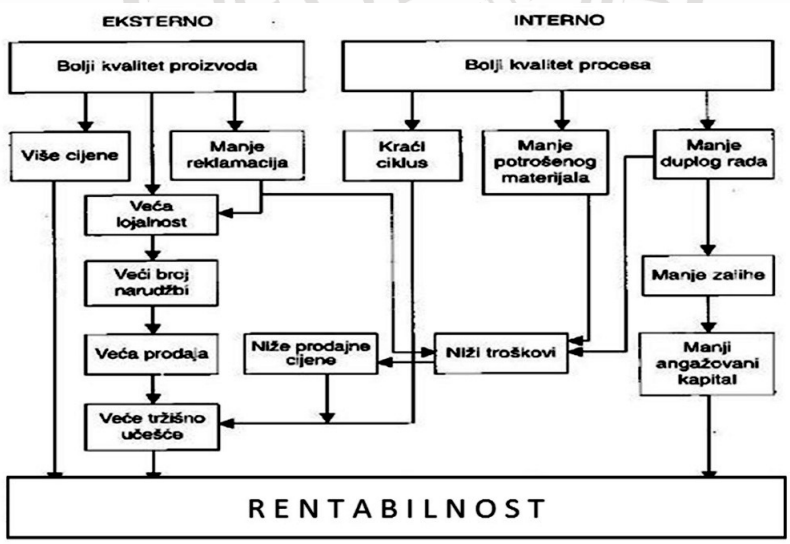
- definisanje ciljeva zaštite,
- definisanje/rafiniranje procesa,
- definisanje/rafiniranje/uspostavljanje merenja procesa,
- (re)uspostavljanje osnovnog sistema (*baseline*) performansi procesa,
- kreiranje modela performansi procesa,
- kalibracija/vrednovanje modela performansi procesa,
- upotreba modela za predviđanje rezultata procesa ili promena definicije procesa,
- implementacija perspektivnih promena,
- merenje i analiza performansi procesa,
- izveštaj o prilikama za promene i problemima.

Za analizu performansi procesa mogu se koristiti brojni alati, kao što su: *histogrami, Pareto dijagrami, dijagrami toka/trenda procesa, kontrolne tabele* itd. Svaki proces u fazi realizacije (toka procesa) ima standardna odstupanja (standardnu devijaciju), koja se kreće u nekim prihvatljivim granicama *zone kontrole* kvaliteta procesa. Takođe, tok procesa prate manji ili veći hronični gubici (greške, otpad...). Svaka devijacija izvan granica standardne devijacije procesa (sporadični špic) predstavlja uzroke kašnjenja procesa i zahteva ponovljeni rad. Cilj poboljšanja svakog procesa je da se hronični gubici smanje, sporadični špicevi što pre otklone ili proaktivno spreče, a granice zone kontrole procesa smanje. Na slici 2.6. prikazan je primer interpretacije statističke kontrole procesa u menadžment sistemu i poboljšavanju procesa.



Slika 2.6 Interpretacija statističke kontrole procesa

Menadžment sistem procesa je od odlučujućeg značaja za kvalitet procesa i proizvoda rada tih procesa. *Kvalitet procesa* je merilo upotrebne vrednosti određenog proizvoda/usluge tog procesa. *Proces je kvalitetan ako zadovoljava zahteve korisnika i ako odgovara korisničkoj nameni***.** *Kvalitet proizvoda* je određen kvalitetom procesa za njegovo projektovanje, razvoj, proizvodnju i održavanje. Glavne determinante kvaliteta posla su *ljudi, procesi, tehnologije i metodi* primene tehnologija i izvršavanja radnih zadataka. Menadžment sistem kvaliteta procesa, koji integriše i disciplinuju rad ljudi i primenu tehnologija i metoda rada, obezbeđuje efektivno, efikasno i rentabilno poslovanje, veći kvalitet proizvoda i konkurentnost (slika 2.7).



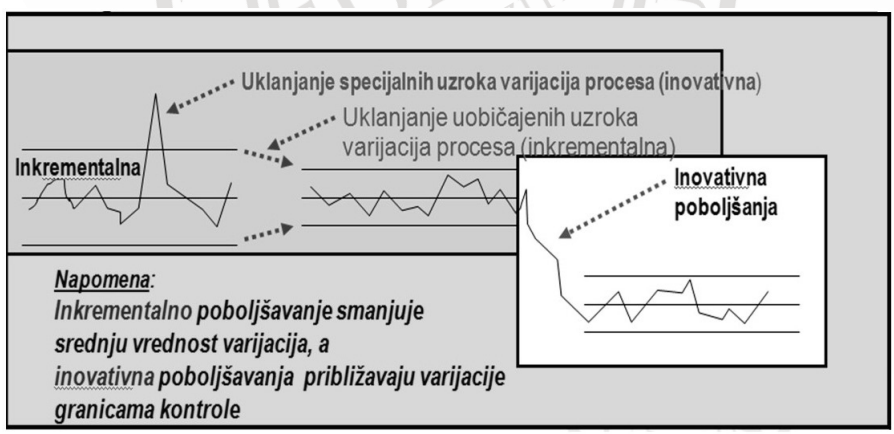
Slika 2.7 Rentabilnost poslovanja [*31*]

2.4.3. Tipovi kvaliteta procesa

U odnosu na kvalitet, procesi se mogu klasifikovati kao *improvizovani, poboljšani i institucionalizovani.*

Improvizovane procese neformalno i ad hoc izvršavaju korisnici (praktičari). Procesi nisu formalno opisani, definisani, zahtevani i izvršavani. Izvršavanje procesa zavisi od sposobnosti i motivacije praktičara koji ih primenjuju. Razumevanje statusa procesa je ograničeno. Proces je generalno nestabilan, a organizacija nema vremena za njegovo poboljšavanje. Zato se proces konstantno popravlja i ponovo uspostavlja.

Poboljšani procesi imaju opis konzistentan načinu na koji se izvršavaju; upravljani su, dokumentovani, definisani i kontinualno poboljšavani. Menadžment i zaposleni organizacije ih eksplicitno podržavaju. Procesi su dobro kontrolisani, a ponovljivost se regularno *evaluira* i nameće. Konstruktivno se koriste metrike i *rezultati* rada procesa, a tehnologije i metodi rada se uvode na disciplinovan način. Poboljšavanje procesa je strategijski zadatak, a može biti *inkrementalno*, koje smanjuje srednju vrednost varijacija i *inovativno*, koje merljivo poboljšava proces, metod i tehnologiju organizacije. Ova poboljšanja podržavaju ciljeve sistema kvaliteta i poboljšanja performansi procesa. Inkrementalno i inovativno poboljšanje često nije lako razlikovati. Jedan od načina da se uoči razlika je sposobnost identifikovanja *mikro* i *makro poboljšanja procesa*. Mikro poboljšanja su inkrementalna, a makro – inovativna. Razlike mikro i makro poboljšanja procesa mogu se sagledati analizom *statističke kontrole procesa* (slika 2.8).



Slika 2.8 Inkrementalna i inovativna poboljšanja procesa

Institucionalizovan proces postaje kada organizacija izgradi infrastrukturu koja podržava *efektivne, ponovljive* i *konstantno* primenjivane procese. Kultura rada organizacije nasleđuje i prenosi institucionalizovan proces na nove generacije zaposlenih, a menadžment podržava i neguje takvu kulturu rada. Ovi procesi traju duže od ljudi koji su ih definisali, formalno opisali, uspostavili, izvršavali i održavali.

Uspostavljanje stabilnog (zrelog) procesa zahteva podršku menadžmenta za neprekidno poboljšavanje procesa, primenu standardnih procesa organizacije i individualnu inicijativu. Za poboljšavanje operativnih procesa, organizacija može da preduzme brojne neformalne mere, kao što su: *uklanjanje koraka koji ne dodaju novu vrednost – usporavaju tok procesa, povećanje produktivnosti (efektivnosti i efikasnosti), povećanje adaptivnosti (fleksibilnosti i skalabilnosti) i povećanje korisničke prihvatljivosti procesa.* Stabilni procesi podržavaju poslove organizacije, ohrabruju zaposlene da uvek pružaju svoj maksimum i omogućavaju kreativan rad.

2.4.3.1 Proces najbolje prakse

Proces najbolje prakse se može definisati kao proces koji je: *formalno opisan i definisan, dostupan* (dokumentovan)*, usklađen sa standardima* (prihvatljiv)*, ponovljiv* (kontinualno poboljšavan)*; ima nekoliko vitalnih i više trivijalnih rešenja* (efikasan i skalabilan) *i dovodi do željenog rezultata* (efektivan)*; otporan na vanredne događaje* (adaptivan)*, podražava model procesa* (obezbeđuje indikatore progresa i okvire) *i legalan* (usklađen sa zakonom i regulativama). Procese dobre ili najbolje prakse zaštite informacija tretira nekoliko relevantnih međunarodni standarda sa neznatno različitim pristupima [12, 23, 51, 65, 109].

Opis procesa može biti *neformalan* i *formalan*. Proces neformalno opisuju korisnici/praktičari koji ga primenjuju. Ovaj opis je kratak, jasan, odnosi se na osnovne elemente toka procesa i nije dovoljno dobar da dokumentuje proces za njegovo definisanje. Proces formalno opisuju specijalisti, koji uključuju sve elemente dekomponovanog procesa (prema SE i OOM). Formalni opis se koristi u modelima za evaluaciju i poboljšavanje procesa (npr. SSE CMM, CMMI itd.). Za formalni opis, proces se dekomponuje u sastavne komponente – aktivnosti.

Većina uzoraka za formalni opis definisanog procesa uključuje komponente ETVX (*Entry Criteria, Tasks, Verification and eXit Criteria*) formata (IBM i SEI):

- *ulazni kriterijumi aktivnosti* (npr. da se izvrši prethodna aktivnost);
- *izlazni kriterijumi aktivnosti* (npr. proizvod rada prethodne aktivnosti);
- *ulaz aktivnosti* (npr. resursi, standard, zahtev);
- *izlaz aktivnosti* (npr. očekivani proizvod rada procesa,rezultat);
- *izvršioci aktivnosti* (*agenti* — relevantni učesnik, član projektnog tima i sl.) i
- *sledeća aktivnost* (npr. aktivnost, čiji početak zavisi od izvršavanja ove aktivnosti, može početi samo kada se ona završi).

Za formalan opis procesa treba poznavati elemente dekompozicije komponenti i aktivnosti procesa, kao što su: *namena, izvršioci, ulazne veličine, proizvod rada, kriterijum za početak, kriterijum za uspešno kompletiranje*, *potreban rad* za izvršavanje aktivnosti, *podaktivnosti* koje je potrebno izvršiti za izvršavanje neke aktivnosti, *metrika* za izvršavanje aktivnosti i *prethodna i sledeća* aktivnost. Formalni opis procesa sadrži brojne elemente, koje je potrebno dobro definisati, da bi korisnik mogao razumeti, upravljati i poboljšavati proces [86].

Za definisanje procesa zaštite potrebno je da bude *formalno opisan* i da uključi odnosnu *politiku, standarde* i *procedure* zaštite, sa sledećim atributima procesa: *naziv, namena,*

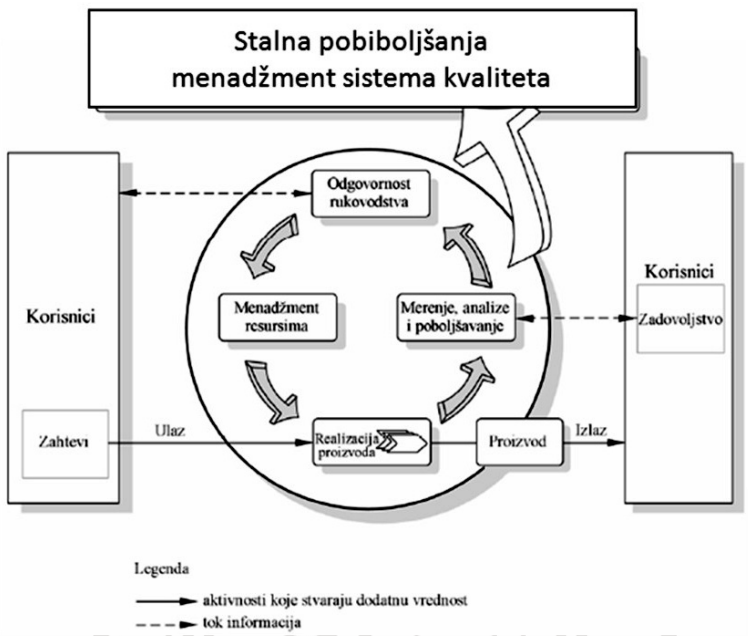
obim, ulazi, ulazni kriterijumi, aktivnosti, procedure, specifikovane uloge, merenja, validacija, obrasci, izlazi i izlazni kriterijumi.

Naziv procesa treba da bude jednostavan i da sadrži glagol i imenicu, npr. *dizajnirati novi proizvod zaštite. Namena* procesa treba da počinje sa „je da ...", npr. „*je da izbaci novi proizvod zaštite na tržište, sa najnovijom tehnologijom i u planiranom roku*". *Obim* procesa precizno definiše gde proces počinje i završava i šta je specifično uključeno, a šta isključeno, npr. „*Proces počinje sa izradom plana projekta zaštite, a završava kada korisnici prihvate servis zaštite. Proces uključuje sve proizvodne faze, ali isključuje dizajn pakovanja*". *Ulazi* procesa mogu biti opipljivi (npr. pisani podaci – korisnički zahtevi za servis zaštite) ili verbalni (npr. usmeni zahtevi za poboljšanje mehanizma zaštite). *Izlazi* procesa mogu biti proizvodi ili servisi zaštite, koji treba da odgovaraju bezbednosnim zahtevima i prihvaćenim specifikacijama kupca; mogu biti opipljivi (proizvod) ili neopipljivi (saveti). *Kontrole i provere* procesa zaštite mogu biti interne – kontrola kvaliteta *validacijom* ili *procedurom* organizacije, ili eksterne – kontrola specifikacija zahteva korisnika, zakonskih ograničenja, intelektualne svojine i dr. *Resursi* procesa zaštite su sve materijalne i nematerijalne stvari koje proces mora imati da bi transformisao ulazne veličine u izlazne, uključujući i ljudske resurse (razvoj svesti o potrebi zaštite, obuku i obrazovanje) i pripisane *uloge* (vlasnik informacione imovine, odgovorno lice za tretman rizika itd.) i odgovornosti ljudi za izvršavanje procesa, odgovarajuće alate i opremu, sekvencijalne korake (*šta* treba raditi), procedure i metode (*kako* se zadaci izvršavaju) i međusobne odnose ovih zadataka (tok procesa).

Definisan proces je preduslov za neprekidno i održivo poboljšanje produktivnosti, troškova i vremena rada procesa. Definisanjem se poboljšavaju komunikacija i razumevanje *tekućih* i *željenih procesa*, pomažu planiranje i realizacija planova, obezbeđuje kapacitet za izučavanje iskustava i obezbeđuju lakša analiza i poboljšanje standardnih procesa organizacije. Proces zaštite se smatra definisanim kada je *dokumentovan (formalno opisan), izvršena obuka za rad u procesu, a proces se dnevno praktično izvršava*. Da bi se izradila dokumentacija procesa, autori moraju dobro razumeti tekući proces i imati viziju o željenom procesu. Dekompozicija servisa /proizvoda procesa zaštite, prema izlaznim *rezultatima* ili *proizvodima rada procesa,* dobar je metod za početak izrade definisanog procesa zaštite.

Primer: Zahteva se definisanje *procesa za uspostavljanje funkcionalno operativnog PKI sistema***.** PKI sistem treba dekomponovati kroz formalni opis funkcionalnih modula: *CA, RA, Direktorijum* itd. Zatim, dekomponovati ove module u njihove sastavne komponente (aktivnosti): *CA u osnovne module, RA u sastavne komponente* itd., sve do osnovnih komponenti koje još uvek daju specifičan *proizvod rada*. Za dobijanje bilo kojeg *proizvoda rada,* treba dokumentovati procese za izvršavanje tog rada. Sada se za svaki izlazni *proizvod rada*, do poslednjeg nivoa dekomponovanih modula (CA itd.) i drugih komponenti na istom nivou dekompozicije, identifikuju sve *osnovne aktivnosti* (bazične prakse) koje treba izvršiti da se dobije taj *proizvod rada*. Pri tome treba obavezno obuhvatiti logističku podršku organizacije i svih organizacionih jedinica, koje na bilo koji način učestvuju u procesu zaštite, što uključuje procenu *zadataka* koje treba izvršiti za kompletiranje procesa — *ulaza i izlaza, zavisnosti, uloga i odgovornosti***.**

Dobro definisan i formalno opisan proces je u osnovi svakog sistema kvaliteta. Generički model menadžment sistema kvaliteta zasnovanog na procesima prikazan je na slici 2.9.



Slika 2.9 Model menadžment sistema kvaliteta zasnovanog na procesima

2.4.4. Modeli procesa zaštite

Kako je u sistemskom pristupu *kvalitet komunikacije i veza sa ostalim sistemima*, važan elemenat svakog sistema, sistem zaštite može se definisati i kao skup *procesa* — $\mathbf{p}_i$ koji međusobno komuniciraju, što se u matematičkoj interpretaciji može izraziti relacijom [10]:

$$\mathbf{P} = \{\mathbf{p}_1, \mathbf{p}_2, ..., \mathbf{p}^n\}$$

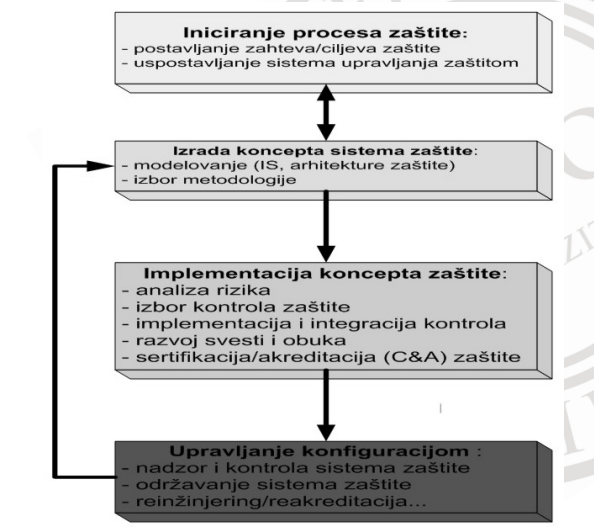
Gde se svaki $\mathbf{p}_i$ predstavlja skupom: $\mathbf{D}_i$ – bezbednosnih događaja, $\mathbf{U}_i$ – uslova iz okruženja (pretnji, bezbednosnih zahteva) i $\mathbf{F}_{si}$ – bezbednosnih funkcija koje su rezultat odvijanja procesa zaštite, a koje opisuju međuzavisnost *uslova* ($\boldsymbol{u}_i$) *i događaja* ($\boldsymbol{d}_i$) kroz skup *slučajeva* (***S***). *Skup uslova* (***U***) *i skup događaja* (***D***) definišu se *formalnim modelom* sistema. *Slučaj* ($\boldsymbol{s}_i$) je skup uslova i događaja koji su istovremeno ispunjeni. Promena ispunjenja uslova, koja prevodi sistem iz jednog u drugo bezbednosno stanje, naziva se *bezbednosni događaj*. Dakle, *formalni model* dinamičkog sistema zaštite može se predstaviti skupom:

$$(\mathbf{U, S, D, r})$$

Gde je: $U = (u_1, u_2, ..., u_n)$ – skup uslova, $P(U) = K$ – skup mogućih kombinacija uslova, $S = (s_1, s2, ..., s_k) \subseteq K$ – skup slučajeva, $D = (d_1, d_2, ..., d_m)$ – skup bezbednosnih događaja, $r = S'D'S$ – relacija dostupnosti pojave događaja d_i.

Za svaki bezbednosni događaj $d \in D$ potrebno je definisati skup preduslova – e^* i skup postuslova – $^*e$. Formalni model sistema (U,S,D,r) zadovoljava načela razdvajanja, ako postoje dve funkcije: preduslova: $D \rightarrow K$ i postuslova: $K \rightarrow D$.

Prvi korak u sistemskom pristupu zaštiti uključuje funkcionalno razlaganje na osnovne elemente sistema: *ulazne veličine, procese, izlazne veličine i okruženje*. Očekuje se da procesi koji transformišu ulazne veličine u izlazne povećavaju vrednosti izlaznih veličina i aktivnosti u odnosu na ulazne, zbog sinergijskog delovanja brojnih komponenti sistema zaštite, što ne mora biti uvek slučaj. Otuda je *suštinska potreba da se procesi zaštite neprekidno evaluiraju i poboljšavaju*, kontrolišu i kvantitativno upravljaju, sa krajnjim ciljem proaktivnog predviđanja izlaznih performansi procesa zaštite i njihovog uticaja na poslovne procese i misiju organizacije. Generički tok procesa sistema zaštite prikazan je na slici 2.10 [30].



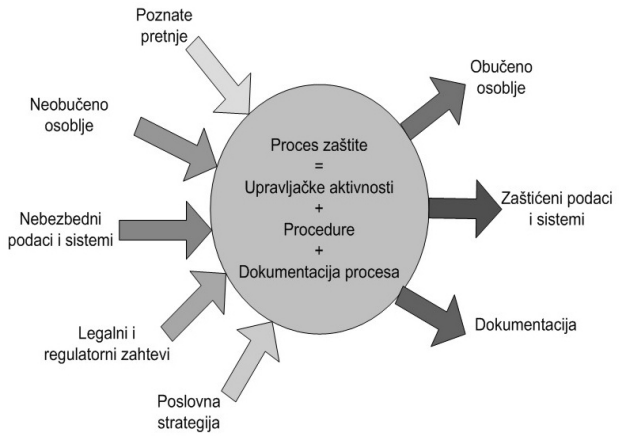
Slika 2.10 Generički proces sistema zaštite

Okruženje sistema zaštite predstavlja *kontekst*, koji ograničava i određuje namenu IKT sistema sa integrisanim (pod)sistemom zaštite u organizaciji. U odnosu na ograničenja koja nameću okruženje i poslovanje organizacije, razlikuju se struktura, politika i procedure zaštite IKT sistema. Sistem zaštite dobija ulazne veličine iz okruženja u vidu dinamički promenljivih pretnji, bezbednosnih zahteva, kompjuterskog incidenta, vanrednog događaja itd., a zatim obezbeđuje, procesima zaštite obrađene, izlaze i odgovore prema okruženju.

U sistemskom i procesnom pristupu, *sistem zaštite* se može *modelovati* kao proces koji transformiše neke ulazne veličine u neke izlazne veličine (slika 2.11). Sistem zaštite se u ovoj interpretaciji posmatra kao *koherentna* celina tri ključna elementa: *ulaznih veličina, procesa* (uključujući upravljačke aktivnosti, procedure i dokumentaciju) i *izlaznih veličina*, čije se interakcije odvijaju u realnom kontekstu – okruženju, koje nameće ograničenja sistema [30, 86].

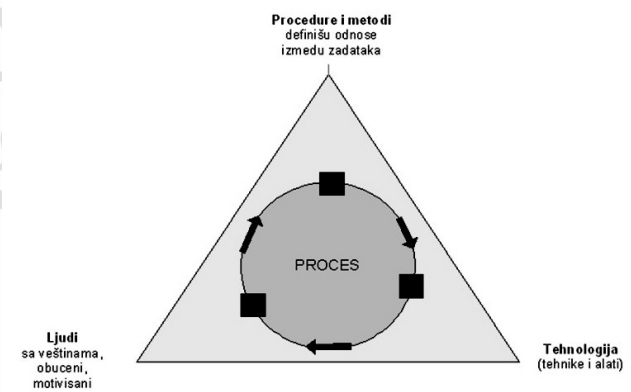
Ulazne veličine u proces zaštite mogu biti akcije, metode i operacije, odnosno, poznate pretnje, neosposobljeno osoblje, nezaštićena informaciona imovina i dr. Procesi su fundamentalni gradivni blokovi sistema zaštite, koji transformišu ulazne veličine u izlazne, objedinjuju upravljačke i druge aktivnosti zaštite, procedure i dokumentaciju procesa zaštite. Procesi zaštite dodaju novu vrednost i povećavaju kvalitet sistema zaštite. Sve što se čini

u oblasti zaštite je – proces, bilo da je dokumentovan ili nije. Procesi zaštite interaktivno deluju sa drugim procesima organizacije, pošto izlaz iz jednog procesa čini ulaz u drugi proces organizacije. Dakle, svaki proces je deo većeg procesa pa se organizacija (poslovni sistem) bilo koje veličine može posmatrati kao jedan veliki proces ili *kompleksna mreža procesa*, čiji je najviši nivo sama organizacija. *Izlazne veličine* iz procesa zaštite su procenjene pretnje i rizici, osposobljeno osoblje, zaštićeni podaci i sistemi, usvojeni plan zaštite itd.



Slika 2.11 Proces zaštite kao transformator ulaznih parametara u izlazne

Procesi zaštite se mogu definisati[1] kao *integrator tri ključna atributa posla:* (1) *osposobljenih korisnika,* (2) *tehnika i alata i* (3) *procedura i metoda* za izvršavanje zadataka (slika 2.12). Ovaj procesni model sistema zaštite ističe, da se neprekidnim poboljšavanjem procesa zaštite, integralno i konzistentno disciplinuju angažovanost ljudi, metodi rada i tehnike primene alata zaštite i *optimalno troše resursi*, čime se postiže najveća produktivnost – efektivnost i efikasnost sistema zaštite [70].



Slika 2.12 Proces kao integrator ljudi, metoda i tehnologije

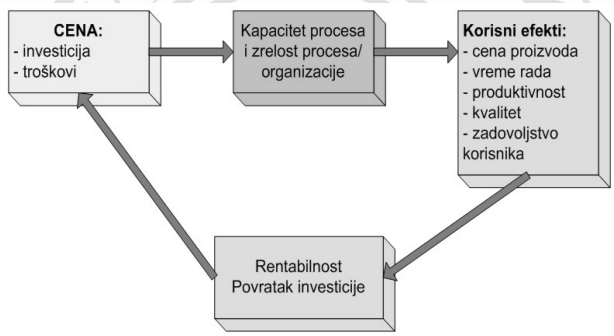
Kako je *kvalitet procesa zaštite* jedna od ključnih determinanti troškova zaštite, isporuke i kvaliteta servisa i mehanizama zaštite i kritičan faktor produktivnosti procesa IKT sistema i poslovnih procesa organizacije, prirodno je očekivati da organizacije radije usmeravaju pažnju na *poboljšavanje procesa zaštite*, nego na nabavku skupe tehnologije zaštite, ili angažovanje teško dostupnih i skupih specijalista zaštite ili unapređivanje metoda rada u praksi zaštite. Prvi korak u poboljšavanju procesa zaštite je *evaluacija* tekućeg stanja bezbednosti informacija.

1 U modelima sazrevanja procesa tipa CMM (*Capability Maturity Model*).

Model procesa nije proces nego dijagnostički alat statusa procesa. Proces se nalazi u realnom sistemu i glavama ljudi. Zato se realan proces i njegov opis u datom kontekstu, uvek razlikuje od opisa u modelu procesa. Model procesa može se koristiti za brojne aktivnosti, kao što su [70]:

- dijagnoza stanja tekućih praksi organizacije metodom evaluacije,
- uspostavljanje ciljeva i prioriteta za poboljšanje procesa,
- uspostavljanje stabilnih procesa poboljšanjem procesa organizacije,
- određivanje početne tačke projekta za poboljšanje procesa,
- agregacija iskustava iz primene procesa u organizaciji,
- definisanje značaja poboljšanja procesa za organizaciju itd.

Primena nekog modela (PDCA[2], SSE CMM, CMMI…) procesa u organizaciji ima svoju *cenu*, *prednosti* i *nedostatke* (slika 2.13). Troškovi primene nekog modela procesa variraju u zavisnosti od brojnih faktora: ciljeva, veličine, kulture rada, strukture i tipa procesa organizacije. Generalno, organizacije sa SE primenom modela procesa rentabilno zatvaraju proizvodni ciklus i ostvaruju znatan povraćaj investicija [70].



Slika 2.13 Troškovi, prednosti i nedostaci uvođenja modela procesa

2 PDCA (*Plan, Do, Check, Act*) – model procesnog pristupa primenjen u ISMS standardu.

2.5 REZIME

Sistemsko inženjerstvo (SE) je logički pristup za struktuirano modelovanje kompleksnih sistema i konceptualni alat za analizu efikasnosti i efektivnosti sistema. S*istemsko inženjerstvo bezbednosti informacija* — SSE definiše i uspostavlja izbalansiran skup bezbednosnih ciljeva, transformiše bezbednosne zahteve u dostignute bezbednosne ciljeve. Osnovu SE i SSE čine *sistemsko mišljenje* i *sistemska analiza* koja predstavlja sveobuhvatan pristup rešavanju problema. Metodologijom SA utvrđuju se performanse sistema, ograničenja, resursi i interakcije sa okruženjem.

U SA eksperimentiše se i radi sa *modelima* realnog sistema. U modelovanju IKT i sistema zaštite koriste se narativni i grafički modeli. Primena matematičkih modela za kompleksne sisteme ne daje najbolje praktične rezultate. Za potrebe SSE analize, bolje rezultate daju *strukturni* i *objektno orijentisani modeli (OOM),* čija je osnovna prednost smanjenje kompleksnosti. *Strukturni model* sistem posmatra kroz *subjekte* koji izvršavaju dozvoljene aktivnosti nad *objektima* sistema, prema utvrđenim *pravilima*. Ovaj model nije primenljiv u ranoj fazi analize. *OOM*, koji nema konceptualne razlike sa realnim sistemima, može se primenjivati u svim fazama razvoja i realizacije kompleksnih sistema. *OOM* karakterišu *inkapsulacija*, *nasleđivanje* i *polimorfizam*. Za smanjenja kompleksnosti zaštite informacija uvode se grane objekata za struktuiranje bezbednosnog cilja i za struktuiranje sredstva za postizanje tog cilja.

Procesni pristup podrazumeva da se u svim fazama životnog ciklusa sistema zaštite primenjuje SA, sa dekompozicijom procesa do atomizovanih aktivnosti. Proces je sekvencijalno izvršavanje aktivnosti koje transformišu ulazne veličine u izlazne, integrišući rad ljudi, tehnologija i metodologija i koristeći zajedničke resurse radi postizanja zajedničkog cilja. Za kvalitet procesa i proizvoda rada tih procesa, od odlučujućeg značaja je menadžment procesa. Menadžment procesa uključuje *razvoj, dizajn, implementaciju, održavanje, nadzor, kontrolu i poboljšavanje procesa*. Jedna od najmoćnijih metoda menadžmenta procesa, *statističko upravljanje procesom,* obuhvata prikupljanje, obradu, prezentacije i analizu podataka. Za predviđanje performansi i procenu efekata promena procesa koriste se *modeli performansi procesa***.** U odnosu na *kvalitet,* jednostavna klasifikacija procesa je na *improvizovane, poboljšane i institucionalizovane.*

Modeli procesa najboljih praksi formalno opisuju procese i obezbeđuje povratak investicije. Za formalan opis procesa treba poznavati elemente dekompozicije komponenti i aktivnosti procesa, kao što su: *namena, izvršioci, ulazne veličine, proizvod rada, kriterijum za početak, kriterijum za uspešno kompletiranje*, *potreban rad*, *podaktivnosti*, *metrika* za izvršavanje aktivnosti i *prethodna i sledeća* aktivnost. Neformalni metodi poboljšavanja procesa zahtevaju logičku analizu procesa i poboljšavanje *produktivnosti, adaptivnosti i korisničke prihvatljivosti*.

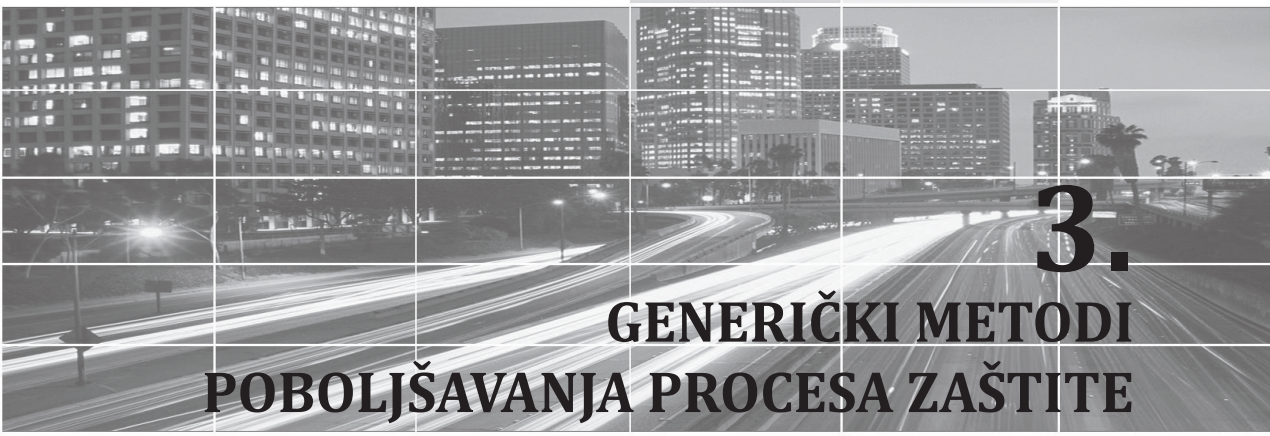
2.6 PITANJA ZA PONAVLJANJE

1. Sistem se definiše kao:
   a. uređeni i integrisani skup podataka, procesa, interfejsa, mreža, tehnologija i ljudi u cilju podrške i poboljšanja poslovnih operacija, upravljanja, planiranja, predviđanja, koordinisanja i donošenja odluka
   b. skup objekata i njihovih međusobnih veza usmerenih ka ostvarivanju zajedničkog cilja
   c. skup elemenata koji je nešto više nego zbir svih njenih delova
   d. skup svrsishodno povezanih objekata (komponenti, elemenata) sa njihovim međusobnim dinamičkim vezama, odnosima i uticajima i interakcijom sa relativnim okruženjem, radi izvršavanja zajedničkog cilja i svrhe postojanja.
2. Sistemski pristup ili sistemsko inženjerstvo je:
   a. logički pristup struktuiranom modelovanju kompleksnih fenomena
   b. softverska aplikacija za podršku sistemske analize
   c. aplikacija naučno-inženjerskih aktivnosti koja transformiše operativne potrebe u model
   d. menadžment tehnologije evolutivnog procesa životnog ciklusa sistema.
3. Sistemsko mišljenje je:
   a. naučni alat za istraživanje kompleksnih fenomena i realnih problema
   b. okvir za razumevanje međuzavisnosti, ponovljivosti i uočavanje obrazaca promena, koji fokusira pažnju na procese i dinamičke strukture
   c. drugi naziv za mišljenje analitičara sistema koje nema posebna pravila
   d. disciplina koja dopunjuje analitičko mišljenje i obezbeđuje viđenje celine sistema.
4. Sistemska analiza je:
   a. sveobuhvatan pristup problemima i njihovom rešavanju
   b. metodologija kojom se utvrđuju performanse sistema, ograničenja, zahtevi za resursima i interakcije sa okruženjem
   c. softverska aplikacija za podršku procesima analize kompleksnih sistema.
5. Metodologije i okviri su:
   a. mehanizmi menadžmenta koji dodaju strukturu procesima zaštite
   b. grupišu se zajedno, najčešće kao *upravljačke kontrole zaštit*
   c. grupišu se zajedno, najčešće kao operativne *kontrole zaštite*
   d. razvijaju se na bazi internih i/ili opšte prihvaćenih industrijskih standarda
   e. uspostavljaju se u kontekstu organizacije za svaki projekat zaštite.
6. Za razvoj programa i sistema zaštite, generalno se koriste metodologije na bazi:
   a. politike zaštite
   b. SDLC (razvoja životnog ciklusa)
   c. upravljanja rizikom
   d. najbolje prakse zaštite
   e. ISO/IEC 27001 i ISO/IEC 21827.
7. Standardne metodologije i okviri zaštite za razvoj IKT sistema odgovaraju:
   a. u potpunosti za projektovanje savremenih IKT sistema
   b. u potpunosti za projektovanje sistema za e-poslovanja i *Cloud Computing*
   c. samo ako su kombinovani i prilagođeni kontekstu i okruženju organizacije
   d. samo ako su usaglašeni sa normativima zaštite.
8. Osnovne komponente strukturnog modela bezbednog IKT sistema su:
   a. skup objekata, subjekata i pravila
   b. skup aktivnih *objekata*, koji koriste i pristupaju subjektima IKT sistema
   c. skup pravila sistemskog mišljenja i analize za projektovanje IKT sistema
   d. skup objekata čije se ponašanje opisuje njihovim međusobnim dejstvima.

9. Osnovni koraci u procesu strukturnog modelovanja sistema zaštite su:
   a. analiza i ažuriranje topologije mrežnog plana i grupisanje komponenti istog tipa u istu grupu
   b. analiza plana zaštite, ažuriranje topologije mrežnog plana i određivanje zona bezbednosti
   c. određivanje troškova zaštite i grupisanje komponenti istog tipa u istu grupu
   d. analiza plana zaštite i definisanje kategorija bezbednosnih ciljeva za svaku zonu.
10. Grane objekata informacione imovine u OOM sistema zaštite obuhvataju:
   a. raspoloživost, poverljivost, integritet, autentifikaciju i neporecivost
   b. upravljačke kontrole, raspoloživost, poverljivost, integritet i autentifikaciju
   c. upravljačke, tehničke i organizaciono–operativne kontrole
   d. raspoloživost, poverljivost, integritet.
11. Grane objekata za zaštitu u OOM sistema zaštite obuhvataju:
   a. raspoloživost, poverljivost, integritet, autentifikaciju i neporecivost
   b. upravljačke kontrole, raspoloživost, poverljivost, integritet i autentifikaciju
   c. upravljačke, tehničke i organizaciono–operativne kontrole
   d. raspoloživost, poverljivost i integritet.
12. Strukturna svojstva OOM za projektovanje sistema zaštite su:
   a. inkapsulacija, nasleđivanje, polimorfizam, grane objekta
   b. subjekti, objekti i pravila zaštite
   c. nivo dekompozicije, komponente objekta i kontejner zaštite
   d. grane objekta, komponente zaštite i definisan program zaštite.
13. Procesni razvoj sistema zaštite zahteva:
   a. definisane procese zaštite
   b. neformalni opis procesa zaštite
   c. kontrolu i poboljšanje procesa zaštite
   d. formalni opis procesa zaštite.
14. Osnovne komponente svakog procesa čine:
   a. uloge i odgovornosti, alati i tehnike, koraci, procedure i metode i njihovi odnosi
   b. struktura i granice, ulazni resursi, aktivacija, oblik transformacije, trajanje, izlazni resursi
   c. ulazi, uloge i odgovornosti, alati i tehnike, oblik transformacije, izlazni resursi
   d. struktura i granice, uloge i odgovornosti, alati i tehnike, ulazni resursi i procedure.
15. Definisan proces uključuje, najmanje:
   a. struktura i granice, ulazni resursi, aktivacija, oblik transformacije, trajanje, izlazni resursi
   b. uloge i odgovornosti, alate i tehnike, korake, procedure i metode i njihove odnose
   c. uloge i odgovornosti, alati i tehnike, oblik transformacije, izlazni resursi
   d. struktura i granice, uloge i odgovornosti, alati i tehnike, ulazni resursi i procedure.
16. Proces je:
   a. model skupa aktivnosti čiji je redosled izvršavanja bitan
   b. transformator ulaznih veličina u izlazne
   c. skup sekvencijalno izvršavanih aktivnosti sa zajedničkim ciljem i resursima
   d. integrator glavnih atributa posla (ljudi tehnologija i metoda).
17. Model procesa je:
   a. životni ciklus i tok realnih procesa
   b. softverska aplikacija
   c. aproksimacija realnog procesa na određenom nivou apstrakcije
   d. proces.
18. Parametri procesa su:
   a. vlasnik procesa, obim i granice, produktivnost i adaptivnost
   b. fleksibilnost, korisnička prihvatljivost, skalabilnost i obrada rezultata

c. merljivost, mogućnost korekcije grešaka i prevencija
d. dokumentovanost, uticaj na okolinu.

19. Formalni opis procesa:
    a. vrše specijalisti, koji opisuju sve elemente dekomponovanog procesa
    b. vrše korisnici koji opisuje glavne elemente dekomponovanog procesa
    c. sadrži ulaze i ulazne kriterijume, izlaze i izlazne kriterijume i očekivane proizvode rada
    d. ne obuhvata izvršioce, prethodne i sledeće aktivnosti drugog procesa.
20. Glavni koraci poboljšavanja procesa uključuju:
    a. upotrebu referentnog modela procesa i evaluaciju tekućeg stanja procesa
    b. upotrebu neformalnog modela procesa i verifikaciju dokumentacije
    c. prikupljanje objektivnih dokaza o implementaciji aktivnosti procesa
    d. verifikaciju i konsolidovanje objektivnih dokaza i definisanje glavnih nalaza
    e. definisanje profila zrelosti procesa i akcionih planova za poboljšanje procesa.
21. Institucionalizovan proces:
    a. postaje kada organizacija formalno definiše proces koji podržava menadžment
    b. postaje kada organizacija izgradi podršku menadžmenta, kulturu rada i infrastrukturu za podršku efektivnih i ponovljivih procesa
    c. postaje kada se formalno opisan proces definiše i prenese na drugi projekat
    d. obično ne traje duže od ljudi koji su ih uspostavili, izvršavali i održavali.
22. Proces *najbolje prakse zaštite* se definiše sledećim atributima:
    a. neformalno opisan, kontinualno evaluiran i usklađen sa politikom poslovanja
    b. dokumentovan, prihvatljiv, efektivan, efikasan i adaptivan
    c. formalno opisan i usklađen sa planom zaštite
    d. neformalno opisan, dokumentovan, prihvatljiv, efektivan, efikasan i adaptivan.



3. GENERIČKI METODI POBOLJŠAVANJA PROCESA ZAŠTITE

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Koncepte struktuiranog i nestruktuiranog poboljšanja procesa
- ☑ Poboljšanja produktivnosti, adaptivnosti i korisničke prihvatljivosti procesa
- ☑ Kriterijume za formalni opis i definisanje procesa
- ☑ Značaj evaluacije procesa na bazi referentnog modela procesa
- ☑ Značaj potpune (kompletirane) komunikacije za menadžment procesa

3.1 UVOD

Kvalitet sistema zaštite zavisi od kvaliteta procesa koji se primenjuju za projektovanje, razvoj, implementaciju, integraciju i održavanje servisa zaštite [18]. Ova premisa odnosi se podjednako na procese i hardversko–softverske proizvode zaštite. *Kvalitet procesa* ima brojne atribute i definicije, od kojih je sledeća univerzalno prihvatljiva — *proces je kvalitetan ako zadovoljava zahteve korisnika i ako odgovara korisničkoj nameni. Kvalitet hardversko–softverskih proizvoda zaštite u potpunosti zavisi od kvaliteta procesa za projektovanje i razvoj tih proizvoda* [30]. Glavne determinante kvaliteta proizvoda zaštite su ljudi, procesi, tehnologije i metodi izvršavanja radnih zadataka u procesima za projektovanje i razvoj tih proizvoda. Prema kriterijumima kvaliteta procesi zaštite mogu biti *improvizovani*, *poboljšani* i *institucionalizovani* [30, 86].

Za poboljšavanje i uspostavljanje stabilnih (zrelih) procesa osnovni zahtev je da su procesi definisani i formalno opisani i da se obezbedi podrška menadžmenta organizacije. Pri tome, uvek treba zagovarati primenu standardnih procesa organizacije, podsticati individualnu inicijativu i nikada ne potcenjivati kritičan značaj ljudskih resursa za izvršavanje svakog procesa. Prva mera za poboljšanje operativnih procesa je uklanjanje koraka koji ne dodaju novu vrednost procesu i koji mogu samo usporavati dostizanje postavljenih poslovnih ciljeva [84]. U stabilizaciji procesa zaštite potrebno je povećavati produktivnost

(efektivnost, efikasnost i ponovljivost) procesa, čime se oslobađa vreme za angažovanje pojedinaca na kreativnijim poslovima zaštite. Dakle, ne treba primenjivati procese zaštite, stabilisati ih i poboljšavati zbog samih procesa, nego uspostavljati toliko stabilne procese zaštite koji podržavaju pouzdan rad poslovnih IKT sistema, a time i poslovnih procesa organizacije.

3.2 KONCEPTI POBOLJŠAVANJA PROCESA ZAŠTITE

Koristi od poboljšanja (sazrevanja) procesa za organizaciju su brojne [18]:

- poboljšani procesi omogućavaju razumevanje aktivnosti i toka procesa,
- zaposleni potpunije i efektivnije razvijaju svoje potencijale,
- veća je verovatnoća uspešnog uvođenja novih tehnologija (tehnika i alata),
- sa dobro definisanim, kvantitativno kontrolisanim i kontinualno poboljšavanim procesima moguće je upravljanje svim vrstama promena i
- povećava se predvidljivost izlaznih performansi procesa.

Poboljšavanje procesa je klasični cilj menadžmenta kvaliteta procesa, a koristi brojne *neformalne* (nestruktuirane) i *formalne* (struktuirane) pristupe i metode.

3.2.1 Neformalni metod poboljšanja stabilnosti procesa zaštite

Neformalni metodi i pristupi za poboljšavanje procesa mogu biti vrlo različiti, zavisno od kulture rada organizacije, stručnosti zaposlenih i tipa procesa. Uglavnom su nestruktuirani i fokusiran na povećanje stabilnosti procesa, odnosno, otklanjanje svih glavnih uzroka smanjenja *produktivnosti*, *adaptivnosti* i *korisničke prihvatljivosti* procesa. Produktivnost procesa je očekivani izlazni rezultat, adaptivnost je sposobnost procesa da se prilagođava promenama okruženja, a korisnička prihvatljivost podrazumeva da dizajn procesa zadovoljava zahteve krajnjih korisnika.

Iskustva iz prakse ukazuju da mnogi procesi zaštite ne proizvode očekivane rezultate i pored primene solidne metodologije. Procesi zahtevaju stalni nadzor i poboljšavanje, jer samo neprekidno poboljšavan proces može postati stabilan i ponovljiv. U neformalnom pristupu moguće je korišćenje i neke metodologije za poboljšavanje *produktivnosti*, *adaptivnosti* i *korisničke prihvatljivost*. Kako to, u principu, zahteva promenu operativnih procedura, može se uključiti značajan bezbednosni rizik, pa uvek više odgovara *struktuiran, formalni pristup* poboljšanju procesa [18, 86].

3.2.1.1 Poboljšanje produktivnosti

Produktivnost procesa može se definisati kao mera u kojoj se očekivani izlaz može postići sa fiksnim skupom resursa. *Produktivnost* je najkritičniji elemenat procesa, jer ako proces ne ispuni očekivane rezultate smatra se da nije izvršen, a što je veća produktivnost, proizvodi se bolji izlazni rezultat procesa. Uzroci smanjenja produktivnosti procesa mogu biti različiti, ali se mogu svrstati u četiri opšte grupe razloga:

1. *Neodgovarajući bezbednosni ciljevi kontrola zaštite* utiču negativno na produktivnost, preusmeravajući resurse sa aktivnosti koje bi dale bolje rezultate u smanjivanju rizika. Cilj *kontrole zaštite* očigledno je neadekvatan ako značajno ne smanjuje rizik ili ne zadovolji administrativne ili zakonske zahteve.
2. *Nerealni ciljevi servisa zaštite,* ugovoreni ili definisani sa korisnikom, od presudnog značaja su za efektivnost izvršavanja procesa zaštite. Dobar primer je servis logičke kontrole pristupa i procedura autorizacije, gde nerealna očekivanja zaposlenih, koja premašuju kapacitete administratora, dovode do blokiranja servisa.
3. *Neefikasni kontrolni mehanizmi* mogu smanjiti produktivnost procesa, jer mogu brzo zastariti i postati neefikasni, ako se regularno ne nadgledaju. Na primer, digitalno potpisan dokument ne daje novu vrednost, sve dok se ne verifikuje.
4. *Slabo projektovan tok procesa zaštite* i neodgovarajuće pripisivanje odgovornosti, često je uzrok problema u procesima zaštite. Na primer, kada se nekom menadžeru dodeli odgovornost da odobrava zahteve za bezbednosno relevantne promene konfiguracije sistema, a poznato je da oni retko na vreme izvršavaju taktičke zadatke.

Glavni faktori koji utiču na produktivnost procesa su *efektivnost, efikasnost i ponovljivost*, što se može izraziti sledećom funkcionalnom zavisnošću [30]:

$$P\ (produktivnost) = f\ (efektivnosti,\ efikasnosti,\ ponovljivosti)$$

gde P = f(x) označava funkcionalnu zavisnost P od x, a ne preciznu relaciju.

Efektivnost procesa zaštite suštinski označava da se „*čine prave stvari*" i odražava u kojoj meri neka aktivnost ispunjava postavljene bezbednosne ciljeve. Efektivan proces zaštite je onaj koji smanjuje rizik u skladu sa očekivanjem (ni previše ni premalo). *Efikasnost* procesa zaštite odnosi se na „*ispravno izvršavanje pravih stvari*", a meri troškove proizvodnje izlaznih rezultata u odnosu na ulaz, što znači da će visoko efikasan proces proizvesti očekivani izlazni rezultat po najnižoj proizvodnoj ceni. *Ponovljivost procesa* ili proizvodni ciklus procesa je mera brzine sa kojom se izlazni rezultat može proizvesti. Skraćivanjem proizvodnog ciklusa (ili perioda ponavljanja) smanjuje se kašnjenje između ulaznih parametara i proizvodnje izlaznih rezultata. Sva tri atributa stabilnosti procesa su međuzavisna. Na primer, nema smisla tvrditi da je neki proces efikasan, a da nije efektivan i obrnuto.

Poboljšavanje efektivnosti procesa je sinonim za uklanjanje svake aktivnosti koja ne dodaje novu vrednost, što, u stvari, znači uklanjanje svake aktivnosti koja ne doprinosi transformaciji ulaznih parametara u izlazne rezultate. Odlučujući faktor za procenu aktivnosti koja dodaje vrednost procesu, najčešće je zdrav razum. Na primer, otvorena su pitanja koji se nivo dokumentacije i opisa procesa zahteva za smanjenje rizika na optimalan način, koje sastavne komponente sistema zaštite treba definisati, ili kako proceniti nivo osposobljenosti u zaštiti. U dokumentaciji procesa zaštite, treba koristiti formalizovane opise procedura i njih održavati ažurnim, što podrazumeva da svaki put za svaku promenu ne treba raditi novu dokumentaciju za dati proces zaštite. Prvi korak u poboljšanju efektivnosti procedure zaštite je da se proveri da li se rizik smanjuje na odgovarajući način i na prihvatljivi nivo.

Poboljšavanjem efikasnosti procesa zaštite, u skladu sa definicijom smanjenja proizvodnih troškova, ne znači da brži proces nužno postaje i efikasniji. Za poboljšavanje efikasnosti procesa klasifikuju se mere poboljšavanja na *organizacione, logičke i tehnološke* (odnose se na alate). *Organizacione mere* mogu poboljšavati efikasnost procesa promenom načina na koji procedure utiču na korisnike. Zbog toga organizacioni metodi za povećavanje efikasnosti procesa imaju veliki uticaj na korisničku prihvatljivost, što se mora uzeti u obzir u projektovanju procesa.

Primeri organizacionih metoda za povećavanje efikasnosti procesa zaštite su:
- postavljanje realističnih bezbednosnih ciljeva,
- praćenje korisničkih očekivanja,
- određivanje prioriteta poboljšavanja
- smanjenje zavisnosti od skupa specifičnih veština i
- određivanje adekvatnosti pripisanih odgovornosti.

Efikasnost se poboljšava i postavljanjem realnih ciljeva i potpisivanjem SLA sporazuma sa TTPS provajderom zaštite [13], čime se eliminiše nepotrebno praćenje ponašanja krajnjih korisnika, a administratori mogu posvetiti više vremena ključnom procesu, umesto rada sa nezadovoljnim korisnicima. Smanjenjem zavisnosti procesa od skupa specifičnih veština, takođe se povećava efikasnost zato što je lakše i jeftinije angažovati nedovoljno osposobljeno osoblje. U ovom slučaju dobit se može postići razvojem onih veština koje stvaraju veću vrednost. Logički metodi poboljšavanja efikasnosti usmereni su na poboljšavanje logičkog dizajna procedura. Ovi metodi se takođe koriste za poboljšavanje dizajna individualnih procedura korigovanjem grešaka u logičkom toku, što pak rezultira u povećanju troškova. Konačno, efikasnost se često može poboljšati automatizovanjem manuelnih procesa, posebno gde su u pitanju administrativne procedure. Kreiranje korisničkih naloga i uspostavljanje predefinisanih prava pristupa zahteva mnogo rada i vremena na velikim sistemima. Automatizovanjem ovih aktivnosti obezbeđuje se značajno povećanje produktivnosti.

Poboljšavanje ciklusa procedure odnosi se na skraćenje vremena, potrebnog da se aktivnosti procesa počnu i završe. Zato je poboljšavanje ciklusa ekvivalentno bržem izvršavanju procedure i predstavlja povećanje produktivnosti. U sistemu zaštite smanjenje ciklusa procedure najvažniji je instrument za povećanje zadovoljstva korisnika, što ne važi samo za rutinske administrativne procese nego i za procese za razvoj i nabavku operativnog i softvera za zaštitu. Vreme ciklusa možemo poboljšavati uklanjanjem aktivnosti koje ne povećavaju vrednost, bržim izvršavanjem ili smanjenjem kašnjenja između aktivnosti.

3.2.1.2 Poboljšanje adaptivnosti procesa

Adaptivnost je značajan atribut procesa zaštite koji se izvršavaju u uslovima brojnih promena okruženja (pretnji, tehnologija i dr.). Uzroci nedovoljne adaptivnosti procesa zaštite mogu biti:

- dizajn procesa reflektuje specifične, a ne generičke zahteve,
- nedovoljno se koriste uloge i odgovornosti u izvršavanju procesa zaštite,
- nedovoljno se obraća pažnja na *kompenzacione* kontrole zaštite,
- ne ugrađuju se potencijalni, realno očekivani, novi zahtevi u dizajn procesa.

Iako većina procedura zaštite odgovara generičkim zahtevima, u praksi se često dobro uklapaju u realni kontekst. Tipičan primer je zahtev za procedure za kontrolu vanrednog događaja. Takođe, ako su procedure dizajnirane za specifičan sistem, malo je verovatno da će imati koristi od kompenzacionih kontrola razvijenih u drugoj arhitekturi sistema zaštite. Procedure na bazi uloga fleksibilnije su od onih koje reflektuju organizacionu strukturu. Ovo je važno za veće organizacije gde su promene česte. Procedure i kontrole zaštite projektovane za specifični IKT sistem, ne uzimajući u obzir arhitekturu sistema, značajno smanjuju mogućnost korišćenja kompenzacionih kontrola zaštite.

Adaptivnost je sposobnost procesa da se prilagođava promenama okruženja – pretnji, tehnologija, zahteva, što određuje njegova *fleksibilnost* i *skalabilnost*. Fleksibilnost je sposobnost asimilacije novih funkcionalnih zahteva, a skalabilnost — sposobnost da proces može prihvatiti povećan obim zahteva [30, 86]:

adaptivnost = f (fleksibilnosti, skalabilnosti)

Poboljšavanje fleksibilnosti procesa uključuje modifikaciju procesa na bilo koji način koji olakšava uključivanje potencijalnih promena u funkcionisanju. Jedan od najlakših puteva za povećanje fleksibilnosti je smanjenje kompleksnosti. Ovo jednostavno odražava činjenicu da je lakše razumeti uticaj promena u jednostavnijem sistemu nego u kompleksnom sistemu. U skladu sa ovim principom, dizajn procesa treba da koristi princip modularnosti. Procedure treba da imaju ograničene i vrlo definisane obime, a zavisnost između procedura da se drže na minimumu. Kontrola toka između procedura treba da bude što više standardizovana, što uključuje minimizaciju specifičnih slučajeva koje treba rešavati. U IKT sistemu proceduralne korake koji se oslanjaju na funkcionalnost posebnih sistema, treba zameniti sa generičkim koracima gde god je moguće.

Poboljšavanje skalabilnosti je ključno pitanje u visoko distribuiranom okruženju, gde standardne procedure kao što su autorizacija i kontrola pristupa, analiza log datoteka i menadžment ranjivosti, potencijalno treba vršiti na stotinama i više platformi u nekoj prosečnoj organizaciji. Važne tehnike za menadžment skalabilnosti su određivanje prioriteta izvršavanja i isporuke rezultata procesa i upravljanje gradacijom (prava pristupa, nivoa bezbednosti, ranjivosti, pretnji itd.). Obe ove tehnike obezbeđuju skalabilnost po nekoj ceni. U prvom slučaju, skalabilnije procedure koncentrišu se na one rezultate koji najviše dodaju novu vrednost.

Primer: Procedura analize log datoteka može se napraviti skalabilnom, određivanjem prioriteta i proaktivnom kontrolom onih logova koji najviše doprinose smanjenju rizika. Slično, procedure za detekciju i otklanjanje ranjivosti mogu se napraviti skalabilnijim, koncentrišući se na ranjivosti sa srednjim ili visokim nivoom rizika u gradaciji uticaja — *nizak, srednji, visok*. Ovaj se kompromis pravi na bazi procene rizika, a omogućava upravljanje rizikom za više sistema po cenu ignorisanja ranjivosti od faktora *niskog* uticaja rizika [86].

Slična argumentacija primenjuje se kada se menja granulacija *kontrola zaštite* sa ciljem povećavanja skalabilnosti. Mehanizmi za kontrolu pristupa klasični su primer u ovoj oblasti. Održavanjem granularnih prava pristupa korisnika za milione datoteka i stotine zaposlenih, nije lako izvodljivo. Zbog toga se i korisnici koji pristupaju objektima IKT sistema i objekti kojima korisnici pristupaju, u većini IKT sistema svrstavaju u grupe, čime se bitno smanjuje granularnost kategorija objekata i prava pristupa. Međutim, za većinu srednjih i velikih organizacija ova tehnika može biti nedovoljna za stvarnu kontrolu i može biti neophodan dalji nivo apstrakcije. Osnovna ideja ovog pristupa je da, iako je granularnost smanjena, stvarni nivo kontrole je porastao zbog porasta skalabilnosti procesa u celini.

3.2.1.3 Poboljšanje korisničke prihvatljivosti

Neki proces može biti uspešan u praksi, samo ako je usklađen sa zahtevima krajnjeg korisnika i dizajniran tako da se uklapa u kulturu rada organizacije. Dizajn procesa sa aspekta korisničke prihvatljivosti uključuje sledeće relevantne faktore:

1. *kompleksnost*: smanjenje kompleksnosti dovodi do boljeg razumevanja i rešavanja problema zaštite;
2. *zavisnost od skupa specifičnih veština*: samo sa dobrim razumevanjem bezbednosnih procesa korisnici mogu prepoznati neobične pojave i nenormalne događaje; normalno je da korisnici mogu imati veštine za neke bezbednosne procese, ali se ne može očekivati da imaju specifične veštine za sve;
3. *psihološka prihvatljivost*: osnovni psihološki problem je što rutinski zadaci, kao što su brojne procedure zaštite, slabo motivišu korisnike da ih korektno i konzistentno izvršavaju. Na korisničku prihvatljivost utiče niz različitih faktora, uključujući mnoge već pomenute. Na primer, zaposleni verovatno neće biti motivisani da učestvuju u procesu koji je očigledno neefikasan i mogu biti frustrirani kada su procesi ne-efektivni. Na korisničko prihvatanje procedura jako utiču kulturološka iskustva, nivo razumevanja i psihološki faktori [30, 86]:

Korisnička prihvatljivost = f (kulturološkog uticaja, kompleksnosti, psihološkog uticaja).

Kulturološki uticaj je najznačajniji za korisničku prihvatljivost promena svake vrste. Primeri ovog fenomena su brojna propala udruživanja organizacija iz različitih zemalja zbog nemogućnosti prevazilaženja kulturoloških razlika. Moćna tehnika za uvođenje značajnijih promena je ona koja omogućava da zaposleni sami vode proces promena. Osnovna ideja je da se onima koji izvršavaju tekuću proceduru obezbedi pomoć u identifikovanju zahteva za promene i rešenja. Iako ovo ponekad zahteva dosta rada, objašnjavanja i instrukcija, velika je verovatnoća da će konačan rezultat biti trajan. Međutim, određeni nivo otpora promenama neizbežan je i u nekoj meri poželjan. Otpor promenama je koristan zato što primorava one koji uvode promene da opravdaju svoje aktivnosti, ne samo u odnosu na druga alternativna rešenja nego i u odnosu na postojeći model rada i ponašanja. Važno je imati na umu da otpor promenama deluje u oba pravca. Kako se zaposleni opiru promenama tako i oni koji ih uvode nerado menjaju svoje navike. Gde god je moguće, najbolji pristup je uvođenje malih promena na regularan način, obezbeđujući dobru pripremu zaposlenih za svaku promenu.

Ovo omogućava da se ljudi postepeno prilagođavaju novom načinu ponašanja i izvršavanja procedura i da izbegnu drastične promene.

Smanjenje kompleksnosti je važno za poboljšavanje procesa u fazi projektovanja samog procesa i *načinu komunikacije* postavljenih ciljeva i samog projekta procesa zaposlenim. Naime, nije teško shvatiti zašto se veća kompleksnost svakog fenomena prihvata sa manjim stepenom poverenja i nema razloga da je zaštita informacija izuzetak od ovog pravila. Brojne procedure iz softverskog inženjerstva mogu se primeniti na probleme pojednostavljivanja projekta procesa. U praksi, kod smanjivanja kompleksnosti, odlični rezultati postižu se primenom zdrave logike. Na primer, broj tačaka odlučivanja u proceduri dobra je indikacija kompleksnosti – više tačaka znači veću kompleksnost. Nažalost, čak i kada su procesi dobro projektovani, savremena tehnika za zaštitu informacija nije lako razumljiva za većinu korisnika, a eksperti zaštite koriste složenu terminologiju za opisivanje problema i rešenja u zaštiti. Deo problema kompleksnosti je i način na koji se informacije (razvoj svesti o potrebi zaštite, obuka i formalno obrazovanje u zaštiti) prenose korisnicima. Izbegavanje stručnih izraza, izrada i održavanje kratke, konkretne i jasne dokumentacije značajno doprinose smanjenju kompleksnosti same dokumentacije zaštite. Jednostavni alati kao što su dijagrami toka i kontrolne čekliste mnogo pomažu, posebno kada ih prate objašnjenja i primeri poznati prosečnim korisnicima.

Uticaj psiholoških faktora određuje meru u kojoj se ljudi vežu za dobijene zadatke. Psihološki faktori su brojni, uključujući sposobnost ljudi za izvršavanje zadataka i stepen zainteresovanosti za iste. Ako je sposobnost pojedinca za izvršavanje zadataka znatno iznad ili ispod zahtevanog nivoa, motivacija će verovatno opasti. U prvom slučaju nedostatak motivacije nastaje zbog stalnih neuspeha da se postigne zahtevani standard izvršavanja procesa, a u poslednjem — zbog nedostatka izazova za izvršavanje tog procesa. Aktivno upravljanje radnim zadacima obezbeđuje da zaposleni dobiju zadatke u granicama svojih sposobnosti, da su zadaci dovoljno raznoliki, stimulativni i da povećavaju motivaciju i produktivnost. Jedan od način da se ovo postigne je i korišćenje *metoda progresivnog sazrevanja procesa*, kojom se identifikuju posebne oblasti aktivnosti i relevantni skup potrebnih aktivnosti od interesa za zaposlene. Planiranju zadataka može se zatim pristupiti na sličan način kako se planiraju obuka i obrazovanje u zaštiti. Korisna tehnika je i rotiranje uloga članova tima za izvršavanje zadataka.

3.2.2 Formalni, struktuirani pristup za poboljšavanje procesa

Formalni, struktuirani pristup za poboljšanje procesa, na bazi modela procesa, zahteva potpuno razumevanje i dokumentovanje tekućih procesa, njihovo dekomponovanje, određivanje prioriteta procedura za poboljšanje, identifikovanje željene situacije za svaku proceduru, planiranje implementacije inkrementalnih poboljšanja (akcioni plan) i implementaciju i upravljanje zavisnostima između procedura. Prvi korak poboljšavanja, bilo kojeg procesa, je razumevanje tekućeg procesa. Kada se proces potpuno shvati, onda se verifikuje da li je korektno dokumentovan, pošto je dokumentacija procesa osnova za dalju modifikaciju. Proces se može dokumentovati kroz brojne *procedure* i *aktivnosti*, koje su potencijalno podržane sa jedan ili više alata (mehanizama).

Procedure se rangiraju po redosledu stabilnosti, na bazi broja problema i težine posledica poznatih elemenata procesa. Kako poboljšanje procesa zahteva vreme, primarno se treba koncentrisati na one procese koji izazivaju najteže posledice. Kada se odrede prioriteti poboljšavanja procedura, može početi rad na identifikovanju metoda za poboljšavanje. U slučajevima relativno disjunktnih procedura, gde je mala međuzavisnost procedura, poboljšanje se najbolje postiže tretiranjem svake procedure odvojeno. Ako su zavisnosti jake, lakše je ispitati i poboljšavati odnosnu grupu međuzavisnih procedura u isto vreme. U oba slučaja treba proveriti konzistentnost poboljšavanja procesa [30, 86].

Planiranje implementacije poboljšanja kroz seriju *inkrementalnih* koraka, opravdano je zbog potencijalnog rizika. Naime, u slučaju pogrešnog koraka u procesu poboljšavanja lakše se vratiti nazad sa malim pomakom, nego sa velikim pomakom. Ovaj se pristup može primeniti na poboljšanje stabilnosti, odnosno, *produktivnosti, adaptivnosti i korisničke prihvatljivosti* procesa. U svim pristupima i metodima poboljšavanja procesa od izuzetnog je značaja komunikacija između svih učesnika u procesu koje obezbeđuje dvosmerno i *potpuno* razumevanje svake poruke. Koncept *formalnog poboljšanja* procesa uključuje određene preduslove i korake. Glavni preduslov za poboljšanje procesa je da proces mora biti *definisan.* Za definisanje procesa dobro je koristiti kontrolne liste kriterijuma u formi *pitanja i dogovora* (tabela 3.1) i uzorke za opis procesa i procedura (tabele 3.2,3.3, 3.4) [18].

Tabela 3.1 *Uzorak kriterijuma za definisanje procesa*

1. Ulazni kriterijumi aktivnosti
P: Kada ova aktivnost može početi? Opiši uslove pod kojim neka aktivnost može početi. **O:** **Upisati stanje aktivnosti.** **Primer**: odobren *plan testiranja*, definisane odgovornosti za izradu p*lana projek*ta.
2. Izlazni kriterijumi aktivnosti
P: Kada je ova aktivnost kompletirana (izvršena)? Opiši uslove pod kojima se neka aktivnost može proglasiti kompletiranom i da se može odrediti sledeća aktivnost. **O:** **Upisati stanje proizvoda, lice koje izvršava aktivnost ili samu aktivnost.** **Primeri***: plan projekta* je spreman za reviziju, angažovanje kupca je potvrđeno i ugrađeno u vremenski plan projekta, kontrolni mehanizmi su spremni za promene prema planu.

3. Ulaz aktivnosti
P: Koji se međuproizvodi rada koriste za ulaz u ovu aktivnost? Ulaz je veza ili link između date aktivnosti i njenog rezultata rada. Ulazi su *proizvodi rada* —rezultati prethodnih aktivnosti, koje opisivana aktivnost koristi. **O:** **Ime rezultantnog proizvoda rada.** **Primer**i: izjava o izvršenom radu, odobrena alokacija zahteva.
4. Izlaz aktivnosti
P: Šta su rezultati ili proizvodi rada proizvedeni sa ovom aktivnosti? Izlaz je veza ili link između date aktivnosti i njenog rezultata rada. Izlazi su rezultati proizvedeni sa opisivanom aktivnosti. **O:** **Ime rezultantnog proizvoda rada.** **Primeri***:* deo programskog koda, procedura testa, specifikacija projekta (dizajna), odobrena *Izjava o izvršenom ra*du.
5. Izvršioci aktivnosti
P: Ko izvršava ovu aktivnost? Ovo je veza ili link između date aktivnosti i izvršioca te aktivnosti. To je organizaciona jedinica, uloga zaposlenih ili automatizovani agent odgovoran za izvršavanje aktivnosti. **O:** **Spisak organizacionih jedinica, uloga ili automatizovanih agenata koji učestvuju ili se rad na njih odnosi.** **Primeri***:* odeljenje za *Sistem kvaliteta* (QA), menadžer projekta (PM), vodeći inženjer za razvoj softvera, rukovodilac zaštite itd.
6. Sledeća aktivnost
P: Koja je sledeća aktivnost? Tok aktivnosti je uslovna veza ili link između dve aktivnosti. Tok aktivnosti definiše redosled izvršavanja aktivnosti i generalno zavisi od izlaznih kriterijuma. **O:** **Proizvedeni rezultat.** **Prim**eri: finalni proizvod rada aktivnost ili međuproizvod koji vodi u sledeću aktivnost.

Procesi se mogu opisati prema uzorcima u skraćenoj (tabela 3.2) i dugoj verziji (tabela 3.3), a procedure se mogu opisati prema uzorku u tabeli 3.4.

Tabela 3.2 *Uzorak kratke verzije opisa procesa*

Proces: *Upravljanje bezbednosnim zahtevima*	
Akcija	*Odgovornost*
Dobijanje radnog zahteva od kupca	SM, PM
Revizija radnog zahteva	PM
Izrada inicijalnog plana budžeta, potrebnog rada i vremena	PM
Inicijalno planiranje	PM, PT
Zahtevi na konceptualnom nivou	PM, PT, kupac
Identifikovanje faktora rizika i dokumentovanje	PM
Nacrt specifikacije zahteva	PM, PT
Tehnička revizija	PM, PT, QA
Revizija kupca	Kupac
Rafiniranje zahteva	PM, PT, kupac
Izrada matrice za praćenje zahteva (RTM)	PM, PT
Revizija zahteva i RTM	PM, kupac, PT, QA
Revizija/ažuriranje faktora rizika	PM
Ažuriranje procena i vremenskog plana	PM
Revizija zahteva, vremenskog plana i procena	PM, PT, QA, kupac
Konačna specifikacija zahteva	PM, analitičari
Odobravanje i potpisivanje	Kupac, QA, PM, SM, EPG
Osnovna specifikacija zahteva	PM, CCB, EPG
Procena, praćenje i unošenje promena	PM, CCB, QA, EPG, kupac, PT

LEGENDA:

Configuration Control Board (CCB) – telo za kontrolu konfiguracije i upravljanje dokumentacijom

Engineering Process Group (EPG) – SE tim za implementaciju

Senior Manager (SM) — stariji menadžer

Project Manager (PM) — menadžer projekta

Quality Assurance (QA) — predstavnik sistema kvaliteta

Poject Team (PT) — projektni tim

Tabela 3.3 Uzorak *duge verzije opisa procesa*

Naziv procesa: Upravljanje zahtevima
Sadržaj
1.0 Uvod 1.1 Namena 1.2 Obim 1.3 Upravljanje promenama 1.4 Uloge i odgovornosti 2.0 Opis procesa 2.1 Pregled procesa 2.2 Tok procesa 2.3 Detalji procesa 2.3.1 Razvoj specifikacije zahteva 2.3.1.1 Opis 2.3.1.2 Ulazni kriterijumi/ulazi 2.3.1.3 Zadaci/aktivnosti 2.3.1.4 Revizije 2.3.1.5 Izlazni kriterijumi/izlazi 2.3.2 Razvoj RTM (matrice praćenja zahteva) 2.3.2.1 Opis 2.3.2.2 Ulazni kriterijumi/ulazi 2.3.2.3 Zadaci 2.3.2.4 Izlazni kriterijumi/izlazi 2.3.3 Izmene zahteva 2.3.4 Verifikacija 2.3.4.1 Stepen angažovanja glavnog menadžmenta 2.3.4.2 Stepen angažovanja projekt menadžera (PM) 2.3.4.3 Stepen angažovanja predstavnika sistema kvaliteta (QA) 2.3.4.4 Revizija proizvoda 2.3.4.5 Revizija menadžmenta 2.3.4.6 Revizija kupaca 3.0 Resursi i finansiranje 4.0 Merenja 5.0 Obuka 6.0 Referentna dokumenta

Tabela 3.4 *Uzorak za opis procedure*

R. br. Dokumenta:	Datum:
R. broj revizije:	
Opis: (*ime procedure*)	
Ova procedura uključuje…… Primarni cilj aktivnosti je da….	
Ulazni kriterijumi/ulazi:	Izlazni kriterijumi/izlazi:
Uloge: Ime uloge: Šta ona/on rade?	
Imovina: Standardi, referentni materijal, izlazni proizvodi rada, prethodni opisi procesa…	
Kratak sadržaj zadataka (Lista glavnih zadataka/koraci procesa): Zadatak 1 Zadatak 2 Zadatak 3 Zadatak 4	
KORACI PROCEDURE	
Zadatak 1: Detalji koraka 1 (aktivnost 1) Detalji koraka 2 (aktivnost 2) Detalji koraka 3 (aktivnost 3) Detalji koraka 4 (aktivnost 4)	
Zadatak 2: Detalji koraka 1 Detalji koraka 2 Detalji koraka 3 Detalji koraka 4	
Nastavak… (koliko ima zadataka)	

Osnovni koraci *procesa* formalnog poboljšanja procesa su**:**

1. *evaluacija* stanja zrelosti procesa prema referentnom *modelu procesa;*
2. *prikupljanje objektivnih* dokaza o implementaciji praksi (aktivnosti) procesa;
3. *verifikacija* i konsolidovanje objektivnih dokaza;
4. *definisanje glavnih nalaza i profila zrelosti* procesa i
5. *definisanje akcionih planova* za poboljšavanje procesa.

Svi formalni metodi poboljšavanja procesa zahtevaju određeni metod za evaluaciju procesa sa ciljem poboljšavanja na bazi referentnog *modela procesa*.

3.2.2.1 Evaluacija procesa zaštite

Ključni alat za postizanje željenih rezultata u formalnom pristupu poboljšavanju procesa je metodologija *evaluacije* (*appraisal*[1]), koju primenjuje osposobljen *tim za evaluaciju* (TE) na bazi nekog referentnog modela procesa najbolje prakse (npr. SSE CMM, CMMI…) [10, 18, 33]. Cilj svake evaluacije, na bazi bilo kojeg modela poboljšanja procesa, jeste da se identifikuju jake i slabe tačke u organizaciji i, ako se zahteva — izvrši rangiranje evaluiranih procesa. TE procenjuje i revidira tekuću praksu u organizaciji i procenjuje koliko dobro su ove prakse usklađene sa zahtevima modela *najbolje prakse,* tipično kritičnih procesa, a kojeg TE koristi u procesu evaluacije kao referentni model. Na taj način, organizacija koja primenjuje prakse i procese u skladu sa zahtevima modela, formira solidnu osnovu za poboljšavanje procesa. Ako organizacija odluči da sama razvija stabilne procese, bez korišćenja modela procesa, treba očekivati puno neproduktivnog rada i troškova resursa organizacije.

Procesno orijentisani modeli i metodi *evaluacije* rezultat su evolucije načina razmišljanja i naučnog mišljenja o poslu, poslovnom sistemu, menadžmentu i navikama zaposlenih. Procesi su centralni gradivni blokovi oko kojih su strukturirani tipični poslovi cele *industrijske ere*, u kojoj su *finansije* strategijski resurs, *upravljanje* usmereno na ostvarivanje novih vrednosti i *nagrađivanje* izvršilaca, a *struktura zaposlenih* — na rad i izvođenje projekata. U nastupajućoj *informacionoj eri znanja*, poslovi su struktuirani oko *sistema,* gde su SE (SSE) znanja, objektno orijentisani i procesni pristup od presudnog značaja, menadžment se integriše sa sistemima, a *znanje* postaje neopipljivi strateški resurs i deli se u zajednici zaposlenih i šire [6].

Evaluacija je prvi korak u fazi identifikovanja tekućeg stanja i poboljšanja procesa. Pojam *evaluacije* (eng. *evaluation*) označava sistematsko prosuđivanje i određivanje primarnih (bitnih) i/ili sekundarnih vrednosti nekog evaluiranog entiteta – *evaluanda* (cilja, misije, strategije, projekta, programa, procesa, organizacije i sl.). Evaluaciju treba pojmovno razlikovati od *merenja*, koje je u suštini deskriptivni, a ne evolutivni proces. Bliski termini su *ocenjivanje, vrednovanje i verifikacija*. *Ocenjivanje* se može definisati kao poređenje opservirane vrednosti sa standardnom, a ocena kao količnik opservirane i standardne vrednosti. *Vrednovanje* ili *validacija* je potvrđivanje da proizvod/servis zaštite ispunjava svoju korisničku namenu i ima očekivani *kvalitet*. *Verifikacija* je potvrđivanje da proizvod/servis zaštite odražava specifikovane zahteve politika, standarda i/ili korisnika. Evaluaciju izvode osposobljeni *evaluatori*. *Proces evaluacije* se sastoji od određenog broja faza i koraka i uvek je svrsishodan – ima za cilj stvaranje kognitivnih pretpostavki za efikasno i efektivno odlučivanje i delovanje; uključuje odgovornosti *evaluatora* i *evaluanda* [6]. Za evaluaciju procesa zaštite razvijeno je više standarda, modela i okvira, od kojih svaki ima određene prednosti i nedostatke.

3.2.2.2 Standardi za poboljšavanje proizvoda i procesa zaštite informacija

Generički *cilj procesa evaluacije je da pokaže da sistem ispunjava specifične bezbednosne zahteve pod specifičnim uslovima*. Sistem koji to ispunjava naziva se *poverljiv*, a *poverenje*

1 SEI institut: *Appraisal* - evaluacija nezavisnog tima sertifikovanih evaluatora na bazi referentnog CMM.

se zasniva na specifičnim *indikatorima objektivnih dokaza nivoa bezbednosti* (EAL), koji garantuju da je sistem bezbedan [*53*].

Za evaluaciju se primenjuje formalna metodologija koja obuhvata tehnike merenja poverenja na bazi *specifičnih bezbednosnih zahteva* i *objektivnih dokaza* koji garantuju određeni nivo bezbednosti. *Opšta metodologija za evaluaciju* proizvoda i sistema zaštite na bazi CC standarda obezbeđuje [16]:

- skup zahteva koji definišu funkcionalnost sistema zaštite,
- skup zahteva za garantovanu bezbednost, koji opisuje korake za uspostavljanje odluke da sistem ispunjava svoje funkcionalne zahteve,
- metod za određivanje stepena ispunjavanja funkcionalnih zahteva sistema na bazi analize objektivnih dokaza garantovane bezbednosti i
- metriku čiji rezultati indiciraju koliko se može verovati sistemu u odnosu na bezbednosne funkcionalne zahteve sistema (EAL).

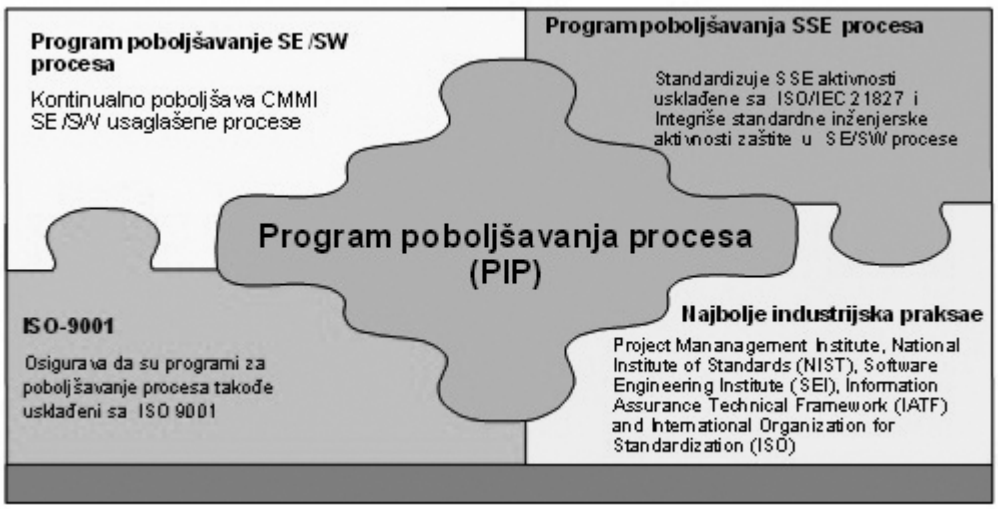
Evaluacija podrazumeva nezavisnu i objektivnu procenu i merenja garantovane bezbednosti koju obavljaju nezavisni eksperti – *evaluatori*. Proces evaluacije sistema zaštite može uključivati procenu: *konzistentnosti, kompletnosti, tehničke pouzdanosti i nivoa zaštite od pretnji, administracije sistema zaštite, korisnika, instalacija, dokumentacije zaštite, konfiguracije i korišćenja sistema* [54].

Za potrebe formalnog, struktuiranog poboljšavanja (sazrevanja) procesa, vremenom su razvijeni brojni modeli i okviri procesa. Korišćenje nekog *modela procesa* za poboljšavanje procesa rentabilno je iz više razloga. Pored toga što organizacija može usaglasiti svoje procese sa iskustveno dokazanom najboljom praksom, tipično kritičnih procesa za većinu organizacija sa različitim poslovnim profilima, neki modeli sadrže integrisane procese iz više oblasti primene (disciplina), tzv. *oblasti procesa* koje se mogu prilagođavati ili, ako ih model ne obuhvata, proširiti sa specifičnim ciljevima i praksama procesa organizacije za specifičan kontekst i okruženje (npr. SSE CMM i CMMI modeli integrisanih procesa) [30].

Generalno, za evaluaciju i poboljšavanje multidisciplinarnih procesa, kakvi su i procesi zaštite, potrebno je uspostaviti više okvira. Poboljšani procesi povećavaju uniformnost proizvoda, smanjuju ponavljanje rada i grešaka, nepotrebno trošenje radne snage, alata i materijala, dakle, povećavaju kvalitet izlaznih proizvoda rada sa manjim troškovima resursa. Ostale dobiti od poboljšanja kvaliteta procesa su niža cena proizvoda, zadovoljniji korisnici i kupci i više rada i zaposlenih, što je značajno zbog konkurentnosti organizacije na tržištu. Tradicionalne metrike performansi procesa, za merenje finansijskih performansi operativne efikasnosti i drugih parametara procesa, nisu adekvatne za prikazivanje progresa u promeni ponašanja, efektivnosti rada i poboljšanju procesa.

Razvijeni metodi i procesi evaluacije ugrađeni su u nekoliko okvira za poboljšavanje procesa, pri čemu se metod evaluacije oslanja na referentni model procesa, npr. SSE CMM model koristi SSAM (*System Security Appraisal Method)* metod evaluacije, a CMMI model — SCAMPI (*Standard CMMI Appraisal Method for Process Improvement*) metod evaluacije itd. U jednoj organizaciji modeli za poboljšavanje procesa mogu se preklapati na nivou organizacije, što znači da može biti više okvira za evaluaciju iste prakse, ako se koriste različiti metodi evaluacije i referentni modeli procesa. Za rešenje ovog problema, organizacije razvijaju arhitekturu procesa, koja opisuje akviziciju, interfejse, međuzavisnosti i druge odnose

između elemenata internih i eksternih procesa. Zbog ograničenja i usmerenosti okvira za poboljšavanje procesa, u organizacijama su često razvijani i održavani paralelni procesi i korišćeni različiti standardi za *program poboljšanja procese* – PIP (*Process Improvement Program*) kao dopunu industrijskih standarda kvaliteta proizvoda i procesa (slika 3.1) [74, 70].



Slika 3.1 Programi za poboljšanje procesa

Razvojem integrisanih modela sazrevanja (poboljšavanja) procesa tipa SSE CMM i CMMI, koji kombinuju nekoliko okvira procesa za specifične discipline (inženjerske, sistemske, za razvoj softvera, nabavku, davanje usluga, zaštitu), otvara se mogućnost integracije procesa u organizaciji i smanjuje broj potrebnih okvira za evaluaciju. Međutim, iako ovi modeli obezbeđuju širok obim procesa, ni jedan od njih nije sasvim dovoljan za sve potrebe i nije potpuno eliminisao potrebu za merenjem usaglašenosti sa drugim standardima i modelima za evaluaciju i poboljšavanje procesa [18, 30, 69, 74].

Model sazrevanja procesa zaštite — SSE CMM obezbeđuje uputstvo za najbolju praksu zaštite, poboljšavanje tekućih procesa do optimalnih procesa najbolje prakse zaštite i opštu integrisanu viziju za poboljšavanje procesa u celoj organizaciji. Cilj poboljšavanja procesa zaštite, svakako, nije poboljšavanje procesa radi samih sebe, nego – poboljšavanje ukupnih kapaciteta IKT sistema organizacije za ostvarivanje poslovnih ciljeva i misije organizacije. Kvalitet *modela procesa* raste sa povećanjem broja oblasti primene i disciplina [74].

Generalno, razvoj *integrisanih procesa,* usaglašenih za primenu u više disciplina, veoma je kompleksan poduhvat — organizaciono, upravljački i tehnički. Međutim, poboljšavanje procesa koje obezbeđuju integrisani modeli (SSE CMM i CMMI tipa), samo po sebi ne implicira postojanje integrisanih procesa u organizaciji. Za prelazak organizacije na višestruko usaglašene i integrisane procese potrebno je generisati strategiju razvoja i poboljšanja integrisanih procesa, deriviranu iz strateških ciljeva poslovanja organizacije. Ključni koraci u procesu razvoja ove strategije su [18, 30]:

1. *kvantifikacija poslovnih ciljeva*, za određivanje *obima* uključivanja organizacije u razvoj integrisanih procesa;
2. *definisanje usaglašene, integrisane strategije organizacije,* određivanjem vremenskog plana za usaglašavanje i okvira za evaluaciju i poboljšanje procesa;
3. *analiza rentabiliteta strategije za* rafiniranje strategije;
4. *identifikovanje i analiza rizika* implementacije strategije;
5. *razvoj plana kolaboracije relevantnih učesnika*;
6. *procena ukupnog rizika* za svaki metod evaluacije multidisciplinarnih i integrisanih procese. Pored uobičajenih faktora rizika poboljšavanja procesa, sledeći faktori rizika, generalno, imaju visoku verovatnoću uticaja:
   a. *održavanje učešća i podrške menadžmenta* u toku celog procesa,
   b. *održavanje zahtevanog nivoa kolaborativne saradnje TE i poboljšanje procesa*.
   c. *održavanje finansiranja tokom projekta*,
   d. *isticanje značaja podrške izvršnih menadžera* poboljšavanju i integraciji procesa, kroz postavljenje rada kao poslovnih ciljeva,
   e. *kreiranje neophodne korisničke prihvatljivosti* u organizaciji,
   f. *obezbeđivanje potpune komunikacije i razumevanja* u organizaciji i
   g. *obezbeđivanje potrebnih znanja iz više metoda za evaluaciju i poboljšavanje procesa,* radi boljeg razumevanja integrisanog okvira.

Ovi najčešći faktori rizika po intenzitetu, verovatnoći pojave i uticaju na integrisane procese, tipični za tranziciju organizacije sa multidisciplinarnih na integrisani okvir za evaluaciju i poboljšanje procesa, zavise od veličine, geografske distribucije i poslovnih modela organizacije. Ublažavanje faktora rizika vrši se prema planu za tretman rizika [69, 58]. U svakom pristupu poboljšanju procesa od posebnog značaja je kvalitetna, *potpuna* (uspešno završena, kompletirana) dvosmerna komunikacija svih učesnika u procesu. Svaka *potpuna* komunikacija ima određene osnovne parametre [103].

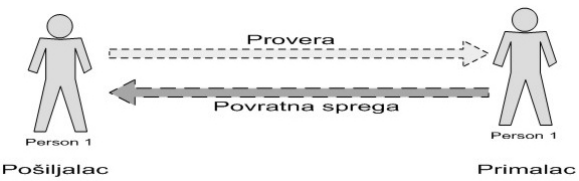
3.3 OSNOVNI PARAMETRI POTPUNE KOMUNIKACIJE

Za efektivnost procesa od primarnog značaja je *potpuna* komunikacija. Potpuna komunikacija uključuje zatvorenu petlju koja sadrži sledeće ključne komponente: *pošiljaoca, poruku, prenosni medij, primaoca i povratnu vezu* (slika 3.2)**.** Ako bilo koja od ovih komponenti nije efektivna, komunikacija nije potpuna i prenose se samo fragmenti podataka.



Slika 3.2 Zatvorena petlja komunikacije

Pre, za vreme i ponekad umesto prenosa formalne poruke, pošiljalac i primalac uspostavljaju interaktivnu *proveru* za razmenu glavnih poruka (slika 3.3).



Slika 3.3 Interakcija za razmenu poruka

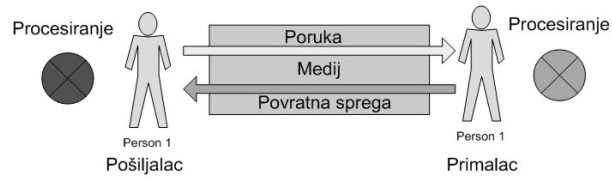
Provera može uključivati kontakt pogledima, neki ritual, kao što je rukovanje, tehničku aktivnost, kao što je *mašinsko pregovaranje* (tipa *Kerberos* autentifikacionog protokola, modema, faks mašina, telefonske konekcije itd.). Iako se u društvenom kontekstu ova interakcija smatra prenosom poruka, ona to nije, nego je priprema za stvarni prenos poruka, a osigurava da prenos počne i pomaže učesnicima da održavaju i po potrebi prilagođavaju tu interakciju za uspešnu razmenu poruka.

Poruka se može preneti kroz neki medij kao što je govor, e-pošta, video komunikacija ili memorandum. Medij se može izabrati na bazi nekog kriterijuma kao što su zahtevi za efikasnost, kreiranje kontrolnih tragova, minimizaciju distorzija itd., ali i na bazi neopipljivih razloga, kao što je percepcija o kritičnosti, tačnosti i relevantnosti poruka, koju izbor medija može stvoriti. Izbor medija se vrši kada pošiljalac uspostavi nameru za komunikaciju, uzimajući u obzir elemente poruka i potrebu za ublažavanjem rizika od distorzije poruka u prenosnom mediju.

Kada se jednom kanal komunikacije uspostavi, pošiljalac bira jezik i način *kodiranja* inicijalne poruke, ako je moguće na bazi razumevanja kapaciteta primaoca. Ovaj izbor jezika može biti intuitivan i neformalan ili striktno kontrolisan, zavisno od kritičnosti poruke. Inicijalna poruka se šalje primaocu, bilo istovremeno ili posle pažljivog uređivanja. Kodiranje u realnom vremenu može pozitivno uticati na percepciju značaja i ozbiljnosti poruke, jer se pretpostavlja da pošiljalac ne može sebi dopustiti da kodira ili šifruje beznačajne ili pogreške informacije.

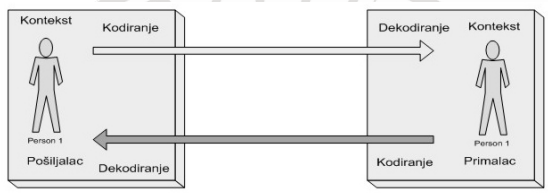
Za netrivijalne transakcije (npr. finansijske), pošiljalac ne može pretpostavljati da je poslata poruka došla do željenog odredišta. Zato poruke često uključuju zahteve za potvrdu o prijemu ili druge odgovore primaocu (npr. slanje verifikovanog digitalnog potpisa kao potvrde o prijemu). Aktivnost primaoca uključuje *dekodiranje* (interpretaciju) poruke i neku formu procesiranja. Često, čak i visoko obučeni i motivisani ljudi mogu imati percepcijsku ili kognitivnu prepreku koja ometa procesiranje određenog tipa poruka. Pošiljalac takođe, može koristiti multi-modnu komunikaciju da poboljša pouzdanost korektnog prijema i procesiranja.

Posle procesiranja, primalac dekodira i prenosi odgovor pošiljaocu. Kada originalni primalac dekodira i procesira odgovor, komunikaciona petlja je kompletirana (slika 3.4). Komunikacije u realnom svetu su veoma dinamične, tako da se ova petlja brzo može ponavljati više puta. U nekim slučajevima, povratna petlja može kasniti, kao u slučaju radio– emisije koja ispunjava želje slušaoca.



Slika 3.4 Kompletirana komunikaciona petlja

Aktivnosti komunikacione petlje događaju se u *kontekstu*, koji često nije isti za primaoca i pošiljaoca (slika 3.5). Na primer, mnogi nesporazumi potiču u toku interakcije pojedinca sa različitih nivoa odgovornosti, a drugi između ljudi različitih specijalnosti. Ove grupe imaju različite kontekste (kompetencije i referentne okvire) koji mogu izazvati stvarne komunikacijske probleme.



Slika 3.5 Konteksti komunikacione petlje

Čak i u istom domenu može biti radnih grupa sa različitim specijalnostima, o čemu postoje brojni primeri iz realnih projekata. Drugi faktor koji potencira uticaj konteksta u poslovnom svetu je sve češće iznajmljivanje usluga za deo ili ceo projekat. Tipičan primer uticaja konteksta na komunikaciju su problemi koji nastaju u interakciji strana iz različitih kultura rada, različitih procesa, jezika, nacionalnosti i religija.

Takođe, savremeni termin „*menadžment znanja*" stvara pogrešnu koncepciju da znanje može biti lako uskladišteno i prenošeno. Često mislimo da prenosimo znanje, a, u stvari, prenosimo podatke, zato što se pravo znanje ili značenje nalazi u glavama ljudi, a ne u rečima ili slikama koje koristimo u komunikaciji. Dakle, oni koji iniciraju komunikaciju moraju razumeti kompletnu komunikacionu petlju i odgovore na sledeća ključna pitanja:

- Kako znati da je primalac primio i propisno interpretirao poruku i zaključio onako kako to mi očekujemo?
- Čak i kada korisnik naizgled radi ono što očekujemo, da li znamo da ta akcija nije slučajna ili veštačka?

Za kompletiranje komunikacije značajni su i neki drugi faktori. Svaka komunikacija zahteva adekvatan *propusni opseg* koji diktira kolika se količina informacija može preneti i primiti. Kada pošiljalac generiše suviše mnogo poruka za procesiranje, primalac može, na bazi internih kriterijuma, izabrati one na koje može odgovoriti. Pošiljalac ili medij mogu uticati na ograničenje propusnog opsega, u kom slučaju se poruke gube, degradiraju ili kasne.

U različitim tipovima komunikacija na kvalitet prenosa poruka, pored propusnog op-

sega, mogu uticati i drugi faktori, kao što su problemi u procesu pregovaranja modema, kašljanje kod glasovnih poruka i sl. Za uspešnu komunikaciju poruke i povratna sprega moraju stizati nepromenjeni. Zato se moraju minimizirati distorzije u mediju i učesnicima. Kod elektronskih poruka proverava se *integritet podataka*. U govornoj komunikaciji možemo pitati da li nas sagovornik čuje ili tražiti da se poruka ponovi. Rizik od distorzije poruka raste kada se poruke prenose posredno, preko drugih ljudi ili elektronskih repetitora. Glasine su popularni primer verbalne distorzije poruka, a deseta generacija fotokopije je primer elektronske distorzije.

Efikasnost transmisije i *sinhronizacija* takođe mogu generisati indirektan oblik distorzije. Ljudi su u velikoj meri sposobni da simultano procesiraju više izvora poruka, sa većom ili manjom efikasnosti. Loša sinhronizacija stvara neku vrstu preopterećenja informacija, što primorava primaoca da se često reorijentiše, a na taj način smanjuje sposobnost procesiranja dolazećih podataka.

Međutim, koliko god podaci bili efikasno prenošeni, nekonzistentne poruke uvek stvaraju ozbiljne distorzije i probleme kod kodiranja i procesiranja. Na primer, neki ljudi generišu daleko više poruka nego što su svesni, a nekada je sadržaj tih poruka konfliktan. *Kodiranje, dekodiranje, kontekst, mešovite poruke, informaciono preopterećenje i razne distorzije*, generalno, mogu generisati šum u komunikacionoj petlji, koji prirodno želimo smanjiti u svim oblicima komunikacija.

3.3.1 Značaj potpune komunikacije za poboljšavanje procesa zaštite

Kvalitetna komunikacija među učesnicima svakog projekta i procesa, bez sumnje je od presudnog značaja za uspešan ishod. Elemenat *komunikacije* potenciraju gotovo svi modeli sazrevanja procesa. Komunikacija je posebno značajna za procese zaštite iz nekoliko bitnih razloga [103]:

- slabije su definisani od procesa IKT sistema, pa je dobra komunikacija neophodna za identifikovanje, razumevanje i definisanje tih procesa,
- kompleksnost IKT sistema dodatno povećava još kompleksniji sistem zaštite, a kvalitetna komunikacija povećava razumevanje i smanjuje kompleksnost, i
- dobra komunikacija pomaže bolje razumevanje visoko stručne terminologije zaštite, čime se dodatno smanjuje kompleksnost sistema.

Od svih modela zrelosti SSE CMM i CMMI modeli specifično i najpotpunije obuhvataju značaj elementa komunikacije za razvoj i poboljšavanje procesa [20]. Ovi modeli se, generalno, mogu koristiti kao vodič za dokumentovanje i razvoj politike, procedura i procesa, ali je pravi fokus modela na *procese* i *poboljšanje procesa,* što uključuje znanja i veštine ljudi, metode koje slede i alate koje koriste za izvršavanje svojih aktivnosti. Za poboljšanje procesa zaštite važnije je imati fokusiranu i razumljivu dokumentaciju, koja detaljno prati način izvršavanja praksi i procesa zaštite, nego sveobuhvatnu dokumentaciju koju niko ne razume, ne čita i ne sprovodi, niti je može povezati sa realnim aktivnostima. Zbog toga dokumentacija zaštite, sama za sebe, ne poboljšava prakse i procese, nego je sredstvo za uspostavljanje *komunikacije* između nameravanih i stvarno implementiranih praksi i procesa zaštite. Na taj način elemenat *komunikacije* neposredno utiče na poboljšavanje praksi i procesa zaštite.

Razumevanje komponenti potpune komunikacije i njihov odnos sa komponentama CMM modela, može imati veliki uticaj na uspešnost poboljšavanja procesa.

Ljudi koriste brojne forme komuniciranja za različite situacije. Za poslovne komunikacije ta forma može zavisiti od infrastrukture, skupa veština, logističke podrške ili prirode komuniciranih poruka. Same poruke mogu uključivati poslovne ciljeve, politiku, izgradnju tima za ublažavanje rizika, planove itd. Sve forme komunikacija moraju podržavati ove kompleksne kontekste i odgovarati svakodnevnom radnom okruženju. Generalno, komunikacije mogu imati različite *forme*: govor, govor tela, izraze lica, mimiku, zvučne signale, formalna dokumenta, e-poštu, pisma, *web* stranice itd. Međutim, bez obzira na formu, svaka potpuna komunikacija ima određene osnovne komponente.

3.4. REZIME

Poboljšanje procesa je klasični cilj menadžmenta kvaliteta procesa. Za poboljšanje procesa postoje brojni *neformalni* (nestruktuirani) i *formalni* (struktuirani) pristupi i metodi. *Neformalni metodi* za poboljšanje procesa mogu biti različiti, zavisno od kulture rada organizacije, stručnosti zaposlenih i tipa procesa; uglavnom su nestruktuirani i fokusirani na povećanje stabilnosti procesa — otklanjanje glavnih uzroka smanjenja *produktivnosti*, *adaptivnosti* i *korisničke prihvatljivosti* procesa. Produktivnost procesa je očekivani izlazni rezultat primenjenog procesa, adaptivnost — sposobnost da se proces prilagođava promenama okruženja, a korisnička prihvatljivost podrazumeva da dizajn procesa zadovoljava zahteve krajnjih korisnika.

Glavni faktori produktivnosti procesa su *efektivnost, efikasnost i ponovljivost, a* uzroci smanjenja se mogu svrstati u sledeće grupe razloga: *neodgovarajući bezbednosni ciljevi kontrola i nerealni ciljevi servisa zaštite, neefikasni kontrolni mehanizmi i slabo projektovan tok procesa zaštite.* Smanjenjem ovih faktora povećava se produktivnost procesa. Adaptivnost (*fleksibilnost* i *skalabilnost*) je sposobnost procesa da se prilagođava promenama okruženja. Uzroci nedovoljne adaptivnosti procesa zaštite mogu biti dizajn, slabo korišćenje *kompenzacionih* kontrola i predviđanje novih zahteva u projektu procesa itd. *Poboljšanje fleksibilnosti i skalabilnosti procesa* zaštite je ključno pitanje u visoko distribuiranom okruženju. Na korisničko prihvatanje procedura jako utiču kulturološka iskustva, nivo razumevanja i psihološki faktori. *Kulturološki uticaj* je najznačajniji za prihvatanje promena svake vrste, zbog prirodnog otpora korisnika. Dobra tehnika je da zaposleni sami vode proces promena. *Smanjenje kompleksnosti* je važno za poboljšanje procesa u fazi projektovanja, *načinu komunikacije* postavljenih ciljeva i u izvođenju samog projekta. *Uticaj psiholoških faktora* je mera u kojoj se ljudi vežu za dobijene zadatke, a najznačajniji faktori su sposobnost pojedinca i motivacija.

Formalni pristup za poboljšanje procesa, na bazi modela procesa, zahteva potpuno razumevanje i dokumentovanje tekućih procesa, njihovo dekomponovanje i određivanje prioriteta procedura za poboljšanje. Koncept *formalnog poboljšanja* procesa zahteva da proces bude *definisan* tj. *formalno opisan*. Ključni alat za postizanje željenih rezultata u formalnom pristupu poboljšavanju procesa je metodologija *evaluacije.* Najpoznatiji standard za evaluaciju proizvoda zaštite je ISO/IEC 15408, a procesa zaštite — ISO/IEC 21827 (SSE CMM).

Generalno, za evaluaciju i poboljšavanje multidisciplinarnih procesa, potrebno je uspostaviti više okvira za evaluaciju i poboljšanje. Razvojem integrisanih modela sazrevanja procesa (SSE CMM, CMMI i iCMMI itd.) otvara se mogućnost integracije procesa u organizaciji i smanjuje broj potrebnih okvira za evaluaciju. Za efektivnost procesa zaštite od primarnog značaja je *potpuna* ili *kompletna* komunikacija, koja uključuje zatvorenu petlju *pošiljaoca, poruke, prenosnog medija, primaoca i povratne veze.*

3.5. PITANJA ZA PONAVLJANJE

1. Zrelost procesa je:
   a. određena kvalitetom procesa koji se koristi za razvoj i održavanje proizvoda
   b. određena formalnim definisanjem procesa
   c. mera u kojoj je proces eksplicitno definisan, upravljan, merljiv i efektivan
   d. opseg očekivanih rezultata kada se proces konzistentno izvršava i daje očekivani izlaz.
   e. mera u kojoj je proces eksplicitno definisan, upravljan, merljiv i efektivan
2. Kvalitet proizvoda je:
   a. određena kvalitetom procesa koji se koristi za razvoj i održavanje proizvoda
   b. određena formalnim definisanjem procesa
   c. mera u kojoj je proces eksplicitno definisan, upravljan, merljiv i efektivan
   d. opseg očekivanih rezultata kada se proces konzistentno izvršava i daje očekivani izlaz.
3. Kapacitet procesa je:
   a. određen kvalitetom procesa koji se koristi za razvoj i održavanje proizvoda
   b. određen formalnim definisanjem procesa
   c. opseg očekivanih rezultata kada se proces konzistentno izvršava i daje očekivani izlaz.
4. Poboljšanje produktivnosti procesa zahteva poboljšanje:
   a. efektivnosti, efikasnosti i ponovljivosti
   b. efektivnosti, efikasnosti i fleksibilnosti
   c. adaptivnosti, fleksibilnosti i skalabilnosti
   d. kulturološkog i psihološkog uticaja i smanjenje kompleksnosti procesa.
5. Poboljšavanje adaptivnosti procesa zahteva poboljšanje:
   a. efektivnosti, efikasnosti i ponovljivosti
   b. efektivnosti, efikasnosti i fleksibilnosti
   c. fleksibilnosti i skalabilnosti
   d. kulturološkog i psihološkog uticaja i smanjenje kompleksnosti procesa.
6. Poboljšavanje korisničke prihvatljivosti procesa zahteva poboljšanje:
   a. efektivnosti, efikasnosti i ponovljivosti
   b. efektivnosti, efikasnosti i fleksibilnosti
   c. adaptivnosti, fleksibilnosti i skalabilnosti
   d. kulturološkog i psihološkog uticaja i smanjenje kompleksnosti procesa.
7. Formalni pristup za poboljšanje procesa je:
   a. nestruktuiran i zasnovan na bazi modela procesa
   b. struktuiran i zasnovan na bazi modela procesa
   c. zahteva definisanje i dokumentovanje tekućih procesa
   d. ne zahteva dekomponovanje procesa i određivanje prioriteta za poboljšanje
   e. zahteva planiranje i implementaciju inkrementalnih poboljšanja.
8. Procesi se mogu poboljšavati samo ako su:
   a. dekomponovani u procedure i aktivnosti
   b. poboljšavani u celini
   c. formalno opisani, definisani i dokumentovani
   d. neformalno opisani i dokumentovani.

9. Osnovni koraci *procesa* formalnog poboljšanja procesa su:
   a. evaluacija stanja i prikupljanje objektivnih dokaza o implementaciji procesa
   b. evaluacija dokumentacije i prikupljanje dokumentovanih dokaza o implementaciji
   c. verifikacija i konsolidovanje objektivnih dokaza
   d. verifikacija i konsolidovanje izjava i intervjua
   e. definisanje glavnih nalaza organizacije i akcionih planova za poboljšanje procesa.
10. Evaluacija procesa je:
   a. prvi korak identifikovanja stanja, procenom na bazi strogo utvrđenih kriterijuma
   b. sistematsko prosuđivanje i određivanje bitnih i/ili nebitnih vrednosti entiteta
   c. deskriptivan proces koji u osnovi nije evolutivan
   d. količnik opservirane i standardne vrednosti.
11. Procenjivanje je:
   a. prvi korak identifikovanja stanja, procenom na bazi strogo utvrđenih kriterijuma
   b. sistematsko prosuđivanje i određivanje bitnih i/ili nebitnih vrednosti nekog entiteta
   c. deskriptivan proces koji u osnovi nije evolutivan
   d. količnik opservirane i standardne vrednosti.
12. Ocena je:
   a. prvi korak identifikovanja stanja, procenom na bazi strogo utvrđenih kriterijuma
   b. sistematsko prosuđivanje i određivanje bitnih i/ili nebitnih vrednosti nekog entiteta
   c. deskriptivan proces koji u osnovi nije evolutivan
   d. količnik opservirane i standardne vrednosti.
13. Za prelazak na integrisane procese potrebno je generisati strategiju sa sledećim koracima:
   a. kvantifikacija poslovnih ciljeva, definisanje usaglašene i integrisane strategije
   b. kvantifikacija bezbednosnih ciljeva
   c. analiza rentabiliteta, identifikovanje i analiza rizika strategije
   d. kvalifikacija poslovnih ciljeva,
   e. razvoj plana saradnje učesnika i procena ukupnog rizika integrisanih procesa.
14. Proces evaluacije može uključivati procenu:
   a. konzistentnosti, kompletnosti, tehničke pouzdanosti i nivoa zaštite od pretnji
   b. hakerskih napada, malicioznih programa i ranjivosti sistema
   c. administracije sistema zaštite, konfiguracije i korišćenja sistema
   d. korisnika, instalacija, dokumentacije zaštite.
15. Potpuna komunikacija je posebno značajna za procese zaštite zbog:
   a. slabijeg identifikovanja, razumevanja i definisanja procesa IKT i sistema zaštite
   b. boljeg razumevanje visoko stručne terminologije zaštite
   c. kompleksnosti normativa, standarda, politike i procedura sistema zaštite
   d. boljeg identifikovanja, razumevanja i definisanja procesa zaštite
   e. slabijeg razvoja i razumevanja procesa i terminologije zaštite.
16. Dokumentacija zaštite:
   a. sama za sebe, ne poboljšava prakse i procese
   b. sama za sebe, poboljšava prakse i procese zaštite
   c. uspostavlja *komunikaciju* između planiranih i implementiranih praksi i procesa
   d. neposredno utiče na poboljšanje praksi i procesa zaštite.



4. EVOLUCIJA STANDARDA KVALITETA ZAŠTITE INFORMACIJA

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Potrebu razvoja standarda kvaliteta proizvoda i procesa zaštite informacija
- ☑ Opšte riterijume (CC) za evaluaciju kvaliteta proizvoda zaštite informacija
- ☑ Osnovne funkcionalnosti, prednosti i nedostatke izvornih standarda zaštite
- ☑ Značaj razvoja standarda menadžment sistema zaštite informacija (ISMS)
- ☑ Prednosti i nedostatke generičkih modela sazrevanja procesa (CMM) Komplementarnost i kompatibilnost relevantnih standarda i modela zaštite

4.1 UVOD

Nekoliko međunarodnih standardizacionih tela pokazalo je tokom više godina interes za oblast zaštite informacija, kao što su Britanski institut za standarde – BSI [12], Nemačka agencija za zaštitu informacija – BSI (*Germany*) [14], Međunarodna organizacija za standardizaciju – ISO [56], Međunarodna komisija za elektrotehniku – IEC i Nacionalni institut za standarde i tehnologiju – NIST [77]. U ovoj oblasti ISO/IEC su objavili najviše standarda, od kojih je najznačajnija serija ISO/IEC 27000, veoma slična seriji standarda ISO 9000. Standarde zaštite informacija donosi *Međunarodni tehnički komitet za standardizaciju ISO/IEC JTC1/SC27* [61].

Generalno, razvijene su brojne metodologije za menadžment sistem kvaliteta proizvoda i procesa, koje mogu doprineti proizvodnji bezbednih (bez *bagova*) programskih kôdova i pouzdanih hardverskih rešenja za zaštitu informacija [67, 70].

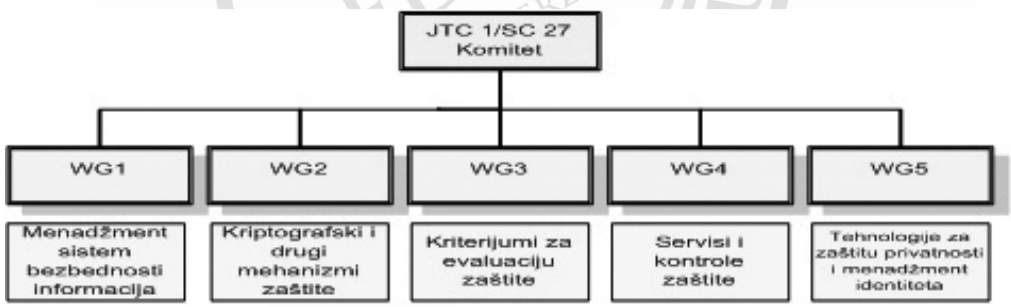
4.2. MEĐUNARODNA TELA ZA STANDARDIZACIJU ZAŠTITE INFORMACIJE

Standardi postoje za komponente i sisteme zaštite, organizacije i profesionalce u zaštiti, a donose ih međunarodna, akreditovana tela (tabela 4.1).

Tabela 4.1 *Relevantna međunarodna tela za standardizaciju u oblasti zaštite*

Međunarodna standardizaciona tela u oblasti zaštite informacija	
BSI	*British Standards Institute*
BSI (German)	*Bundesamt fuer Sicherheit in der Informationstechnik*
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
NIST (USA)	*National Institute for Standards and Technology*

U oblasti bezbednosti informacija najviše standarda je objavila ISO organizacija. Za menadžment sistem bezbednosti informacija, najznačajnija je serija ISO/IEC 27000 standarda, koja liči na seriju industrijskih standarda ISO 9000 za kontrolu kvaliteta. Standarde zaštite informacija donosi *Međunarodni tehnički komitet za standardizaciju ISO/IEC JTC1/SC27***,** formiran 1990. godine (slika 4.1) [30,61].



Slika 4.1 Organizaciona šema Tehničkog komiteta ISO/IEC JTC 1SC 27

Obim poslova Komiteta *JTC1/SC27* su standardi za zaštitu informacija, uključujući generičke metode, tehnike i uputstva, koji obuhvataju sve aspekte zaštite informacija i privatnosti, kao što su: *metodologija menadžmenta bezbednosnih zahteva; ISMS, kriptografski i drugi mehanizmi zaštite, dokumentacija i terminologija zaštite, bezbednosni aspekti menadžmenta identiteta i zaštite privatnosti, metodologija i kriterijumi za evaluaciju zaštite* itd. Komitet ima radne grupe za ISMS – **WG1**, kriptografske algoritme i druge mehanizme zaštite – **WG2**, kriterijume za procenu/evaluaciju zaštite – **WG3**, servise i kontrole zaštite – **WG4** i tehnologije za zaštitu privatnosti i upravljanje identitetom – **WG5** [61].

4.3 STANDARDI I MODELI KVALITETA PROIZVODA I PROCESA ZAŠTITE

4.3.1 Generički standardi procesa i proizvoda zaštite

U standardu ISO/IEC 15443 navedeni su svi metodi i sredstva za menadžment kvaliteta na bazi *evaluacije* [54]:

- *proizvoda zaštite* (ISO 15408, ITSEC/ITSEM, TCSEC/TPEP, ISO 9646, ISO 14598),
- *okruženja* (personala i organizacije) sistema zaštite (TCMM, ISO 13407),
- *procesa zaštite* (ISO 21827, ISO 9000-3. deo, *ISO 9001:2008, ISO 15504, CMMI v. 1.3)*.

Za evaluaciju kriptografskih modula razvijen je standard FIPS-140-2 [79].

Međutim, od brojnih standarda kvaliteta, relativno mali broj se odnosi na bezbednost informacija. Na primer, ISO 9001:2008 standard kvaliteta industrijskih proizvoda i procesa sadrži neke elemente garancije kvaliteta procesa za proizvodnju operativnog i softvera za zaštitu [54]. Od početka 1980-ih, međunarodna zajednica za zaštitu računara razvijala je kriterijume i metodologije za evaluaciju sistema kvaliteta proizvoda zaštite informacija. Prvu javnu i široko korišćenu tehniku obezbedili su *Kriterijumi za evaluaciju poverljivog računarskog sistema* – TCSEC (*Trusted Computer System Evaluation Criteria*) [80]. Primenjivani gotovo dve decenije, TCSEC kriterijumi su pokazali brojne slabosti, kao što su: *ograničeni obim, problemi sa evaluacijom, povezivanje bezbednosti i funkcionalnosti, ne priznavanje evaluacije* i dr.

Iako su zahtevi za evaluaciju bezbednosnih karakteristika IKT proizvoda široko prihvaćeni, brojni eksperti zaštite nalaze da je proces za evaluaciju i sertifikaciju IKT proizvoda vremenski zahtevan i vrlo skup. Rezultat toga je da proizvodi IKT i sistema zaštite dolaze na tržište *kroz dugu i skupu evaluaciju* ili *bez evaluacije.* U prvom slučaju bezbedni proizvodi dolaze na tržište sa velikim zakašnjenjem, a u drugom – kupci se oslanjaju samo na tvrdnje proizvođača o kvalitetu proizvoda. Važno je uočiti da evaluacija *bezbednosti* proizvoda zahteva isključivo ispitivanje proizvoda i njihove dokumentacije, a ne obraća pažnju na *procese* za njihovo projektovanje i proizvodnju.

Standard *TCSEC* je pokušao da definiše neke procese koji omogućavaju uspostavljanje visoke *garantovane bezbednosti* IKT sistema, ali isti zahtevaju testiranje sistema na proboj, korišćenje formalnih matematičkih metoda i upravljanje konfiguracijom. Zato su proizvođači u razvoju poverljivih (bezbednih) proizvoda i računarskih sistema, povećali primenu specifičnih procedura ovog standarda. Međutim, sve prednosti od primene ovih procedura nisu se mogle postići u *nedisciplinovanom i nekonzistentnom radnom okruženju*. Procesno orijentisani modeli, tipa PDCA i SSE CMM, nude novi pristup obezbeđivanju *garantovane bezbednosti* proizvoda i sistema zaštite, na bazi neprekidnog poboljšanja procesa i poverenja u SSE grupu procesa zaštite [9].

Kasnije su razvijene nove metodologije za rešavanje uočenih problema, od kojih su najznačajnije međunarodni *Kriterijumi za evaluaciju zaštite IKT sistema* – ITSEC (*Information Technology Security Evaluation Criteria*) [16,63] u Evropi, *Kanadski kriterijumi za evaluaciju proizvoda poverljivih računarskih sistema* – CTCPEC (*Canadian Trusted Computer Product*

Evaluation Criteria), Federalni standardi za procesiranje informacija – FIPS (*Federal Information Processing Standards*) i *NIST* (*National Information Standard and Technology*) u SAD [79, 75]. Ove fundamentalne metodologije dovele su do razvoja standarda ISO/IEC 15408, tzv. *Opštih kriterijuma za evaluaciju proizvoda i sistema zaštite* – CC (*Common Criteria*), široko prihvaćenog, ali, vremenom, potpuno zapostavljenog zbog izuzetno kompleksne i skupe primene od strane malog broja akreditovanih entiteta za sertifikaciju [63].

Standardi TCSEC, ITSEC, ITSEM i CC za evaluaciju procesa i proizvoda zaštite, danas nemaju širu praktičnu primenu.

4.3.2 Standard za evaluaciju kriptografskih algoritama i modula

Za evaluaciju kriptografskih algoritama i modula koji implementiraju kriptografske algoritme ili procese, razvijen je (u NSA i NIST, SAD i Agenciji za zaštitu informacija Kanade) i najviše se praktično koristi, NIST standard FIPS 140-2 (1994 – danas) [79]. Namenjen je za evaluaciju kriptomodula, softvera, izvršnih procesora i operativnih sistema koji uključuju kriptomodule. Standard uključuje četiri rastuća *indikatora nivoa bezbednosti* – **L1** do **L4,** a obuhvata sledeće komponente: *osnovni projekat, dokumentaciju, uloge, menadžment kriptografskog ključa, testiranje, fizičku zaštitu od EM interferencija, ublažavanje rizika, tehničku specifikaciju, portove i interfejse, model konačnog broja stanja i druge elemente*. Ključni kriterijumi zahteva za bezbednosne nivoe (L1-L4) kriptomodula prikazani su u tabeli 4.2:

Tabela 4.2 *Kriterijumi indikatora kriptografskih nivoa bezbednosti (L)*

L	Opis kriterijuma
L1	Zahteva FIPS sertifikovani kriptološki algoritam; izvršavanje softverskih i memorijskih komponenti na IKT sistemu za opšte namene sa neevaluiranim OS; fizičku zaštitu istu kao za objekte IKT sistema u standardnoj upotrebi.
L2	Zahteva veću fizičku zaštitu od regularne, kućište otporno na TEMPEST (*Transient Electro-Magnetic Pulse Surveillance Technology*) prisluškivanje ili rad u restriktivnom prostoru [66]; autentifikaciju operatora za specifične servise na bazi uloga; izvršavanje softverskih i memorijskih komponenti i na višenamenskom sistemu, ali sa evaluiranim OS za najmanje EAL2 nivo, uz primenu jednog od CC specifikovanih profila zaštite.
L3	Zahteva veću fizičku zaštitu koja sprečava pristup kritičnim bezbednosnim parametrima unutar modula; autentifikaciju na bazi identiteta operatera; rigorozno čitanje i izmenu kritičnih bezbednosnih parametara; softverske i memorijske komponente OS, evaluirane za EAL3 nivo, a može se koristiti i ekvivalentni, evaluirani poverljivi OS; poverljiv prenosni put i neformalan model politike zaštite.
L4	Zahteva „zaštitnu zonu" oko modula, uključujući zaštitu od uticaja okruženja ili fluktuacije napona i temperature izvan dozvoljenog opsega modula; softverske i memorijske komponente OS, evaluirane za bezbednosni nivo L3 i EAL4, a može se koristiti i ekvivalentni, evaluirani poverljivi OS.

4.3.3 Komparativna analiza izvornih standarda zaštite

Industrijski standardi za sistem kvaliteta ISO-9000/9001, namenjeni za proizvodne organizacije, uz više interpretacija mogu se primeniti za razvoj i proizvodnju softvera [38]. Dok se ISO 9000 sertifikat daje samo organizacijama, modeli sazrevanja procesa mogu se primeniti za individualne grupe ili projekte unutar organizacije. ISO 9001 pokriva veći obim proizvoda nego CC standard, što znači da organizacija koja želi ISO 9001:2008 sertifikat, mora implementirati sistem kvaliteta koji pokriva više oblasti.

Komparativna analiza funkcionalnih i bezbednosnih zahteva izvornih standarda TCSEC, ITSEC, CC i FIPS 140-2, specifično namenjenih za sistem kvaliteta proizvoda i sistema zaštite, indicira da ovi standardi u praksi zaštite imaju neke zajedničke karakteristike [27]: *prilično su nefleksibilni, imaju za cilj procenu nivoa bezbednosti, teški su i zahtevni za korišćenje u kompleksnim sistemima, zahtevaju specifikaciju okruženja u kojem se koriste, zahtevaju poverljive administratore, korisni su samo za sertifikaciju proizvoda zaštite i imaju slične indikatore nivoa bezbednosti*.

U tabeli 4.3 prikazani su *indikatori nivoa bezbednosti za evaluaciju* u ovim standardima [30].

Tabela 4.3 *Indikatori nivoa bezbednosti standarda TCSEC, ITSEC, CC i FIPS -140-2*

TCSEC (1983 – 1990)	**ITSEC (1991 – 2001)**	**CC (1998 – danas)**	**FIPS 140 (1994 – danas)**
D	E0	nema ekvivalent	
nema ekvivalent	nema ekvivalent	EAL1	privatne lab. za testiranje
C1	E1	EAL2	OS za FIPS 140-2 L2
C2	E2	EAL3	OS za FIPS 140-2 L3
B1	E3	EAL4	OS za FIPS 140-2 L4
B2	E4	EAL5	
B3	E5	EAL6	
A1	E6	EAL7	

4.4. RAZVOJ STANDARDA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

4.4.1 Razvoj standarda *najbolje prakse* zaštite informacija

Standardi u zaštiti informacija i IKT sistema su brojni, ali mnogi nisu šire prihvaćeni. Među prvima šire prihvaćenim standardima menadžment sistema zaštite informacija, svakako su ISO/IEC 13335-1 [52] i ISO/IEC 17799:2000 koji je usvojen u EU, Australiji i Novom

Zelandu [3, 38]. U većini razvijenih zemalja u svetu usvojeni su nacionalni ekvivalenti ovog standarda, izuzev SAD. Smatra se analognim ISO 9000 standardu u oblasti bezbednosti informacija, ali je lakši za primenu. Standard ISO/IEC 17799:2000 sadrži dva dela [38]:

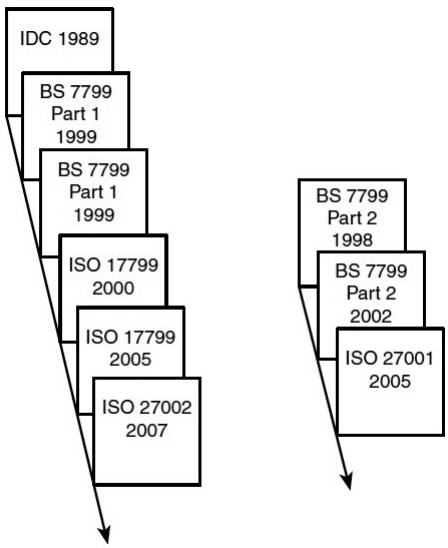
1. standard najbolje prakse zaštite – zahtevi za implementaciju ISMS-a i
2. BS 7799 – specifikaciju zahteva za izbor *kontrola zaštite [12]*.

U suštini, standard ISO/IEC 17799:2000, predstavlja zahteve i smernice za implementaciju menadžment sistema zaštite informacije (ISMS-a) i izbor *kontrola zaštite* sa instrukcijama šta treba raditi u praksi zaštite, ali ne daje odgovore **kako** to treba uraditi. Zahtevi za ISMS obuhvataju *obim, politiku zaštite, analizu rizika, izjavu o primenljivosti, menadžment sistem razvoja i održavanja zaštite* i *dokumentaciju zaštite.* Razvijen je iz britanskog standarda BS 7799 (1995, revidiranog 1998), kao ISO/IEC 17999:2000. Prvi deo BS 7799 i ISO/IEC 17999:2000 praktično su identični, a preuzeti drugi deo BS 7799 (1999) je standard za implementaciju *upravljačkih, operativnih i tehničkih kontrola zaštite*. Standard nije tehnički, ne zavisi od specifične tehnologije i ne obezbeđuje nikakvu metriku za evaluaciju zaštite, ali je kompatibilan i poziva se na EAL sistem CC standarda, a može se kombinovati sa metrikom SSE-CMM modela sazrevanja procesa zaštite [35, 101]. Standard sugeriše koje kontrole zaštite treba uključiti u program zaštite, ali ne i **kako** ih treba razviti, implementirati i administrirati. Zahteva izbor kontrola zaštite na bazi *procene rizika, normativnih okvira i specifičnih principa, ciljeva i zahteva zaštite* konkretne organizacije, ali ne obezbeđuje metodologiju za procenu rizika, kao ni uputstvo za kreiranje i čuvanje podataka za pravosudne i forenzičke potrebe. Standard posvećuje veliku pažnju definisanju politike zaštite na nivou organizacije sa instrukcijom šta dokument treba da sadrži, ali ne nudi detalje **kako** se ta politika razvija. Revizijom kontrola zaštite (2005), standard je preimenovan u ISO/IEC 17799:2005 (ISO/IEC 27001). Osnovne karakteristike standarda ISO/IEC 17799:2000 date su u tabeli 4.4 [38].

Tabela 4.4 *Osnovne karakteristike standarda ISO/IEC 17799:2000*

Struktura	10 glavnih sekcija, 36 bezbednosnih ciljeva, 127 glavnih kontrola zaštite, nekoliko hiljada uputstava i instrukcija
Sekcije zahteva (4-8)	politika zaštite, organizacija zaštite, klasifikacija i kontrola objekata (IKT sistema) zaštite, personalna zaštita, fizička zaštita i zaštita okruženja, operativno upravljanje, kontrola pristupa, razvoj i održavanje sistema zaštite, upravljanje kontinuitetom poslovanja, usaglašenost.
Bezbednosni ciljevi	politika zaštite, organizacija zaštite, klasifikacija i kontrola objekata IKT sistema, personalna zaštita, fizička zaštita i zaštita okruženja, operativni menadžment, kontrola pristupa, razvoj sistema i održavanje, menadžment kontinuiteta poslovanja, usaglašenost.

Kratka istorija evolucije ISO/IEC standarda zaštite informacija prikazana je na slici 4.2.



Slika 4.2 Razvoj ISO/IEC standarda zaštite informacija

4.4.2 Razvoj modela sazrevanja procesa

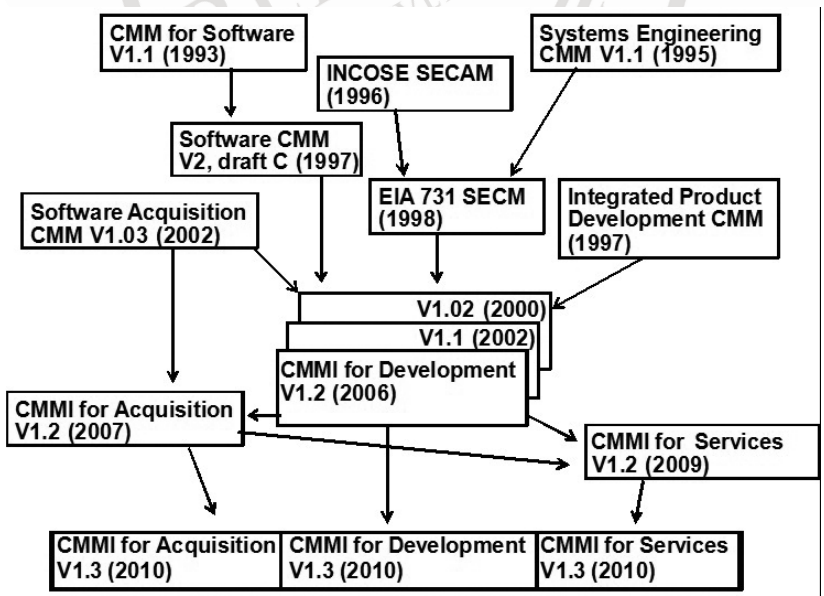
Merenje je opšte prihvaćen princip za *upravljanje neke aktivnosti* u procesu zaštite. *Merenje* daje jednokratni uvid u specifične merne parametre sistema zaštite, poređenjem u odnosu na predefinisani merni etalon, a rezultati zavise od razumevanja zahteva. Osnovu kvaliteta aktivnosti i procesa čine merenja i *metrike*.

Metrike zaštite različito definišu razni autori i standardi [8]. Prihvatljiva je definicija da je *metrika analiza rezultata merenja, namenjena za procenu trenda i odlučivanje na višem nivou menadžmenta, ili sredstvo za objektivnu ili subjektivnu interpretaciju agregiranih mernih podataka višekratnog merenja u dužem vremenskom periodu*. Metrika zaštite je od posebnog značaja za procese *digitalne forenzičke istrage* kompjuterskog incidenta i kriminala, jer obezbeđuje *ponovljivost* testiranja i merenja digitalnih dokaza po zahtevu pravosudnih organa, što zahteva standardni kriterijum za priznavanje posrednog digitalnog dokaza pred sudom. Metrika zaštite IKT sistema zahteva dalji istraživački rad. Istraživanja su potvrdila da je merenje performansi u zaštiti IKT sistema važno, ali da se prednosti merenja mogu ostvariti samo kada se metrika primenjuje kao *proces*, uz korišćenje agregiranih mernih podataka. Međutim, većina organizacija ne koristi metrike zaštite informacija kao proces, a još manji broj integriše taj proces u TQM menadžment sistem. *Metrički sistem* je skup kriterijuma, parametara, mernih uređaja, analize agregiranih podataka i jedinica za generisanje i prikazivanje rezultata merenja, koji podrazumeva procese *evaluacije* i/ili *monitoringa* performansi servisa zaštite. Dakle, rezultati *merenja* su objektivni i sirovi podaci koji mogu automatski da se generišu, dok su *metrike* interpretacije tih podataka [85].

Menadžment sistem zaštite informacija je oblast koja nema dobro definisane metrike i još uvek ne postoji konsenzus oko ključnih indikatora, što uglavnom potiče od prikrivanja

bezbednosnih incidenata. Organizacije koje su imale hakerski napad, nerado to objavljuju, a one koje nisu – ćute, jer ne žele da izazovu napadače. Procesi zaštite informacija uključuju niz analiza koje zahtevaju donošenje odluka, a kvalitetne odluke se donose kada postoji metrika. Bezbednosno svesne i odgovorne organizacije mere aktivnosti zaštite i dokumentuju efektivnost metrika zaštite. U praksi zaštite informacija najčešće se primenjuju sledeće metrike: *snage kriptografskog algoritma; kvalitativne* (npr. *nizak, srednji, visok* uticaj); *kvantitativne* (npr. *cost-benefit analiza*); *softverskog inženjerstva* (*SwE*), *detekcije anomalija* (IDPS/NIDPS); *srednjeg vremena napada; intervjua; poslovnih procesa; provere sistema zaštite* i *modela sazrevanja procesa zaštite (SSE CMM). Objekti merenja* u sistemu zaštite informacija mogu biti *organizacija*, *proizvod* (u planu, razvoju ili radu), *tehnički sistem* (hardver, softver, komunikaciona infrastruktura, komponente i sistem zaštite u celini) itd. [92,106].

Posebnu grupu modela i standarda zaštite informacija sa *inherentnom metrikom*, čine *procesno orijentisani modeli* sazrevanja kapaciteta procesa, razvijeni na bazi generičkog CMM modela, kao što su: SE CMM (*System Engineering Capability Maturity Model*), SW CMM (*Capability Maturity Model for Software Developement*), SSE CMM (*System Security Engineering Capability Maturity Model*), iCMM (*Integrated Capability Maturity Model*) i CMMI (*Capability Maturity Model Integration*). SSE CMM v.2, objavljena 2001., postaje ISO standard *ISO/IEC 21827 (EOS, 2001),* v.3 – izlazi juna 2003., a v.4 – 2010. [101]. Pored *otkrivanja objektivnih dokaza* stvarne implementacije praksi i procesa (kao raniji modeli), CMM modeli zasnivaju proces evaluacije na *otkrivanju* i *verifikaciji* objektivnih dokaza *konzistentne i disciplinovane* implementacije, izvršavanja i institucionalizacije praksi i procesa, što je znatno viši kvalitet. Kratak pregled istorije razvoja CMMI modela prikazan je na slici 4.3 [18].



Slika 4.3 Pregled istorije razvoja CMM modela procesa [55]

Generički CMM, razvijen na inicijativu NSA (1993 – 95) i više usmeren na upravljačke i organizacione procese i aktivnosti, referentni je model zrelih praksi i procesa u specifikovanim disciplinama, koji se koristi za procenu kapaciteta za izvršavanje te discipline. CMM modeli se razlikuju po *disciplini primene*, *strukturi komponenti i putu sazrevanja*, *definisanju nivoa zrelosti* i *kapaciteta procesa*. Model obezbeđuje referentni skup *najboljih praksi* za evaluaciju i poboljšanje procesa, primarno razvijenih da kreiraju metrički sistem *organizacijskih procesa* za životni ciklus sistema, identifikuje većinu *projektnih i upravljačkih* praksi i procesa i obuhvate najbolje *SE prakse* za razvoj i menadžment industrijskih procesa [55].

Poverljivi CMM – TCMM (*Trusted Capability Maturity Model)*), razvijen ranih 1990-ih kao *Metodologija poverljivog softvera* – **TSM** (*Trusted Software Methodology*) na bazi generičkog CMM, namenjen je za bezbednosnu procenu softvera u fazi razvoja. Tipičan je predstavnik standarda za *procenu kvaliteta u odnosu na pretnje iz proizvodnog okruženja*. TSM definiše nivoe poverenja u softverski proizvod sa: *nizak* – otpornost na nenamerne ranjivosti i *visok* – dodaje procese za zaštitu od malicioznih programa u razvoju softverskih proizvoda. TSM je kasnije harmonizovan sa CMM u TCMM, koji je orijentisan samo na razvojno okruženje i upravljačke i organizacione aktivnosti. TCMM nije više u upotrebi.

Na bazi generičkog CMM-a, razvijeni su brojni modeli sazrevanja procesa sa glavnim karakteristikama metrike i primene, prikazanim u tabeli 4.5 [18].

Tabela 4.5 *Objavljeni modeli sazrevanja procesa zaštite*

Model sazrevanja	Opis metrike progresivnog sazrevanja	Komentar
NIST CSEAT IT Security Maturity Model	1. politika 2. procedura 3. implementacija 4. testiranje 5. integracija	fokusiran prema nivoima dokumentacije
Citogrup's Information Security Evaluation Model (CITI-ISEM)	1. usklađenost 2. prepoznavanje 3. integracija 4. opšta praksa 5. kontinualno poboljšanje	fokusiran prema svesti organizacije o potrebi zaštite i usvajanju zaštite
CobiT Maturity Model	1. inicijalni/*ad hoc* 2. ponovljiv ali intuitivan 3. definisan 4. upravljan i meren 5. optimizovan	fokusiran na proveru (*auditing)* specifičnih procedura
P-CMM (Personal Capability Maturity Model)	1. inicijalni 2. ponovljiv 3. definisan 4. upravljan 5. optimizovan	fokusiran na sazrevanje kompetencija ljudskih resursa

Model sazrevanja	Opis metrike progresivnog sazrevanja	Komentar
SSE CMM model sazrevanja procesa zaštite	1. neformalno izvršavan 2. planiran i praćen 3. dobro definisan 4. kvantitativno kontrolisan 5. kontinualno poboljšavan	fokusiran prema SSE procesima i dizajnu softverskih proizvoda zaštite
CERT/CSO Security Capability Assesment	1. postojeći 2. ponovljiv 3. namenjen (određenom licu) 4. dokumentovan 5. revidiran i ažuriran Četiri nivoa: 1. inicijalni 2. razvojni 3. uspostavljen 4. upravljan	fokusiran prema merenju kvaliteta u odnosu na nivoe dokumentovanja
CMMI DEV v.1.3 za razvoj	Kapaciteta (CL) i zrelosti (CM) procesa: 1. nekompletan (kontinualna) 2. izvršavan (kontinualna) 3. inicijalan (fazna) 4. upravljan (kontinualna, fazna) 5. definisan (kontinualna, fazna) 6. kvantitativno kontrolisan (fazna) 7. optimalan (fazna)	fokusiran na procese razvoja IS i softverskih proizvoda; 22 oblasti procesa
CMMI SVC v.1.3. za pružanje usluga	Kapaciteta (CL) i zrelosti (CM) procesa: 1. nekompletan (kontinualna) 2. izvršavan (kontinualna) 3. inicijalan (fazna) 4. upravljan (kontinualna, fazna) 5. definisan (kontinualna, fazna) 6. kvantitativno kontrolisan (fazna) 7. optimalan (fazna)	fokusiran na procese davanja usluga; 24 oblasti procesa, od čega 11 specifičnih u odnosu na CMMI DEV v.1.3
CMMI AQV v.1.3 za nabavku	Kapaciteta (CL) i zrelosti (CM) procesa: 1. nekompletan (kontinualna) 2. izvršavan (kontinualna) 3. inicijalan (fazna) 4. upravljan (kontinualna, fazna) 5. definisan (kontinualna, fazna) 6. kvantitativno kontrolisan (fazna) 7. optimalan (fazna)	fokusiran na procese nabavke; 22 oblasti procesa od čega 6 specifičnih u odnosu na CMMI DEV v.1.3

4.4.3 Model sazrevanja procesa zaštite (SSE-CMM)

Model i metod sazrevanja procesa zaštite – SSE-CMM, razvijen isključivo za oblast zaštite (NSA i DoD, *SAD*), sadrži jedanaest specifičnih SSE oblasti procesa (OP) za zaštitu informacija. U nekim zonama poklapa se sa standardom ISO/IEC 15408. SSE CMM meri zrelost i kapacitete organizacije za izvršavanje procesa zaštite. Model pretpostavlja da samo disciplinovan i konzistentan metod sa zrelim procesima i kapacitetima, daje dobar proizvod i sistem zaštite, ali *ne sugeriše specifičnu metodologiju, kontrole ili uputstva za zaštitu*. Kao i svi CMM modeli, uvek teži najvišem nivou sazrevanja kapaciteta za izvršavanje procesa zaštite. Model nije toliko fleksibilan kao CC standard, ali ima dobru *sistemski* i *procesno orijentisanu* metriku. Kako proces sazreva postaje sve više ponovljiv, bolje kontrolisan, dokumentovan, merljiv, definisan i institucionalizovan.

Standard ISO/IEC 21827 (SSE-CMM) sadrži SSE CMM – model sazrevanja, *inženjerskih, upravljačkih* i *organizacionih* (OP) i SSAM – metod za evaluaciju zrelosti procesa na bazi SSE CMM modela. Generalno, može se primeniti za *merenje poboljšanja zrelosti*, *evaluaciju zrelosti kapaciteta* i *garantovanu bezbednost* procesa zaštite.

U tabeli 4.6 dat je zbirni pregled osnovnih karakteristika primenjivanih standarda kvaliteta proizvoda i procesa zaštite i opšte prihvaćenih ISMS standarda [35].

Tabela 4.6 *Pregled relevantnih parametara primenjivanih standarda zaštite*

Standard	Kratak opis relevantnih parametara
TCSEC (1985-1999)	Prva glavna metodologija za evaluaciju zaštite; skup kriterijuma za evaluaciju komercijalnih kompjuterskih proizvoda zaštite.
ITSEC (1991-2001)	Obuhvata rešenja za neke nedostatke TCSEC; fleksibilnost u definisanju bezbednosnih zahteva i evaluaciju svakog tipa proizvoda i sistema zaštite.
SSE CMM (1997-danas)	Definiše zahteve za OP, sazrevanje procesa zaštite i metodologiju za evaluaciju (SSAM) nivoa zrelosti kapaciteta procesa zaštite organizacije.
ISO/IEC 15408 (1996-2005)	Opšti model za evaluaciju bezbednosnih ciljeva, definisanje bezbednosnih zahteva i izradu specifičnih *profila zaštite* za proizvode i sisteme.
ISO 17799 (2000-2005)	Uspostavlja uputstvo i opšte zahteve za menadžment sistem zaštite informacija (ISMS) u organizaciji.
ISO 27001 (2005-danas)	Uspostavlja uputstvo i opšte zahteve za menadžment sistem zaštite informacija (ISMS) u organizaciji.

4.4.4. Ostali relevantni standardi i regulative zaštite informacija

4.4.4.1 ISO/IEC 13335-1 (IT Security Managament)

Ovaj ISO/IEC standard, razvijen iz tehničkog izveštaja, sastoji se od sledeće serije smernica za merenja tehničkih kontrola zaštite [52]:

- **ISO/IEC 13335-1:2004** dokumentuje koncepte i modele za menadžment tehnologija zaštite informacija i komunikacija;
- **ISO/IEC TR 13335-3:1998** dokumentuje tehnike za menadžment bezbednosti IT, posle revizije zamenjen sa ISO/IEC 27005;
- **ISO/IEC TR 13335-4:2000** pokriva izbor tehničkih kontrola zaštite, posle revizije zamenjen sa ISO/IEC 27005;
- **ISO/IEC TR 13335-5:2001** pokriva smernice za menadžment mrežne zaštite, posle revizije zamenjen sa ISO/IEC 18028-1 i ISO/IEC 27033.

4.4.4.2 Standard za zaštitu podataka industrije platnih kartica (PCI)

Industrija platnih kartica – PCI (*The Payment Card Industry*) je razvila *standard za zaštitu podataka* – DSS (*Data Security Standard*). U razvoju su učestvovale brojne PCI kompanije, uključujući *American Express, Discover Financial Services, JCB, Master Card Worldwide* i *Visa International*. Standard sadrži dvanaest ključnih zahteva, koji uključuju ISMS, politiku i procedure zaštite, mrežnu arhitekturu, projektovanje i izradu softvera i druge kritične mere. Ovi zahtevi su organizovani u sledeće oblasti:

1. izgradnja i održavanje bezbedne mreže,
2. zaštita podataka vlasnika kartice,
3. održavanje programa za menadžment ranjivosti,
4. implementacija jakih mera kontrole pristupa,
5. regularni monitoring testiranje mreža,
6. održavanje politike zaštite informacija .

4.4.4.3 COBIT

Standard *Ciljevi kontrola za informacije i odnosne tehnologije* – COBIT (*Control Objectives for Information and related Technology*) je *"kontrolni okvir koji povezuje IT inicijative sa poslovnim zahtevima, organizuje IT aktivnosti u generalno prihvaćen model procesa, identifikuje glavne IT resurse koje treba angažovati i definiše menadžment ciljeva kontrola koje treba upravljati"* [19]. Standard je objavio *IT Governance Institute* (ITGI), 1995, a poslednja verzija 4.1 je objavljena 2007. COBIT 4.1 sadrži sedam sekcija: *(1) kratak sadržaj, (2) COBIT okvir, (3) plan i organizacija, (4) akvizicija i implementacija, (5) isporuka i podrška, (6) monitoring i evaluacija i (7) prilozi, uključujući rečnik termina*. Standard sadrži 34 ključna IT procesa.

COBIT je šire prihvaćen kao set smernica za menadžment IT, koji sinhronizuje zahteve za kontrolu, tehnička pitanja i poslovni rizik. *COBIT Security Baseline,* baziran na COBIT 4.1, fokusiran je na specifične faktore rizika za bezbednost IT u malim i velikim organizacijama.

4.4.4.4 ISO/IEC 20000 serija standarda (ITIL)

Biblioteka infrastrukture informacione tehnologije – ITIL (*Information Technology Infrastructure Library*) je kolekcija najbolje prakse menadžmenta IT servisa – ITSM (*IT service management*), fokusirana na procese IT servisa, sa centralnom ulogom korisnika. Razvijen u Velikoj Britaniji (OGC – *United Kingdom's Office of Government Commerce*), standard je od 2005. uključen u ISO/IEC 20000 standard unutar ITSM.

Samoprocena menadžmenta ITIL servisa može se izvršiti pomoću upitnika koji se održava na web sajtu *IT Service Management Forum*-a. Ovaj upitnik pomaže kod evaluacije sledećih oblasti menadžmenta: *(a) menadžment nivoa servisa, (b) menadžment finansija, (c) menadžment kapaciteta, (d) menadžment kontinuiteta servisa, (e) menadžment dostupnosti, (f) desk servis, (g) menadžment incidenta, (h) menadžment problema, (i) menadžment konfiguracije, (j) menadžment promena i (k) menadžment isporuke servisa*.

4.4.4.5 Zakoni i regulative zaštite

Pored raznih industrijskih standarda objavljene su i razne regulative i smernice, od kojih su šire prihvaćene regulative u SAD – *SOX, COSO, HIPAA i FISMA* [111].

Sarbanes-Oxley Act – SOX (2002), poznat kao *Zakon o reformi računovodstva javnih preduzeća i zaštiti investitora*, namenjen je za "*zaštitu investitora poboljšanjem tačnosti i pouzdanosti otkrivanja informacija korporacija u saglasnosti sa bezbednosnim zakonima i za druge namene*". Ovaj zakon se odnosi na sve kompanije koje su na spisku berze u SAD. Zahtevi SOX indirektno sugerišu da menadžment razmatra kontrole zaštite informacija u organizaciji i da ih usaglašava sa SOX[1].

Okvir COSO (*Committee Of Sponsoring Organisations of the Treadway Commission*) inicira integralni proces i evaluaciju interne provere. Okviri COSO i COBIT se koriste tako da zadovolje usaglašenost sa SOX. Okvir sadrži pet komponenti: *kontrolu okruženja, procenu rizika, proveru, informacije i komunikacije i monitoring*

Zakon o računovodstvu i prenosivosti zdravstvenog osiguranja – **HIPAA** (*The Health Insurance Portability And Accountability Act)*, (SAD, 1996), namenjen je za poboljšanje prenosivosti i neprekidnosti zdravstvenog osiguranja, za zaštitu od gubitka, pronevere i zloupotrebe zdravstvenog osiguranja, zdravstvenu zaštitu itd. Zakon definiše standarde zaštite za zdravstvene informacije, uključujući tehničke kapacitete sistema za skladištenje i održavanje zdravstvenih informacija, troškove zaštite, obuku zaposlenih, vrednost kontrolnih tragova u zdravstvenom IKT sistemu za potrebe malih pružaoca zdravstvenih usluga i zahteva odgovarajuću administrativnu, tehničku i fizičku zaštitu integriteta i poverljivosti informacija. Potpun set pravila HIPAA standarda dostupan je na web sajtu [111].

1 Engl.: http://www.sans.org/reading_room/whitepapers/legal/1426.php.

Zakon o menadžmentu federalnog informacionog sistema SAD – FISMA (*Federal Information Security Management Act*), deo *US E-Government Act* (*Public Law* 107-347 objavljenog 2002. godine), zahteva od federalnih agencija SAD da razviju, dokumentuju i implementiraju programe zaštite informacija i IKT sistema, koji podržavaju operativne procese i imovinu agencija, uključujući: *periodičnu procenu rizika, dokumentovanje politike i procedura zaštite, planiranje zaštite, periodičnu evaluaciju i testiranje efektivnosti politike, procedura i kontrola zaštite, plan kontinuiteta poslovanja itd.*

Standardi za procesiranje federalnih informacija FIPS su serija publikacija NIST-a sa smernicama prilagođenim i dostupnim, po zakonu FISMA. *FIPS Publication 199*[2], „*Standards for Security Categorisation of Federal Information and Information Systems*", je prvi obavezni standard zaštite objavljen pod FISMA zakonom. *FIPS Publication 200*, *"Minimum Security Requirements for Federal Information and Information Systems"* je drugi obavezni set standarda zaštite za federalne informacije i IKT sisteme, SAD-a, koji sadrži sedamnaest oblasti zaštite: *(a) kontrolu pristupa; (b) svest o potrebi zaštite i obuku; (c) proveru i odgovornost; (d) sertifikaciju, akreditaciju i bezbednosnu procenu; (e) menadžment konfiguracije; (f) planiranje vanrednih događaja; (g) identifikaciju i autentifikaciju; (h) odgovor na incidente; (i) održavanje; (j) zaštitu medija; (k) fizičku i zaštitu okruženja; (l) planiranje; (m) personalnu zaštitu; (n) procenu rizika; (o) akviziciju sistema i servisa; (p) zaštitu sistema i komunikacija i (q) integritet sistema i informacija.* Federalne agencije moraju ispuniti minimum zahteva definisanih u ovom standardu, izborom kontrola zaštite iz NIST SP 800-53.

4.5 KOMPLEMENTARNOST I KOMPATIBILNOST STANDARDA ZAŠTITE

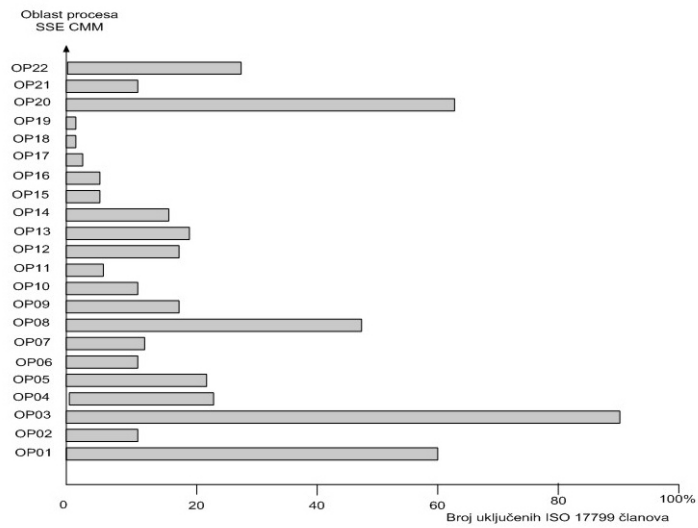
U praksi gotovo ni jedan standard ili model procesa zaštite, sam za sebe nije dovoljan za rešavanje većine problema u zaštiti informacija. Međutim, brojni modeli i standardi imaju oblasti koje se u određenoj meri dopunjavaju i preklapaju, zadržavajući individualne prednosti za specifične aspekte primene. Cilj je sagledati kompatibilnosti i komplementarnosti relevantnih standarda i modela zaštite, utvrditi prednosti i nedostatke za *konkretne uslove primene i okruženja* i omogućiti korisnicima izbor adekvatnih standarda i modela za rešavanje problema zaštite u realnom kontekstu i okruženju, umesto, po pravilu najskupljih rešenja *najboljih* praksi namenjenih za *tipične organizacije* i *okruženja*. Od posebnog značaja je izbor što bržih, jeftinijih, nedestruktivnih i dovoljno efektivnih metoda za merenje zrelosti, evaluaciju i poboljšanje procesa zaštite informacija. Primer kompatibilnosti standarda ISO/IEC 15504 i ISO/IEC 21827 (SSE CMM) dat je u tabeli 4.7.

2 Engl.: FIPS PUB 199, *Federal Information Processing Standards Publication — Standard for Federal Information and Information Systems*, www.nist.gov February 2004.

Tabela 4.7 *Kompatibilnost ISO/IEC 21827 i ISO/IEC 15504*

ISO/IEC 21827 – model sazrevanja procesa	**ISO/IEC 15504 – okvir za merenje procesa**
(*Nije eksplicitno definisan, implicitno se odnosi.*)	*Nivo 0: nekompletan proces*
Nivo kapaciteta 1: izvršen neformalno	Nivo 1: izvršen proces
CF 1.1. bazične prakse su izvršene	OP 1.1. atribut performansi procesa
Nivo kapaciteta 2: planiran i praćen	*Nivo 2: upravljan proces*
CF 2.1 planiranje performansi CF 2.4. praćenje performansi	OP 2.1: atribut upravljanja performansama
CF 2.2: disciplinovanje performansi CF 2.3: verifikovanje performansi	OP 2.2: atribut upravljanja proizvodom rada
Nivo kapaciteta 3: dobro definisan	*Nivo 3: uspostavljen proces*
CF 3.1: definisanje standardnog procesa CF 3.2: izvršavanje definisanog procesa	OP 3.1: atribut definicije procesa
Nije specifično obuhvaćen u ovoj tački, ali su ovi aspekti obuhvaćeni ranije u sledećim GP: GP 2.1.1: alociraj resurse GP 2.1.2: pripiši odgovornosti GP 2.1.5: obezbedi obuku	OP 3.2: atribut resursa procesa
CF 3.3: koordiniranje prakse zaštite	*Nema direktnog ekvivalenta*
Nivo kapaciteta 4: kvantitativno kontrolisan	*Nivo 4: predvidljiv proces*
CF 4.1: uspostavljanje merljivih ciljeva kvaliteta	OP 4.1: atribut merenja
CF 4.2: objektivno upravljanje performansama	OP 4.2: atribut kontrole procesa
Nivo kapaciteta 5: kontinualno poboljšavan	*Nivo 5: optimizovan proces*
CF 5.1: poboljšavanje kapaciteta organizacije CF 5.2: poboljšavanje efektivnosti procesa	OP 5.1: atribut poboljšavanje procesa OP 5.2: atribut promene procesa

Na *bar* dijagramu (slika 4.4) data je procena korelacija oblasti procesa (OP) SSE CMM modela i uključenih članova ISO/IEC 17799:2000 standarda [8, 38, 104].



Slika 4.4 Korelacija ISO/IEC 21827 i ISO/IEC 17799:2000 *standarda*

Rezultati jasno indiciraju da su prvih 11 SSE OP SSE-CMM modela najbolje pokrivene sa ISO/IEC 17799 standardom, dok su projektne i organizacione OP slabije pokrivene. Od SSE OP sa ISO/IEC 17799 najbolje su pokriveni: *administriranje kontrola zaštite, koordinacija sistema zaštite i nadzor i kontrola sistema zaštite*. OP – *obezbeđenje bezbednosnog ulaza,* predstavljena je prilično dobro, a OP *za procenu uticaja, rizika i ranjivosti* zastupljene su umereno u ISO/IEC 17799. Međutim, OP – *verifikacija i validacija zaštite,* slabo je zastupljena u ISO/IEC 17799, što indicira da proizvođači softvera koji primenjuju ISO/IEC 17799 standard, imaju povećan rizik. Kratak uporedni pregled SSE-CMM modela procesa zaštite i drugih standarda i modela za poboljšanje nivoa bezbednosti informacija, dat je u tabeli 4.8.

Tabela 4.8 *Uporedni pregled SSE CMM i drugih standarda i modela IKT zaštite*

Model	Cilj	Pristup	Obim	Status
SSE CMM	definiše, evaluira i poboljša SSE kapacitete	kontinualni/fazni SSE model sazrevanja i metod evaluacije	SSE organizacije	v.3.0
SE-CMM	poboljša SE proces sistema ili proizvoda	kontinualni CMM model sazrevanja SE praksi i metod evaluacije	SE organizacije	videti EIA 731

Model	Cilj	Pristup	Obim	Status
SW CMM	poboljša menadžment razvoja softvera	fazni CMM model praksi SwE i upravljanja	organizacije za SwE	u CMMI v.1.2
TCMM	poboljša proces razvoja visoko integrisanog KW i njegovog okruženja	fazni CMM model SwE i praksi upravljanja, uključujući i zaštitom	SE organizacije	nepoznat
CMMI	integriše postojeće procese za proizvodnju proizvoda/sistema, akviziciju i davanje servisa	kontinualna i fazna prezentacija, sa SCAMPI metodom evaluacije	SE organizacije	CMMI v.1.2
EIA 731	definiše, poboljša i proceni SE kapacitete	kontinualni CMM model i metod evaluacije	SE organizacije	objavljen
CC	povećava bezbednost korišćenjem profila zaštite (PP) za proizvode zaštite	skup funkcionalnih i bezbednosnih zahteva za zaštitu, sa procesom evaluacije (EAL nivoi)	IKT sistemi	V.2.0
Okvir za merenje procesa zaštite	poboljšava bezbednost sistema, obezbeđujući širok opseg argumenata	struktuiran pristup za kreiranje argumenta garantovane bezbednosti i efikasnu proizvodnju dokaza	SSE organizacije	u razvoju
ISO 9001	poboljšava upravljanje sistemom kvaliteta organizacije	specifični zahtevi za prakse upravljanja kvalitetom	servisne organizacije	u širokoj primeni
ISO/IEC 15504	poboljšava i procenjuje procese za razvoj KW i sve druge procese	Sw CMM model i metod evaluacije	SwE organizacije	svih devet delova objavljeno
ISO 13336	poboljšava procese upravljanja IKT zaštitom	uputstvo o procesima za dostizanje i održavanje odgovarajućih nivoa zaštite informacija i servisa	SSE organizacije	slabo se koristi, objavljeno pet delova.

Model sazrevanja procesa zaštite komplementaran je i sa ISO/IEC 13335 i NIST standardima (tabela 4.11) [9, 38, 52, 76].

Tabela 4.9 *Komplementarnost SSE CMM, ISO/IEC 17799, ISO/IEC 13335 i NIST*

SSE CMM	ISO/IEC 17799	**ISO/IEC 13335**	**NIST *Security HANDBOOK (NIST SP 800-12)***
OP 01	sekcija 5, 6, 8	član 17 — praćenje	poglavlje 10 — personalno/korisnička pitanja poglavlje 14 — bezbednosna analiza u operaciji podrške
OP 02	Uvod	član 10 — korporacijska analiza rizika	poglavlje 7 — upravljanje rizikom u sistemu zaštite IT
OP 03	Uvod	član 10 — korporacijska analiza rizika	poglavlje 7 — upravljanje rizikom u sistemu zaštite IT
OP 04	Uvod	član 10 — korporacijska analiza rizika	poglavlje 7 — upravljanje rizikom u sistemu zaštite IT poglavlje 4 — kombinovane pretnje
OP 05	Uvod	član 10 — korporacijska analiza rizika	poglavlje 7 — upravljanje rizikom u sistemu zaštite IT
OP 06	Sekcija 10	član 14 — implementacije sistema zaštite	poglavlje 9 — bezbednosna garancija
OP 07	Sekcija 2.6	član 13 — plan zaštite IT	poglavlje 6 — upravljanje programom zaštite
OP 08	Sekcija 10	član 17 — praćenje	poglavlje 18 — kontrolni tragovi poglavlje 12 — upravljanje kompjuterskim incidentom
OP 09	Sekcija 1, 3, 5	član 8 — korporacijska politika zaštite IT član 11 — preporuke zaštite IT član 12 — politika zaštite IT sistema član 13 — plan zaštite IT član 15 — svest o zaštiti	poglavlje 5 — politika zaštite računara poglavlje 13 — svest, obuka obrazovanje poglavlje 15 — fizička zaštita i zaštita od uticaja okoline
OP 10	Sekcija 1, 7, 8, 9	član 8 — korporacijska politika zaštite IT član 11 — preporuke zaštite IT član 12 — politika zaštite IT sistema član 13 — plan zaštite IT	poglavlje 8 — planiranje zaštite u ŽCSZ poglavlje 11 — upravljanje van. dog. poglavlje 16 — I & autentifikacija poglavlje 17 — logička AC poglavlje 19 — kriptografija
OP 11	Sekcija 10	član 17 — praćenje član 14 — implementacija sistema zaštite	poglavlje 8 — planiranje zaštite u ŽCSZ poglavlje 18 — kontrolni tragovi

4.6 REZIME

Od brojnih industrijskih standarda kvaliteta, relativno mali broj se odnosi na bezbednost IKT sistema i informacija. Prvu javnu i široko korišćenu tehniku obezbedio je TCSEC standard (1983 – 1999, SAD), koji je pokušao da definiše neke procese za uspostavljanje visoke garantovane bezbednosti IKT sistema. U Evropi su ranih 1990-ih razvijeni standardi ITSEC i ITSEM, koji su, razdvajanjem funkcionalnih i bezbednosnih zahteva, imali veću fleksibilnost od TCSEC standarda. Indikatori nivoa bezbednosti ITSEC evaluacije (E0-E6) rangirani su od nebezbednog (E0) do visoko zaštićenog (E6). Na bazi iskustava iz ova dva standarda razvijen je međunarodni standard ISO/IEC 15408 (poznat kao CC), za evaluaciju kvaliteta proizvoda zaštite. Iako dobar i detaljan, ovaj standard nije široko primenjivan u praksi, zbog skupe i vremenski zahtevne evaluacije i malog broja akreditovanih entiteta za sertifikaciju. Indikatori evaluacije nivoa bezbednosti – EAL definisani su u standardu za sedam nivoa evaluacije od početnog EAL1 do EAL 7. Za evaluaciju kriptografskih algoritama i modula razvijen je i najviše se praktično koristi NIST standard FIPS 140-2, sa ***četiri*** nivoa bezbednosti, od osnovne zaštite (L1) do rigorozne zaštite sa restriktivnim prostorom (L4).

Standard ISO/IEC 17799:2000, nastao spajanjem sa britanskim BS 7799 za specifikaciju zahteva za izbor *kontrola zaštite*, praktično je prvi široko prihvaćen međunarodni standard za menadžment sistem zaštite informacija (ISMS). Revizijom ovog standarda 2005. godine nastao je danas poznati standard ISO/IEC 27001 (ISMS), kao i čitava serija tzv. standarda ISO/IEC 27K, po ugledu na poznatu seriju ISO 9000.

Standard i model sazrevanja procesa zaštite (SSE-CMM) obezbeđuje rezultatski i procesno orijentisanu metriku zrelosti procesa zaštite i visoku komplementarnost sa ISMS, ISO/IEC 15504 i CMMI. Svi standardi i modeli zaštite informacija, orijentisani na proizvode ili procese zaštite, uključujući i modele sazrevanja procesa (CMM tipa), u velikoj meri su međusobno kompatibilni i komplementarni.

4.7 PITANJA ZA PONAVLJANJE

1. Standarde zaštite informacija donosi:
   a. ISO/IEC 27001
   b. Međunarodni tehnički komitet za standardizaciju ISO/IEC JTC1/SC27
   c. NIST
   d. BCI.
2. Standardi kvaliteta na bazi evaluacije proizvoda zaštite su:
   a. ISO/IEC 21827, *ISO 9001:2008, ISO/IEC 15504, CMMI v.1.3*
   b. ISO/IEC 15408, ISO/IEC 14598
   c. TCMM, ISO 13407.
3. Standardi kvaliteta na bazi evaluacije okruženja:
   a. ISO/IEC 15408, ISO/IEC 14598
   b. ISO/IEC 21827, *ISO 9001:2008, ISO/IEC 15504, CMMI v.1.3*
   c. TCMM, ISO 13407.
4. Standardi kvaliteta na bazi evaluacije *procesa zaštite:*
   a. ISO/IEC 15408, ISO/IEC 14598
   b. ISO/IEC 21827, *ISO 9001:2008, ISO/IEC 15504, CMMI v.1.3*
   c. TCMM, ISO 13407.
5. Standard opštih kriterijuma za evaluaciju proizvoda sistema zaštite je:
   a. ISO/IEC 27001
   b. ISO/IEC 21827
   c. ISO/IEC 27006
   d. ISO/IEC 15408.
6. Specifičnosti standarda opštih kriterijuma za evaluaciju proizvoda sistema zaštite su:
   a. zasnovan na ISO/IEC 9001 standardu
   b. definiše indikatore bezbednosti EAL1-EAL7
   c. definiše indikatore bezbednosti E0-E7
   d. danas se praktično ne koristi
   e. danas se široko koristi u celom svetu.
7. Najpoznatiji standard za evaluaciju kriptografskih algoritama i modula je:
   a. ISO/IEC 27006 koji sadrži četiri indikatora nivoa bezbednosti (L1-L4)
   b. ISO/IEC 15405 koji sadrži četiri indikatora nivoa bezbednosti (L1-L4)
   c. FIPS 140-2 koji sadrži četiri indikatora nivoa bezbednosti (L1-L4)
   d. NIST SP 800-53 koji sadrži četiri indikatora nivoa bezbednosti (L1-L4).
8. Među prvima šire prihvaćenim standardima menadžment sistema zaštite informacija je:
   a. BS 7799
   b. ISO/IEC 13355-2
   c. ISO/IEC 13335-1:2004
   d. ISO/IEC 17799:2000
   e. ISO/IEC 17799:2005.
9. Modeli sazrevanja (poboljšavanja) procesa zaštite zasnivaju se na generičkom modelu:
   a. SSE CMM
   b. CMM
   c. CMMI
   d. SSAM.
10. Jedinstven standard sazrevanja (poboljšavanja) procesa zaštite je:
    a. ISO/IEC 21827 (iCMM)
    b. ISO/IEC 21827 (CMMI)
    c. ISO/IEC 21827 (SSE-CMM)
    d. ISO/IEC 21827 (iCMM).
11. Ostali relevantni standardi zaštite podataka i informacija su:
    a. ISO/IEC 13785, DSS, COBIT, ITIL, zakoni i regulative *SOX, COSO, HIPAA i FISMA*
    b. ISO/IEC 13335, COBRA, , ITIL, zakoni i regulative
    c. ISO/IEC 13335, COBIT, ITIL, zakoni i regulative *SOX, COSO, HIPAA i FISMA*
    d. ISO/IEC 13335, DSA, COBIT, ITIL, *SOX, COSO, HIPAA i FISMA*.



5. EVOLUCIJA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Generičku metodologiju i principe menodžment sistemo zaštite informacija (ISMS)
- ☑ Generički proces i značaj uloga i odgovornosti u ISMS-u
- ☑ Upravljačke kontrole menadžment sistema zaštite informacija (ISO, NIST)
- ☑ PDCA model procesa za uspostavljanje; implementaciju; održavanje i poboljšanje ISMS-a
- ☑ Metrike za evaluaciju i poboljšanje ISMS-a
- ☑ Potrebu razvoja i komplementarnost ISO/IEC menadžment sistema

5.1 UVOD

Značaj menadžment sistema zaštite informacija raste sa porastom obima e-–poslovanja, a time i kritičnosti procesa zaštite i legalne odgovornosti menadžera za neadekvatnu zaštitu od malicioznih napada i zloupotreba. Proces menadžment sistema zaštite obuhvata sveukupnu infrastrukturu *proceduralnih* i *tehničkih kontrola zaštite,* u kojima je čovek faktor odlučivanja, što znači da se proces ne može ograničiti samo na kontrolu pristupa sistemu ili na menadžment tehnologije zaštite informacija. Menadžment sistem zaštite mora obuhvatiti organizacione i operativne aktivnosti, aktivnosti za oporavak sistema posle vanrednog događaja i incidenta, kao i metriku za potvrdu efektivnosti procesa upravljanja.

Skup procesa za uspostavljanje, implementaciju, održavanje i odlaganje sistema zaštite informacija naziva se *menadžment sistem zaštite informacija* – ISMS (*Information Security Management System*), prema ključnom standardu ISO/IEC 17799:2005 (ISO/IEC 27001 ili ISMS standard) i primenljiv je u organizacijama svake veličine i tipa. Osnovni mehanizam je *politika zaštite*. Klasa upravljačkih kontrola zaštite obuhvata sledeće relevantne familije *kontrola zaštite*: *procena rizika, planiranje zaštite, akvizicija sistema i servisa, evaluacija kontrola zaštite, sertifikaciju i akreditaciju sistema zaštite*, koje u kontekstu menadžment sistema zaštite informacija obavezno treba razmatrati i prilagođavati okruženju. Skup aktivnosti za održavanje i oporavak sistema posle pada, naziva se *menadžment kontinuiteta poslovanja* – BCM (*Business Continuity Management*) [40, 44, 94], koji se uobičajeno tretira jedinstveno sa planiranjem vanrednih događaja i oporavka sistema – DRP (*Disaster Recovery Planing*) [5]. U procesima ISMS-a, BCM-a i DRP-a od posebnog značaja je određivanje uloga i odgovornosti za izvršavanje i kontrolu procesa.

5.2 RAZVOJ METODOLOGIJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

U konceptu reaktivnih sistema, menadžment zaštite informacija se u velikoj meri može poistovetiti sa menadžmentom rizika u IKT okruženju. Iako je ova identičnost prilično očigledna i intuitivno prihvatljiva, nije sasvim tačna. Naime, razvijene su brojne tehnike i metode za menadžment rizika u IKT okruženju, dok se komparativno slabija pažnja posvećuje aspektu menadžmenta procesa zaštite u celini. Posledica je da prosečni korisnici vide zaštitu informacija kao tešku i komplikovanu oblast.

Tradicionalna imovina organizacije je dominantno opipljiva u formi materijalne imovine, opreme, zgrada, stolova, novca, zlata itd. Imovina savremene organizacije se sve više predstavlja digitalnim podacima i opravdano definiše kao *informaciona imovina* (čista, hardverska, humana) u kojoj su *informacije* najznačajnija imovina organizacija. Zato se zaštita informacione imovine može predstaviti zaštitom tri ključna atributa informacija – *poverljivosti, integriteta i raspoloživosti* (CIA).

Menadžment sistem zaštite informacija, generalno obuhvata tehnike upravljanja brojnim kontrolama zaštite računarskog sistema (RS) i mreže (RM), a obezbeđuje se dokumentovanim i implementiranim procedurama zaštite, ugrađenim u procese administracije zaštite i rutinske računarske i mrežne operacije za održavanje CIA informacija i servisa. Specifične aktivnosti za koje se definišu i implementiraju procedure menadžment sistema zaštite informacija uključuju: *procenu rizika, logovanje bezbednosnih događaja, antivirusnu zaštitu, detekciju upada u RM-u, procenu ranjivosti i odgovor na incidente, fizičku i zaštitu okruženja, kontrolu pristupa, razvoj i održavanje sistema, personalnu zaštitu i obuku, upravljanje vanrednim događajem, nadzor i kontrolu i proveru usaglašenosti prakse zaštite sa standardima i politikom zaštite*.

Tehnike menadžment sistema zaštite brojne su i obuhvataju sve kategorije upravljanja: *manuelnog* (npr. planiranjem), *poluautomatskog* (npr. CRAMM metod za upravljanje rizikom) i *automatskog* (npr. EUA paketi za automatsku implementaciju ovlašćenja pristupa

u velikim sistemima i sl.). U oblasti menadžmenta sistema zaštite informacija, brojni su otvoreni problemi i očekuje se dalji razvoj.

5.2.1 Principi menadžment sistema zaštite informacija

Opšte prihvaćeni principi zaštite informacija (*GAISP*), su osnovni skup konzistentnih principa za menadžment sistem zaštite [26, 75]. Namenjeni su menadžerima u poslovnom sistemu za razvoj svesti o potrebi zaštite i efektivnije upravljanje sistemom zaštite informacija. Kako je menadžment bezbednosnog rizika najbliža aproksimacija menadžmenta zaštite, u razvoj procesa menadžment sistema zaštite informacija, ugrađen je skup od pet principa menadžmenta rizika[1]:

1. procena rizika i određivanje bezbednosnih zahteva;
2. uspostavljanje sistema za centralno upravljanje rizikom;
3. implementacija rentabilnih politika i kontrola zaštite;
4. promovisanje svesti o potrebi i obuka;
5. nadzor i kontrola sistema zaštite i evaluacija efektivnosti i usklađenosti.

5.2.2 Razvoj uloga i odgovornosti u ISMS-u

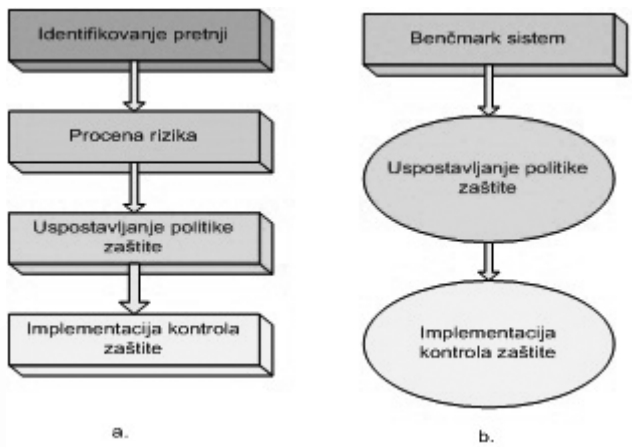
U organizaciji procesa menadžment sistema zaštite informacija sve uloge i odgovornosti moraju biti definisane i dodeljene svim zaposlenima [47, 56]. Lice odgovorno za ISMS je imenovano lice za zaštitu informacija organizacije (npr. CIO-*Corporate Information Officer*), ali je trend da se ovom poslu posveti puno radno vreme, kao što je rukovodilac sistema zaštite informacija organizacije − CISSO (*Corporate Information System Security Officer*), koji je odgovoran za zaštitu informacija u celoj organizaciji i angažovan puno radno vreme. Trend je podizanje odgovornosti za menadžment sistema zaštite na nivo profesionalnog menadžera − CIAO *(Corporate Information Assurance Officer),* koji je ovlašćen i za sertifikaciju sistema zaštite [56].

Najznačajniji resurs na raspolaganju svakom menadžeru sistema zaštite, svakako je tim dobro obučenih specijalista zaštite koji poseduje različita i specifična znanja, veštine i iskustva, relevantna za lokalnu sredinu i okruženje. Najbolja praksa zaštite zahteva da svaki član tima neprekidno, *proaktivno* usavršava znanja i veštine, jer samo dobro osposobljen tim garantuje postizanje dugoročnih bezbednosnih ciljeva. Pri tome treba praviti razliku između veština raspoloživih na tržištu (tipa CISP − *Certified Information Security Professionals,* SANS i dr.) i specifičnih veština i iskustava za datu organizaciju i okruženje, stečenih radom u konkretnoj organizaciji. Ova znanja poseduje mali broj ljudi i najčešće nisu dokumentovana i dostupna širem krugu profesionalaca u zaštiti. Obe kategorije znanja i veština u zaštiti podjednako su značajne, s tim da je specifično obučene specijaliste zaštite teže zaposliti i zadržati.

1 NIST SP 800-30.

5.2.3 Generički procesi menadžment sistema

Generički procesi menadžmenta IKT sistema uključuju *funkcionalnu, informacionu, komunikacionu i organizacionu* oblast menadžmenta. *Generički proces* ISMS-a u osnovi sadrži četiri koraka: (1) *identifikovanje pretnji, (2) procenu rizika, (3) uspostavljanje politike zaštite i (4) implementaciju kontrola zaštite za ublažavanje rizika* (slika 5.1 a).



Slika 5.1 Generički proces ISMS-a (a) i usaglašenosti sa ISBS *(b)*

Druga opcija je razvoj osnovnog mehanizma za menadžment zaštite na strateškom nivou – *politike zaštite,* gde se koristi standardni *sistem identifikatora progresa* – BS (*Benchmark System)*. *Sistem identifikatora progresa zaštite informacija* – ISBS (*Information Security Benchmark System)* predstavlja preporučeni nivo izvršavanja politika zaštite u normalnim uslovima i garantuje implementaciju dobrog programa zaštite. Usaglašenost sa ISBS znači da je organizacija imala dobru procenu pretnji i rizika i da je implementirala adekvatne kontrole zaštite za ublažavanje faktora rizika (slika 5.1 b) [64].

5.3 RAZVOJ STANDARDA MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

Implementacija ISMS-a, na bazi ISO/IEC 27001 i ISO/IEC 27002 standarda i uputstva za razvoj i implementaciju ISMS standarda [102], obezbeđuju efektivan menadžment sistem zaštite informacija. Procesni pristup PDCA (*Plan, Do, Check, Act*) predstavlja metodologiju za implementaciju ISMS. Standard ISO 27002 obezbeđuje *kontrole zaštite* za efektivnost ISMS-a, a ISO/IEC 27001 − smernice za implementaciju ISMS primenom PDCA procesa. U tabeli 5.1 prikazana je kratka istorija razvoja ISO/IEC standarda zaštite informacija.

Tabela 5.1 *Razvoj ISMS standarda zaštite informacija*

Godina	Aktivnost u razvoju standarda zaštite informacija
1989.	DTI (*The U.K. Department of Trade and Industry*) uspostavlja radnu grupu za izradu standarda dobre prakse zaštite *User Code of Practice* – liste *kontrola zaštite.*
1995.	*User Code of Practice* objavljen kao Britanski standard (BS) - *BS 7799:1995, Part 1*
1998.	Drugi deo standarda je dodat i objavljen kao *BS 7799:1998, Part 2* za merenje i monitoring *Part 1* i benčmarking za sertifikaciju.
1999.	Standard *Part 1* je objavljen kao *BS 7799:1999 Part 1,* predložen kao ISO standard.
2000.	Standard *ISO 17799* je objavljen kao *ISO 17799:2000.*
2002.	Objavljena revizija Part 2 standarda kao *BS 7799:2002, Part 2*
2005.	Revidiran standard *ISO 17799* i objavljen kao *ISO 17799:2005* i promenjeno ime u *ISO 27002:2005.*
2007.	Standard *BS 7799, Part 2*, ponovo revidiran i objavljen kao ISO 27001:2005.

Na izradi međunarodnih standarda zajedno rade ISO i IEC. U okviru združenog tehničkog komiteta (JTC1) radna grupa WG 1 je razvila ISMS standard za menadžment sistem zaštite informacija. Cilj WG 1 je identifikacija zahteva za novi razvoj ISO standarda i razvoj uputstava za uspostavljanje, implementaciju, rad, monitoring i održavanje ISMS standarda. Za podršku ovog plana razvoja ISO/IEC je doneo odluku da uvede novi sistem numeracije serije međunarodnih standarda za zaštitu informacija ─ 27000. Familija standarda ISO/IEC 2700 prikazana je u tabeli 5.4.

Table 5.2 *Familija standarda ISO/IEC 27000*

ISO/IEC standard	Namena standarda
27001	menadžment sistem zaštite informacija (ISMS), (BS 7799, Part 2 od 2007. g)
27002	katalog kontrola zaštite za smanjivanje rizika (ISO/IEC 17799:2005)
27003	uputstvo za implementaciju ISMS (BS 7799, *Part 2 Annex B*)
27004	metrika i merenja performansi i efektivnosti ISMS
27005	menadžment rizika (BS 7799, Part 3)
27006	sertifikacija i akreditacija sistema zaštite
27007	sistem za proveru (*audit*) zaštite informacija (u radu)
27008	uputstvo za kontrole sistema za proveru zaštite (u radu)
27010	uputstvo za menadžment zaštite komunikacija (u radu)
27011	uputstvo za ISMS telekomunikacionih organizacija (u radu)

ISO/IEC standard	Namena standarda
27013	uputstvo za integrisani menadžment IKT servisa i ISMS (u radu)
27014	usmeravanje bezbednosti informacija (u radu)
27015	uputstvo za ISMS finansijskih organizacija (u radu)
27031	standard za kontinuitet poslovanja fokusiran na IKT sistem (u radu)
27032	uputstvo za zaštitu kiber prostora (u radu)
27033	standard za zaštitu računarskih mreža (menja ISO/IEC 18028) (u radu)
27034	uputstvo za zaštitu aplikacija (u radu)
27035	standard za menadžment kompjuterskog incidenta (menja ISO TR 18044) (u radu)
27036	uputstvo za zaštitu podugovarača (u planu)
27037	uputstvo za digitalne dokaze (u planu)
27038	uputstvo za redukciju digitalnih podataka (u planu)
27040	uputstvo za zaštitu sistema za skladištenje podataka (u planu)
27799:2008	ISMS zdravstvenih informacija primenom ISO/IEC 27002 (u planu)
Ostali ISO27k	bezbednost u *cloud computing* okruženju, bezbednost IKT u lancu snabdevanja, taksonomije u zaštiti informacija, troškovi zaštite itd.

Imajući u vidu da bezbednost informacija nije odredište do koga treba stići, nego dinamičan proces koji se ciklično ponavlja, u razvoju ISO/IEC standarda razmatraju se i drugi standardi zaštite, kao što su NIST, ISO/IEC 13335, BSI (E) itd.

5.3.1 UVOD U STANDARD ISO/IEC 27001 (ISMS)

Standard ISO/IEC 27001 obezbeđuje smernice za kreiranje menadžment sistema zaštite informacija (ISMS-a) i referentnu listu kontrola zaštite iz ISO/IEC 27002 za uspostavljanje i održavanje ISMS-a .

Standard ISO/IEC definiše ISMS kao "*deo menadžment sistema totalnog kvaliteta (TQM), zasnovanog na pristupu proceni poslovnog rizika, za uspostavljanje, implementaciju, rad, monitoring, proveru, održavanje i poboljšanje sistema zaštite informacija*." TQM[2] sistem u organizaciji uključuje sve standarde menadžment sistema kvaliteta. Familija ISO/IEC 9000 je serija standarda za menadžment sisteme kvaliteta, a ISO/IEC 27000 − za menadžment sistem kvaliteta zaštite informacija sa terminologijom koja je primenljiva za sve menadžment sisteme i koja usmerava akcije za uspostavljanje, održavanje i poboljšanje ISMS-a. Alternativna imena za ISMS su **SMP** (*Security Management Program*) i **IAP** (*Information Assurance Program*). U ISO standardima termin „*sistem*" znači „*proces*" ili „*metodologiju*", a ne aktuelni uređaj ili aplikaciju, a *program zaštite* znači isto što i ISMS u ISO terminologiji.

2 Heleta, M., *TQM – modeli izvrsnosti i integrisani menadžment sistemi,* Zavod za udžbenike, Beograd, 2010.

Za uspostavljanje efektivnog ISMS-a potrebno je implementirati mnogo detalja. Menadžment rizika i sistema zaštite uključuju brojne kategorije ili komponente zaštite, kao što su: *organizaciona, fizička i personalna zaštita, upravljanje imovinom, zaštita komunikacija, menadžment kompjuterskog incidenta i vanrednog događaja, akvizicija ili razvoj IKT, kontinuitet poslovanja, kontrola pristupa* itd. Svaka od ovih kategorija sastoji se od više bezbednosnih podkategorija i elemenata zaštite.

Primer: *Kategorija kontrole pristupa uključuje korisnički, mrežni i pristup operativnom sistemu; mrežni pristup sadrži bezbednosne elemenate kao što su politika, autentifikacija korisnika, dijagnostika udaljenog pristupa, kontrola mrežnih konekcija i mrežnog rutiranja.*

Broj detalja sistema zaštite može biti obiman i konfuzan, pa postoji potreba da se generiše neki okvir za definisanje svih bezbednosnih pitanja organizacije. Za svaku organizaciju dobra polazna tačka u implementaciji ISMS-a je razvoj *menadžment okvira zaštite* – SMF[3] (*Security Management Framework*), koji obezbeđuje nacrte za definisanje diskusija, planova, implementacije, praćenja i izveštavanja svih pitanja zaštite relevantnih za organizaciju [61]. Kako proces razvoja ISMS-a koristi termine, koncepte, uzorke, alate za analizu i izveštavanje itd., sa specifičnim značenjem i namenom, uspostavljanje baze značenja i namena ovih elemenata zaštite u fazi razvoja SMF-a, obezbeđuje bolje razumevanje načina upotrebe u procesu razvoja i održavanja ISMS-a.

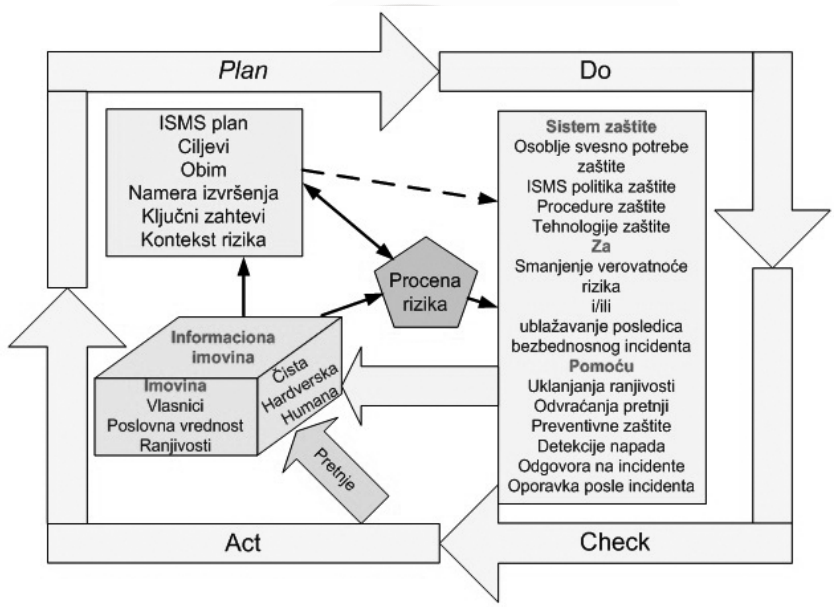
Dobar SMF se zasniva na industrijskim standardima u pogledu sveobuhvatnosti, konzistentnosti i generalnog promovisanja primene najbolje industrijske prakse (NIST, FIPS, STIGs, ENISA itd., a po potrebi *Sarbanes–Oxley*, HIPAA i dr.)[4]. Iako SMF kao osnovu koristi ISO/IEC 27002, pre se može reći da ga čine ISO/IEC 27001 i ISO/IEC 27002 zajedno, sa dodacima ili modifikacijama za specifične potrebe organizacije. Glavna prednost izrade sveobuhvatnog SMF-a je jedinstveni okvir koji opisuje sva identifikovana bezbednosna razmatranja. Iako se u SMF-u obuhvate svi bezbednosni elementi, to ne znači da organizacija obavezno treba da za svaki od njih implementira zaštitu. Validna odluka o implementaciji zaštite za neki bezbednosni elemenat iz SMF-a donosi se na bazi procene rizika. Mehanizme zaštite ne treba implementirati, ako poslovni rizik za neki elemenat nije dovoljno velik da se isplati tretman rizika, što detaljnije pokazuju procesi interne ili nezavisne provere i sertifikacije ISMS-a.

Precizno praćenje standarda ISO/IEC 2002, podrazumeva dogmatski pristup ISMS-u. Zavisno od bezbednosnih potreba, specifičnosti konteksta i profila rizika organizacije, sugeriše se fleksibilniji pristup ISMS-u, u kojem se dodaje, menja, briše ili reorganizuje nešto iz standarda ISO/IEC 27002. Cilj ovog pristupa je da se generiše *SMF specifičan za organizaciju*, koji se zasniva na industrijskim standardima i obezbeđuje smernice za razvoj ISMS-a usaglašenog sa TQM sistemom organizacije. Za sertifikaciju implementacije ISMS-a zahtevaju se poglavlja četiri do osam standarda ISO/IEC 27001.

3 SMF u organizaciji može biti obiman, ali kao metodološka kategorija ne postoji.

4 *Engl.: National Institute of Standards and Technology, Federal Information Processing Standards, Security Technical Implementation Guides, European Network and Information Security Agency, Health Insurance Portability and Accountability Act.*

Dakle, SMF je okvir bezbednosnih kategorija (ili komponenti), potkategorija i elemenata za unapređivanje GAISP principa *konzistentnosti* i *sveobuhvatnosti* zaštite. Jednom generisan, SMF se može primeniti i za praćenje razvoja ISMS-a i sistema zaštite, distribuciju i ocenu efektivnosti politike, standarda i procedura zaštite, primenljivih za svaku bezbednosnu kategoriju (slika 5.2). Takođe, neki servisi zaštite mogu biti uspostavljeni interno ili automatizovano, a neke obezbeđuju TTPS provajderi zaštite. SMF obezbeđuje okvir u kojem treba razvijati ISMS dokumentaciju i alate za usaglašavanje menadžment sistema zaštite informacija sa drugim u TQM sistemu organizacije. Alati za usaglašavanje menadžment sistema sadrže upitnike za prikupljanje informacija i identifikovanje bezbednosnog stanja, alate za analizu i procesiranje prikupljenih informacija, alate za izveštavanje, prenos rezultata i praćenje progresa aktivnosti poboljšanja sistema zaštite.



Slika 5.2 Okvir menadžment sistema zaštite (SMF)

Vrlo korisna primena SMF je za praćenje usaglašenosti menadžment programa sa zahtevima standarda i za generisanje poslovnih zahteva i inicijativa zaštite. Praćenje usaglašenosti obezbeđuje, između ostalog, procenu zahteva za finansiranje sistema zaštite i održavanja bezbednosnih operacija i u slučaju restrikcije budžeta. Na primer, vrlo je teško isključiti neke mehanizme zaštite (npr. IDPS) ili operacije menadžmenta kompjuterskog incidenta iz projekta zaštite u slučaju nedostatka finansijskih sredstava. Formalno usaglašavanje SMF-a i implementacije ISMS-a sa standardima, omogućava da se na bazi procene poslovnog rizika generišu podaci za povratak investicije za zaštitu − ROSI (*Return on Security Investment*) [43]. Okvir SMF-a zasnovan na ISO/IEC 27002 treba da sadrži, najmanje, sledeće kategorije:

- politiku zaštite (*Security Policy*),
- plan menadžmenta zaštite (*Security Management Plan*),
- menadžment imovine organizacije (*Asset Management*),
- personalnu zaštitu (*Personnel Security*),
- fizičku zaštitu (*Physical Security*),
- menadžment operacija (prakse) zaštite – OP (*Operations Management*),
- menadžment pristupa – AM (*Access Management*),
- garantovan kvalitet rešenja zaštite − SQA (*Solution Quality Assurance*),
- menadžment kompjuterskog incidenta – IM (*Incident Management*),
- menadžment kontinuiteta poslovanja - BCM (*Business Continuity Management*) i oporavka sistema posle vanrednog događaja − DRM (*Disaster Recovery Management*) i
- menadžment procesa usaglašavanja – CM (*C ompliance Management*).

Prednosti SMF-a uključuju sledeće:

- obezbeđuje *listu termina i definicija zaštite* za bolje razumevanje,
- omogućava *konzistentne rezultate,*
- obezbeđuje *alat za planiranje i pripremu poslovanja i zaštite informacija,*
- obezbeđuje *alat za efektivno prikupljanje informacija* (bez intervjua) o ciljnim pitanjima, istraživanju i alatima za automatsko otkrivanje koji čine osnovu za: *analitičke alate* – za dostizanje nivoa usaglašenosti zahteva; poređenje – za traženje prihvatljivog rešenja i za *pripremljenost* − korišćenjem industrijskog standarda u cilju uklanjanje potencijalne arbitraže,
- omogućuje *poređenje rezultata* organizacija koje koriste isti standard,
- obezbeđuje osnovu *alata za izveštavanje*: kompletnosti, konzistentnosti i razumevanja u kontekstu interpretacije i *dostavljanje povratne informacije* o bezbednosnim operacijama i popravljanju servisa za evidentiranje i
- obezbeđuje osnovu *za procenu progresa i tekućeg stanja zaštite* informacija.

Kako većinu bezbednosnih zahteva treba interpretirati, od velike je koristi za organizaciju da razvije *smernice za interpretaciju* značenja i namene sadržaja u SMF okviru. Svaka organizacija, u zavisnosti od konteksta i bezbednosnih potreba, treba da razvije svoje specifične smernice za interpretaciju SMF-a. U tabeli 5.3 dat je uzorak SMF okvira i *smernica za interpretaciju* značenja i namene *politike zaštite*. Okvir je prilično obiman, a aktuelne *smernice za interpretaciju* značenja i namene SMF-a, mogu se razlikovati u organizacijama, zavisno od poslovnih ciljeva, okruženja i drugih zahteva za usaglašenost. Na primer, zdravstveni informacioni sistem treba da se usaglasi i sa standardom HIPAA. Standard ISO/IEC 27001 koristi termin „*normativne reference*" kojim označava prezentaciju uobičajenih termina i definicija i osigurava razumevanje svih relevantnih učesnika

Tabela 5.3 *Uzorak SMF okvira i smernica za interpretaciju politike zaštite*

Kategorija/ pod-kategorija/ elemenat zaštite	Zahtev za usaglašenost	Interpretacija/komentar
Politika zaštite		*Ako je potrebno, treba razjasniti neki elemenat.*
Politika zaštite informacija		Organizaciji treba politika zaštite koja podržava misiju organizacije i reflektuje zahteve za usaglašenost.
Dokumentacija	Menadžment generiše politiku zaštite koja uključuje *kontrole zaštite* informacija i jasne smernice za implementaciju.	Uspešan program zaštite mora imati određene izvršne i menadžerske uloge i odgovornosti. Smernice za efektivan program zaštite moraju biti dokumentovane sa politikom zaštite.
Distribucija	Politiku zaštite treba distribuirati u organizaciji i svi zaposleni moraju biti upoznati, u cilju razvoja svesti o potrebi zaštite i prihvatanju politike.	Da bi se politika zaštite primenjivala, svi zaposleni i ostali relevantni učesnici moraju biti upoznati sa svojim pravima i obavezama i kako primenjivati politiku u praksi zaštite.
Pregled (revizija) politike	Politiku zaštite treba pregledati i revidirati (proveravati) u regularnim intervalima ili u slučaju značajnih promena, koje utiču na aktuelnu politiku zaštite; takođe, treba da postoji odgovorno telo u organizaciji koje prati i revidira politiku i sve promene politike zaštite.	Treba definisati događaje koji zahtevaju reviziju politike zaštite: vremenski termin; kompjuterski incident; promene poslovanja, tehnologije i okruženja itd. Uspostaviti radnu grupu (tim) za reviziju politike zaštite u skladu sa poslovnim terminima.

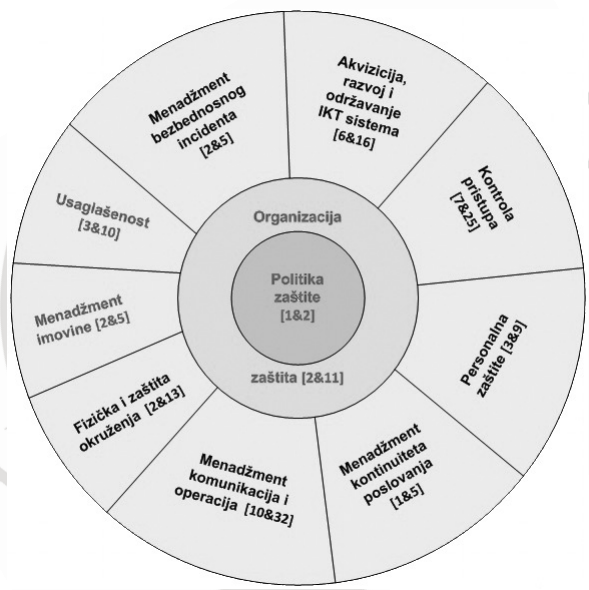
5.3.2 Uvod u standard ISO/IEC 27002

Standard ISO/IEC 27002 [57], obezbeđuje uvid u *kontrole zaštite* informacione imovine, ali ne i kako primeniti te *kontrole*. Standard ISO/IEC 27001 obezbeđuje metodološko uputstvo za uspostavljanje menadžment sistema zaštite informacija, koji nameće dobru praksu i disciplinovani izbor i primenu *kontrola zaštite*. Procedure za realnu implementaciju *kontrola zaštite* zavise od organizacije, fizičkog i tehničkog okruženja. Standard ISO/IEC 27002 sadrži 12 poglavlja, od čega 11 poglavlja (2-12) obuhvata *ciljeve zaštite* za glavne kategorije (broj ciljeva za svaku kategoriju je dat u zagradi) i broj pripadajućih *kontrola zaštite po kategoriji* (slika 5.3):

1. procena i tretman rizika
2. politika zaštite (1)
3. organizacija zaštite informacija (2)
4. menadžment imovine organizacije (2)
5. zaštita ljudskih resursa (3)
6. fizička zaštita i zaštita okruženja (2)

7. menadžment komunikacija i operacija zaštite (10)
8. kontrola pristupa (7)
9. akvizicija, razvoj i održavanje IKT sistema (6)
10. menadžment bezbednosnog incidenta (2)
11. menadžment kontinuiteta poslovanja (1)
12. usaglašenost (3).

Standard ISO/IEC 27005 detaljno opisuje menadžment i procenu rizika [58]. *Kontrole zaštite* treba birati u odnosu na *ciljeve kontrola*, obezbeđene u standardu ISO*/*IEC 27002. Na slici 5.3 treba zapaziti da će prve četiri kategorije (crvene) uvek biti primenljive, a da brojke u zagradama referenciraju brojeve ciljeva kontrola i broj zastupljenih kontrola zaštite svake kategorije u standardu.



Slika 5.3 Kategorije kontrola zaštite u standardu ISO/IEC 27002

Ovih 11 poglavlja pokriva oko 39 ključnih elemenata i 134 *kontrole* zaštite[5]. U tabeli 5.4 ilustrovane su generička struktura i kratki opis individualnih kontrola zaštite, koji treba koristiti za pisanje politike i procedura zaštite, a iz ciljeva kontrola treba derivirati njihovu namenu.

5 NIST SP 800-53 A za osnovnu zaštitu sadrži 196 kontrola grupisanih u 3 klase i 18 familija.

Table 5.4 *Struktura kontrole zaštite u standardu ISO/IEC 27002*

Kontrola	Definicija kontrole zaštite sa izjavom koja se odnosi na potrebne kvalitete za ispunjavanje zahteva kontrole.
Smernice za implementaciju	Uključuje informacije za implementaciju kontrole i smernice za ispunjavanje zahteva kontrole.
Druge informacije	U nekim kontrolama se nalazi klauzula „druge informacije", gde su reference na informacije koje se odnose na specifičnu kontrolu.

U praksi zaštite standardi ISO/IEC 27001 i 27002 koriste se zajedno. Dok ISO/IEC 27001 predstavlja *menadžment sistem* za bezbednost informacione imovine i to više tipa **kako** (tj. procedure za uspostavljanje menadžment sistema koje usmeravaju **kako** uspostaviti i održavati *kontrole zaštite*), ISO/IEC 27002 predstavlja uputstvo za primenu kontrola zaštite i to više tipa **šta** (tj. lista korisnih *kontrola*). Ipak, ISO/IEC 27001 nije skup procedura koje obuhvataju svaku ISO/IEC 27002 kontrolu zaštite, nego pre predstavlja menadžment proces za uspostavljanje svesti o potrebi zaštite, organizacione infrastrukture, plana implementacije i održavanja *kontrola* zaštite. Organizacije uglavnom nastoje da se sertifikuju za standard ISO/IEC 27001, a retko za ISO/IEC 27002. U Aneksu A standarda ISO/IEC 27001 referencirane su iste kontrole zaštite iz ISO/IEC 27002 i sa istom numeracijom, ali sa skraćenim opisom. Oba standarda zajedno sa uputstvima za implementaciju obezbeđuju sigurnu ISO/IEC 27001 sertifikaciju. Dobro projektovana arhitektura sistema zaštite obezbeđuje raznovrsnu zaštitu po dubini, primenom kontrola zaštite sa kombinacijom funkcija za:

- *odvraćanje*: sprečava ili redukuje verovatnoće pojave neželjenih događaja,
- *izbegavanje*: eliminiše poznate ranjivosti i sprečava kreiranja novih,
- *zaštitu*: zaštita imovine od izlaganja neželjenim bezbednosnim događajima,
- *detekciju*: identifikacija bezbednosnog događaja,
- *reakciju*: odgovor ili protivmera bezbednosnom događaju i
- *oporavak*: restauracija integriteta, raspoloživosti i poverljivosti imovine.
- sertifikaciono telo za verifikaciju kompetencija proverivača (*auditor*).

5.3.3. Komplementarnost ISMS standarda sa drugim ISO standardima

Organizacije ISO/IEC obezbeđuju brojne standarde za menadžment sisteme. Tako je serija ISO 9000 namenjena za menadžment kvaliteta, ISO 14000 za menadžment okruženja, a ISO 27000 − za menadžment sistema zaštite informacija. Standard ISO/IEC 27001 predstavlja uvod u odnose ISMS-a sa drugim standardima menadžment sistema i harmonizuje se sa drugim standardima menadžment sistema, obezbeđujući konzistentnu i integrisanu implementaciju TQM sistema organizacije. Implementacija ISMS-a sa drugim standardima menadžment sistema, često se naziva *Program menadžmenta usaglašavanja* − CMP (*Compliance Management Program*). Za implementaciju, monitoring i poboljšanje, ISMS standard koristi PDCA model procesnog pristupa, koji koriste i drugi ISO standardi menadžment sistema. Svi ISO standardi menadžment sistema imaju sledeće zajedničke karakteristike:

- zasnovani su na angažovanju menadžmenta,
- imaju definisane odgovornosti,
- dokumentuju *kontrole,*
- aktivnosti menadžmenta se evidentiraju (*Record Management*),
- zahteva se obuka zaposlenih,
- zahteva se revizija menadžmenta,
- vrši se interna provera,
- vrše se korektivne i preventivne akcije,
- primenjuje se PDCA model[6] za implementaciju, rad i održavanje,
- zahtevaju se procesi nezavisne provere (*audit*),
- primenjuje se šema za procenu kvaliteta, zasnovana na standardu ISO 19011:2002[7],
- uključuju zahteve zasnovane na sličnim standardima i

5.4 PROCESNI PRISTUPI ZA USPOSTAVLJANJE ISMS-a

PDCA model se koristi u industrijskoj proizvodnji više od 50 godina, a čine ga ciklično ponavljane aktivnosti, dizajnirane da pokreću neprekidno poboljšanje procesa. Model je prvi razvio i opisao *Walter Shewarks*[8], ali ga je više popularisao *Edward Deming* za neprekidno poboljšavanje procesa. PDCA model se može koristiti za implementaciju ISMS-a, prema specifikaciji u ISO/IEC 27001 standardu. U tabeli 5.5 dat je kratak opis faza PDCA modela.

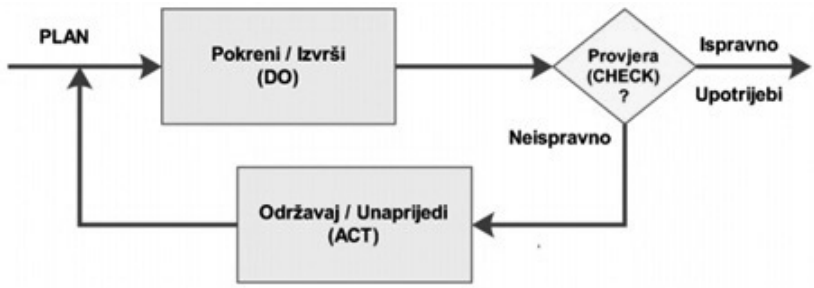
Tabela 5.5 *Kratak opis faza PDCA modela procesa*

PDCA	Kratak opis
Planiranje	Definiše obim ISMS i politiku zaštite. Identifikuje i procenjuje rizik. Bira ciljeve kontrola zaštite za tretman rizika. Formuliše plan za tretman rizika i priprema SOA dokument.
Primena	Implementira plan za tretman rizika. Implementira izabrane kontrole zaštite za postizanje ciljeva kontrola u okviru menadžmenta rizika poslovanja.
Provera	Izvršava procedure monitoringa. Preduzima pregled i kontrolne mere i vrši internu proveru (*audit*) ISMS sistema.
Delovanje	Implementira poboljšanja ISMS.

6 PDCA model se koristi u BS 7799, Part 2 i ISO 27001, ISO 9001 i ISO 14001.
7 Engl.: ISO 19011:2002 – *Guidelines on Quality and/or Environmental Management System Audit.*
8 Engl.: Shewhart, Walter Andrew (1939), *Statistical Method for the Viewpoint of Quality Control*,New York: Dover. (1980), Economic Control of quality of manufactured product/50th Anniversary Commemorative Issue. American Society For Quality, http:en.wikipedia.org/wiki/Shewhart_cycle.

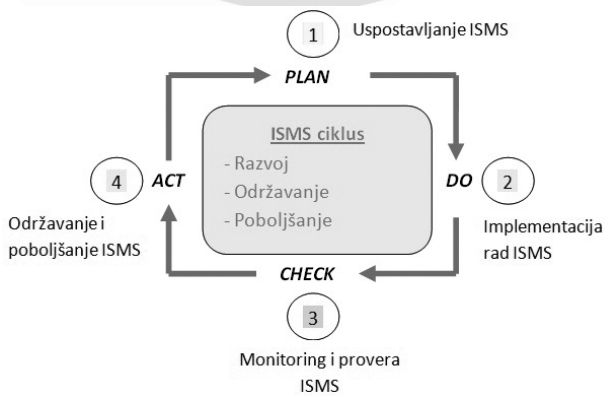
Primena PDCA modela obezbeđuje višekratno korišćenje investicije u praksi menadžment sistema. Faze PDCA modela obuhvataju smernice o tome kako:

- uspostaviti politiku, ciljeve, procese i procedure za menadžment rizika (*Plan*),
- implementirati i operativno primenjivati praksu ISMS-a (*Do*),
- izvršiti procenu i merenja performansi politike zaštite (*Check*) i
- kako poboljšati ISMS i izvršiti korektivne i preventivne akcije (*Act*) (slika 5.4).



Slika 5.4 PDCA procesni model

U okviru prve faze PDCA procesa organizacija definiše obim ISMS-a, skuplja detaljne informacije o obimu imovine, procenjuje rizik na bazi obima imovine i poslovnih procesa i procenjuje primenljivost kontrola zaštite (SoA) iz ISO/IEC 27002 standarda. Zatim, selektuje odgovarajuće kontrole zaštite i donosi relevantne i racionalne odluke u procesu izrade saopštenja o njihovoj primenljivosti (SoA). Sledeći korak je implementacija kontrola zaštite, a zatim slede aktivnosti monitoringa i provere kontrola zaštite i sprovođenja procedura poboljšanja ISMS-a. Koristeći ulazne podatke iz interne menadžerske provere ISMS-a, u poslednjoj fazi PDCA modela implementiraju se poboljšanja, čime se balansira menadžment rizika sa ciljevima poslovanja. Na slici 5.5 prikazan je funkcionalni model PDCA procesa.



Slika 5.5 Funkcionalni model PDCA procesa

U tabeli 5.6 prikazani su koraci faza PDCA modela procesnog pristupa.

Tabela 5.6 *Koraci faza PDCA modela procesnog pristupa*

PDCA faze	Koraci
Faza planiranja i uspostavljanja (*Plan*)	proces i proizvodi (rezultati rada) faze planiranja definicija oblasti primene procena trenutnog stanja bezbednosti (*Security Baseline*) proces procene rizika izjava o primenljivosti (SoA) pregled dokumentacije o fazi planiranja
Faza primena (implementacije) (*Do*)	proces i proizvodi faze implementacije plan tretmana rizika identifikovanje i raspored resursa politika i procedure za vođenje evidencije (zapisa) metrike i merenja izrada i sprovođenje plana upravljanja kontinuitetom poslovanja (BCMP) kontrola procesa implementacije obuka o implementiranim kontrolama zaštite upravljanje operacijama i resursima procedura za implementaciju sistema zaštite informacija pregled dokumentacije faze implementacije
Faza monitoringa i provere (*Check*)	proces i proizvodi faze provere izvođenje operativnog plana procena usaglašenosti pregled efektivnosti *kontrola zaštite* ISMS-a pregled nivoa preostalog rizika sprovođenje interne provere ISMS sprovođenje redovne provere ISMS-a evidentiranje akcija i događaja koji utiču na ISMS pregled dokumentacije faze provere
Faza održavanja i poboljšanja (*Act*)	proces i proizvodi faze delovanja implementacija identifikovanih poboljšanja korektivne i preventivne akcije primena stečenih iskustava prenošenje rezultata relevantnim učesnicima i svim zaposlenim obezbeđivanje bezbednosnog cilja nastavljanje drugog ciklusa PDCA procesa pregled dokumentacije faze delovanja.

5.4.1. Drugi pristupi za uspostavljanje ISMS-a

Za uspostavljanje ISMS standarda i razumevanje ISO terminologije mogu se koristiti i drugi pristupi, kao što je koncept *tranzicije bezbednosnog stanja* za procenu rizika, koji uključuje četiri faze [102]:

1. stanje kakvo treba da bude (*to-be state*),
2. stanje kakvo jeste (*as-is state*),
3. plan tranzicije (*transition plan*) iz jednog u drugo bezbednosno stanje i
4. operativni rad i održavanje.

U kontekstu menadžmenta poslovnog rizika, stanje kakvo treba da bude (*to-be state*) je ciljno stanje upravljanja rizikom, koje definiše kombinacija ISO/IEC 27001 i ISO/IEC 27002 standarda, a uključuje angažovanje menadžmenta, organizacionu strukturu, obim, politiku, standarde, procedure i drugo. Poznavanje stanja između *tekućeg* i *željenog* obezbeđuje podatke za razvoj *plana tranzicije* iz jednog u drugo stanje.

U fazi ciljnog stanja definišu se ciljevi zaštite u terminima menadžmenta poslovnog rizika i okvir u kojem treba uspostaviti ISMS. Sadržaj ISMS-a određuju poslovni ciljevi. U PDCA modelu ove aktivnosti se nalaze u fazi *planiranja*, a elaboracija SMF okvira u 3. poglavlju ISMS standarda.

U fazi stanja kakvo jeste određuje se tekuće stanje bezbednosti informacija u odnosu na ISMS, definisan u fazi *to-be* stanja. Ova faza obuhvata procese otkrivanja, analize razlika (*gap* analize) i izveštavanja o nalazima, koji su pokriveni u 3. poglavlju ISMS standarda, uključujući osnovni set pitanja za otkrivanje stanja i uzorke obrazaca. U PDCA modelu ove aktivnosti se primenjuju u fazama *planiranja* i *provere*.

U faza planiranja tranzicije definišu se detalji o prelasku iz *as-is* u *to-be* stanje. Realni proces tranzicije može zahtevati više od jednog budžetskog ciklusa, zavisno od obima aktivnosti potrebnih za dostizanje ISMS ciljeva. Realno je očekivati da organizacija alocira resurse za prioritetno smanjivanje najvećih faktora rizika. U ISMS standardu detalji o razvoju plana tranzicije opisani su u četvrtom poglavlju. U procesu plana tranzicije generišu se sledeća dokumenta:

- *izveštaj o analizi poboljšanja sistema zaštite*, koji je detaljan i može uključivati formalnu izjavu o bezbednosnim ciljevima (tj. formalnu definiciju projekta), model troškova sa strukturom rada − WBS (*Work Breakdown Structure*) i plan projekta sa kontrolnim tačkama progresa i vremenom isporuke;
- *plan tranzicije,* struktiuran dokument;
- *ugovor o nivou usluga* − SLA (*Service Level Agreement*) za spoljne snabdevače ili interne operacije (npr. ciljevi *uptime* rada su 99% od operativnog rada), koji može biti deo dokumenta plana tranzicije; u PDCA modelu ovaj plan se kreira u fazi *činjenja* i *delovanja*.

U fazi operativnog rada i održavanja obezbeđuje se tekuća podrška ISMS-u, uključujući periodični pregled *to-be* stanja. Revizija se zahteva posle pojave novog standarda/regulative ili promena ugovornih obaveza i poslovnog okruženja. U ovoj fazi obezbeđuju se merenja i metrike performansi, u odnosu na SLA i najčešće generišu brojni bezbednosni izveštaji, kao

što su log izveštaji i analiza uzroka napada. U PDCA modelu ove aktivnosti se izvršavaju u fazama *provere* i *delovanja*.

5.4.2 Razvoj metrika za evaluaciju ISMS-a

Za određivanje efektivnosti i efikasnosti procesa menadžment sistema zaštite informacija, uvodi se metrički sistem performansi procesa na bazi brojnih kriterijuma, kao što su:

- broj incidenata koji izazivaju probleme kritične za poslovanje,
- broj novih implementacija koje kasne zbog bezbednosnih razloga,
- broj kritičnih poslova koji se oslanjaju na IKT sistem sa planom za kontinuitet poslovanja,
- broj kritičnih objekata infrastrukture IKT sistema sa automatskim nadzorom,
- nivo svesti zaposlenih o etičkim principima i principima zaštite,
- broj potpuno usaglašenih ili dopuštenih odstupanja od bezbednosnih zahteva,
- procenat razvijenih i dokumentovanih planova i politika zaštite,
- procenat planova i politika zaštite sa kojima su upoznati svi zaposleni itd.

Kako standard ISO/IEC 17799:2005 ne nudi nikakvu metriku za merenje performansi procesa menadžment sistema zaštite informacija, može se uspešno koristiti SSE-CMM model, specifično primenjen na ove procese [9]. Skala nivoa sazrevanja procesa menadžment sistema zaštite informacija ima sledeće glavne karakteristike:

0. **nivo**: *ne postoji* — menadžment proces uopšte nije primenjen,
1. **nivo**: *inicijalni proces* — menadžment procesi su *ad hoc* i neregularni,
2. **nivo**: *ponovljiv* — menadžment procesi su planirani, ponovljivi i slede regularni obrazac,
3. **nivo**: *definisan* — menadžment procesi su dokumentovani i upoznata je cela organizacija,
4. **nivo**: *kvantitativno upravljan* — procesi su kvantitativno kontrolisani i mereni,
5. **nivo**: *optimizovan* — primenjena najbolja praksa menadžment sistema zaštite informacija.

Izlazni rezultati kvalitetnog ISMS procesa obezbeđuju brojne prednosti kao što su**:**

- *strategijsko usaglašavanje***:** bezbednosni zahtevi definišu se prema poslovnim zahtevima organizacije, rešenja sistema zaštite uklapaju se u procese organizacije, investiranje u zaštitu usaglašeno sa strategijom razvoja i prihvaćeno na bazi procene rizika;
- *dodavanje nove vrednosti***:** standardan set praksi zaštite je usaglašen sa najboljom praksom zaštite, propisno su određeni prioriteti i distribuiran rad na oblasti koje imaju najveći uticaj i daju najveće poslovne rezultate; rešenja zaštite su kompletna, primenjena i prihvaćena u celoj organizaciji; neprekidno se poboljšava kultura zaštite;
- *upravljanje rizikom:* prihvaćen je i usaglašen profil rizika organizacije; visok je nivo razumevanja o izloženosti riziku i svesti o prioritetima menadžmenta rizika;
- *merenje performansi procesa:* definisan je set metrika; proces merenja sa povratnom spregom za progresivno poboljšanje, obezbeđuje nezavisnu bezbednosnu garanciju.

U pripremi i implementaciji efektivnog procesa ISMS-a, projektanti moraju razmatrati i obezbedi odgovore menadžerske strukture na brojna pitanja, kao što su:

1. Pitanja za glavne menadžere:
   - Da li su informacije i zaštita informacija kritični za organizaciju? Ako jesu, da li menadžment shvata kritičnost zaštite informacija?
   - Da li je menadžment izdao dokument *Politika zaštite informacija?* Ako jeste, da li se *Politika zaštite* stalno ažurira? Ako ne, zašto?
   - Koja su tri kritična objekta informacione imovine organizacije? Koliko poverenje ima menadžment u raspoloživost, integritet i poverljivost ovih objekata?
   - Da li menadžment zna gde je najranjiviji IKT sistem organizacije?
   - Da li organizacija može nastaviti poslovanje, ako su kritični IKT sistemi nisu raspoloživi?
   - Kakve bi bile posledice gubitka zarade i klijenata ili poverenja investitora?
   - Kakve bi posledice bile ako bi IKT infrastruktura bile neoperativna?
   - Koji su informacioni objekti obuhvaćeni zakonima i regulativama?
   - Koje je institucionalne mere menadžment preduzeo da obezbedi usklađenost informacionih objekata sa zakonima i regulativama?
   - Da li *Politika zaštite informacija* obuhvata uloge i odgovornosti menadžerske strukture, pokriva identifikovane rizike, uspostavlja infrastrukturu za tretman rizika i odgovarajući nadzor i procedure za povratne informacije?
   - Da li je organizacija ikada imala nezavisnu bezbednosnu proveru svog IKT sistema?
   - Da li je organizacija obezbedila obuku i razvoj svesti o potrebi zaštite svim korisnicima?
   - Da li je menadžment uveren da je zaštita IKT sistema adekvatna u organizaciji?
2. Pitanja za izvršne menadžere:
   - Kako se menadžerska struktura informiše o stanju sistema zaštite? Kada je poslednji put menadžment informisan o bezbednosnim rizicima i stanju sistema zaštite?
   - Kada je poslednji put izvršena procena rizika kritičnih objekata? Kada je planirana sledeća procena rizika?
   - Da li procena rizika uključuje kontinuitet poslovanja ako kritični servisi nisu raspoloživi? Da li procena pokriva posledice bezbednosnih incidenata — gubitak zarade, klijenata i poverenja investitora i neoperativnosti IKT infrastrukture?
   - Da li procena rizika razmatra koji su informacioni objekti pokriveni zakonima i regulativama? Da li su izrađene adekvatne procedure koje obezbeđuju usaglašenost?
   - Da li je procena rizika regularni dnevni red na sastancima menadžmenta IKT sistema i da li menadžment pokreće inicijative za poboljšanje?
   - Kako se organizacija postavlja u odnosu na praksu zaštite drugih organizacija? Kakva je najbolja praksa zaštite u organizaciji i kako se organizacija upoređuje sa drugima?
   - Kada je poslednja izjava (saopštenje) politike zaštite izdata u organizaciji?

- Da li politika zaštite adekvatno obuhvata zaštitu kritičnih IKT sistema, značaj zaštite za menadžment, procenu rizika, kontrole zaštite za ublažavanje rizika, nadzor i procedure?
- Kada je specijalista zaštite izvršio poslednji put proveru performansi sistema zaštite?
- Da li je adekvatan proces informisanja uprave o zaštiti?
- Kakve su mere zaštite od virusa i malicioznih napada na RS povezanim na Internet?
- Da li su sistemi aktivno monitorisani i da li se redovno izveštava uprava o rezultatima?
- Kako je organizovan, da li je adekvatan i da li su obuhvaćeni svi zaposleni u programu razvoja svesti o potrebi zaštite, uzimajući u obzir procenjene faktore rizika?
- Koje su mere fizičke zaštite primenjene za zaštitu IKT sistema i da li su adekvatne?
- Kada je poslednji put vršena nezavisna provera (*audit)* sistema?
- Da li menadžment prati preporuke proverivača (*auditor*-a)?
- Da li postoji izrađen *program zaštite* koji pokriva sva gore pomenuta pitanja?
- Da li su jasno određene kontrolisane odgovornosti za izvršavanje programa?

Osnovne faze koje menadžment treba izvršiti da bi obezbedio implementaciju efektivnog ISMS menadžment sistema zaštite informacija su:

1. Usvajanje standarda najbolje prakse zaštite

a. Na nivou glavnog menadžera:

- uspostaviti vlasništvo nad informacijama i odgovornosti izvršnih menadžera,
- formirati *Komitet za proveru* (*auditing)* koji potpuno shvata svoju ulogu,
- obezbediti da interni i eksterni *proveravači* usaglašavaju način zaštite informacija u toku provere sa komitetom za *proveru* i menadžerima,
- zahtevati da menadžer zaštite izveštava *Komitet za proveru* o progresu,
- razviti praksu uključivanja menadžera u upravljanje vanrednim događajem, na osnovu usaglašenog plana i
- uspostaviti bezbednosne funkcije koje pomažu menadžmentu u razvoju i sprovođenju politike zaštite u organizaciji.

b. Na nivou izvršnih menadžera:

- formirati merljivu i, za menadžment, transparentnu strategiju zaštite na bazi *benčmarkinga*, modela sazrevanja procesa, *gap* analize i neprekidnog izveštavanja,
- voditi sastanke za godišnju analizu rizika, pripremljenu od strane specijalista za zaštitu i *proverivača*, koji treba da rezultiraju sa akcionim planom,
- razviti scenario "*šta ako*" o bezbednosnom riziku, koristeći znanja specijalista,
- uspostaviti jasne i tehnološki kontinuirane, testirane i ažurirane programe,
- sistem zaštite *proveravati* na bazi jasnih procesa i odgovornosti *proverivača*,
- razviti jasnu politiku i detaljna uputstva za zaštitu i prezentirati ih svim zaposlenim,
- konstantno procenjivati ranjivosti kroz monitoring, testiranje na upad i proveru plana upravljanja vanrednim događajem,

- učiniti poslovne procese i IKT sistem za podršku, otpornim na određene greške,
- uspostaviti sistem osnovne zaštite i striktno monitorisati usaglašenost,
- instalirati anti-maliciozne programe i često testirati sisteme na upad,
- povećati zaštitu svih kritičnih servera i platformi, primenjujući jaku autentifikaciju,
- pristup korisnika IKT sistemu zasnivati na bazi uloga i odgovornosti i usaglašavati metod autentifikacije sa poslovnim rizikom i
- uključiti zaštitu u poboljšanje poslovanja i primeniti stimulativne mere i sankcije.

2. Razmatranje kritičnih faktora uspeha

Ova aktivnosti treba da obezbedi:

- razumevanje da je razvoj dobrog programa zaštite vremenski zahtevan,
- odgovornost menadžera zaštite za izvršavanje programa i izveštavanje glavnog menadžera o bezbednosnim funkcijama organizacije,
- jedinstveno shvatanje menadžmenta i zaposlenih o značaju, zahtevima, ranjivostima, pretnjama, da razumeju i prihvataju svoje odgovornosti u zaštiti,
- nezavisnu periodičnu evaluaciju i proveru politike i arhitekture sistema zaštite,
- menadžeru zaštite kapacitete za administriranje, monitoring, testiranje na upad, detekciju, zapise i analizu *log* događaja, izveštavanje i reagovanje na incidente,
- jasno definisane uloge i odgovornosti za menadžment rizika i zaštitu,
- uspostavljanje politike koja definiše granice i prihvatljivost rizika,
- definisane, usaglašene i finansirane odgovornosti i procedure za poboljšanje menadžmenta rizika,
- nezavisnu proveru strategije zaštite, da bi se obezbedila objektivnost i ponovljivost,
- identifikaciju i neprekidno monitorisanje kritične komponente infrastrukture,
- primenu SLA sporazuma za razvoj svesti o značaju zaštite, kooperativnost snabdevača i kontinuiteta poslovanja,
- razmatranje i odluku o nametanju politike zaštite u vreme njenog razvoja,
- implementaciju procesa provere svesti, razumevanja i usaglašenosti prakse zaštite sa politikom,
- dobru zaštitu svih aplikacija pre i u toku razvoja,
- usaglašenost *politike zaštite informacija* sa opštim strateškim planovima,
- angažovanje menadžmenta u zaštiti i kontroli politike zaštite, potpune komunikacije, razumevanja i usaglašenosti,
- konzistentnu aplikaciju SMF okvira za razvoj, formulisanje, uspostavljanje, razumevanje i usaglašenost politike zaštite,
- svest da su, napadi organizovanog kriminala i drugih autsajdera u porastu, iako insajderi ostaju primarni izvori bezbednosnih pretnji,
- dužnu pažnju zaštiti privatnosti i poverljivosti podataka, autorskih i drugih prava koja se odnose na podatke,
- podršku menadžmenta da zaposleni izvršavaju svoja prava i dužnosti na etički i bezbedan način i
- lični primer i istinsko lidersko ponašanje menadžmenta sistema zaštite.

3. Uvođenje metrike i sistema merenja performansi zaštite

a. Metrike za određivanje efektivnosti sistema zaštite [69, 95, 106]:

- broj incidenata koji izazivaju javnu kompromitaciju organizacije,
- broj novih implementacija koje kasne zbog bezbednosnih razloga,
- broj kritičnih poslovnih procesa koji se oslanjaju na IKT sistem koji ima adekvatan BCP,
- broj komponenti kritične infrastrukture sa automatskim monitoringom raspoloživosti,
- stepen razvoja svesti zaposlenih o etičkom ponašanju u izradi bezbednosnih zahteva, primeni principa zaštite i izvršavanju dužnosti na etički i bezbedan način,
- potpuna usaglašenost ili odobrena odstupanja od minimalnih bezbednosnih zahteva i
- procenat planova i politika zaštite sa kojima su upoznati svi učesnici itd.

5.5 REZIME

Savremeni sistem zaštite odnosi se na informacionu imovinu (čistu, hardversku i humanu) sa težištem na zaštitu CIA informacija. U standardima zaštite (ISO, NIST, BSI...) na menadžment sisteme odnose se *upravljačke i organizacione* (tzv. *proceduralne*) kontrole zaštite, a *GAISP principi* čine osnovni skup principa za menadžment sistem zaštite, u kojem sve uloge i odgovornosti moraju biti definisane i dodeljene svim zaposlenima.

Generički proces menadžment sistema IKT, zasnovan na objektno orijentisanom pristupu, uključuje *informacione*, *funkcionalne, komunikacione* i *organizacione* aspekte, sa manuelnim, poluatomatskim i automatskim tehnikama. Dobar pristup za uspostavljanje menadžment sistema zaštite informacija, obezbeđuju standardi *IEC/ISO 27001* (ISMS) sa preporučenim kontrolama zaštite (ISO/IEC 27002). Glavni ciljevi standarda su uspostavljanje i implementacije programa zaštite, selekcija i izbor resursa i *kontrola zaštite*. Osnovna komponenta programa zaštite je *politika zaštite* na bazi analize rizika. Za određivanje efektivnosti i efikasnosti ISMS-a, uvode se metrike performansi procesa na bazi brojnih kriterijuma, uključujući metriku modela progresivnog sazrevanja procesa zaštite (*SSE CMM)*, specifično sa skalom od pet nivoa zrelosti.

U pripremi i implementaciji efektivnog procesa ISMS-a moraju se obezbediti odgovori menadžmenta na brojna pitanja. U procesu uspostavljanja ISMS-a osnovni zadaci menadžmenta organizacije su izbor i usvajanje standarda zaštite, analiza kritičnih faktora uspeha i uvođenje metrika performansi zaštite. Efektivan ISMS, implementiran na bazi ISO/IEC 27001/2 i uputstva za razvoj i implementaciju ISMS-a na bazi PDCA modela procesa. Standard ISO/IEC 27001 obezbeđuje smernice za kreiranje menadžment sistema za zaštitu informacija (ISMS) i referentnu listu kontrola zaštite iz ISO/IEC 27002, za uspostavljanje i održavanje ISMS-a. Za specifičnu organizaciju dobra polazna tačka u implementaciji ISMS-a je razvoj SMF *okvira*, koji obezbeđuje bolje razumevanje načina upotrebe termina, koncepata, uzoraka, alata za analizu i izveštavanje itd., u razvoju i održavanju ISMS-a, kao i povratak investicije i smernice za razvoj ISMS-a, usaglašenog sa TQM sistemom organizacije.

Brojni ISO standardi koriste PDCA model procesa, što obezbeđuje komplementarnost i integraciju u TQM više ISO standarda menadžment sistema. PDCA model sadrži faze planiranja, implementacije, održavanja i provere i poboljšavanja procesa ISMS.

Za uspostavljanje ISMS-a i razumevanje ISO terminologije mogu se koristiti i drugi pristupi, kao što je koncept *tranzicije bezbednosnog stanja* za procenu rizika, koji uključuje faze stanje kakvo treba da bude (*to-be state*),stanje kakvo jeste (*as-is state*), plan tranzicije (*transition plan*) iz jednog u drugo bezbednosno stanje i operativni rad i održavanje.

5.6 PITANJA ZA PONAVLJANJE

1. Menadžment reaktivnog sistema zaštite se približno može predstaviti sa:
   a. menadžmentom web aplikacija
   b. menadžmentom računarskih mreža OSI modela
   c. menadžmentom rizika u IKT sistemu
   d. menadžmentom IKT sistema.
2. Termin *informaciona imovina* obuhvata:
   a. imovinu računarskog sistema i računarske mreže
   b. čistu informacionu imovinu, hardversku i humanu imovinu organizacije
   c. informacije u pisanom i elektronskom obliku i računarske programe
   d. informacije u elektronskom i pisanom obliku i dokumentaciju organizacije.
3. U OO pristupu sistem zaštite informacija štiti sledeći set atributa:
   a. poverljivost, integritet i autentičnost
   b. poverljivost, integritet i raspoloživost
   c. raspoloživost, integritet i neporecivost
   d. poverljivost, neporecivost i autentičnost.
4. Osnovni skup konzistentnih principa za menadžment sistem zaštite čine:
   a. NIST principi menadžmenta rizika
   b. opšte prihvaćeni principi zaštite informacija (GAISP)
   c. OECD principi zaštite informacija
   d. ISO principi zaštite informacija.
5. Uloge i odgovornosti u zaštiti informacija:
   a. definiše organizacija samo u slučaju kompjuterskog incidenta i kriminala
   b. definiše organizacija kao za sve poslovne procese
   c. nisu značajne za proaktivno delovanje u zaštiti
   d. od presudnog su značaja za proaktivno delovanje u zaštiti.
6. Generički procesi menadžmenta IKT sistema uključuju:
   a. informacione, komunikacione i organizacione menadžment procese
   b. informacione, funkcionalne i organizacione menadžment procese
   c. informacione, funkcionalne, komunikacione i organizacione procese
   d. informacione, komunikacione i organizacione menadžment procese.
7. Generički proces ISMS-a u osnovi sadrži sledeći set koraka:
   a. procenu rizika, uspostavljanje politike zaštite i implementaciju kontrola
   b. procenu ranjivosti, uspostavljanje politike i implementaciju kontrola zaštite
   c. identifikovanje pretnji i ranjivosti, procenu rizika, uspostavljanje politike zaštite i implementaciju kontrola zaštite
   d. procenu rizika, procenu imovine, uspostavljanje politike zaštite i implementaciju kontrola zaštite.

8. Dobru metriku performansi procesa ISMS-a nude standardi:
   a. ISO/IEC 17799:2000
   b. ISO/IEC 27001:2005
   c. ISO/IEC 21827:2002
   d. ISO/IEC 13355:2004.
9. Metodologija za implementaciju ISMS-a zasniva se na:
   a. IDEAL procesnom pristupu
   b. *šest sigma* procesnom pristupu
   c. PDCA procesnom pristupu
   d. pristupu *odozdo nagore*
   e. pristupu *odozgo nadole.*
10. Standard ISO/IEC 27001 obezbeđuje:
    a. katalog *kontrola zaštite* za efektivnost ISMS-a i tretman rizika
    b. uputstvo za implementaciju ISMS-a
    c. smernice za implementaciju ISMS-a primenom PDCA procesnog pristupa
    d. metodologiju menadžmenta rizika.
11. Standard ISO/IEC 27005 obezbeđuje:
    a. katalog *kontrola zaštite* za efektivnost ISMS-a i tretman rizika
    b. uputstvo za implementaciju ISMS-a
    c. smernice za implementaciju ISMS-a primenom PDCA procesnog pristupa
    d. metodologiju menadžmenta rizika.
12. Standard ISO/IEC 27002 obezbeđuje:
    a. katalog *kontrola zaštite* za efektivnost ISMS-a i tretman rizika
    b. uputstvo za implementaciju ISMS-a
    c. smernice za implementaciju ISMS-a primenom PDCA procesnog pristupa
    d. metodologiju menadžmenta rizika.
13. Standard ISO definiše ISMS kao:
    a. specifičan menadžment sistem zaštite informacija
    b. deo menadžment sistema totalnog kvaliteta (TQM) organizacije
    c. deo menadžment sistema IKT
    d. deo menadžment sistema kvaliteta (familije ISO/IEC 9000).
14. Okvir menadžment sistema zaštite informacija (SMF) obezbeđuje:
    a. definisanje svih bezbednosnih pitanja organizacije
    b. nacrte za definisanje diskusija, planova, implementacije, praćenja i izveštavanja
    c. politiku zaštite, plan upravljanja vanrednim događajem, plan tretmana rizika
    d. termine, koncepte, uzorke, alate za analizu i izveštavanje.
15. Standard ISO/IEC 27002 predstavlja:
    a. menadžment sistem bezbednosti informacione imovine
    b. uputstvo za sertifikaciju i akreditaciju
    c. uputstvo za primenu i katalog kontrola zaštite
    d. uputstvo za internu proveru sistema zaštite organizacije.
16. *Kontrole zaštite* kombinuju sledeće funkcije zaštite, za:
    a. odvraćanje, detekciju i zaštitu
    b. izbegavanje, zaštitu i reagovanje na incident
    c. odvraćanje, izbegavanje, zaštitu i reagovanje na incident
    d. izbegavanje, identifikaciju, zaštitu i neporecivost.
17. Najvažniji, zajednički, integracioni faktor ISO menadžment sistema je:
    a. terminologija, uzorci i obrasci
    b. PDCA procesni pristup
    c. metodologija dokumentacija
    d. definisane uloge i odgovornosti
    e. obuka i interna provera.
18. Proces procene rizika vrši se u PDCA fazi:
    a. implementacije
    b. provere
    c. planiranja
    d. poboljšanja.
19. Za uspostavljanje ISMS standarda:
    a. mogu se koristiti i drugi pristupi
    b. ne mogu se koristiti i drugi pristupi
    c. ne može se koristiti koncept tranzicije bezbednosnog stanja
    d. može se koristiti PDCA procesni pristup.

20. Standard ISO/IEC 27001 klasifikuje informacionu imovinu u:
    a. informacije, podatke, hardver, softver, mrežna infrastruktura
    b. može se koristiti model brzog odgovora
    c. informacije, računarske sisteme, računarske mreže, korisnike (ljude)
    d. čistu informacionu imovinu, fizičku imovinu, humanu imovinu.

UNIVERZITET AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM



6. MENADŽMENT SISTEM ZAŠTITE INFORMACIJA (ISMS)

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Model i procese uspostavljanja menadžment sistema zaštite informacija (ISMS-a)
- ☑ Primenu principa (OECD, Gaisp) i modela PDCA procesa u ISMS standardu
- ☑ Strukturu i zahteve (metodološke i za kontrole zaštite) ISMS standarda
- ☑ Značaj definisanja uloga, odgovornost, obima i granica ISMS-a
- ☑ Komplementarnosti ISO/IEC menadžment sistema
- ☑ Neke otvorene probleme i preporuke za ISMS

6.1 UVOD

Menadžment sistem zaštite informacija — ISMS (*Information Security Management System*) je sistem za uspostavljanje, kontrolu rada, poboljšanje i kontinualno obezbeđivanje odgovarajuće zaštite za informacionu imovinu. Za uspostavljanje ISMS-a značajni su tehnologija i dokumentacija, ali su kritični elementi — upravljivi procesi planiranja i rada, usaglašeni sa dokumentovanim procedurama, odlukama i akcijama. ISMS zavisi od dobro osposobljenih i svesnih ljudi, koji su najveća snaga, ali, bez tehnologije, i najveća ranjivost sistema.

Postojeći sistemi zaštite u većini organizacija, uglavnom su razvijani metodom *odozdo nagore*, što reflektuje taktičke odluke, individualna rešenja zaštite i pretežnu *ad hoc* primenu tehnologija. Godinama agregirane tehnologije zaštite i druga *ad hoc* rešenja, onemogućili su izgradnju koherentnog sistema zaštite sa svojstvima za brze odgovore na kompjuterski incident. Ovakva rešenja zaštite nisu se mogla nazvati *sistemom zaštite*. Generalno, taktička rešenja zaštite moguće je konvertovati u efektivan ISMS, samo uspostavljanjem sistemskih procedura usaglašenih sa poslovnim potrebama i neprihvatljivim rizikom, a zatim, poboljšavanjem ISMS-a i postepenim razvojem ciljne arhitekture sistema zaštite.

Kako je ISMS samo jedan aspekt IKT sistema, u većini zakonodavstava i nacionalnih standarda, generalni menadžer je odgovoran za bezbednost informacija po principu da mora *osigurati dobre performanse IKT sistema, kad i gde god se to zahteva,* kao i usaglasiti program sa regulatornim zahtevima. Menadžment promena poslovanja, pretnji i ranjivosti, obezbeđuje se neprekidnim razvojem ISMS-a, primenom PDCA modela procesa.

6.2 USPOSTAVLJANJE MENADŽMENT SISTEMA ZAŠTITE INFORMACIJA

6.2.1 Principi i model menadžment sistema zaštite informacija

Fundamentalnu osnovu za uspostavljanje ISMS sistema čine principi zaštite. Organizacija OECD[1] je uspostavila devet sledećih principa za zaštitu IKT sistema i mreža sa ciljem promovisanja kulture zaštite svih učenika:

1. *svest o potrebi zaštite*: učesnici treba da budu svesni potrebe zaštite IKT sistema i mreža i šta mogu uraditi da poboljšaju bezbednost;
2. *odgovornost:* učesnici su odgovorni za bezbednost IKT sistema i mreža;
3. *blagovremeni odgovor:* svi učesnici treba da reaguju blagovremeno i kooperativno da spreče, detektuju i odgovore na kompjuterski incident;
4. *etičnost:* učesnici treba da poštuju legitimne interese drugih;
5. *demokratičnost:* bezbednost IKT sistema i mreža mora biti kompatibilna sa bitnim vrednostima demokratskog društva;
6. *procena rizika:* učesnici treba da vrše procenu rizika;
7. *arhitektura i implementacija sistema zaštite:* učesnici treba da implementiraju sistem zaštite, kao bitan elemenat IKT sistema i mreža;
8. *menadžment sistema zaštite:* učesnici treba da usvoje sveobuhvatan pristup menadžment sistemu zaštite;
9. *preispitivanje:* učesnici treba da revidiraju i ponovo procenjuju bezbednost IKT sistema i mreža i izvrše odgovarajuće modifikacije politike, procedura, metrika i prakse zaštite.

Ovi principi se primenjuju na svaku politiku i operativni nivo menadžmenta sistema zaštite informacija i mreža. Standard ISMS, korišćenjem PDCA modela i procesa sekcija **četiri** do **osam** standarda, obezbeđuje okvir i metodologiju menadžment sistema zaštite informacija za implementaciju OECD principa. U tabeli 6.1 prikazana je komplementarnost OECD principa i ISMS procesa i faza PDCA modela.

1 Engl.: ***O****rganisation for* ***E****conomic* ***C****o-operation i* ***D****evelopment*) *Guidelines for the Security of Information Systems i Networks.*

Tabela 6.1 *Komplementarnost OECD principa i PDCA modela*

OECD principi	Korespondirajući ISMS proces i PDCA faza
Svest – učesnici treba da su svesni potrebe za zaštitom IKT sistema i mreža i sopstvenog angažovanja za poboljšavanje zaštite.	Ova aktivnost je deo faze ***Do*** (videti 4.2.2 i 5.2.2).
Odgovornost – svi učesnici su odgovorni za bezbednost informacionih sistema i mreža.	Ova aktivnost je deo faze ***Do*** (videti 4.2.2 i 5.1).
Reagovanje – učesnici sarađuju u prevenciji, detekciji i pravovremeno na bezbednosne incidente.	Reagovanje je deo aktivnosti monitoringa faze ***Check*** (videti 4.2.3 i 6 do 7.3) i aktivnosti reagovanja iz faze ***Act*** (videti 4.2.4 i 8.1 do 8.3). Takođe, može da se uključi u neke aspekte faza ***Plan*** *i* ***Check***.
Procena rizika – učesnici sprovode procenu rizika.	Ova aktivnost je deo faze ***Plan*** (videti 4.2.1) i a ponovna procena rizika je deo faze ***Check*** (videti 4.2.3 i 6 do 7.3).
Dizajn i implementacija zaštite – učesnici ugrađuju zaštitu kao ključni element IKT sistema i mreža.	Nakon kompletiranja procene rizika biraju se kontrole za tretiranje rizika, kao deo faze ***Plan*** (videti 4.2.1). Potom, faza ***Do*** (videti 4.2.2 i 5.2) pokriva implementaciju i operativno korišćenje tih kontrola.
Menadžment zaštite – učesnici usvajaju sveobuhvatan pristup menadžmentu zaštite.	Upravljanje rizikom je proces koji uključuje prevenciju, detekciju i reagovanje na incidente, tekuće održavanje i proveru (*audit*). Svi ovi aspekti sadržani su u fazama ***Plan***, ***Do***, ***Check*** *i* ***Act***.
Ponovna procena – učesnici sprovode reviziju i ponovo procenjuju zaštitu IKT sistema i mreža, kao i odgovarajuće modifikacije politike, prakse, metrika i procedura zaštite.	Ponovljena procena zaštite informacija je deo faze ***Check*** (videti 4.2.3 i 6 do 7.3) gde se sprovode redovne revizije za proveru efektivnosti ISMS menadžment sistema zaštite informacija, a poboljšanja zaštite u fazi ***Act*** (videti 4.2.4 i 8.1 do 8.3).

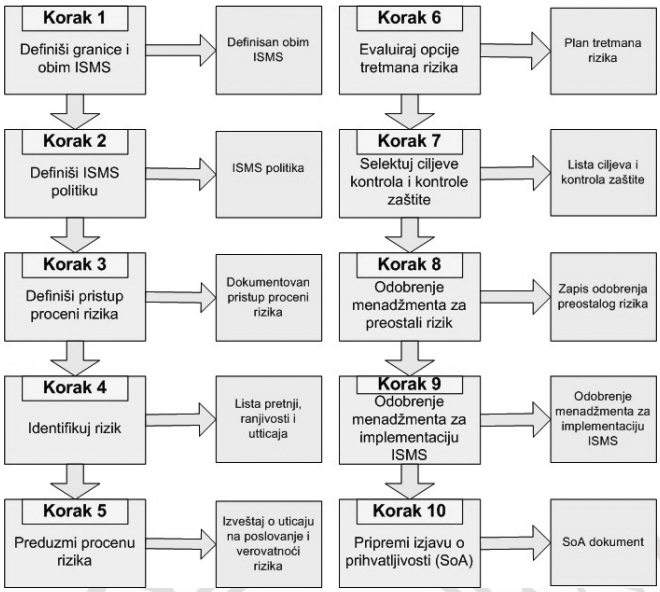
Na bazi OECD i NIST principa zaštite generisani su opšte prihvaćeni principi zaštite – GAISP (*Generally Accepted Information Security Principless*) (tabela 6.2) [30].

Tabela 6.2 *Opšte prihvaćeni (GAISP) principi zaštite*

GAISP princip	Opis
Svesti o potrebi zaštite	Svi relevantni učesnici treba da budu svesni primenljivih pretnji za bezbednost IKTS i tehnologija zaštite informacija.
Odgovornosti	Ovlašćenja i odgovornosti moraju u sistemu zaštite biti jasno definisani, shvaćeni, prihvaćeni i kontrolisani.
Stalnog preispitivanja	Rizik za informacionu imovinu mora se regularno periodično procenjivati, a procesi zaštite neprekidno unapređivati.
Demokratičnosti	U procesima zaštite treba jednako uvažavati privatnost, lična i autorska prava i dostojanstvo svih učesnika.
Etičkog ponašanja	Informacije koje se štite treba da budu etički prihvatljive, a administriranje zaštite u skladu sa opštim kodeksom ponašanja.
Integracije	Principi, standardi i mehanizmi treba da budu komplementarni i sinergijski integrisani u politiku, procedure i kontrole zaštite.
Multidisciplinarnosti	Principi, standardi i mehanizmi zaštite treba da sveobuhvatno uključuju sve relevantne aspekte različitih disciplina.
Proporcionalnosti	Kontrole zaštite treba projektovati, implementirati i primenjivati za zaštitu informacija, proporcionalno proceni rizika.
Blagovremenosti	Sve komponente zaštite treba da blagovremeno sprečavaju napade na IS.

Model za uspostavljanje, implementaciju, primenu, monitoring, proveru, održavanje i poboljšavanje menadžment sistema zaštite informacija, obezbeđuje standard ISO/IEC 27001 koji definiše ISMS kao *"menadžment sistem koji uključuje organizacionu strukturu, politiku, procedure, planiranje, odgovornosti, procese, praksu i resurse"* [56]. Usvajanje ISMS-a predstavlja strateški cilj organizacije, a projektovanje i implementacija ISMS-a zavise od njenih poslovnih potreba, ciljeva i procesa, bezbednosnih zahteva, veličine i složenosti organizacije. Naime, podrazumeva se da će ISMS i podsistemi koji ga podržavaju, tokom vremena doživeti određene *izmene*. Nivo implementacije ISMS-a se *usklađuje* prema potrebama organizacije, npr. manje složene organizacije zahtevaju jednostavnije rešenje ISMS-a. Standard se, takođe, može koristi za internu i eksternu *procenu usaglašenosti*. U svetu trenutno postoji jedanaest akreditovanih entiteta za nezavisnu ISMS sertifikaciju. Opšte zahteve za sertifikaciona tela definiše dokument *ISO/IEC Guide 62*.

Uvođenje ovog standarda omogućava da organizacija usaglasi ili integriše svoj ISMS sa zahtevima postojećeg menadžment sistema organizacije. Takođe, ISMS standard ne zahteva implementaciju svih odredbi, a za korektnost njegove primene odgovorni su sami korisnici. Usaglašavanje sa ISO/IEC standardima ne oslobađa organizacije od zakonskih odgovornosti. Na slici 6.1 prikazan je tok procesa uspostavljanja ISMS-a sa koracima i izlaznim rezultatima svakog koraka [45].



Slika 6.1 Tok procesa uspostavljanja ISMS-a

Da bi se podržala *konzistentnost i integracija* TQM sistema organizacije, ISMS je usaglašen sa ISO/IEC 9001:2000 i ISO/IEC 14001:2004 (tabela 6.3), što znači da se izborom jednog menadžment sistema može odgovoriti zahtevima ostalih standarda.

Tabela 6.3 Komplementarnost ISO 9001:2000, ISO 14001:2004 i ISO/IEC 27001:2005

ISO/IEC 27001:2005	ISO/IEC 9001:2000	ISO/IEC 14001:2004
0 Uvod 0.1 Opšte napomene 0.2 Procesni pristup 0.3 Kompatibilnost sa drugim menadžment sistemima	**0 Uvod** 0.1 Opšte napomene 0.2 Procesni pristup 0.3 Veza sa ISO 9004 0.4 Kompatibilnost sa drugim menadžment sistemima	**Uvod**
1 Oblast primene 1.1 Opšte napomene 1.2 Primena	**1 Oblast primene** 1.1 Opšte napomene 1.2 Primena	**1 Oblast primene**
2 Normativne reference	**2 Normativne reference**	**2 Normativne reference**
3 Termini i definicije	**3 Termini i definicije**	**3 Termini i definicije**

ISO/IEC 27001:2005	ISO/IEC 9001:2000	ISO/IEC 14001:2004
4 Menadžment sistem zaštite informacija 4.1 Opšti zahtevi 4.2 Uspostavljanje i rad ISMS 4.2.1 Uspostavljanje ISMS 4.2.2 Implementacija i rad ISMS 4.2.3 Monitoring i revizija ISMS 4.2.4 Održavanje i poboljšavanje	**4 Menadžment sistem kvaliteta** 4.1 Opšti zahtevi 8.2.3 Monitoring i merenja procesa 8.2.4 Monitoring i merenja proizvoda	**4 EMS zahtevi** 4.1 Opšti zahtevi 4.4 Implementacija i operativni rad 4.5.1 Monitoring i merenja
4.3 Zahtevi za dokumentaciju 4.3.1 Opšte 4.3.2 Kontrola dokumentacije 4.3.3 Kontrola zapisa	4.2 **Zahtevi za dokumentaciju** 4.2.1 Opšte 4.2.2 Priručnik kvaliteta 4.2.3 Kontrola dokumenata 4.2.4 Kontrola zapisa	4.4.5 Kontrola dokumentacije 4.5.4 Kontrola zapisa
5 Odgovornosti menadžmenta 5.1 Angažovanje menadžmenta	**5 Odgovornosti menadžmenta** 5.1 Angažovanje menadžera 5.2 Fokus kupca 5.3 Politika sistema kvaliteta 5.4 Planiranje 5.5 Odgovornost, ovlašćenja i komunikacija	4.2 Politika zaštite okruženja (*Environmental policy*) 4.3 Planiranje
5.2 Menadžment resursa 5.2.1 Obezbeđivanje resursa 5.2.2 Obuka, svest i stručnost	**6 Menadžment resursa** 6.1 Obezbeđivanje resursa 6.2 Humani resursi 6.2.2 Kompetencije, savest i obuka 6.3 Infrastruktura 6.4 Radno okruženje	4.4.2 Kompetencije, savest i obuka
6 Interna provera ISMS-a	8.2.2 Interna provera	4.5.5 Interna provera
7 Menadžerska revizija ISMS-a 7.1 Opšte 7.2 Ulazi revizije 7.3 Izlazi revizije	**5.6 Menadžerska revizija ISMS**-a 5.6.1 Opšte 5.6.2 Ulazi revizije 5.6.3 Izlazi revizije	**4.6 Menadžerska revizija ISMS**-a
8 Poboljšanje ISMS-a 8.1 Kontinualno poboljšanje	**8.5 Poboljšanje** 8.5.1 Kontinualno poboljšanje	
8.2 Korektivne akcije	8.5.3 Korektivne akcije	4.5.3 Korektivne akcije neusaglašenosti i preventivne akcije
8.3 Preventivne akcije	8.5.3 Preventivne akcije	
Annex A Ciljevi kontrola i kontrole **Annex B** OECD principi i ISMS Međunarodni Standard **Annex C** Korespodencija između ISO 9001:2000, ISO 14001:2004 i ISMS	**Annex A** Veza između ISO 9001:2000 i ISO 14001:1996	**Annex A** Smernice za korišćenje međunarodnog standarda **Annex B** Veza između ISO 14001:2004 i ISO 9001:2000

Da bi obezbedila efektivan rad, svaka organizacija ima potrebu da identifikuje i upravlja raznim aktivnostima i procesima.

6.2.2 Procesni pristup u ISMS standardu

Procesni pristup je primena sistema procesa u organizaciji, koji svojom međusobnom interakcijom identifikuju druge procese i njihovo upravljanje. Standard ISO/IEC 27001 primenjuje *procesni pristup* za uspostavljanje, implementaciju, operativni rad, monitoring, proveru, održavanje i poboljšavanje ISMS-a. *Procesni pristup menadžment sistemu zaštite informacija* u ISMS standardu ističe značaj:

- razumevanja *bezbednosnih zahteva* organizacije i potrebe za uspostavljanjem politike i ciljeva zaštite informacija,
- implementacije i primene kontrola zaštite za *menadžment ukupnog poslovnog rizika* organizacije,
- *monitoringa i provere* efektivnosti ISMS-a i
- *kontinualnog poboljšavanja,* na bazi objektivnih mernih rezultata.

Standard ISO/IEC 27001 primenjuje PDCA model na sve ISMS procese (slika 6.2), koji obezbeđuje robustan model za implementaciju *OECD principa upravljanja zaštitom IKT sistema i mreža,* kao i smernice za procenu rizika, projektovanje i implementaciju kontrola zaštite, menadžment i regularnu proveru sistema zaštite. PDCA model ISMS-a transformiše ulazne bezbednosne zahteve i očekivanja u izlaze koji zadovoljavaju te zahteve i očekivanja, putem međusobno povezanih akcija i procesa (*zahtevi* 4 do 8 *Standarda*).



Slika 6.2 PDCA model ISMS procesa

Primer 1 – *Bezbednosni zahtev* može biti da narušavanje bezbednosti informacija ne izazove ozbiljnije finansijske posledice i/ili gubitak ugleda i poverenja.
Primer 2 – *Očekivanje* može biti da postoje obučeni ljudi koji su u stanju da odgovore na ozbiljne bezbednosne incidente, na primer, hakerski napad na *web* sajt za e-poslovanje.

U tabeli 6.4 mapirane su faze PDCA procesnog pristupa i ISMS standarda

Tabela 6.4 *Komplementarnost PDCA procesnog modela i ISMS standarda*

ISMS standard	Faza PDCA modela procesa
Faza planiranja – *uspostavljanje ISMS-a*	
1	Organizacija *definiše oblasti* na koje će se primenjivati ISMS.
A.5.1	Organizacija *definiše politiku zaštite* za oblasti definisane u tački 1.
4.2.1c)	Organizacija identifikuje adekvatan okvir i pristup proceni rizika, koji će davati ponovljive i uporedive rezultate, usaglašene sa poslovnim i drugim zahtevima.
4.2.1d)	Identifikovanje rizika.
4.2.1e)	Procena (analiza i evaluacija) rizika.
4.2.1f)	Identifikovanje i evaluacija opcija tretmana rizika.
4.2.1g)	Izbor ciljeva kontrola i kontrola zaštite (iz aneksa A) za ispunjenje kriterijuma iz okvira za menadžment rizika, uključujući implementirane kontrole, zakonske zahteve i druge obaveze, navedene u izjavi o primenljivosti (SoA) (**4.2.1j)2)**).
ISMS standard	**Faza PDCA modela procesa**
4.2.1h)	Izjava o primenljivosti (SoA) potvrđuje da menadžment prihvata preostali rizik.
4.2.1i)	Nadležnost menadžmenta da odobri implementaciju ISMS-a i preostali rizik.
Faza primene – *implementacija i rad ISMS-a*	
4.2.2.a)	Plan tretmana rizika odražava odluke uspostavljene u fazi planiranja i identifikuje akcije menadžmenta, odgovornosti i prioritete za tretman faktora rizika.
Faza provere – *kontrola i provera primene ISMS-a*	
4.2.3)	Monitoring, interna i nezavisna provera i menadžerska revizija ISMS-a.
Faza delovanja – *održavanje i poboljšavanje ISMS-a*	
4.2.4)	Održavanje i poboljšavanje ISMS.

6.2.3 Obim i primena ISMS-a

Standard ISMS-a pokriva sve tipove organizacija, a u kontekstu okruženja i poslovnog rizika organizacije, specificira zahteve za uspostavljanje, implementaciju, primenu, monitoring, proveru, održavanje i poboljšavanje dokumentovanog ISMS-a. Takođe, za smanjenje rizika na prihvatljiv nivo, specificira *zahteve* za implementaciju *kontrola zaštite* usaglašenih

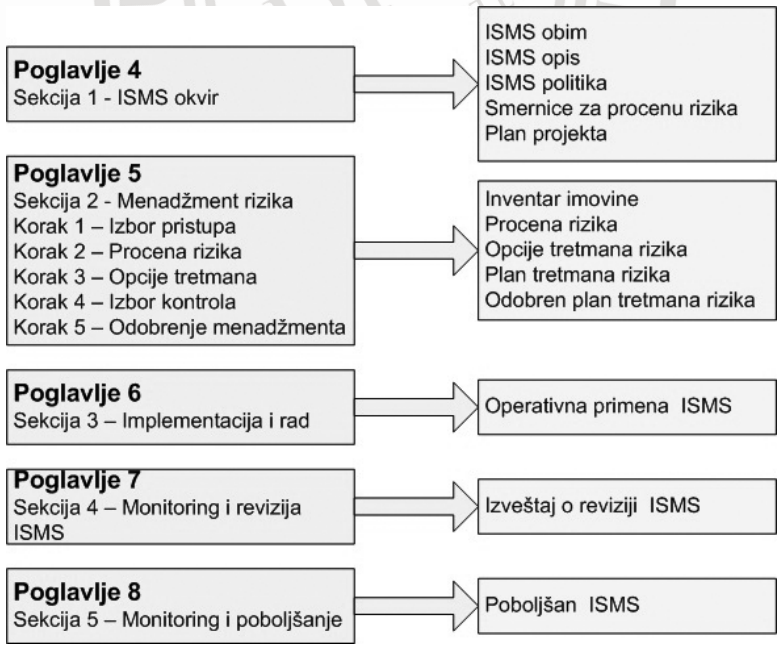
sa potrebama organizacije. Generalno, ISMS standard u Aneksu A obezbeđuje adekvatan izbor kontrola zaštite (134), uputstva za implementaciju *kontrola zaštite* i poverenje svih zainteresovanih strana, usmeravajući aktivnosti na najkritičnije poslovne procese. Kataloge *kontrola zaštite* sa detaljnom strukturom (klase, familije, kontrole) i opisom njihove namene, robusnosti i fleksibilnosti za osnovni, povećani i visoki nivo zaštite informacija nude NIST standardi (SP 800-53 A, B, C) i ISF (*International Security Forum*, verzija 4) [30].

6.2.4 Zahtevi ISMS standarda

Standard ISO/IEC 27001 sadrži dve vrste zahteva za menadžment zaštite informacija:

- *metodološki zahtevi* — poglavlja od 4 do 8, gde se objašnjava kako razviti i upravljati zaštitom informacija:
  poglavlje 4: *Menadžment sistem zaštite informacija (ISMS*),
  poglavlje 5: *Odgovornost menadžmenta,*
  poglavlje 6: *Interna provera ISMS-a,*
  poglavlje 7: *Menadžerska provera ISMS-a* i
  poglavlje 8: *Poboljšanje ISMS*-a.
- *zahtevi za kontrole zaštite – Annex A* standarda ISO/IEC 27001:
  1. kontrolni ciljevi (*Control Objectives*)
  2. bezbednosne kontrole (*Security controls*).

Struktura relevantnih poglavlja i sekcija ISMS standarda prikazana je na slici 6.3.



Slika 6.3 Struktura relevantnih sekcija ISMS-a

Zahtevi ISMS standarda su generički i tako postavljeni da mogu biti primenljivi u organizaciji svakog tipa, karaktera i veličine. Ako neka organizacija želi da usaglasi svoj ISMS sa ovim standardom, *nije prihvatljivo izostavljanje* nekih od zahteva navedenih u poglavljima 4 do 8 standarda. Ako se ispostavi da je neophodno *izuzeti* određene *kontrole zaštite,* da bi se zadovoljili *kriterijumi prihvatljivog rizika*, potrebno je da to odgovorno lice *obrazloži sa* dokazom da su odnosni rizici prihvatljivi. Takođe, ako se neke *kontrole zaštite izostave*, usaglašenost sa ISMS standardom neće biti prihvaćena, *osim ako* takvi izuzeci ne doprinose zaštiti informacija organizacije, u skladu sa bezbednosnim zahtevima, ustanovljenim na bazi procene rizika ili usaglašavanja sa zakonskim zahtevima i propisima. Ukoliko u organizaciji *već postoji* operativan menadžment sistem poslovnih procesa (npr. prema ISO 9001: 2008 ili ISO 14001), u većini slučajeva takav menadžment sistem je komplementaran i u velikoj meri može odgovoriti zahtevima ISMS standarda.

ISMS standard zahteva obaveznu primenu određenih dokumenata. *Opšti zahtev standarda* je da u kontekstu menadžmenta operativnog rizika za IKT i poslovni sistem, organizacija: (1) *uspostavlja, (2) implementira, (3) primenjuje, (4) monitoriše, (5) proverava, (6) održava i (7) poboljšava* dokumentovan ISMS sistem. Za *uspostavljanje i menadžment dokumentovanog ISMS* organizacija preduzima brojne aktivnosti, kao što su:

a. definisanje obima i granica ISMS-a u skladu sa tipom IKT sistema, lokacijom, opremom, tehnologijama i razlozima za opravdanje izuzeća iz oblasti primene;

b. *definisanje ISMS politike* (nadskup *politika zaštite* informacija, koje mogu biti izrađene u okviru jednog dokumenta) u skladu sa karakteristikama poslovanja, tipom organizacije, lokacijom, opremom i primenjenim tehnologijama, koja:
   1. uključuje *okvir* za postavljanje ciljeva, smernica i principa zaštite informacija,
   2. zadovoljava poslovne, normativne i ugovorne bezbednosne *zahteve*,
   3. odgovara *strateškim ciljevima menadžmenta operativnog rizika* organizacije i
   4. uspostavlja kriterijume za evaluaciju rizika.

c. definisanje pristupa za procenu operativnog rizika organizacije.

*Metodologija za procenu rizika***,** koja obezbeđuje *uporedive i ponovljive rezultate***,** određuje se u skladu sa ISMS organizacije, identifikovanom zaštitom poslovnih informacija, zakonskim i ugovornim zahtevima**.** Primeri *metodologija za procenu rizika* mogu se naći u standardima ISO/IEC TR 13335-3, ISO/IEC 27005, NIST SP 800-30.

Sledeći korak je uspostavljanje kriterijuma za prihvatanje rizika i identifikovanje prihvatljivih nivoa rizika (5.1f) Standarda).

d. Identifikovanje rizika uključuje sledeće aktivnosti:
   1. identifikovanje imovine i vlasnika[2] imovine u oblastima primene ISMS,
   2. identifikovanje pretnji za informacionu imovinu,
   3. identifikovanje ranjivosti informacione imovine koje pretnje mogu iskoristiti i
   4. identifikovanje uticaja faktora rizika na CIA informacione imovine.

2 Izraz 'vlasnik' predstavlja osobu ili entitet koji ima odgovornost, delegiranu od strane menadžmenta, za kontrolu, proizvodnju, održavanje, korišćenje i zaštitu imovine. Izraz 'vlasnik' ne podrazumeva da lice zaista ima *vlasnička prava* nad imovinom.

e. Analiza i evaluacija rizika uključuje sledeće aktivnosti*:*

1. *procenu uticaja* narušavanja (otkaza, proboja, zaobilaženja) sistema zaštite na poslovanje organizacije, zbog gubitka CIA informacione imovine,
2. *procenu realne verovatnoće* proboja sistema zaštite i uticaja na imovinu, kad pretnje iskoriste ranjivosti i *evaluaciju tekuće kontrole* zaštite,
3. *grupisati faktore rizika* i odrediti nivoe rizika i
4. *utvrditi nivoe prihvatljivosti zahteva za* tretman rizika**,** primenom *kriterijuma za prihvatanje rizika,* uspostavljenim u fazi pripreme (4.2.1c)2 standarda).

f. Identifikovanje i evaluacija tretmana rizika podrazumeva razmatranje opcija tretmana rizika – *izbegavanje, prihvatanje, transfer* i *ublažavanje*, u skladu sa politikom organizacije i kriterijumima za prihvatanje rizika (videti 4.2.1c)2)) .

g. Izbor ciljeva kontrola i kontrola zaštite za tretman rizika vrši se u skladu sa *zahtevima* identifikovanim u procesu *procene* (4.2.1c) i *obrade* 4.2.1f) *rizika*. U izbor kontrola se uključuju *kriterijumi prihvatljivog rizika* (videti 4.2.1c)2)), kao i zakonski *zahtevi,* propisi i ugovorne obaveze. U skladu sa identifikovanim zahtevima zadaju se *ciljevi* i vrši *izbor* odgovarajućih kontrola zaštite iz *Aneksa A* ISMS-a. Moguće je implementirati *dodatne ciljeve* kontrola i *kontrole*. Aneks A sadrži listu *osnovnih* kontrola zaštite tipičnih organizacija (ukupno 134) i predstavlja polaznu osnovu za izbor kontrola, gde korisnici ISMS Standarda mogu proveriti da nisu nešto prevideli[3].

h. Prihvatanje preostalog rizika odobrava menadžment, potpisivanjem *Izjave o primenljivosti* — SoA (*Statement of Aplicability*) koja daje pregled odobrenih i usvojenih rešenja za tretman rizika i opravdava izuzimanje nekih kontrola sa razlozima, koji moraju omogućiti unakrsnu proveru, da se ne izostave greškom i, u tom smislu, treba:

1. *navesti izabrane* ciljeve kontrola i kontrole (4.2.1g) i *razloge* za njihov izbor,
2. *navesti postojeće* ciljeve kontrola i kontrole (4.2.1e)2)) i
3. *opravdati razloge* izostavljanja nekih ciljeva kontrola i kontrola iz *Aneksa A*.

6.2.4.1 Implementacija i rad ISMS (4.2.2 standarda)

Za implementaciju ISMS-a, organizacija treba da preduzme sledeće aktivnosti:

a. formuliše plan tretmana rizika koji identifikuje kontrole zaštite, resurse, odgovornosti i prioritete za menadžment rizika (5.0 standarda),

b. *implementira plan tretmana rizika*, za postizanje planiranih ciljeva kontrola zaštite, koje uključuju finansijsku analizu i dodelu uloga i odgovornosti,

c. implementira upravljačke, operativne i tehničke kontrole zaštite (odabrane u fazi 4.2.1g standarda), da bi se zadovoljili njihovi ciljevi,

d. definiše metrike za merenje efektivnosti kontrola ili grupe kontrola zaštite u cilju povećanja njihove efektivnosti i specificira način korišćenja mernih rezultata, da bi se dobili uporedivi i produktivni rezultati (4.2.3b standarda), koji omogućavaju da organizacija utvrdi kvalitet dostizanja ciljeva kontrola,

3 Detaljnije i brojnije kontrole zaštite sadži NIST-ov standard NIST SP 800-53 koji opisuje 198 kontrola za osnovnu zaštitu informacija.

e. *implementira program* razvoja svesti i *obuke* o zaštiti (5.2.2 standarda),
f. upravlja aktivnostima i procesima primene ISMS-a u praksi zaštite,
g. upravlja (administrira) resursima ISMS-a u praksi zaštite (5.2 standarda) i
h. implementira procedure i kontrole zaštite za detekciju i reagovanje na bezbednosne incidente (4.2.3a standarda).

6.2.4.2 Monitoring i provera ISMS-a (poglavlje 4 i 5 standarda)

U ovoj fazi životnog ciklusa ISMS-a, organizacija preduzima sledeće korake:

a. *sprovodi neprekidni monitoring i proveru* efektivnosti implementiranih procedura i kontrola zaštite u cilju:
   1. *detektovanja grešaka* u rezultatima procesiranja,
   2. *identifikovanja* incidenata, pokušaja i realizovanih napada na sistem zašite,
   3. *obezbeđivanja za menadžment uvida* u sprovođenje delegiranih uloga i odgovornosti i u primenu implementirane tehnologije zaštite, u odnosu na očekivanja,
   4. *podrške otkrivanju bezbednosnih događaja*, da bi se korišćenjem indikatora i predznaka proaktivno predupredila pojava bezbednosnih incidenata i
   5. *utvrđivanja efektivnosti* akcija koje su preduzete za rešavanje incidenta.
b. *sprovodi redovnu proveru efektivnosti ISMS-a* — ISMS politike, ciljeva kontrola zaštite i kontrola zaštite, uzimajući u obzir rezultate provere sistema zaštite (uključujući i testiranje na proboj), incidente, rezultate merenja efektivnosti, sugestije i reakcije svih uloga;
c. *meri efektivnosti kontrola zaštite* u cilju verifikacije ispunjenja bezbednosnih zahteva;
d. *revidira procenjene i preostale faktore rizika* u planiranim intervalima i identifikuje prihvatljive nivoe rizika, u odnosu na promene u organizaciji, okruženju, tehnologijama, poslovnim ciljevima, zakonima itd.;
e. *redovno sprovodi internu proveru ISMS-a* (6.0 standarda) za interne potrebe;
f. *redovno sprovodi menadžersku reviziju ISMS-a*, radi provere adekvatnosti obima ISMS-a i identifikacije mogućnosti poboljšanja ISMS procesa (7.1 standarda);
g. *ažurira planove zaštite* sa nalazima monitoringa i revizije i
h. *vodi zapise* (log datoteke bezbednosno relevantnih događaja) o aktivnostima i događajima, koji mogu imati uticaj na efektivnost i rad ISMS-a (4.3.3 standarda).

6.2.4.3 Održavanje i poboljšanje ISMS-a (6 i 7 standarda)

U fazi održavanja i poboljšanja ISMS-a, organizacija redovno sprovodi sledeće korake:

a. implementira identifikovana poboljšanja u ISMS-u,
b. primenjuje korektivne i preventivne akcije (8.2, 8.3 standarda), sopstvena i tuđa iskustava iz zaštite.
   1. Obaveštava zainteresovane strane o preduzetim merama i poboljšanjima, sa odgovarajućim nivoom detalja i, po potrebi, dogovara se o daljim akcijama.
   2. Obezbeđuje da poboljšanja ispune svoje ciljeve.

6.2.4.4. Zahtevi ISMS standarda za dokumentaciju i zapise

Dokumentacija ISMS-a *uključuje* zapise (evidencije) o odlukama menadžmenta, *prati* odluke i politike menadžmenta i *obezbeđuje* ponovljivost zapisa. Važno je omogućiti *demonstraciju* veze između implementiranih *kontrola zaštite* i rezultata procesa za procenu i tretman rizika, sa jedne i ISMS politike i ciljeva zaštite, sa druge strane.

a. Preporučena ISMS dokumentacija zaštite uključuje:

1. dokumentovane izjava ISMS politike (4.2.1b standarda) i bezbednosnih ciljeva,
2. oblast primene ISMS-a (4.2.1a standarda),
3. procedure i kontrole za podršku ISMS-a,
4. opis metodologije za procenu rizika (4.2.1c standarda),
5. izveštaj o proceni rizika (4.2.1c do 4.2.1g standarda),
6. plan tretmana rizika (4.2.2b standarda),
7. dokumentovane procedure za efektivno planiranje, primenu, kontrolu i za opisivanje metrike efektivnosti procesa i kontrola zaštite informacija (4.2.3c standarda),
8. druge zapise koje zahteva ISMS standard (4.3.3 standarda), i
9. izjavu o primenljivosti (SoA).

Termin "*dokumentovana procedura*" u ISMS standardu podrazumeva da je procedura *uspostavljena*, *dokumentovana*, *implementirana* i *održavana*. Obim ISMS dokumentacije može da se razlikuje, u zavisnosti od veličine i vrste poslovanja organizacije, oblasti primene i kompleksnosti bezbednosnih zahteva i menadžment sistema. Dokumenta i zapisi mogu biti *u bilo kojoj formi* i na bilo kojem medijumu. U **Prilogu 6.1** prikazana je dokumentacija preporučena ISMS standardom.

b. Kontrola dokumentacije (4.2.3 standarda)
ISMS dokumentacija mora biti zaštićena i *kontrolisana*. *Dokumentovane procedure* se uspostavljaju da definišu akcije menadžmenta, kao što su:

1. odobravanje adekvatnosti dokumenata za publikovanje,
2. ponovljeno odobravanja dokumentacije nakon pregleda i ažuriranja,
3. obezbeđivanje identifikovanja izmena i statusa revizije dokumenata;
4. obezbeđivanje dostupnosti relevantnih verzija na mestu primene,
5. obezbeđivanje razumljivosti i preglednosti dokumenta,
6. obezbeđivanje prenosa, čuvanja, distribucije i raspoloživosti dokumentacije,
7. obezbeđivanje identifikacije dokumenata eksternog porekla,
8. obezbeđivanje kontrole distribucije dokumenata,
9. sprečavanje nenamernog korišćenja starih verzija dokumenata i
10. dodeljivanje odgovarajuće identifikacije starim verzijama dokumenata.

c. Kontrola zapisa (4.3.3 Standarda)
Zapisi se uspostavljaju i održavaju da obezbede *dokaze usaglašenosti* sa zahtevima i *efektivnosti* rada ISMS-a. Zapisi moraju biti *zaštićeni i kontrolisani*, pošto ISMS uključuje sve relevantne zakonske zahteve, propise i ugovorne obaveze; moraju biti čitljivi, sa jednostavnim identifikatorima i pristupom. Za menadžment zahteva, zapisi

moraju biti *dokumentovani* i *implementirane kontrole* za *identifikovanje, skladištenje, zaštitu, korišćenje, pristup, period zadržavanja i distribucije zapisa.* Zapisi se vode za sve procese iz poglavlja 4.2 standarda i za svaki događaj značajnijeg bezbednosnog incidenta, koji se odnosi na ISMS. Primeri zapisa mogu biti knjige gostiju, izveštaji rezultata provere i popunjeni obrasci za logičku kontrolu pristupa.

6.2.4.5 Odgovornosti menadžmenta u ISMS-u (5.0 standarda)

Standard ISMS zahteva da menadžment obezbeđuje *dokaze o svom angažovanju* za uspostavljanje, implementaciju, primenu, monitoring, pregled, održavanje i poboljšavanje ISMS-a putem:

1. izrade i implementacije ISMS politike,
2. obezbeđivanja uspostavljanja ciljeva i planova ISMS-a,
3. delegiranja uloga i odgovornosti u sistemu zaštite informacija,
4. saopštenja o značaju dostizanja bezbednosnih ciljeva i usaglašavanja sa politikom zaštite informacija, zakonskim obavezama i potrebom za neprekidnim poboljšavanjem sistema zaštite,
5. obezbeđivanja resursa za uspostavljanje, implementaciju, primenu, monitoring, reviziju, održavanje i poboljšavanje ISMS-a (5.2.1 standarda),
6. odlučivanja o kriterijumima za prihvatanje rizika i prihvatljivim nivoima rizika,
7. potvrde da je interna ISMS kontrola sprovedena (6 standarda) i
8. sprovođenja menadžerskih provera ISMS (7 standarda).

6.2.4.6 Upravljanje resursima (5.2 standarda)

Menadžment organizacije treba da obezbedi resurse neophodne za:

1. uspostavljanje, implementaciju, primenu, monitoring, proveru, održavanje i poboljšavanje ISMS-a,
2. podršku poslovnih zahteva procedurama zaštite informacija;
3. identifikovanje zakonskih zahteva, propisa i ugovornih obaveza,
4. održavanje adekvatne zaštite korektno implementiranim kontrolama zaštite,
5. sprovođenje neophodnih provera i adekvatno reagovanje na rezultate i za
6. zahtevano poboljšavanje efikasnosti i efektivnosti ISMS-a.

6.2.4.7 Obuka, svest o potrebi i kompetencije zaposlenih (5.2.2 standarda)

Menadžment organizacije je odgovoran da obezbedi *kompetentno* osoblje za izvršavanje zadataka, prema definisanim odgovornostima u ISMS-u. Ovaj zahtev standarda organizacija izvršava na bazi:

1. utvrđivanja neophodne stručnosti osoblja čiji rad utiče na ISMS,
2. obezbeđivanja obuke ili preduzimanja sličnih akcija (npr. zapošljavanja kompetentnog osoblja),

3. evaluacije efektivnosti preduzetih akcija i održavanja zapisa o edukaciji, obuci, veštinama, iskustvu i kvalifikacijama (4.3.3 standarda) i
4. razvoja svesti relevantnog osoblja o značaju njihove uloge u sistemu zaštite informacija i razumevanja doprinosa u ostvarivanju ciljeva ISMS-a.

6.2.4.8 Interna provera ISMS-a (6.0 standarda)

Menadžment organizacije, takođe, organizuje i sprovodi internu *proveru* ISMS-a u planiranim intervalima, radi utvrđivanja u kojoj meri su *ciljevi kontrola, kontrole, procesi i procedure* ISMS-a:

1. adekvatni zahtevima ISO/IEC 27001 standarda i relevantnih zakona i propisa;
2. adekvatni identifikovanim bezbednosnim zahtevima za zaštitu informacija;
3. efektivno implementirani i održavani i
4. izvršavani u skladu sa očekivanjima.

Interna provera je *planiran* program koji uključuje razmatranja statusa i značaja procesa i oblasti koje treba proveriti, kao i rezultate prethodnih provera. Proces provere ima definisane kriterijume, obim, period sprovođenja i metod rada. Izbor *nepristrasnih* proveravača (*auditors*) obezbeđuje da proces provere bude *objektivan*. Proveravač ne sprovodi proveru sopstvenog posla, a *dokumentovana procedura* definiše njegove *odgovornosti* i *zahteve* za planiranje i sprovođenje provere, izveštavanje o rezultatima i održavanje rezultata provere (4.3.3 standarda).

Menadžment proveravanog dela organizacije preduzima akcije za *eliminisanje* otkrivenih neusaglašenosti i njihovih uzroka. Dodatne aktivnosti uključuju verifikaciju preduzetih akcija i izveštaje o rezultatima verifikacije (8 standarda). *Uputstvo za sprovođenje interne provere* ISMS može se naći u standardu ISO 19011:2002 — *Uputstvu za proveru menadžment sistema kvaliteta i/ili okruženja*. Procedura interne provere ISMS data je u poglavlju 12.

6.2.4.9 Menadžerska revizija ISMS-a (7.0 standarda)

Menadžment sprovodi *menadžersku reviziju ISMS-a u planiranim intervalima*, što obezbeđuje neprekidnu usaglašenost, adekvatnost i efektivnost ISMS-a. Ova revizija sadrži procenu elemenata za *poboljšavanje* i potrebe za *izmenama* u ISMS-u, uključujući izmene bezbednosnih ciljeva i politike zaštite informacija. *Rezultati* revizije se precizno dokumentuju, a *zapisi* održavaju u skladu sa zahtevom 4.3.3. standarda.

Ulazne veličine u proces menadžerske revizije ISMS-a uključuju:

1. rezultate internih i nezavisnih provera ISMS-a,
2. reakcije zainteresovanih strana,
3. tehnike, proizvode ili procedure, koje organizacija koristi za poboljšanje rada i efektivnosti ISMS-a,
4. status preventivnih i korektivnih akcija,
5. neadekvatno referencirane ranjivosti ili pretnje u prethodnoj proceni rizika;
6. rezultate merenja efektivnosti kontrola zaštite,

7. dodatne akcije prethodnih menadžerskih provera,
8. sve izmene koje mogu uticati na efektivnost ISMS-a i
9. preporuke za poboljšavanje ISMS.

Izlazne veličine procesa menadžerske revizije uključuju sve *diskusije i aktivnosti* vezane za:

1. poboljšanje efektivnosti ISMS-a (8 standarda);
2. ažuriranje procene rizika i plana tretmana rizika;
3. modifikaciju procedura i kontrola koje utiču na bezbednost informacija, ukoliko je neophodno, reagovanje na interne ili eksterne događaje koji mogu uticati na ISMS, uključujući izmene: *poslovnih i bezbednosnih zahteva, poslovnih procesa koji utiču na postojeće poslovne zahteve, zakonskih zahteva i regulativa, ugovornih obaveza i nivoa rizika i/ili kriterijuma za prihvatanje rizik;.*
4. potrebe za resursima;
5. poboljšanje metrike efektivnosti kontrola zaštite.

6.2.4.10 Poboljšavanje ISMS-a (8.0 standarda)

Organizacija je odgovorna za *kontinualno poboljšavanje efektivnost ISMS-a* (8.1 standarda) na bazi:

1. *politike* zaštite informacija,
2. bezbednosnih *ciljeva*,
3. rezultata interne *provere*,
4. *analize* monitoringa događaja,
5. korektivnih i preventivnih akcija i
6. menadžerske revizije (7 standarda).

Organizacija preduzima *korektivne akcije* za *eliminisanje uzroka neusaglašenosti* sa ISMS zahtevima (8.2 standarda), čime proaktivno sprečava njihovo ponavljanje. *Dokumentovana procedura* za korektivne akcije definiše zahteve za:

1. *identifikovanje* neusaglašenosti,
2. utvrđivanje *uzroka* neusaglašenosti,
3. *evaluiranje potreba* za akcijama sprečavanja ponavljanja neusaglašenosti,
4. određivanje i *implementaciju* neophodnih korektivnih akcija,
5. *evidentiranje* rezultata preduzetih akcija (4.3.3 standarda) i
6. *proveru* preduzetih korektivnih akcija.

Organizacija određuje akcije za *eliminisanje potencijalnih uzroka* neusaglašenosti sa ISMS zahtevima (8.3 standarda), čime *predupređuje* njihovu pojavu. Preduzete *preventivne akcije* odgovaraju uticaju potencijalnih problema. *Dokumentovana procedura za preventivne akcije* definiše zahteve za:

1. identifikovanje potencijalnih neusaglašenosti i njihovih uzroka,
2. preventivne akcije sprečavanja pojave neusaglašenosti,
3. određivanje i implementaciju neophodnih preventivnih akcija,

4. evidentiranje rezultata preduzetih akcija (4.3.3 standarda) i
5. reviziju preduzetih preventivnih akcija.

Zatim organizacija treba da identifikuje promenjene nivoe rizika i zahteve preventivnih akcija koje najviše utiču na promenu rizika. Prioritet preventivnih akcija se određuje na osnovu rezultata procene rizika. Preventivne akcije su često jeftinije od korektivnih i treba ih primenjivati gde god je moguće.

6.3. OTVORENI PROBLEMI MENADŽMENTA ZAŠTITE INFORMACIJA

Osnovne prepreke i problemi menadžmenta ISMS spadaju u dve potencijalne kategorije — dobijanje neophodne podrške menadžerske strukture za izvršavanje strateškog plana implementacije ISMS-a i dobijanje neophodne podrške ostalih organizacionih (ne IT) jedinica za realizaciju politike zaštite [1, 9, 10, 14].

U teoriji i praksi zaštite česti su sledeći problemi:

a. *u oblasti menadžment sistema zaštite informacija,* često je problem objektivna evaluacija imovine kompleksnih sistema sa velikom infrastrukturom, posebno u:
   1. *klasifikaciji* imovine *organizacije* — određivanje prioriteta evaluacije,
   2. *evaluaciji podataka i proceni ranjivosti sistema* — nedostaju *čvrsti* kriterijumi,
   3. *kvalitativnoj proceni* — subjektivnost i unos faktora neodređenosti,
   4. *kompleksnoj infrastrukturi sistema* — teorija verovatnoće nije dobar pristup,
   5. *uticaju para pretnja/ranjivost na privatnost i poverljivost* — nepotpuno definisanje i merenje,
   6. *upravljanju ličnim podacima* — nedostaje standard najbolje prakse.

Perspektivni i obećavajući pristupi rešavanju nekih od navedenih problema su primena:

1. *teorije dokaza* (*Dempster-Shafer Theory of Evidence)*,
2. *Fuzzy Set Theory* (*membership functions, aggregations, defizzification*) i
3. *Fuzzy logic*, za procenu ranjivosti.

b. U oblasti procene ranjivosti tekući problemi su:

1. teškoće razumevanja stvarnog uticaja ranjivosti, a zbog toga i rizika za informacionu imovinu u realnom okruženju. Na nivou mreže/servera postoji više raspoloživih alata, koji tretiraju ranjivosti na različite načine, pa čak i nestandardno imenuju ranjivosti i izloženosti sistema;
2. obilje informacija iz procesa analize ranjivosti sistema i preobilni izveštaji otežavaju menadžment rezultata analize ranjivosti sistema;

kašnjenje razvoja bezbednosnih popravki (zakrpa) i korekcija ranjivosti otežava blagovremenu korekciju i pomeranje sistema u bezbednije stanje; delimično rešenje je koncept *proaktivne zaštite*.

U ovoj oblasti potrebna su istraživanja u *standardizaciji alata* za procenu ranjivosti sistema, *usaglašavanju standardizacionih tela* za procenu ranjivosti (***CIDF*** *–Common Intrusion*

Detection Framework, ***IETF*** *– International Engineering Task Force,* ***IDWG*** *– Intrusion Detection Working Group,* **CVE** *– Common Vulnerabilities and Exposures....*) i *usvajanje standardnog formata izveštaja o analizi ranjivosti – VARF* (*Vulnerability Assesment Report Format*), koji definišu format podataka za razmenu informacija o ranjivostima sistema i olakšava interakciju sa procesom menadžmenta rizika. Koncept VARF-a sadrži set *XSLT* transformacija koje transformišu rezultate izlaza iz alata za analizu ranjivosti sa otvorenim izvornim kodom u usaglašen VARF format izveštaja, koji omogućava dalje procesiranje rezultata analize rizika [11, 49].

c. U oblasti detekcije i sprečavanja upada u sistem (IDPS) osnovni problemi su [standardizacija interoperabilnosti,

1. usaglašavanje međunarodnih tela za standardizaciju,
2. identifikovanje ograničenja IDPS sistema i
3. identifikovanje tekućih problema IDPS sistema.

6.4. PREPORUKE ZA MENADŽMENT SISTEM ZAŠTITE INFORMACIJA

Standard ISMS identifikuje one komponente programa zaštite, čijim se efektivnim menadžmentom ispunjavaju svi zahtevi zaštite. Standard fokusira pažnju na sledećih deset kategorija menadžmenta zaštite informacione imovine:

1. *dokument politike zaštite*: osigurava da je organizacija svesno i eksplicitno pristupila zaštiti relevantne informacione imovine i da menadžment podržava politiku zaštite,
2. *alociranje odgovornosti za zaštitu*: definiše lica i entitete odgovorne za zaštitu informacione imovine,
3. *obrazovanje i obuka u oblasti zaštite:* jedna je od najvažnijih i najefikasnijih mera zaštite za korisnike i menadžere poslovnih sistema,
4. *upravljanje bezbednosnim incidentom i izveštavanje*: izveštavanje o svakom incidentu treba da bude pravovremeno, potpuno i proaktivno radi sprečavanja ponavljanja sličnog incidenta,
5. *kontrola malicioznih programa*: mora biti adekvatna porastu pretnji od malicioznih programa i napada,
6. *plan menadžmenta vanrednog događaja i kontinuiteta poslovanja*: obezbeđuje raspoloživost resursa, odgovornost i procese za razvoj plana i oporavak sistema,
7. *zaštita intelektualne svojine:* zahteva se zbog zakonskih restrikcija,
8. *zaštita baza podataka*: obavezna je jer sadrže agregirane, arhivirane i poverljive podatke i informacije,
9. *zaštita integriteta, raspoloživosti, poverljivosti i privatnosti informacija*: u skladu sa bezbednosnim zahtevima za zaštitu CIA informacija i
10. *usaglašenost sa politikom zaštite*: mora se razmatrati regularno u procesima monitoringa, provere, sertifikacije i akreditacije sistema zaštite.

6.5. REZIME

Standard ISO/IEC 27001 primenjuje PDCA model na sve ISMS procese i nudi robustan model za implementaciju *principa zaštite (OECD, NIST i GAISP),* kao i uputstva i smernice za procenu rizika, projektovanje i implementaciju zaštite, upravljanje zaštitom i ponovnu procenu i poboljšanje ISMS procesa.

Funkcionalni model procesa ISMS-a zasniva se na opšte prihvaćenim principima zaštite OECD (GAISP). Procesi uspostavljanja, održavanja i poboljšanja ISMS-a mogu imati presudni značaj za konkurentnost i poslovni ugled organizacije. Informaciona imovina organizacije izložena je pretnjama iz širokog opsega izvora. Brojni IKT sistemi nisu projektovani tako da budu bezbedni. Bezbednost ostvarena tehničkim kontrolama je ograničena i treba je podržati *proceduralnim* kontrolama zaštite. Identifikovanje kontrola zahteva pažljivo planiranje. Efektivan ISMS, kao minimum zahteva angažovanje svih relevantnih učesnika. Bitno je da organizacija identifikuje svoje zahteve za bezbednost iz *rezultata procene rizika, zakonskih ugovornih i drugih obaveza* i *skupa principa, ciljeva i poslovnih zahteva*.

ISMS se definiše kao *menadžment sistem koji uključuje organizacionu strukturu, politiku, procedure, planiranje, odgovornosti, procese, praksu i resurse za bezbednost informacione imovine.* Prema ISMS standardu, zahtevi za bezbednost identifikuju se procenom rizika za bezbednost informacione imovine organizacije. Troškovi kontrola zaštite treba da su uravnoteženi sa štetom za poslovanje, koja bi mogla nastati kao rezultat otkaza sistema zaštite. Rezultati procene rizika koriste se kao smernice za utvrđivanje odgovarajuće akcije menadžmenta i prioriteta tretmana rizika, kao i za implementaciju izabranih kontrola za ublažavanje rizika. Procenu rizika potrebno je periodično ponavljati kako bi se obuhvatile nastale promene.

Na bazi odluke za tretman rizika (SoA), vrši se izbor i implementacija *kontrola zaštite* za smanjenje rizika na prihvatljiv nivo, na osnovu ISO/IEC 27002 standarda, ili iz drugih standarda (npr. NIST SP 800-53), ili se mogu projektovati nove kontrole za specifične potrebe organizacije. Projektovanje i implementacija ISMS-a organizacije predstavlja *strateški cilj* organizacije, a *zavise* od njenih poslovnih potreba, ciljeva i procesa, bezbednosnih zahteva, veličine i složenosti organizacije. Nivo implementacije ISMS-a se *usklađuje* prema potrebama organizacije, a standard se može koristi za internu i eksternu *procenu usaglašenosti* i ISO/IEC 27001 sertifikaciju.

6.6 PITANJA ZA PONAVLJANJE

1. Mogu li svi tipovi organizacija neposredno imati koristi od implementacije ISMS-a?
   a. Ne, potreban je razvoj svesti o potrebi zaštite u mnogim organizacijama.
   b. Da.
   c. Po potrebi.
2. Da li standard zahteva da organizacije implementiraju ISMS u celini (sekcije 4 to 8) pre faze 1 *online* provere (*desktop rewiev*)?
   a. Ne.
   b. Da.
   c. Po potrebi.
3. Treba li u fazi 1 provere preko sajta dostaviti veliki broj dokumenata na proveru?
   a. Ne.
   b. Da.
   c. Samo ona koja se bezbedno mogu slati Internetom ili predati u pisanoj formi.
4. Može li organizacija obezbediti dokumenta u elektronskoj formi za proces provere?
   a. Ne.
   b. Da.
   c. Po potrebi.
   d. Ako su u pdf formatu sa pasvord zaštitom i restrikcijom kopiranja.
5. Šta proveravač traži u fazi 3 provere na lokaciji?
   a. Upoređuje dokumenta politike, standarda i procedura sa aktuelnom praksom.
   b. Zahteva validaciju praksi zaštite neposredno ili opservacijom rada ovlašćenih korisnika.
   c. Upoređuje praksu zaštite sa zakonom i regulativama.
6. Da li proveravač treba da proveri da li su kontrole zaštite korektno implementirane i konfigurisane?
   a. Ne, zato što to nije primarni zadatak provere.
   b. Da, zato što je to primarni zadatak provere.
   c. Po potrebi.
7. Da li proveravač posećuje lokaciju zajedno sa tehničkim specijalistima?
   a. Ne, verifikaciju i validaciju prakse zaštite može sam izvršiti.
   b. Da, validacija prakse zaštite je detaljna i vremenski zahtevna.
   c. Po potrebi.
   d. Samo na zahtev proveravane organizacije.
8. Šta ISMS treba da zaštiti? Da li fokus politike zaštite treba da bude na informacije ili tehnologiju?
   a. Samo informacije relevantne za organizaciju.
   b. Samo informacione tehnologije relevantne za organizaciju.
   c. Po potrebi i informacije i informacione tehnologije.
   d. Istovremeno informacije i informacione tehnologije relevantne za organizaciju.
9. Kakav uticaj na organizaciju mogu imati kompromitovane informacije? (Koji odgovor najviše odgovara?)
   a. Na osetljive informacije, fizičku imovinu, ljude.
   b. Na osetljive informacije, papirna dokumenta, fizičku imovinu.
   c. Na osetljive informacije, softvere, servise, ljude, brend, poslovni ugled.
   d. Na papirna dokumenta, softvere i ljude.
10. Može li organizacija, distribuirana na više lokacija, definisati obim, zahtevati sertifikaciju i dobiti ISMS sertifikat samo za jednu lokaciju?
    a. Ne, to nije uobičajeno ni lako.
    b. Da, moguće je, ali nije uobičajeno ni lako.
    c. Po potrebi, ako to odobri sertifikator.
    d. Da, ali morate opisati sve veze sa drugim lokacijama.

11. Može li konsultant učestvovati u implementaciji, a zatim u proveri istog sistema zaštite?
    a. Ne, to je sukob interesa.
    b. Da, moguće je, ali nije uobičajeno.
    c. Da, to nije sukob interesa.
    d. Da, ali mora opisati svoju ulogu u implementaciji.
12. Može li nezavisni proveravač (*auditor*) davati savete za implementaciju, kada vrši nezavisnu proveru sistema u organizaciji?
    a. Ne, to je sukob interesa.
    b. Da, moguće je, ali nije uobičajeno.
    c. Ne, to je u sukobu sa vodećim smernicama (*governance guidelines*).
    d. Da, to je u skladu sa vodećim smernicama.
13. Koliko je lako implementirati ISMS?
    a. Relativno lako, zavisno od tekućeg sistema zaštite.
    b. Podjednako je lako implementirati prihvatljiv ISMS i usaglašen ISMS za ISO/IEC 27001 sertifikat.
    c. Lakše je implementirati prihvatljiv ISMS, nego usaglašen ISMS za ISO/IEC 27001 sertifikat.
    d. Teže je implementirati prihvatljiv ISMS nego usaglašen ISMS za ISO/IEC 27001 sertifikat.
14. Ako organizacija već ima implementirane ISO/IEC 9001 i ISO 9019, može li integrisati ISO/IEC 27011 i ISMS standarde u postojeći sistem kvaliteta?
    a. Ne, to nije moguće ni lako.
    b. Da, moguće je, ali nije uobičajeno ni lako.
    c. Da, jer su ovi standardi menadžment sistemi i koriste isti model (PDCA) procesa za implementaciju.
    d. Da, organizacija može ISMS implementirati nezavisno, ili razviti integrisani (TQM) menadžment sistem.
15. Šta je sertifikaciono telo u informacionoj bezbednosti?
    a. Akreditovani entitet – TTP organizacija koja proverava/sertifikuje ISMS neke organizacije prema standardu menadžment sistema zaštite.
    b. Vodeći proveravač koji proverava/sertifikuje ISMS neke organizacije prema nekom standardu.
    c. Specijalista zaštite koji proverava/sertifikuje efektivnost kontrola zaštite prema politici zaštite.
16. Koja su tela akreditovana za ISMS standard?
    a. Nije akreditovano ni jedno telo.
    b. Akreditovano je nekoliko desetina tela.
    c. Akreditovano je jedanaest tela.
    d. Akreditovana su četiri tela.
17. Ko originalno piše ISMS i standarde zaštite?
    a. Potkomitet 27 (SC27).
    b. ISO/IEC joint technical committee (JTC1).
    c. Working Group 1 (WG1) SC27 potkomiteta.
    d. Working Group 4 (WG4) SC27 potkomiteta.
18. Šta predstavlja dokument *ISO/IEC Guide 62*?
    a. Smernice za implementaciju ISMS.
    b. Opšte zahteve za sertifikaciona tela.
    c. Smernice za implementaciju kontrola zaštite.
    d. Smernice za procenu rizika.
19. Koja je razlika između tela za sertifikaciju i akreditaciju?
    a. Akreditaciono telo, obično na nacionalnom nivou, daje ovlašćenje TTP organizaciji (sertifikacionom telu) da izdaje sertifikate.
    b. Akreditovano telo izdaje sertifikate o usaglašenosti prema nekom standardu.
    c. Sertifikaciono telo se samoakreditуje na osnovu razvijenih kapaciteta za sertifikaciju.
    d. Oba tela izdaju sertifikate o usaglašenosti prema nekom standardu.
20. Gde se može nabaviti kopija ISO standarda?
    a. Preko web adrese www.iso.org.
    b. Preko nacionalnog zavoda za standardizaciju.
    c. Preko web sajta Amazon-a.

d. U specijalizovanoj knjižari za standarde.

21. Kakva je razlika između starog BS 7799 i novog ISO/IEC 27001 standarda?
    a. Nema nikakve razlike.
    b. Razlika je u promeni strukture kontrola zaštite BS 7799.
    c. Razlika je suštinska i velika.
    d. Razlika je samo u formi i strukturi standarda.
22. Šta je ISO/IEC 27001 standard?
    a. Novo ime međunarodnog standarda BS 7799 od 2005.
    b. Standard za kontrole zaštite.
    c. Novo ime standarda ISO/IEC 17799 od 2005. godine.
    d. Standard koji opisuje zahteve za implementaciju ISMS.
    e. Standard za procenu rizika.
23. Šta je standard ISO 27002?
    a. Novo ime međunarodnog standarda BS 7799 od 2005. godine.
    b. Standard za kontrole zaštite.
    c. Standard koji opisuje zahteve za implementaciju ISMS.
    d. Standard za procenu rizika.
    e. Novo ime standarda ISO/IEC 17799 od 2005. godine.
24. Može li se za implementaciju ISMS koristiti neki drugi standard?
    a. Ne može.
    b. Ne preporučuje se.
    c. Ni jedan standard ne pokriva sve potrebne menadžment sisteme organizacije.
    d. Mogu NIST standardi koje pokrivaju zaštitu informacija i menadžment sistem informacione bezbednosti.
    e. Treba izabrati jedan ISMS standard pa onda detalje dopunjavati iz drugih standarda po potrebi organizacije.
25. Menadžment sistem bezbednosti informacija je:
    a. proces uspostavljanja sistema zaštite informacija
    b. proces, koji treba neprekidno poboljšavati
    c. proces procene rizika poslovanja do prihvatljivog nivoa usaglašenosti
    d. proces za dostizanje i održavanje prihvatljivog nivoa usaglašenosti sa ISMS standardom
    e. rezultat procesa usaglašenosti sistema zaštite sa ISMS standardom.
26. Kako korisnik može utvrditi da ISMS menadžment sistem funkcioniše?
    a. Opservacijom operacija zaštite (funkcionisanja servisa, mehanizama i protokola).
    b. Uvođenjem metrika i merenja efektivnosti ISMS operacija.
    c. Evaluacijom procesa zaštite.
    d. Implementacijom smernica iz standarda ISO/IEC 27004.
27. Da li je implementacija ISMS-a suviše zahtevna za manje organizacije?
    a. Troškovi zaštite neke imovine ne treba da budu veći od vrednosti te imovine.
    b. Organizacija treba da utvrdi poslovne razloge i opravdanje za ISMS sertifikaciju.
    c. Svaki tip organizacije treba da implementira kompletan ISMS.
    d. Manje organizacije ne treba da implementiraju ISMS.
    e. Manje organizacije mogu selektivno implementirati odgovarajuće delove ISMS.
28. Da li je važno da organizacija dobije sertifikat?
    a. Sertifikacija je potvrda da je organizacija stvarno implementirala ISMS.
    b. ISMS sertifikat ne može biti marketinška prednost organizacije.
    c. U slučaju spora ISMS sertifikat potvrđuje menadžmenta rizika organizacije.
    d. Dobijanje ISMS sertifikata uglavnom nije važno za organizaciju.
29. Da li je pametno uključiti bezbednosne zahteve u sve ugovore?
    a. Ne, ne treba u svakom ugovoru uključiti bezbednosne zahteve.
    b. Bezbednosne zahteve treba selektivno uključiti u značajnije ugovore.
    c. Da, u svakom ugovoru treba uključiti bezbednosne zahteve.
    d. Bezbednosne zahteve treba uključiti samo u informatičke ugovore.



7. PLANIRANJE ISMS-a I MENADŽMENT RIZIKA

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Primenu PDCA faze planiranja za planiranje i uspostavljanje ISMS-a
- ☑ Potrebu definisanja obima ISMS-a i politike zaštite informacija
- ☑ Značaj procesa menadžmenta i procene rizika za uspostavljanje ISMS-a
- ☑ Analizu i izbor kontrola zaštite za tretman rizika
- ☑ Potrebu planiranja tretmana rizika i izrade izjave o primneljivosti (SoA)

7.1 UVOD

Razvoj ISMS je sistematičan proces, koji zahteva podršku menadžmenta, angažovanje resursa organizacije i alate za podršku, kao što su uzorci, obrasci i nacrti dokumenta. U procesu razvoja ISMS-a koristi se PDCA model i kontrole zaštite iz Aneksa A standarda ISO/IEC 27001 ili ISO/IEC 27002. Nivo detalja razvoja i dokumentacija zavise od bezbednosnih ciljeva i želje organizacije za dobijanje ISMS sertifikata, koji zahteva striktnu primenu preporučene dokumentacije, procesa i kontrola zaštite.

Standard ISO/IEC definiše ISMS kao *deo TQM sistema organizacije,* a za dobijanje sertifikata zahteva obaveznu implementaciju poglavlja 4 do 8 standarda ISO/IEC 27001. Takođe, ISO zahteva da pristup implementaciji i primeni ISMS-a u operativnoj praksi, bude isti kao u drugim ISO menadžment sistemima, tj. da se primenjuje PDCA procesni model i koriste ISO terminologija i preporučena dokumentacija.

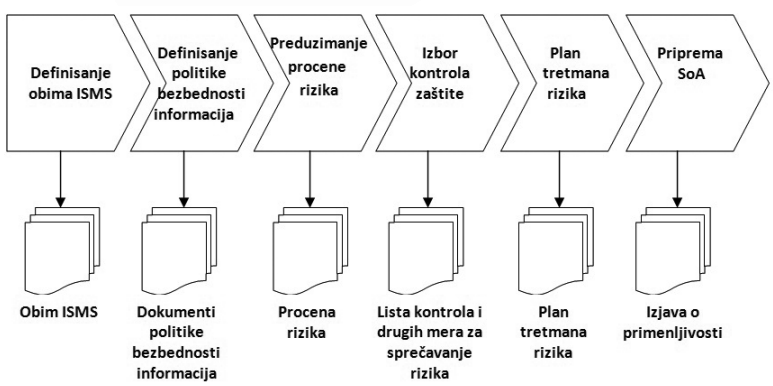
7.2 PRIMENA PDCA MODELA PROCESA U ISMS-u

Model PDCA procesa obezbeđuje implementaciju, održavanje, proveru i poboljšanje ISMS-a u kontinualnom ciklusu i balansira menadžment rizika sa operativnim ciljevima organizacije. Glavni cilj primene PDCA modela procesa je implementacija ISMS-a u TQM sistem organizacije, a *kritični faktori uspeha* su [102]:

- uključivanje glavnog menadžmenta (npr. predstavnika izvršnih direktora),
- eksplicitna podrška glavnog menadžera (npr. pisani dokument koji jasno navodi da je usaglašenost sa ISO/IEC 27001 strategijska odluka organizacije),
- smernice politike zaštite organizacije, koje preporučuju PDCA pristup,
- jasno artikulisani bezbednosni zahtevi, koji odražavaju poslovne potrebe,
- usaglašenost politike zaštite sa misijom i poslovnim ciljevima organizacije,
- sporazum sa menadžmentom o procesu implementacije ISMS,
- uspostavljanje *menadžera zaštite informacija* za ISMS i sertifikaciju,
- uspostavljanje *tima za zaštitu informacija*,
- obezbeđivanje razvoja svesti o potrebi zaštite, obuke i obrazovanja,
- uspostavljanje metrike i sistema merenja za evaluaciju performansi ISMS-a i
- generisanje izveštaja za menadžment, sa težištem na nove vrednosti.

7.3 PDCA FAZA *PLANIRANJA I USPOSTAVLJANJA ISMS*-a

Svaka faza PDCA modela ima *proizvode rada*, kao što su planska dokumenta za implementaciju, operativna (politika, procedure, standardi), dokumenta za praćenje performansi ISMS-a itd. Na slici 7.1 prikazana je faza planiranja sa dokumentima svakog (pod)procesa, koja uključuju: *okvir za menadžment zaštite* – SMF (*Security Management Framework*), *obim ISMS, politiku zaštite informacija, procenu rizika, izbor kontrola zaštite, plan tretmana rizika i SoA dokument*. Ako organizacija planira ISO/IEC 27001 sertifikaciju, ova dokumenta treba pregledati pre provere na samoj lokaciji i izraditi plan aktivnosti (**Prilog 7.1**).



Slika 7.1 Dokumentacija i proizvodi rada faze planiranje

Faze planiranja je namenjena za pripremu organizacije za implementaciju ISMS-a, a uključuje *definisanje obima i granica primene ISMS-a i ISMS politike, procenu rizika, inventar imovine i analizu poslovnih procese*. Prvi korak u fazi planiranja je definisanje obima i politike ISMS-a, uključujući procenu rizika za kritičnu imovinu, zaposlene i poslovne procese. Procena rizika identifikuje faktore rizika koji su relevantni za sve aspekte poslovanja organizacije unutar obima i granica primene ISMS-a. Izbor metoda i definisanje obima procene rizika su smernice za aktuelnu implementaciju ISMS-a. Kreiranjem SMF-a u kojem se definišu specifičnosti ISMS-a, organizacija obuhvata sva relevantna pitanja i razmatra sve aspekte SMF-a sa razumevanjem značenja i namene i specifikacijom primera za svaki bezbednosni zahtev u terminima opcija menadžmenta rizika. Standard ISO/IEC 27001 zahteva izradu dokumenta SoA, koji artikuliše ciljeve kontrola zaštite i specifične kontrole, relevantne za ISMS konkretne organizacije.

7.3.1 Definisanje obima ISMS-a

Definisanje obima ISMS-a opisuje *granice primene ISMS procesa* u odnosu na zahteve poslovanja, tipove i lokacije IKT sistema, mrežnu infrastrukturu, opremu i tehnologije i razloge za opravdanje bilo kojeg isključivanja iz oblasti primene. U odnosu na *informacije i IKT sistem,* definisanje obima ISMS-a obezbeđuje lakše upravljanje poslovnim rizikom. Obim ISMS-a, takođe, obuhvata zakonske, regulatorne ili druge zahteve za usaglašavanje i čini formalni dokument u paketu ISMS dokumentacije.

7.3.2 Definisanje politike zaštite informacija

Standard ISO/IEC 27001 definiše politiku zaštite informacija u dva dela — *ISMS politiku* i sveobuhvatnu *politiku zaštite informacija* koja uključuje skup politika zaštite različitih komponenti sistema zaštite. Standard NIST-a definiše *politiku zaštite informacija* na nivou organizacije — (*Security Policy)*, na nivou IKT sistema — (*System Specific Policy*) i na nivou komponente sistema zaštite — (*Topic Specific Polisy*) [76].

7.3.2.1 ISMS politika zaštite

ISMS politika zaštite je menadžment plan i sa slojem kontekstualne arhitekture sistema zaštite, čini osnovu ISMS menadžment sistema i nižih slojeva arhitekture, uključujući SMF okvir za adaptaciju specifične politike operativne komponente zaštite i tehničkih kontrola. Posle standarda, *ISMS politika zaštite* je drugi ključni korak u uspostavljanju bezbednosne kulture, u kojoj su svi zaposleni postaju svesni potrebe zaštite i uloge koju imaju u sistemu zaštite informacija. ISMS politika uspostavlja *okvir za menadžment rizika*, koji zahteva uspostavljanje konteksta poslovnog rizika u obimu ISMS-a, razmatranje poslovnih, zakonskih i ugovornih zahteva i uspostavljanje pristupa menadžmentu rizika i kriterijuma za evaluaciju i estimaciju faktora rizika. *Obim ISMS politike* može biti celo preduzeće, poslovna linija holding kompanije itd., sa opisom lokacija i međusobnih odnosa sa aspekta operacija, tehničke povezanosti, međuzavisnosti, ključne imovine i ključnih poslovnih proces.

ISMS politika demonstrira nameru i angažovanje menadžmenta organizacije u zaštiti informacija, a sadrži saopštenja za uspostavljanje vizije i smernica za sistem zaštite informacija i dostizanje dugoročnih i kratkoročnih ciljeva zaštite poverljivosti, integriteta i raspoloživosti informacione imovine. Takođe, sadrži saopštenja o tome šta uključiti u program implementacije ISMS-a, a šta isključiti. Za potrebe provere, saopštenja *ISMS politike* moraju eksplicitno sugerisati razmatranje svih *kontrola zaštite* iz standarda ISO/IEC 27002 i eksplicitnih razloga za sva isključivanja *kontrola*. Politika treba da sadrži namenu ISMS-a za podršku programu menadžmenta usaglašenosti sa regulativama, zakonom i drugim zahtevima, kao i saopštenja koja prenose eksplicitnu angažovanost menadžmenta, njihovu odgovornost, potrebu menadžerske provere ISMS-a i spremnosti da obezbede sve potrebne resurse za podršku programa zaštite informacija. U **Prilogu 7.2** prikazan je primer obrasca i sadržaja za izradu ISMS politike.

ISMS politika, takođe, identifikuje informacionu imovinu koju treba zaštititi, ciljeve kontrola i kontrole zaštite i stepen zahtevanog nivoa garantovane bezbednosti. Ona inicira generisanje seta dokumenata koji obezbeđuju smernice za sve aspekte ISMS-a. Ovaj set dokumenata treba da ima koherentnu strukturu hijerarhijskog tipa: *uputstvo (priručnik) za zaštitu – procedure – radne instrukcije*, koja obezbeđuje odgovarajući okvir[1].

7.3.2.2 *Sveobuhvatna politika zaštite informacija*

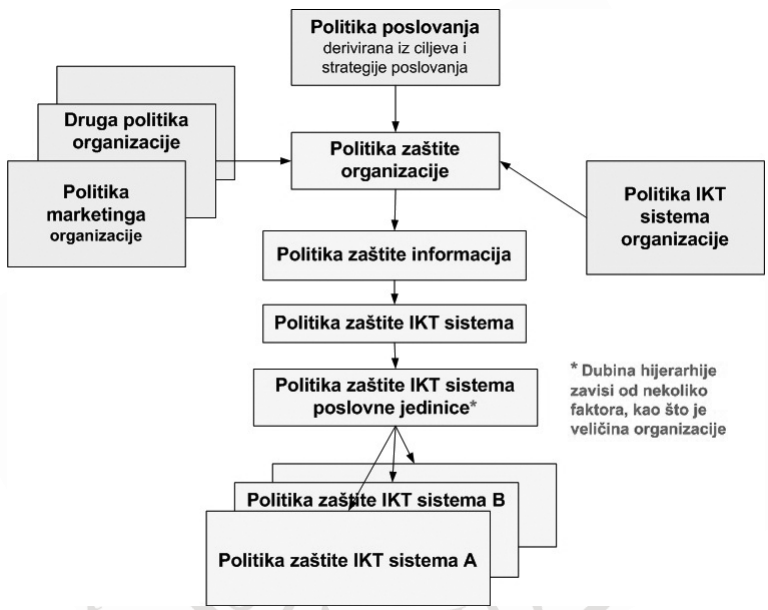
Generički, *politika zaštite informacija* treba da odražava najbolju praksu, tj. da je kratka, fleksibilna, obezbeđuje akcije i ima mehanizme za nametanje sprovođenja, da sadrži minimum specijalističkih termina i akronima i da jasnim jezikom i terminima industrijskih standarda, prenosi smernice kroz *saopštenja* i druge elemente. Hijerarhija razvoja *politike zaštite* tipične organizacije prikazana je na slici 7.2.

Fokusiranje politike na ciljne grupe korisnika na svim nivoima izvršavanja strateških i taktičkih planova i aktuelnih zadataka, obezbeđuje veću korisničku prihvatljivost. Politika zaštite je dugoročna, menja se na bazi procene rizika i ne može se vezati za životni vek proizvoda ili servisa zaštite. Specifikacije, način upotrebe itd. proizvoda i tehnologija zaštite, nalaze se u standardima i procedurama, a ne u politici zaštite. Sveobuhvatna politika zaštite informacija u organizaciji može uključivati *saopštenja* koja se odnose na brojne standardizovane i druge, promenljive komponente i aspekte zaštite i može uključivati sledeće atribute:

1. obim, namenu i ciljeve ISMS-a,
2. ISMS politiku,
3. značaj zaštite informacija za organizaciju,
4. održavanje bezbednosti informacione imovine,
5. menadžment okvir zaštite informacija u organizaciji (SMF),
6. procedure za odobravanje sistema zaštite informacija,
7. odgovornosti za zaštitu informacija,
8. procesi za kontinuitet poslovanja i testiranje sistema za proboj,
9. svest o potrebi zaštite i obuka o zaštiti informacija,

1 Engl.: Standard AS ISO 10013:2003, *Guidelines for quality management system documentation.*

10. objašnjenje o načinu izveštavanja incidenta i posledica,
11. kontrola malicioznih programa,
12. klasifikacija informacija organizacije,
13. zaštita zapisa organizacije,
14. zaštita podataka,
15. usaglašenost sa ISMS politikom,
16. tim za zaštitu i
17. kontrola pristupa.



Slika 7.2 Hijerarhija politike organizacije

U definisanju **obima ISMS-a** treba izbegavati uopštene formulacije, tipa: „*U opsegu ISMS-a je cela organizacija*". Obim ISMS treba biti specifičan – sa nazivom i adresom lokacije, opisom operacija na svakoj lokaciji, prema bezbednosnoj kategorizaciji ili organizacionoj klasifikaciji, sa opisom hijerarhijske strukture i relevantnih odnosa između glavnih delova organizacije. Iako opis obima ISMS-a treba da bude koncizan, ako sadrži više detalja — biće tačniji rezultati procesa menadžmenta rizika. Generički **cilj politike zaštite** je da svi zaposleni organizacije treba da slede ISMS politiku koja je deo ISMS menadžment sistema. U sekciji „*Ciljevi*" politike je **saopštenje o nameni** koje ukazuje na situacije koje nisu specifično obuhvaćene u politici, standardu i procedurama ili iskustvu. U slučaju neodređenosti ciljeva, treba se držati namene politike. Generička namena politike je zaštita CIA imovine.

ISMS politika zaštite na nivou organizacije je dokument, namenjen za menadžment i sve relevantne učesnike u implementaciji ISMS-a i treba da odražava jako uverenje menadžmenta da nezaštićene informacije mogu ozbiljno ugroziti poslovanje organizacije. Dokument

treba da bude kratak (nekoliko stranica), javan i namenjen za sve zaposlene. Standardi ISO vide *ISMS politiku* kao skup preporučenih politika komponenti sistema zaštite, koje mogu biti izrađene kao jedan dokument pod imenom *ISMS politika* ili kao posebni dokumenti. *ISMS politika* i politika zaštite informacija su deo okvira ukupnog menadžment sistema organizacije (TQM). Dakle, zaštita informacija i menadžment zaštite informacija su samo dva od više drugih aspekata organizacije, čiju koordinaciju i kumulativni uspeh organizacije, u velikoj meri, obezbeđuju ISO menadžment sistemi.

Saopštenje o **značaju informacione bezbednosti** za organizaciju treba da bude kratko, eksplicitno i generalno usaglašeno sa misijom, glavnim vrednostima i održivim razvojem organizacije. Može uključivati i saopštenje o efektu specifičnih kontrola iz opsega SoA dokumenta, sa fokusom na dodavanje nove vrednosti, kao i saopštenje o mehanizmu usaglašavanja i nametanja politike, sa disciplinskim i drugim merama za nesprovođenje.

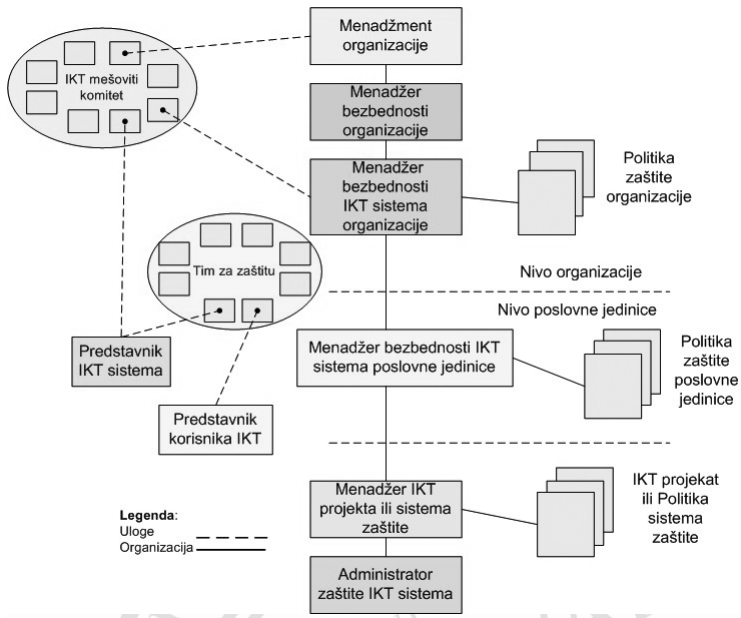
Za **održavanje procesa zaštite informacione imovine**, u politici zaštite informacija treba formalno opisati procese zaštite informacija, koji se, uglavnom, razlikuju od aktuelnog stanja procesa. Zatim, treba opisati operativni menadžment ISMS-a i ciljeve aktivnosti kao što su: *monitoring, interna, menadžerska i nezavisna provera, održavanje planova za kontinuitet poslovanja (BCP), oporavak sistema od katastrofa (DRP) i antivirusnu zaštitu*. Korisno je naglasiti potrebu za internom i menadžerskom proverom ISMS-a i kako te aktivnosti pomažu operativni menadžment ISMS-a.

Komentar o **menadžment okviru zaštite** (SMF) pretpostavlja formalni okvir, sličan ili usaglašen sa ISO/IEC standardima menadžment sistema. U kontekstu SMF, treba razmotriti integraciju ISMS-a u TQM. U SMF ISMS-a detaljnije treba opisati način implementacije i održavanja ISMS-a. Standard ISMS-a vidi angažovanje menadžmenta kao „*dokaz njihovog angažovanja za uspostavljanje, rad, monitoring, kontrolu, održavanje i poboljšavanje ISMS-a*".

Zahtevi za dokumentaciju za ISO/IEC 27001 sertifikaciju uključuju „*zapis odluke menadžmenta i dokaz da su akcije menadžmenta rizika u skladu sa odlukama menadžmenta i politikom zaštite*". Na kraju, angažovanjem glavnog menadžera organizacije obezbeđuje se razvoj *politike zaštite*, kao pokretača svih aktivnosti za implementaciju ISMS-a. Deo te politike uključuje disciplinovan pristup razvoju i implementaciji ISMS-a, opisan u fazi *implementacije* ISMS PDCA modela.

U fazi planiranja multifunkcionalni tim, sa predstavnicima menadžmenta, poslovnih procesa, IKT sistema i pravnikom organizacije, treba da izradi najveći deo plana, *smernice, sankcije* i *arbitražu* za nesprovođenje politike zaštite u procesu razvoja i implementacije ISMS-a. Većina organizacija ovaj tim naziva *tim, forum ili radna grupa za zaštitu informacija* – SWG (*Security Working Groop*) ili *tim za upravljanje kompjuterskim incidentom* – CIRT/CERT (*Computer Incident/Emergency Response Team*) [17, 110]. *Smernice* uspostavljaju politiku, obim ISMS-a i određuju ograničenja, tj. raspoložive finansijske i druge resurse. Smernice za *sankcije* i *arbitražu* su namenjene za sprečavanje potencijalnih konflikata, koji mogu nastati između operativnih zahteva i prakse zaštite, nacionalnih zakona i lokalnih regulativa itd. Za dnevni operativni rad ISMS-a, najbolje rešenje je imenovati *menadžera zaštite informacija* ili *ISMS menadžera* i jasno definisati uloge i odgovornosti svih zaposlenih, bez obzira koju hijerarhijsku strukturu organizacija ima (slika 7.3) [52].

.



Slika 7.3 Organizacija menadžment sistema zaštite

Procedura za odobravanje sistema zaštite informacija obuhvata pripisivanje uloga, kontrolisane odgovornosti (*accountability*) i koordinaciju sistema zaštite u celoj organizaciji. Ovaj proces treba opisati za celu organizaciju, čime se izbegavaju pojedinačna mišljenja i izbor nekonzistentnih i nekompletnih kontrola zaštite, često u sukobu sa operativnim ciljevima. Mešoviti tim za upravljanje sistemom zaštite informacija osigurava generisanje reprezentativnih kontrola zaštite iz različitih oblasti organizacije i omogućava sprečavanje potencijalnih administrativnih konflikata.

Opštu i kontrolisanu odgovornost (*accountability),* kao i metrički sistem za praćenje performansi i menadžment sistema zaštite informacija, treba definisati i uspostaviti centralizovano za svaku komponentu sistema zaštite, što je suprotno opštoj izjavi da je „*bezbednost informacija odgovornost ljudskih resursa ili informacione tehnologije*". Kontrolisana, individualna odgovornost obezbeđuje komunikaciju tipa „*šta si uradio i šta ćeš uraditi*?" i uvek daje bolje rezultate.

U politici zaštite treba opisati potrebu za planom **menadžmenta kontinuiteta poslovanja** (BCP), uključujući i plan za *oporavak od katastrofalnog pada sistema* (DRP) i ostale relevantne preventivne i mere za oporavak sistema. U planove treba uključiti *saopštenja* u vezi menadžmenta, odgovornosti i redovnog testiranja BCP i DRP planova, kao i preventivna testiranja sistema zaštite na proboj.

Saopštenja politike koja se odnose na **svest o potrebi zaštite, obuku i edukaciju o zaštiti informacija**, treba da uključuju sve apstraktne slojeve progresa u učenju:

svest → *razumevanje* → *primena* → *efektivna primena* → *sigurna primena.*

Svi zaposleni moraju biti svesni potrebe zaštite i treba da razumeju barem osnovne principe zaštite, što često nije slučaj. Većina zaposlenih prihvata politiku zaštite, koju u potpunosti ne razume, pa je potrebno implementirati sistem zaštite transparentan za aktivnosti korisnika.

Primer: Sestra u prijemnom odeljenju zdravstvene ustanove je svesna da treba da zaključa računar kada se privremeno udalji, jer razume da štiti privatnost pacijenata, ali ne i zahteve HIPPA standarda i zakona za tu aktivnost, što je prvi nivo razumevanja potrebe za zaštitom. Profesionalci u IKT možda neće razumeti usaglašenost standarda organizacije i standarda zaštite, ali mogu razumeti zahteve politika zaštite, što je dublji nivo razumevanja. Profesionalci za bezbednost informacija razumeju i realizuju zahteve za usaglašenost, politiku i procedure zaštite, što je najviši nivo razumevanja.

U saopštenju za **upravljanje kompjuterskim incidentom** treba opisati potrebu za uspostavljanjem infrastrukture za odgovor na kompjuterski incident i prikupljanje podataka iz aktivnosti nadzora, detekcije, izveštavanja, trijaže, eskalacije, izolacije, tretiranja, oporavka i analize osnovnog uzroka incidenta i reakcije organizacije. Treba uključiti potrebu za definisanjem posledica i standardizacijom izveštaja i načina prijave kompjuterskog incidenta. U **Prilogu 7.3** prikazan je dijagram toka procesa i metod za određivanje prioriteta reagovanja na kompjuterski incident.

Za **kontrolu malvera** (malicioznih programa) i napada na računarsku mrežu, uključujući spam, viruse, trojance i ostale poznate napade sa Interneta, treba opisati opšti metod održavanja procesa i mehanizme zaštite (npr. AV programe).

U saopštenju za **klasifikaciju informacija** treba opisati metod koji se koristi i sugerisati jednostavan sistem klasifikacije, npr. koji obuhvata tri različite klase informacija : (1) *poverljive,* samo za posebne grupe zaposlenih, (2) *interne*, za sve zaposlene i (3) *javne informacije*, za sve učesnike. Komplikovana klasifikacija stvara konfuziju i nedoslednost, pošto treba da izbalansirate prekomernu zaštitu i zahteve za izuzeća sa nedovoljnom zaštitom, kada postoji povećana pretnja za otkrivanje osetljivih informacija. Zahtevi za preveliku zaštitu mogu dovesti do toga da neki korisnici zanemare politiku zaštite, a za nedovoljnu zaštitu – do otkrivanja osetljivih informacija. Sa metodom klasifikacije informacija treba usaglasiti sve detalje o **čuvanju važnih zapisa** i opisati označavanje i rukovanje kao i nametanje primene, a za **zaštitu podataka unutar organizacije** treba obuhvatiti uskladištene, procesirane i prenošene podatke i zahtev za upravljanje identitetom i privilegijama. Autentifikacija (verifikacija identiteta) obezbeđuje svim legalnim korisnicima logički pristup IKT sistemu, a autorizacija prava pristupa i privilegije, definišu se na bazi *uloga* [30].

Usaglašavanje sa ISMS politikom, takođe, treba opisati u politici zaštite, a za više informacija referencirati se na ISO/IEC 27002 poglavlje 15. „*Usaglašavanje*". U politici zaštite treba opisati potrebu za uspostavljanjem *tima za zaštitu informacija*, uključujući zadatke tima. Više informacija o multifunkcionalnom timu nalazi se u ISO/IEC 27002, sekcija *kontrola*, 6.1.2, „*Koordinacija bezbednosti informacija*". Na kraju treba opisati potrebu za kontrolom pristupa, koja uključuje brojne aktivnosti kao što su: davanje ovlašćenja, pregled, ukidanje i proveru servisa kontrole pristupa, a više informacija o *kontroli pristupa* nalazi se u ISO/IEC 27002, *sekcija* 11.

Svih s*edamnaest* navedenih elemenata su deo dokumenta *politika zaštite informacija* i treba ih izraziti običnim, svakodnevnim i razumljivim jezikom da bi se obezbedila veća korisnička prihvatljivost. Ovaj dokument je autorski rad koji izražava strateški pravac organizacije, čije specifičnosti nisu namenjene za javnost. *Politike zaštite informacija* može biti deo dokumenta ISMS *politika*. Isticanje značaja politike zaštite informacija obezbeđuju razlog i ulaz u izradu ISMS *politike*.

Sadržaj politike zaštite informacija može varirati od organizacije do organizacije, u skladu sa profilom rizika, operativnim i radnim okruženjem i ukupnim ciljevima programa ISMS-a. Politika zaštite informacija sadrži *saopštenja* (smernice, instrukcije) i prenosi odgovore na pitanja *ko, šta, zašto, kada, gde i kako* treba da ispuni njenu namenu, kao i detalje o kreiranju politike, proveri i akreditaciji sistema i efektivnom vremenu važnosti politike. Prvo *saopštenje* politike je informacija o tome šta je politika (*šta*), zatim, o nameni (*zašto*), o obimu (*gde*) i ko je obuhvaćen smernicama politike, što se odnosi na uloge i odgovornosti za izradu, implementaciju, menadžment i proveru politike. Međutim, često je praktičnije uloge i odgovornosti pripisati u saopštenjima politike komponente zaštite, čime se u slučaju promene uloge i odgovornosti u organizaciji, menja samo ta politika, a *ISMS politika* se samo ažurira, što je delimično odgovor na pitanje kada. U **Prilogu 7.2** nalazi se primer uzorka apstraktne *ISMS politike* u formi *saopštenja* o ciljevima i samoj politici.

Sam proces pisanja politike zaštite je izvan okvira implementacije ISMS-a. Međutim, treba koristiti standardne formate za politiku, standarde i procedure, koji obezbeđuju konzistentnost, sveobuhvatnost i lakoću korišćenja/čitanja. U **Prilogu 7.4** prikazan je „*Primer obrasca za izradu politike, standarda i procedure zaštite*", a u tabeli 7.1 kratak nacrt generičke strukture sadržaja politike zaštite.

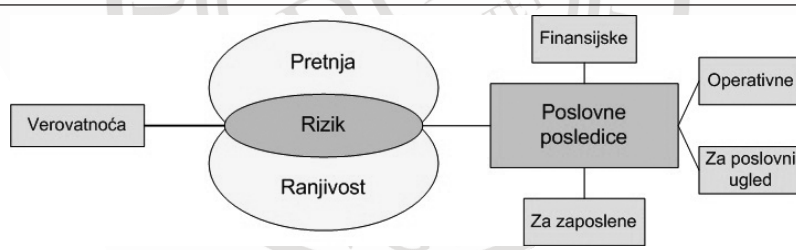
Tabela 7.1 Nacrt sadržaja politike zaštite

Nacrt sadržaja politike i procedura zaštite	**Opis/*primer teksta***
Kratkoročni bezbednosni cilj	Odabrati kontrole zaštite za smanjenje faktora rizika [*specifične*] informacione imovine.
Dugoročni bezbednosni cilj	Navesti dugoročne ciljeve politike i procedura zaštite.
Odgovornost	Pripisati odgovornost za politiku i procedure — obično vlasnik.
Namena	Proširenje uopštenih detalja za povećanje kvaliteta i bezbednosti procesa uključenih u kontrolu zaštite.
Ko, šta, kada, gde, kako	*Šta* su dugoročni ciljevi i *kako* se mogu postići? *Kada* se izvode zadaci i *ko* ih izvodi? *Gde* su oni primenljivi?
Izveštavanje	Definisanje ciljeva izveštavanja sa primerom uzoraka izveštaja za promovisanje sveobuhvatnosti i konzistentnosti.
Metrika	Identifikovanje metrike i implementacija merenja za procenu efektivnosti politike i procedura zaštite.

Politiku zaštite treba regularno ažurirati, najmanje jednom godišnje i definisati događaj koji će inicirati reviziju (npr. svakih dvanaest meseci, glavne promene itd.). Dokumentovanje svih ovih detalja osigurava *intelektualnu sinergiju* u organizaciji i opšti okvir očekivanja, kroz *uputstvo za interpretaciju SMF-a* i opšte razumevanje terminologije zaštite i menadžmenta rizika. Detaljnim dokumentovanjem zaštite organizacija sprečava da znanje i iskustva ostanu u glavama nekoliko ljudi, kada napuste organizaciju iz bilo kojeg razloga. Brojne su organizacije implementiraju sasvim dobar sistem zaštite informacija, ali nemaju ni jednu dokumentovanu proceduru. Dokumentovanjem znanja i promovisanjem učenja na bazi iskustava, organizacija obezbeđuje *dobru praksu zaštite* dostupnu za sve zaposlene.

7.3.3 Menadžment bezbednosnog rizika organizacije

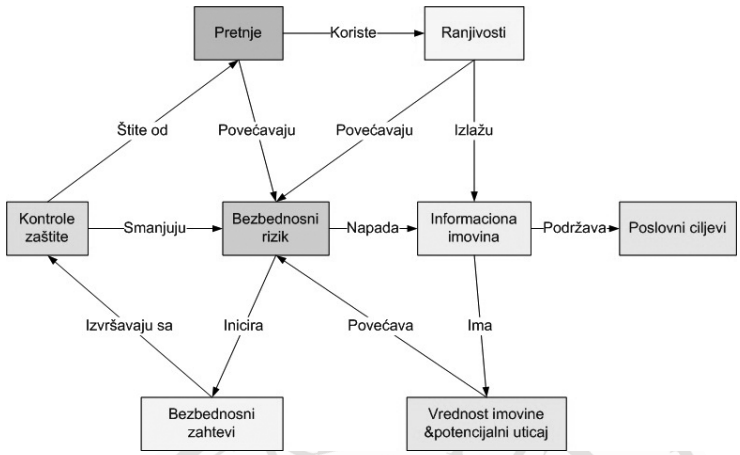
Primarna korist organizacije od zaštite informacione imovine je da izbegne gubitke zbog nedovoljne bezbednosti, koji uglavnom imaju direktnu ili indirektnu štetu. *Bezbednosni rizik za informacionu imovinu* može se definisati kao kombinacija verovatnoće bezbednosnog događaja i njegove štetne posledice. Bezbednosni događaj se javlja kada neka pretnja iskoristi jednu ili više ranjivosti i nanese negativne posledice informacionoj imovini organizacije. *Menadžment bezbednosnog rizika informacione imovine* je sistematična primena ISMS politike, procedura i prakse zaštite u zadacima i procesima uspostavljanja konteksta, identifikacije, analize, tretmana, monitoringa i komunikacije informacija o bezbednosnom riziku. Menadžment rizika je strategijski pristup bezbednosti informacione imovine (slika 7.4).



Slika 7.4 Model menadžmenta bezbednosnog rizika

Sistem zaštite informacija tretira faktore rizika tako što smanjuje verovatnoću njihove pojave ili ublažava njihove posledice i mora da obezbedi povratak investicije, jer troškovi zaštite ne mogu sami sebe opravdati. *Povratak investicije za troškove zaštite informacija* (ROSI) obično se zasniva na proceni izbegavanja gubitaka koji bi se mogli dogoditi, ako zaštite ne bi bilo [43]. Potencijalni gubici reflektuju verovatnoću realizacije rizika i očekivanih troškova za otklanjanje posledica. Međutim, poboljšani procesi menadžmenta zaštite informacija, mogu sami obezbediti ROSI, pošto zahtevaju neprekidne aktivnosti. Takođe, potrebno je razumeti i poznavati potencijalne pretnje, ranjivosti i njihove posledice — nanetu štetu informacionoj imovini. Efektivni menadžment rizika podrazumeva određivanje prioriteta, izbor i primenu adekvatnih kontrola u tretmanu rizika. Pri tome treba analizirati sve faktore rizika — koje treba i koje ne treba tretirati.

Na slici 7.5 prikazane su komponente bezbednosnog rizika i njihovi odnosi [52].



Slika 7.5 Međuzavisnosti komponenti bezbednosnog rizika

Pripremne aktivnosti menadžmenta rizika obezbeđuju informacije za razvoj arhitekture sistema zaštite i operativne politike komponente zaštite, koje zatim daju detaljnije smernice za menadžment rizika i razvoj plana zaštite. Izvršni menadžment mora odlučiti o nivou prihvatljivog rizika, što utiče na resurse za uspostavljanje i rad ISMS-a. Proces menadžmenta rizika uključuje sledeće glavne faze:

- uspostavljanje konteksta za menadžment rizika,
- identifikovanje potencijalnih faktora rizika za informacionu imovinu,
- procenu rizika (analizu i evaluaciju rizika),
- identifikovanje i evaluaciju opcija tretmana rizika i
- izbor, planiranje i implementacija rentabilnog tretmana rizika.

Implementacija ISMS-a se oslanja na efektivni menadžment rizika, tako da preporučena ISMS dokumentacija zahteva izbor metoda menadžmenta rizika[2]. U sekciji *4.2.1* standarda ISO/IEC 27001, opisan je zahtev za proces menadžmenta rizika, koji obuhvata instrukcije za:

- definisanje pristupa proceni rizika za organizaciju,
- identifikovanje rizika za organizaciju,
- analizu i evaluaciju rizika,
- izbor opcija za procenu rizika i evaluaciju svake, u odnosu na poslovne ciljeve,
- izbor ciljeva za tretman rizika organizacije,
- izbor odgovarajućih kontrola zaštite za tretman rizika i
- razvoj SoA dokumenta za svaki faktor rizika.

Proces menadžmenta rizika se sastoji od tri ključna (pod)procesa — *procene rizika, izbora kontrola zaštite i plana tretmana rizika*. U obimu ISMS-a organizacija procenjuje faktore rizika za poslovanje i informacionu imovinu sa primarnim fokusom na poslovne procese

2 ISO/IEC 13355-3, NIST SP – 80-30, ISO/IEC 27005, CRAMM, OCTAVE, BAR — brza analiza rizika itd.

i funkcije, kritične za misiju i poslovne ciljeve. Kritični procesi i funkcije obezbeđuju servise za misiju i donose nove vrednosti, a ostali su — za njihovu podršku. Podela poslovnih procesa i funkcija na kritične i za podršku, omogućava različite stepene njihove zaštite, tj. primenu kontrola za *osnovni, srednji* ili *najviši nivo* zaštite. Ako su poslovni procesi i funkcije u primarnom fokusu za procenu rizika, onda su u sekundarnom fokusu — ljudi koji ih izvršavaju, informacije, IKT sistem infrastruktura i radno okruženje. Procena rizika počinje sa procenom kritičnih procesa i identifikovanjem ključnih uloga i tehnologija za njihovo izvršavanje. Svi procesi, funkcije, uloge ili tehnologije, koje nisu ključne, čine podršku. Kritični faktori su zaposleni, tehnologije i infrastruktura koju koriste u izvršavanju ključnih procesa. Posle identifikovanja ključne i imovine za podršku, tim identifikuje i bira opcije za menadžment rizika — *prihvatanje, deljenje, prenos ili ublažavanje rizika,* a zatim, vrši izbor i implementaciju kontrola zaštite. U praksi zaštite informacija postoji više pristupa za procenu rizika (tabela 7.2).

Tabela 7.2 *Pristupi proceni rizika*

Pristup	Kratak opis
1.	usmeren na *hardversku imovinu i* procenu ranjivosti i uticaj na CIA informacija
2.	usmeren na *pretnje* i evaluaciju imovine koja ima najveću verovatnoću napada
3.	usmeren *na ključne poslovne procese i funkcije* i identifikaciju ključne podrške.

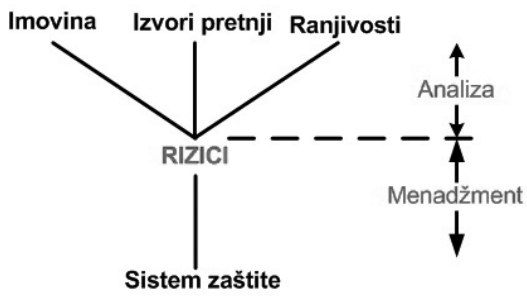
Tipični *bezbednosni ciljevi* procene rizika su — *identifikovati potencijalne pretnje, ranjivosti i faktore rizika i utvrditi verovatnoće da pretnja/e iskoriste ranjivosti i da negativno utiču na poslovanje*. U kontekstu ISMS-a, menadžment rizika treba da obuhvata barem zahteve iz sekcije *4.2.1* standarda ISO/IEC 27001, koji uključuju:

- definicije pristupa i metoda za procenu rizika,
- formalni plan za procenu rizika,
- vreme procene rizika, tj. identifikovanje perioda u godini,
- učestanost procene rizika, npr. najmanje na dvanaest meseci,
- pregled i dopunu pristupa i metoda za procenu rizika,
- procenu rizika,
- ažuriranje izjave o primenljivosti (SoA) i
- ažuriranje akcija koje proističu iz rezultata procene rizika.

Nezavisna analiza rizika može dati objektivnu procenu, ali je u nekim tipovima organizacija neprihvatljiva. Procena rizika može biti neinvazivna u odnosu na operativne procese, ali, ipak, oduzima vreme i zahteva angažovanje menadžera, administratora, operatera i ostalih zaposlenih. Koordinacija svih aktivnosti obezbeđuje se izradom *plana za procenu rizika* sa eksplicitnim zahtevom za aktivno angažovanje svih relevantnih učesnika. Neki autori preporučuju deljenje aktivnosti procesa procene rizika na korake, gde se svaki korak odnosi na određeni aspekt, a aktivnosti se mogu izvršavati paralelno.

U praksi zaštite termin *menadžment rizika* često se koriti jedinstveno i obuhvata menadžment i analizu rizika (slika 7.6).

Glavna aktivnost u menadžmentu rizika je identifikacija i izbor skupa kontrola zaštite za optimalni nivoi zaštite ili redukciju procenjenog rizika na prihvatljivi nivo. Standard ISO/IEC 27001 ne obuhvata detaljan opis metodologije za procenu bezbednosnog rizika. Za izbor i razvoj specifične metodologije za procenu rizika, mogu se koristiti standardi, kao što su ISO/IEC/IEC TR 13335-3, ISO/IEC 27005, NIST SP 800-30. Prema standardu ISO/IEC 27005 proces uspostavljanja *konteksta za analizu rizika* odvija se kroz četiri osnovne faze:



Slika 7.6 Pojednostavljeni odnosi i tok podataka u procesu menadžmenta rizika u IKT

1. definisanje osnovnih parametara za upravljanje rizikom,
2. definisanje obima i granica analize i procene rizika,
3. uspostavljanje i organizacija tima za menadžment rizika i
4. uspostavljanje strukture i procesa za analizu i procenu rizika.

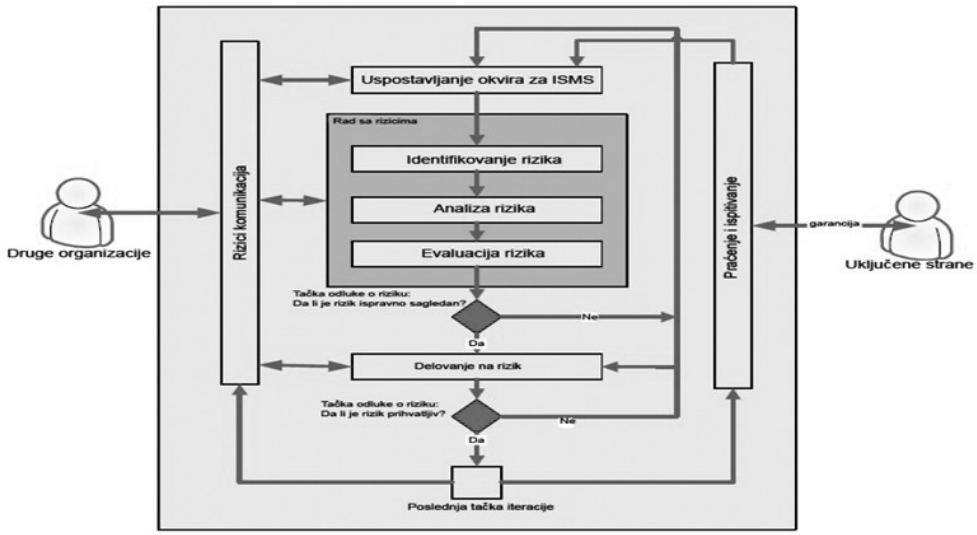
Definisanje parametara za upravljanje rizikom uključuje *izbor odgovarajućeg pristupa za procenu rizika i potencijalno raspoloživih resursa* za uspostavljanje tima za menadžment rizika, kao i *definisanje kriterijuma za: evaluaciju, procenu uticaja i prihvatanje rizika*. *Definisanje obima procesa menadžmenta rizika* uključuje strateške i kratkoročne poslovne ciljeve, procese, strategiju i politiku zaštite organizacije, legalne i normativne zahteve, oblast primene i razloge za isključivanje nekog objekta iz procesa. *Definisanje granica* procesa uključuje poslovne ciljeve i politiku, imovinu, socijalno-kulturološko okruženje i poslovne procese i aktivnosti. *Uspostavljanje i organizacija tima za menadžment rizika* uključuje identifikaciju i analizu relevantnih učesnika, izbor lidera i članova tima, definisanje uloga i odgovornosti i uspostavljanje zahtevanih odnosa i komunikacije. *Struktura procesa menadžmenta rizika uspostavlja* se u odnosu na strateške poslovne ciljeve organizacije, a obuhvata *uspostavljanje konteksta za menadžment rizika, identifikovanje, analizu, evaluaciju i procenu rizika, tretman rizika i prihvatanje preostalog rizika* (slika 7.7).

U praksi zaštite koriste se četiri osnovna metoda za estimaciju rizika, koja se u osnovi zasnivaju na generičkoj metodologiji, ali imaju različite fokuse i estimacije [58]:

- metod matrice rizika sa predefinisanim vrednostima (ISO/IEC 13335-3);
- metod merenja rizika rangiranjem pretnji prema rezultatima procene rizika;
- metod procene verovatnoće uticaja i mogućih posledica i
- metod distinkcije između prihvatljivog i neprihvatljivog rizika.

Potencijalno prihvatljiva metodologija za menadžment i procenu bezbednosnog rizika *za informacionu imovinu* je metodologija od 12 koraka[3] (tabela 7.3) [102].

3 Standard NIST SP 800-30.



Slika 7.7 Struktura procesa menadžmenta rizika

Tabela 7.3 *Proces menadžmenta rizika*[4]

Korak	Performanse	Opis
1.	Lista informacione imovine	Procenu rizika početi popisivanjem važnih informacija o imovini koja podržava ključne poslovne funkcije.
2.	Bezbednosna kategorizacija imovine	Kategorizacija omogućava određivanje prioritetne imovine kritične za poslovanje, kao i analizu pretnji i ranjivosti, koja je neophodna za visoko kritičnu imovinu.
3.	Procena ranjivosti	Identifikovati ranjivosti imovine na osnovu informacija iz liste imovine vlasnika, napravljene pre procene rizika.
4.	Procena pretnji	Prepoznati pretnje i identifikovati ih pre incidenta, a gde je pretnja ostvarena, proceniti verovatnoću ponavljanja pretnje. Pregledati iskustva iz baza znanja.
5.	Procena uticaja pretnji	Proceniti verovatnoću da će pretnja dovesti do narušavanja sistema bezbednosti informacija.
6.	Procena verovatnoće iskorišćenja ranjivosti	Proceniti da li specifična pretnja može iskoristiti ranjivost.
7.	Procena sistema i politike zaštite	Proceniti efektivnost sistema zaštite i sprovođenja tekuće ili planirane politike zaštite.
8.	Procena verovatnoće	Proceniti verovatnoću realizacije pretnje i pregledati analize stanja informacione bezbednosti sličnih kompanija.

4 Primer dobre baze znanja: CSI / FBI *Computer Crime Survey,* www.gocsi.com).

Korak	Performanse	Opis
9.	Procena uticaja	Proceniti uticaj iskoristive ranjivosti nekom pretnjom. Vrednost uticaja se određuje stepenom intenziteta datog faktora rizika, odnosno: **uticaj** = **pretnja** × **ranjivost.**
10.	Procena faktora rizika	Rizik je verovatnoća da će neka pretnja/e iskoristiti ranjivost i negativno uticati na informacionu imovinu organizacije, tj. **rizik = verovatnoća** × **uticaj**.
11.	Plan tretmana (ublažavanja) rizika	Ovaj dokument je deo ISMS dokumentacije i obuhvata faktore rizika za kritične operacije, koje je potrebno smanjivati kroz implementaciju *kontrola zaštite.*
12.	Izbor *kontrola zaštite*	Izabrati kontrole zaštite iz standarda (ISO/IEC 27002 ili NIST SP 800-53 A, B, C) za smanjenje faktora rizika.

Korak 1: Lista informacione imovine

Prvi korak u procesu menadžmenta rizika je imenovanje menadžera i vlasnika informacija, identifikacija i popis ključne *informacione imovine* na svakoj lokaciji unutar obima i granica primene ISMS-a. Resursi za zaštitu ne obezbeđuju apsolutnu zaštitu sve imovine u svakom trenutku, pa identifikovanje ključne imovine obezbeđuje upotrebu ograničenih resurse zaštite. Imovina se može identifikovati kao ključna, utvrđivanjem uticaja gubitka *CIA* na ispunjenje misije i ključnih poslovnih ciljeva — ako je uticaj kritičan, onda je to ključna imovina. U identifikovanju ključne *informacione imovine* za procenu rizika, mogu pomoći šema klasifikacije informacija i zakonske obaveze zadržavanja evidencija. Drugi bitni pokretači za procenu rizika mogu biti *ključni poslovni procesi, zaposleni i infrastruktura (IKT sistem, zgrade, softver, oprema), informacije od vrednosti za organizaciju, brend i ugled organizacije*. Dobru metodologiju za procenu kritičnih procesa i imovine organizacije nudi metod analize rizika i evaluacije ranjivosti od operativno kritičnih pretnji za imovinu organizacije — OCTAVE (*Operationally Critical Threat, Assets and Vulnerability Evaluation*) [48, 81].

Za izradu inventara informacione imovine mogu se koristiti poslovne informacije, upitnici i intervjui. Tim za zaštitu pregleda listu imovine, po potrebi menja, preporučuje i odobrava, a menadžment kontroliše i odobrava konačni spisak.

U tabeli 7.4 dat je uzorak sadržaja liste informacione imovine, koja može varirati, zavisno od tipa organizacije i oblasti rada. Referentni broj obezbeđuje jedinstveni identifikator za svaku imovinu, a atributi imovine uključuju *opis, specifikaciju vlasnika, korisnike, lokaciju, kritičnost i faktor rizika*.

Tabela 7.4 *Uzorak sadržaja liste informacione imovine organizacije*

Broj ref.	Korisnici imovine	Tip imovine	Vlasnik imovine
A1	Ime/org. jedinica	Opis	Lokacija
	Kritičnost	Faktor rizika	

Korak 2: Kategorizacija informacione imovine

Visoko kritična imovina je primarni deo procene rizika, pa imovinu organizacije treba klasifikovati po kategorijama *vrednosti za poslovne procese*. Imovina niske *vrednosti* za poslovanje, takođe, mora biti uključena u proces procene rizika. Kategorizacija informacione imovine obezbeđuje uvid u kritičnost imovine za poslovne procese, a počinje sa osnovnim pregledom kojim se utvrđuje da li imovina zahteva dodatnu analizu. Ovaj pregled obuhvata svojstvenu vrednost imovine kao i vrednost poslovne funkcije te imovine, tj. da li imovina podržava ili obezbeđuje ključni servis poslovnom procesu? Primer vrednovanja informacione imovine dat je u **Prilogu 7.5.** Kategorizacija informacione imovine vrši se u fazi analize rizika i obezbeđuje ulazne veličine za plan kontinuiteta poslovanja i oporavka sistema posle pada. U tabeli 7.5 dat je primer kriterijuma za kategorizaciju informacione imovine.

Tabela 7.5 *Primer kriterijuma za kategorizaciju informacione imovine*

Rizik	Uticaj
K1	**Veliki uticaj**: šteta ili gubitak poverljivosti, integriteta ili raspoloživosti informacione imovine ima veliki uticaj na normalan rad. Najduži podnošljiv ispad je 24 sata ili manje. Kritičan faktor je veoma visok sa vrednošću K1.
K2	**Pravni uticaj**: šteta ili gubitak poverljivosti, integriteta ili raspoloživosti informacione imovine ima pravno dejstvo. Imovina je relevantna za pravne zahteve i važna za organizaciju. Najduži podnošljiv ispad je 24 do 72 sata. Kritičan faktor je visok sa vrednošću K2.
K3	**Mali uticaj**: šteta ili gubitak poverljivosti, integriteta ili raspoloživosti informacione imovine ima mali uticaj na normalan rad. Najduži podnošljiv ispad je 73 sata do 6 dana. Kritičan faktor je nizak sa vrednošću K3.
K4	**Bez uticaja**: šteta ili gubitak poverljivosti, integriteta ili raspoloživosti imovine nema uticaj na normalan rad. Najduži podnošljiv ispad je 7 ili više dana. Kritičan faktor je veoma nizak sa vrednošću K4.

Kategorije kritičnosti (K1 do K4), za najkritičniju imovinu za organizaciju K1 i K2, zahtevaju detaljnu analizu, procenu (održavanja, nadzora, ublažavanja i oporavka) i smanjenje rizika. Kategorizacija informacione imovine je deo dokumentacije zaštite koju proveravač obavezno pregleda u procesu provere usaglašenosti sa ISO/IEC 27001 standardom. Na bazi ovog primera svaka organizacija treba da proceni vrednost *velikog i drugih negativnih uticaja* za svaku imovinu. Ako organizacija nema sopstvenu metodologiju za bezbednosnu kategorizaciju, može koristiti smernice iz FIPS publikacije 199[5] i literature [7].

U tabeli 7.6 prikazana je šema za vrednovanje rizika, odnosno, *zbirno evidentiranje informacija o imovini, poslovnim procesima koje imovina podržava, ranjivostima, pretnjama i relevantnim vrednovanjima*. Svaku imovinu treba vrednovati u odnosu na pretnje, verovatnoću pojave pretnje, nivo ranjivosti, sistem zaštite, verovatnoću uticaja i rizika.

5 Engl.: NIST, *FIPS 199*, http://www.itl.nist.gov/fipspubs, 2009.

Tabela 7.6 *Obrazac za evaluaciju i vrednovanje rizika*

Broj reference	**Imovina:**		
Vlasnik imovine:		Kritična vrednost:	
Korisnici imovine:			
Opis imovine (ime, lokacija, tip, mreža, komunikacije, bezbednosna kategorija):			
Podržane poslovne funkcije:			
Lista pretnji	Lista ranjivosti		
Vrednost pretnji:	Vrednost ranjivosti:	Vrednost zaštite:	
Vrednost verovatnoće:	Vrednost uticaja:	Faktor rizika:	
Ostale informacije kao i akcije koje treba preduzeti:			

Korak 3: Procena ranjivosti

Koraci od tri do deset definišu analizu i procenu komponenti rizika za svaku pojedinačnu imovinu. Taksonomija ranjivosti ključne imovine obuhvata *tehničke elemente* (npr. softver, hardver), *prirodne fenomene* (npr. oluja, poplava), *eksterne događaje* (npr. snabdevač zatvara firmu) i *ljude* (npr. ključno znanje ostaje nezabeležno). Za efikasnu procenu treba razmatrati sledeće kategorije ranjivosti informacione imovine:

- *informacija u svim formatima* (intelektualna svojina, zaštita privatnosti itd.),
- *hardverske opreme* (IT, mrežne infrastrukture, opreme za ključne poslove),
- *procedura* (menadžmenta, operacija, administracije, podrške),
- *zaposlenih i*
- *eksternih faktora zavisnosti*.

U tabeli 7.7 data je lista primera ranjivosti koje treba evidentirati u obrazac za evaluaciju (tabela 7.5). Specifični detalji se odnose na *tip i lokaciju imovine, poslovne procese koje podržava i vlasnika ili osobu odgovornu za imovinu*.

Tabela 7.7 *Primer dokumentovanja ranjivosti*

Ranjivost	**Uzrok**	**Stanje**
stres	nestabilna električna energija	bez promena; kontrola upravljanja na mestu
nedostatak fizičke zaštite	nezaštićene linije veze	nedostatak dokumentacije
spoljni saradnik bez nadzora	odsustvo zaposlenog	bez BCP-a na lokaciji
nedostatak obuke	nezaštićeno skladištenje	pogrešne pretpostavke

Ranjivosti treba posmatrati u kontekstu poslovnih ciljeva i procesa organizacije, a ranjivosti kritičnih informacija u svim formatima i ostale kritične informacione imovine, u odnosu na gubitak CIA. Eksterne zavisnosti su svi faktori, kritični za ostvarivanje očekivanih rezultata poslovanja organizacije.

Primer: Prekid snabdevanja sirovinama proizvođača uređaja, koji može uključivati vezane ranjivosti, kao što su performanse aplikacije za podršku snabdevanja sirovinama, automatizacija narudžbina, obračun troškova i raspoloživost goriva za transport sirovina, štrajkovi, promene u okruženju itd. Iako se sve ranjivosti ne odnose na bezbednost informacija, odnose se na poslovni rizik i zahtevaju procenu rizika.

Korak 4: Procena pretnji

Procena ranjivosti obezbeđuje primarni uvid u pretnje u oblasti primene ISMS-a. Npr. za organizaciju na velikoj nadmorskoj visini pretnja od poplava nije ranjivost, ali gubitak električne energije usled oluje — jeste. U tabeli 7.8 dati su primeri pretnji.

Tabela 7.8 Primeri pretnji

greške osoblja	kvar	voda
vatra	greška u održavanju	vreme
prašina	softverska greška	zemljotres
sabotaža	nasilan ulaz	prekid strujnog kruga

Sve pretnje, svaku pojedinačnu imovinu, treba evidentirati u obrascu za evaluaciju rizika (tabela 7.6). Pre vrednovanja svake pojedinačne imovine, treba mapirati pretnje sa procenjenim ranjivostima. U tabeli 7.9 dat je primer mapiranja parova *pretnje – ranjivosti* za datu imovinu. Na primer, može se desiti nasilni ulaz zbog nedostatka fizičke zaštite ili greška u održavanju zbog napetih, frustriranih i preopterećenih radnika ili nedostatka smernica i procedura. Nakon mapiranja pretnji sa ranjivostima i evidentiranja rezultata u obrascu za evaluaciju (tabela 7.6), počinje vrednovanje parametara za procenu rizika.

Tabela 7.9 *Naziv imovine <naziv>*

Pretnja	Ranjivost
nasilan ulaz	nedostatak fizičke zaštite
greška u održavanju	stres i nedostatak dokumentacije
sabotaža	nezaštićene komunikacione linije

Stablo pretnji, lista tipičnih pretnji (tabela P 7.5.1) i humanih pretnji (tabela P.7.5.2), prema standardu ISO/IEC 27005 date su u **Prilogu 7.6,** a tipični parovi pretnje/ ranjivosti prema standardu ISO/IEC 27005 prikazani su u **Prilogu 7.7.**

Korak 5: Vrednovanje pretnji

Procenom verovatnoće da će neka pretnja dovesti do povrede sistema zaštite informacija, vrednuju se pretnje. Za vrednovanje pretnji mogu se koristiti informacije iz tabele 7.6, istorijskih podataka organizacije i tuđih iskustava, pri čemu se traže odgovori na pitanja, kao što su: *Da li u organizaciji ranije realizovala tekuća pretnja? Kolika je učestalost pojave pretnje*? *Postoje li slične organizacije koje imaju iskustva sa ovom pretnjom? Postoje li raspoloživi podaci o učestalosti pojave pretnje? Da li su te organizacije slične ovoj (npr. fizička blizina, zajedničke prirodne pretnje i sl.)?* U Tabeli 7.10. dati su primeri smernica za vrednovanje pretnji.

Tabela 7.10 *Smernica za procenu pojave pretnje i štete za organizaciju*

P	Opis i verovatnoća
N	**Istorija**: ova pretnja nije narušila bezbednost informacione imovine u toku prošle godinu, a malo je verovatno da će se dogoditi. **Verovatnoća**: okruženje ili znanje i rezonovanje nisu bili preduslov da se pretnja za narušavanje bezbednosti dogodi, a malo je verovatno i da će se dogoditi.
R	**Istorija**: ova pretnja za narušavanje bezbednosti nije se pojavila u protekla tri meseca. **Verovatnoća**: okruženje ili znanje i rezonovanje su malim delom ili retko preduslov da se dogodi pretnja za narušavanje bezbednosti.
I	**Istorija**: ova pretnja za narušavanje bezbednosti se pojavila u protekla tri meseca i verovatno je da će se ovo ponoviti. **Verovatnoća**: okolina ili znanje i rezonovanje bili su preduslov da se dogodi pretnja za narušavanje bezbednosti i verovatno je da će se ovo ponoviti.

Kod vrednovanja pretnje, treba proceniti koliko je realno da pretnja izazove gubitak CIA-e informacione imovine. Za evidentiranje verovatnoće pojave pretnje (**P**) mogu se primeniti različiti stepeni gradacije, na primer: **N** (*neizvesno*), **R** (*retko*), **I** (*izvesno)*. Procenitelj evidentira rezultat vrednovanja u obrascu za evaluaciju rizika (tabela 7.6) za svaku imovinu. Treba zapaziti da različiti metodi vrednovanja pretnje koriste različite vrednosti merenja, npr., *kvantitativni metod* vrednovanja rizika (prema Tabeli 7.6) zahteva numeričke vrednosti gradacije pretnje, umesto kvalitativne skale (**N, R** i **I**), a može se ilustrovati matematičkom relacijom: ***pretnja* × *ranjivost* = *uticaj; verovatnoća* × *uticaj* = *rizik***.

Korak 6: Vrednovanje ranjivosti

Ranjivosti ključne informacione imovine vrednuju se na bazi rezultata mapiranja pretnje — ranjivosti, evidentiranih u obrascu za evaluaciju (tabela 7.6). Za svaku imovinu, treba vrednovati koliko je realno da pretnja iskoristi specifičnu ranjivost i nanese štetu ili izazove gubitak CIA-e. Izmerene vrednosti u ovom slučaju mogu se gradirati sa (tabela 7.11): **N** (*niska*), **S** (*srednja*) i **V** (*visoka*). Rezultate evaluacije iz abele 7.6 treba evidentirati za svaku pojedinačnu imovinu. Može se primeniti i alternativna skala sa većom granulacijom (npr. N, S-N, S, S-V, V), Za kvantitativno izračunavanje verovatnoće rizika može se koristiti numerička skala (npr. 1, 2, 3, 4, 5).

Tabela 7.11 *Primer kvalitativne procene da će pretnja/e iskoristiti ranjivost*

P	Opis
N	Ranjivost je mala i malo je verovatno da je neka pretnja može iskoristi i naneti gubitak CIA-e imovine.
S	Ranjivost postoji i može se otkriti, a pretnja je može iskoristiti i naneti gubitak CIA-e imovine.
V	Ranjivost je velika i pretnja je lako može iskoristiti i naneti gubitak CIA-e imovine.

Korak 7: Vrednovanje sistema zaštite i implementirane *politike zaštite*

U ovom koraku treba pregledati politiku i kontrole zaštite za svaku imovinu i utvrditi da li je zaštita dovoljna, tako da pretnje ne mogu iskoristiti ranjivosti i izazvati gubitak CIA-e imovine. Kategorije sistema zaštite obuhvataju *fizičke* (primeri u tabeli 7.12), *tehničke* (hardversko-softverske), *personalne* i *proceduralne* kontrole zaštite.

Tabela 7.12 *Primeri kontrola fizičke zaštite*

Spoljašnje barijere	Kontrole ulaza na posed	Ograde
kapije	čuvari	kamere za nadzor
vrata na ulazu u zgradu	ključevi, brave sa šifrom, kartice za prolaz, biometrika za kontrolu ulaza	vrata kancelarija i centra za obradu podataka
detektori za požar	detektori poplava	zidovi otporni na bombe
čuvari	alarm za provalnike	rezervno napajanje

Tabela 7.13 predstavlja primere nekoliko opštih *tehničkih kontrola* za fizičku i logičku zaštitu informacione imovine — servera, mrežne infrastrukture (rutera, habova, svičeva, kablova) i medija (čvrstih diskova, CD-a, USB-e, trake za arhiviranje itd.).

Tabela 7.13 *Tehničke kontrole sistema zaštite*

Plan za oporavak sistema u slučaju pada	Detekcija malicioznog softvera (*malvera*)
testiranje sistema zaštite	tragovi za pregled (*audit*) i logovi
lozinke i autentifikacija	logička barijera (*Firewall*)
sistemi za detekciju i sprečavanje upada (IDPS)	tim za odgovor na incidente
mehanizmi za šifrovanje/dešifrovanje	virtualne privatne mreže (VPN)
mehanizmi zaštite operativnog sistema	upravljanje unutrašnjim pretnjama

Primeri *kontrola personalne zaštite* prikazani su u tabeli 7.14. Cilj je da se zaposle ljudi sa niskim ili da se izbegne zapošljavanje ljudi sa visokim bezbednosnim rizikom. Takođe, ne treba zapošljavati određenu klasu ljudi na neke pozicije. Pored toga, cilj ove komponente zaštite je da zaposleni postanu svesni svojih odgovornosti u sistemu zaštite i da dobiju adekvatnu obuku i obrazovanje.

Tabela 7.14 *Personalna zaštita*

Provera pre zapošljavanja	Sporazum o poverljivosti
svest zaposlenog o potrebi zaštite	opis posla
politika personalne zaštite	etički programi

U tabeli 7.15 dati su primeri proceduralnih *kontrola zaštite*. Procedure obezbeđuju: *dobru praksu zaštite; smanjuju zavisnost od stanja svesti o potrebi zaštite, obuke, samoinicijative i veštine pojedinaca; sadrže brojna iskustva iz različitih aspekata zaštite organizacije i promovišu doslednost, principijelnost i sveobuhvatnost*.

Tabela 7.15 *Primeri procedura zaštite*

Procedura	Opis
Planiranje kontinuiteta poslovanja (BCP)	bezbednost radnih grupa; bezbednost menadžmenta; struktura za bezbednosnu procenu;
Procena usaglašenosti	karakteristike politike i procedura zaštite (npr. lozinke, šifrovanje uskladištenih i prenošenih podataka);
Plan zaštite od malicioznih programa	kontrola i izveštavanje o incidentima;
Politika zaštite informacija	ISMS politika;
Kontrola pristupa	integrisana fizičko – logička kontrola pristupa IKT sistemu.

U tabeli 7.16 date su smernice za vrednovanje metoda zaštite za *nisku*, *srednju* i *visoku* procenu. Utvrđivanje kvaliteta implementiranog sistema zaštite obezbeđuje osnovu za kasnije korektivno delovanje.

Tabela 7.16 Vrednovanje metoda implementiranog sistema zaštite

Vrednost	Kriterijum za procenu
Niska (**N**)	Ako je sveukupna zaštita 60% ispod moguće, sistem zaštite nije prihvatljiv.
Srednja (**S**)	Ako je sveukupna zaštita između 60% i 70% moguće zaštite, sistem zaštite je prihvatljiv, ali je potrebno izvršiti reviziju određenih aspekata zaštite.
Visoka (**V**)	Ako je sveukupna zaštita viša od 70% moguće, sistem zaštite je kvalitetan.

Korak 8: Procena verovatnoće

U ovom koraku utvrđuje se verovatnoća da će pretnja/e iskoristiti ranjivost. Izraz *verovatnoća* može se odnositi na matematičku vrednosti ili na subjektivnu procenu. Matematička vrednost verovatnoće daleko je složenija i teško je odrediti tačnu vrednost. Subjektivna procena verovatnoće se lakše definiše i često je dovoljno dobra za praktične zadatke. Za subjektivno, kvalitativno vrednovanje verovatnoće koriste se sledeće skale gradacije:

- *pretnji:* **N** (neizvesno), **R** (retko) ili **I** (izvesno);
- *ranjivosti:* **N** (niska), **S** (srednja) ili **V** (visoka) i
- *sistema zaštite*: **N** (niska), **S** (srednja) ili **V** (visoka).

Kombinacija ovih vrednosti obezbeđuje procenu *verovatnoće faktora rizika* (tabela 7.17). Prvo treba pronaći procenjenu vrednost pretnje u gornjem redu: **N, R** ili **I**, zatim, pronaći procenjenu vrednost za ranjivost u drugom redu: **N. S, V**, a na kraju — procenjenu vrednost za metod sistema zaštite u levoj koloni: **N, S, V**.

Tabela 7.17 *Matrica za vrednovanje verovatnoće faktora rizika*

Pretnje		Neizvesno (**N**)			Retko (**R**)			Izvesno (**I**)		
Ranjivost		N	S	V	N	S	V	N	S	V
Metod zaštite	**V**	G	F	E	F	E	D	E	D	C
	S	F	E	D	E	D	C	D	C	B
	N	E	D	C	D	C	B	C	B	A

Verovatnoća faktora rizika za procenjene vrednosti pretnje, ranjivosti i sistema zaštite, nalazi se u ćeliji matrice gde se ove tri vrednosti seku, a označava slovima **A** do **G**, gde **A** ima najveću, a **G** — najmanju verovatnoću rizika za informacionu imovinu. Dobijene verovatnoće faktora rizika interpretiraju se na sledeći način:

- **A** – redovno ili često 6
- **B** – često 5
- **C** – izvesno 4
- **D** – povremeno 3
- **E** – retko 2
- **F** – neizvesno 1
- **G** – veoma neizvesno 0

Korak 9: Procena uticaja

U analizi uticaja faktora rizika razvija se scenario "*šta ako*" za svaki razmatrani faktor rizika, tj. potencijalni uticaj pretnje koja iskoristi ranjivost, na poslovne procese posle gubitka CIA-e informacione imovine. Procenjuje se verovatnoća pojave i intenzitet uticaja svakog faktora rizika, kao i njihove kombinacije. Pri tome svojstvena vrednost imovine nije toliko važna koliko vrednost poslovnog procesa, koji od nje zavisi. Ako se razmatraju *zavisnosti*

između predmetne i ostalih objekata imovine, predmetna imovina se može ukloniti iz podrške ključnim poslovnim procesima, ali *zavisnost* i dalje ostaje kritična.

U tabeli 7.18 prikazane su smernice za utvrđivanje vrednosti uticaja sa gradacijom *nizak* **(N),** *srednji* **(S),** *visok* **(V)**. Rezultate treba evidentirati u obrascu za evaluaciju rizika (tabela 7.6). Uticaj se određuje u odnosu na vrednost imovine i potencijalni gubitak poslovnih operacija, usled gubitka poslovnih procesa koje imovina podržava.

Tabela 7.18 *Smernica za utvrđivanje vrednosti uticaja rizika*

	Opis
Uticaj	Nastaje kada pretnja iskoristi ranjivost i dovede do povrede ili gubitka poverljivosti, integriteta ili raspoloživosti imovine i nanese štetu organizaciji.
N	Uticaj na povredu ili gubitak poverljivosti, integriteta ili raspoloživosti imovine ili imidž organizacije ili brend, je minimalan.
S	Uticaj na povredu ili gubitak poverljivosti, integriteta ili raspoloživosti imovine ili imidž ili brend organizacije, postoji, ali se ne smatra skupim i kritičnim.
V	Uticaj na povredu ili gubitak poverljivosti, integriteta ili raspoloživosti imovine ili imidž ili brend organizacije, postoji i smatra se veoma skupim i kritičnim.

Korak 10: Procena faktora rizika

U 10. koraku dodeljuje se faktor rizika svakoj imovini. U tabeli 4.19 date su smernice za određivanje faktora rizika. Pronađe se vrednost uticaja iz devetog koraka u gornjem redu (**N, S, V**), zatim, vrednost verovatnoće iz obrasca za evaluaciju (tabela 7.6), dobijene u koraku 8 za tu imovinu (**A — G**). Ubace se vrednosti uticaja iz tabele 7.18 i vrednosti za verovatnoću rizika iz tabela 7.17 u tabelu 7.19. Numerička vrednost u preseku ovih vrednosti je faktor rizika.

Tabela 7.19 *Matrica za određivanje faktora rizika*

Uticaj		**Nizak (N)**	**Srednji (S)**	**Visok (V)**
Verovatnoća	G	0	1	2
	F	1	2	3
	E	2	3	4
	D	3	4	5
	C	4	5	6
	B	5	6	7
	A	6	7	8

Ako je faktor rizika **4** ili veći, preporuka je da se faktor rizika smanji implementacijom *kontrola zaštite*. Izolovana procena vrednosti imovine, sama po sebi nije značajna; od šireg interesa je vrednost poslovnog procesa i funkcije, koje imovina podržava. Osnovne metodologije procene rizika se fokusiraju na imovine (*interni fokus*), ili na pretnje (*eksterni i interni*

fokus) ili na *poslovne procese* koji dodaju novu vrednost. Fokus na *ključne* poslovne procese smanjuje kompleksnost, jer sužava prostor procene i tretmana rizika samo na imovinu koja podržava te procese. Ranjivosti kritične imovine sužavaju prostor pretnji samo na pretnje koje mogu iskoristiti te ranjivosti. U **Prilogu 7.8** prikazan je nacrt sadržaja izveštaja o analizi i proceni rizika.

Korak 11: Plan tretmana rizika

Tim za procenu rizika piše *plan tretmana* (ublažavanja) *rizika* koji obezbeđuje smernice za opcije menadžmenta svakog faktora rizika — *ignorisanje, prihvatanje, deljenje, prenošenje ili ublažavanje* rizika. *Plan tretmana rizika* (tabela 7.20) precizira akcije i obezbeđuje razloge za svaku akciju.

Tabela 7.20 *Primer sadržaja plana tretmana rizika*

Lista akcija	Lista prioriteta imovine, rizika i kako obuhvatiti svaki rizik
Izbor kontrole zaštite	Izabrati odgovarajuću kontrolu iz standarda ISO/IEC 27002 ili NIST SP 800-53 A,B,C.
SoC	Napraviti sažetak izabranih kontrola (*Summary of Selected Controles*).
BCM	Detaljno opisati BCP i DRP u procesu menadžmenta kontinuiteta poslovanja (BCM).
SoA	SoA je lista SoC, kontrola koje nisu izabrane i razloga za to.
Izrada politike i procedura zaštite	Opisati detaljne instrukcije korak po korak, kako napisati politiku i procedure zaštite.
Implementacija	Opisati kako će plan biti implementiran u izgradnji ISMS-a.

Faktori rizika koji zahtevaju akciju čine ulazne veličine u proces implementacije ISMS-a i bitno utiču na stanje bezbednosti informacione imovine u organizaciji. Svaka akcija u planu tretmana rizika ulazi u *plan projekta zaštite*. U principu, ni jedan identifikovani rizik se ne sme ignorisati, nego se svrstava u kategoriju *prihvatljivih faktora rizika*, koja se konačno definiše potpisivanjem SoA dokumenta. Ako se rizik deli (npr. sa osiguravajućim zavodom), što je povoljnije od ublažavanja, tada treba sve ugovoriti sa osiguravačem. Akcije za *ublažavanje faktora rizika* su ključne u procesu implementacije ISMS-a.

U *planu tretmana rizika* treba prikazati svaki faktor rizika, izabrani metod za tretman rizika i procenu usaglašenosti svakog tretmana sa politikom zaštite. U praksi zaštite, često za deo faktora rizika ne postoji nikakva politika, pa je ažuriranje politike zaštite prvi korak u procesu menadžmenta rizika. Tabela 7.20 sadrži primer sadržaja plana tretmana rizika, a **Prilog 7.9 —** uzorak *plana tretmana rizika*.

Ulazni podaci za *plan tretmana rizika* su rezultati dokumenta SoA. U planu je bolje referencirati link prema SoA, a ne kopirati ga, jer je održavanje SoA dokumenta je dovoljno teško, a više kopija dovodi do konfuzije i povećanja troškova održavanja. Lista akcija u *planu*

je lista prioriteta za izbor kontrola zaštite sa opisom ublažavanja faktora rizika za svaku imovinu organizacije. *Plan tretmana rizika* sadrži više stavki u jednoj tabeli. Za bolju preglednost i sprečavanje dupliranja informacija korisno je podeliti plan na više tabela i treba izbegavati suvišne detalje, da bi se sprečilo ponavljanje. *Plan tretmana rizika* treba da sadrži smernice za opis procesa za implementaciju kontrola i razvoj politike i procedura zaštite, bez suvišnih detalja. Smernice mogu uključiti predloge politike zaštite, procesa provere i akreditacije, kontaktne informacije itd. U tabeli 7.21 dat je nacrt *plana tretmana rizika*.

Tabela 7.21 *Primer nacrta plana tretmana rizika*

Lokacija:						Odeljenje:		
Izvršeno od strane:						Datum:		
Pregled menadžmenta:						Datum:		
Ime imovine	Broj reference	Prioritet	Mogući tretman	Opcije	Faktor rizika posle tretmana	Odgovor-nosti (A/R)	Početna odgovor-nost	Dinamika

Konačna forma i sadržaj plana zavise od specifičnosti organizacije. Plan treba da obuhvata lokaciju i odeljenje u kome se rizik tretira, ime osobe i krajnji rok za realizuje plana, pregled/odobrenje menadžera, datum, detalje za praćenje imovine, prioritet tretmana rizika i odgovornosti. Svaki faktor rizika koji se ne nalazi u planu je, prema standardu, *preostali rizik*. U SoA treba uspostaviti događaje za iniciranje povremenog pregleda i održavati listu preostalih faktora rizika.

Korak 12: Izbor kontrola zaštite

Kontrole zaštite su akcije, mere i mehanizmi za ublažavanje rizika. Izbor pravih kontrola je od suštinskog značaja za zaštitu imovine i ublažavanje faktora rizika. Za ISO/IEC 27001 sertifikaciju, treba izabrati primenljive kontrole zaštite iz ISO/IEC 27002 standarda. Neke kontrole zaštite, neophodne za organizaciju, ne moraju biti u ISO/IEC 27002 standardu, pa se preporučuje izrada *menadžment okvira zaštite* (SMF) na bazi tog standarda, a po potrebi usaglašenog i sa drugim standardom (npr. NIST).

Cilj izbora kontrole na bazi procene rizika je da se smanje ili uklone ranjivosti i/ili pretnje, a time i rizik ili da se smanji uticaj i obezbedi oporavak sistema posle napada. U ovoj fazi se pravi lista *sažetka izabranih kontrola – SoC,* koja povezuje imovinu sa kontrolama i čini deo plana tretmana rizika i implementacije ISMS-a. U tabeli 7.22 dat je primer jedne stavka u SoC sa referentnim brojem, opisom i stepenom kritičnosti imovine, identifikacijom faktora rizika, preventivnim merama i listom izabranih kontrola iz ISO/IEC 27001 standarda za

svaku stavku imovine. Iste kontrole se mogu primeniti za jednu i više imovina koje zahtevaju sličnu zaštitu. Kod izbora kontrola zaštite osnovno pravilo je *prioritet biranja* kontrola, koje zahteva: (1) *zakon ili drugi propis, (2) specifičnost poslovnog okruženja organizacije i (3) standard ISO/IEC 27001/2.*

Tabela 7.22 *Primer sažetka izabranih kontrola (SoC) iz ISO/IEC 27001*

Broj reference	Opis	Faktor rizika	Kritičnost	Druge prevencije	Lista izabranih kontrola zaštite
001	*Backup* sistem	vrednost	vrednost		A.10.5.1
002	…	…	…	…	…

Izabrane relevantne kontrole treba pregledati i isplanirati implementaciju svake od njih, što iziskuje određene troškove, uključujući i potencijalne troškove od rizika gubitka zbog nesprovođenja svake kontrole, pa uvek treba procenjivati da li je dobit veća od troškova. Ova analiza podstiče planiranje, određivanje prioriteta implementacije kontrola i pomaže konačnu odluku za ublažavanje ili prihvatanje rizika. Treba naglasiti da ISO/IEC 27001 sertifikacija ne zahteva implementaciju svih kontrola, ali zahteva kompletno poznavanje svih faktora rizika i obrazloženje za sve akcije tretmana rizika. Dokument SoA ilustruje stav organizacije prema menadžmentu rizika, kroz izbor opcija tretmana rizika.

U tabeli 7.23 prikazan je obrazac za prikupljanje detalja o imovini i izabranoj kontroli za njenu zaštitu. Većina informacija u ovom obrascu već se nalazi u ostalim obrascima procesa uspostavljanja ISMS-a, što je dobar argument za stvaranje *baze podataka o zaštiti*, skupljenih putem intervjua, upitnika ili iz prakse zaštite. Generisanje i održavanje ove *baze* je dodatni trošak, ali potencijalno može smanjiti troškove održavanja dokumentacije zaštite i konsolidovati detalje iz više različitih dokumenata.

Tabela 7.23 *Uzorak obrasca za opis imovine*

Opis informacione imovine						
Broj reference	**Lista zadataka iz procene rizika**	**Odgovornost**	**Faktor rizika**	**Datum početka**	**Datum završetka**	**Status (N,S,V)**
1	(akcija koju treba izvesti)					
2						

Izbor preventivnih mera zaštite:
1. napraviti akcioni plan za tretman rizika,
2. u plan uključiti odgovornosti, faktore rizika, datum početka i završetka i status (N, S, V),
3. izabrane kontrole iz standarda ISO/IEC 2700 navesti sledećim redosledom:
   - kontrole zahtevane zakonom ili drugim propisima,
   - kontrole preporučene dobrom praksom i poslovanjem i
   - kontrole izabrane za smanjenje faktora rizika.

Procena faktora rizika vredi za određeno vreme, pošto se scenario pretnji brzo menja, pa se i procena mora sukcesivno ažurirati. Proces menadžmenta rizika od 12 koraka periodično se ponavlja kao deo kontinuiranog poboljšanja ISMS-a.

7.3.4 Priprema izjave o primenljivosti (SoA)

Priprema *Izjave o primenljivosti (SoA)* je poslednji zadatak u PDCA fazi planiranja. Dokument SoA obuhvata svaki elemenat zaštite iz standarda ISO/IEC 27002. U **Prilog 7.10** dat je *uzorak izjave o primenljivosti* sa atributima za: (1) *referencu kontrole, (2) naziv kontrole, (3) izjavu o primenljivosti i (4) sažetak kontrole zaštite (SoC)*. Cilj SoA dokumenta je da obezbedi razmatranje svih elementa i razloga za izbor opcije tretmana rizika. SMF okvir obezbeđuje pristup sa kontrolnom listom, čime se osigurava da su svi propusti svesno napravljeni i da nije bilo previda. U tabeli 7.24 prikazan je primer atributa za SoA dokument.

Tabela 7.24 *Primer izjave o primenljivosti (SoA)*

Referenca kontrole	Opis	Implementacija	Tipični dokazi	Pristup proceduri	Komentar
A.10.7.2	Dodati rezač papira i implementiran proces za sigurno odlaganje medija.	potpuna		Molimo pogledajte kontrolu i dokument politike zaštite.	Smanjuje rizik od neovlašćenog pristupa poverljivim informacijama. Pogledajte rezultate u planu tretmana rizika.

Prva kolona je broj kontrole u Aneksu A ISO/IEC 27001 standarda, a druga opisuje potrebne akcije, uključujući plan tretmana rizika. U trećoj koloni je opisan status implementacije politike za tu kontrolu — *u potpunosti, delimično ili nije uopšte*. Četvrta kolona opisuje kontrolu koja nije izabrana ili sprovedena, sa opisom razloga, a peta opisuje pristup procedurama. Poslednja kolona je za komentare, npr. opravdanje za izuzimanje kontrole. Sadržaj tabele i tip detalja zavise od pristupa menadžmentu rizika i nivoa zahteva da se detalji konsoliduju u manji broj dokumenata.

7.4 REZIME

U fazi planiranja sastavljaju se dokumenta relevantna za ISMS implementaciju. Proces implementacije ISMS počinje sa dokumentom *ISMS smernice za fazu planiranja*. Faza planiranja može uključivati brojna dokumenta kao što su dokument o obimu i granicama ISMS-a, ISMS politika, politika zaštite informacija, lista informacione imovine, procena rizika, plan tretmana rizika, izjava o primenljivosti (SoA), izbor kontrola zaštite (SoC), standardi,

proceduralne smernice, uzorci, merenja i metrike za ocenu efektivnosti — implementacije, nadzora, provere i izmene ISMS-a. Sva ova dokumenta su sastavni deo i doprinose implementaciji ISMS-a. U odnosu na stav organizacije prema zaštiti informacija treba obezbediti odgovarajuću klasifikaciju za svu ISMS dokumentaciju. Generisani skup dokumenata u fazi planiranja daje smernice za aktivnosti u fazi implementacije ISMS-a.

Bezbednosni rizik za informacionu imovinu je kombinacija verovatnoće bezbednosnog događaja i njegove štetne posledice. Bezbednosni događaj se javlja kada neka pretnja iskoristi jednu ili više ranjivosti i nanese negativne posledice informacionoj imovini. *Menadžment bezbednosnog rizika informacione imovine* je sistematična primena ISMS politike, procedura i prakse zaštite u procesima uspostavljanja konteksta, identifikacije, analize, tretmana, monitoringa i komunikacija o bezbednosnom riziku. Opcije za upravljanje rizikom su *prihvatanje, deljenje, prenos i ublažavanje rizika.* Sistem zaštite informacija tretira faktore rizika tako što smanjuje verovatnoću njihove pojave ili ublažava njihove posledice. Posle identifikacije, analize i evaluacije faktora rizika vrši se izbor i implementacija kontrola zaštite za tretman rizika.

U praksi zaštite termin *menadžment rizika* često obuhvata menadžment i analizu rizika. Potencijalno prihvatljiva metodologija za menadžment bezbednosnog rizika sadrži dvanaest koraka: *(1) lista informacione imovine, (2) bezbednosna kategorizacija informacione imovine, (3) procena ranjivosti, (4) procena pretnji, (5) procena uticaja, (6) procena verovatnoće pretnje, (7) procena politike zaštite, (8) procena verovatnoće uticaja, (9) procena uticaja, (10) procena faktora rizika, (11) plan tretmana rizika i (12) izbor kontrola zaštite.*

7.5 PITANJA ZA PONAVLJANJE

1. Glavni cilj primene PDCA modela procesa je:
   a. implementacija ISMS u TQM sistem organizacije
   b. implementacija ISMS u menadžment sistem IKT sistema
   c. implementacija ISMS u menadžment sistem okruženja
   d. implementacija ISMS u menadžment sistem rizika.
2. Proizvodi rada faze planiranja uključuju:
   a. SMF okvir i obim ISMS
   b. GAISP principe zaštite
   c. politiku zaštite informacija i procenu rizika,
   d. izbor kontrola zaštite, plan tretmana rizika i SoA dokument.
3. Namena PDCA faze planiranja je:
   a. implementacija ISMS-a
   b. održavanje i provera ISMS-a
   c. priprema organizacije za implementaciju ISMS-a
   d. monitoring i poboljšanje ISMS-a.
4. Procena rizika poslovanja, uključujući bezbednosni rizik vrši se obavezno u:
   a. PDCA fazi implementacije
   b. PDCA fazi provere i održavanja
   c. PDCA fazi planiranja
   d. PDCA fazi monitoringa i poboljšavanja.
5. Okvir za menadžment zaštite (SMF) se definiše:
   a. pre PDCA faze planiranja u terminima menadžmenta rizika
   b. u toku PDCA faze planiranja u terminima menadžmenta poslovnog rizika
   c. u toku PDCA faze implementacije u terminima menadžmenta rizika
   d. u PDCA fazi provere ISMS-a u terminima menadžmenta rizika.

6. Obim i granice ISMS-a se definišu u odnosu na:
   a. zahteve poslovanja, tipove i lokacije IKT sistema
   b. mrežnu infrastrukturu, opremu i tehnologije
   c. lokaciju ISP i servera IKT sistema, humanu imovinu i servise zaštite
   d. zakonske, regulatorne ili druge zahteve za usaglašavanje.
7. ISMS standard preporučuje definisanje:
   a. ISMS politike i politike zaštite informacija kao jedinstvenog dokumenta
   b. ISMS politike i politike zaštite informacija kao odvojenih dokumenata
   c. samo ISMS politike
   d. samo politike zaštite informacija.
8. Sveobuhvatna *politika zaštite informacija* u organizaciji može uključivati:
   a. saopštenja 17 preporučenih komponenti sistema zaštite uključujući ISMS politiku
   b. saopštenja komponenti sistema zaštite po potrebi organizacije bez ISMS politike
   c. saopštenja 17 preporučenih komponenti sistema zaštite bez ISMS politike
   d. saopštenja 17 preporučenih i drugih komponenti sistema zaštite po potrebi organizacije sa ISMS politikom.
9. Aktivna i eksplicitna podrška i uključivanje menadžmenta u ISMS sistem su:
   a. kritični faktori uspeha programa implementacije ISMS-a
   b. malo značajni faktori uspeha programa implementacije ISMS-a
   c. značajni za balansiranje menadžmenta rizika sa potrebama i raspoloživim resursima
   d. beznačajni za balansiranja menadžmenta rizika sa potrebama i resursima.
10. Bezbednosni rizik za informacionu imovinu je:
    a. pretnje i njihove štetne posledice
    b. ranjivosti i njihove štetne posledice
    c. kombinacija verovatnoće bezbednosnog događaja i njegove štetne posledice
    d. iskoristiva ranjivost sa nekom pretnjom.
11. Menadžment bezbednosnog rizika informacione imovine je:
    a. strategijski pristup bezbednosti informacione imovine
    b. procena rizika
    c. analiza i procena rizika
    d. sistematična primena ISMS politike, procedura i prakse zaštite informacija.
12. Sistem zaštite informacija tretira faktore rizika tako što:
    a. smanjuje verovatnoću njihove pojave ili ublažava njihove posledice
    b. smanjuje pretnje
    c. smanjuje ranjivosti sistema
    d. deli i prenosi rizik.
13. Hijerarhijski pristup menadžmentu rizika informacione imovine uključuje nivoe:
    a. uprave, poslovnih procesa, servisa zaštite
    b. organizacije, poslovnih procesa, IKT sistema, sistema zaštite
    c. organizacije, poslovnih procesa, pretnji
    d. organizacije, ranjivosti sistema, sistema zaštite.
14. Prvi pristup proceni rizika je:
    a. usmeren na *pretnje* i evaluaciju imovine sa najvećom verovatnoćom napada
    b. usmeren na poslovne funkcije i imovinu ključnu za misiju organizacije
    c. usmeren *na oblast hardverske imovine* organizacije
    d. usmeren na ranjivosti IKT sistema.
15. Drugi pristup proceni rizika je:
    a. usmeren *na oblast hardverske imovine* organizacije
    b. usmeren na poslovne funkcije i imovinu ključnu za misiju organizacije
    c. usmeren na *pretnje* i evaluaciju imovine sa najvećom verovatnoćom napada
    d. usmeren na ranjivosti IKT sistema.
16. Treći pristup proceni rizika je:
    a. usmeren *na oblast hardverske imovine* organizacije
    b. usmeren na poslovne funkcije i imovinu ključnu za misiju organizacije
    c. usmeren na *pretnje* i evaluaciju imovine sa najvećom verovatnoćom napada
    d. usmeren na ranjivosti IKT sistema.

17. Tipični bezbednosni ciljevi za procenu rizika su:
    a. identifikovati faktore rizika
    b. identifikovati kritične poslovne procese i kritičnu imovinu organizacije
    c. identifikovati ranjivosti i potencijalne pretnje
    d. utvrditi verovatnoću da pretnja/e iskoriste ranjivosti i uticaja na poslovanje.
18. Potencijalno prihvatljiva metodologija za procenu i menadžmenta rizika:
    a. sadrži proces od 7 koraka
    b. sadrži proces od 12 koraka
    c. sadrži proces od 9 koraka
    d. sadrži proces od 10 koraka.
19. Procena neodređenosti rizika uključuje kvalitativno vrednovanje verovatnoće:
    a. događaja pretnje, iskoristive ranjivosti, efektivnosti kontrola zaštite
    b. događaja pretnje, servisa zaštite, rizika
    c. događaja pretnje, iskoristive ranjivosti, metoda zaštita i rizika
    d. događaja pretnje, efektivnosti *kontrola* zaštite, metoda zaštita, rizika.
20. Generički metod procene bezbednosnog rizika procenjuje vrednosti:
    a. imovine (A), napada (N), konfiguracije (K) i uticaja (U)
    b. imovine (A), pretnji (T), ranjivosti (V) i uticaj (U)
    c. imovine (A), pretnji (T), ranjivosti (V), rizika (R) i efektivnosti metoda zaštite (Ekz)
    d. imovine (A), pretnji (T), ranjivosti (V), uticaj (U) i rizika (R).
25. Kriterijumi za prihvatanje rizika se definišu u fazi:
    a. izrade politike zaštite
    b. uspostavljanja i organizacije tima za procenu rizika
    c. definisanja obima i granica analize i procene rizika
    d. definisanja osnovnih parametara za upravljanje rizikom.
26. U proceni rizika za određivanje vrednosti A obično je odgovoran i mora učestvovati:
    a. glavni menadžer organizacije
    b. specijalista zaštite
    c. pravnik organizacije
    d. digitalni forenzičar.
27. Inventar imovine i taksonomije relevantnih pretnji i ranjivosti su izlazi iz procesa:
    a. uspostavljanja okvira za ISMS
    b. identifikovanja rizika
    c. ublažavanja (delovanja na) rizika
    d. prihvatanja rizika.
28. Faktori neodređenosti rizika se uključuju u fazi:
    a. uspostavljanja okvira za ISMS
    b. identifikovanja rizika
    c. estimacije rizika
    d. analize rizika
    e. prihvatanja rizika.
29. U fazi procene ranjivosti (V), testiranje na proboj:
    a. proverava ranjivost mrežnih programa
    b. proverava mogućnost zaobilaženja kontrola zaštite sa aspekta izvora napada
    c. proverava ranjivost TCP/IP protokola
    d. naziva se hakerski napad.
30. Najznačajniji izlaz iz procene rizika je dokument:
    a. plan tretmana rizika
    b. *lista prioriteta prihvatljivog rizika*
    c. *lista prioriteta neprihvatljivog rizika*
    d. *izjava o primenljivosti kontrola zaštite (SOA*).



8.
IMPLEMENTACIJA, PROVERA I POBOLJŠANJE ISMS-a

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Primenu PDCA „Do" faze za implemenentaciju procesa i procedura ISMS-a
- ☑ Izlazne rezultate i dokumentaciju procesa PDCA faze implementacije ISMS-a
- ☑ Primenu PDCA „Check" faze za kontrolu i proveru operacija ISMS-a
- ☑ Izlezne rezultate i dokumentaciju PDCA faze provere ISMS procesa
- ☑ Primenu PDCA „Act" faze za monitoring i poboljšanje ISMS-a i PDCA procesa
- ☑ Izlezne rezultate i dokumentaciju PDCA faze poboljšanja ISMS-a i PDCA procesa

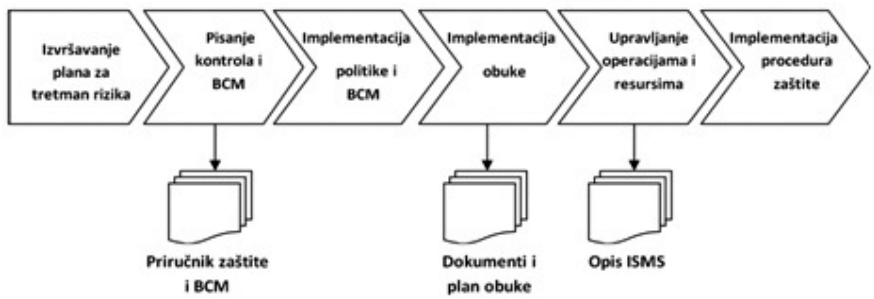
8.1 UVOD

Sa aspekta menadžmenta, sistem zaštita informacija treba da se posmatra kao integralni deo procesa rada i strateškog planiranja organizacije. Posebno je značajno da donosioci odluka i izvršni menadžeri prepoznaju faktore bezbednosnog rizika i shvate značaj kontrole rizika u razvoju programa zaštite. Ovakav stav najvišeg menadžmenta presudno doprinosi da se program zaštite shvati krajnje ozbiljno na svim nivoima, a posebno na nivou izvršnih menadžera u organizaciji, kao i da specijalisti zaštite obezbede neophodne resurse za implementaciju efektivnog sistema zaštite. Najbolja prakse zaštite sugeriše da se koriste različiti događaji u organizaciji za povećanje interesa zaposlenih sa zaštitom, kao što su *kompjuterski incident, interna obuka zaposlenih o potrebi zaštite informacija i značaju za ukupan rad organizacije, sve lične inicijative itd.*

Zaštita informacija predstavlja propulzivni pokretač efikasnog i efektivnog rada organizacije, ako se primenjuje tehnički pouzdani i dobro zaštićen IKT sistem. Drugim rečima, sistem zaštite omogućava potpuno iskorišćenje svih prednosti koje IKT sistemi pružaju u povećanju efikasnosti i efektivnosti rada, smanjujući potencijalni rizik na prihvatljivi novo za organizaciju, posebno u slučajevima korišćenja Internet aplikacija i širenja broja korisnika koji imaju prava pristupa podacima i informacijama u IKT sistemu organizacije.

8.2 IMPLEMENTACIJA ISMS-a (*Do phase*)

U fazi planiranja se uspostavljaju dokumenta koja će voditi proces *implementacije* ISMS-a u fazi „*Primene*" (slika 8.1). Ključni deo te faze je sprovođenje plana za tretman rizika, generisanog u procesu menadžmenta rizika. Standardi ISO/IEC 27001/2 ne nude smernice za implementaciju kontrola zaštite. U standardu ISO/IEC 27003, *Security Management System Implementation Guidance*, nalazi se više detalja o primeni PDCA modela za uspostavljanje, planiranje, implementaciju, funkcionisanje i održavanje ISMS-a.



Slika 8.1 Proces PDCA faze primene

Implementacija *plana tretmana rizika* počinje sa pisanjem (ili ažuriranjem) politike za svaku kontrolu zaštite, koja predstavlja okvir za upravljanje aktivnostima u fazi implementacije ISMS-a. Procedure zaštite obezbeđuju smernice *kako* sprovesti i primeniti politiku, a standardi obezbeđuju smernice *šta* treba upotrebiti za implementaciju i sprovođenje te politike. Svest o potrebi zaštite, obuka i obrazovanje, pripremaju zaposlene za aktivno učešće u implementaciji ISMS-a. Ostale aktivnosti obuhvataju menadžment i funkcionisanje ISMS-a, uključujući pripremu za reagovanje na kompjuterski incident. Inicijalna pripreme implementacije ISMS prikazana je u **Prilogu 8.1.**

8.2.1 Implementacija plana tretmana rizika

Plan tretman rizika nabraja faktore rizike, identifikuje odgovornosti svih zaposlenih u organizaciji u procesu menadžmenta rizika, uloge i odgovornosti menadžera za uspostavljanje strategije menadžmenta rizika, kao i akcija za sprovođenje strategije u taktičke i operativne zadatke za *rad, nadzor, praćenje i izveštavanje* o aktivnostima menadžmenta rizika.

8.2.2 Pisanje politike i procedura komponenti zaštite

ISMS politika i *politika zaštite informacija* podržavaju bezbednost informacione imovine na visokom nivou apstrakcije, ali ne identifikuju specifične kontrole zaštite. Zato je početni korak u fazi primene – razvoj (ažuriranje) politike za svaku kontrolu zaštite ili klasifikacija kontrola zaštite u SoC, koja se opravdava u SoA dokumentu.

Primer: U SoC dokumentu se navodi da će organizacija koristiti lozinke kao deo celokupnog programa za upravljanje pristupom, što zahteva da se napiše *politika za upravljanje lozinkama* i obezbede sveukupne smernice za upotrebu lozinki. Politika za upravljanje lozinkom mora da: *bude koncizna*, da sadrži „*upotrebu jakih lozinki*" i nabroji tekuće standardne specifikacije za jaku lozinku (npr. **X** broj slova sa **Y** brojeva specijalnih karakteristika, **Z** brojeva numeričkih karaktera i neki broj velikih slova pomešan sa malim). Procedura za upravljanje lozinkom objašnjava kako treba generisati i koristiti jake lozinke.

Razdvajanje dokumenata zaštite obezbeđuje modularnost i omogućava pojedinačno ažuriranja. Na primer, ako programi za razbijanje lozinki ukažu da je tekući standard za jake lozinke probijen, isti se relativno lako modifikuje i definiše, dok politika i procedure ostaju iste, tj, administrator i dalje koristi iste instrukcije da postavi lozinke i istu konfiguraciju za jačanje lozinki, a samo menja standard za generisanje lozinke.

Za ISO/IEC 27001 sertifikaciju, treba koristiti smernice za kontrole zaštite (ISO/IEC 27002) za izradu politike, standarda i procedura. Svaka ISO/IEC kontrola ima kontrolni broj koji se može ugraditi u sve odnosne dokumente. Bolji pristup je razdvajanje ISO/IEC reference kontrola zaštite od dokumenata i izrada matrice usaglašenosti (poglavlje 6., „*Menadžment usaglašenosti*", *radni okvir za pravljenje matrica usaglašenosti*), koja povezuje svaki dokument ili skup dokumenata sa određenom ISO/IEC kontrolom zaštite.

Svaka politika počinje sa *izjavom o nameni* koja sadrži opšte ciljeve ISO/IEC kontrola i određuje specifičnosti politike. Korisne instrukcije za pisanje politike, standarda i procedura za bilo koju datu kontrolu zaštite, obezbeđuju odgovori na sledeća pitanja:

- Zašto je kontrola izabrana?
- Ko je odgovoran za izbor, implementaciju, nametanje primene kontrole?
- Kako neko implementira, nameće primenu kontrole?
- Koje mere i metrike će pokazati primenu kontrole?
- Da li su te metrike dovoljne za izveštaj o aktivnosti ili neki drugi izveštaj koji pokazuje primenu, efektivnost primene i efektivnost zaštite?
- Da li su politika i procedure jasne, realne i čitljive?
- Da li su predugačke?
- Da li su politika i procedure izvodljive i obezbeđuju dovoljne smernice?
- Da li su svi delovi ISO/IEC kontrola u politikama, standardima i procedurama?
- Da li postoje bilo kakva sredstva za merenje efektivnosti politika uz pomoć procedura?
- Koji je cilj performanse politike? Da li je jasno formulisan?
- Šta možemo da izmerimo? Kako možemo da izmerimo? Da li će to biti adekvatno predstavljeno?
- Da li postoji datum objavljivanja u dokumentu?
- Da li postoji datum poslednjeg pregleda u dokumentu?
- Da li je jasno ko je odgovoran za održavanje dokumenta?

8.2.3 Izbor metrike i merenja ISMS-a

Metrike i merenja određuju razliku između tekuće prakse zaštite i potencijalnog kvaliteta politike, standarda i procedura zaštite. Namena metrike i merenja je da zabeleži tekuće stanje i efektivnost operacija sistema zaštite. U tom smislu treba razmotriti sledeće aspekte, tražeći odgovore na pitanja:

- **Identifikujte predmetnu kontrolu zaštite**:
  - Zašto birate ovu kontrolu zaštite?
  - Koji je cilj za ovu kontrolu zaštite?
  - Ko su odgovorni za politiku napisanu za tu izabranu kontrolu?
  - Da li zaista obavljaju svoje odgovornosti?
  - Da li postoji politika?
  - Da li postoji standard?
  - Da li postoji procedura?
  - Da li je to dobra politika? Zabeležite atribute koji definišu dobru politiku i uporedite atribute aktuelne politike!
- **Identifikujte predmetni standard i proceduru**:
  - Da li je to dobar standard?
  - Da li je to dobra procedura?
  - Odgovorite na ista prethodna pitanja, uporedite i utvrdite da li unutar organizacije postoje dobri standardi i dobra politika!

Identifikujte predmetnu praksu zaštite:

- Da li postoji praksa zaštite u organizaciji?
- Da li postoji dobra praksa zaštite?
- Da li praksa zaštite organizacije koristi procedure?
- Ko je odgovoran (možda klasifikacija zaposlenog) za sprovođenje procedura?
- Ko je odgovoran za praćenje efektivnosti procedure?
- Kako odgovorna osoba meri i koje metrike performansi procesa zaštite koristi?
- Koji izveštaji postoje za praćenje efektivnosti kontrola zaštite?
- Postoji li mogućnost da se zabeleži početno stanje sistema zaštite (*secirity baseline*) i kasnija stanja, tako da se omogući analiza trenda?

Metrika je atribut za merenje kvaliteta performansi sistema zaštite. Na primer, postojanje tima za zaštitu je jedna metrika. Činjenica da tim uopšte postoji dopušta definisanje *metrike za ocenu efektivnosti tima*. Merenja efektivnosti tima mogu uključivati *stepen multifunkcionalnosti, učestalost sastanaka, prisustvo sastancima, način formiranje, zadatke, rezultate rada tima* itd. Ako su, na primer, svi članovi tima iz IKT sektora, tada je stepen multifunkcionalnosti tima nizak. Merenje efektivnosti tima je i razlikovanje kompetencija članova tima za zaštitu u poređenju sa referentnim timom koji definiše dobru praksu, na bazi industrijskih standarda, iskustva organizacije ili indirektnog iskustva sličnih organizacija (npr. CIRT — *Computer Incident Response Team* ili CERT *Computer Emergency Response Team* [17]).

U tabeli 8.1 dati su neki primeri za početni razvoj metrika i merenja ISMS-a.

Tabela 8.1 *Izvod smernica za razvoj metrika i merenja za politiku zaštite*

Kategorija/ Potkategorija/ Element zaštite	**Metrika**	**Merenja**	**Proračuni (ako su primenljivi)**
Politika zaštite			
Politika zaštite informacione imovine		Izmerite postojanje i kvalitet politikezaštite informacija!	
Dokumentacija	Politika postoji. Menadžment sistem pregledan i odobren.	Da li politika postoji?	% završene politike= (broj tekućih/broj planiranih politika)
Rasprostiranje	Primerci politike podeljeni. Politika preuzeta.	Da li je obaveštenje primljeno? Da li je politika preuzeta?	% zaposlenih koji primaju obaveštenja; % zaposlenih koji preuzmu politiku
Provera politike	Definisanje događaja za iniciranje provere. Kreiranje multifunkcionalnog tima za proveru.	Koji događaj inicira proveru politike? Ko je odgovoran za proveru politike? Koja poslovna jedinica ima prezentaciju pred timom za zaštitu?	% prezentacija = (# poslovnih jedinica u timu za zaštitu / # ciljanih poslovnih jedinica u timu za zaštitu)
Plan menadžmenta zaštite			

Neki rezultati merenja mogu biti u procentima, a neki — jednostavno registrovanje sa *da, ne, nepoznato* ili *neprimenljivo* (N/A). Moguće je, čak, izmeriti subjektivnu procenu usaglašenosti sa objektivnim vrednostima.

Primer: Treba primeniti jednostavnu skalu tipa *ne postoji (neusaglašenost), slaba usaglašenost, srednja usaglašenost, visoka usaglašenost i kompletna usaglašenost* sa navedenim ciljevima. Neusaglašenost je jasna sama po sebi. *Slaba usaglašenost* može značiti da postoji samo parče papira sa rečima *Politika zaštite informacija*, tj. politika postoji, ali je slabog kvaliteta. *Srednja usaglašenost* znači dobar pokušaj da se postigne politika usaglašenosti, ali i dalje nedostaju mnoge stavke. *Visoka usaglašenost* nagoveštava da je skoro tu i da će se sa par minornih poteza postići *kompletna* usaglašenost. Ako se ova subjektivna skala procene usaglašenosti prevede u objektivnu, tipa **0, 1, 2, 3, i 4** respektivno, dobije se objektivno (kvantitativno) merenje subjektivne (kvalitativne) procene.

Sadržaj tabele 8.1 je izvod iz tabele za kompletan razvoji metrike i merenja iz standarda ISO/IEC 27004. Za usaglašavanje sa standardima ISO/IEC zahteva se merenje efektivnosti i performansi implementacije ISMS-a. Identifikovanje korisnih metrika i merenja performansi sistema zaštite informacija je problematično, jer se na različitim nivoima organizacije traže različita značenja u rezultatima merenja [92, 106, 116].

Primer: Administrator logičke barijere (*firewall*) – (FW) želi da zna koliko je IP paketa blokirano, koliko je potencijalnih napada bilo i kakve su specifičnosti tih napada. Ovo zahteva filtriranje očekivanog saobraćaja i izolovanje izuzetaka za dalju analizu, kako bi se otkrili potpisi i obrasci napada. Glavni izazov za administratora *FW*-a je upravljanje obimom detalja u logovima radi identifikovanja realnih pretnji. Međutim, izvršni direktor koji traži opravdanje za održavanje veoma skupe poslovne inicijative za upravljanje rizikom, ni najmanje nije zainteresovan za broj blokiranih IP paketa na *FW*-u. Ovaj primer ukazuje na potrebu za različitim metrikama i merenjima. Da bi se rešio ovaj problem od relativnog značenja, metrike na nivou *FW*-a treba da prikuplja podatke o funkcionisanju *FW*-a. Isto važi i za mrežne sisteme za detekciju i sprečavanje upada (NIDPS), *antivirusne, antispy, antispam* programe i sve ostale mehanizme zaštite. Ti podaci vremenom ukazuju na operativne trendove, što pokazuje efektivnost mehanizama zaštite, npr. FW1 je blokirao ukupno X paketa sa Y identifikovanih kao potencijalnih napada. Ovi operativni trendovi postaju deo ukupnog izveštaja o zaštiti, koji zatim prelazi u izveštaj o menadžmentu rizika, tj. o menadžmentu usaglašavanja.

Tako nivo izvršnih menadžera može zahtevati opravdanje investicije za zaštitu kod borda direktora ili izveštaj o performansama sistema zaštite za relevantne učesnike. U tom smislu zahtevaju se i različite metrike i sistemi merenja performansi sistema zaštite. Administrator aplikativnog softvera i administrator mreže traže statistiku vremena aktivnog rada i otkaza sistema, a administrator zaštite broj blokiranih *malvera* i pokušaja proboja FW-a. Menadžer zaštite agregira sve ove mehaničke podatke o performansama sistema u operativni izveštaj koji odražava ukupne performanse sistema. Metrike na najvišem nivou reflektuju performanse poslovanja, a tehničke performanse – u atributima poslovnih vrednosti; na izvršnom nivou pokazuje poslovne vrednosti operacija zaštite u formi povratka investicija. Neki predlozi za primenu metrika i merenja efektivnosti ISMS-a dati su u sledećoj listi:

1. *Kvantifikacija rezultata procene rizika:*
   - vrednost poslovnih funkcija, npr. *web* sajt za e-trgovinu u terminima profitabilnosti,
   - vrednost imovine, npr. stvarna vrednost servera za e-trgovinu,
   - ranjivosti (na serveru **X** potencijalne poznate i aktuelne otkrivene procenom ranjivosti),
   - plan oporavka (aktivnosti planirane za otklanjanje ranjivosti).
2. *Menadžment ranjivosti*:
   - tekuće aktivnosti za podizanje svesti o novim ranjivostima i popravkama,
   - menadžment aktivnosti za proaktivno ublažavanje ranjivosti,
   - verovatnost pojave pretnji, tj. verovatnoća napada *malvera i*
   - menadžment incidenta i izveštavanje (broj incidenata).
3. *Vreme od otkrivanja do registrovanja*:
   - obezbediti uvid u svest o potrebi zaštite i stanje zapisa bezbednosnih događaja.
4. *Vreme od registrovanja incidenta do trijaže i eskalacije*:
   - obezbediti uvid u stanje *deska za pomoć* i efektivnost tima za odgovor na incidente.

5. *Vreme od eskalacije do izolacije, fiksiranja i oporavka*:
   - obezbediti uvid u efektivnost tima za upravljanje incidentom u rešavanju problema.
6. *Vreme od oporavka do potpune analize uzroka i uticaja na poslovanje organizacije*:
   - obezbediti uvid u stanje procesa za analizu uzroka i angažovanja tima za zaštitu sa ciljem da se jedan događaj nikada ne ponovi ili barem smanji efekat ponovljenog incidenta.
7. *Menadžerska provera ISMS*:
   - pokazati angažovanje dela menadžmenta na zaštiti poslovnog okruženja,
   - izmena upravljačkih kontrola,
   - provera log fajlova (dnevnika rada),
   - nalazi interne provere sistema zaštite (koliko organizacija poznaje ili misli da poznaje sebe),
   - nalazi spoljne provere sistema zaštite (nezavisna procena i testiranje BCP i DRP planova).
8. *Praćenje*:
   - svesti o potrebi zaštite, npr. broj zaposlenih koji otvara *e-mail* sa materijalom,
   - obuka o zaštiti, npr. broj zaposlenih koji prisustvuju *web* seminarima i
   - obrazovanje o zaštiti, npr. broj dobijenih ili obnovljenih sertifikata.

Ova lista nije konačna, što zavisi od specifičnosti organizacije i zahteva da se istaknu poslovne vrednosti sistema zaštite informacija. Kada se piše politika na bazi izabranih kontrola zaštite za ublažavanje rizika, treba definisati *kratkoročni cilj*, *tip* i *dugoročni cilj merenja efektivnosti* politike zaštite. U tabeli 8.2 prikazane su definicije ova tri faktora, kao i opis drugih faktora za razvoj procedura za implementaciju politike zaštite.

Table 8.2 *Definicije faktora za implementaciju metrike politike zaštite*

Faktor	Opis
Kratkoročni ciljevi	Opisati željeni rezultat implementacije jedne ili više kontrola zaštite; ovaj detalj treba uključiti u politiku zaštite.
Tip	Opisati tip metrike, tj. koji tip aktivnosti dostiže cilj; na primer, rezultat, izlaz, implementacija ili neka druga aktivnost.
Dugoročni cilj	Opisati kriterijum koji određuje da je cilj postignut.
Namena	Opisati razloge za uvođenje metrike.
Dokaz o implementaciji	Opisati dokaz o postojanju politike i procedura zaštite; deo interne provere ISMS-a za potvrdu da su metrike implementirane i efektivne.
Frekvencija	Opisati koliko često treba skupljati metričke podatke, npr. nedeljno, mesečno ili godišnje, zavisno od poslovanja i učestalosti promena.
Metod evaluacije	Opisati proračun i tip očekivanih rezultata, kao što su procenat i broj.
Izvor podataka	Lista lokacija podataka.
Indikacije	Informacije o značenju metrika i merenja i trenda performansi.

Ovi faktori obezbeđuju smernice za kreiranje konzistentnih procedura sa jasnom formulacijom *dugoročnih ciljeva zaštite* i merenja za postizanje tih ciljeva. Prema PDCA modelu procesa, implementacija politike pomoću procedura obezbeđuje konzistentnost i ponovljivosti operacija i ostavlja tragove za internu proveru i validaciju implementacije ISMS-a.

8.2.4 Selekcija i implementacija kontrola zaštite

Za obezbeđivanje SMF-a i smernica za izbor i implementaciju odgovarajućih kontrola zaštite preporučuje se primena standarda ISO/IEC 27002. Sam proces selekcije i implementacije kontrola zaštite je specifičan za svaku organizaciju. Generalno, prvo treba razmotriti sekciju kontrola zaštite sa aspekta *da li organizacija uopšte ima potrebu za kontrolama zaštite*? U svakom slučaju treba navoditi razloge, što je bitno za izradu SoA dokumenta. Za sve izabrane kontrole zaštite, treba razmotriti koje su *karakteristike kontrola* potrebne organizaciji za implementaciju. Standardi ISO/IEC 27002 (NIST SP 800-53) obezbeđuju smernice za izbor karakteristika (nivoa robusnosti) različitih kontrola zaštite.

Koristeći politiku zaštite kao smernicu i balansirajući između zahteva za zaštitu i raspoloživih resursa, profesionalci za zaštitu odlučuju koje karakteristike kontrola zaštite čine *najbolju praksu*, a koje – *prihvatljivu praksu* zaštite. U ovoj tački organizacija shvata koje su kontrole zaštite neophodne i koje karakteristike svake od njih treba da implementira. Zatim, tim za zaštitu, na bazi uputstava vendora opreme za zaštitu i rezultata obuke, obezbeđuje uvid u implementaciju i uvođenje u primenu kontrola zaštite.

8.2.5 Razvoj svesti o potrebi, obuka i obrazovanje u zaštiti

Na osnovu akademskog i profesionalnog iskustva, učenje, generalno, napreduje kroz faze *razvoja svesti o potrebi, razumevanja, korišćenja stečenog znanja i efektivne upotrebe znanja*. Učenje počinje od trenutka kada čovek *ne zna šta ne zna*, a svest o potrebi prevazilazi tu prepreku. Takođe, postoji razlika između površnog poznavanja *nečega* o *nečemu* i stvarnom poznavanja toga.

Svest o potrebi zaštite obezbeđuje poznavanja *nečega* o zaštiti, a razumevanjem čovek prepoznaje potrebu za zaštitom i počinje da shvata svoju ulogu. Prihvatajući ulogu u zaštiti, počinje da koristi merenja zaštite, da ih *svesno* primenjuje, stiče nove veštine i efektivno koristi alate za zaštitu. Svest o potrebi zaštite zahteva se za sve zaposlene, a metodi razvoja mogu biti različiti, od orijentacije novozaposlenih na nove poslove ili odgovornosti do periodičnog podsećanja i demonstracija dramatičnih primera zloupotreba i šteta od kompjuterskog kriminala u svetu itd.

Selektivna i primerena *obuka u zaštiti* je namenjena za zaposlene u IT sektoru, administratore sistema, zaposlene koji unose podatke i profesionalce u zaštiti. Takođe, profesionalci u zaštiti zahtevaju permanentno, formalno obrazovanje, sa širim i dubljim znanjem o zaštiti informacija, osim rada sa mehanizmima zaštite.

Obrazovanje u zaštiti može se verifikovati stečenom diplomom (ili master diplomom), specifično za bezbednost informacija ili međunarodnim sertifikatom (npr. CISSP — *Certified Information System Security Professional*). Postojanje svesti o potrebi zaštite, iskustava i

ekspertskih znanja u organizaciji, zahtev je ISMS standarda i deo provere za ISO/IEC 27001 sertifikaciju. Primeri merenja i metrika za praćenje ovih faktora mogu biti, za:

1. *Svest o potrebi zaštite informacija*:
   - broj *e-mail*-ova poslatih u kampanji za razvoj svesti o potrebi zaštite,
   - broj povratnih potvrda da su *e-mail*-ovi otvoreni,
   - rezultati intervjua o aktivnostima za razvoj svesti o potrebi zaštite i
   - rezultati ankete o svesti o potrebi zaštite.
2. *Obuku o zaštiti informacija*:
   - broj održanih profesionalnih seminara i
   - broj profesionalaca sertifikovanih za mehanizme zaštite (npr. za *firewall*).
3. *Obrazovanje o zaštiti informacija*:
   - broj diplomiranih u disciplinama koje se odnose na zaštitu informacija i
   - broj profesionalaca sa sertifikatima o zaštiti (broj novih sertifikata, broj obnovljenih sertifikata koji ukazuju na kontinuitet učenja).

8.2.6 Menadžment operativne primene ISMS-a i sistema zaštite

Ciljevi menadžmenta implementiranog ISMS-a su efektivno upravljanje tekućim operacijama i rizikom poslovanja organizacije, kao i održavanje prihvatljivog nivoa rizika za CIA informacione imovine (generisanje SoA dokumenta). Za postizanje ovih ciljeva zahteva se alokacija odgovarajućih resursa, koji uključuju osposobljene profesionalce i alate za zaštitu. Menadžment operacija ISMS-a uključuje zaposlene, menadžere, alate za rad i upravljanje.

U procesu menadžmenta implementiranog ISMS-a prvi korak je dokumentovanje procedura za *operativne aktivnosti, upravljanje promenama, dodeljivanje uloga (npr. razdvajanje dužnosti), implementaciju i operativnu primenu alata za zaštitu*. Osnovni zahtev ISO standarda je da su procedure usklađene sa standardom, ponovljive i da daju konzistentne rezultate, što zahteva obimnu dokumentaciju.

8.2.7 Menadžment bezbednosnog incidenta

Proces menadžmenta bezbednosnog incidenta zahteva uključivanje politike, procedura, infrastrukture i alata za podršku. Efektivan *plan menadžmenta* bezbednosnog *incidenta* treba da uključuje, najmanje, sledeće aktivnosti [78]:

- *pripremu:* uputstva i procedure za rukovanje incidentom, digitalnu forenzičku istragu, zahtevanu dokumentaciju i BCP;
- *registrovanje*: procedure, alati, odgovornosti i lica za izveštavanje o incidentu;
- *procenu:* procedure i odgovornosti za istragu i određivanje intenziteta;
- *menadžment:* procedure i odgovornosti za sve aktivnosti oko incidenta, ograničenje štete, saniranje i izveštavanje;
- *oporavak:* procedure i odgovornosti za uspostavljanje normalnih IKT servisa;
- *reviziju:* procedure i odgovornosti za aktivnosti posle incidenta, uključujući zakonske implikacije i analizu trenda.

Proces menadžmenta incidenta informacione bezbednosti obuhvata sledeće faze:

- monitoring,
- detekcija,
- registrovanje,
- trijaža,
- eskalacija,
- odgovor,
- izolacija,
- oporavak,
- analiza uzroka incidenta i
- usvajanje i prenošenje iskustava organizaciji.

Monitoring sistema zaštite je odgovornost svih zaposlenih u organizaciji. Organizacija treba da investira u obuku i obrazovanje profesionalaca u zaštiti i da ih pripremi za menadžment incidenta, a sve zaposlene, kroz program razvoja svesti o potrebi zaštite da — izbegavaju rizično ponašanje, shvataju pretnje iz okruženja i monitorišu anomalije i neprihvatljive aktivnosti.

Detekciju incidenta obezbeđuju u prvom redu mehanizmi zaštite, ali i profesionalci u zaštiti i zaposleni. Detekciju incidenta mogu vršiti *tehničke* i *proceduralne* kontrole zaštite, što zahteva implementacija odgovarajućih mehanizama zaštite.

Primer: F*irewall* može alarmirati napad odbijanja servisa – DoS (*Denial-of-Service attack*); antivirusni program (AVP) na *e-mail* serveru može detektovati napad crva sa Interneta; IDPS sistem može otkriti i sprečiti anomaliju u mrežnom saobraćaju; zaposleni može primetiti da finansijski podatak u bazi podataka ne odgovara očekivanoj vrednosti od prethodnog dana; manuelna evaluacija log datoteke može ukazati na napade iznutra itd.

Registrovanje incidenata zahteva infrastrukturu za podršku, koja uključuje *help desk*, *e-mail* za pristup *help desku*, direktan pristup, autentifikacioni sistem za praćenje registrovanih incidenta i vremena odgovora (sa metrikom i merenjima) i tim za odgovore na kompjuterski incident (CIRT) ili tim u centru za bezbednosne operacije, (SOC[1]) koji je tipično deo centra za mrežne operacije (NOC[2]). Zavisno od intenziteta incidenta, za procenu se može angažovati ekspertski tim (interni ili iznajmljeni).

Trijažu incidenata vrše *help desk*, CIRT, SOC ili NOC. *Help desk* treba pripremiti za rukovanje sa poznatim bezbednosnim događajima (npr. izolovanje virusa, brisanjem inficiranih fajlova i restauracijom čistih fajlova), trijažu i prepoznavanje eskalacije incidenta. CIRT i NOC se moraju pripremiti da, u slučaju eskalacije, angažuju ekspertski tim za menadžment kompjuterskog incidenta.

Eskalacija incidenata zahteva pripremu za angažovanje timova različitih eksperata. Za praćenje eskalacije incidenta, u prvom redu, treba što više automatizovati alate za zaštitu,

1 Engl.: SOC – *Security Operations Center.*
2 Engl.: NOC – *Network Operations Center.*

npr. kao što AVP na desktop računaru izoluje i tretira inficirane fajlove. Zatim, potrebno je obučiti zaposlene da što pre prijave svaku anomaliju u sistemu zaštite, entitetu/licu imenovanom u politici menadžmenta kompjuterskog incidenta.

Odgovor na incident pretpostavlja da organizacija raspolaže timom sa ekspertskim znanjima i uspostavljenim resursima za pravovremeno reagovanje na incidente. *Ad hoc* odgovor nije efektivan, kao pripremljen i planiran odgovor uvežbanog tima sa odgovarajućim alatima, koji mogu uključivati forenzičke tehnike i alate za Internet forenzičku istragu, programe za analizu *malvera* itd.

Izolacija kompjuterskog incidenta i svakog bezbednosnog problema, treba da bude u domenu odgovornosti tima za menadžment incidenta, što nekada može značiti isključivanje ključnih servera sa mreže, odnosno prekid poslovnih operacija.

Restauracija i oporavak sistema je primarni cilj ove faze i pretpostavlja tretman simptoma kompjuterskog incidenta. Organizacija mora razumeti da do proboja sistema zaštite gotovo uvek može doći (jer praktično nema apsolutne zaštite), pa zato mora razviti kapacitete (kompetentan tim, tehnike i alate) za oporavak sistema i vraćanje servisa u stanje normalnog rada.

Analiza uzroka incidenta je obavezna aktivnost tima za menadžment incidenta, koji treba da identifikuje svaki bezbednosni problem. Uzroci nastalog bezbednosnog problema mogu biti tehnički, organizacioni, personalni ili proceduralni faktori. Proces analize uzroka incidenta je metodičan proces *sistemske analize* kombinacije ovih faktora, koja identifikuje relevantan doprinos pojavi incidenta svakog od njih. Ovi nalazi obezbeđuju uvid u to kako treba sprečiti ponavljanje incidenta ili smanjiti efekte ponovljenog incidenta primenom efektivnije kontrole zaštite. Međutim, za efektivnu analizu uzroka kompjuterskog incidenta i *trajno sprečavanje* njegovog ponavljanja, najčešće su neophodne forenzička znanja, tehnike i alati. U tom smislu konvergiraju *znanja, tehnike i alati za zaštitu* i *za digitalnu forenzičku istragu* u jedinstven kapacitet za menadžment kompjuterskog incidenta.

Prenošenje iskustava organizaciji je odgovornost tima za menadžment incidenta. Rezultati rada tima obezbeđuju podatke za prenošenje iskustava svim zaposlenim u organizaciji. Zaposleni, u okviru svojih odgovornosti, treba da implementiraju aktivnosti koje se odnose na sprečavanje ponavljanja stvarnog uzroka incidenta.

Primer: ako je uzrok incidenta *proceduraln*i, treba modifikovati procedure i obučiti personal za njihovu primenu; ako je *nesavesni personal*, treba modifikovati program o razvoju svesti o potrebi zaštite, a ako je *ranjivost softvera*, treba obezbediti bezbednosnu popravku itd.

Postoji više načina za merenje efektivnosti odgovora na kompjuterski incident. Dokumentovani rezultati ovih merenja doprinose razvoju efektivnijeg odgovora na incident. Korisna dokumenta su kratki izveštaji korisnika o incidentu i izveštaji tima za menadžmenta incidenta.

8.2.8 Povratak investicija u zaštitu informacija (ROSI)

Kao profesionalci u zaštiti, da bi obezbedili podršku menadžmenta za implementaciju ISMS standarda, u prvom redu potrebno je da [43]:

1. razumete kako vaš menadžment razmišlja i šta je važno za organizaciju,
2. na bazi ovog razumevanja procenite dobit od implementacije ISMS standarda,
3. procenite troškove takvog projekta i
4. obezbedite podršku menadžmenta sa ovim argumentima na jednom sastanku.

Za ovo je nekad potrebno par sati, a nekada i godine. U svakom slučaju sa ovakvim pristupom može se dobiti podrška menadžmenta i do 50% brže!

Ako se suočite sa primedbom menadžmenta da su kontrole zaštite koje predlažete suviše skupe i, ako je teško objasniti menadžmentu koje se posledice mogu dogoditi u slučaju incidenta, a treba da dokažete da se isplati investirati u zaštitu informacija, onda može pomoći tehnika proračuna povratka investicija u zaštitu – ROSI (*Return on Security Investment*) prema sledećem obrascu:

ROSI = (ukupna vrednost ublažavanja rizika – troškovi kontrola)/troškovi kontrola

Dakle ulaganje u zaštitu je profitabilno ako su efekti ublažavanja rizika veći od očekivanih troškova kontrola zaštite. Proračun ROSI može se izvršiti u tri koraka: *(1) proračunati sve relevantne troškove incidenta, uključujući verovatnoće incidenta, (2) proračunati troškove kontrola/mera zaštite i nivo smanjenja rizika i (3) proračunati da li je dobit – efekat smanjenja rizika — veća od ulaganja u kontrole/mere zaštite* [72].

Ovaj proračun je veoma složen jer zavisi od brojnih faktora neodređenosti. Brojni autori smatraju da nije moguće egzaktno računati SROI i ne postoji konzistentan izvor informacija za proračun SROI. Na Internetu postoje određene informacije i više metoda za proračun SROI, a najviše na sajtu www.gocsi.com.

Primer: **U proračun troškova incidenta treba uračunati**:

- obim potencijalnog incidenta (pogođeni objekat, lokaciju, proces...),
- troškove nabavke opreme i drugih materijala,
- troškove rada i zaposlenih na rešavanju incidenta,
- troškove legalnih/ugovornih kazni za ne ispunjavanje obaveza zbog incidenta i
- gubitke zarade od postojećih i potencijalnih klijenata.

U proračun troškova kontrola/mera zaštite treba uračunati:

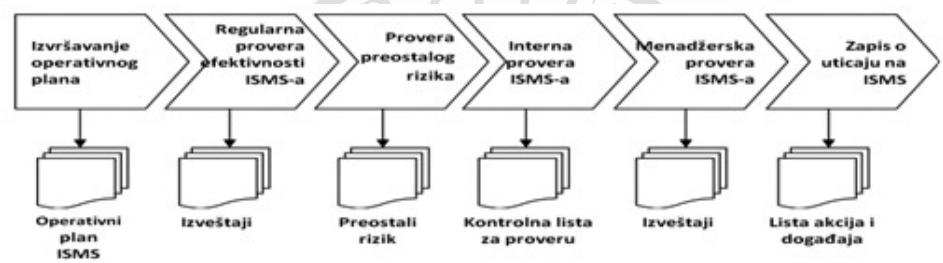
- kupovnu vrednost hardvera, softvera, implementacije servisa itd.,
- preostalu vrednost kontrola/mera zaštite, kad iste više nisu u upotrebi,
- spoljne troškove održavanja (servisiranja, popravki itd.) i
- interni troškovi održavanja kontrola/mera zaštite (uglavnom zaposleni).

Ove troškove najbolje je računati na godišnjem nivou. Očigledno, izuzetno je teško računati troškove za potencijalne gubitke, a još teže predvideti precizno verovatnoću događaja incidenta, posebno ako ne postoji njegova statistika. Međutim, i ovakva *procena* ROSI može

biti od koristi. Bolja metodologija (*Advanced Measurement Approach*) je u razvoju u okviru BASEL II u bankarskom sektoru, a najvažnije je koristiti zdravu logiku i uzimati u obzir menadžersku perspektivu troškova i gubitaka, koja često može biti različita, ali je relevantna za donošenje odluke.

8.3 PROVERA IMPLEMENTIRANOG ISMS-a

U fazi provere (*Check Phase*) vrše se revizije politike i procedura zaštite. Cilj ove faze je da se verifikuje postojanje politike i procedura zaštite, njihova primena u organizaciji i efektivnost u podršci procesa menadžmenta rizika i poslovnih ciljeva organizacije. Proces faze provere uključuje regularnu *nezavisnu, internu i menadžersku proveru* implementiranog i operativnog ISMS-a. Na slici 8.2 prikazani su koraci faze provere PDCA modela procesa.



Slika 8.2 PDCA faza provere implementiranog ISMS-a

Faze provere počinje sa poslednjim korakom faze primene — sa implementiranim ISMS-om i zahtevom za regularnu proveru efektivnosti ISMS-a, da bi se postigli operativni ciljevi i ciljevi menadžmenta rizika organizacije. Provera usaglašenosti treba da se zasniva na odobrenoj listi kontrola zaštite iz plana za tretman rizika (SoA) i politici zaštite, kreiranoj na bazi tog plana. Jedan od pristupa za gradaciju zahteva za efektivnost kontrola zaštite implementiranog ISMS-a prikazan je u tabeli 8.3.

Tabela 8.3 *Kriterijumi za proveru efektivnosti kontrola zaštite*

Kriterijum zahteva:	Opis
Efektivnost kontrole	Kontrole zaštite su efektivne kad smanjuju rizik i da rade kako se zahteva u svim odnosnim dokumentima.
Poboljšanje kontrole	Kontrole zaštite smanjuju neke faktore rizika i rade kako se zahteva u većini odnosnih dokumenata.
Novu kontrolu	Kontrola zaštite ne postoji za dati rizik ili kontrola ne radi kako treba.
Nije primenljivo ili se ne zahteva kontrola	Ne postoji odgovarajuća kontrola zaštite koja se može koristiti. Prihvatljivi rizik je nizak i implementacija kontrola nije opravdana ili postoji kompenzujuća (univerzalna) kontrola zaštite.

Usaglašenost prakse sa politikom zaštite, takođe, može biti predmet interne ili eksterne (nezavisne) provere performansi ISMS-a od strane akreditovanog sertifikacionog tela.

Sledeći korak je *provera preostalog rizika* i poređenje sa prihvatljivim rizikom, zatim balansiranje tekućih kontrola zaštite sa poslovnim vrednostima informacione imovine koju štite. Menadžerska provera rezultata interne provere ISMS-a i preostalog rizika, vrednuje njihovo razumevanje i usaglašenost sa ISMS-om i obezbeđuje ulaze za potencijalnu modifikaciju i poboljšanje ISMS-a u fazi delovanja (*Act phase*).

8.3.1 Izvršavanje operativnog plana

Za *efektivan ISMS* zahteva se formalni operativni plan, kao i metrike i merenja za obezbeđivanje operativne funkcionalnosti ISMS-a, u skladu sa poslovnim ciljevima i procenom rizika u organizaciji. ISMS može biti kompleksan i različiti delovi zahtevaju proveru u različito vreme. Vremenski plan i kontrolna (*ček*) lista za proveru ISMS-a su deo operativnog plana. U tabeli 8.4 predstavljena je čeklista za praćenje provera ISMS-a, registrovanje prethodne i planiranje sledeće provere. U redovima tabele navedeni su elementi za praćenje i proveru, a u kolonama meseci u godini. Simboli u tabeli označavaju planiranu proveru – P i narednu proveru – N.

Tabela 8.4 *Primer čekliste za praćenje provera ISMS-a*

Elementi ISMS	**Meseci (1-januar,….,12-decembar)**											
	1	2	3	4	5	6	7	8	9	10	11	12
Nalazi poslednje provere	P	N	P	P	P	P	P	P	P	P	P	P
Promene politike zaštite informacija i operativnog okruženja	P	N	P	P	P	P	P	P	P	P	P	P
Promene ISMS politike i operativnog okruženja	P	N	P	P	P	P	P	P	P	P	P	P
Interna organizaciona struktura i spoljni saradnici		N			P			P			P	P
Odgovornosti za imovinu, menadžment rizika, preostali rizik		P										
Zaposleni pre, u toku, premešteni ili otpušteni				P								
Restriktivna zona, oprema, mehanizmi zaštite						P						
Operativne procedure i odgovornosti					P							
Kontrola pristupa								P				
Zahtevi za zaštitu IKT sistema								P				
Zahtevi za zaštitu IKT sistema									P			
Menadžment bezbednosnih događaja, incidenata i ranjivosti	P	N	P	P	P	P	P	P	P	P	P	P
Menadžment BCP – priručnik, testiranje					P							
Provera usaglašenosti			P				P				P	P
Menadžerska provera ISMS-a				P								

Za *operativnu efektivnost ISMS-a* primenjuju se metrike i merenja koja mogu uključivati SLA ugovore u formi ciljeva, ciljnih vremena operativnog rada (*Uptime Goals*) (tabela 8.5) ili tolerisanog vremena prekida rada (*Downtime Tolerance*) IKT sistema (tabela 8.6) [62].

Tabela 8.5 Smernice za proračun ciljeva godišnjeg rada (uptime) IKT sistema

	Cilj	Dani	Sati	Minuti
	100.000%	365.00	8,760.00	525,600.00
59 s	99.999%	365.00	8,759.91	525,594.74
49 s	99.990%	364.96	8,759.12	525,547.44
39 s	99.900%	364.64	8,751.24	525,074.40
29 s	99.000%	361.35	8,672.40	520,344.00
	98.000%	357.70	8,584.80	515,088.00
	95.000%	346.75	8,322.00	499,320.00
	90.000%	328.50	7,884.00	473,040.00

Tabela 8.6 Smernice za proračun tolerisanog vremena prekida rada IKT sistema

	Cilj	Dani	Sati	Minuti
	100.000%	365.00	8,760.00	525,600.00
59 s	99.999%	0.00	0.09	5.26
49 s	99.990%	0.04	0.88	52.56
39 s	99.900%	0.37	8.76	525.60
29 s	99.000%	3.65	87.60	5,256.00
	98.000%	7.30	175.20	10,512.00
	95.000%	18.25	438.00	26,280.00
	90.000%	36.50	876.00	52,560.00

Ove tabele obezbeđuju vremenske implikacije u danima, časovima i minutima za lako razumevanje posledica angažovanja (*uptime*) ili pada (*downtime*) IKT sistema.

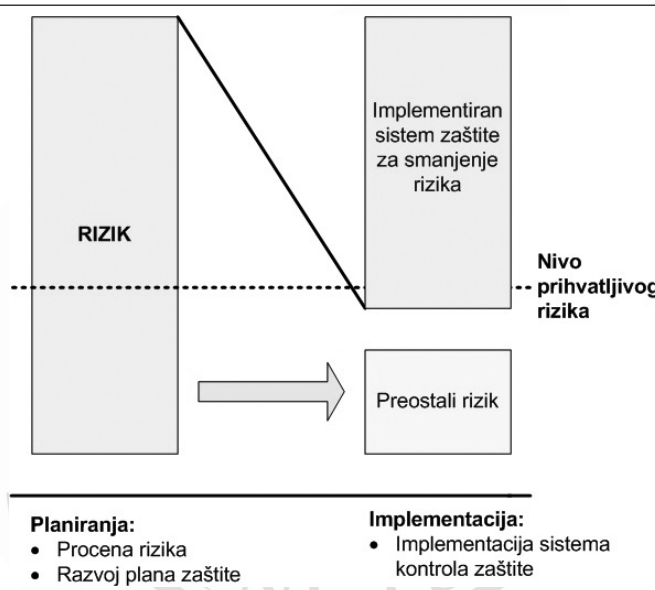
Primer: Ako se želi *uptime* od pet do devet sekundi godišnje ili obezbeđivanja funkcionalnosti od 99,99% vremena, to implicira *downtime* ne viši od 5,26 minuta godišnje. Pri tome treba odrediti da li je *downtime* vreme zbog servisa, greške hardvera ili bezbednosnih razloga. Ako se zaista zahteva godišnji operativni *uptime* od pet do devet sekundi, treba obezbediti redundantne funkcionalnosti – promocije, neprekidno zapošljavanje itd.

Druge metrike mogu uključiti praćenje bezbednosnih događaja i odgovora na njih, što podrazumeva da postoje svest o potrebi zaštite, alati za detektovanje anomalija i spremnost organizacije za upravljanje incidentom. U odnosu na svest o potrebi zaštite, obuku i obrazovanje, metrike mogu uključiti brojne provere pre zapošljavanja personala, slanje materijala

za razvoj svesti e-poštom i praćenje broja otvaranja i potvrda o prijemu itd. Većina metrika je specifična za organizaciju.

8.3.2 Provera nivoa preostalog rizika

Periodičnom proverom rizika identifikuje se i objašnjava svaki preostali rizik, poređenjem sa prihvatljivim, posebno onaj koji je veći od prihvatljivog rizika, usklađenog sa politikom zaštite. Pošto se poslovno okruženje brzo menja, preporučuje se periodična provera preostalog rizika. Na slici 8.3 prikazane su međuzavisnosti implementiranog sistema zaštite i rizika informacione bezbednosti.



Sl. 8.3 Međuzavisnost sistema zaštite i rizika [52]

Implementirani sistem zaštite smanjuje procenjeni bezbednosni rizik na prihvatljivi nivo. Potpisom dokumenta SoA menadžment organizacije prihvata preostali rizik. Politika zaštite informacija i plan tretmana rizika zahtevaju da se preostali rizik neprekidno monitoriše i regularno proverava. Cilj provere preostalog rizika je da se spreči eskalacija nekih faktora preostalog rizika iznad nivoa prihvatljivog rizika.

8.3.3 Interna provera ISMS-a

Internom proverom ISMS-a, organizacija utvrđuje da li postoje politika i procedure zaštite, a ako postoje i ako su u upotrebi, evaluira njihovu efektivnost. Glavna pitanja interne provere su da li postoji politika i procedura za određenu kontrolu zaštite, da li ih organizacija koristi i da li ih koristi efektivno? Upitnik za internu proveru, modelovan na bazi smernica

za sadržaj politike zaštite (videti tabelu 7.1), obezbeđuje proveru postojanja, ali i kvaliteta politike i procedura zaštite. U toku provere treba registrovati koje aspekte kontrola zaštite je organizacija implementirala, a koje nije (što je važnije). Proverom se skupljaju podaci za oba aspekta. Opšte smernice za izradu upitnika za internu proveru uključuju sledeća pitanja:

Identifikuj predmetnu kontrolu zaštite.

- Zašto je izabrana ova kontrola zaštite?
- Ko je odgovoran za politiku napisanu za tu izabranu kontrolu?
- Da li postoji politika zaštite?
- Da li postoji procedura?
- Da li organizacija u praksi zaštite koristi procedure?
- Ko je odgovoran za implementaciju procedure?
- Ko je odgovoran za praćenje efektivnosti procedure?
- Da li postoji metrika za praćenje efektivnosti procedure?
- Kako odgovorno lice meri ove metrike?
- Koji izveštaji postoje za praćenje efektivnosti kontrole?

U tabeli 8.7 dat je generički obrazac za internu proveru ISMS-a, a specifični detalji zavise od tipa organizacije.

Tabela 8.7 *Obrazac za internu proveru ISMS-a*

Ime proverivača:						**Podaci:**
Odlična	Prihvatljiva	Za poboljšanje	Nepotpuna	Promena kontrole	Kompletna	**Kontrola zaštite**: *<Primedba proverivača>* **Opravdanje**: *<Kratak opis>*
						Za politiku i procedure postoji jasna odgovornost.
						Politika zaštite postoji, a sadržaj zadovoljava ili premašuje ciljeve.
						Procedura postoji, a sadržaj zadovoljava ili premašuje ciljeve.
						Zaposleni koriste procedure u svom radu.
						Postoje metrike i merenja za procenu efektivnosti procedura.
						Postoje izveštaji o praćenju efektivnosti kontrola.
Dodatni detalji:						

Generalno, *cilj interne provere je da se utvrdi stanje sistema zaštite organizacije sa najmanje troškova*. Efektivan proces interne provere sistema zaštite zahteva angažovanje nezavisnog TTP provajdera usluga, koji koristi kratku jednostavnu formu upitnika za agregaciju rezultata iz više izvora.

U tabeli 8.8 dat je izvod potencijalnog upitnika za internu proveru tekućeg stanja ISMS-a, koji obuhvata 40 kategorija sistema zaštite — od *menadžmenta rizika i menadžmenta usaglašenosti,* preko *kriptografije*, *zaštite privatnosti* itd., do *fizičke zaštite* [39]. Malo je verovatno da će se koristiti sva pitanja iz upitnika, zbog velikog broja detalja i slabe korisničke prihvatljivosti u konkretnoj organizaciji. Naime, detaljna pitanja iz upitnika su pre okvir iz kojeg konkretna organizacija treba da izabere adekvatan skup pitanja za internu proveru sistema zaštite u specifičnom okruženju.

Tabela 8.8 *Primer strukture upitnika za internu proveru ISMS-a (Audit Checklist)*

Kategorija sistema zaštite	Broj interne reference	Broj reference standarda	Pitanje	Odgovori			
				Da	Ne	N/A	N/P
Menadžment rizika	1	ISO 27005					
Menadžment rizika	1.1		Da li organizacija ima politiku koja sadrži potrebu za menadžmentom rizika?				
Menadžment rizika	1.2		Da li ta politika zahteva, specificira ili na drugi način obuhvata sledeće:				
Menadžment rizika	1.2.1		*identifikaciju prihvatljivog rizika za organizaciju?*				
Menadžment rizika	1.2.2		*Procenu rizika?*				
Menadžment rizika	1.2.3		*Komponente rizika, uključujući:* *oblast pretnji?* *oblast imovine?* *oblast ranjivosti?* *oblast uticaja na poslovanje?*				
Menadžment rizika	1.2.4		Izveštavanje o rezultatima procene rizika, npr: *gap analizu između prihvatljivog i tekućeg rizika*?				
Menadžment rizika	1.2.5		Izveštaj o analizi tretmana rizika, npr: specifikacija (plan) kako pojačati sistem zaštite ili smanjiti rizik na prihvatljiviji nivo?				
Menadžment rizika	1.2.x		**Napomena**: Postavite dodatna pitanja koja za specifičnu organizaciju određuju kvalitet kontrola!				
Menadžment rizika	1.3		Da li organizacija ima proceduru koja opisuje kako implementirati i nametnuti politiku menadžmenta rizika?				
Menadžment rizika	1.4		Da li ova procedura zahteva specifične ili na drugi način obuhvata sledeće:				

Kategorija sistema zaštite	Broj interne reference	Broj reference standarda	Pitanje	Odgovori			
				Da	Ne	N/A	N/P
Menadžment rizika	1.4.1		*širinu obima*: procenu oblasti pretnji, imovine, ranjivosti i poslovnog uticaja?				
Menadžment rizika	1.4.2		*Dubinu obima*: intervjui – pitanja? Verifikaciju – opservacije? Validaciju – ličnu proveru?				
Menadžment rizika	1.4.x		**Napomena**: Postavite pitanja koja razjašnjavaju procedure za implementaciju politike tipa: „*Da li imate proceduru koja opisuje kako implementirati politiku X?*“				
Menadžment rizika	1.5		Da li organizacija primenjuje u praksi gore opisane procedure?				
Menadžment rizika	1.6		Da li ova praksa uključuje ili na drugi način obuhvata sledeće:				
Menadžment rizika	1.6.x		**Napomena**: postavite pitanja koja razjašnjavaju praksu organizacije tipa: „*Da li stvarno izvršavate politiku koja propisuje X?*“				
Menadžment usaglašenosti	2	ISO/IEC 27001/2					
Menadžment usaglašenosti	2.1		Da li organizacija ima politiku za menadžment usaglašenosti?				
Menadžment usaglašenosti	2.2.1		*Obim*: eksplicitni poslovni zahtevi, implicitni zahtevi menadžmenta rizika (zahtevi zaštite) i eksplicitni zahtevi zaštite.				
Menadžment usaglašenosti	2.2.2		.....				
.....							
Fizička zaštita	31						
Fizička zaštita	31.1		Da li organizacija ima politiku fizičke zaštite?				
Fizička zaštita	....						
Fizička zaštita	31.2.10		Da li su ulazna vrata označena tako da ne ukazuju na osetljive zone?				

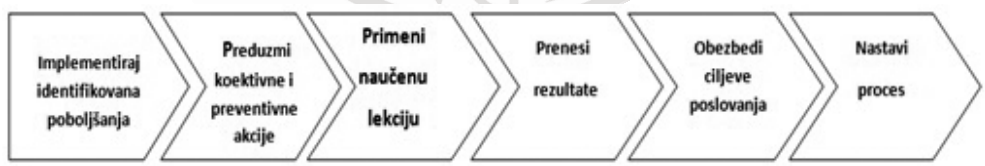
8.3.4 Regularna menadžerska revizija ISMS-a

Standard ISO/IEC 27001 zahteva regularnu menadžersku reviziju ISMS-a. Menadžere, uglavnom, interesuje izveštavanje o efektivnosti ISMS-a u kontekstu podrške poslovnim ciljevima organizacije, a manje — specifičnosti procedura, standarda i mehanizama zaštite. Tim za zaštitu upravlja generisanjem neophodnih dokumenata za menadžersku reviziju. Rezultati menadžerske revizije efektivnosti ISMS-a koriste se za reviziju politike zaštite. Tim za zaštitu koristi rezultate provere i izveštaj menadžerske provere za razvoj plana provere ISMS-a, koji obezbeđuje ulazne veličine u PDCA fazu poboljšavanja (*Act Phase*). Dokumentacija koja se generiše u fazi provere sadrži osetljive informacije i mora se bezbedno skladištiti, a uključuje:

- metrike i merenja za individualne izabrane kontrole zaštite,
- ažuriranu listu preostalih faktora rizika,
- kontrolnu listu za internu proveru (*Audit checklist*),
- rezultate procesa interne provere ISMS-a i
- akcioni plan (lista stavki) poboljšanja ISMS-a.

8.4 POBOLJŠAVANJE ISMS-a (*Act Phase*)

U ovoj fazi PDCA procesa obezbeđuju se uslovi za poboljšanje ISMS-a (slika 8.4). Inicijative za poboljšanje ISMS-a dolaze iz faze provere i mogu uključivati zahteve za *modifikaciju, dodavanje ili odustajanje od preventivnih* (zaštite, monitoringa) i *korektivnih* (detekcije, registrovanja, eskalacije, odgovora) *mera.* Sva stečena iskustva treba primeniti na nove inicijative, a rezultate preneti svim delovima organizacije, ponavljajući neprekidno da je *zaštita informacija proces, a ne odredište*. Poslednji korak zahteva kontinualnu proveru i poboljšanje, inherentno ciklusu PDCA procesa.



Slika 8.4 PDCA faza poboljšanja procesa (Act phase)

U fazi provere monitoriše se i revidira efektivnost ISMS-a, a jedan od izlaznih rezultata je preporuka za poboljšanje ISMS procesa. Ovo poboljšanje se implementira u poslednjoj fazi (*Act phase*) PDCA modela. Sugestija za poboljšanje ISMS-a može doći iz procesa monitoringa sistema zaštite u odnosu na ciljeve SLA-a ili iz procesa interne provere. Rezultati menadžerske provere ISMS-a, inicirane promenama u poslovnom okruženju i zahtevom za usaglašavanje, takođe, mogu biti ulazi za poboljšanje ISMS-a. Na kraju, izvor podataka za

poboljšanje ISMS-a mogu biti rezultati spoljne (nezavisne) provere ISMS-a, kojom se verifikuju i vrednuju performanse implementiranih kontrola zaštite, politike i procedura ISMS-a. Tim za zaštitu informacija organizacije izvršava i nadgleda proces poboljšanja ISMS-a.

Stečena iskustva se uglavnom odnose na događaje, koji su najteže pogodili organizaciju, a u organizaciji se identifikuju periodičnom proverom politike, procedura i operativnih rezultata ISMS-a. Organizacija, takođe, treba da koristi i tuđa iskustva za poboljšanje ISMS procesa iz industrijske prakse zaštite, zbornika radova sa naučnih konferencija, seminara i drugih izvora. Sva iskustva treba ugraditi u PDCA smernice u fazi ažuriranja dokumentacije zaštite, kao i u ISMS politiku i procedure. Takođe, treba skupljati podatke o modifikaciji metrika i merenja, distribuciji informacija, internoj proveri ISMS-a i drugim projektima modifikacija u organizaciji.

Za obuku o rezultatima poboljšanja ISMS-a, kao i kod implementacije ISMS-a u organizaciji, zahtevaju se dodatne aktivnost, kao što su izmene u programu razvoja svesti o potrebi zaštite, obuci i obrazovanju u zaštiti itd.

Posle implementacije svake kontrole zaštite, treba je verifikovati i vrednovati, tj. uveriti se da je kontrola implementirana, da radi kako je namenjeno i da zadovoljava ciljeve ISMS-a.

Na kraju ove faze, poslednji korak PDCA procesa vodi u fazu planiranja, tj. obnavljanja PDCA ciklusa, sa fokusom na nove pretnje i ranjivosti i promene okruženja. Dokumenta, koja se generišu u fazi poboljšavanja, su revizije svih prethodnih dokumenata, uključujući:

- ISMS smernice za fazu poboljšavanja,
- metrike i merenja,
- ažuriranje preostalog rizika,
- kontrolne lista za proveru (*Audit checklist*),
- rezultate interne i menadžerske provere i
- akcioni plan poboljšanja ISMS-a (lista stavki koje treba uraditi).

Kao rezultat rada svih faza PDCA modela generišu se sledeća dokumenta:

- *ISMS politika*
- *obim ISMS-a*: lista značajnih poslovnih funkcija (*lista ključnih poslovnih procesa*); lista informacione imovine sa klasifikacijom u kontekstu podrške poslovanja;
- *politika komponenti zaštite* koje podržavaju ISMS politiku: politika koja usmerava izbor i implementaciju kontrola zaštite, npr. *politika lozinke*, *politika udaljenog pristupa, politika e-poslovanja* itd.;
- *ISMS procedure*: smernice koje pokazuju kako implementirati politiku zaštite;
- *ISMS standardi*: specifične kontrole za implementaciju politike;
- *metodologija procene rizika*: dokumentuje kako organizacija vrši procenu rizika;
- *nalazi procene rizika*: rezultat primene metodologije procene rizika u organizaciji;
- *plan tretmana rizika*: lista metoda na koji organizacija tretira svaki faktor rizika – *prihvata, ignoriše, prenosi, deli ili ublažava;*
- *procedure***:** više dokumenata koja sadrže precizno izvršavanje aktivnosti efektivnog planiranja, rada, kontrola sistema zaštite informacija i odnosnih procesa i metrike;
- *zapisi i logovi*: evidentiraju relevantne događaje koji pokazuju usklađenost sa ISO standardima zaštite.

Međutim, za projektovanje ISMS-a, korisna su sledeća dokumenta zaštite, iako ih standard ISO/IEC 27001 specifično ne zahteva:

- priručnik za zaštitu,
- plan kontinuiteta poslovanja (BCP),
- plan oporavka od pada sistema (DRP),
- plan obuke,
- materijal za obuku,
- opis rada ISMS-a,
- plan menadžmenta bezbednosnog incidenta,
- plan metrika i merenja, uključujući usaglašavanje sa poslovnim pokretačima i menadžmentom poslovnog rizika,
- ažurna lista preostalog rizika,
- kontrolna lista za proveru ISMS-a (*Audit checklist*),
- rezultati interne provere ISMS-a,
- proces provere i ažuriranja ISMS-a, uključujući događaje za iniciranje provere (npr. vremenski plan, incident, promene poslovnog okruženja itd.) i
- akcioni plan poboljšanja ISMS-a (*ISMS improvement list*).

Nacrt sadržaja plana projekta za poboljšanje procesa zaštite dat je u **Prilogu 8.2.**

8.5 REZIME

Za razvoj i implementaciju ISMS-a i programa zaštite informacija primenjuje se PDCA model procesa. ISMS je samo jedan od ISO menadžment sistema u okviru TQM menadžment sistema organizacije, sa krajnjim ciljem implementacije, održavanja i poboljšanja totalnog menadžment sistema poslovanja. Svaka od četiri faze PDCA modela pokriva različite aspekte ISMS-a — uspostavljanje, implementaciju, proveru i poboljšanje.

U *fazi primene* implementira se ISMS, razvija sveobuhvatni program zaštite informacione imovine i generišu dokumenta relevantna za ISMS operacije. Implementacija plana ISMS-a nameće sprovođenje zahteva za usaglašenost. Menadžment rizika olakšava rad na uspostavljanju operativnih funkcija — *servisa mehanizama i protokola sistema zaštite*. Alati zaštite nameću politiku usaglašenosti sistema zaštite. U ovoj fazi mogu da se generišu *priručnik za zaštitu* koji uključuje sve do sada opisane kontrole zaštite i *plan menadžmenta kontinuiteta poslovanja*.

U *fazi provere* revidira se i proverava efektivnost servisa (kontrola) zaštite. Jedno merenje efektivnosti predstavlja procena usaglašenosti. Rezultati PDCA faze provere uključuju reviziju zahteva za usaglašenost, sa ciljem da se utvrdi u kojoj meri zadovoljavaju tekuće zahteve za usaglašenost (npr. novog zakona i regulativa informacione bezbednosti i menadžmenta rizika). Procena usaglašenosti, takođe, određuje tekući nivo usaglašenosti u odnosu na postojeće zahteve. Ovaj proces identifikuje razlike i tretira svaku razliku u terminima menadžmenta rizika.

U *fazi poboljšanja*, preduzimaju se akcije koje implementiraju brojne rezultate i nalaze iz faze provere u sve procese organizacije, sa ciljem neposrednog poboljšanja PDCA procesa i ISMS-a i indirektno – poboljšanje poslovnih procesa organizacije.

Sva preporučena dokumenta zaštite podržavaju uspostavljanje, implementaciju i tekuće održavanje ISMS-a i ključni su faktori za ISO/IEC 27001 sertifikaciju. Proces ISMS-a podržavaju i brojna druga dokumenta, uzorci, obrasci i opšti elementi ISMS standarda, kao što su: *definicija uloga i odgovornosti, kontrola dokumenata, zapisi menadžmenta, obuka, menadžerska i interna provera, korektivne i preventivne akcije, PDCA model, proces provere, zahtevi u sličnim standardima* itd. Za program razvoja svesti o potrebi zaštite, obuku i formalno obrazovanje generišu se *relevantni materijali, dokumentovani plan i operativni opis ISMS-a*. Menadžment kompjuterskog incidenta generiše *izveštaj o incidentu i ekspertski izveštaj* o uzrocima incidenta. Politika zaštite obezbeđuje zahteve za kreiranje ovih dokumenata i procedura za njihovu upotrebu, kao i zahteve za uzorke, obrasce i alate za skupljanje podataka, analizu i izveštavanje, koji doprinose proveri ISMS-a za ISO/IEC 27001 sertifikaciju.

Lista dokumenata, koju generišu sve faze PDCA modela procesa i formalno definiše ISMS standard, podržava uspostavljanje, implementaciju i održavanje ISMS-a i predstavlja ključni elemenat za proveru i ISO/IEC 27001 sertifikaciju. ISMS podržavaju i brojni obrasci, upitnici, kontrolne liste i drugi aktuelni detalji. Sva preporučena i druga dokumenta uključuju zajedničke elemente ISMS standarda, koji se zasnivaju na angažovanju menadžmenta — *uloge i odgovornosti, kontrolu dokumenata, obuku, menadžersku reviziju, internu proveru i korektivne i preventivne akcije*.

8.6 PITANJA ZA PONAVLJANJE

1. Ključni procesi *faze primene* su:
   a. sprovođenje plana za tretman rizika
   b. ažuriranje politike kontrola zaštite
   c. izrada plana zaštite
   d. implementacija procedura zaštite.
2. Implementacija *plana tretmana rizika* počinje sa:
   a. razvojem svesti o potrebi zaštite
   b. pisanjem (ili ažuriranjem) politike za svaku kontrolu zaštite
   c. izradom procedure zaštite
   d. formiranjem tima za zaštitu.
3. Plana za tretman rizika sadrži:
   a. listu svih faktora rizika
   b. identifikaciju odgovornosti svih zaposlenih u menadžmentu rizika
   c. akcije za sprovođenje politike zaštite
   d. operativne zadatke za aktivnosti menadžmenta rizika.
4. Standard ISO/IEC 27001 za dokumentaciju preporučuje:
   a. razdvajanje dokumenata zaštite
   b. izradu jedinstvenog dokumenta zaštite
   c. modularnost dokumenata zaštite
   d. precizna, kratka i korisnički usmerena dokumenta zaštite.
5. Izjava o *nameni politike zaštite*:
   a. obavezan je deo svake politike zaštite
   b. proizvoljan je deo svake politike zaštite
   c. sadrži specifične ciljeve kontrola zaštite
   d. sadrži opšte ciljeve kontrola zaštite.
6. Glavna namena metrika i merenja u sistemu zaštite je da:
   a. utvrdi tekuće stanje i efektivnost operacija sistema zaštite
   b. utvrdi broj napada sa Interneta
   c. utvrdi progres u funkcionalnosti, sveobuhvatnosti, usaglašenosti itd.
   d. utvrdi broj internih napada.
7. *Merenje* u sistemu zaštite je:
   a. čin poređenja u odnosu na definisan etalon
   b. *atribut* za merenje kvaliteta performansi sistema zaštite
   c. agregacija rezultata višekratnog merenja
   d. utvrđivanje jednokratnog stanja sistema zaštite.
8. *Metrika* u sistemu zaštite je:
   a. čin poređenja u odnosu na definisan etalon
   b. *atribut* za merenje kvaliteta performansi sistema zaštite
   c. agregacija rezultata višekratnog merenja
   d. utvrđivanje jednokratnog stanja sistema zaštite.
9. Identifikovanje i izbor korisnih metrika i merenja sistema zaštite informacija je:
   a. uglavnom trivijalan zadatak
   b. problematično, jer se na svim nivoima traže različita značenja u rezultatima
   c. jednostavno, jer se na svim nivoima traže ista značenja u rezultatima
   d. neizvodljivo, jer ne postoje merenja i metrike u zaštiti informacija.
10. U politici zaštite, za ublažavanje rizika, obavezno treba definisati:
    a. kratkoročni cilj merenja efektivnosti politike zaštite
    b. način skladištenja metričkih podataka
    c. tip merenja efektivnosti politike zaštite
    d. dugoročni cilj merenja efektivnosti politike zaštite.
11. Proces selekcije i implementacije kontrola zaštite je:
    a. strogo definisan standardom zaštite
    b. uglavnom određen smernicama SMF okvira za zaštitu
    c. nepromenljiv za sve organizacije
    d. specifičan za svaku organizaciju.

12. Da li je moguće računati povratak investicija za implementaciju ISMS (SROI)?
    a. Ne postoji konzistentan izvor informacija za proračun SROI.
    b. Nije moguće računati SROI.
    c. Na Internetu postoje određene informacije i više metoda za proračun SROI.
    d. Najviše korisnih informacija nalazi se na sajtu www.gocsi.com.
13. Svest o potrebi zaštite obezbeđuje:
    a. poznavanje nečega o zaštiti
    b. razumevanje nečega u zaštiti
    c. posedovanje specifične veštine u zaštiti
    d. znanje i sposobnost izvođenja obuke u zaštiti.
14. Obuka u zaštiti obezbeđuje:
    a. poznavanje nečega o zaštiti
    b. razumevanje nečega u zaštiti
    c. posedovanje specifične veštine u zaštiti
    d. znanje i sposobnost izvođenja obuke u zaštiti.
15. Obrazovanje u zaštiti obezbeđuje:
    a. poznavanje nečega o zaštiti
    b. razumevanje nečega u zaštiti
    c. posedovanje specifične veštine u zaštiti
    d. znanje i sposobnost izvođenja obuke u zaštiti.
16. Glavni ciljevi menadžmenta implementiranog ISMS-a su:
    a. upravljanje promenama
    b. efektivno upravljanje tekućih operacija zaštite i rizika poslovanja organizacije
    c. održavanje kontinuiteta poslovanja organizacije
    d. održavanje prihvatljivog nivoa rizika za CIA informacione imovine.
17. P*roces menadžmenta* bezbednosnog *incidenta* treba da uključi, najmanje:
    a. politiku, procedure i alata za podršku
    b. pripremu, procenu, menadžment, oporavak i reviziju
    c. politiku, procedure, infrastrukturu i alata za podršku
    d. pripremu, registrovanje, procenu, menadžment, oporavak i reviziju.
18. Efektivan *plan menadžmenta* bezbednosnog *incidenta* treba da uključi, najmanje:
    a. politiku, procedure, infrastrukturu i alate za podršku
    b. politiku, procedure i alate za podršku
    c. pripremu, registrovanje, procenu, menadžment, oporavak i reviziju
    d. pripremu, procenu, menadžment, oporavak i reviziju.
19. Detekciju incidenta obezbeđuju:
    a. u prvom redu profesionalci u zaštiti, pa zaposleni i mehanizmi zaštite
    b. u prvom redu zaposleni, pa mehanizmi zaštite i profesionalci u zaštiti
    c. mehanizmi zaštite, profesionalci u zaštiti i zaposleni
    d. isključivo mehanizmi zaštite.
20. Odgovor na kompjuterski incident zahteva:
    a. formiranje multidisciplinarnog tima koji uključuje i digitalnog forenzičara
    b. formiranje multidisciplinarnog tima koji ne zahteva digitalnog forenzičara
    c. *ad hoc* odgovor bez plana i prethodne pripreme
    d. pripremljen i planiran odgovor uvežbanog tima sa odgovarajućim alatima.
21. Proces PDCA faze provere uključuje:
    a. regularnu nezavisnu proveru implementiranog i operativnog ISMS-a
    b. kontrolu implementacije ISMS-a
    c. regularnu internu i menadžersku proveru implementiranog i operativnog ISMS-a
    d. izbor kontrola zaštite za poboljšanje implementiranog i operativnog ISMS-a.
22. Operativna efektivnost ISMS-a zahteva:
    a. primenu metrike i merenja
    b. određivanje ciljnih vremena operativnog rada (*Uptime Goals*)
    c. određivanje ciljnog tolerisanog vremena prekida rada (*Downtime Tolerance*)
    d. uspostavljanje tima za zaštitu informaciju.

23. Ulazni podaci u PDCA fazu poboljšanja uzimaju se iz:
    a. plana zaštite
    b. plana tretmana rizika
    c. interne, nezavisne i menadžerske provere
    d. izjave o primenljivosti (SoA).

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM



9. SERTIFIKACIJA, AKREDITACIJA I USAGLAŠAVANJE ISMS-a

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Metodologiju i strukturu procesa sertifikacije i akreditacije (C&A)
- ☑ Uloge i odgovornosti, faze i aktivnostie i dokumentacij C&A procesa
- ☑ Menadžment procesa C&A – faza pred-sertifikacije, sertifikacije, post-sertifikacije, akreditacije i post-akreditacije
- ☑ Sertifikacija i usaglašavanje sa standardima ISO/IEC 27001/2
- ☑ Menadžment proces usaglašavanja bezbednosti informacija (IA CPM)

9.1 UVOD

Sertifikacija je proces procene efektivnosti sistema *kontrola zaštite* informacione imovine i usaglašenosti sa standardima zaštite. Složenost sistema je glavni problem u procesu sertifikacije, jer je za kompleksniji sistem teže detaljno evaluirati sve njegove kontrole zaštite. Rezultati sertifikacije obezbeđuje ovlašćenom menadžeru informacije donošenje odluke o puštanju sistema u rad ili sertifikatoru da proceni nivo usaglašenosti sistema zaštite sa standardom.

Akreditacija je formalna autorizacija za rad IKT sistema i integrisanog (pod)sistema zaštite, koju daje nadležni menadžer organizacije, na bazi rezultata sertifikacije. Akreditacijom menadžment, takođe, potvrđuje da prihvata preostali rizik. Formalizacije procesa akreditacije smanjuje mogućnost da IKT i sistem zaštite budu pušteni u rad, bez odgovarajuće kontrole menadžmenta. Posle značajnih promena u IKT sistemu, okruženju ili tehnologijama, ponavljaju se procesi sertifikacije i akreditacije.

Brojne organizacije preduzimaju nezavisnu proveru i ISO/IEC 27001 sertifikaciju. ISMS sertifikat važi oko tri godine i onda se zahteva resertifikacija [87]. Bezbednosna usaglašenost podrazumeva primenu PDCA ciklusa, *ciljeva* i *kontrola zaštite* prema Aneksu A ISO/IEC 27001 i ISO/IEC 27002. Međutim, moguće je dobijanje ISO/IEC 27001 sertifikata i uspostavljanjem usaglašenosti sa drugim ISO i srodnim standardima zaštite (npr. *SOX,* HIPAA ili FISMA). Uspostavljanjem okvira za menadžment zaštite (SMF), kao osnove za bezbednosnu usaglašenost, omogućava razvoj jedinstvene metodologije i alata koji realizuju, registruju i dokazuju usaglašenost sa svim primenljivim bezbednosnim zahtevima. Glavni ciljevi uspostavljanja bezbednosne usaglašenosti sa standardima su *identifikovanje razlika* između generičkog *menadžment programa usaglašenosti* (CMP) i menadžment programa bezbednosne usaglašenosti (IA CMP) i opisivanje metodologije, procesa, alata i obrazaca za planiranje, uspostavljanje, implementaciju, održavanje, proveru i izmenu IA CMP.

9.2 ORGANIZACIJA PROCESA SERTIFIKACIJE I AKREDITACIJE

9.2.1 Uloge i odgovornosti u procesu sertifikacije i akreditacije

Ključne uloge i odgovornosti u procesu *sertifikacije i akreditacije* (S/A) su: (1) *naimenovani akreditator* – DAA (*Designated Acreditation Authority*), (2) *sertifikator*/sertifikaciono telo (CA) koje sertifikuje i izdaje sertifikat, (3) *rukovodilac programa* ili vlasnik sistema koji zahteva sertifikaciju i (4) *specijalista za zaštitu.* Za veći integritet i objektivnost akreditacije, mogu se uvesti i dodatne uloge [89].

Akreditator je obično stariji menadžer koji ima ovlašćenja da: *formalno odobri rad IKT sistema na prihvatljivom nivou rizika; nadgleda budžet; odobri dokumenta zaštite, sporazume i odstupanja od politike zaštite; zabrani ili zaustavi rad sistema, ako je rizik neprihvatljiv i formalno donosi akreditacionu odluku,* za – *punu, privremenu* ili *odbijenu akreditaciju sistema*, a na osnovu rezultata sertifikacije i procene rizika. Ovu odluku dokumentuje u *akreditacionom paketu* koji sadrži *izjavu o akreditaciji*, *sertifikacioni paket* i *obrazloženje odluke*.

Sertifikator/*CA* je odgovoran za: *procenu usaglašenosti sa bezbednosnim zahtevima ISMS standarda; koordinaciju svih aktivnosti; nezavisnu tehničku i netehničku procenu sistema zaštite i generisanje sertifikacionog paketa*. Da bi se sačuvala objektivnost sertifikacinog procesa, sertifikator treba da bude nezavisan od vlasnika, korisnika i administratora zaštite. U svetu je mali broj sertifikacionih tela za zaštitu informacija (11), sa trendom rasta[1]. Generički zahtevi za sertifikaciona tela propisani su u ISO/IEC *Guide 62* dokumentu.

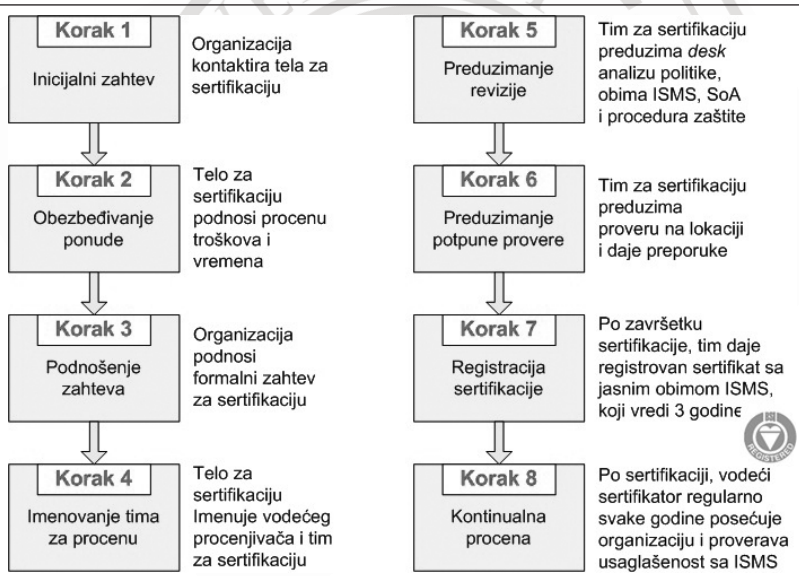
Rukovodilac programa/vlasnik sistema, odgovoran za IKT sistem u toku životnog ciklusa, u kontekstu sistema zaštite obezbeđuje: *razvoj i rad sistema prema bezbednosnim zahtevima plana zaštite; adekvatnu obuku u zaštiti; koordinaciju rada; potrebno osoblje i informacije za sertifikatora/tim; troškove sertifikacije i uvid u sertifikacioni izveštaj pre dostavljanja akreditatoru*.

1 Engl.: BS 7799: BSI, Certification Europe, DNV, JACO IS, KEMA, KPMG, SFS-Sertifiointi Oy, SGS, STQC, SAI Global Limited, UIMCert GmbH.

Specijalista za zaštitu sistema u radu odgovoran je za *svakodnevnu bezbednost IKT sistema, upravljanje incidentom, razvoj svesti o potrebi zaštite, obuku i obrazovanje, razvoj politike zaštite, usaglašenost prakse i politike zaštite, identifikovanje sistema za resertifikaciju ili reakreditaciju* i za *stručno rukovođenje programom zaštite* sistema u razvoju. Po potrebi mogu se uključiti i druge uloge (korisnici, menadžeri programa zaštite i administratori zaštite [89].

9.2.2 Proces sertifikacije

Standard ISO/IEC 27006 daje uputstva i smernice telima za sertifikaciju i akreditaciju ISMS-a. Cilj procesa sertifikacije nije da se dokaže potpuna zaštita, nego da se ugrade procesi planiranja, implementacije, nadzora, provere i menadžmenta promena sistema zaštite i dokaže nivo usaglašenosti politike, standarda i procedura zaštite organizacije sa referentnim standardima ISO/IEC 27001/2. O*rganizaciona struktura procesa* nezavisne ISMS sertifikacije sadrži 8 koraka (slika 9.1).



Slika 9.1 Organizaciona struktura procesa nezavisne ISMS sertifikacije

U prvom koraku organizacija šalje akreditovanom *sertifikacionom telu* (**CA**) inicijalni *zahtev za ponudu* za sertifikaciju. U drugom koraku ST razmatra zahtev, vrši pripremu, procenjuje troškove i uspostavlja profakturu za formalnu sertifikaciju. Zatim, u trećem koraku, organizacija podnosi CA-u formalni zahtev za sertifikaciju, a u ćetvrtom koraku CA imenuje vodećeg sertifikatora koji postaje glavni kontakt za organizaciju. U petom koraku sertifikator pregleda dokumenta zaštite – *procenu rizika, politiku i procedura, obim ISMS-a i SoA* i identifikuje greške, propuste i slabosti u ISMS-u. U šestom koraku sertifikaciono telo proverava stanje na lokaciji organizacije i daje preporuke. Po završenoj proveri, u sedmom

koraku, sertifikator daje registrovani sertifikat sa jasno identifikovanim obimom ISMS-a. U osmom koraku, sertifikator u regularnim intervalima svake godine posećuje organizaciju i pomaže održavanje nivoa sertifikacije ISMS-a. Sam proces sertifikacije obično se sastoji od sledećih faza i aktivnosti, sa manjim varijacijama između sertifikatora/CA:

- **FAZA pre provere**: izbor akreditovanog CA-a, priprema za sertifikaciju,
- **FAZA provere** (ispitivanja, testiranja), aktivnosti: pre posete lokaciji – *faza 1, faza 2;* za vreme posete lokaciji – *faza 3 i* posle posete lokaciji – *faza 4* i
- **FAZA posle provere.**

Većina sertifikatora opisuje svoje aktivnosti u *fazama* i to *pre, za vreme i posle provere*, kao i *pre, za vreme i posle posete lokaciji* ispitivane organizacije. Neki standardi kao NIST SP 800 37 definišu bezbednosne nivoe procesa sertifikacije – SLC1, SLC2 i SLC3, koji se razlikuju po dubini i intenzitetu provere (ispitivanja i testiranja) sistema kontrola zaštite [89].

Faza pre provere uključuje izbor sertifikatora i pripremu materijala za podršku procesa sertifikacije. Organizacija mora da izabere akreditovano CA za sertifikaciju usaglašenosti sa ISMS standardom. U pripremi *procesa provere*, organizacija prikuplja sva relevantna dokumenta i obaveštava odgovarajuće osoblje o predstojećim aktivnostima. Pre posete sertifikator pregleda dokumentaciju, u toku posete – proverava da li je praksa zaštite usaglašena sa dokumentacijom, a posle posete – analizira rezultate i dostavlja izveštaj organizaciji. U ovoj tački mogu se zahtevati korektivna akcije, pre akreditacije sistema i izdavanja sertifikata.

Izbor i imenovanje akreditovanog CA u praksi, najčešće, određuje nacionalno akreditaciono telo (**AT**), koje akredituje sertifikatora/tim, koji tada postaje akreditovano CA za predmetni standard/e. Organizacija ne može da sertifikuje samu sebe da je usaglašena sa ISO/IEC 27001 standardom; takvu proveru mora da sprovede TTP, koji se izuzima samo u slučaju da je učestvovao u uspostavljanju ISMS-a. Cilj sertifikacije je da se potvrdi postojanje i usaglašenost prakse zaštite i odgovarajuće dokumentacije ISMS-a u organizaciji.

U fazi pripreme procesa sertifikacije sertifikator/tim generiše sveobuhvatni spisak (tabela 9.1) materijala i aktivnosti koje su neophodne za pripremu organizacije za proveru. Sertifikator interno proverava postojanje i kvalitet svakog dokumenta u poređenju sa ISO/IEC 27001/2 standardima, kao i praksu organizacije u odnosu na dokumentaciju, koja uključuje primenjene standarde, politiku i procedure zaštite.

Tabela 9.1 *Spisak dokumenata i aktivnosti za pripremu procesa sertifikacije*

Dokumentacija	Opis
Oblast ISMS	Dokument koji opisuje granice ISMS-a.
Klasifikacija informacione imovine	Dokument iventara važne informacione imovine; uključuje klasifikaciju imovine sa naznačenom vrednosti za organizaciju.
Politika ISMS	Izražava politiku organizacije u odnosu na ISMS.
Politika zaštite informacija	Opisuje ISMS organizacije običnim rečnikom; u nekim slučajevima ISMS politika može biti deo ovog dokumenta.
Procena rizika	Opisuje procese, standarde, obrasce i metode procene rizika.

Dokumentacija	Opis
Izbor kontrola zaštite iz ISO/IEC 27001/2 (SoC)	Dokument sa listom odgovarajućih kontrola zaštite iz ISO/IEC 27001/2.
Plan tretmana rizika	Dokument sa planom tretmana faktora rizika organizacije.
Izjava o primenljivosti (SoA)	Uključuje listu svih ISO/IEC 27001/2 kontrola i izjave za svaku o tretmanu kontrole u kontekstu menadžmenta poslovnog rizika.
Priručnik zaštite informacija	Dokument koji uključuje sve kontrole i procedure zaštite organizacije.
Menadžment kontinuiteta poslovanja	Dokument koji upravlja kontinuitetom poslovanja i oporavkom organizacije posle incidenta; uključuje BCP i DRP.
Dokumenti za razvoj svesti, obuku i obrazovanje o zaštiti	Dokumenti koji opisuju svest o potrebi zaštite informacija, obuku i obrazovanje zaposlenih, uključujući i plan primene, npr. obuka novozaposlenih.
Opis funkcionalnosti ISMS	Dokument koji opisuje operacije i funkciju ISMS-a, uključujući i lokaciju dokumenta ISMS-a.
Dokument o menadžmentu incidenta	Dokument koji opisuje proces i procedure menadžmenta bezbednosnog incidenta.
Metrike i merenja	Opisuje primenu za merenje efektivnosti ISMS operacija, vrednost za poslovanje i podatke menadžmentu i timu zaštite.
Ažuriranje preostalog rizika	Na bazi dokumenta koji opisuje ovaj proces, usaglašen sa planom tretmana rizika i SoA.
Plan za proveru i (spitivanje, testiranje)	Opisuje internu proveru, nije obavezan za nezavisnu proveru, ali sertifikator može zahtevati na uvid plan za internu proveru.
Rezultati interne/ nezavisne provere	Ovaj dokument utiče na ISMS i, često je osnova za ulaz u plan tretmana rizika i poboljšanja ISMS operacija.
Plan za poboljšanje ISMS	Opisuje poboljšanja ISMS-a na bazi interne/nezavisne provere.

Faza provere u procesu sertifikacije uključuje četiri tipična koraka (tabela 9.2): aktivnosti *faza 1 i 2* pre poseta, *faze 3* – u toku posete i *faze 4* – posle posete lokaciji.

Tabela 9.2 *Koraci faze provere u procesu sertifikacije*

Koraci provere	Opis
1	Angažovanje sertifikatora i početak procesa ispitivanja; predaja dokumentacije sertifikatoru na pregled.
2	Provera postojanja, kvaliteta i adekvatnosti dokumentacije; ako je ocena pozitivna, sertifikator pristaje na posetu organizaciji.
3	Poseta organizaciji i provera na lokaciji svih tvrdnji iz ISMS dokumentacije; prenos nalaze menadžmentu posle provere na lokaciji.
4	Sertifikator analizira rezultate i kreira izveštaj koji predaje organizaciji.

U fazi 1: angažovanje sertifikatora i početak ispitivanja dodeljeni sertifikator traži svu dokumentaciju vezanu za ISMS, koju preuzima (NE u prilogu e-pošte) potpisom *ugovora o čuvanju tajnosti* – NDA (*Non Disclouse Agreement*) i proverava.

U fazi 2: pregled dokumenata ISMS-a, sertifikator utvrđuje *usaglašenost sa zahtevima* ISO/IEC 27001/2 za politiku, procedure i praksu zaštite i *stepen primene* PDCA modela u uspostavljanju i menadžmentu odgovarajućih atributa ISMS-a u organizaciji. Posle poređenja ispitivanog ISMS-a sa ISO standardima, proces se može ubrzati pripremom dokumenata (npr. SMF okvira sa uzorcima obrazaca) usaglašenih sa ISO standardima. Sertifikator procenjuje da li je organizacija spremna za posetu i proveru na lokaciji, a ako nije, proces provere se završava uz preporuke za korekcije i dalju pripremu. Ako sertifikator oceni da dokumentacija zadovoljava, posećuje organizaciju i proverava stanje ISMS-a u odnosu na dokumentaciju. Iako sertifikator prvo gleda dokumenta zaštite, važnija je i praksa zaštite, koja, ipak, sama za sebe nije dovoljna za dobijanje sertifikata. Naime, ako nije dobro dokumentovana, praksa je *dobra* koliko i ljudi koji je izvršavaju i prestaje njihovim odlaskom. Posle pregleda dokumenata zaštite sertifikator pravi izveštaj (tabela 9.3).

Tabela 9.3 *Izveštaj o pregledu dokumenata posle faze 1*

Izveštaj *faze 1*	**Opis**
Pregled dokumenata	izveštaj o pregledu, kompletnosti, dokumenovanju i radu ISMS-a

Pre posete lokaciji sertifikator treba da izradi *plan posete*, sa dinamikom intervjua i drugih aktivnosti sa zahtevom da mu na lokaciji za proveru kontakti iz organizacije asistiraju kod intervjua ili pristupa IKT sistemu i određenim informacijama, radi ocene efektivnosti implementiranih kontrola zaštite. Ako sertifikator ne dolazi sa ovakvim unapred pripremljenim materijalima i planom, organizacija treba da predloži da to uradi, da bi se optimizovao proces provere.

Faza 3: poseta organizaciji i provera na lokaciji vrši se posle ocene sertifikatora da je dokumentacija usaglašena sa ISO standardima sa ciljem procene svesti zaposlenih o potrebi zaštite i stepena usaglašenosti prakse sa dokumentacijom zaštite. Ova faza uključuje *razgovore, verifikaciju prisustva i kvaliteta* servisa i mehanizama zaštite i *ocenu efektivnosti* kontrola zaštite. Kvalitet i efektivnost servisa i mehanizama zaštite određuju se u procesu *validacije* – u odnosu na ono što organizacija tvrdi da primenjuje. Deo provere na lokaciji odnosi se na *utvrđivanje usaglašenosti* prakse i dokumentacije zaštite. Procenu *efektivnosti kontrola zaštite* sertifikator može izvršiti *opservacijom* aktivnosti u procesima zaštite ili *neposrednom proverom* (probom). U proceni opservacijom, sertifikator posmatra aktivnosti izvršioca procesa zaštite i procenjuje usaglašenost sa standardima, politikom i procedurama. Sertifikator može zahtevati pristup i logovanje na sistem i *neposrednom proverom* izvršiti određene aktivnosti validacije (npr. korišćenje lozinki, zaštićenih komunikacija, fizičke zaštite i drugih mehanizama zaštite.)

Primer: Sertifikator može neposredno proveriti fizičku zaštitu kad dolazi na razgovor sa menadžerom: *na ulazu maše rukom sigurnosnim kamerama i prolazi kroz zadnja vrata na drugoj strani ulaznog lobija, zatim, prolazi kroz nekoliko spratova stepenicama, ulazi na svaki sprat, pita zaposlene o pravcu kretanja (ako ga niko ne prati) i otvara ormane sa podacima. Ako svi zaposleni imaju bedževe sa slikom ili radio–frekvencijske identifikatore (RFID) za kontrolu ulask/izlaska iz zgrade, ova validacija fizičke zaštite se može smatrat uspešnom.*

Obim i dubina *neposredne* provere je kritična za trajanje provere na lokaciji. Mnoge aktivnosti mogu zavisiti od prethodnih nalaza. Jedan metod je da se proceni kredibilitet osoblja za vreme razgovora sa njima. Visoki nivo svesti zaposlenih, opšte znanje o zaštiti i znanje o bezbednosnim ciljevima i praksi zaštite, mogu uveriti sertifikatora da organizacija razume i *radi prave stvari*. Neke aktivnosti na lokaciji su standardne i treba ih izvršiti (npr. provera lozinke), a druge su specifične za organizaciju (npr. procesiranje *smart* kartica).

Provera, takođe, može zavisiti od primarnih nalaza, npr. *testiranje ranjivosti sistema na upad* može implicirati određivanje posledica napada. Testiranja sistema na upad mogu biti *invazivna* – metodom etičkog hakinga ili *neinvazivna* – pasivna ispitivanja. Iako je dobro poznavati gde su tačke upada u sistem, treba izbegavati da invazivne aktivnosti izazovu prekid rada. *Neinvazivne* procene su češće i mogu da otkriju korisničke naloge i lozinke, ali ih ne mogu zloupotrebljavati.

Izveštaji potencijalnih rezultata iz treće faze (tabela 9.4) uključuju nalaze provere u formatu prema zahtevu standarda, trenutno stanje organizacije, analizu razlika (*gap*), analizu saniranja posledica incidenta i preporuke za premošćavanje razlika. Sertifikator može da koristi termin *neusaglašenost,* koji definiše stanje suprotno zahtevima ISMS standarda i da klasifikuje nalaza u tri kategorije neusaglašenosti:

Značajna: može biti potpuni pad sistema ili odsustvo kontrole ili cilja zaštite, određenog zahteva, formalne dokumentacije ili tekuće prakse zaštite. Na primer, poglavlja 4 do 8 su obavezni zahtevi ISO/IEC 27001 za dobijanje sertifikata, pa je odsustvo bilo kog od ovih zahteva značajna neusaglašenost.

Minorna: može bit rezultat nedostatka ili nejasnoće dela politike zaštite, gde politika (ili drugi dokument) postoji, ali njen kvalitet nije u skladu sa ciljevima ISO standarda, ili postoji kompletna dokumentacija, ali je nedosledna praksa zaštite – zaposleni izvršavaju neke aktivnosti, ali ne sve koje zahteva ISO standard. Za popravku manjih neusaglašenosti može se ostaviti period kraći od šest meseci i

Beznačajna: ova neusaglašenost se takođe klasifikuje, iako ima mali uticaj na ISMS.

Tabela 9.4 *Izveštaji provere posle 3. faze*

Izveštaji provere	Opis
Lista dokumenata	lista dokumenata koji su deo izveštaja i status svakog dokumenta;
Zbirni izveštaj	izveštaj o proveri koju je izvršio sertifikator;
Nalazi provere	izveštaj o neusaglašenosti sa standardima i korekcijama pre sledeće provere (za 6 meseci);
Preporuke	izveštaj koji sadrži preporuku sertifikatora da se organizacija prijavi za sertifikaciju i/ili otkloni eventualne nedostatke pre prijave.

Faza 4: Isporuka nalaza je formalna predaja rezultata sertifikacije menadžmentu organizacije, sa prezentacijom – nalaza, neusaglašenosti, opcija i preporuka za dalje aktivnosti. Izveštaji se usaglašavaju sa zahtevima ISO/IEC 27001/2 standarda. Sertifikator klasifikuje svaku neusaglašenost (značajnu, minornu, beznačajnu). Organizacija dostavlja pisani odgovor za svaku razliku, tretirajući neusaglašenosti na bazi odluke o prihvatanju ili planu tretmana rizika. Rezultat četvrte faze obezbeđuje uslove za akreditaciju – izdavanje ili odbijanje ISMS sertifikata. U slučaju odbijanja, organizacija čeka šest meseci za novi pokušaj sertifikacije, a u međuvremenu koriguje sve nedostatke prema preporukama sertifikatora. Kako ISO/IEC 27001 sertifikat važi tri godine, organizacija i sertifikator se mogu dogovoriti o trogodišnjem planu nadzora ISMS-a, za bolju pripremu procesa resertifikacije. Plan uključuje više poseta sertifikatora i revizije delova ISO/IEC standarda, na koje treba usmeriti pažnju. Specifični planovi mogu varirati u skladu sa promenama ISO/IEC standarda ili sa promenama poslovnog okruženja. Svaka poseta je mala provera sa izveštajem o rezultatima i nalazima, uključujući zahteve, razlike, opcije i preporuke. Ovakav nadzor ISMS-a je dobra praksa i olakšava proces resertifikacije.

9.2.3 Sertifikacija usaglašenosti sa ISMS standardom

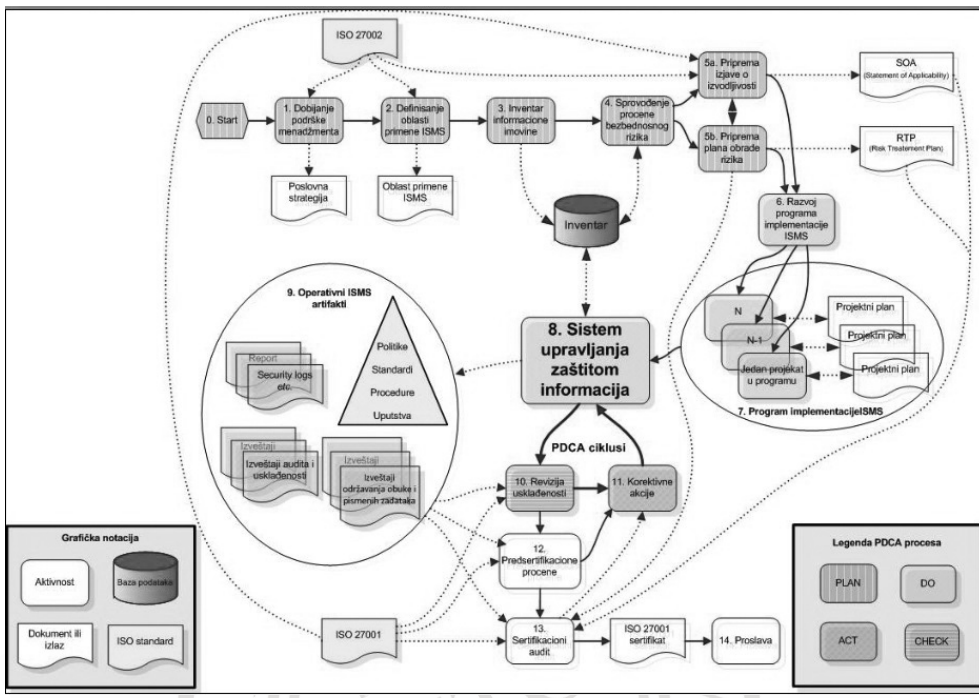
Sertifikacija usaglašenosti ISMS neke organizacije sa standardom u velikoj meri zavisi od niza faktora, kao što su veličina budžeta, značaj informacione imovine, izloženost riziku i obim IKT operacija, uključujući i spoljnu saradnju. Odgovornost za bezbednosnu usaglašenost i sertifikaciju je na organizaciji. Bezbednosna usaglašenost znači primenu PDCA ciklusa i propisnu primenu ciljeva kontrola i kontrola zaštite prema Aneksu A ISO/IEC 27001, u skladu sa poslovnim potrebama i prioritetima. Organizacije usaglašene sa ISO 9000 – menadžment sistemom kvaliteta imaju dobru osnovu za ISMS sertifikaciju. Sertifikacija obezbeđuje nezavisnu garanciju menadžmentu da je informaciona imovina odgovarajuće zaštićena i upravljana. Iako se sve kontrole ISO/IEC 27001 standarda mogu primeniti, za svaku organizaciju mora se razmotriti njihova primenljivost i neophodnost. Mogu se koristiti i druge primenljive kontrole zaštite za različite potrebe (npr. *CobiT* – 318 kontrola, *NIST* – 396, *QUALIS* – oko 2000 itd.), a ponekad su potrebne i dodatne kontrole.

Standard ISO/IEC 27001 je tehnički neutralan i ne zahteva upotrebu ni jedne specifične tehnologije zaštite. Važno je da se kontrole zaštite implementiraju u skladu sa *arhitekturom sistema zaštite*, a ne jednostavnom selekcijom sa liste. Sa promenama faktora rizika i kapaciteta organizacije ISMS se neprekidno razvija, a primenljivost zavisi od poslovnih potreba, politike zaštite, profila rizika itd. Iako se, u principu, očekuje sertifikacija celog ISMS-a, treba razmotriti rentabilnost sertifikacije za organizaciju i definisati obim sertifikacije ISMS-a na bazi SoA. Međutim, usaglašen ISMS može biti znatno veći od sertifikovanog dela koji može imati svoj dodatni SoA dokument. Nesertifikovane delove ISMS-a (npr. distribuirane lokacije), treba proveravati u procesu interne ili eksterne provere.

Za većinu organizacija sa osetljivim informacijama, dovoljno je da sertifikuje sledećih devet kategorija (komponenti) sistema zaštite informacione imovine:

1. *politiku zaštite:* organizacija mora razviti politiku zaštite, dostupnu u SLA dokumentu;
2. *nadzor i proveru prakse zaštite*: odnosi se na primenu politike zaštite u praksi zaštite;
3. *regularnu procenu rizika*: obezbeđuje menadžment promena i proaktivnu zaštitu;
4. *autorizaciju i autentifikaciju pristupa*: obezbeđuju CIA informacija;
5. *personalnu zaštitu*: uključuje bezbedno ponašanje zaposlenih i upotrebu imovine;
6. *menadžment incidenta*: održava sistem zaštite na prihvatljivom nivou rizika;
7. *proveru usaglašenosti*: sa zakonom, politikom zaštite ili bezbednosnim zahtevima;
8. *fizičku zaštitu*: obezbeđuje osnovnu zaštitu od neovlašćenog pristupa i zloupotreba i
9. *kontinuitet poslovanja*: obezbeđuje nastavak poslovanja, kritičnog za misiju i ciljeve.

Proces implementacije ISMS-a je samo jedna faza ukupnog procesa uspostavljanja usaglašenosti sa standardima i zahtevima za ISO/IEC 27001 sertifikaciju, koja se može obezbediti i kroz opšti proces za uspostavljanje usaglašenosti sa drugim srodnim standardima (SOX, HIPAA, FISMA itd.) [89]. Generički pristup uspostavljanju usaglašenosti, primenljiv na više standarda, posebno ako postoje zahtevi za unakrsnu usaglašenost, od najveće je koristi. Usaglašenost sa ISO/IEC 27001 implicira makar delimičnu usaglašenost sa drugim propisima i standardima zaštite. Uspostavljanjem SMF okvira, kao osnove za sve relevantne zahteve za bezbednosnu usaglašenost, omogućava organizaciji razvoj jedinstvene metodologije i alata za otkrivanje, analizu i izveštavanje, koji realizuju, registruju i dokazuju usaglašenost sa svim primenljivim bezbednosnim zahtevima. Proces implementacije i sertifikacije ISMS-a prikazan je na Slici 9.2.



Slika 9.2 Proces implementacije i sertifikacije ISMS-a

9.2.4 Akreditacija ISMS-a

Na osnovu informacija iz sertifikacionog paketa, akreditator razmatra preostali rizik za sistem i donosi akreditacionu odluku i odluku o prihvatanju preostalog rizika. Akreditaciona odluka može biti: *(1) potpuna, (2) delimična (privremena, uslovna) i (3) odbijena (neprihvaćena) akreditacija* [89, 117].

Potpuna akreditacija potvrđuje da su bezbednosni zahtevi zadovoljavajući, kontrole zaštite korektno implementirane, primenjivane i efektivno rade. Sistem je ovlašćen za rad u okruženju, navedenom u planu zaštite, sa nekoliko restrikcija u procesiranju (ako ih ima). Akreditacionu odluku potvrđuje akreditaciono pismo sa akreditacionim paketom u prilogu, koji sadrži: *(1) akreditaciono pismo, (2) plan zaštite i (3) izveštaje*. U većini slučajeva akreditacioni paket se izvodi iz sertifikacionog, a mogu se izostaviti i osetljive informacije iz plana zaštite, izveštaja o testiranju i evaluaciji sistema zaštite i izveštaja o proceni rizika. Delimična akreditacija znači da nema usaglašenosti sa svim bezbednosnim zahtevima iz plana zaštite ili sve kontrole zaštite nisu primenjene ili efektivne. Odobrava se privremeni rad sistema, u određenom periodu i pod određenim uslovima, do potpune akreditacije sistema, što se specificira u akreditacionoj odluci. Sve se restrikcije pažljivo kontrolišu, a akreditacioni akcioni plan omogućava *resurse za završetak plana na vreme, minimizaciju rizika, prihvatljivost preostalog rizika i rad kritičnih sistema.*

Odbijena akreditacija potvrđuje da sistem ne odgovara bezbednosnim zahtevima i kontrolama, navedenim u planu zaštite; preostali rizik je neprihvatljivo visok, a aktivnosti sistema nisu kritične za trenutne potrebe organizacije. Sistem u razvoju nije ovlašćen za dalji razvoj, a sistem u radu se zaustavlja. Akreditator izdaje akreditaciono pismo o neprihvatanju rezultata sertifikacije, uključujući dodatnu dokumentaciju, koja potvrđuje odluku o odbijanju akreditacije [117].

9.3 USPOSTAVLJANJE USAGLAŠENOSTI SA STANDARDIMA

9.3.1 Organizaciona struktura menadžment sistema usaglašenosti

Proces uspostavljanja ISMS-a u organizaciji je samo jedan slučaj celokupnog procesa *programa menadžmenta usaglašenosti* (CMP), gde su zahtevi za usaglašenost, u kontekstu postizanja ISO/IEC 27001 sertifikata, dati u standardima ISO/IEC 27001/2. Međutim, moguće je apstrahovati process ISO/IEC 27001 sertifikacije u opšti process menadžmenta usaglašenosti ili program menadžmenta usaglašenosti (CMP), koji obuhvata više zahteva za usaglašenost (npr. HOPAA, FISMA, drugi ISO standardi itd.). Opšti pristup procesu provere usaglašenosti daje mogućnost unakrsnog refrenciranja zahteva iz jednig standard sa brojnim zahtevima iz drugih relevantnih standard za organizaciju. Dakle dostizanje ISO/IEC 27001 sertifikacije implicira usaglašenost i sa više drugih standarda i regulativa. Izgradnjom okvira menadžmenta bezbednosti informacija (SMF) obezbeđuje razvoj jedinstvene metodologije i seta alata za otkrivanje, analizu i izveštavanje koji uspostavlja, prati i dokazuje usaglašenost sa svim primenljivim bezbednosnim zahtevima.

Menadžment usaglašenosti sa standardima bezbednosti informacija je samo jedan deo sveobuhvatnog CMP (*Compliance Management Program*). Menadžment program za obezbešivanje usaglašenosti bezbednosti informacija (IA CMP (Information Assurance CMP) zahteva uspostavljanje: IA CMP *okvira, procesa za identifikovanje svih relevantnih zahteva za usaglašenost, obrazaca za nabrajanje svih relevantnih zahteva za usaglašenost, kreiranje matrice za praćenje zahteva za usaglašenost i unakrsno refrenciranje za upravljanje svim primenljivim aktivnostima usaglašavanja*.

Proces IA CMP sadrži sledeće korisne alate, od kojih neki koriste ISO/IEC 27002 kao osnovu: *okvir CMP, okvir IA CMP, SE zahtevi za IA CMP, IA CMP metodologiju za procenu, alate za menadžment usaglašenosti, metriku za merenje usaglašenosti.*

Glavni ciljevi uspostavljanja usaglašenosti sa standardima bezbednosti informacija su *identifikovanje razlika* između implementiranog ISMS-a (sistema zaštite) i referentnog programa IA CMP i o*pisivanje metodologije, procesa, alata i obrazaca za planiranje, implementaciju, održavanje, proveru i izmenu* IA CMP. Program CMP omogućava primenu bilo kojih zahteva za usaglašenost, uključujući i zahteva ISO/IEC 27001. Proces usmeravanja daje smernice i identifikuje ISO/IEC 27001 sertifikaciju kao strategijski cilj. Tako standard ISO/IEC 27001 postaje spoljni eksplicitni zahtev, a ISO/IEC 27002 – *spoljni implicitni zahtev za usaglašenost*. Dekomponovanjem ovih dokumenata u kategorije i elemente sistema zaštite dobija se SMF okvir i proširljiv CMP koji podržava dobijanje ISO/IEC 27001 sertifikata [102].

U fazi planiranja CMP-a, korisno je razumeti uloge i aktivnosti na nivoima smernica (S), menadžmenta (M) i operacija (O). Smernice daju glavni i izvršni menadžeri na najvišem nivou, koji su odgovorni za uspostavljanje strategije i odobravanje politike zaštite. *Menadžment* se izvršava na najvišem i srednjem menadžerskom nivou, gde se: *generišu taktički planovi za implementaciju strategije; interpretira strategija zaštite i prevodi u akcione planove na taktičkom nivou; obezbeđuju ulazi za razvoj strateških inicijativa; razvijaju standardi i procedure koje definišu šta koristiti i kako nametati politiku zaštite; planira razvoj i uspostavlja operacija zaštite*. *Operacije zaštite*, po instrukcijama menadžmenta, *implementiraju taktičke planove u formi operativne infrastrukture, servisa, mehanizama i protokola zaštite, gde zaposleni implementiraju servise, mehanizme i protokole za nametanje politike zaštite, primenom standarda i procedura i obezbeđuju ulazne veličine za razvoj standarda i procedura zaštite.*

Menadžment usaglašenosti treba da bude pragmatična sekvenca događaja sa dobro definisanim izlaznim rezultatima i kontrolnim tačkama za identifikaciju i menadžment poslovnog rizika. U tabeli 9.5 prikazani su ključni zahtevi za CMP u kontekstu PDCA modela, u odnosu na organizacione funkcije *smernica (S), menadžmenta (M) i operacija (O).*

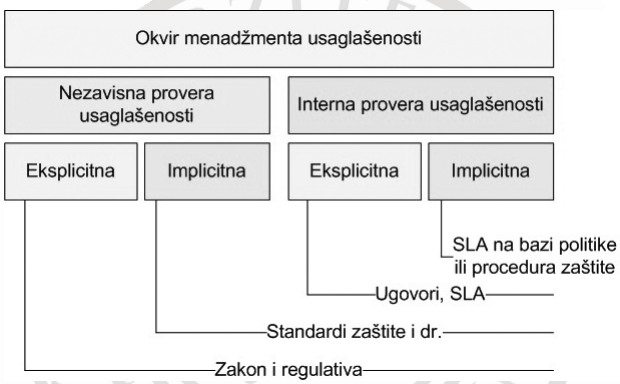
Tabela 9.5. *Struktura menadžmenta usaglašenosti u kontekstu PDCA*

Zahtev	PDCA	S, M, O	Komentar
Identifikovanje	Planiranje	S, M	Identifikovanje zahteva za usaglašenost.
Uspostavljanje	Planiranje	S, M	Definisanje okvira i inicijativa za CMP.
Planiranje	Primena	M	Razvoj planova za implementaciju CMP inicijativa.
Implementacija	Primena	M, O	Implementacija CMP inicijativa.
Monitorisanje	Provera	O	Monitoring efektivnosti operacija CMP-a.
Održavanje	Provera	S, M, O	Izveštavanje i provera rezultata monitoringa. Svaki organizacioni nivo obezbeđuje održavanje u granicama svojih odgovornosti. Izveštaj sadrži detalje o razlikama procenjenih i standardnih zahteva za usaglašenost, a u procesu provere daju se preporuke za smanjivanje tih razlika u terminima opcija menadžmenta poslovnog rizika.
Poboljšanje	Delovanje	S, M, O	Obezbeđivanje povratnih informacija za organizaciju, koje se odnose za reviziju CMP-a – najčešće inicijative za smanjenje razlika usaglašenosti ili faktora rizika u tim razlikama.

9.3.2 Uspostavljanje usaglašenosti sa standardima

Uspostavljanje usaglašenosti sa standardima je uvek obimno i specifično za tipične organizacije. Na primer, zdravstvena organizacija ima potrebu da se usaglasi sa propisima za odlaganje opasnog medicinskog otpada, što je kritično za bezbednost zaposlenih i građana i deo sveobuhvatnog CMP-a za zdravstvenu organizaciju. Za uspostavljanje CMP-*a* potrebno je definisati: *okvir, proces za identifikovanje svih relevantnih zahteva za usaglašenost, obrasce za registrovanje svih relevantnih zahteva za usaglašenost, matricu zahteva za evidentiranje i praćenje, indeks za unakrsno referenciranje primenljivih zahteva za poboljšanje aktivnosti usaglašavanja i izbegavanje redundancije (čime se smanjuju troškovi)*.

Svi zahtevi za usaglašenos sa standardima dati su u CMP-u. Efikasan CMP počinje generisanjem *okvira za uspostavljanje usaglašenosti*, koji identifikuje, registruje i pruža *smernice* za definisanje svih relevantnih zahteva za usaglašenost (slika 9.3).



Slika 9.3 Okvir menadžment sistema zahteva za usaglašenost sa standardima

Spoljni zahtevi za usaglašenost sa standardima su izvan organizacije i najčešće su pravne ili regulatorne prirode, a mogu biti i smernice iz prakse organizacije, a *interni zahtevi* – uključuju izjave o nameni, ciljevima, politici, ugovornim obavezama i interesima organizacije. *Eksplicitni zahtevi* su nabrojani u *zahtevu za ponudu* – RFP (*Request for Proposal*) ili ugovoru, a *implicitni* – su izvedeni iz *eksplicitnih zahteva*, ili iz usaglašenosti sa eksplicitnim standardima.

Primer: U Srbiji *eksplicitni zahtev* za ponudu (npr. nabavku ERP sistema u javnom preduzeću) može da zahteva usaglašenost sa *Zakonom o javnim nabavkama*. *Implicitni zahtevi* uključuju standarde i preporuke *Agencije za standardizaciju*, kao i standarde za proveru Ministarstva finansija (poreske uprave). Nizak nivo usaglašenosti sa ovim zahtevima može ugroziti finansiranje; zbog toga je navođenje analize Ministarstva finansija kao *implicitnog spoljnog zahteva* za usaglašenost opravdano za ublažavanje rizika od nedovoljnog finansiranja.

Spoljni eksplicitni zahtevi uključuju standarde za usaglašenost (npr. ISO/IEC 9000, ISO/IEC 27001/2), ali ne postoji propis koji može primorati organizaciju da se sertifikuje npr. prema ISO/IEC 27001. Organizacija za uspostavljanje ISMS-a bira ISO/IEC 27001 standard po sopstvenoj odluci. *Unutrašnji eksplicitni* zahtevi uključuju interne SLA sporazume između, npr. mrežnih operatora i različitih poslovnih grupa. *Unutrašnji implicitni zahtevi* uključuju usaglašenost sa praksom zaštite drugih organizacija preko poslovnih ugovora (tabela 9.6).

Tabela 9.6 *Prošireni okvir za menadžment zahteva za usaglašenost sa standardima*

Zahtevi za usaglašenost sa standardima	
Spoljni	*Eksplicitni*: zakoni, regulative, smernice, direktive i instrukcije.
	Implicitni: aktivnosti za podršku eksplicitnih zahteva koje smanjuje rizik.
Unutrašnji	*Eksplicitni*: izjava o ciljevima, politika, procedure, standardi, ugovori.
	Implicitni: svaka aktivnosti za podršku eksplicitnih zahteva.

Takođe, mogu uključiti dokumenta koja nisu navedena, ali su deo projekta, npr. principi, ograničenja itd. koji se ne smatraju tipičnim zahtevima za usaglašenost, ali pružaju smernice i mogu biti uključena u okvir za menadžment bezbednosti informacija, koji usmerava razmišljanje u različitim pravcima i dekomponuje probleme na upravljive delove.

9.3.3 Program menadžment sistema usaglašenosti ISMS-a

Program menadžment sistema usaglašenosti informacione bezbednosti (IA CMP) usmerava pažnju na usaglašenost bezbednosnih zahteva sa standardima, a sastoji se od sledećih korisnih alata, od kojih su neki na bazi ISO 27002 standarda:

- okvir za uspostavljanje usaglašenosti sa standardima,
- okvir za uspostavljanje informacione bezbednosti (SMF),
- sistem inženjerski zahtevi za uspostavljanje usaglašenosti,
- metodologija za određivanje usaglašenosti sa standardima,
- alati za menadžment usaglašenosti sa standardima i
- metrika usaglašenosti sa standardima.

U uslovima brze informatizacije svih segmenata društva, bezbednost informacija poslovnih sistema više nije luksuz, već postaje zakonska obaveza i praktična potreba. Štaviše, organizacije zahtevaju dokaz o povratku investicije – ROI (*Return On Investment*) na svim glavnim alociranim stavkama budžeta, što je teško, ali ne i nemoguće ostvariti. Detaljan *plan zaštite informacija*, usklađen sa poslovnim procesima, omogućava ROI u zaštitu – ROSI (*Return on Security Investment*)[2].

2 Dobar izvor informacija za proračun RSOI je godišnji izveštaj i pregled kompjuterskog kriminala FBI Instituta za bezbednost računara – CSI (*Computer Security Institute*), na www.gocsi.com.

Okvir SMF pruža osnovu i smernice za definisanje programa zaštite. Primarni cilj SMF je održavanje stabilnosti poslovanja i kompletiranje svake bezbednosne inicijative, korišćenjem okvira kao liste planiranih akcija koje treba izvršiti. U kontekstu IA CMP, SMF pruža osnovu za definisanje **svih** bezbednosnih zahteva.

Primer: Poglavlje 3, "*Foundational Concepts and Tools for an ISMS*" je SMF na bazi ISO/IEC 27002. Profesionalci u zaštiti u organizaciji mogu da prošire SMF da bi zadovoljili sve interne, eksterne, eksplicitne i implicitne bezbednosne zahteve IA CMP-a. Pomoću tabele 3.1. u poglavlju 3., kao osnove za ISMS, pravi matricu zapisa koja povezuje sve relevantne bezbednosne elemente prema sopstvenim zahtevima. Ova tabela onda postaje matrica *zapisa za praćenje*, koja povezuje zahteve sa bezbednosnim inicijativama koje ih ispunjavaju.

Sa uspostavljenim SMF okvirom, u kome se uopšteno razmatraju zahtevi za zadovoljenje standarda i specifičnih bezbednosnih zahteva, potrebno je disciplinovati *sistem inženjerske* (SE) procese za određivanje i registrovanje zahteva.

9.3.3.1 Sistem inženjerski zahtevi za menadžment usaglašenosti

Sistemsko inženjerstvo – SE (*Systems Engineering*[3]) je *disciplinovan* pristup uspostavljanju i implementaciji kompleksnih sistema, a sistemsko inženjerstvo bezbednosti – SSE (*Security System Engineering*) je deo okvira SE i uvod u mnogo kompleksniji proces menadžmenta usaglašenosti sa ISO/IEC 27001 standardom, koji zahteva efektivni menadžment rizika organizacije i disciplinovan SE pristup.

Prvi korak u S*SE bezbednosnih zahteva* je identifikovanje i nabrajanje zahteva za usaglašenost sa ISMS standardom, uz pomoć *okvira za menadžment zahteva za usaglašenost sa standardima* (videti sliku 9.2). Drugi korak je identifikovanje postojećih bezbednosnih zahteva za usaglašenost na bazi SMF okvira. Sistemski pristup zahteva da profesionalci u zaštiti usaglašavaju svaki bezbednosni element iz SMF-a sa dokumentima zahteva za usaglašenost, u terminima menadžmenta rizika. *SSE bezbednosnih zahteva* uspostavlja potreban skup zahteva za usaglašenost, koji identifikuje i integriše poslovne zahteve, procese i menadžment rizika i zahteve za bezbednosnu usaglašenost i bezbednosne inicijative. Procesi SSE zahtevaju identifikovanje i nabrajanje dokumenata za usaglašenost informacione bezbednosti. U tabeli 9.7 dat je uzorak matrice za praćenje zahteva za usaglašenost.

3 * Više informacija o sistemskom inženjerstvu imate na sajtu www.incose.org

Tabela 9.7 *Matrica za praćenje zahteva za usaglašenost*

Broj zahteva[4]	Naziv zahteva	Izvor	Referenca	Komentar
EE.1	HIPAA pravilo tajnosti	Propis	http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf	Primenljivo samo na delove organizacije koje rade u SAD i primenjuju njene zakone.
EE.2	HIPAA pravilo bezbe-dnosti	Propis	Http://www.cms.hhs.gov/Hipaageninfo/downloads/Hipaalaw.pdf	Primenljivo samo na delove organizacije koje rade u SAD i primenjuju njene zakone.
EE.3	Evropska direktiva za zaštitu podataka	Propis	http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf	Primenljivo samo na delove organizacije koje rade u SAD i primenjuju njene zakone.
EI.1	U.S. FSG*, po-glavlje 8	Propis	http://www.ussc.gov/2006guid/TABCON06.htm	Pruža smernice za određi-vanje krivice organizacije u sporu.
IE.1	ISO 27002		www.iso.org	Smernice za kontrole zaštite
IE.2	ISO 27001	Standard	www.iso.org	Smernice za razvoj ISMS-a
IE.3	Politika X	Politika xxx	www.intranet.xxx	Politika organizacije za <TBD>
Itd.				
*FSG – Federalna uputstva o kažnjavanju (*Federal Sentencing Guidelines*)				

Svaki dokument zahteva za usaglašavanje treba dekomponovati u skup *kategorija i elemenata za usaglašavanje*. Tabele 9.7 do 9.9 predstavljaju seriju zahteva i elementa, po funkcionalnom redosledu. Zahtevi za usaglašenost na visokom nivou apstrakcije lako se uspostavljaju i nestaju, pa odvajanje zahteva za usaglašenost od bezbednosnih inicijativa, doprinosi dugotrajnom održavanju dokumentacije zahteva za usaglašavanje. Ovo odvajanje je moguće preko matrice zahteva, zasnovane na SMF okviru, specifičnom za organizaciju. U tabeli 9.8 dat je primer matrice za praćenje zahteva za usaglašenost, a u tabeli 9.9 – za praćenje politike, standarda i procedura (PSP), koje se menjaju prema potrebama organizacije. Identifikacija zahteva brojevima, pruža mogućnost njihovog praćenja.

4 EE = eksterni - eksplicitni; EI = eksterni - implicitni; IE = interni - eksplicitni; II = interni - implicitni

Tabela 9.8 *Matrica za praćenje zahteva za usaglašenost – Izvod iz FSG smernica*

FSG referentni broj	Strana	Referenca	Opis smernice	Interpretacija/ komentari
1	476	§8B2.1	Efikasni program usaglašavanja i etike.	Definišite program usaglašavanja i etike, izraziti šta je potrebno i implementirati program usaglašavanja i etike!
2	476	§8B2.1 (a)(1)	Izvršavati dužnu pažnju u sprečavanju i otkrivanju kriminalnih aktivnosti!	Implementirati program menadžmenta rizika i uključiti menadžment usaglašenosti!
3	476	§8B2.1 (a)(2)	Na druge načine promovisati kulturu organizacije i ohrabriti etičko ponašanje i pridržavanje zakona za sprečavanje i detekciju kriminalnog ponašanja!	Odraziti želju organizacije u politici i razvoju svesti i implementirati metriku za praćenje svesti i razumevanje etičkih i pravnih zahteva!
Itd.				

Tabela 9.9 *Obrazac matrice za praćenja PSP-a*

Ref. broj	PSP	Opis zahteva	Stepen	Prati	V&V
PO.AA.001	Politika	politika za etički program	mora	FSG.1	TBD
ST.AA.001	Standard	standard za etički program	mora	FSG.2	TBD
PR.AA.001	Procedura	procedura za etički program	mora	FSG.3	TBD
Itd.					

U skladu sa *SSE zahteva za usaglašenost*, treba definisati SMF okvir, specifičan za organizaciju i koristiti ga za pravljenje matrica zahteva koji povezuju svaki element SMF-a sa njegovim zahtevima za usaglašenost, kao i za evidentiranje PSP-a svakog elementa zaštite i procedure za lozinku, koji se usaglašavaju sa višim zahtevima.

Primer: Može se koristiti lozinka kao stavka u SMF-u za povezivanje SOX, HIPAA i ISO 27002 standarda, koja ukazuje da postoji politika lozinke i njena lokacija (www.xxx.intranet/ security/policies), kao i standardi i procedure lozinki i njihove lokacije. Ako neki standard preporučuje nove lozinke (npr. HIPAA FSR već predlaže lozinku od 22 karaktera, koja uključuje bar dva velika slova, četiri broja i tri specijalna karaktera), SMF omogućava usaglašavanje sa HIPAA FSR standardom pripadajuće politike, standarda i procedura.

Ako neke nove ranjivosti zahtevaju izmenu procedure, treba je povezati sa odgovarajućim propisima i modifikovati bez konflikta sa smernicama propisa. SMF tabele za praćenja evidencija omogućavaju praćenje procedure do propisa koji je podržava. Takođe, SMF može podržati praćenje zahteva za usaglašenost servisa zaštite (npr. tima za zaštitu sa ISO 27002 i HIPAA FSR) i mehanizama zaštite (npr. AV programa sa ISO 27002, SOX i HIPAA standardima). U Tabeli 9.10 prikazan je opšti primer tabele praćenja zahteva za usaglašenost, koja ima referencu u RFP-u. Identifikovanje tipova zahteva pomaže u određivanju motivacije za ispunjavanje zahteva.

Tabela 9.10 Obrazac matrice za praćenje zahteva za usaglašenost

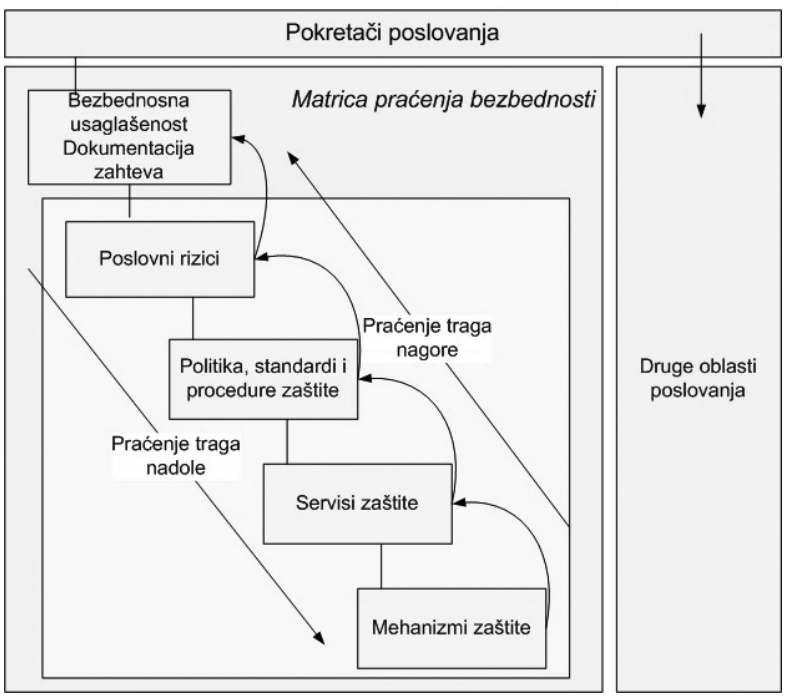
Izvor zahteva	Identifikacioni broj zahteva (projekt)	Opis zahteva	Stepen	Prati	V&V
XYZ RFP	1		mora	(*identifikacioni broj zahteva*)	
	2		treba		
	3		može		
	n				

Generalno, organizacija može imati veliku matricu zahteva za usaglašenost u CMP-u, sa fokusom na IA CMP. Organizacija može izabrati praćenja zahteva za usaglašenost *nagore* – da usaglasi svaki bezbednosni elemenat sa zakonom i poslovnim zahtevima ili *nadole* – svaki zahtev sa bezbednosnom inicijativom (servisom, mehanizmom itd.).

Postoje brojne vrste izvora zahteva koji pružaju uvid u to kako odrediti *stepen značaja zahteva*, npr. zakonski i ugovorni zahtevi su najčešće obavezujući. Neki od izvora zahteva su: *zakon, propis, instrukcija, direktiva, RFP* (Zahtev za ponudom), *CONOPS* (Koncept rada), *ugovor i SOW* (Izjava o radu). *Stepen značaja zahteva* označava stepen fleksibilnosti u odgovoru na zahtev, tj. u stvarnoj primeni zahteva. Neki zahtevi su značajni toliko da se *moraju* izvršiti, a „ *treba*" označava mogućnost kompromisa. Stepen „ *može*" znači da ne postoji obaveza, ali se preporučuje, ako je primenljiv u okviru postojećih resursa. Neki zahtevi sa stepenom „ *može*" se mogu primeniti kao nerazdvojiv deo implementacije nekog drugog zahteva. Praćenje stepena značaja zahteva omogućuje timu za zaštitu da prikaže dodatnu vrednost odobrene inicijative. Kolona „ *prati*" je veza premu zahtevu u oba pravca, što je često zbunjujuće, pa se preporučuje izbor jednog. Praćenje *nagore* prati usaglašavanje bezbednosne inicijative sa zakonom X, a *nadole* – svakog zahteva sa bezbednosnom inicijativom. Oba pristupa imaju prednosti, ali organizacija treba izabrati jedan.

Verifikacija i validacija (V&V) opisuju način testiranja nivoa i kvaliteta ispunjavanja zahteva. Verifikacija određuje da li su servis, mehanizam, proces, standard itd. stvarno implementirani, a validacija – da li oni stvarno rade kako je namenjeno? V&V opcije uključuju *intervju, pregled, proveru, testiranje, simulaciju* ili njihovu kombinaciju, u zavisnosti od situacije.

Na slici 9.4 prikazana je struktura matrice za praćenje sa fokusom na bezbednost, počevši od poslovnih zahteva za usaglašavanje sa propisima koji iniciraju izbor zahteva za bezbednosno usaglašavanje iz SMF-a. Identifikacija i numeracija poslovnih faktora rizika u kontekstu SMF-a, polazi od zahteva za bezbednosno usaglašavanje. Politika se usaglašava sa poslovnim rizicima koji podstiču njeno kreiranje, a mehanizmi zaštite se usaglašavaju sa servisima koje podržavaju. Iako nivo detalja usaglašavanja može biti veliki, održavanje dokumentacije zahteva neznatni napor, zbog brzine donošenja preciznih, pouzdanih bezbednosnih odluka u odnosu na poslovne zahteve, a, posebno, *mogućnosti dokazivanja poslovne vrednost bezbednosti informacija*.



Slika 9.4 Matrice praćenja bezbednosnog usaglašavanja: pregled

U tabeli 9.11 nabrojani su različiti poslovni zahtevi, na primer, poslovni plan koji navodi strategijsku prednost ISO/IEC 27001 sertifikacije.

Tabela 9.11 *Matrica za praćenje zahteva – Poslovni pokretači (Business Drivers – BD)*

Izvor zahteva	<Projekt> Identifikacija zahteva	Opis zahteva	Stepen	Vodi ka	V&V
Poslovni plan kompanije X	BD1	ISMS sertifikacija za komparativnu prednost u elektronskom komercijalnom hosting servisu	mora	<ID zahteva> dobijanju strategijske inicijative za 5% učešća na tržištu	dobijanje sertifika-cije ISO 27001 od strane CA
Itd.					

U tabeli 9.12 nabrojani su dokumenti zahteva za usaglašavanje – CRDM (*Compliance Requirement Document Matrix*) koji podržavaju ovu bezbednosnu inicijativu. Kolona *praćenja* povezuje ova dokumenta sa poslovnim zahtevom. Jedan metod povezivanja zahteva je korišćenje tabele skraćenica, kao prefiksa kojeg prati broj zahteva u toj tabeli.

Tabela 9.12 *Matrica dokumenata zahteva za usaglašavanje (CRDM)*

Referenca zahteva[a]	Naslov zahteva	Izvor	Referenca	Komentar	Prati
IE.1	ISO 27001	Industrijski standard	www.iso.org	primenljivo samo na organizacije koja radi u <SAD> i podležu njenim propisima	BD1
IE.2	ISO 27002	Industrijski standard	www.iso.org	primenljivo samo na organizacije koja radi u <SAD> i podležu njenim propisima	BD1
[a]EE = eksterno - eksplicitno; EI = eksterno - implicitno; IE = interno - eksplicitno; II = interno -implicitno					

U tabeli 9.13 prikazan je početak SMF-a, kao deo matrice za praćenje zahteva. Kako se SMF zasniva na ISO/IEC 27002, sve kategorije i elementi se mogu pratiti prema IE.2 zahtevu u tabeli 9.12, što je drugi način za dodeljivanje identifikacije zahtevima.

Tabela 9.13 *Matrica za praćenje zahteva na bazi SMF-a*

Izvor zahteva	<Projekt> Identifikacija zahteva	Opis zahteva	Stepen	Vodi ka	V&V
Interni poslovni zahtev	1	uspostavljanje ISMS	mora	IE.1	ISMS dokumentacija
Itd.					
	2	politika zaštite informacija	mora	IE.2	*politika zaštite*
	3	dokument politike zaštite informacija	mora	IE.2	*politika zaštite*
		pregled politike zaštite informacija	mora	IE.2	procedura zaštite
Itd.					

Kombinacija identifikacije zahteva pokazuje da se mogu uspešno koristiti različite metode, po izboru organizaciju i sa težištem na konzistentnost primene. Tabele praćenja obuhvataju bezbednosne inicijative i specifičnosti servisa i mehanizama zaštite. Disciplinovana izrada zahteva, u okviru poslovnih zahteva, obezbeđuje konzistentnost, sveobuhvatnost i opravdanje početnih troškova svake bezbednosne inicijativa i troškova implementacije i održavanja tekuće operacije. Prednost je mogućnost pregleda poslednjih, najjačih mehanizama zaštite i određivanja mere u kojoj odgovaraju strategijskoj inicijativi.

9.3.3.2. Metodologija menadžmenta bezbednosne usaglašenosti

Identifikovanje zahteva za usaglašenost i izrada matrice za praćenje zahteva su prvi koraci metodologije menadžmenta usaglašenosti. Implementacija bezbednosnih inicijativa uspostavlja bazu za operacije sistema zaštite, doprinoseći boljem menadžmentu bezbednosne usaglašenosti. Sledeći korak je određivanje tekuće usaglašenosti sistema zaštite informacija, što zahteva definisanje sveobuhvatne *metodologije za određivanje bezbednosne usaglašenosti sa* ISO/IEC 27001 *standardom,* koja za nezavisnu proveru obuhvata sledeće aktivnosti: *(1) menadžmenta projekta; (2) pre angažovanja; (3) angažovanja; (4) pre posete; (5) u toku posete lokaciji; (6) posle posete lokaciji; (7) isporuke i odjave i (8) posle angažovanja.*

Za internu proveru, koja je dobra praksa pre angažovanja spoljne firme, organizacija može izostaviti deo aktivnosti, u zavisnosti od cilja provere. Interna provera omogućava identifikaciju ranjivosti bezbednosne usaglašenosti i usmeravanje pažnju na teže propuste pre angažovanja nezavisnog proveravača.

(1) Menadžment projekta usaglašenosti je meta-pogled na projekat procesa procene usaglašenosti, koji uključuje aktivnosti *planiranja, praćenja progresa, identifikacije rezultata i povećanja vrednosti*. Struktura menadžmenta projekta usaglašenosti uključuje: *dekompoziciju posla* – **WBS** *(Work Breakdown Structure), plan projekta, definicije faza projekta, definicije isporuke rezultata, upravljanje resursima za rad i kapitalom i dobijenu vrednost*.

Tabela 9.14 predstavlja opšti WBS i plan projekta za razvoj ISMS-a na bazi ISO/IEC 27001 standarda. U zavisnosti od kompleksnosti bezbednosnih zahteva, ekspertize tima za zaštitu, tekućih procedura zaštite i raspoloživog budžeta za menadžment poslovnog rizika, svaka organizacija će imati drugačiji WBS. Takođe, vreme za dobijanje ISO/IEC 27001 sertifikata može značajno varirati sa veličinom organizacije, primenjenim okvirom, tekućim procedurama zaštite, internom ekspertizom itd.

Tabela 9.14 *Opšti WBS za razvoj ISMS-a na bazi ISO/IEC 27001 standarda*

ID zadatka	Zadatak	Trajanje (dani)	Odgovornost
Faza 1: Definisanje ISMS			
	identifikacija bezbednosnih zahteva organizacije		
	definisanje bezbednosnih zahteva organizacije		
	definisanje politike održavanja sistema bezbednosti		

ID zadatka	Zadatak	Trajanje (dani)	Odgovornost
	definisanje politika zaštite informacija		
	politika održavanja sistema bezbednosti	0	
	primenjene politike zaštite	0	
	dokumenti zahteva za usaglašavanje	0	
	definisanje završetka ISMS projekta	0	
Faza 2: Procena rizika			
	analiza uticaja rizika na poslovanje		
	ID poslovne funkcije		
	ID osoblja		
	ID infrastrukture za podršku		
	procena ranjivosti		
	procena pretnji		
	procena rizika	0	
	završetak procesa procene rizika	0	
Faza 3: Razvoj ISMS-a			
	otkrivanje tekućih procedura zaštite		
	analiza razlika (*gap* analiza)		
	razvoj SoA dokumenta		
	dokument razvoja ISMS-a	0	
	završetak razvoja ISMS		
Faza 4: Primena ISMS-a			
	razvoj plana implementacije ISMS-a		
	kampanja za razvoj svesti o potrebi ISMS-a		
	prezentacije		
	praćenje statusa ISMS-a		
	dokument plana razvoja ISMS-a	0	
	završetak implementacije ISMS-a		
Faza 5: Priprema faze pred-sertifikacije			
	interna provera (upitnici, intervjui, opservacije...)		
	izveštaj nalaza interne provere	0	
	analiza		

ID zadatka	Zadatak	Trajanje (dani)	Odgovornost
	izveštaj nalaza interne provere i akcioni plan	0	
	korektivne akcije		
	završetak pripreme faze pred-sertifikacije	0	
Faza 6: Faza sertifikacije proveravane organizacije			
	pre posete		
	faza 1		
	faza 2		
	poseta na lokaciji		
	faza 3		
	posle posete lokaciji		
	faza 4		
	završetak faze sertifikacije organizacije	0	

WBS u redovima tabele 9.14 prikazuje *glavne zadatke* u sveukupnom planu projekta, koji uključuje mnogo više detalja, kao što su izvori, dinamika, gantogrami, kritični tokovi itd. po elementu reda. *Trajanje* označava vreme isporuke rezultata koraka, a definicije faza, uz neznatne varijacije, su deo plana projekta za razvoj ISMS-a i provere usaglašenosti za ISO/IEC 27001 sertifikaciju. Ostvarena vrednost – EV (*Earned Value*) je metod za praćenje progresa projekta do završetka, u granicama budžeta i vremena. EV može biti veoma složen i daje bolje rezultate kod velikih i kompleksnih projekata. U svakom slučaju, dobar menadžer projekta procenjuje nedeljne i mesečne troškove, beleži rast troškova prema projektovanim i po potrebi ubrzava rad na projektu.

(2) Pre angažovanja menadžmenta na aktivnostima *procene usaglašenosti*, zahteva se sastanak između izvođača, proveravača i sponzora aktivnosti. Izvođač procesa sertifikacije usaglašenosti za ISO/IEC 27001 sertifikaciju, može biti akreditovano CA, ali i interni profesionalac zaštite informacija koji proverava usaglašenost prakse zaštite prema zahtevima standarda. Za ovaj sastanak, zahteva se izrada plana, dokumentacija i potpis menadžera na sadržaj, zadatke, troškove itd. Sve aktivnosti se izvršavaju pre nego što sponzor angažuje izvođača, a uključuju generisanje: (*a) zahteva za ponudu (RFP), (b) modela troškova, (c) definicije projekta i (e) kriterijuma uspešnosti projekta*.

Zahtev za ponudu (RFP), koji objašnjava ciljeve klijenta (sponzora) i niz aktivnosti za postizanje tih ciljeva, uključuje aktivnosti koje treba izvršiti, oblast rada i troškove aktivnosti, listu rezultata za isporuku i indikatore progresa procesa. Potpis menadžera, koji odobrava oblast provere, rezultate i troškove, obezbeđuje se pre angažovanja tima za sertifikaciju. Ovo formalno daje sigurnost mendžmentu organizacije za dobijanje očekivanih rezultata i pruža osnovu za poboljšanje ISMS-a. Aktivnosti izvan oblasti projekta mogu biti dobre, ali i kritične za bezbednost organizacije.

Generička struktura za definisanje projekta treba da sadrži najmanje sledeće elemente: *(1) izjavu o nameni projekta; (2) dinamički plan projekta; (3) sadržaj projekta; (4) ciljeve projekta; (5) oblast projekta; (6) pretpostavke; (7) projektni tim; (8) plan projekta; (9) procenu rizika projekta i (10) kontrolne tačke za praćenja progresa projekta.*

Svrha definicije projekta je da se odrede ciljevi i usklade sa *oblasti primene*, *ulogama* i *odgovornostima* i *rezultatima projekta*; da se *prati progres*, *revidira plan i definišu faktori uspeha projekta*.

(3) Angažovanje tima za sertifikaciju usaglašenosti počinje posle potpisivanja RFP-a i ugovora, a uključuje sledeće aktivnosti: (a) *pre posete lokaciji* – učesnici, plan, rokovi; (b) *u toku posete lokaciji* – intervjui, testiranje...; (c) *posle posete lokaciji* – analiza, praćenje progresa, izveštavanje; (d) *ukupna ocena organizacije* – nalazi snage i slabosti, zbirni izveštaj i (e) *isporuka rezultata* – prezentacija inicijalnih nalaza, pregled i revizija, isporuka konačnih nalaza i odjava.

(4) U fazi pre posete sertifikator/tim se priprema za posetu i rad na lokaciji, da bi se smanjili troškovi putovanja i rada. Identifikuju se članovi tima i rokovi za procenu usaglašenosti, uključujući ankete, upitnike i intervjue, koji štede vreme i troškove posete. Specifičnosti mogu varirati u zavisnosti od ciljeva.

(5) U toku posete lokaciji sertifikator/tim prati plan, uključujući prikupljene podatke, dokumente i druge bitne dokaze. Ako je neophodna V&V, sertifikator može opservacijom na licu mesta, potvrditi prisustvo, efektivnost i efikasnost raznih mera zaštite; može zahtevati neposrednu validaciju, što znači direktan pristup IKT i sistemu zaštite, uključujući fizičku zaštitu.

(6) Posle posete lokaciji analiziraju se rezultati rada na lokaciji, a mogu uključiti i izjave sakupljene telefonom i e-poštom. Na kraju, sertifikator piše izveštaj, ili seriju izveštaja, koji izražavaju status zahteva za usaglašenost, nalaze sertifikacije, razlike između zahteva i nalaza, opcije i preporuke za rešavanje tih razlika. Ovi izveštaji sertifikatora čine *sertifikacioni paket* koji je osnova za *punu akreditaciju* (tj. izdavanje ISO/IEC 27001 sertifikata), ili za *uslovnu akreditaciju* ili za *odbijenu akreditaciju*.

(7) Isporuka rezultata može biti na kraju faze angažovanja ili u toku procesa kroz definisane korake, ako je angažovanje duže i na više lokacija, što omogućava da korisnici na određenim lokacijama koriguju neke aspekte, pre konačne isporuke rezultata. Na taj način se može sačuvati ugled organizacije i omogućiti priprema za učešće u aktivnostima koje slede.

(8) Posle angažovanja aktivnosti sertifikatora/tima uključuju: (a) *usvajanje iskustava* i (b) *izmenu i poboljšanje procesa.* Svako angažovanje ostavlja određena iskustva, kao što su bolje planiranje i izvršenje svih faza projekta. Usvajanje ovih iskustava i modifikovanje procesa za procenu usaglašenosti omogućuva konstantno poboljšanje i konkurentnost na tržištu.

9.3.3.3 Alati za menadžment sistem usaglašenosti

Za menadžment usaglašenosti, termin *alati* podrazumeva dokumenta koja definišu metodologiju, uzorake, obrasce za analizu itd. Metodologija menadžmenta usaglašenosti

koristi set *alata* za izvođenje aktivnosti, koji mogu biti specifični za organizaciju, ali se svi zasnivaju na ISO ili drugim standardima zaštite. Namena svih alata za menadžment ili procenu usaglašenosti je da se dobiju konzistentni, kompletni i ponovljivi rezultati, nezavisno od lokacije i vremena procene, kao i da se kroz proces kontinualne revizije i poboljšanja ISMS-a, omogući agregacija iskustava. Alati za menadžment usaglašenosti se mogu svrstati u sledeće kategorije alata za: *(1) tim za menadžment usaglašenosti; (2) menadžment projekta; (3) aktivnosti pre angažovanja; (4) aktivnosti u toku angažovanja; (5) aktivnosti posle angažovanja; (6) aktivnosti pre posete lokaciji; (7) aktivnosti u toku posete lokaciji; (8) aktivnosti posle posete lokaciji i (9) za isporuku rezultata i uručivanje sertifikata.*

(1) Tim za menadžment usaglašenosti može imati na raspolaganju materijale za obuku i pripremu za angažovanje, smernice za interpretaciju, uzorke za sve aktivnosti, kontaktne informacije za članove, procedure, pretpostavke, vremenski plan, budžet i obim dokumenta, konzistentnu komunikaciju sa klijentima i standardne formate dnevnog reda, vremenskog plana rada na lokaciji, e-pošte i prezentacije rezultata.

(2) Alat za menadžment projekta uključuje: standardni ili specifično prilagođen alat za WBS; uzorke plana projekta i za praćenje troškova angažovanja, izveštaja o statusu projekta, vremenskog plana, dnevnog reda za posetu lokaciji i instrukcija za analizu rezultata; standardne formate za komunikaciju, sastanke i dnevni red i alate za statističku analizu.

(3) Alati za fazu pre angažovanja uključuju obrasce za definisanje projekta, ugovore, izjave o radu i druga dokumenta koja izražavaju obim i detalje o izvršenom radu. Važni alati su modeli troškova i cene rada.

(4) Alati za fazu angažovanja su uglavnom obrasci za otkrivanje kao što su *ček liste* i metodi njihove efektivne primene, intervjui i instrukcije za intervjuisanje. Za razvoj konzistentnog seta alata i smernica za interpretaciju rezultata usaglašenosti koristi se SMF okvir. Kako je većina procena po prirodi subjektivna, tj. sertifikator upoređuje nalaze sa zahtevima za usaglašavanje i opisuje razlike subjektivnim terminima, izveštaji se značajno razlikuju među sertifikatorima. Korisni su alati za kvantifikaciju nalaza sertifikacije ili razlika procene usaglašenosti, kao što su skale tipa *nizak, srednji, visok* ili 1, 2, 3, sa instrukcijom kriterijuma za određivanje nivoa usaglašenosti. Ovi alati omogućavaju proračune suma, srednje vrednosti, procenta, minimuma i maksimuma, upoređivanje lokacija i agregaciju rezultata sa svih lokacija.

(5) Alati za fazu posle angažovanja uključuju alate za statističko procesiranje kvantifikovanih agregiranih i rezultata sa lokacija, obrasce za izveštavanje nalaza, analizu razlika, remedijaciju i preporuke za remedijaciju. Zavisno od kompleksnosti organizacije, ovi izveštaji mogu biti u jednom ili odvojenim dokumentima.

(6) Alati za isporuku rezultata procene usaglašenosti uključuju standardne obrasce za prezentaciju, isporuku rezultata i kompletiranje projekta.

9.3.3.4 Metrika procesa menadžment sistema usaglašenosti

U svim praktičnim aplikacijama (sistema, procesa, softvera itd.), primarni zadatak je da to funkcioniše, a zatim da radi efektivno i efikasno, sa fokusom na performanse, troškove menadžmenta rizika i zahteve za usaglašenost. U pristupu korisnika, razlikuju se *upotreba,*

efektivna upotreba i bezbedna upotreba aplikacije. Zakonska regulativa zahteva dokaz o bezbednosti i akcijama zaštite. Za objektivnu procenu bezbednosti rada aplikacije u poslovnim procesima koriste se *metrike zaštite*. Metrika usaglašenosti, kao podskup metrike zaštite, uključuje:

1. *nivo usaglašenosti*: prisustvo, kvalitet i praksa merenja zaštite,
2. *menadžment standarda, politike i procedura*: razvoj, provera,
3. *distribuciju*: svest o potrebi, razumevanje, usaglašenost i
4. *praćenje procesa ublažavanja/remedijacije*.

(1) Procena nivoa usaglašenosti određuje tekuće stanje sistema zaštite informacija i poredi ga sa bezbednosnim ciljevima, koji sadrže sve relevantne zahteve za bezbednosnu usaglašenost. Bezbednosne ciljeve artikuliše SMF okvir, a sistem zaštite uključuje politiku, standarde, procedure, servise, mehanizme i tim za zaštitu. *Nivo* ili stepen tekućeg stanja *usaglašenosti* u poređenju sa bezbednosnim ciljevima, određuje se procesom *sertifikacije* ili *procene usaglašenosti*. Razlikuju se tri kategorije metrika usaglašenosti, za – *prisustvo, kvalitet i praksu*. Metrika za prisustvo određuje da li uopšte postoji metrika zaštite, tj., politika, servisi i mehanizmi zaštite. Ako organizacija za usaglašenost koristi referentni standard ISO/IEC 27002, može se izračunati broj primenjenih *kontrola* iz standarda prema broju raspoloživih, izraženih u *procentima*. Za određivanje *kvaliteta* sistema zaštite, proverava se da li sistem sadrži karakteristike koje ga čine dobrim. Standard za *dobru zaštitu* specifičan je za svaku organizaciju i veoma zavisi od uloge zaštite u poslovnom sistemu.

Primer *dobre politike zaštite* sadrži sledeće atribute kvaliteta*: definiciju i značaj bezbednosti informacija za organizaciju; ciljeve i obim programa zaštite; izjavu menadžmenta da je zaštita u funkciji poslovanja; izjavu o potrebi menadžmenta programa zaštite; izjavu o potrebi usaglašenosti organizacije sa politikom zaštite; izjavu o menadžmentu rizika, koji uključuje usaglašenost sa zakonom, svest o potrebi, obuku i obrazovanje o zaštiti, BCP i DRP.*

Cilj je usvojiti standard koji definiše šta sadrži dobra politika zaštite, a zatim uporediti tekuću politiku sa standardnom i odrediti kvalitet postojeće politike. Na primer, ako postoji osam atributa dobre politike, izračuna se broj atributa koji postoji u proveravanoj politici; ako je to šest, onda je nivo usaglašenosti atributa 75%. Za smanjenje kompleksnosti i troškova ukupne bezbednosne usaglašenosti, efektivan i jednostavan metod je rangirati nivoe usaglašenosti na sledeći način: *ne postoji, niska, srednja, visoka i potpuna usaglašenost*. Zatim se izvrši kvantifikacija sa 0, 1, 2, 3 i 4 respektivno za numeričku prezentaciju skale. Određivanje *nepostojanja* zaštite je očigledno – postoji ili ne. *Potpuna usaglašenost* je kad sistem zaštite sadrži najmanje sve zahtevane atribute iz standarda. *Nizak* nivo usaglašenosti je neki procenat atributa od 0%, do 49%, *srednji* – od 50% do 84%, a *visok* – od 85% do 99%. Prema ovoj šemi, primer od 75% je srednja usaglašenost, ili nivo usaglašenosti 2, ili uz skalu 0 – 4, 50% nivoa usaglašenosti: ((2/4)x100)=50%). Sličan proračun se primenjuje za svaku komponentu sistema zaštite u standardu zaštite. Procena nivoa usaglašenosti atributa omogućava dodatno ponderisanje težinskim faktorima.

Primer: Neka u politici zaštite nedostaju atributi *ciljeva* programa zaštite i zakonske *usaglašenosti*. Organizacija može odlučiti da su ciljevi značajniji od usaglašenosti, pa se atribut ciljeva ponderiše sa 2. Koristeći skalu težinskih faktora sa dva nedostajuća elementa, gde je 1 ponderisani atribut, daje nivo usaglašenosti atributa od 66,67% (tabela 9.15). Ako postoje oba ponderisana atributa, a nedostaju dva neponderisana atributa, nivo usaglašenosti atributa je 77,78%. Ponderisanje dodaje neznatnu kompleksnost, ali daje tačniju sliku, reflektujući ono što je važno za organizaciju.

Tabela 9.15 *Primer skale ponderisanja težinskih faktora*

Atribut	Težinski faktor	Prisustvo	Poen
X	1	1	1
X	2	0	0
X	1	1	1
X	1	0	0
X	1	1	1
x	1	1	1
x	1	1	1
x	1	1	1
	9	6	6
	nivo usaglašenosti	66,6%	

U cilju dobijanja konzistentnih rezultata, svaki tip ponderisanja se objavljuje u smernicama i ne zavisi od proveravača i procesa provere. Konzistentnost rezultata obezbeđuje bolju statistiku, sa trendom obezbeđivanja dokaza za poslovnu vrednost informacione bezbednosti.

Postojanje dobre procedure ne implicira nužno dobru praksu zaštite i aktuelnu primenu te procedure u praksi zaštite, ali ni dobra praksa zaštite ne implicira postojanje dobre procedure, ako organizacija izostavi najbolje operacije iz procedure. Zato treba proceniti usaglašenost prakse i procedura zaštite. Prvo se procenjuje da li praksa zaštite uopšte postoji, zatim, kakav je njen kvalitet. Ako procedura postoji, onda nivo striktnosti njenog sprovođenja određuje nivo usaglašenosti prakse zaštite. Generalno, nivo usaglašenosti od 50% ne znači da sistem zaštite ne valja sam po sebi, niti da se ne može akreditovati, već da kontrole zaštite sadrže oko pola karakteristika navedenih u zahtevima za bezbednosnu usaglašenost. Termin *nivo usaglašenosti* je neutralniji i implicira fokus na popravku postojećeg programa zaštite, a ne na njegovu ocenu tipa *prolazi* ili *ne prolazi*.

(2) Menadžment politike, standarda i procedura zaštite, generalno obezbeđuje detaljnu specifikaciju relevantnih faktora zaštite. Politika specificira *zašto* treba štititi informacije, standard – *šta,* a procedure - *kako, kada, gde i ko* treba da obezbedi zaštitu informacija. Politika zaštite pokreće ponašanje organizacije, kroz specifikaciju prakse zaštite i usklađivanje sa strateškim pokretačima poslovanja. Primer generičkog pokretača poslovanja je *menadžment rizika*, koji je istovremeno primer pokretača menadžmenta usaglašenosti. Standardi specificiraju servise i mehanizme za implementaciju politike zaštite, a procedure zaštite - *kako* koristiti standarde za implementaciju politike zaštite, *kada* i *gde* ih primeniti i *ko* je odgovoran za primenu.

(3) Metod distribucije programa za procenu svesti o potrebi zaštite i obuku, zahteva verifikaciju prijema i korisničke prihvatljivosti materijala programa. Slanje materijala, npr. e-poštom, omogućava praćenje potvrda o prijemu, a uz pretpostavku da svaki korisnik koji otvori prilog isti pročita – omogućava procenu korišćenja materijala. Alat za merenje nivoa razumevanja može biti kviz, test ili anketa.

(4) Praćenje ublažavanja i remedijacije uključuje preporuke, definisanje i praćenje projekata oporavka sistema, alate za otkrivanje i analizu razlika, snimanje nalaza i razvoj uzoraka obrazaca za procenu usaglašenosti. Konzistentna upotreba SMF okvira omogućava praćenje ovih aktivnosti između više dokumenata. Metrike kreirane u kontekstu SMF-a mogu se koristiti za uspostavljanje ISMS programa i tekuću proveru usaglašenosti, koja inicira ublažavanje rizika i druga merenja progresa ISMS-a. Ključna dobit od metrika i merenja je objektivna procena ROSI-a, koja određuje poslovnu vrednost bezbednosti informacija, u meri njene operativne efektivnosti.

Primer: Ključna poslovna funkcija jedne banke je procesiranje finansijskih transakcija i njen gubitak može izazvati veliko nezadovoljstvo klijenata. Mere zaštite CIA finansijskih transakcija povećava poslovnu vrednost banke. Primenjene metrike i merenja namenjeni su za procenu ove poslovne vrednosti sistema zaštite transakcija.

U tabeli 9.16 prikazan je uzorak obrasca za definisanje praćenja usaglašenosti programa ISMS-a [102]**.**

Tabela 9.16 *Uzorak obrasca za definisanje usaglašenosti ISMS programa*

Broj zahteva	Komponenta zaštite	Standard zaštite	Detalji plana zaštite	Odgovornost	Vodi trag do
ID zahteva	opis komponente zaštite <*plan zaštite*>	kratak sadržaj standarda *plana zaštite*	definišu specifičnosti *plana zaštite*	za definiciju implementacije plana zaštite i održavanje	jedinstvenog identifikatora zahteva
ID za plan komponente zaštite	referenca na standard zaštite	kratak opis zahteva	specifikacija plana zaštite za određenu komponentu zaštite	plan specifično navodi odgovornosti za implementaciju, rad i održavanje	drugih zahteva ili inicijativa, npr. HIPAA
itd.					

9.4 REZIME

Razvoj procesa sertifikacije i akreditacije (S/A) obuhvata definisanje uloga i odgovornosti, identifikovanje IKT sistema za S/A, izbor tipa akreditacije, upravljanje procesom S/A i izradu S/A dokumentacije. Osnovna namena sertifikacije je definisanje korektnosti implementacije, efektivnosti kontrola zaštite i usaglašenosti sa standardom zaštite (ISO/IEC 27001, NIST).

Sertifikacija je postupak tehničke i netehničke provere kontrola zaštite IKT sistema, koji obezbeđuje neophodne informacije za proces akreditacije. Proces sertifikacije sadrži faze *predsertifikacije, sertifikacije i posle sertifikacije*. *Akreditacija* je proces autorizacije sistema za rad na prihvatljivom nivou rizika, posle glavne modifikacije ili razvoja novog IKT sistema, a može biti *potpuna, delimična ili odbijena*.

Usaglašavanje je zadovoljavanje seta zahteva koji mogu biti zakonski, regulatorni, ugovorni, operativni i drugi. Menadžment usaglašenosti je koordinacija resursa i aktivnosti za zadovoljavanje seta *zahteva za usaglašenost*. Na *menadžment usaglašenosti* primenjuje se PDCA model, poređenjem ovih zahteve sa pokretačima poslovanja u terminima menadžmenta rizika i definisanjem programa menadžmenta usaglašenosti (CMP). Efektivan CMP uspostavlja se kontinualno ponavljanim PDCA ciklusom koji neprekidno podržava implementaciju i operativnu primenu *procesa, metrike i provere menadžmenta usaglašenosti*.

Strategijske smernice za menadžment usaglašenosti dolaze iz procesa menadžmenta rizika, a razlozi za se određuju u fazi uspostavljanja i planiranja ISMS-a, u terminima poslovnog rizika. *Menadžment program usaglašenosti bezbednosti informacija* (IA CMP) je pokušaj uspostavljanja sveobuhvatnog okvira za pristup menadžmentu bezbednosti informacija. Okvir SMF-a je uvek specifičan za organizaciju i uključuje zahteve za usaglašenost sa zakonom, regulativama i standardima zaštite. Organizacija mora neprekidno menjati sistem zaštite, sa promenama poslovnog okruženja, faktora rizika, pretnji i ranjivosti. Dobro rešenje zaštite informacija je agilan i proširljiv sistem, adaptivan na promene, a obezbeđuje ga IA CMP na bazi standarda ISO/IEC 27001/2. Dakle, postizanje ISO/IEC 27001/2 sertifikata je slučaj IA CMP pristupa. Ako je cilj ISO/IEC 27001 sertifikacija, okvir IA CMP se prilagođava da zadovolji taj standard i naziva se ISMS. Program zaštite se definiše u kontekstu SMF okvira, zasnovanog na standardu ISO/IEC 27002, koji se, zatim, modifikuje tako da zadovolji specifične potrebe organizacije. Alternativna osnova za uspostavljanje SMF i IA CMP okvira mogu biti COBIT, NIST SP 800-53, ISF v.4 i drugi standardi zaštite.

9.5 PITANJA ZA PONAVLJANJE

1. Ključne uloge i odgovornosti u procesu *sertifikacije i akreditacije su:*
   a. akreditator, sertifikator, rukovodilac programa, izvršni menadžer
   b. akreditator, sertifikator, menadžer zaštite, specijalista za zaštitu
   c. akreditator, sertifikator, rukovodilac programa, specijalista za zaštitu
   d. akreditator, sertifikator, administrator sistema, specijalista za zaštitu.
2. Organizaciona struktura procesa nezavisne ISMS sertifikacije sadrži*:*
   a. šest koraka
   b. osam koraka
   c. četiri koraka
   d. sedam koraka.
3. Cilj procese sertifikacije je:
   a. formalna autorizacija ili odobrenje uslova za rad sistema
   b. procena efektivnosti *kontrola zaštite* IKT sistema
   c. procena rizika i dokazivanje potpune zaštite
   d. procena usaglašenosti prakse sa politikom i procedurama zaštite.
4. Proces sertifikacije sadrži sledeće ključne faze:
   a. faza pre provere
   b. faza testiranja
   c. faza provere
   d. faza posle provere.
5. Sertifikaciju usaglašenosti organizacije sa ISO/IEC 27001 standardom može izvršiti:
   a. sama organizacija
   b. organizacija uz pomoć stručnog konsultanta
   c. nezavisno akreditovano sertifikaciono telo
   d. akreditovano sertifikaciono telo koje je učestvovalo u implementaciji ISMS-a.
6. U pripremi procesa provere, pre posete lokaciji:
   a, organizacija prikuplja sva relevantna dokumenta zaštite
   b. sertifikator proverava da li je praksa zaštite usaglašena sa dokumentacijom
   c. sertifikator pregleda dokumentaciju zaštite
   d. sertifikator analizira rezultate, dostavlja izveštaj organizaciji i predlaže korekcije.
7. U toku posete lokaciji:
   a. organizacija prikuplja sva relevantna dokumenta zaštite
   b. sertifikator proverava da li je praksa zaštite usaglašena sa dokumentacijom
   c. sertifikator pregleda dokumentaciju
   d. sertifikator analizira rezultate i dostavlja izveštaj organizaciji i predlaže korekcije.
8. Posle posete lokaciji:
   a. organizacija prikuplja sva relevantna dokumenta zaštite
   b. sertifikator proverava da li je praksa zaštite usaglašena sa dokumentacijom
   c. sertifikator pregleda dokumentaciju
   d. sertifikator analizira rezultate i dostavlja izveštaj organizaciji i predlaže korekcije.
9. Provera procene rizika u fazi sertifikacije obuhvata:
   a. kontrolu pristupa, kontrole zaštite, upravljanje vanrednim događajem i incidentom
   b. administraciju zaštite, testiranje proaktivne zaštite i plana vanrednih događaja
   c. kontrolu usklađenosti procena rizika sa zahtevima
   d. dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema.
10. Provera dokumentacije politike zaštite u faza sertifikacije obuhvata:
    a. kontrolu pristupa, kontrole zaštite, upravljanje vanrednim događajem i incidentom
    b. zadatke administracije, testiranje proaktivne zaštite i plana vanrednih događaja
    c. kontrolu usklađenosti procena rizika sa zahtevima
    d. dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema.

11. Provera tekuće konfiguracije u fazi sertifikacije obuhvata:
    a. kontrolu pristupa, kontrole zaštite, upravljanje vanrednim događajem i incidentom
    b. zadatke administracije, testiranje proaktivne zaštite i plana vanrednih događaja
    c. proveru kritičnih komponenti konfiguracije
    d. dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema.
12. Provera projektne dokumentacije u fazi sertifikacije obuhvata:
    a. kontrolu pristupa, kontrole zaštite, upravljanje vanrednim događajem i incidentom
    b. dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema
    c. zadatke administracije, testiranje proaktivne zaštite i plana vanrednih događaja
    d. kontrolu usklađenosti procena rizika sa zahtevima.
13. Provera planova i procedura u fazi sertifikacije obuhvata:
    a. kontrolu pristupa, kontrole zaštite, upravljanje vanrednim događajem i incidentom
    b. dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema
    c. zadatke administracije, testiranje proaktivne zaštite i plana vanrednih događaja
    d. kontrolu usklađenosti procena rizika sa zahtevima.
14. Proces akreditacije je:
    a. formalna autorizacija ili odobrenje uslova za rad sistema
    b. procena efektivnosti *kontrola zaštite* IKT sistema
    c. procena rizika i dokazivanje potpune zaštite.
15. Ključni koraci faze akreditacije su:
    a. implementacija plana akreditacije
    b. tretman rizika
    c. donošenje odluke o akreditaciji.
16. Akreditacija može biti:
    a. potpun, delimična, odbijena
    b. otvorena, zatvorena i kodirana
    c. javna, tajna i interna.
17. Akreditacioni paket obično sadrži:
    a. akreditaciono pismo, plan zaštite i izveštaj
    b. akreditaciono pismo, sertifikacioni paket i izveštaj
    c. akreditaciono pismo, plan testiranja i izveštaj.
18. Sertifikacija usaglašenosti sa ISMS standardom je odgovornost:
    a. sertifikacionog tela
    b. sertifikovane organizacije
    c. menadžera za zaštitu informacija.
19. Za većinu organizacija sa osetljivim informacijama dovoljno je da:
    a. sertifikuje dvanaest kategorija (komponenti) sistema zaštite
    b. sertifikuje metodologiju menadžmenta bezbednosnog rizika
    c. sertifikuje devet kategorija (komponenti) sistema zaštite
    d. sertifikuje sedamnaest kategorija (komponenti) sistema zaštite.
20. Glavni ciljevi uspostavljanja usaglašenosti ISMS-a sa standardima su:
    a. identifikovanje razlika između generičkog CMP i IA CMP
    b. opisivanje metoda, procesa, alata i obrazaca za menadžment usaglašenosti ISMS-a
    c. identifikovanje razlika između plana zaštite i ISMS standarda
    d. identifikovanje razlika između plana zaštite i tretmana rizika.
21. U fazi planiranja CMP uloga glavnog i izvršnog menadžmenta je:
    a. usmeravanje operacije i identifikovanje ISMS sertifikacije kao strateškog cilja
    b. implementacija servisa, mehanizma i protokola za nametanje politike zaštite
    c. razvoj i primena standarda i procedura zaštite
    d. generisanje taktičkih akcionih planova za implementaciju strategije.
22. U fazi planiranja CMP uloga zaposlenih je:
    a. usmeravanje operacije i identifikovanje ISMS sertifikacije kao strateškog cilja
    b. implementacija servisa, mehanizma i protokola za nametanje politike zaštite

c. uspostavljanje strategije i odobravanje politike zaštite
d. razvoj i primena standarda i procedura zaštite.

23. Menadžment programa usaglašenosti ISMS-a sadrži:
a. SMF okvir i okvir za uspostavljanje usaglašenosti sa standardima
b. SE zahteve za uspostavljanje usaglašenosti sa standardima
c. sistem inženjerske zahteve za implementaciju kontrola zaštite
d. metodologiju i alate za menadžment usaglašenosti sa standardima.

24. Spoljni zahtevi za usaglašenost sa standardima su:
a. izjava o ciljevima, politika, procedure, standardi, ugovori
b. zakoni, regulative, smernice, direktive i instrukcije
c. neophodne aktivnosti za podršku koje se odnose na eksplicitni zahtev
d. neophodne aktivnosti za podršku koje smanjuje rizik na prihvatljiv nivo.

25. Unutrašnji zahtevi za usaglašenost sa standardima su:
a. izjava o ciljevima, politika, procedure, standardi, ugovori
b. zakoni, regulative, smernice, direktive i instrukcije
c. neophodne aktivnosti za podršku koje se odnose na eksplicitni zahtev
d. neophodne aktivnosti za podršku koje smanjuje rizik na prihvatljiv nivo.

26. Sistem inženjerski pristup za praćenje zahteva za usaglašenost zahteva:
a. identifikovanje i nabrajanje dokumenata za usaglašenost informacione bezbednosti
b. dekomponovanje svakog zahteva u kategorije i elemenate za usaglašavanje
c. kombinovanje zahteva za usaglašavanje sa bezbednosnim inicijativama
d. istovremeno praćenje zahteva za usaglašenost nadole ili nagore.

27. Nivo i kvalitet ispunjavanja zahteva za usaglašenost dokazuje se:
a. intervjuisanjem korisnika sistema zaštite
b. procesima verifikacije i validacije i njihovom kombinacijom
c. proverom sprovođenja politike zaštite
d. proverom efektivnosti implementiranih kontrola zaštite.

28. Sveobuhvatna metodologija za određivanje usaglašenosti ISMS-a obuhvata aktivnosti:
a. menadžmenta projekta usaglašenosti, pre angažovanja i angažovanje
b. procenu rizika i efektivnosti kontrola zaštite
c. pre posete, posetu lokaciji, posle posete lokaciji, isporuku rezultata provere
d. verifikaciju sprovođenja politike zaštite.

29. Alati za menadžment usaglašenosti se ne mogu svrstati u sledeće kategorije, za:
a. aktivnosti u toku posete lokaciji
b. tim za menadžment rizika
c. menadžment projekta tretmana rizika
d. aktivnosti posle posete lokaciji.

30. Metrika usaglašenosti ne uključuje:
a. nivo usaglašenosti
b. menadžment bezbednosnog incidenta
c. distribuciju politike zaštite
d. praćenje procesa ublažavanja/remedijacije.



10. MODEL SAZREVANJA PROCESA ZAŠTITE

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Strukturu modela sazrevanja procesa zaštite (SSE CMM)
- ☑ Funkcionalni značaj reprezentacija SSE CMM modela (fazne i kontinulane)
- ☑ Strukturu dimenzije „oblati primene" SSE CMM modela (22 oblasti procesa - OP)
- ☑ Strukturu dimenzije „sazrevanja" nivoa kapaciteta OP (CL) i nivoa zrelosti OP (CM)
- ☑ Glavne slučajeve primene SSE CMM modela u praksi zaštite informacija
- ☑ Primenu SSE CMM metodologije za evaluaciju i poboljšanje procesa zaštite

10.1 UVOD

Opšte je prihvaćen princip da se neka aktivnost može dobro upravljati samo ako se može meriti. Osnovni atribut kvaliteta aktivnosti i procesa čine metrike i merenja. Istraživanja su potvrdila da su metrike i merenja performansi sistema zaštite informacija važni, ali da se prednosti mogu ostvariti samo kada se metrika primenjuje kao proces, uz korišćenje agregiranih mernih podataka. Međutim, većina organizacija ne koriste metriku zaštite kao proces, a još manji broj integriše taj proces u sistem kvaliteta i poslovne procese.

Posebnu grupu modela i standarda kvaliteta procesa zaštite čine *procesno orijentisani modeli* za merenje nivoa zrelosti i kapaciteta procesa zaštite, razvijeni na bazi generičkog CMM[1] (*Capability Maturity Model*) modela, kao što su: SE CMM (*System Engineering Capability Maturity Model*), SW CMM (*Capability Maturity Model for Software Developement*), SSE CMM (*System Security Engineering Capability Maturity Model*), iCMM (*Integrated*

1 Razvijen u Institutu SEI (*Software Engineering Institute)*, *Carnegy Mellon* Univerziteta u SAD-u, na inicijativu NSA (1993-95).

Capability Maturity Model) i CMMI (*Capability Maturity Model Integration*). Dok su ranije tehnike i modeli za merenje i evaluaciju zrelosti procesa, bazirale proces evaluacije samo na *otkrivanju* objektivnih dokaza stvarne implementacije praksi i procesa, CMM metodi evaluacije zasnivaju proces evaluacije na *otkrivanju* i *verifikaciji* objektivnih dokaza implementacije, izvršavanja i institucionalizacije praksi i procesa, što predstavlja znatno viši kvalitet evaluacije procesa. CMM je više usmeren na upravljačke i organizacione procese i aktivnosti, kao referentni model zrelih praksi i procesa u specifikovanim disciplinama za procenu grupnih kapaciteta za izvršavanje tih disciplina [55].

10.2 RAZVOJ I STRUKTURA GENERIČKOG MODELA SAZREVANJA PROCESA

Modeli CMM se razlikuju po: *disciplini* (softver, zaštita, sistemi, akvizicija itd.); *strukturi komponenti* (kontinualna i fazna reprezentacija); *definisanju nivoa zrelosti procesa* (put poboljšavanja) i *nivoa kapaciteta procesa* (institucionalizacija) [55].

Generički CMM daje arhitekturu ili strukturu procesa, definiše ciljne karakteristike procesa i ključne atribute za specifične procese i obezbeđuje referentni model *najboljih praksi* i procesa za evaluaciju i poboljšavanje, ali ne obezbeđuje operativno uputstvo. Većina CMM modela procesa ima dimenzije *nivoa kapaciteta procesa* – CL (*Capability Level)* i/ili *nivoa zrelosti procesa* – ML (*Maturity Level*), koji se koriste za evaluaciju i poboljšavanje procesa. Za lakše shvatanje dimenzija modela, potrebno je definisati ključne termine iz standarda ISO/IEC 21827 [101]:

Definicija 186: ***Kapacitet procesa*** *predstavlja opseg očekivanih rezultata koji se mogu postići kada se proces konzistentno sledi i izvršava i obezbeđuje predviđanje izlaznih* ***performansi*** *projekta.*

Definicija 187: ***Performansa procesa*** *je mera aktuelnih rezultata postignutih izvršavanjem procesa.*

Definicija 188: ***Zrelost procesa*** *je mera u kojoj je proces eksplicitno definisan, upravljan, merljiv, kontrolisan i efektivan.*

Generički CMM modeli razvijeni su primarno da kreiraju sistem merenja *procesa organizacije* u životnom ciklusu sistema [71, 32, 24], identifikuju većinu *projektnih i upravljačkih* praksi i procesa i obuhvate najbolje SE *prakse* za razvoj i upravljanje procesima za proizvodnju softvera i organizacije u celini [67]. Poverljivi CMM – TCMM (*Trusted Capability Maturity Model)*, razvijen ranih 1990-ih, na bazi generičkog CMM, za bezbednosnu procenu softvera u fazi razvoja, tipičan je predstavnik standarda za *procenu kvaliteta u odnosu na pretnje iz proizvodnog okruženja*. Poverljivi CMM je nastao kao *metodologija poverljivog softvera – TSM* (*Trusted Software Methodology*), koja definiše nivoe poverenja: *nizak* – otporan na nenamerne ranjivosti i *visok* – dodaje procese za zaštitu od malicioznih programera u razvoju softverskih proizvoda. TSM je kasnije harmonizovan sa CMM u

TCMM, primenljiv samo za procese i sisteme. TCMM nije više u upotrebi. Poznatiji tipovi, strukture (reprezentacije) i oblasti primene CMM-a prikazani su u tabeli 10.1 [32].

Tabela 10.1 *CMM modeli, reprezentacije i oblasti primene*

CMM	Reprezentacija	Oblast primene
Sw CMM	fazna	razvoj softvera
SE CMM	kontinualna	sistemsko inženjerstvo
Sw Acquisition CMM	fazna	akvizicija softvera
SSE CMM	kontinualna	inženjering zaštite
Personal Sw Process	fazna	razvoj sw za korisnike (pojedince)
FAA-iCMM	fazna	Sw inženjering SE i akvizicija
IPD CMM	kontinualna	razvoj integrisanog proizvoda
People CMM	fazna	razvoj kompetencija zaposlenih
SPICE Model	kontinualna	razvoj softvera

10.3 MODEL I METOD SAZREVANJA PROCESA ZAŠTITE

Na bazi generičkog CMM-a, razvijeni su brojni modeli, kao i model sazrevanja procesa zaštite – SSE-CMM[2], Integracioni CMM – CMMI® i Integrisani CMM – iCMM [18, 33]. Dinamika razvoja *modela i metoda sazrevanja procesa zaštite* – SSE CMM ilustrovana je u tabeli 10.2 [20].

Tabela 10.2 *Razvoj SSE CMM modela*

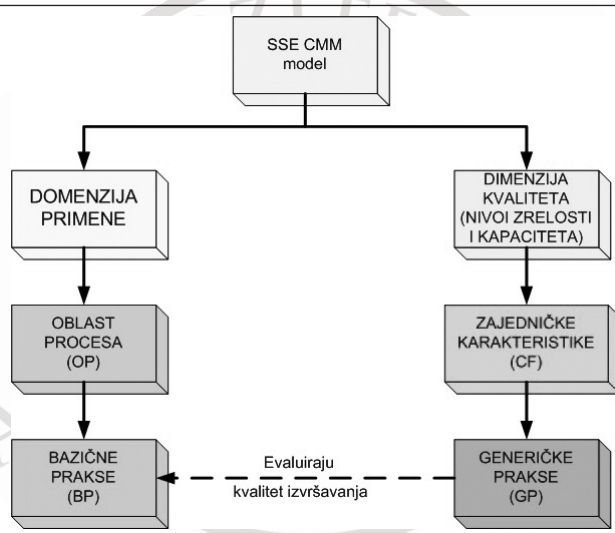
Objavljen	Naziv modela
1993.	NSA inicirala razvoj CMM za inženjering zaštite
1995.	SEI radna grupa CMU razvila SSE CMM
1996.	objavljen SSE CMM v.1.0
1996-98.	pilot projekti SSE CMM u 7 organizacija u SAD
1999.	objavljena SSE CMM v.2.0 i SSAM (*Security System Appraisal Method*) v.2.0
2002.	SSE CMM potvrđen kao standard ISO/IEC 21827
2003.	objavljena SSE CMM v.3.0
2004/05.	ISSEA (*International Systems Security Engineering Association*) podnela zahtev za akreditaciju tela za SSE CMM sertifikaciju lica – *ISO/IEC 21827 Apraiser Certification Body for Persons*
2004.	usaglašavanje SSE CMM i CMMI v.1.1
2004.	usaglašavanje SSAM sa CMMI SCAMPI Appraisal
2007.	SSE CMM Verzija
2007.	usaglašavanje SSE CMM i CMMI v.1.2

2 Razvijen po zahtevu *Nacionalne bezbednosne agencije* (NSA) i *Ministarstva odbrane* (DoD), *SAD.*

Model SSE-CMM je procesno orijentisana metodologija za razvoj bezbednog IKT sistema na bazi *organizacionih* i *projektnih* (*upravljačkih*) praksi i procesa, u celini preuzetih iz SE CMM i originalno razvijenih *sistem-inženjerskih procesa zaštite* (*SSE*). *Međunarodna asocijacija za sistemsko inženjerstvo u oblasti zaštite* (ISSEA), dalje razvija teoriju i praksu SSE CMM-a, tako da SSE CMM v. 2 postaje standard ISO/IEC 21827**:**2002, a poslednja v. 3 je objavljena 2007. Model i standard SSE CMM sadrži dva modula: (1) *SSE CMM v.3.0, model i metod* sazrevanja procesa zaštite i (2) *SSAM v.2.0 – metod evaluacije* nivoa kapaciteta (CL) i nivoa zrelosti procesa (ML) koji koristi *SSE CMM* kao referentni model [100].

Struktura SSE-CMM modela organizovana je u dve *dimenzije* (slika 10.1) [33, 101]:

1. *dimenziju primene***,** koja obuhvata *SSE, projektne i organizacione oblasti procesa* (OP) i
2. *dimenziju kvaliteta procesa*: *sazrevanja procesa* – ML (*Maturity Level*) u faznoj (stepenastoj) reprezentaciji *i nivoa kapaciteta procesa* – CL (*Capability Level*) u kontinualnoj reprezentaciji komponenti modela.



Slika 10.1. Struktura SSE CMM modela sazrevanja procesa zaštite

SSE CMM model ima dve *reprezentacije* strukturnih komponenti *puteva sazrevanja* ili *poboljšavanja* procesa. Generalno, *reprezentacija* predstavlja organizaciju, način primene i prezentacije komponenti modela i puta sazrevanja procesa, a može biti *kontinualna* i *fazna*. *Kontinualna reprezentacija* modela odnosi se na progresivno, inkrementalno ili inovativno, kontinualno poboljšavanje procesa individualnih OP od 0. do 5. *nivoa kapaciteta* (CL), a *fazna* – na progresivno poboljšavanje više ili svih OP organizacije od 1. do 5. *nivoa zrelosti* (ML) procesa (tabela 10.3).

Tabela 10.3 *Nivoi kapaciteta – CL i zrelosti – ML procesa SSE CMM modela*

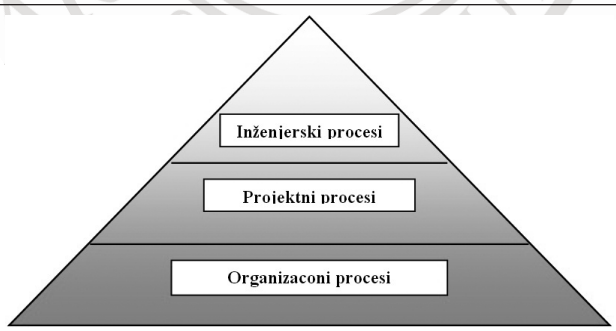
Nivo CL/ML	Kontinualna reprezentacija – CL	Fazna reprezentacija – CM
0	ne izvršava se	(ne prikazuje se)
1	izvršavan neformalno	inicijalni
2	ponovljiv, planiran i praćen	ponovljiv, planiran i praćen
3	dobro definisan	dobro definisan
4	kvantitativno upravljan	kvantitativno upravljan
5	kontinualno poboljšavan	kontinualno poboljšavan

10.3.1 Dimenzija primene SSE CMM modela

Dimenzija primene definiše *šta* treba da se postigne sa SSE, projektnim i organizacionim OP, a nivoi kapaciteta/zrelosti određuju *nivoe kvaliteta* postizanja tih ciljeva, odnosno *kako* se dobro te OP izvršavaju.

Oblast primene obuhvata tri *kategorije* OP, koje su na slici 10.2 prikazane prema nivou uticaja na sazrevanje procesa organizacije:

- *SSE*: za inženjersku analizu procesa, sa najvećim doprinosom za organizaciju,
- *projektne:* za projektovanje, upravljanje i koordinaciju rada na projektu, sa srednjim doprinosom za organizaciju i
- *organizacione*: za organizaciju ljudi i procesa koje ti ljudi izvršavaju u projektu, sa najnižim, ali fundamentalnim doprinosom za organizaciju.



Slika 10.2 SSE CMM kategorije procesa

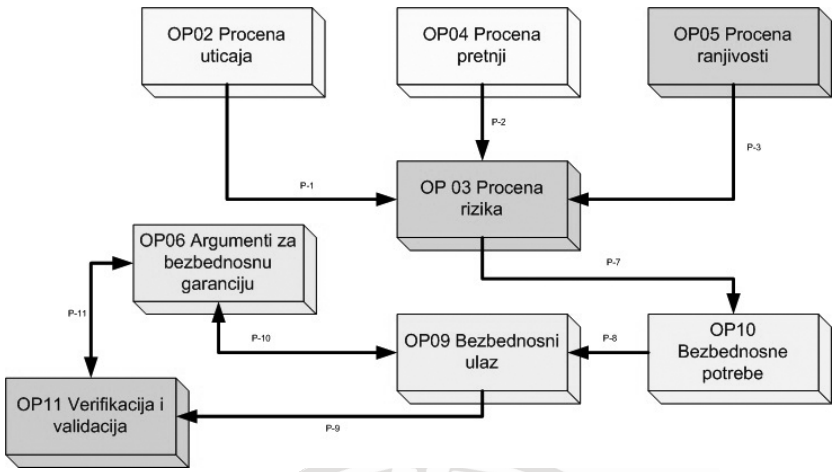
Model sadrži ukupno 22 OP**:** 11 – SSE, *5* – projektnih i 6 – organizacionih OP. *Kategorije OP SSE CMM* prikazane su zbirno u tabeli 10.4 [30].

Tabela 10.4 *Oblasti procesa u tri opšte kategorije SSE CMM*

SSE OP	Upravljačke (projektne) OP	Organizacione OP
OP01 – administriranje sistema zaštite	**OP12:** obezbeđivanje sistema kvaliteta	**OP17**: definisanje SE procesa organizacije
OP02 – procena uticaja	**OP13.** upravljanje konfiguracijom	**OP18**: poboljšavanje SE procesa organizacije
OP03 – procena bezbednosnog rizika	**OP14:** upravljanje rizikom projekta	**OP19**: upravljanje razvojem proizvodne linije
OP04 – procena pretnji	**OP15.** monitorisanje tehničkih aktivnosti	**OP20**: upravljanje okruženjem za podršku SE procesa
OP05 – procena ranjivosti sistema	**OP16:** planiranje tehničkih aktivnosti	**OP21:** obezbeđivanje potrebnih znanja i veština
OP06 – izgradnja bezbednosne garancije (*security assurance*)		**OP22**: koordinacija bezbednosnih aspekata sa snabdevačima
OP07 – koordinacija sistema zaštite		
OP08 – nadzor i kontrola sistema zaštite		
OP09– obezbeđivanje bezbednosnog ulaza		
OP10 – specifikacija bezbednosnih potreba		
OP11 – verifikacija i validacija proizvoda/ sistema zaštite		

Oblasti procesa (OP) iz sve tri kategorije u suštini su slične i treba ih razmatrati integralno, jer se samo takvim pristupom obezbeđuje progresivno poboljšanje ukupnih kapaciteta za razvoj programa zaštite. SSE CMM obezbeđuje OP za kompletno pokrivanje životnog ciklusa sistema zaštite. Svaka OP sadrži specifične *bazične prakse,* primenljive u svim fazama oblasti primene. SSE CMM *ne propisuje* specifične OP ili aktivnosti, nego *daje opšti model* za *formiranje i grupisanje* međusobno zavisnih OP *i aktivnosti najbolje prakse zaštite* (slika 10.3) [35].

Ostale međuzavisnosti OP, kao i OP i GP modela date su u tabeli 10.5. Značaj ovih međuzavisnosti je višestruk. Dok su BP, CF i GP (CL) komponente modela koje direktno utiču na institucionalizaciju procesa u organizaciji, mnoge OP utiču na institucionalizaciju podržavajući implementaciju GP. Poznavanje ovih zavisnosti pomaže da se efektivno implementiraju GP. Neke OP sadrže više BP. Kada su sve BP implementirane, mogu implementirati GP ili generisati *proizvod rada* koji se koristi za implementaciju GP.



Slika 10.3 Međusobni odnosi bezbednosno orijentisanih OP

Tabela 10.5 *Međuzavisnosti OP i GP SSE CMM modela procesa*

OP	Zavisi od OP	Zavisi od GP, BP
OP01		
OP02	OP03, OP04, OP05,OP09, OP10, OP11	
OP03	OP02, OP04, OP05, OP06, OP09, OP10	BP.04.05, BP.05.03, BP.02.05
OP04	OP03, OP02, OP05	BP.08.02,
OP05	OP03, OP09, OP10	BP.08.02,
OP06	OP07	GP 3.3.3
OP07		GP 3.3.1, GP 3.3.2, GP 3.3.3
OP08	OP03, OP05	
OP09	OP10	GP 3.3.2
OP10	OP09, OP06, OP07	GP 2.3.2, GP 3.3.3,
OP11	OP06, OP07, OP15	GP 2.3.2
OP12	OP11, OP15	GP 2.3.1
OP13	OP01, OP06, OP10	GP 2.2.2, GP 2.4.1
OP14	OP07, OP15, OP16	
OP15	OP01, OP08, OP07, OP16	GP 2.4.2
OP16	OP07	GP 2.1.1, GP.2.1.2, GP 2.1.6
OP17	OP07	GP 2.1.3, GP 3.1.1, GP 3.1.2
OP18	OP17, OP09	GP 2.1.3, GP 5.1.2
OP19	OP06	GP 5.2.3, GP 5.2.4
OP20	OP03, OP06, OP09	GP 2.1.4
OP21	OP09	GP 2.1.5
OP22	OP10	

U SSE CMM modelu OP su opisane u standardnom formatu sa: *rednim brojem*, *nazivom, ciljem i kratkim opisom*, kao u sledećem primeru:

OP1 – Administracija kontrola zaštite
Opis: uspostavlja odgovornosti u programu zaštite, upravlja konfiguracijom sistema zaštite, upravlja programima za podizanje svesti o potrebi, obuci i obrazovanju i upravlja servisima i mehanizmima kontrola zaštite. Namena ove OP je da održava zaštitu u operativnom stanju.
Cilj: kontrole zaštite su propisno primenjene i konfigurisane.
Bazične prakse (BP):
1.1.1. Uspostavi odgovornosti za kontrole zaštite i upoznaj sve zaposlene u organizaciji!
1.1.2. Upravljaj konfiguracijom sistema kontrola zaštite!
1.1.3. Upravljaj programom za razvoj svesti o potrebi, obuke i edukacije za sve korisnike!
1.1.4. Upravljaj periodičnim održavanjem i administracijom servisa i mehanizama zaštite!

Detaljan, integralani opis OP i BP SSE CMM modela dat je u literaturi [101].

Bazične prakse (BP), čije se izvršavanje *obavezno zahteva* za postizanje bezbednosnih ciljeva neke OP, čine skup odnosnih, kolektivno izvršavanih osnovnih aktivnosti OP-a. Da bi se postigla namena OP nije toliko važno kakvog su kvaliteta BP-e, nego da su samo implementirane. Smatra se da svaka od identifikovanih BP doprinosi efektivnom izvršavanju OP i zbog toga se BP unutar specifične OP mora izvršiti. Model sadrži ukupno 129 BP, od kojih je 61 organizovano u 11 SSE OP, a preostalih 68 BP odnosi se na projektne i organizacione OP (tabeli 10.6) [101].

Tabela 10.6 *Broj BP po OP u SSE CMM modelu*

SSE OP	Broj BP	Projektne i organizacione OP	Broj BP
OP 01	4	OP 12	8
OP 02	6	OP13	5
OP 03	6	OP 14	6
OP 04	6	OP15	6
OP 05	5	OP 16	10
OP 06	5	OP 17	4
OP 07	4	**OP 18**	4
OP 08	7	OP 19	5
OP 09	6	**OP 20**	7
OP 10	7	**OP 21**	8
OP 11	5	**OP 22**	5
Ukupno BP=129	61		68

Bazična praksa se mora izvršiti u implementiranom procesu (OP), primenjuje su u životnom ciklusu sistema i, uglavnom, ne preklapa se sa drugim BP. Generalno, *BP--e* predstavljaju *najbolju praksu zaštite*, ne specificiraju neki metod ili alat, već su pre preporučena organizacija za izvršavanje aktivnosti u OP. Lista BP se u OP prikazuje sa: *rednim brojem, nazivom, opisom, primerom proizvoda rada i napomenom* kao u sledećem primeru:

OP19 – Upravljaj razvojnom linijom proizvoda zaštite
BP.19.01 Definiši razvoj proizvoda!
BP.19.02 Identifikuj tehnologiju za novi proizvod ili pomoćne strukture koje će omogućiti organizaciji nabavku, razvoj i primenu tehnologije za konkurentsku prednost!
BP.19.03 Napravi neophodne promene u razvoju, za podršku razvoja novog proizvoda!
BP.19.04 Osiguraj da su na raspolaganju kritične komponente za planirani razvoj proizvoda!
BP.19.05 Ubaci novu tehnologiju u razvoj proizvoda, marketing i proces proizvodnje!
Opis BP:
BP.19.01 Definiši razvoj proizvoda!
Definiši tipove proizvoda koje treba ponuditi!
Opis: Definiše proizvodnu liniju koja podržava strateške ciljeve organizacije, razmatra snagu i slabosti organizacije, konkurentnost, potencijalnu veličinu tržišta i tehnologija!
Primer proizvoda rada:
• definicija linije proizvoda zaštite
Napomena: definisanje linije proizvoda zaštite omogućava efektivniju iskoristivost (ponovno korišćenje) objekata i veći potencijalni povratak investicija u zaštitu (ROSI). **....**

10.3.2 Dimenzija sazrevanja kapaciteta procesa

Dimenzija kapaciteta (*Capability Side*) obuhvata tri kategorije atributa procesa:

- *generičke prakse* – ***GPs*** (***G****eneric* ***P****ractices*)**,**
- *zajedničke (opšte) karakteristike* – ***CFs*** (***C****ommon* ***F****eatures*) i
- *nivoe kapaciteta procesa* – ***CLs*** (**C**apability **L**evels).

Dok je *oblast primene* lako razumljiva i intuitivno prihvatljiva, teže je razumeti dimenziju kapaciteta SSE CMM modela, koja definiše *kvalitet izvršavanja* BP i OP. Dimenzija kapaciteta SSE CMM modela sadrži ukupno trideset GP**,** koje se izvršavaju kroz izvršavanje BP-a i *evaluiraju kvalitet* njihovog izvršavanja. GP-e se grupišu u ukupno dvanaest CF-a, raspoređenih na pet *nivoa zrelosti kapaciteta* (*CL*).

Generičke prakse (GP) predstavljaju izvorne, opšte radnje čije se izvršavanje zahteva u svim OP u domenu primene i direktno određuju kapacitete organizacije za izvršavanje procesa, odnosno *kvalitet izvršavanja* BP procesa (OP). U modelu, GP su grupisane prema opštim karakteristikama u CF prema svojoj zrelosti, koja raste sa stepenom uvođenja metrike modela, a CF se grupišu po nivoima kapaciteta (CL) od 1. do 5., od kojih svaki CL sadrži nekoliko CF-*a*. *GP-e* sa većom zrelosti ukazuju na viši nivo kapaciteta procesa. GP

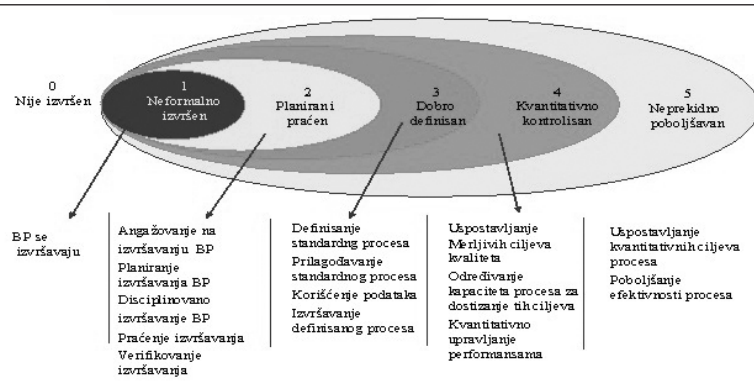
moraju biti izvršene u nekoj OP, u toku izvršavanja BP, da bi se odgovarajuća OP pripisala nekom nivou zrelosti kapaciteta – CL. Stepen implementacije GP koristi se za *evaluaciju* i progresivno poboljšavanje procesa. GP-e određuju nivo *implementacije* i *institucionalizacije* BP i poboljšavaju kapacitet svakog procesa u konkretnoj kategoriji OP [30, 101].

Opšte karakteristike (CF) su svi opšti aspekti procesa, grupisani u logičke oblasti – nivoe kapaciteta (CL). CF sadrže jednu ili više GP i *sredstvo su za kategorizaciju GP*. Kategorije CF su vrlo slične kroz sve OP. CF se nazivaju *institucionalizacione,* zato što osiguravaju da su OP efektivne, ponovljive i stabilne i da obezbeđuju potrebnu infrastrukturnu podršku. CF su organizovane na pet (šest) aktivnih CL (1 – 5.), gde se 0. nivo izostavlja/ne izvršava, zavisno od *reprezentacije* modela. U tabeli 10.7 prikazana je distribucija CF po CL u kontinualnoj reprezentaciji modela.

Tabela 10.7 *Zajedničke karakteristike (CF) po nivoima kapaciteta (CL)*

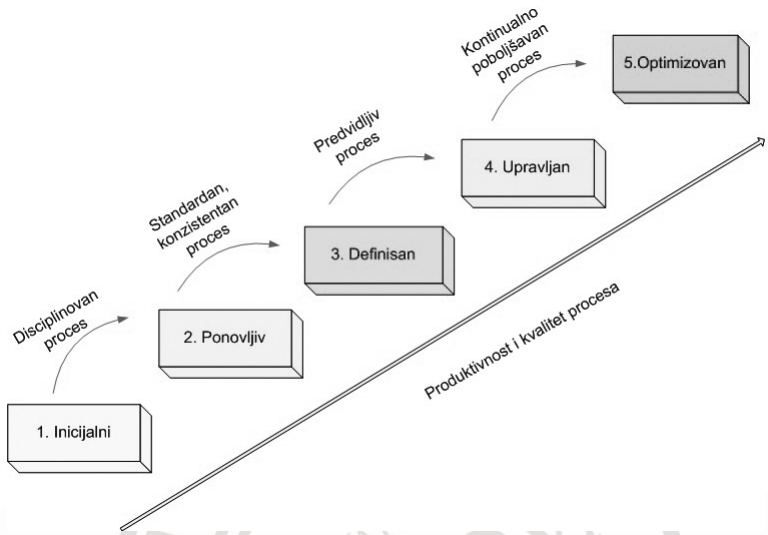
Nivo kapaciteta (CL)	Zajedničke karakteristike (CF)
1.	1.1. BP su izvršene
2.	2.1. Planiranje performansi 2.2. Disciplinovanje aktivnosti 2.3. Verifikacija aktivnosti 2.4. Praćenje aktivnosti
3.	3.1. Definisanje standardnog procesa 3.2. Izvršavanje definisanog procesa 3.3. Koordinacija procesa
4.	4.1. Uspostavljanje merljivih ciljeva kvaliteta 4.2. Objektivno upravljanje aktivnostima
5.	5.1. Poboljšanje organizacionih kapaciteta 5.2. Poboljšanje efektivnosti procesa

Grafički model progresivnog rasta CL-a sa pripadajućim CF u *kontinualnoj* prezentaciji prikazan je na slici 10.4 [74].



Slika 10.4 Nivoi kapaciteta (CL) procesa zaštite u kontinualnoj reprezentaciji

Put sazrevanja procesa sa glavnim atributima nivoa zrelosti – *ML*, u *faznoj reprezentaciji* SSE CMM, ilustrovan je na slici 10.5.



Slika 10.5 Put sazrevanje procesa (ML) SSE CMM modela

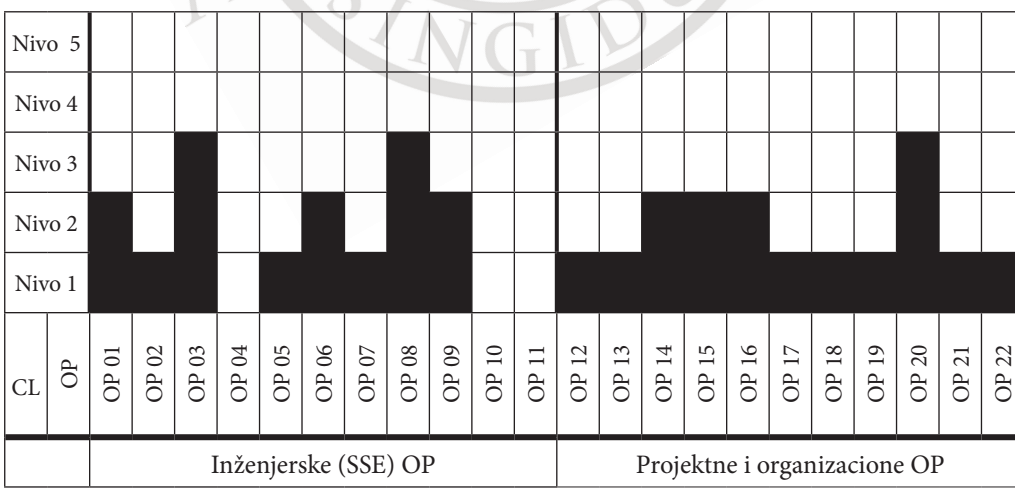
Skraćen opis CF, distribuiranih po CL u *kontinualnoj reprezentaciji* SSE-CMM-a prikazan je u tabeli 10.8 [30].

Tabela 10.8 *Raspored CF po CL SSE CMM modela*

CL	CF po nivoima kapaciteta
1	**Izvršavan neformalno** *CF 1.1: BP su izvršene* – u organizaciji se izvršava neki proces zaštite koji uključuje BP--e. Postoje politika zaštite i specifične prakse upravljanja i standarda zaštite.
2	**Planiran, kompletiran, praćen i kontrolisan** *CF 2.2: Disciplinovano izvršavanje* – postoje procesi za upravljanje projektima i dokumentacijom. *CF 2.3: Verifikovano izvršavanje* – vrši se vrednovanje akcija, projekata i skupa procesa i praksi dizajniranih za ispitivanje efektivnosti kontrola za tretman rizika. *CF 2.4: Praćenje izvršavanja* – prate se procesi kontrole kvaliteta koji se odnose na specifične projekte, strateške inicijative ili menadžment zaštite; cilj je verifikovati da li postoji kvalitetan proces za uspostavljanje metrika za operativni rad i održavanje i kapaciteta za efektivnu implementaciju upravljanja promenama.

CL	CF po nivoima kapaciteta
3	**Dobro definisan** *CF 3.1: Definisanje standardnih proc*esa – disciplinovano prilagođavanje standardnih procesa organizacije, nezavisno od inicijative, projekta ili oblasti primene. *CF 3.2: Izvršavanje definisanog procesa* – kako postojanje procesa ne znači da se precizno izvršava, treba otkriti dokaze koji *objektivno potvrđuju* da se proces primenjuje, u skladu sa dokumentacijom o kvalitetu i reviziji kvaliteta izvršavanja procesa, akcionim planovima i dnevnim redovima i isporukama rezultata. *CF 3.3: Koordiniranje procesa* – verifikacija postojanja procesa i koraborativnih dokaza, kao što su planovi projekata i isporuka, koji potvrđuju usklađenost praksi.
4	**Kvantitativno kontrolisan** *CF 4.1: Uspostavljanje merljivih ciljeva zaštite* – mere se poslovni ciljevi organizacije, sakupljaju i koriste bazični merni podaci sa projekata, ali ne u celoj organizaciji. *CF 4.2: Objektivno upravljanje performansama* – metrika se ugrađuje u šire procese za postizanje poslovnih ciljeva organizacije.
5	**Kontinualno poboljšavan** *CF5.1: Poboljšavanje kapaciteta organizacije* – inkrementalno se poboljšavaju upravljačke prakse procesa sa prethodnih CL-a, koriste stečena iskustva i unapređuje kultura rada. Ovaj CL je teško dostići zato što zahteva prakse koje podržavaju poslovne ciljeve, dokaze o tim praksama, kao i dokaze o ROSI, što je složeno. *CF5.2*: *Poboljšavanje efektivnosti procesa* – GP-e ove CF fokusirane su na izgradnju standardnih procesa od procesa koji se neprekidno, kontrolisano poboljšavaju. Eliminišu se uzroci defekata u kontinualno poboljšavanim standardnim procesima. GP ove CF obezbeđuju optimalne procese.

Nivoi kapaciteta (*CL*) *ne mogu imati diskontinuitet*, tj. OP mora biti zadovoljena za CL1, da bi se mogla poboljšavati za CL2 i tako redom (slika 10.6).



Slika 10.6 Sazrevanje kapaciteta OP u SSE CMM modelu

Jedan CL sadrži jednu ili više CF i sa nominalnim povećanjem, povećavaju ukupne kapacitete OP. Postoji više načina da se GP grupišu u CF i CF u CL. Nivoi CL se definišu kao jedinstveni skup praksi sa opštim karakteristikama (CF) u svim OP koje se izvršavaju interaktivno, sa ciljem da se obezbedi glavno poboljšanje kapaciteta za izvršavanje procesa. Svaki nivo kapaciteta dekomponuje se u skup CF-*a* koje sadrže skup GP. U modelu svaka GP je detaljno opisana posle kratkog opisa CF.

Primer: Opis GP, CF i CL u SSE CMM modelu

CL1 – Izvršen neformalno

Kratak opis: BP ove OP generalno se izvršavaju, ali ne rigorozno, planirano i praćeno. Izvršavanje BP zavisi od individualnih znanja, veština i napora. Proizvodi rada OP ispituju se na bazi izvršavanja BP. Pojedinci u organizaciji prepoznaju da neka akcija treba biti izvršena i postoji opšta saglasnost da je neka akcija izvršena, kada i gde se to zahteva. Postoji i neki proizvod rada procesa koji se može identifikovati.

Lista CF – Ovaj nivo kapaciteta sadrži sledeće CF-a:

• CF 1.1 – *BP-e su izvršene*

Kratak opis: GP-e ove CF ukazuju da se BP ove OP izvršavaju na neki način. Međutim, velika je verovatnoća da konzistentnost, izvršavanje i kvalitet proizvoda rada ovog procesa mnogo variraju, zbog nedostatka implementiranih kontrola.

Lista GP – CF se sastoji od sledećih GP-i:

• GP 1.1.1 – *izvrši proces*

Opis: izvrši proces koji implementira BP OP tako da klijentu obezbedi proizvod rada/ servis.

Napomena: proces može biti »neformalni«, a klijent(i) OP mogu biti interni i eksterni.

Skraćeni pregled komponenti dimenzije nivoa kapaciteta SSE CMM v.3.0 modela dat je u **Prilogu 10.1**.

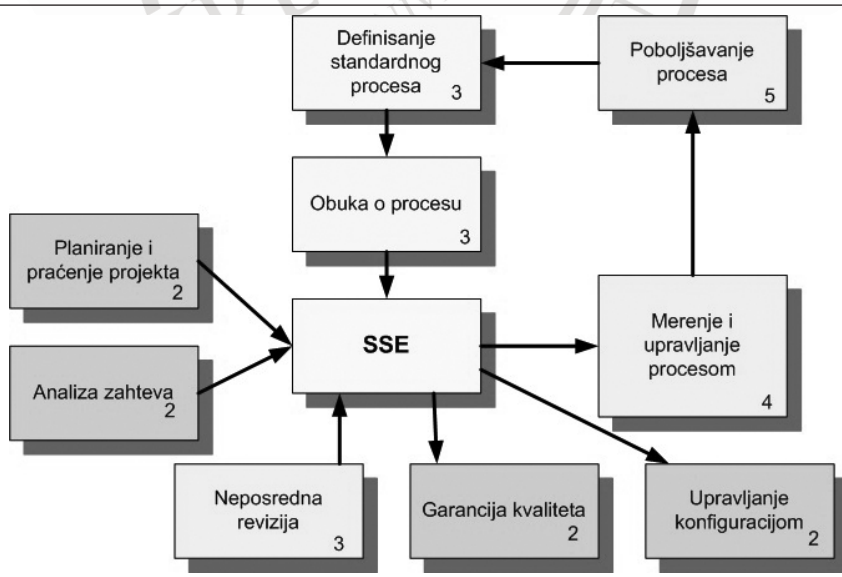
Glavni principi sazrevanja procesa i kapaciteta SSE CMM V. 3.0 modela izvedeni su iz opštih, logičkih principa SE upravljanja projektom (tabela 10.9).

Tabela 10.9 *Principi sazrevanja procesa zaštite u SSE CMM modelu*

Opšti principi	Principi sazrevanja procesa u SSE CMM-u
1. Morate nešto uraditi da bi njime upravljali.	**1**. *Nivo neformalnog izvršavanja procesa* fokusiran na izvršavanje procesa koji sadrži bazične prakse.
2. Razumeti šta se događa na projektu pre definisanja procesa u organizaciji.	**2**. *Nivo planiran i praćen* fokusiran je na definisanje nivoa projekta, planiranje i izvršavanje.
3. Koristiti sve naučeno na projektu za formiranje procesa u celoj organizaciji.	**3**. *Nivo dobro definisan* fokusiran je na disciplinovano izvršavanje i formiranje standardnih procesa organizacije od definisanih procesa.

Opšti principi	Principi sazrevanja procesa u SSE CMM-u
4. Ne možete nešto meriti dok ne znate šta je to.	*Metrika* zahteva skupljanje i korišćenje osnovnih mernih podataka na projektu što ranije (i na 1. CL-u), merenje i korišćenje mernih podataka u celoj organizaciji očekuje se na 3.CL, a posebno na 4.CL kvantitativno kontrolisan nivo.
5. Upravljanje mernim sistemom ima smisla samo kada merite prave stvari.	**4**. *Nivo kvantitativno kontrolisan*, fokusiran je na povezivanje merenja sa poslovnim ciljevima organizacije.
6. Kultura neprekidnog poboljšanja zahteva formiranje dobre prakse upravljanja, definisane procese i merljive ciljeve.	5. *Nivo neprekidnog poboljšanja* podržavaju sva inkrementalna poboljšanja na prethodnim nivoima, zatim se pojačava pomakom u razvoju kulture rada koja održava postignute rezultate.

U *kontinualnoj reprezentaciji* SSE CMM-a organizacija može dostići različite nivoe zrelosti u različitim OP sa dinamikom i resursima koji su na raspolaganju. Ovo dopušta organizaciji da se fokusira na one OP koje su relevantne za specifične oblasti poslovanja. Model obezbeđuje progresivni rast kvaliteta izvršavanja i broja izvršavanih GP koje indiciraju dostizanje nivoa CL/ML. Na slici 10.7 ilustrovano je kako organizacija, koja je dostigla 2. CL/ML može dostići više nivoe, ako formalno opiše i definiše standardni proces i vrši obuku o procesu (treći nivo), meri performanse (četvrti nivo) i upravlja i poboljšava procese (peti CL/ML) [69].



Slika 10.7 Implementacija SSE CMM nivoa zrelosti SSE procesa

Sa porastom nivoa CL/ML OP, veliki broj GP se formalizuje, dokumentuje i standardizuje u celoj organizaciji. Na primer, planiranje i praćenje projekta postoji u nekoj formi na prvom i drugom nivou, ali na trećem nivou počinje korišćenje procesa organizacije i alata za upravljanje projektom. Na drugom nivou vrši se neformalna revizija, dok se na trećem nivou zahteva formalizovana i koordinirana revizija sa drugim funkcijama za razvoj i održavanje sistema zaštite. Za više nivoe kapaciteta (četvrtom i petom) uključuju se metrike i merenja performansi i neprekidno poboljšanje procesa (OP).

10.4 PRIMENA SSE CMM MODELA ZA RAZVOJ PROGRAMA ZAŠTITE

Izgradnja sistema zaštite informacija je *tekući proces* koji zahteva tekuću SE analizu pretnji, periodičnu evaluaciju sistema zaštite i stalno poboljšanje procesa zaštite. Model SSE CMM obuhvata *SSE aktivnosti* koje pokrivaju ceo životni ciklus sistema zaštite, a može se primeniti na *proizvođače i provajdere proizvoda zaštite, projektante i integratore sistema zaštite, TTPS provajdere zaštite* i *SSE rešenja zaštite*, kao i na *sve tipove i veličine organizacija* [108, 35].

Bezbednosni ciljevi primene SSE procesa zaštite mogu biti različiti: *razumeti rizik; balansirati bezbednosne zahteve na bazi procene rizika; prevesti zahteve u uputstva i politiku zaštite; integrisati različite discipline i specijalnosti; opisati konfiguraciju sistema i operacija; odrediti prihvatljivost preostalog rizika; uspostaviti garantovanu bezbednost (poverenje u efektivnost kontrola zaštite)* itd.

Model zahteva da organizacija uspostavi SSE procese *najbolje prakse zaštite,* zatim, da meri usaglašenost sa nivoima ML i CL OP modela i povećava ih u skladu sa raspoloživim resursima i bezbednosnim potrebama. Dakle, model definiše *zahteve za procese za razvoj sistema zaštite*, a ne *nivoe poverenja* kao CC i slični standardi, kao i metodologiju za evaluaciju SSE procesa organizacije [34].

Cilj svakog projekta primene modela u praksi zaštite je, da: *unapredi SSE procese u definisanu, zrelu i merljivu disciplinu; omogući definisanje i poboljšanje SSE procesa; unapredi menadžment zaštite; meri performanse sistema zaštite na bazi poverenja u zrelost procesa organizacije* i *obezbedi kontinuitet, ponovljivost i efikasnost procesa za garantovanu bezbednost* sistema zaštite.

Glavni koncept primene modela za razvoj programa zaštite uključuje sledeće kategorije OP: (1) *definisane kriterijume* za merenje ML/CL, (2) *progresivno sazrevanje* ML/CL, (3) *definisan redosled povećanja* ML/CL, (4) *definisan cilj razvoja* ML/CL, (5) *definisan odziv* OP sistema zaštite, (6) *definisane prioritete* i redosled izvršavanja aktivnosti i OP, (6) *merenje progresa sazrevanja* ML/CL OP i (7) *komplementarnost sa drugim uputstvima i standardima* zaštite [83,85].

10.4.1 Razvoj optimalnog programa zaštite

Proces razvoja optimalnog programa zaštite primenom SSE CMM model procesa odvija se u tri glavne faze [85]:

Faza 1 – *Identifikovanje atributa „zrelosti" procesa za razvoj programa zaštite*:

- specifikovanje praksi i procesa prema SSE CMM modelu procesa,
- identifikacija procesa u kontekstu načina izvršavanja i
- identifikacija indikatora za procenu zrelosti kapaciteta procesa zaštite.

Faza 2 – *Merenje zrelosti i progresa sazrevanja procesa za razvoj programa zaštite***:**

- definisanje početnih i željenih nivoa zrelosti procesa i nivoa kapaciteta zaštite,
- procena rizika i *evaluacija* potencijalnih izvršioca za razvoj programa,
- povećavanje zrelosti procesa do željenog nivoa zrelosti programa zaštite i
- *evaluacija* i procena kvaliteta procesa za razvoj programa zaštite.

Faza 3 – *Realizacija programa zaštite*:

- obezbeđivanje opšte podrške menadžmenta,
- razvoj svesti o potrebi zaštite i
- razvoj kapaciteta OP organizacije za implementaciju procesa zaštite.

Glavni kriterijumi za određivanje nivoa kapaciteta programa zaštite IKT sistema, prema zahtevima SSE CMM modela detaljnije su opisani u **Prilogu 10.2**.

10.4.2 Primene SSE CMM za profilisanje procesa organizacija u zaštiti

Model SSE CMM mogu koristiti brojne IKT organizacije, i to [34]**:**

1. *inženjerske organizacije, integratori sistema, programeri aplikacija, isporučioci proizvoda zaštite i poverljivi provajderi servisa zaštite;*
2. *potrošačke organizacije***, koje nabavljaju proizvode/sisteme/servise zaštite od eksternih/internih izvora i krajnji korisnici;**
3. *organizacije za evaluaciju***, sertifikaciju i akreditaciju sistema, evaluatori i procenjivači proizvoda i sistema zaštite.**

SSE-CMM model ne sadrži ni jedan *aktuelan* profil organizacije, ali sadrži koncept za razvoj profila procesa organizacije, odnosno, rangiranja nivoa ML/CL OP. Profilisanje procesa organizacije smatra se važnim aspektom primene SSE CMM modela. U **Prilog 10.3** opisani su referentni profili OP *standardnog sertifikacionog tela (CA)* i *korisničke organizacije*, sa razlozima za izbor CL i OP.

10.4.3 Obezbeđivanje argumenata garantovane bezbednosti

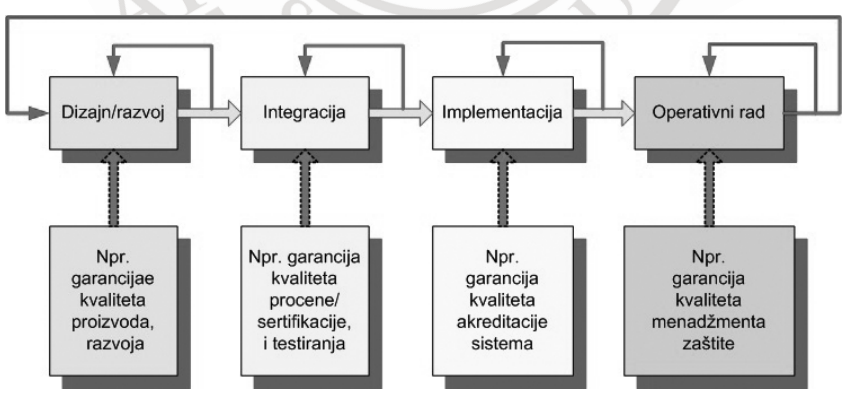
Primenom odgovarajućih SSE CMM aktivnosti i obezbeđivanjem *argumenata garantovane bezbednosti* uspostavlja se poverenje da će proizvod/proces/servis/ sistem zaštite zadovoljiti svoje bezbednosne ciljeve. Poverenje se stiče verifikacijom *dokaza garantovane bezbednosti,* sakupljenih u fazi razvoja, implementacije i iskustava iz operativnog rada

proizvoda/ procesa/servisa/sistema zaštite. *Dokazi garantovane bezbednosti* često se generišu u formi dokumentacije, razvijene u toku izvršavanja SSE aktivnosti. U izgradnji konzistentnog skupa *argumenata garantovane bezbednosti,* vrlo je važno poznavati izvor, bezbednosne zahteve i ciljeve dokaza, pošto različito doprinose izgradnji poverenja. SSE CMM je netradicionalni metod za garanciju kvaliteta bezbednosti IKT sistema, koji dokaze *garantovane bezbednosti* obezbeđuje na bazi evaluacije nivoa kapaciteta SSE procesa organizacije (CL1-CL5).

Izbor metoda za određivanje *garantovane bezbednosti* treba zasnivati na *politici garantovane bezbednosti* IKT proizvoda/procesa/servisa/sistema zaštite, poslovnim ciljevima i vrsti proizvoda/procesa/servisa/sistema zaštite organizacije. Na primer, SSE CMM je primenljiv samo za procese, dok je CC standard primenljiv samo za proizvode zaštite. Izabrani metod za određivanje *garantovane bezbednosti* treba da bude kompatibilan sa okruženjem organizacije, da ima kapacitete za ispitivanje željenih atributa i faza životnog ciklusa proizvoda/procesa/ servisa/ sistema zaštite i da uzima u obzir raspoloživost resursa organizacije za izabrani metod. Metodi za određivanje *garantovane bezbednosti* mogu se svrstati u tri kategorije, na bazi [10]:

- *evaluacije proizvoda rada* nezavisno od procesa razvoja,
- *evaluacije procesa* za razvoj, proizvodnju i operativni rad i
- *evaluacije faktora fizičkog okruženja i personala*.

Procesi za određivanje *garantovane bezbednosti* uključuju brojne nacionalne i međunarodne *de-facto* standarde i pogodne metodologije, koje mogu biti specifični za neku fazu životnog ciklusa. Za postizanja ukupne *garantovane bezbednosti*, u svakoj fazi treba *inkrementalno* povećavati dokaze i agregirati sakupljene argumente *garantovane bezbednosti* (slika 10.8), sve do *operativne* faze životnog ciklusa proizvoda/procesa/servisa/sistema zaštite [67].



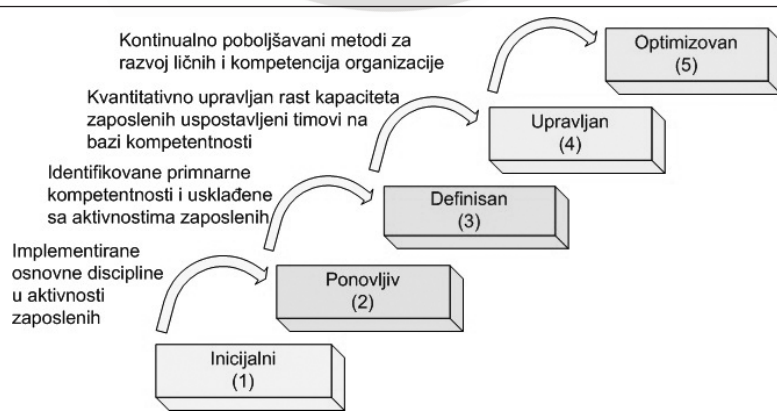
Slika 10.8 Odnosi metoda obezbeđivanja garantovane bezbednosti i redukovanog modela životnog ciklusa

10.4.4 Profilisanje kompetencija zaposlenih u oblasti zaštite (P-CMM)

Generički CMM okvir treba prioritetno primenjivati na prakse koje direktno doprinose povećavanju kapaciteta procesa za izvršavanje poslova organizacije, odnosno, obezbeđivanje proizvoda i servisa zaštite visokog kvaliteta. Kako su znanje, veštine i motivacija zaposlenih u zaštiti kritični za izvršavanje procesa zaštite, prakse i procesi za upravljanje *kompetencijama zaposlenih u zaštiti informacija,* pravi su kandidat za evaluaciju i poboljšavanje nivoa zrelosti tih procesa. Model P-CMM (*Personal CMM*) opisuje poboljšavanje kapaciteta za razvoj kompetencija zaposlenih u zaštiti informacija [21].

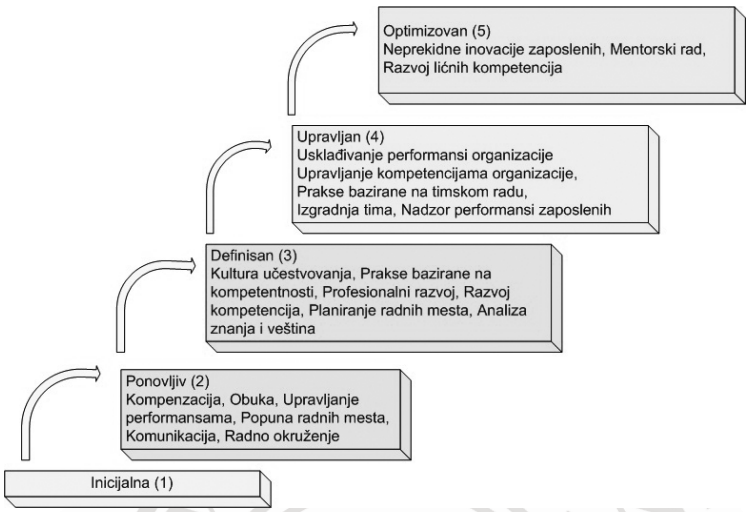
P-CMM sadrži pet razvojnih nivoa zrelosti BP i OP za uspostavljanje i poboljšanje kompetencija zaposlenih. Svaki dostignuti CL u P-CMM-u institucionalizuje nove kapacitete za razvoj kompetencija zaposlenih u zaštiti i obezbeđuje gradivni sloj za kontinualno poboljšanje BP i OP za razvoj kompetencija zaposlenih. P-CMM se može primenjivati za evaluaciju prakse zaposlenih, kao uputstvo za planiranje i implementaciju poboljšanja kompetencija zaposlenih i za kontinualno povećanje kapaciteta za razvoj kompetencija ljudskih resursa u IKT sistemu organizacije. Dugoročni, strateški ciljevi P-CMM-a mogu biti: *poboljšanje kapaciteta organizacije povećanjem kompetencija zaposlenih; povećanje* ***ljudskih kapaciteta*** *(atributa organizacije, a ne pojedinaca); povećanje motivacije pojedinaca, usklađene sa interesima i ciljevima organizacije i zadržavanje kritičnih ljudskih resursa, tj. ljudi sa kritičnim znanjima i veština*ma.

P-CMM obuhvata OP i BP u sledećim oblastima: *radno okruženje, komunikacija, popuna radnih mesta, obuka, upravljanje performansama, kompenzacija, razvoj kompetentnosti, profesionalni razvoj karijere, izgradnja timskog rada i razvoj kulture rada.* Nivoi kapaciteta P-CMM-a se poboljšavaju uspostavljanjem okruženja koje podstiče neprekidno učenje [45], sa kvantitativnom povratnom ocenom o performansama zaposlenih, odnosno, razvojem okvira sazrevanja za izgradnju takvog radnog okruženja u kojem se BP izvršavanju sa malim varijacijama, mogu se ponoviti, brzo preneti na celu grupu zaposlenih i kontinualno poboljšavati. Na slici 10.9 ilustrovano je pet nivoa sazrevanja P-CMM procesa sa ključnim atributima. Kriterijumi za izbor CL P-CMM detaljno su opisani u literaturi [21].



Slika 10.9 Nivoi i atributi CL OP P-CMM modela

Dimenzija OP-a u P-CMM modelu ilustrovana je na slici 10.10.



Slika 10.10 Sazrevanje nivoa i atributi OP P-CMM modela

U tabeli 10.10 navedene su oblasti OP P-CMM modela sa osnovnim atributima na odgovarajućim nivoima zrelosti [21].

Tabela 10.10 *OP P-CMM modela po nivoima zrelosti*

ML	Atribut zrelosti	Oblast procesa (OP)
1.	Inicijalni procesi	ne razmatra se
2.	Ponovljivi procesi	OP1: radno okruženje
		OP2: komunikacija
		OP3: popuna radnih mesta
		OP4: upravljanje performansama
		OP5: obuka
		OP6: kompenzacija za rad
3.	Definisani procesi	OP7: analiza znanja i veština
		OP8: planiranje sistematizacije zaposlenih
		OP9: razvoj kompetentnosti
		OP10: profesionalni razvoj
		OP11: prakse za procenu kompetentnosti
		OP12: kultura učestvovanja

ML	Atribut zrelosti	Oblast procesa (OP)
4.	Upravljani procesi	OP13: mentorsko vođenje
		OP14: izgradnja tima
		OP15: prakse za izbor kompetentnosti tima
		OP16: upravljanje kompetencijama organizacije
		OP17: usklađivanje performansi organizacije
5.	Optimizovani procesi	OP18: razvoj personalne kompetentnosti
		OP19: instruktivna obuka
		OP20: neprekidno inoviranje praksi zaposlenih

Međuzavisnosti OP u P-CMM-u uspostavljaju četiri *kategorije* OP na različitim nivoima zrelosti (ML): (1) *razvoj kapaciteta, (2) izgradnju tima i kulture rada, (3) motivisanje i upravljanje performansama rada i (4) oblikovanje radnog profila zaposlenih* (tabela 10.11).

Tabela 10.11 *Međuzavisnosti kategorije OP-a i nivoa zrelosti u P-CMM modelu*

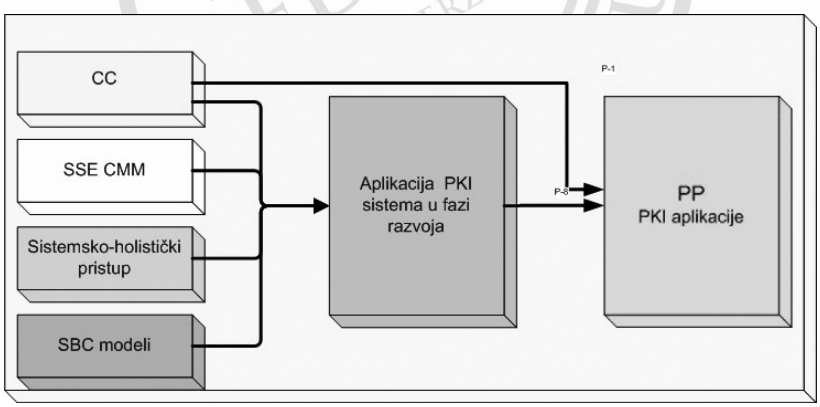
ML	Kategorije procesa (OP)			
	Razvoj kapaciteta	*Izgradnja tima i kulture rada*	*Motivisanje i menadžment performansi rada*	*Oblikovanje radnog profila zaposlenih*
5.	Instruktorska obuka Razvoj ličnih kompetencija	Kontinualno osposobljavanje zaposlenih		
4.	Mentorski rad	Izgradnja tima	Usklađivanje performansi organizacije Razvoj praksi na bazi timskog rada	Upravljanje kompetencijama organizacije
3.	Razvoj kompetencija Analiza znanja i veština	Kultura učestvovanja	Razvoj praksi na bazi kompetentnosti Profesionalni razvoj	Planiranje ljudskih resursa
2.	Obuka, komunikacija	Komunikacija	Kompenzacija Upravljanje performansama Radno okruženje	Popuna radnih mesta

*Dimenzija ML (*fazna reprezentacija*)* P-CMM-a obuhvata pet CF: *(1) angažovanost na izvršavanju praksi, (2) sposobnost izvršavanja praksi, (3) izvršene aktivnosti, (4) merenje i analiza i (5) verifikovanje implementacije*. CF – *Izvršene aktivnosti* opisuje prakse implementacije, a ostale pomažu da se ove prakse institucionalizuju u kulturu rada organizacije, tako da su efektivne, ponovljive i trajne.

10.4.5 Razvoj bezbednosnih zahteva

U svim aspektima zaštite, metrički sistemi doprinose boljem razumevanju procesa i performansi procesa zaštite i bržem odlučivanju za implementaciju *kontrola zaštite*. Metrike zaštite se koriste za: *identifikaciju i određivanje kritičnih i nekritičnih bezbednosnih parametara*; *testiranje i usmeravanje napora za evaluaciju sistema i procesa zaštite; indikatore nivoa implementacije i institucionalizacije kontrola zaštite; merenje ML procesa zaštite i CL organizacije* [107].

U procesu razvoja bezbednosnih zahteva, može se koristiti kombinovana metrika CC (*EAL*) i SSE CMM (*CL*) standarda. Bezbednosni zahtevi mogu se razvijati na bazi evaluacije bezbednosnih funkcija proizvoda zaštite (CC) ili politike zaštite (ISO/IEC 27001). Specifikacija bezbednosnih zahteva za proizvod/sistem zaštite prema CC standardu vrši se kroz *profile zaštite* (PP). Razvoj PP direktno se odnosi na specifikovanje ciljeva zaštite (ST) i bezbednosnih nivoa (EAL). Okvir za razvoj PP proizvoda i sistema zaštite, može se uspostaviti primenom različitih metoda kao što su CC, SSE CMM, model sistema zaštite sa konsenzusom – SBC (*Security By Consensus*) itd. Standardi CC i SSE-CMM koriste se za razvoj potrebnih metrika, identifikovanje bezbednosnih funkcija i analizu pretnji koje se direktno ne odnose na organizaciju i ponašanje korisnika. *Sistemsko-holistički model* i SBC [68], korisne su za razvoj metrika koje se odnose na obuku u zaštiti, personalnu zaštitu i socijalni aspekt zaštite. Međutim, ovi se modeli mogu koristiti i u drugim aspektima istraživanja bezbednosti IKT sistema [115]. Na slici 10.11 predstavljen je primer modela okvira za razvoj PP PKI sistema.



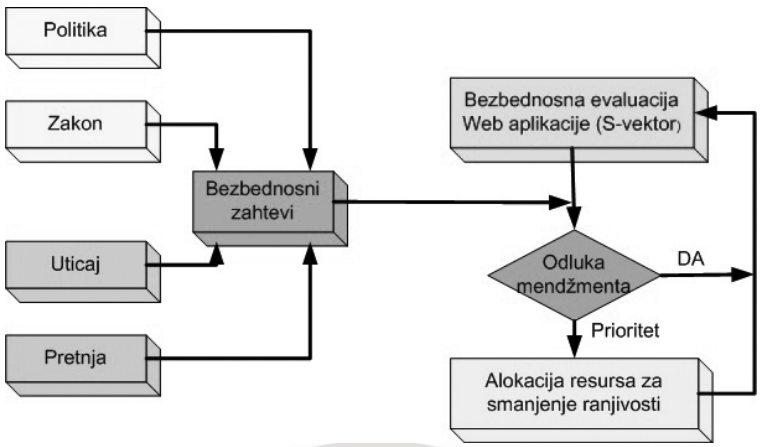
Slika 10.11 Okvir za razvoj profila zaštite PKI sistema

Primer: Za razvoj PP za *X.509 digitalni sertifikat*, korisno je upotrebljavati metriku zaštite koja je pogodna za analizu pretnji i faktora rizika [36, 66, 68]. U cilju veće interoperabilnosti nacionalnog PKI sistema sa drugim PKI sistemima razvijeno je pet tipova *politika sertifikata* (CP) PKI, koje definišu pet bezbednosnih nivoa: (1) *ne postoji*, (2) *rudimentarni, (3) osnovni, (4) srednji i (5) visoki nivo bezbednosti* [61]. U suštini, ovi nivoi su metrike koje koriste klasifikaciju kritičnih i nekritičnih funkcija CP PKI sistema. Standardna metrika SSE CMM može se koristiti za indikaciju dubine CC testiranja specifičnog proizvoda i određivanje EAL nivoa, a NIST-ova metodologija metrika zaštite može biti korisna za merenje ML procesa zaštite organizacije [106]. Ključne oblasti procesa u razvoju PP u CC standardu prikazane su u dekomponovanoj CC klasi – *Evaluacija PP* koja uključuje: *opis TOE; bezbednost okruženja; uvođenje PP; bezbednosne ciljeve; IKT bezbednosne zahteve i eksplicitno navedene bezbednosne zahteve* [16, 53].

Za definisanje i razvoj PP kritične su sledeće OP: *identifikacija kritičnih objekata IKT sistema, pregled politika zaštite, upravljanje rizika, procena ponašanja u sistemu, identifikovanje i analiza pretnji i analiza bezbednosnih funkcija.*

Standardi CC i SSE CMM potvrđuju kompatibilnost u procesu identifikovanja i razvoja bezbednosnih funkcija i metrika zaštite. Dok CC sadrži *tehničke metrike*, SSE CMM sadrži *metrike specifične za procese i sistem zaštite*, koje se više odnose na uticaj *okruženja sistema* i koje su zaista korisne za procenu pretnji iz okruženja. Ova kolaboracija metrika CC i SSE CMM primenjena je direktno u metodologiji vektora zaštite (*S-vektora*) za upravljanje zaštitom web aplikacija [104, 30].

U menadžment sistemu *web* aplikacija metodologija S-vektora primenjuje se u okviru opšte strukture u kojoj metod S-vektora ima značajnu ulogu (slika 10.12). Periodična evaluacija *web* aplikacija daje tekući težinski faktor S-vektora svake *web* aplikacije i inicijalni S-vektor nove *web* aplikacije. Bezbednosni elementi, određeni uticajem i pretnjama, u skladu sa politikom zaštite i legalnim zahtevima, moraju biti mapirani u željeni S-vektor. Menadžment može koristiti metodologiju S-vektora u skladu sa bezbednosnim zahtevima, za određivanje kritične *web* aplikacije sa najvišim prioritetom za usmeravanje resursa za zaštitu [8].



Slika 10.12 Menadžment proces web aplikacija primenom metodologije S-vektora

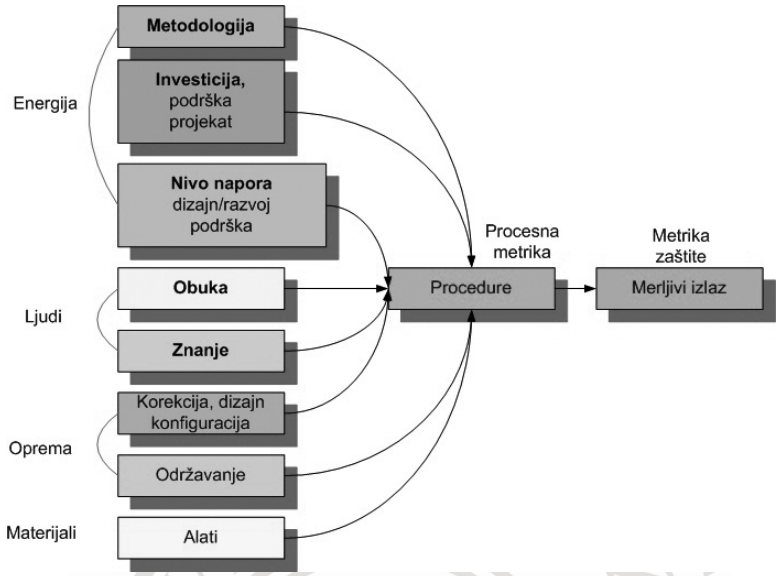
Osnovna prednost metodologije S-vektora je, što omogućava korišćenje dva relevantna standarda – *CC* i *ISMS* za specifične kontrole S-vektora, dok *SSE CMM* model uspostavlja zreo i institucionalizovan okvir za menadžment programa zaštite *web* aplikacije. Metodologija S-vektora sadrži *tehničke, proceduralne i strukturalne* komponente i zbog toga obezbeđuje sveobuhvatniju procenu bezbednosti *web* aplikacija nego ISMS ili SSE CMM standardi pojedinačno.

Glavni nedostatak metodologije S-vektora je što u potpunosti nisu definisana preklapanja i redundantnosti između ISMS i SSE CMM standarda [8, 101, 104]. Za efektivnu implementaciju S-vektora, otvorena su brojna pitanja, kao što su *definisanje obima S-vektora; izbor rentabilnog alata za procenu nivoa zaštite web aplikacija* itd. Zato je *S-vektor još uvek više strategija nego konzistentna metodologija* i potrebna su dalja istraživanja.

10.4.6 Primene metrike sazrevanja kapaciteta procesa zaštite

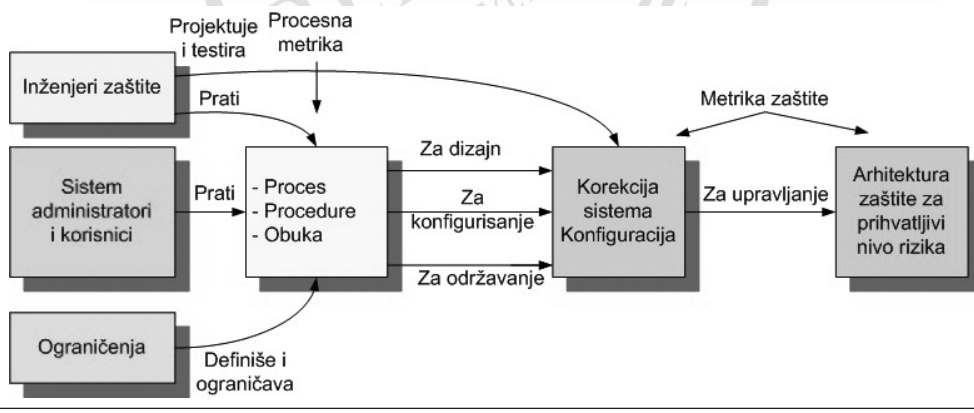
Suštinsko pitanje u primeni SSE CMM modela za menadžment rizika je: „*Kako se može znati da primena procesa opisanih u modelu doprinosi većoj bezbednosti sistema ili operativnih kapaciteta?*“ Odgovor na ovo pitanje daje inherentna, dualna *metrika procesa* i *sistema zaštite* SSE CMM modela [69, 101, 116].

Metrika procesa je specifična metrika kvantitativnih/kvalitativnih dokaza nivoa zrelosti za određenu OP ili binarnih indikatora prisustva/odsustva zrelog procesa. *Metrika sistema zaštite* je merljiv objektivni/subjektivni ili kvantitativni/ kvalitativni atribut performansi SSE procesa SSE CMM modela, koji dokazuje efektivnosti tih procesa. Svaki proces ima ulazne parametre, ograničenja, aktivnosti i izlazne parametre. Izvršavanje, stabilnost, kapacitet, poboljšanje i investiranje glavni su faktori za efektivni menadžment procesa. Na slici 10.13 prikazan je progres metrika zaštite od ulaznih parametara procesa i ograničenja do procedura i merljivih izlaznih parametara [69].



Slika 10.13 Razvoj metrike zaštite

Prvo se ispituje postojanje i izvršavanje svakog procesa, bez procene koliko dobro se proces izvršava. Na slici 10.14 prikazan je odnos između SSE CMM metrika, ulaza u SSE proces, procesa koji se izvršava za postizanje SSE ciljeva i performansi procesa zašite.



Slika 10.14 Odnosi SSE CMM metrike procesa i metrike zaštite

Primer specifičnih entiteta koji mogu biti mereni u SSE procesu i na koje se metrika procesa može primeniti, prikazan je na slici 10.15.



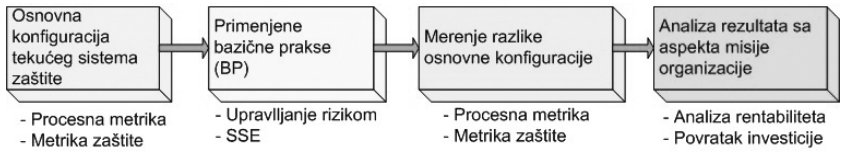
Slika 10.15 SSE CMM merljivi atributi procesa

U SSE CMM metrici sistema zaštite, OP obezbeđuju SSE servise ili razvoj i analizu proizvoda i sistema zaštite. Zatim se mere bezbednosni atributi rezultirajućih proizvoda i sistema, procenom efektivnosti sistema zaštite. Primer je prikazan na slici 10.16.



Slika 10.16 SSE CMM merljivi atributi sistema zaštite

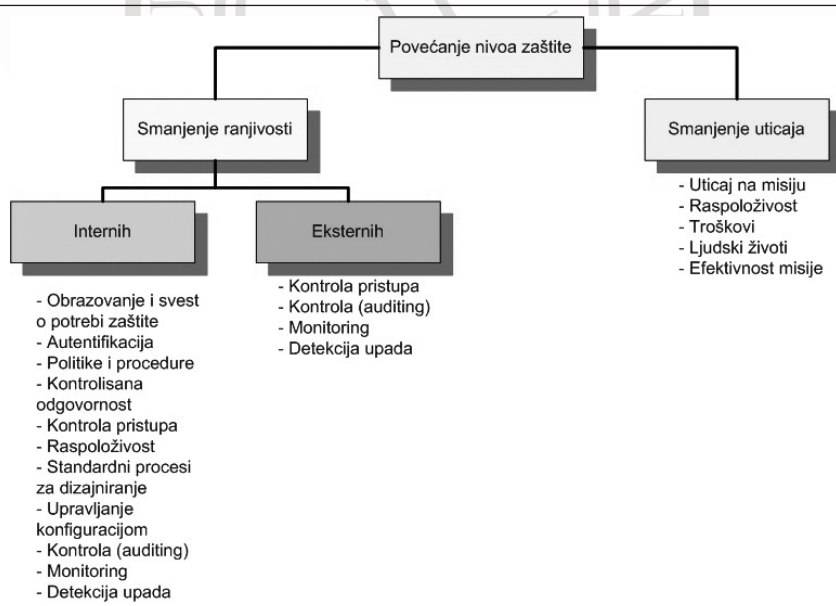
Međutim, ni jedna metrika se ne može uspešno primeniti za merenje efektivnosti zaštite, bez razumevanja relativnog značaja sistema zaštite za misiju organizacije. Izabrana metrika treba da bude relevantna za oblast poslovanja i da uzima u obzir da se mogu meriti samo poznate ranjivosti i pretnje i napadi iz okruženja. Metrike se ne mogu koristiti za apsolutna merenja performansi organizacije, ako nije poznat nivo bezbednosnog stanja sistema *pre* merenja. Dakle, zahteva se poznavanje *osnovne konfiguracije sistema zaštite* i ciljeva poboljšavanja zaštite *pre* i *posle* implementacije novih kontrola zaštite, da bi se dobilo neko značajnije merenje procesa i performansi sistema zaštite (slika 10.17).



Slika 10.17 Primena SSE CMM metrika procesa i sistema zaštite

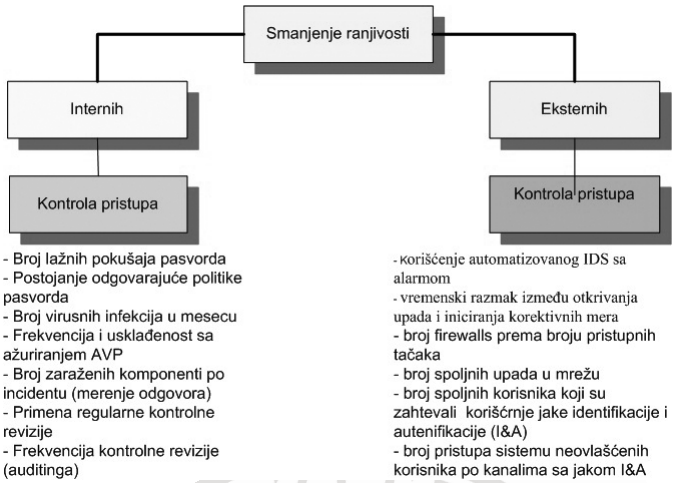
Prvi korak je izmeriti osnovnu konfiguraciju sistema zaštite, primenom procesne i sistemske metrike. Zatim se izvršavaju BP SSE procesa za menadžment rizika, da bi se identifikovale i implementirale mere za poboljšanje sistema zaštite organizacije. U drugoj evaluaciji mere se razlike stanja efektivnosti sistema zaštite *pre i posle* primene preporučenih mera zaštite. Na taj način određuje se relativno poboljšavanje nivoa bezbednosti i efektivnosti sistema zaštite. Dobijeni rezultat treba analizirati u odnosu na ciljeve i misiju organizacije, na bazi analize rentabiliteta ili ROSI, da bi se rezultati mogli interpretirati menadžmentu.

U procesu razvoja metrika zaštite mogu se koristiti brojni metodi. Prihvatljiv pristup za kategorizaciju adekvatne metrike je *odozgo-nadole* (slika 10.18), gde se metrike razmatraju sa aspekta uputstava, politike, korisnika, profesionalca zaštite, kontrolora i menadžera. Da bi *povećali nivo zaštite* profesionalci i kontrolori zaštite usmeravaju pažnju na redukciju faktora rizika na prihvatljiv nivo, a korisnici i menadžeri – na operativne kapacitete, smanjenje troškova, povraćaj investicija u sistem zaštite i korisničku prihvatljivost rešenja zaštite.



Slika 10.18 Dijagram razvoja metrika zaštite

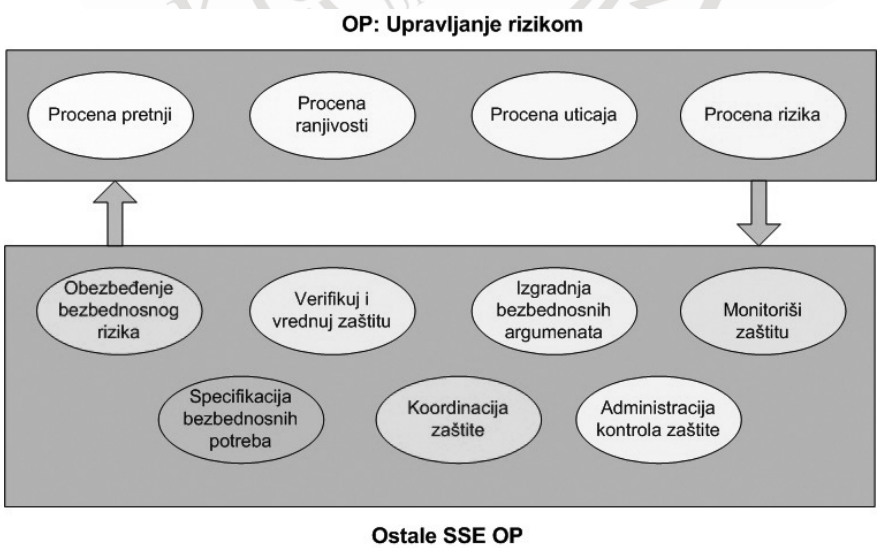
Na slici 10.19 ilustrovana je dekompozicija servisa *Kontrole pristupa* iz dijagrama sa slike 10.18 u skup procesnih i sistemskih metrika.



Slika 10.19 Moguće metrike servisa kontrole pristupa

Na slici 10.19 procesne metrike daju *automatizovani IDS sa alarmom* i *regularna provera (revizija)*, a metrike sistema zaštite – *vremenski razmak između otkrivanja upada i iniciranja korektivnih mera* i *frekvencija provere (revizije)*.

Konkretan primer metrike prikazan je na slučaju samoevaluacije SSE CMM OP za *upravljanje rizikom* za treći nivo kapaciteta (CL3), u odnosu na servise OP i ulogu metrike u tome (slika 10.20). U ovom modelu SSE CMM OP delimo u dve grupe, za: *upravljanje rizikom* i *ostale SSE* OP, sa izostavljanjem brojnih veza između SSE OP.



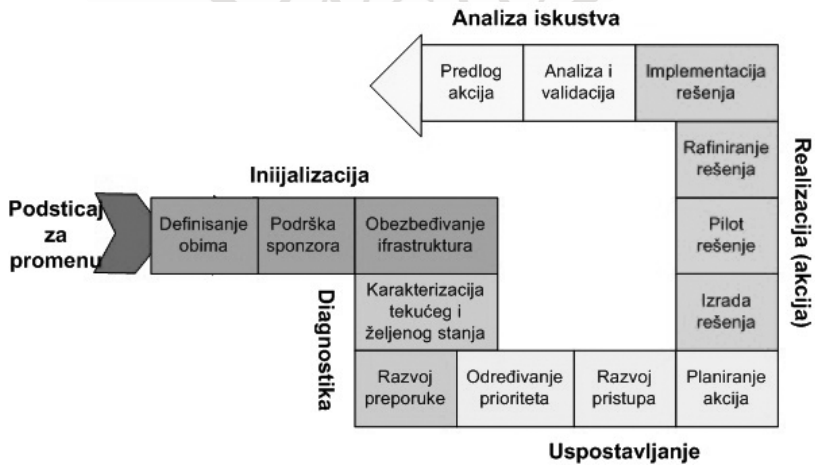
Slika 10.20 Odnosi SSE CMM OP u modelu metrike za OP upravljanja rizikom

Model za CL3 zahteva da su: *izvršene sve BP OP na CL2; performanse planirane (GP 2.1), disciplinovane (GP 2.2); verifikovane (GP 2.3) i praćene (GP 2.4), a standardni procesi definisani (GP 3.1), izvršeni (GP 3.2) i koordinisani (GP 3.3).* Procesna metrika ovih OP je direktna. U prvoj fazi analize, metrika kapaciteta za izvršavanje BP/GP su binarni elementi: *DA/NE* ili *1/0*, što znači da organizacija izvršava ili ne izvršava evaluiranu BP/GP i ne ispunjava kriterijume CL.

Primer: *Kriterijume* za određivanje CL određene OP definišu SSE CMM model i SSAM metod evaluacije: OP dostiže 1.CL ako su sve BP *100%* izvršene, a nivoe 2. – 5.CL, ako je OP sa prethodnog CL izvršena *100%*, a najmanje *80%* OP sa tekućeg CL, pri čemu minimalno *50%* dokaza o izvršavanju i implementaciji BP/GP mora biti dokumentovano da se OP smatra izvršenom, implementiranom i/ili institucionalizovanom na nekom CL.

10.4.7 Implementacija CMM praksi i procesa

Implementacija SSE CMM i CMMI praksi i procesa može se izvršiti prema SEI modelu ***IDEAL (Initiating, Diagnosing, Establishing, Acting, Learning)*** ili nekom drugom modelu (npr. PDCA ili 6 Sigma) za implementaciju procesa [21, 83]. Ulazni parametar u proces implementacije praksi i procesa SSE CMM modela je neka *inicijativa* za promenu, na osnovu koje se vrši priprema – definiše se sadržaj i obim, i obezbedi podrška menadžmenta i infrastruktura. U sledećem koraku faze *dijagnostifikovanja* obima implementacije procesa vrši se karakterizacija tekućih i željenih nivoa zrelosti procesa i daju preporuke. U fazi *uspostavljanja* procesa određuje se profil procesa, razvija pristup i planiraju aktivnosti za implementaciju. U fazi *realizacije* kreira se rešenje i testira pilot-rešenje za implementaciju. U fazi *analize iskustava* implementirano rešenje se analizira, izučavaju se stečena iskustva i daju predlozi za dalje aktivnosti (slika 10.21).



Slika 10.21 Model IDEAL za implementaciju CMMI i SSE CMM procesa

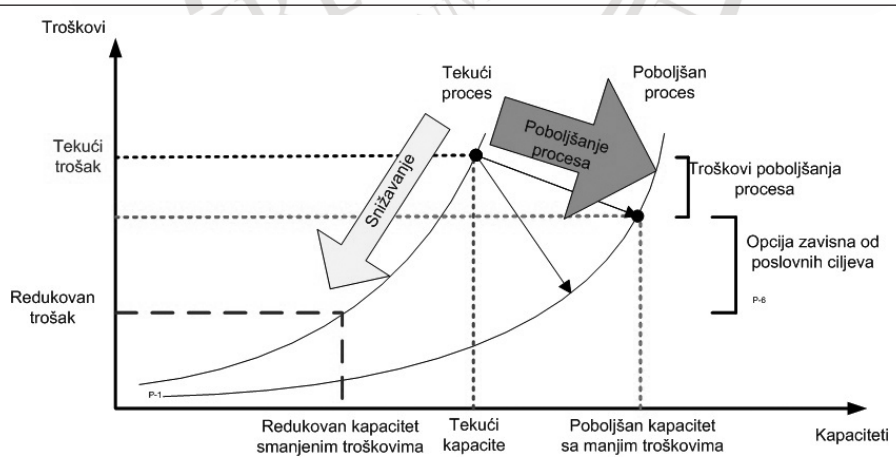
Nacrt sadržaja plana implementacije i operativnog plana poboljšanja procesa zaštite dat je u **Prilogu 10.4.**

10.4.8 Prednosti i nedostaci SSE CMM modela

Osnovna prednost primene SSE CCM modela za razvoj programa zaštite je, što model u *kontinualnoj reprezentaciji* može da meri progresivno sazrevanje individualnih procesa koji su najbitniji, sa kojima se izvršavaju *ključni servisi zaštite* i koji daju *najbolje rezultate* sa *raspoloživom dinamikom i resursima* organizacije. Primenom SSE CMM za definisanje i razvoj optimalnog programa zaštite, obezbeđuje se *poverenje da organizacija realizuje program zaštite prema planu zaštite, a razvoj programa planira u granicama raspoloživih resursa organizacije i meri adekvatnost komponente zaštite za specifikovani proces*.

Glavna prednost primene modela u zaštiti informacija je inherentna metrika sazrevanja procesa zaštite. Generalno, SSE CMM model i metod može se koristiti za: *merenje i poboljšanje zrelosti procesa*, *evaluaciju i profilisanje nivoa zrelosti procesa i kapaciteta zaštite* i *obezbeđivanje garantovane bezbednosti* [85].

Model, takođe, obezbeđuje povratak investicija u zaštitu (ROSI). *Finansijske prednosti* izbora i primene SSE CMM-a za poboljšanje procesa zaštite, grafički su prikazane dijagramom krive zavisnosti *kapaciteti – troškovi koja* ilustruje proces poboljšanja kapaciteta zaštite uz smanjenje troškova, u odnosu na tekuće kapacitete i troškove. Poboljšanje procesa inherentno smanjuje troškove, pa se kriva spušta prema osi *kapaciteta*, a ukupni troškovi smanjuju, uključujući i troškove samog poboljšanja procesa. Nivo troškova uvek zavisi od poslovnih ciljeva organizacije (slici 10.22) [67].



Slika 10.22 Dijagram rasta CL procesa u funkciji porasta troškova (Izvor: Merie Whatley, Texas Instruments. Inc.)

Glavni nedostaci su invazivnost verifikacionog metoda evaluacije procesa i vremenska i finansijska zahtevnost evaluacije i implementacije na bazi modela.

10.5 REZIME

Generički CMM definiše strukturu, ciljne karakteristike i ključne atribute za specifične procese i obezbeđuje referentni model *najboljih praksi* i *procesa* zaštite. Modeli se razlikuju po *disciplini primene (OP), strukturi komponenti* (kontinualna i fazna reprezentacija), *definisanju nivoa zrelosti* (ML) i *kapaciteta procesa* (CL).

Model SSSE-CMM (standard ISO/IEC 21827) je procesno orijentisana metodologija za razvoj sistema zaštite na bazi *organizacionih, projektnih* i *SSE* praksi i procesa. Modul SSAM opisuje metod evaluacije na bazi SSE CMM procesa. SSE CMM je struktuiran u *dimenzije primene* (OP) i *dimenzije sazrevanja procesa* (ML) i *kapaciteta* (CL). Nivoi ML i CL su struktuirani na pet nivoa (šesti se ne prikazuje). Model obuhvata dvadeset i dve oblasti procesa (OP) od kojih jedanaest sistema inženjerskih za zaštitu informacija i jedanaest organizacionih i projektnih. OP se izvršavaju kroz izvršavanje bazičnih praksi (BP), organizovanih prema zajedničkim karakteristikama (CF) u nivoe kapaciteta 1 – 5 (CL) ili nivoe zrelosti procesa (ML). Izvršavanje BP se zahteva, a generičke prakse (GP) evaluiraju *kvalitet izvršavanja* BP i OP u celini. Stepen implementacije GP koristi se za evaluaciju i poboljšanje procesa. U CF se grupišu jedna ili više *GP,* a jedna ili više CF se grupiše u CL – logičke oblasti i *institucionalizacione* kategorije kroz sve *OP*.

Sazrevanja procesa u faznoj reprezentaciji podrazumeva istovremeno podizanje svih OP na viši nivo zrelosti, a u kontinualnoj – poboljšavanje jedne ili grupe OP koje organizacija izabere na bazi kritičnosti za poslovanje i raspoloživih resursa. *Bezbednosni ciljevi SSE procesa* mogu biti menadžment rizika, uspostavljanje bezbednosnih zahteva, integracija SSE disciplina itd. SSE CMM obezbeđuje model za *kontinuitet, ponovljivost, efikasnost i garantovanu bezbednost* procesa zaštite.

Model se primenjuje za razvoj optimalnog sistema zaštite, profilisanje procesa organizacija, bezbednosnu garanciju, profilisanje kompetencija zaposlenih u zaštiti, razvoj bezbednosnih zahteva, procenu kapaciteta za menadžment rizika i zaštite *web* aplikacija. Za implementaciju SSE CMM procesa razvijen je model IDEAL. Glavne prednosti modela su inherentna metrika sazrevanja procesa zaštite i obezbeđen ROSI, a nedostaci su invazivnost verifikacionog metoda evaluacije procesa i vremenska i finansijska zahtevnost evaluacije i implementacije.

10.6 PITANJA ZA PONAVLJANJE

1. Zrelost procesa je:
   a. određena kvalitetom procesa koji se koristi za razvoj i održavanje proizvoda
   b. određena formalnim definisanjem procesa
   c. mera u kojoj je proces eksplicitno definisan, upravljan, merljiv, kontrolisan i efektivan
   d. opseg očekivanih rezultata koji se mogu postići kada se proces konzistentno izvršava.
2. Kapacitet procesa je:
   a. određen kvalitetom procesa koji se koristi za razvoj i održavanje proizvoda
   b. određena formalnim definisanjem procesa

c. mera u kojoj je proces eksplicitno definisan, upravljan, merljiv, kontrolisan i efektivan.
d. opseg očekivanih rezultata koji se mogu postići kada se proces konzistentno izvršava.

3. Generički model sazrevanja procesa je:
   a. TCMM
   b. CMM
   c. SE CMM
   d. SSE CMM.
4. Poverljivi model sazrevanja procesa je nastao iz:
   a. CMM
   b. SSE CMM
   c. TSM
   d. TCMM.
5. SSE CMM je:
   a. procesno orijentisana metodologija
   b. metodologija za evaluaciju i poboljšanje procesa zaštite
   c. model sazrevanja procesa zaštite
   d. integracioni model sazrevanja procesa za proizvodnju, snabdevanje i akviziciju.
6. SSE CMM sadrži sledeće oblasti procesa:
   a. za upravljanje procesima
   b. organizacione, projektne i sistem-inženjerske procese zaštite
   c. za razvoj softverskih proizvoda
   d. za razvoj industrijskih proizvoda.
7. SSE CMM model obuhvata sledeće dimenzije:
   a. dimenziju primene
   b. dimenziju metrike procesa
   c. dimenziju kvaliteta procesa
   d. dimenziju nivoa kapaciteta.
8. Reprezentacija SSE CMM modela predstavlja:
   a. struktuiranje oblasti procesa za rešavanje problema u zaštiti informacija
   b. organizaciju, način primene i prezentacije komponenti i puta sazrevanja procesa
   c. organizacija metoda verifikacije izvršavanja bazičnih praksi
   d. način primene oblasti procesa u operacijama zaštite.
9. Kontinualna reprezentacija SSE CMM modela podrazumeva:
   a. progresivno, inkrementalno/inovativno poboljšanje svih OP na sledeći viši ML
   b. progresivno, inkrementalno/inovativno poboljšanje individualnih OP na viši CL
   c. progresivno, inkrementalno/inovativno poboljšanje individualnih OP na bilo koji ciljni viši ML
   d. progresivno, inkrementalno/inovativno poboljšanje više ili svih OP sa jednog na bilo koji ciljni viši CL.
10. Fazna reprezentacija SSE CMM modela podrazumeva:
    a. progresivno, inkrementalno/inovativno poboljšanje individualnih OP na bilo koji ciljni viši ML
    b. progresivno, inkrementalno/inovativno poboljšanje svih OP na sledeći viši ML
    c. progresivno, inkrementalno/inovativno poboljšanje individualnih OP na viši CL
    d. progresivno, inkrementalno/inovativno poboljšanje više ili svih OP na bilo koji CL.
11. Glavni atributi nivoa sazrevanja kapaciteta procesa (CL) SSE CMM modela su:
    a. ne izvršava se, izvršava se neformalno,
    b. ne prikazuje se, inicijalni
    c. ponovljiv, planiran i praćen, dobro definisan,
    d. kvantitativno upravljan, kontinualno poboljšavan.
12. Glavni atributi nivoa zrelosti procesa (ML) SSE CMM modela su:
    a. ne izvršava se, izvršava se neformalno,
    b. ne prikazuje se, inicijalni
    c. ponovljiv, planiran i praćen, dobro definisan,
    d. kvantitativno upravljan, kontinualno poboljšavan.
13. Oblast primene SSE CMM obuhvata sledeće kategorije oblasti procesa (OP):
    a. SSE, organizacione i za upravljanje procesima
    b. inženjerske, za upravljanje procesima, za upravljanje projektima

c. projektne, organizacione i SSE
d. projektne, organizacione, za proizvodnju.

14. Svaka oblast procesa SSE CMM ima sledeće komponente u svojoj strukturi:
    a. zajedničke karakteristike
    b. specifične prakse
    c. bazične prakse
    d. generičke prakse.
15. Bazična praksa (BP):
    a. mora se izvršiti u implementiranom procesu (OP)
    b. evoluira kvalitet izvršavanja generičkih praksi
    c. predstavljaju izvorne, opšte radnje čije se izvršavanje zahteva u svim *OP*
    d. specifična je za svaku OP
    e. opisuje se u modelu sa rednim brojem i primerom proizvoda rada i napomenom
    f. grupiše se u zajedničke karakteristike raspoređene na pet nivoa.
16. Generička praksa (GP):
    a. opisuje se u modelu sa rednim brojem i primerom proizvoda rada i napomenom
    b. evoluira kvalitet izvršavanja generičkih praksi
    c. predstavljaju izvorne, opšte radnje čije se izvršavanje zahteva u svim *OP*
    d. specifična je za svaku OP
    e. grupišu se u zajedničke karakteristike raspoređene na pet nivoa kapaciteta
    f. logične oblasti opštih aspekata procesa.
17. Opšta karakteristike (CF):
    a. opisuje se u modelu sa rednim brojem i primerom proizvoda rada i napomenom
    b. evoluira kvalitet izvršavanja generičkih praksi
    c. predstavljaju izvorne, opšte radnje čije se izvršavanje zahteva u svim *OP*
    d. grupiše generičke prakse na pet nivoa kapaciteta
    e. logične oblasti opštih aspekata procesa.
18. Implementacija SSE CMM nivoa zrelosti SSE procesa:
    a. vrši se proizvoljno i po želji korisnika na bilo koji nivo kapaciteta/zrelosti
    b. vrši se progresivno sa jednog na sledeći viši nivo kapaciteta/zrelosti
    c. omogućava preskakanje nivoa kapaciteta/zrelosti
    d. ne dozvoljava preskakanje nivoa kapaciteta/zrelosti.
19. SSE CMM model za razvoj optimalnog programa zaštite uključuje sledeće glavne faze:
    a. identifikovanje atributa „zrelosti" procesa za procenu rizika
    b. merenje zrelosti i progresa sazrevanja procesa za razvoj politike zaštite
    c. identifikovanje atributa i merenje zrelosti procesa za razvoj programa zaštite
    d. realizacija programa obuke zaštite.
20. Tipične primene SSE CMM modela su:
    a. profilisanje procesa organizacija u zaštiti
    b. obezbeđivanje tima za menadžment bezbednosnog incidenta
    c. metrika sazrevanja kapaciteta procesa za menadžment rizika
    d. profilisanje kompetencija snabdevača proizvoda zaštite
    e. razvoj politike zaštite.



11. METOD EVALUACIJE I POBOLJŠANJA PROCESA ZAŠTITE

Po završetku ovog poglavlja studenti će razumeti:

- ☑ Ciljeve, tipove, metode i karakteristike evaluacije
- ☑ Strukturu i parametre SSAM metoda evaluacije procesa zaštite
- ☑ Faze procesa SSAM metoda evaluacije na bazi SSE CMM referentnog modela
- ☑ Uloge i odgovornosti učesnika SSAM procesa evaluacije
- ☑ Kriterijume za ocenu nivoa CL/ML, rezultate i načine SSAM izveštavanja
- ☑ Verifikaciju SSAM metoda evaluacije kroz studiju slučaja

11.1. UVOD

Formalnu metodologiju za evaluaciju proizvoda i sistema zaštite obezbeđuje standard *ISO 15408* (*CC*). *Cilj evaluacije* proizvoda i sistema zaštite prema *CC* standardu je da se pokaže da proizvodi i sistemi zaštite ispunjavaju specifične funkcionalne i bezbednosne zahteve pod specifičnim uslovima. Rezultati evaluacije zasnivaju se na specifičnim dokazima bezbednosne garancije (*EAL*). Evaluacija proizvoda i sistema zaštite na bazi CC standarda može se svesti na merenje poverenja koje indicira koliko dobro sistem zaštite ispunjava određene bezbednosne ciljeve. Međutim, kako se povećava kompleksnost IKT sistema, sve je teže obuhvatiti sve bezbednosne ciljeve i postaje sve izvesnije da je perfektan sistem zaštite nedostižan za projektante, evaluatore i korisnike u praksi zaštite [10].

Za evaluaciju i poboljšanje procesa organizacije postoje brojni metodi, od kojih modeli sazrevanja procesa zaslužuju najveću pažnju. Metod evaluacije zrelosti procesa zaštite — SSAM (*System Security Appraisal Method*), specifično razvijen za evaluaciju na bazi SSE CMM referentnog modela, obezbeđuje evaluaciju kapaciteta i zrelosti SSE procesa organizacije. Međutim, sam SSSE CMM model sadrži metodologiju za evaluaciju i poboljšanje procesa zaštite. SSAM metod je primarno namenjen za *nezavisnu* TTP evaluaciju, ali sadrži uputstvo i za *samo-evaluaciju* i samo-poboljšavanje procesa i bolje razumevanje implementacije praksi, razvoja kapaciteta, institucionalizacije i poboljšanja procesa zaštite.

11.2 CILJEVI I IZLAZNI REZULTATI EVALUACIJE

Svaka evaluacija procesa organizacije ima najmanje dva cilja:

1. efikasno sakupiti precizne podatke uz minimalnu destrukciju rada i
2. pomoći u identifikaciji i određivanju prioriteta procesa za poboljšavanje.

Ovi ciljevi mogu se dostići na brojne načine i sa različitim stepenom troškova i tačnosti. Većina metoda evaluacije ima dve glavne kategorije izlaznih rezultata:

1. *nalaze* o slabostima i snazi organizacije i
2. *preporuke* za akcioni plan poboljšanja procesa.

Nalazi obezbeđuju preciznu sliku o procesima, koristeći neki referentni model procesa (npr. CMM) kao okvir za evaluaciju. *Preporuke* obezbeđuju uputstvo za poboljšanje tekućeg stanja procesa organizacije, okvir i katalizator za akcije i angažovanost i podršku organizacije; definišu vlasništvo nad rezultatima evaluacije itd. Najpoznatiji metodi evaluacije na bazi CMM modela su SSAM na bazi SSE CMM i SCAMPI metod evaluacije na bazi CMMI modela integrisanih procesa i njihove varijacije [100]. U izboru metoda evaluacije, sam proces evaluacije zahteva razmatranje najmanje tri faktora: *tačnost, troškove i stepen destrukcije* normalnog poslovanja organizacije. U tabeli 11.1 data je uporedna analiza glavnih atributa nekih metoda evaluacije [97].

Tabela 11.1 *Uporedna analiza atributa metoda evaluacije*

Tip	Tačnost	Troškovi	Destrukcija
Samoevaluacija	niska	niska	niska
Asistirana (mentorisana) samoevaluacija	prilična	niska	niska
Privremeno profilisanje (SCAMPI B)	prilična	niska	niska
Mini-evaluacija	umerena	umerena	umerena
CBA-IPI[SM]	visoka	visoka	visoka
SCE[SM]	visoka	visoka	visoka
SCAMPI[SM]	visoka	visoka	visoka

[SM] – zaštitni znak *Carnegie Mellon University*

Izvođenje procesa evaluacije zahteva određenu pripremu, obuku i logističku podršku. Svaka evaluacija treba da pokriva životni ciklus projekta, a može da varira po dubini detalja, zavisno od tipa evaluacije [10]. Tim za evaluaciju (TE) je kritični deo svakog procesa evaluacije. Veličina i kvalifikacije članova TE, mogu uticati na poverenje sponzora u rezultate evaluacije. Za postizanje ciljeva evaluacije i realizaciju plana evaluacije odgovoran je *vodeći evaluator* (evaluator 1).

11.3 METOD EVALUACIJE SAZREVANJA PROCESA ZAŠTITE

Metod evaluacije sazrevanja procesa zaštite — *SSAM v.2.0* koristi *SSE CMM v.3.0* model sazrevanja procesa za evaluaciju nivoa SSE kapaciteta i zrelosti procesa zaštite organizacije. Metod SSAM evaluacije može se koristiti za *evaluaciju procesa* organizacije koja *razvija proizvode zaštite, ili obezbeđuje servise zaštite, ili integriše i administrira sisteme zaštite ili razvija kompetencije specijalista zaštite*. SSAM metod evaluacije obezbeđuje osnovne, tekuće indikatore izvršavanja aktuelnih BP SSE CMM modela. Posle evaluacije, organizacija može koristiti SSAM metod *poboljšanja procesa* — samo-poboljšanjem ili angažovanjem akreditovane TTP organizacije [100].

SSAM evaluacija je efektivan alat za selekciju snabdevača proizvoda i usluga, obezbeđujući komparativnu procenu kapaciteta potencijalnih snabdevača i informacije za menadžment rizika. Sa dobrom argumentacijom razloga, evaluator može dobiti podršku *sponzora* (inicijatora evaluacije) i potrebne resurse za realizaciju procesa evaluacije. Ubedljivi razlozi, saopšteni kroz ciljeve evaluacije, mogu biti: *praktično upoznavanje sa OP i CL SSE CMM, definisan obim i plan evaluacije, prihvatljivo trajanje procesa evaluacije, prihvatljiv metod izveštavanja rezultata, značaj projekata koje treba uključiti u proces evaluacije i ciljevi koje postavi sponzor evaluacije*. Na primer, ako je primarni cilj evaluacije da demonstrira kapacitete organizacije za obezbeđivanje argumenata za *garantovanu bezbednost*, proces evaluacija treba da usmeri veću pažnju na kvalitet i kompletnost (izvršavanje GP) nego na poboljšanje ukupnih procesa. U slučaju izbora ponuđača proizvoda i usluga primarni cilj je određivanje ukupnih kapaciteta. Sekundarni cilj evaluacije uglavnom je identifikacija snage i slabosti SE kapaciteta organizacije, za upravljanje rizikom programa zaštite. Ciljevi evaluacije treba da budu eksplicitno saopšteni u zahtevu za ponudu — RFP, kojeg sponzor evaluacije dostavlja organizaciji evaluatora [100].

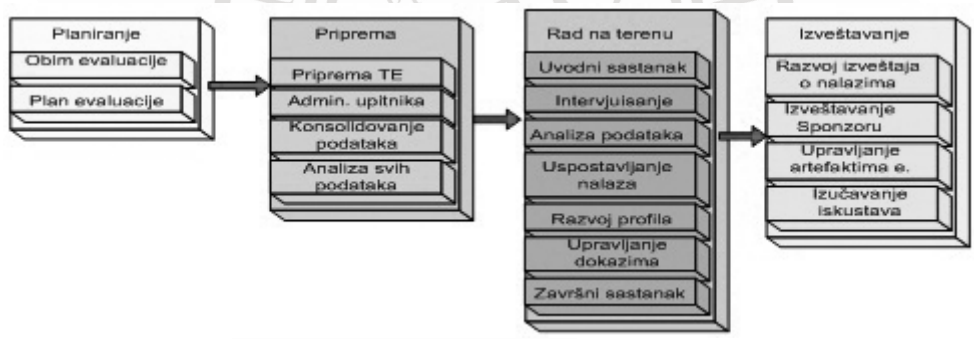
1. Zrelost kapaciteta prema SSE CMM, može se pokazati na više načina zavisno od RFP:
2. Za procenu SSE kapaciteta RFP zahtevi mogu biti uopšteni, zahtevajući da evaluator jednostavno komentariše svoje kapacitete za SSAM profilisanje, bez eksplicitnog zahteva za formalnom SSAM evaluacijom.
3. Ako sponzor želi skraćenu evaluaciju i da samo stekne uvid u zrelost kapaciteta evaluatora, u RFP se može zahtevati odgovor na SSE CMM *Upitnik* ili samoevaluacija prema datom SSE CMM profilu i dostavljanje rezultata na uvid u ponudi za evaluaciju.
4. RFP može zahtevati da nezavisan *tim za evaluaciju* (*TE*) izvrši evaluaciju kapaciteta izvođača evaluacije, s tim da organizacija snosi troškove barem rada TE.
5. RFP može uključivati i zahtev da evaluirana organizacija obezbedi u predlogu *ugovora za evaluaciju* svaki dokaz koji bi organizacija za evaluaciju mogla tražiti u toku izvođenja procesa evaluacije i što je moguće više informacija, pre faze evaluacije na terenu, što povećava tačnost i efikasnost rezultata procesa evaluacije.

Proces SSAM metoda evaluacije obuhvata četiri faze (tabela 11.2):

Tabela 11.2 *Faze procesa SSAM metoda evaluacije*

Faza	Opis
1. Planiranje	Uspostavlja okvir u kojem će se izvoditi evaluacija procesa, kao i logističku pripremu za fazu evaluacije na terenu.
2. Pripreme	Priprema TE za evaluaciju na terenu, preliminarno sakupljanje, analiza, konsolidovanje i administracija podataka iz *upitnika.*
3. Rad na trenu	Istraživanje rezultata preliminarne analize podataka i uključivanje korisnika iz prakse evaluiranog entiteta u prikupljanje podataka i validaciju procesa putem *intervjua*.
4. Izveštavanje	Tim za evaluaciju vrši konačnu analizu svih prikupljenih podataka u toku prethodne tri faze i predstavlja svoje nalaze sponzoru.

Proces SSAM evaluacije detaljno je opisan u dokumentu [100] i koristi se kao *radni dokument.* Grafički model procesa SSAM metoda evaluacije sa glavnim koracima u svakoj fazi, prikazan je na slici 11.1.



Slika 11.1 Model faza i koraka procesa SSAM evaluacije

11.3.1 Uloge i odgovornosti učesnika SSAM procesa evaluacije

Učesnici SSAM procesa grupišu se u tri tipa organizacija uključenih u proces evaluacije: *sponzor*, *evaluator* i *evaluand* (evaluirana organizacija). U tabeli 11.3. prikazane su zahtevane kvalifikacije i tipične odgovornosti primarnih učesnika u procesu evaluacije, od kojih neki imaju višestruke funkcije.

Tabela 11.3 *Kvalifikacije i odgovornosti primarnih učesnika u procesu evaluacije*

Organizacija	Opis	Primarna odgovornost	Kvalifikacije
Sponzor	Inicira zahteve za proces evaluacije	Definisanje namene i ciljeva evaluacije i poboljšanja procesa Posreduje između evaluatora i koordinatora na lokaciji	Sposobnost da podrži aktivnosti evaluacije
Tim za evaluaciju (TE)	Sva lica evaluatora, koja učestvuju u aktivnostima evaluacije	Učestvovanje u procesu evaluacije i poboljšanja procesa	Specifikovana u *Uputstvu za evaluaciju*
Evaluator 1 (*Facilitators*)	Lider tima za evaluaciju	Obezbeđivanje korektnog izvršavanja evaluacije Koordinacija aktivnosti sa sponzorom Razvoj i održavanje plana evaluacije	Specifikovana u *Uputstvu za evaluaciju*
Rukovalac dokaza (evaluator 2)	Održava lanac čuvanja dokaza	Podnosi zahteve, bezbedno čuva i odlaže dokaze koje na zahtev evaluatora daje evaluirana organizacija	Velika veština upravljanja konfiguracijom
Članovi TE sa pravom glasa	Donosioci odluka u timu za evaluaciju	Identifikovanje i analiza podataka i dokaza Razvoj i definisanje nalaza i izveštaja o profilu nivoa procesa	Specifikovana u *Uputstvu za evaluaciju*
Posmatrači	Članovi tima za evaluaciju bez prava glasa	Pomažu članovima TE sa pravom glasa i evaluatorima Prikupljaju iskustva iz SSAM evaluacije	Poznavanje SSE CMM modela i SSAM metoda evaluacije i poboljšanja procesa zaštite
Korisnici procesa na terenu (praktičari)	Svi članovi evaluanda uključeni u proces evaluacije	Prisustvovanje brifinzima Odgovaranje na pitanja u toku intervjua	Zaposleni u evaluiranoj organizaciji
Koordinator evaluacije na terenu	Lice za kontakte iz evaluirane organizacije	Koordinira aktivnosti evaluirane organizacije u toku procesa evaluacije	Poznavanje organizacione strukture, rada, politike i procedura evaluanda
Menadžment	Donosioci odluka na najvišem nivou evaluanda	Davanje i izražavanje podrške za evaluaciju	Sposobnost da angažuje učešće zaposlenih u evaluaciji
PR menadžmenta	Poslove portparola menadžmenta	Obraća se korisnicima na terenu na sastancima	Poznavanje izvršnih poslova evaluanda
Rukovodstvo evaluiranog projekta	Upravlja projektnim aktivnostima i članovima projektnog tima	Popunjavanje SSAM *upitnika* Prikuplja i daje odgovore na pitanja iz *intervjua*	Potvrđeno iskustvo iz izvođenja SSE aktivnosti na dokazanom projektu
Praktičari evaluiranog procesa	Član projektnog tima evaluiranog projekta	Odgovara na pitanja iz *intervjua*	Direktno ili indirektno iskustvo sa nekog relevantnog projekta zaštite

Tipični zahtevi za radno angažovanje u SSAM procesu evaluacije i poboljšanju procesa zaštite organizacije na 3 — 4 projekta prikazani su u tabeli 11.4.

Tabela 11.4 *Zahtevi za radno angažovanje u SSAM procesu evaluacije*

Uloga u evaluaciji	Preporučen broj ljudi	Angažovanje (čovek/sati)	Ukupno angažovanje (čovek/sati)
Sponzor	1	80	80
Evaluatori	2	160	320
Članovi tima sa pravom glasa	4	80	320
Posmatrač	1	80	80
Koordinator na terenu	1	100	100
Rukovodstvo projekta	1 po projektu	10	30
Praktičari projekta	6 po projektu	4	72
Ukupno	**30**	**nije primenljivo**	**1002**

11.3.2 Tipovi SSAM procesa evaluacije

Nezavisna TTP evaluacija je primarna namena SSAM metoda koji sadrži uputstva i za samoevaluaciju. Evaluaciju obavlja akreditovani evaluator, a ciljevi evaluacije variraju u skladu sa potrebama *inicijatora evaluacije ili sponzora*. Sponzor je organizacija ili pojedinac koji zahteva bezbedni proizvodi, sistemi ili servis i inicira proces evaluacije. Odgovoran je za uspostavljanje parametara i ciljeva evaluacije, specifikovanje zahteva i obezbeđivanje podrške procesu evaluacije. Mnoge aktivnosti sponzor može delegirati drugim učesnicima, pre svega SSAM evaluatoru, a TE može mu pomagati u postavljanju zahteva, ciljeva i specifikovanju RFP zahteva.

Ciljevi evaluacije utiču na izbor projekata za evaluaciju i izveštaje rezultata evaluacije. Razlozi za izbor TTP evaluacije su brojni, a uključuju: *kompetencije organizacije za ispunjavanje ugovornih obaveza, razumevanja i ispunjavanja očekivanja klijenata, upravljanja rizikom programa evaluacije* itd.

Samoevaluacija (*asistirana*, *monitorisana*) obezbeđuje organizaciji uvid u sopstvene kapacitete za SSE praksu, značajno smanjuje angažovanje resursa i destrukciju poslova organizacije, u odnosu na TTP evaluaciju. Tipični ciljevi za samoevaluaciju sistema zaštite mogu biti:

- razumeti sva pitanja koja se odnose na domen zaštite,
- razumeti razvoj i implementaciju nove prakse zaštite u organizaciji,
- odrediti ukupne kapacitete zaštite organizacije i
- odrediti progres aktivnosti za poboljšanje procesa.

U proceni relevantnosti SSE CMM modela za organizaciju i projekte koje treba evaluirati prema postavljenim ciljevima za evaluaciju, sponzor treba da razmatra brojna pitanja:

- Da li organizacija primenjuje SSE prakse u razvoju i praksi zaštite?
- Da li organizacija želi da poboljša svoje SSE prakse i poveća bezbednost?
- Da li organizacija želi da uspostavi svoju kompetentnost u izabranoj OP?
- Koji projekti najbolje pokazuju SSE OP koje treba evaluirati?

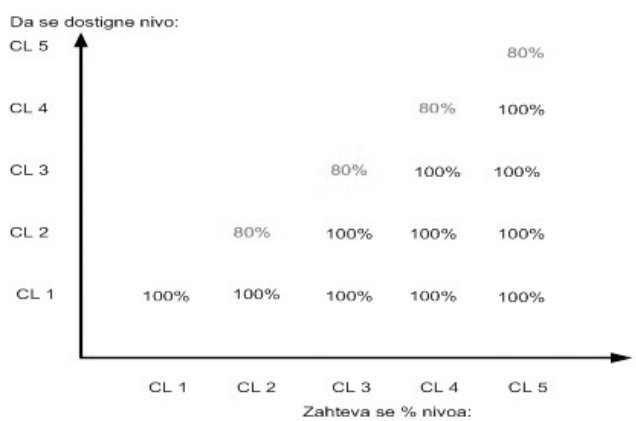
Sponzor, takođe, treba da shvati da svaka SSAM evaluacija neće propisati dobre procese ili naučiti organizaciju kako da poboljša kapacitete za izvršavanje specifičnih procesa, niti da je SSAM evaluacija zamena za evaluaciju proizvoda ili sertifikaciju sistema. Međutim, *SSAM evaluacija može obezbediti važan uvid i uputstvo za budući proces poboljšanja i može izgraditi dodatne argumente za garantovanu bezbednost*. Pre pokretanja zahteva za evaluaciju (RFP) sponzor treba da proceni vrednost potencijalne dobiti od evaluacije, prema njenim troškovima.

11.3.3 Promenljivi parametri procesa evaluacije

Postoji nekoliko komponenti procesa evaluacije koji se mogu prilagođavati u toku faze planiranja, a prema zahtevima sponzora:

OP: sponzor može zahtevati isključivanje nekih OP modela ili prilagođavanje nekih aspekata OP određenim potrebama. Takođe, može ponuditi objektivni dokaz proizvoda rada prakse, koji nije naveden u modelu i prilagoditi terminologiju kulturi rada organizacije.

Nivo CL: sponzor može identifikovati ciljne ili željene nivoe kapaciteta za OP uključene u evaluaciju ili izabrati predefinisane željene profile [37]. U evaluaciji namenjenoj za izbor snabdevača opreme, u RFP se može specifikovati minimalni CL za OP. Cilj može biti jedan nivo za sve OP (ML), ili specifičan nivo za svaku OP (CL). SSAM definiše zahtev za postizanje 1. nivoa CL kroz **100%** izvršavanje svih BP. Svi drugi CL smatraju se postignutim, ako je **100%** dostignut prethodni CL, a **80%** tekući CL. *Kriterijumi za dostizanja CL* definiše SSAM metod evaluacije (slika 11.2), ali sponzor može tražiti da redefiniše kriterijume na bazi značaja specifičnog CL.



Slika 11.2 Kriterijumi za dostizanje nivoa kapaciteta OP SSE CMM modela

Upitnik: upitnik, kao instrument evaluacije, može se prilagođavati u smislu donošenja odluke za eliminisanje specifičnih OP iz razmatranja. Uzorak *upitnika* prikazan je u **Prilogu 11.1.**

Projekat za evaluaciju: Sponzor može specifikovati određene projekte ili tipove projekata za evaluaciju. Na primer, poželjno je u proces evaluacije uključiti projekte vrlo slične po tehnologiji, veličini i obimu ili one za koje treba izvršiti izbor snabdevača. Treba razmatrati i lokacije evaluirane organizacije (radi troškova putovanja TE), a i ciljevi evaluacije mogu uticati na izbor projekata. Neki kriterijumi za izbor projekata za evaluaciju dati su u tabeli 11.5.

Tabela 11.5 *Neki kriterijumi za izbor projekata za evaluaciju*

Cilj procesa evaluacije	Tip projekta
Razumeti sva pitanja u domenu zaštite.	Izabrati projekte unutar domena, koji je fokusiran na oblast zaštite.
Razumeti implementaciju nove prakse u organizaciji.	Izabrati novi projekat koji počinje sa implementacijom nove prakse.
Odrediti ukupne kapacitete organizacije ili snabdevača.	Izabrati projekat koji je reprezentativan za kapacitete organizacije ili snabdevača.
Odrediti progres aktivnosti na poboljšavanju procesa.	Izabrati pilot projekat za poboljšanje procesa.

Izabrane projekte za evaluaciju treba da vode pojedinci ili projektni tim, odgovoran za planiranje resursa, alokaciju, nadzor, kvalitet, kvantitet i bezbednost proizvoda/ servisa projekta. Projekti koje izvršavaju integrisani timovi za razvoj proizvoda, takođe, su podložni evaluaciji. Lokaciju za upitnike i intervjue po različitim projektima treba planirati racionalno, po mogućnosti na istoj lokaciji, zbog troškova. Za pripremu aktivnosti evaluacije na terenu, koristi se *kontrolna lista* kao *pomoćni radni materijal* evaluatora (**Prilogu 11.2).**

Intervju: Za intervjuisanje sponzor može odrediti lica prema funkciji, nadležnosti, nivou odgovornosti ili drugoj kvalifikaciji. Rukovodstvo projekta mora imati jednu kontakt osobu za sve informacije i sadržaje koji se odnose na SSE funkcije projekata. Ako to nije moguće, sponzor može ovlastiti širu grupu praktičara projekta, koji mogu biti intervjuisani, na primer, lica iz grupe za *upitnike*, na bazi pokazanog znanja i iskustva u davanju odgovora na *upitnik*.

Metod izveštavanja: Sponzor može u *planu evaluacije* specifikovati kako i kome u evaluiranoj organizaciji saopštiti rezultate evaluacije — od nesaopštavanja rezultata, preko uopštene prezentacije rezultata svim zaposlenim, pa do detaljno pisanog izveštaja o rezultatima evaluacije.

Dokazi: RFP treba da uključi sve zahteve za dokaze (idealno u formi matrice dokaza) i odgovarajuće prilagođen *SSE CMM upitnik* za korišćenje u procesu evaluaciji. Ove informacije evaluirana organizacija može koristiti kao pomoć u izboru projekata i lica za relevantne učesnike u TE i da počne sakupljati datoteku objektivnih dokaza za TE. RFP treba da uključi svaku formu dokaza koja se modelom dopušta i treba jasno identifikovati *prihvatljiv „tip" dokaza*, ako je evaluiranoj organizaciji dopušteno da izabere specifične

primere. RFP treba da obuhvati i pitanja odlaganja dokaza, indicirajući, na primer, da li dokaz treba vratiti evaluiranoj organizaciji na zadržavanje i čuvanje posle faze rada na terenu ili ostaju kod TE. RFP treba da navede ko i kada može uništiti neki dokaz ili radni papir iz procesa evaluacije. Konstrukcija *radne tabela za praćenje podataka* (DTS) i kriterijumi za registrovanje odgovora na *upitnik* i *intervjue,* kao i za preliminarno i konačno rangiranje, dati su u **Prilogu 11.3.**

Odnosi sa koordinatorom rada na terenu: koordinator rada na terenu je predstavnik evaluanda i saradnik TE u toku evaluacije na terenu. Sponzor određuje koordinatora koji ima neophodan autoritet za neometan razvoj procesa evaluacije. Koordinator je odgovoran za logističku podršku specifikovanu u RFP: obezbeđivanje prostora za rad TE i pristupa objektima, ljudima i dokazima i snabdevanje TE potrebnim materijalnim resursima tokom procesa evaluacije. Uzorci ostalih radnih dokumenata za praćenje dokaza: *formular za zahtevanje dokaza*, *tabela za praćenje zahteva za dokaze*, *tabela za praćenje korišćenja dokaza* i *tabela za praćenje odlaganja dokaza* prikazani su u **Prilogu 11.4.**

11.3.4 Rezultati i izveštavanje SSAM evaluacije

Primarni rezultati SSAM evaluacije procesa su *glavni nalazi* koje evaluator u ime TE referiše i konačno diskutuje na sastanku sa sponzorom i *izveštaj o evaluaciji*. Sastanak za utvrđivanje nalaza uključuje prezentaciju *profila CL/ML* procesa i listu ključnih nalaza procesa/praksi za poboljšanje. *Profil* indicira nivoe CL/ML svake pojedinačne/grupe OP-a organizacije. Glavni nalazi obuhvataju *snagu* i *slabosti* procesa i praksi za evaluirane organizacije. Glavni nalazi se prezentuju sponzoru, ali mogu i celoj organizaciji, ako to sponzor zahteva. Izveštaj o evaluaciji i poboljšanju piše se samo sponzoru i uključuje *dodatne detalje o svakom nalazu, svaki zahtev sponzora za izveštavanje i implikacije nalaza na zahteve sponzora*.

Na kraju procesa evaluacije u skladu sa modelom i metodom, vodeći evaluator može da dostavi referencirane eventualne probleme i iskustava, grupi za razvoj SEI instituta, prema formularu za *izveštaj evaluatora,* datom u modelu [101]. **U Prilogu 11.5** prikazani su ostali važni uzorci modela: *scenariji za održavanje uvodnog i završnog sastanka, prezentaciju profila nivoa rangiranja OP i glavnih nalaza sponzoru i prezentacija konačnog izveštaja, primer direktnih (tipični proizvodi rada) i indirektnih artefakta SSAM evaluacije – SSAM PIID dokument, koji kompletiraju proces SSAM evaluacije i radni materijal.*

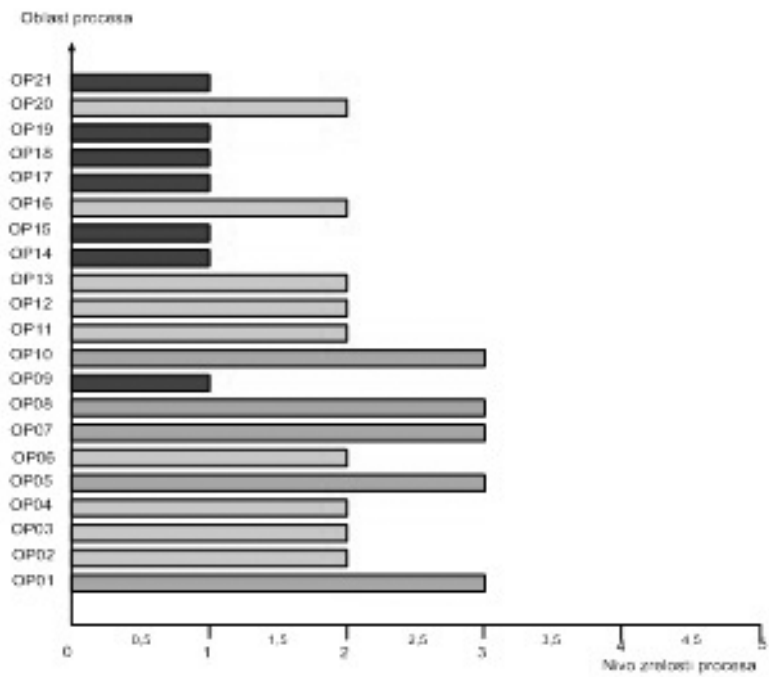
11.4 STUDIJA SLUČAJA: *Asistirana SSAM evaluacija „CAXY"*

11.4.1 Izbor željenog profila procesa

U cilju evaluacije i progresivnog poboljšanja tekućih procesa, evaluand bira željeni profil *procesa najbolje prakse* kao referentni ili sam definiše *željeni profil OP*-a u skladu sa raspoloživim resursima, poslovnim ciljevima i prioritetima, ako referentni model nije dostupan [10].

Sertifikaciono telo (CA) PKI sistema servisira matematičke parove privatnog i javnog ključa sa pridruženim entitetima u *infrastrukturi javnog ključa (PKI)*. Za razliku od servisne organizacije, CA servisira širu zajednicu korisnika, autentifikuje digitalne sertifikate i onda opslužuje klijente. U toku su diskusije o adekvatnoj politici i praksi koje CA treba da sprovode ili da su obavezne za tipična CA. Međutim, zajedničko za sve CA je da sačuva i održava bezbednost i poverenje korisnika. Model SSE CMM pruža prednost zato što ne formuliše poseban proces kojeg treba slediti, prepuštajući to samoj organizaciji, ali *obavezuje* da se zrelost korišćenog procesa upoređuje sa odgovarajućim procesom *najbolje prakse zaštite* iz modela, čak i ako se realni proces razlikuje od njega. Ovaj aspekt SSE CMM-a veoma je važan, pošto mreža CA raste i povećava se nivo međusertifikacija.

Glavni princip za dovođenja organizacije na CL3 je dovođenje SSE procesa na CL3, projektnih na CL2, a organizacionih OP na CL1 nivo zrelosti. Planiranje, nadzor i praćenje projektnih OP na nivou projekta obezbeđuje kontrolu kvaliteta, upravljanje konfiguracijom, upravljanje rizikom i planiranje, što je neophodno za obezbeđivanje podataka za poboljšanje organizacionih OP. Izvršavanjem organizacionih OP dobiju se neophodni resursi za SSE OP za poboljšanje na CL3. Ovi resursi uključuju standardne SE procese organizacije za podršku i stečena SSE znanja i veštine. Referentni profil OP standardnog CA je prikazan na slici 11.3 (videti **Prilog 10.3**).



Slika 11.3 Referentni profil OP standardnog CA

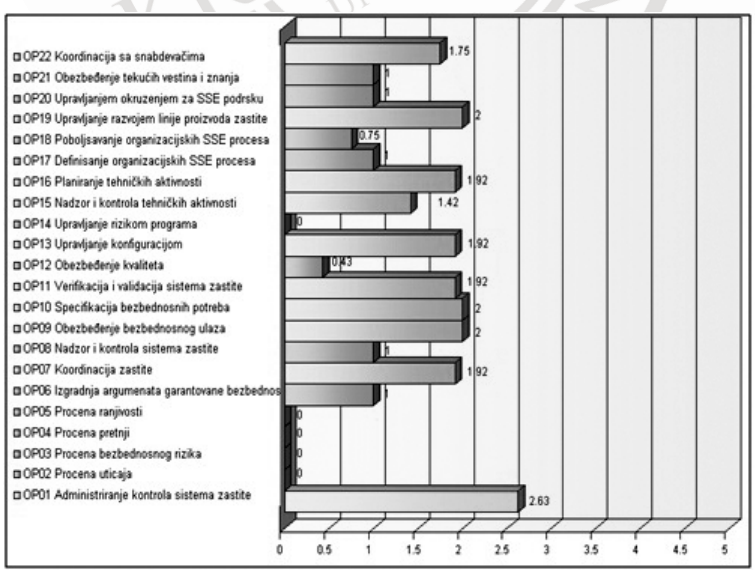
Organizacija koja unapređuje program rada treba da prema značaju odredi prioritete izvršavanja OP-a u odnosu na postavljene ciljeve i da nastoji da najpre poboljša kapacitete u tim OP. Za CA funkcionalno su najznačajnije OP01, OP05, OP07, OP08 i OP10 (*za administraciju zaštite, procenu ranjivosti, koordinaciju zaštite, nadzor i kontrolu zaštite i specifikaciju bezbednosnih potreba*) i samim tim treba da budu na najvišem nivou zrelosti kapaciteta (CL3). Ove OP, CA organizacija regularno koristi, pa moraju biti dobro dokumentovane i definisane. Grupe OP (OP02, OP03, OP04, OP06 i OP11; OP12 i OP13; OP16 i OP20) CA organizacija koristi *periodično*, pa je dovoljno da budu dobro planirane i kontrolisane (na CL2).

Preostale OP (OP09, OP15, OP17, OP18, OP19 i OP21), koje se ređe koriste i na višim CL postižu manju dobit za organizaciju, svrstane su na najniži nivo zrelosti za ovaj profil (CL1). Izvršavanje ovih OP, kada je potrebno - važno je za ovaj profil [34].

11.4.2 Analiza rezultata SSAM evaluacije tekućih procesa CAXY

U procesu SSAM evaluacije CAXY , na bazi referentno SSE CMM modela procesa zaštite, sakupljeni su i konsolidovani dokazi sa tri projekata, primenom sledećih tehnika i alata:

- upitnika i intervjua rukovodstva (LP1, LP2, LP3) i praktičara (PP1, PP2, PP3),
- analize pokrivanja, koraborativnosti i kompletnosti sakupljenih dokaza,
- generisanje DTS (Data Tracking Sheet) tabele za evidentiranje svih dokaza,
- otklanjanja nekonzistentnosti,
- razjašnjavanje poslednjih pitanja kroz naknadni intervju,
- transformacije podataka o dokazima u binarnu formu (1, 0, ?) u tabeli DTS (tabela 11.6),
- automatsko generisanje CL profila tekućih OP tabelom DTS (slika 11.4).



Slika 11.4 Profil nivoa zrelosti kapaciteta tekućih procesa CAXY

Tabela DTS (tabeli 11.6) sadrži atribute za *odgovore na upitnik* u fazi pripreme (O1Q do O3Q) sa ishodom i na lokaciji (L1Q do L3Q) sa ishodom 0 — *negativno* ili 1 – *pozitivno* i ? — *ne znam*, zatim, *odgovore na intervijue* za najmanje tri projekta (P1 do P3) za procenu institucionalizacije OP, sa ishodima *0* — *negativno* i referentnim brojem dokaza ili evidencije dokaza. Posle *koraborativne* verifikacije svih dokaza, članovi TE donose *odluku sa konsenzusom* da je OP implementirana ili ne, što DTS prikazuje u procentima, prema kriterijumu za CL (slika 11.2).

Tabela 11.6 *Atributi DTS tabele za skupljanje i praćenje dokaza*

OP (BP, GP)	Odgovori na upitnik								Odgovori iz intervjua																						Privatljivost dokaza	Konačno rangiranje
	Pripre-mna faza				Rad na terenu				Projekt 1								Projekt 2								Projekt 3								
	O1Q	O2Q	O3Q		L1Q	L2Q	L3Q		L1I	P1.1	P1.2	P1.3	P1.4	P1.5	P1.6		L2I	P2.1	P2.2	P2.3	P2.4	P2.5	P2.6		L3I	P3.1	P3.2	P3.3	P3.4	P3.5	P3.6		
	(0 / 1)				(0 / 1 / ?)				(0 ili referentni broj dokaza (evidencije))																						0/ 1	
OP 01																															1	
BP1	1			33.3%				0.00%																							1	100.00%
1.1	1																														1	
1.2	1																														1	
1.3	1																														1	
1.4	1																														1	
CL2 GP 1...																																
CL3 GP 1...																																
CL4 GP 1...																																
CL5 GP 1...																																
OP 02																															0	

11.4.2.1 Analiza i konsolidacija dokaza

Profil nivoa zrelosti kapaciteta (CL) tekućih procesa evaluiranog CAXY u velikoj meri se podudara sa glavnim nalazima snage i slabosti organizacije, otkrivenim u evaluiranim projektima.

*Od inženjerskih (SSE) OP***,** u *OP01* CAXY dostiže najviši nivo zrelosti kapaciteta (CL2), što je rezultat poslovnih ciljeva i ugovorom preuzetog održavanja i administracije CA modula i PKI sistema implementiranih u evaluiranim projektima (P1, P2, P3). *CAXY*, takođe, administrira i sopstveni CA i ima iskustvo u uspostavljanja i održavanju više CA sa arhitekturom na jednom i tri nivoa u različitim organizacijama. Proces administracije dobro je planiran i kontrolisan i dokumentovan kroz *Microsoft*-ove (MS) standardne politike sertifikacije (CP) i *tehničke* procedure, koje su prilagođene sa brojnim aplikacijama i konkretnim rešenjima razvijenim u CAXY za različite projekte i zahteve klijenata. Ova OP ima tendenciju da brzo postane *dobro definisan* i standardan proces organizacije — *institucionalizovan na CL3* i sa solidnom metrikom, pod uslovom da se formalno opiše i definiše kao standardni proces (OP17) *CAXY-a,* u familiji standardnih procesa za *administraciju PKI sistema na bazi MS tehnologija i Windows platformi*, koja treba da uključi, pored standardnih tehničkih MS procedura, operativne i upravljačke procedure razvijene u praksi CAXY.

U OP2-OP5 CAXY menadžment i projektni timovi imaju visoku svest o potrebi razvoja sopstvene metodologije za menadžment bezbednosnog rizika, što je dokumentovano u dokumentima: *organizaciona struktura* i *planovi rada*. Međutim, ove procese CAXY koristi krajnje neformalno, po eksplicitnom zahtevu korisnika, pošto smatra da je menadžment rizika u realnom okruženju ugovorna obaveza korisnika. Pored toga, koristeći MS tehnologiju i procese najbolje prakse PKI, CAXY ceni da su svi relevantni faktori bezbednosnog rizika podrazumevano ublaženi striktnom implementacijom PKI u skladu sa MS standardnim CP i procedurama, pa nije neophodno vršiti analizu rizika u konkretnom projektu i okruženju, jer se ne očekuje otkrivanje novih značajnijih faktora rizika. CAXY nigde ne planira i formalno ne kontroliše sakupljanje argumenata za garantovanu bezbednost (*OP06*). U procesu administracije i monitoringa PKI sistema, u skladu sa MS procedurama i preuzetom ugovornom obavezom za održavanje sistema, CAXY sakuplja brojne metričke podatke i indikatore *garantovane bezbednosti*, koje, međutim, ne arhivira i ne analizira za potrebe definisanja argumenata garantovane bezbednosti, jer „ne potpisuje SLA ugovore sa klijentima". Procena TE je da CAXY ovu OP neformalno izvršava (CL1), pošto primenjuje MS tehnologiju i najbolju praksu PKI, koje *podrazumevano garantuje* nivo bezbednosti naveden u MS standardnim CP i procedurama.

Oblasti procesa OP 07, OP08, OP09 i OP10, izvršavaju se planirano i kontrolisano na CL2, što je verifikovano *koraborativnim dokazima iz više izvora* na sva tri evaluirana projekta. Brojni, uspešno i na vreme implementirani projekti PKI i CA, indirektan su dokaz da projektni timovi CAXY formalno koordiniraju rad unutar tima i sa drugim grupama i učesnicima projekata, monitorišu operativni rad PKI sistema, obezbeđuju ulazne bezbednosne parametre i definišu bezbednosne potrebe na bazi šturih korisničkih zahteva. Ocena TE je da se sve aktivnosti planiraju za svaki projekat, ali ne jednako striktno i formalno na svim projektima. Osnovni instrument planiranja, alati *MS Project menadžer* i *OneNote,* ne koristi se podjednako i sa svim potencijalnim opcijama na svakom evaluiranom projektu.

OP11 uslovno je na drugom nivou zrelosti kapaciteta (CL2), ali nije *institucionalizovana* na svim projektima CAXY-a. Projektni timovi CAXY-a planiraju i vrše laboratorijsko ispitivanje svakog potencijalnog rešenja PKI za tekući projekat. U ovom ispitivanju verifikuju se rešenja PKI u odnosu na MS standarde i procedure, a u testiranju rešenja u produkcionom okruženju (*pilot testiranje*) vrši se *validacija* implementiranog rešenja u odnosu na kvalitet PKI rešenja i korisničke zahteve. Međutim, CAXY ne planira striktno sve aktivnosti ove OP, posebno analizu i korišćenje rezultata za generisanje argumenata garantovane bezbednosti i zvaničnu sertifikaciju i akreditaciju sistema. Ocena TE je da uz malo napora za formalno dokumentovanje svih GP na CL2, CAXY može, sa tekućim, rigoroznim tehničkim testiranjem PKI rešenja u laboratorijskom (verifikacija) i produkcionom (validacija) okruženju, relativno brzo izgraditi komercijalno rentabilan proces za formalnu *sertifikaciju i akreditaciju PKI sistema*.

Projektne OP se uglavnom izvršavaju regularno, po zahtevu korisnika, ali se ovi procesi formalno slabo planiraju i nedovoljno rigorozno kontrolišu. *OP12* se izvršava sa svega 30% i to u odnosu na *kvalitet proizvoda* — tehničkog rešenja PKI, dok se procena *kvaliteta procesa* za implementaciju i održavanje ovih rešenja, uopšte ne izvršava. Uvođenjem sistema kvaliteta procesa, ovim procesom evaluacije i formalnim planiranjem aktivnosti ove OP, CAXY može dovesti ovu OP sa malo troškova i napora na CL2, odnosno, CL3. U *OP13* sve ugovorom preuzete obaveze za održavanje i administraciju implementiranih rešenja PKI sistema u drugim organizacijama, CAXY izvršava planski i kontrolisano (CL2), izuzev formalnog planiranja procesa monitoringa i praćenja metričkih indikatora statusa procesa upravljanja konfiguracijom PKI sistema (*GP2.4.1*). Izvršavanje *OP14* zanemarljivo je u radu projektnih timova CAXY, na sva tri evaluirana projekta. Bazične prakse se izvršavaju nepotpuno i neformalno. Projektanti sve faktore rizika za izvođenje projekta diskutuju i neposredno rešavaju u fazi laboratorijskog i produkcionog ispitivanja, ali ih formalno ne planiraju i ne dokumentuju. Za potrebe internog PKI sistema razvijena je *matrica faktora rizika* za izvršavanje projekta implementacije PKI sistema u CAXY, što ukazuje na postojanje potrebnih znanja i veština. *OP15* se izvršava na svim evaluiranim projektima u skladu sa ugovornim obavezama. CAXY ima razvijene kapacitete za ovu OP, ali je proces nedovoljno formalno planiran i praćen (oko 40% izvršavanja GP na CL2). Ova OP se relativno brzo i jeftino može podići na CL2 i CL3, jer se neophodni elementi za formalno definisanje i opis procesa već nalaze opisani u standardnim MS procedurama za monitoring i održavanje implementiranih tehničkih rešenja PKI sistema. *OP 16* izvršava se u velikoj meri u skladu sa planom aktivnosti, prati se i izveštava stanje procesa u toku izvođenja projekta. Nedostaje formalno praćenje statusa procesa u skladu sa planom i indikatorima stanja (*GP2.4.1*).

Od šest organizacionih OP, CAXY formalno planira i izvršava (na CL2) samo *OP19* i *OP22*. CAXY nije formalno definisala i opisala svoje tekuće procese (*OP17*), oslanjajući se na dobro definisane MS politike i tehničke procedure za implementaciju i održavanje PKI. Sa ovim procesom evaluacije i predlogom zadataka akcionih planova za poboljšanje procesa, CAXY je dobrim delom izvršila i *OP18,* pri čemu se podrazumeva da su tekući standardni procesi CAXY, u stvari, adaptirani MS procesi najbolje prakse PKI. CAXY neformalno (na CL1), bez formalnog plana i praćenja, *upravlja razvojnim okruženjem za podršku inženjerskih procesa* (*OP20). OP 22* se izvršava regularno i u velikoj meri formalno (oko 60% GP na CL2) sa svim organizacijama sa kojim CAXY ima partnerske odnose. Međutim, ne

planiraju se i ne kontrolišu indikatori izvršavanja ove OP, koji uvode metriku, potrebnu za kvantitativno praćenje na CL3 i CL4 procesa.

11.4.2.2 Analiza glavnih nalaza SSAM evaluacije tekućih procesa CAXY

U procesu SSAM evaluacije CAXY na evaluiranim projektima *P1, P2 i P3* identifikovani su *glavni nalazi*.

Glavne slabosti:

1. U *Sektoru infrastrukture i zaštite* (*de facto* odeljenju *CAXY*) jedan zaposleni pokriva više uloga u životnom ciklusu projekata. Ova činjenica bitno utiče na formalizaciju aktivnosti (*izradi plana projekta, dokumentovanju dnevnih redova značajnijih radnih sastanaka, dokumentovanje analiza izveštaja, arhiviranje i dokumentovanje rezultata analize indikatora stanja procesa* i sl.), za koju zaposleni pored kreativnog rada *nemaju vremena.* Na taj način *ova slabost je opšta prepreka za podizanje svih OP na viši nivo.*
2. *Tekući procesi* koje CAXY primenjuje u radu na tekućim projektima *nisu formalno opisani i* eksplicitno *definisani* kao *standardni procesi* organizacije. Relativno dobro su opisani procesi koji podržavaju primenjivane PKI tehnologije na nivou *tehničke dokumentacije*, u formi procedura i dijagrama, što dobro odgovara nameni – projektovanju, implementaciji, integraciji i održavanju modula PKI sistema klijenata, na bazi *MS* tehnologija i *Windows* platformi. Imovina standardnih procesa distribuirana je na više projekata i u različitim bazama i nije adekvatno dokumentovana i sistematizovana u određeni *repozitorijum imovine standardnih procesa*. Procesi se izvršavaju na određenom projektu, a za drugi projekat u drugoj organizaciji prilagođavaju se već primenjeni procesi, ali se formalno ne formira familija standardnih procesa organizacije na sistematičan način. CAXY projektni tim analizira na stručnim radnim sastancima i izvršava brojne prakse i procedure, ali ih ne dokumentuje, ili ih dokumentuje nepotpuno i neregularno — delom kroz *MS Project manager* ili opisom tehničkih procesa – samo dijagramom toka procesa i gantogramom ključnih aktivnosti ili opisom samo ključnih procedura koje zahteva MS tehnologija, sa retkim dokumentovanjem dnevnih sastanaka i izradom izveštaja o zaključcima radnih dogovora. Ovakva praksa rada je ključna prepreka za *implementaciju i institucionalizaciju generičkih praksi (GP) i podizanje kvaliteta izvršavanja svih BP i OP na viši nivo zrelosti kapaciteta.*
3. *Politika/program zaštite* na nivou organizacije, kao strategijski dokument za zaštitu, nije formalno definisana, napisana i dokumentovana. Nedostaju formalne *politike* za upravljanje brojnim komponentama zaštite, kao i za upravljanje dokumentacijom zaštite i konfiguracijom – *bekapovanjem* osnovne konfiguracije sistema zaštite (*security baseline*), ali se proces izvršava na nivou svakog projekta (*P1, P2, P3*) na bazi MS standardnih procedura. Takođe, nedostaje formalna *ISMS politika zaštite CAXY*, koju CAXY *tim za zaštitu* treba da izradi, prema preporukama standarda ISO/IEC 27001. Ovim bi se stvorile pretpostavke za uspostavljanje OP za menadžment bezbednosnog rizika (*OP02-OP05*) i *uklonila opšta prepreka za poboljšanje više SSE OP na veće CL i sakupljanje argumenata za garantovanu bezbednost.*

4. *Metrike PKI sistema zaštite* nisu eksplicitno planirane i dokumentovane. Ne postoji eksplicitna izjava u politici komponente sistema o uvođenju i korišćenju *sistemske* i *procesne* metrike za stvaranje argumenata garantovane bezbednosti, predviđanje performansi procesa i kontinualno poboljšanje procesa. Iako se brojni metrički podaci sakupljaju u izvršavanju standardnih procedura, ne vrši se metrička analiza sakupljenih indikatora o stanju zaštite sistema. Filtrirani bezbednosno relevantni *log* podaci (na *P1*) prenose se nezaštićenim linijama, ali su predajna i prijemna strana pod stalnim nadzorom CAXY, što organizacija smatra pogodnom zaštitom u postojećim uslovima. *Ova slabosti je opšta prepreka za implementaciju i institucionalizaciju GP na CL2 i CL3 za sve SSE OP.*
5. *Oblasti procesa (OP02, OP03, OP04, OP05)* za menadžment *bezbednosnog rizika* ne izvršavaju se, nisu eksplicitno planirane, ni dokumentovane na bilo koji način. *CAXY* ne koristi ni jednu formalnu ili neformalnu metodu za *analizu i procenu rizika*. Implementaciju PKI sistema *CAXY* vrši na bazi standardnih *MS definisanih politika* (8), tehničkih *procedura* i MS *najbolje prakse zaštite*, pa podrazumeva da su relevantni faktori bezbednosnog rizika već ublaženi takvim rešenjima. *Nepostojanje i neizvršavanje procesa menadžmenta bezbednosnog rizika, za organizaciju tipa CAXY, može se smatrati najvećom slabosti i opštom preprekom za podizanje ovih SSE OP na viši, najmanje CL3 nivo zrelosti.*
6. *OP06* formalno se ne planira i ne izvršava u celini. Međutim, BP koje generišu ove argumente, *neformalno* se izvršavaju u okviru izvršavanja standardnih MS procedura laboratorijskog ispitivanja, pilot testiranja PKI sistema u realnom okruženju i monitoringa rada sistema, ali nisu pokrivene formalnom politikom niti su eksplicitno dokumentovane kao procedure ili proces izgradnje argumenata garantovane bezbednosti. *Ova slabost u izvršavanju BP opšta je prepreka za podizanje ove OP na viši nivo zrelosti, čime bi CAXY stekla veće poverenje klijenata i postigla konkurentsku prednost na tržištu.*
7. *Koordinacija aktivnosti inženjerskih grupa* na projektima zaštite *(OP07, BP07.01 — BP07.04)* izvršava se *neformalno*, ali regularno na svakom projektu — nisu eksplicitno planirane i nisu pokrivene politikom zaštite, ali su delimično dokumentovane na nivou svakog projekta, jer se *de facto* izvršavaju na svakom projektu. Koordinacija inženjerskih grupa ili pojedinaca, nosioca određenih uloga na konkretnom projektu, vrši se na radnim sastancima, sedmičnim ili mesečnim, u toku pripreme projekta, laboratorijskog ispitivanja, implementacije i testiranja u produkcionom okruženju, gde se usaglašavaju sve aktivnosti na nivou projekta između svih učesnika projekta, ali se sve ove aktivnosti neredovno i slabo dokumentuju. *Ova slabost u izvršavanju BP opšta je prepreka za podizanje ove OP na znatno viši nivo zrelosti kapaciteta.*
8. *CAXY nema formalno razvijen menadžment sistem kvaliteta. Sistem kvaliteta proizvoda* (modula PKI) uključuje verifikaciju navedenih funkcionalnosti modula PKI sa ciljem i otklanjanja uočenih nedostataka i defekata u fazi testiranja uzoraka za pripremu projekta, laboratorijskog ispitivanja za ugovoreni projekat i testiranja (validacije) u produkcionom okruženju. Sva ova ispitivanja *kvaliteta proizvoda i tehnologije PKI,* CAXY ne izvršava u odnosu na neki standard, što znači da organizacija formalno nije uvela sistem kvaliteta proizvoda (npr. CC standard) ili procesa (npr.

SSE CMM). *Pošto koristi MS proizvode i tehnologiju koja podržava najbolje PKI prakse, CAXY smatra da sistem kvaliteta proizvoda nije neophodan*. Međutim, *sistem kvaliteta procesa zaštite* ima daleko veći značaj za *CAXY*, sa aspekta poslovnih ciljeva i misije, potrebe formalnog definisanja i opisivanja standardnih procesa i familije standardnih procesa organizacije, kao i stalnog poboljšanja tih procesa. *Asistiranom SSAM samo-evaluacijom* tekućih procesa, na bazi referentnog SSE CMM procesa zaštite, CAXY uvodi prvu fazu *sistema kvaliteta procesa*. *Slabosti u izvršavanju BP12.04 — BP12.08 OP12, opšte su prepreke za podizanje ove OP na više nivoe zrelosti.*

Snaga organizacije:

1. Za svaki projekat formira se projektni tim *kompetentnih izvršilaca*, koji u celini rešava sve projektne zadatke i *administrira* PKI procedure preuzete ugovorom o održavanju na sva tri evaluirana projekta, koristeći pretežno elektronska dokumenta i automatizovane procedure za izveštavanje stanja. *Na ovaj način CAXY može poboljšati sve OP na više nivoe zrelosti, sa malo napora i obezbediti potrebne metričke podatke za brojne SSE OP, formalnim dokumentovanjem, regularnom analizom i korišćenjem rezultata analize za upravljanje procesima.*
2. U evaluiranim projektima razvijene su CP relevantnih komponenti PKI sistema (8), koje pokrivaju sve bitne oblasti projektovanja, implementacije, integracije i održavanja PKI sistema na bazi MS PKI tehnologija i *MS Windows* platformi. Opisane su ključne procedure u skladu sa MS dokumentacijom. *Postojeće CP dobar su uvod u uspostavljanje i kompletiranje sveobuhvatne politike zaštite CAXY, uključujući ISMS politiku.*
3. Iako se metrika procesa ne planira, praktično se na nivou projekta, a u fazi laboratorijskog testiranja uzoraka, ispitivanja u produkcionim uslovima, monitoringa rada i izveštavanja korisnika o incidentima, primenjuju tri tipa metrika: (*1*) *heurističko merenje nedostataka i defekata* i otklanjanje u fazi testiranja uzoraka i laboratorijskog testiranja PKI sistema, gde se podrazumevano primenjuju metrike korišćenih alata za testiranje; (*2*) *automatsko* (e-mail) *dostavljanje metričkih podataka u XML formatu* o stanju bezbednosti i greškama sistema i (*3*) *korisničko izveštavanje* o incidentima u sistemu. Generalno, u procesu monitoringa brojni metrički podaci se skupljaju automatizovanim alatima ili opservacijama korisnika. *Ovakva praksa je dobra osnova za opšte povećanje kvaliteta izvršavanja BP, odnosno, uvođenje metrike na CL2, CL3 i višim nivoima zrelosti SSE OP*.
4. Dobro osposobljeni timovi CAXY mogu, sa neznatnim naporom i veoma rentabilno, poboljšati formalno dokumentovanje i analizu sakupljenih metričkih podataka i podići specifično OP11 za v*erifikaciju i validaciju* tehničkih rešenja na viši nivo zrelosti kapaciteta, čak i na CL3, pošto projektni timovi izvršavaju gotovo sve BP ove OP na zavidnom nivou kvaliteta, ali ih formalno ne dokumentuju i analiziraju. *Ovu OP CAXY perspektivno može vrlo brzo i rentabilno podići na CL4, čime bi organizacija bila osposobljena i za komercijalnu sertifikaciju i akreditaciju PKI rešenja.*

11.4.2.3 Komparativna analiza referentnog i tekućeg profila OP CAXY

Komparativna (*gap*) analiza razlika CL OP tekućeg i željenog profila, direktno ukazuje na prioritetne akcije CAXY za poboljšanje tekućih procesa. Međutim, kod odlučivanja o prioritetu poboljšanja tekućih procesa CAXY, treba uzeti u obzir činjenicu da je za svaku organizaciju rentabilnije poboljšavati najpre sve organizacione OP (OP17-OP22) najmanje na CL1 ili CL2, a zatim poboljšavati projektne OP (OP12-OP16) najmanje na isti, ili viši nivo dobro definisanih procesa — CL3. Poboljšani organizacioni i projektni procesi stvaraju osnovu za efikasno i mnogo efektivnije poboljšanje inženjerskih OP (OP01-OP11) na željeni nivo zrelosti, a prema dinamici i raspoloživim resursima organizacije. Generalno, na najviše nivoe zrelosti treba podići one OP koje proizvode najveću vrednost za organizaciju i koje se koriste regularno i svakodnevno. Na bazi ovakvog pristupa i rezultata komparativne analize tekućeg i željenog CA profila OP, optimalan je sledeći redosled akcija za poboljšanje procesa CAXY, kroz *proizvoljan broj projekata* i sa *projektnim zadacima* definisanim u predlogu plana:

- *organizacione OP* — OP17 i O—P18 na CL1 i OP20 na CL2;
- *projektne OP* OP12 na CL2, OP13 na CL2, OP14 i OP15 stabilisati na CL1;
- *SSE* — OP01, OP05, OP07, OP08 i OP10 na CL3, a OP02, OP03, OP04, OP06 i OP11 na CL2.

11.4.3 Poboljšanje tekućih procesa CAXY

11.4.3.1 Poboljšanje procesa na bazi CMM modela

Poboljšanje procesa zahteva intenzivno angažovanje svih kapaciteta organizacije, pa se broj *procesa* za poboljšanje mora izabrati u skladu sa ukupnim kapacitetima organizacije, tako da ne ometaju normalne aktivnosti. Da bi se ovo postiglo može se koristiti SEI *IDEAL* metodologija za implementaciju i poboljšanje procesa ili *6SIGMA* metodologiju od šest koraka: *izbor, razumevanje, performanse, revizija, izmene* i *implementacija izmena proces,* ili neka druga, po izboru korisnika.

Za pokretanja aktivnosti poboljšanja procesa korisno je razmotriti sledeća pitanja:

- *Motiv* – koji kritični elemenat posla zahteva poboljšanje procesa?
- *Model* – koji referentni model najbolje odgovara praksi organizacije?
- *Metod* – kako se mogu brzo identifikovati prilika za poboljšanje procesa?
- *Menadžment promena* – koji faktori utiču na efektivnost uvedenih promena?
- *Merenja* – koji su kritični faktori za uspostavljanje programa metrike?

Svaki *program poboljšanja procesa* treba da se zasniva na poslovnim ili drugim potrebama organizacije i da je deo strateških ciljeva. Dakle, motiv za pokretanje programa poboljšanja procesa mora imati realno uporište u zahtevima i potrebama organizacije. Model procesa igra važnu ulogu u poboljšanju procesa. U praksi, korisnici, generalno, imaju mentalnu sliku o tome kako skup procesa u organizaciji funkcioniše, a specifični model procesa može da obezbedi najmanje tri elementa:

- terminologiju i konstrukcije za razumevanje procesa;
- standard za poređenje i indikatore za evaluaciju efektivnosti procesa i
- uputstvo za investiranje u poboljšanje procesa.

Pored toga referentni model ili standard procesa često se koristi kao izvor ideja za *dobre procese*. Postoje brojni modeli za poboljšavanje procesa, koje organizacije mogu koristiti za rešavanje kritičnih pitanja. Klasa CMM modela široko se koristi za poboljšavanja procesa. Kontinualna reprezentacija modela ima prednost zbog dobro definisanog puta poboljšavanja procesa za specifične OP. Fazna reprezentacija ima prednost kada organizacija planira poboljšavanje grupe OP, za šta treba dobar poslovni razlog. U izboru referentnog modela za poboljšanje procesa, prvo treba definisati *oblast* poslovanja i oblast relevantnih procesa za tu oblast. Pri tome ne treba pokušavati da model pokriva 100% potrebe organizacije. Ako model obuhvata 60 — 80% kritičnih pitanja organizacije to se mora smatrati uspešnim izborom modela.

U izboru reprezentacije modela koja najbolje odgovara ciljevima poboljšanja procesa, treba koristiti kontinualnu reprezentaciju, ako je cilj poboljšanje nekoliko procesa, a ako je cilj poboljšanje grupe ili svih procesa na viši nivo (najčešće CL1) treba izabrati faznu reprezentaciju (SSE CMM ili CMMI). U izboru tipa CMM modela za poboljšanje procesa ne treba pažnju obraćati na CL/ML nivoe, nego da se proces poboljša i izabere model koji najbolje pokriva kritične procese koje treba poboljšati.

Posle izbora modela procesa za poboljšanje kritičnih procesa organizacije, treba odlučiti kako će organizacija evaluirati usaglašenost svojih praksi i procesa sa parametrima modela, zato što postoje tri osnovna razloga za evaluaciju procesa:

- *identifikacija tekućih procesa sa ciljem njihovog poboljšanja*,
- *evaluacija rizika* za performanse procesa organizacije i
- *sertifikacija* nivoa zrelosti i kapaciteta procesa (ML/CL).

Međutim, kako ne postoji zvanično međunarodno sertifikaciono telo za različite tipove CMM modela, SEI institut preporučuje da evaluaciju na bazi CMM modela procesa, obavlja osposobljen tim za evaluaciju, koji završi preporučenu obuku za rad sa određenim modelom i metodom. Postoje brojni metodi za evaluaciju, od jeftinih tehnika samoevaluacije, privremenog profilisanja i mini evaluacije do evaluacije osposobljenog tima na bazi CMM modela, kao što su SSAM (na bazi SSE CMM) i SCAMPI (na bazi CMMI), metodi evaluacije. Ključni faktori koje treba razmatrati u izboru metoda evaluacije su: *ciljevi evaluacije i željeni izlazni rezultati, tačnost dobijenih rezultata, troškovi pripreme i izvođenja evaluacije i nivo destrukcije koju proces evaluacije unosi u organizaciju.*

Akcioni plan je neophodan izlaz svakog procesa evaluacije i ulazni parametar u implementaciju promena. Organizacija treba da revidira nalaze i preporuke procesa evaluacije i odluči koje će akcije preduzeti u sledećem koraku poboljšanja procesa. Proces poboljšanja podrazumeva da se informacije i iskustva dobijena iz upravljanja individualnim projektima prenose celoj organizaciji radi analize i razvoja u drugim primenljivim projektima i oblastima. Promene u familiji standardnih procesa mogu doći zbog inovacija u tehnologijama ili inkrementalnog poboljšanja na bazi rezultata evaluacije. *Inovativna poboljšanja* obično su inicirana uvođenjem nove tehnologije i obezbeđuju siguran skok u kvalitetu poslovanja. *Inkrementalna poboljšanja* inicirana su internom evaluacijom procesa organizacije sa ciljem

evolutivnog poboljšavanja i prilagođavanja definisanih procesa standardnim procesima organizacije. Poboljšanje standardnog procesa otklanja uobičajene uzroke varijacija procesa u toku izvršavanja. Poboljšanje tekućih OP CAXY na bazi predloženih *zadataka akcionih planova*, treba zasnivati na inkrementalnim poboljšanjima, dokumentovanim u *GP 5.2.2 i 5.2.3* za svaku poboljšanu OP sa ciljevima uspostavljenim u *GP 5.1.1*.

11.4.3.2 Uloge i odgovornosti u projektu poboljšanja procesa

Generičke uloge (pojedinci/grupe) u *projektu poboljšanja procesa (PPP),* na bazi CMM modela procesa, su:

- *sponzor PPP:* lice iz organizacije odgovorno za nadgledanje i kontrolu celokupnih aktivnosti za poboljšanje procesa, koje ima ovlašćenja za alokaciju resursa za poboljšanje procesa; uobičajeno je na nivou direktora ili većem;
- *lice za odnose sa javnošću:* ovo je tipično *direktor marketinga*, koji predstavlja organizaciju po pitanju svih aktivnosti vezanih za poboljšanje procesa. Može, a ne mora biti istovremeno i lider *inženjerske projektne grupe – EPG* za realizaciju projekta poboljšanja procesa; promoviše ideje, pristupe i rezultate poboljšanja;
- *menadžment EPG:* rukovodi/e i revidira/ju rad članova EPG, dodeljuje/u im zadatke, nadzire/u njihov rad i planira/ju dnevne aktivnosti EPG;
- *članovi EPG:* odgovorni su za izradu i striktno sprovođenje dokumentacije za poboljšanje procesa i generisanje metrike za praćenje poboljšanja procesa; rukovode pojedinačnim *grupama za implementaciju procesa* ili *akcionim procesnim timovima* (*PAT*);
- *akcioni timovi za implementaciju procesa (PATs):* generišu dokumentaciju za poboljšanje procesa – politiku, opis procesa, procedure, akcione planove i planove za realizaciju zadataka akcionih timova;
- *spoljni saradnik:* obično jedan ili dva lica koja su spoljni konsultanti, angažovani za pomoć u uspostavljanju planova, vođenju i monitorisanju progresa u poboljšanju procesa; unose lična iskustva i znanja iz poboljšanja procesa.

Ove se uloge, zavisno od tipa i veličine organizacije, mogu prilagođavati, integrisati i objedinjavati u jednom licu/grupi, gde je potrebno i odgovara.

11.4.3.3. Tipična infrastruktura procesa za poboljšanje procesa

Rukovodstvo EPG tipično treba da razvije i uključi sledeće infrastrukturne komponente za uspešnu realizaciju nekog *projekta poboljšanja procesa:*

- uspostavi *potpunu* komunikaciju u organizaciji za efikasnu koordinaciju učesnika,
- uspostavi i popuni EPG, *upravni i izvršni odbor projekta*,
- uspostavi i održava *entitet (lice/a) za kontrolu konfiguracije — CCB* (*Configuration Control Board*), odgovoran za upravljanje dokumentacijom procesa organizacije,
- razvije proceduru CCB kontrole dokumentacije za poboljšanje procesa,
- kreira mehanizme za prezentaciju ideja i postavljanje zahteva za poboljšanje procesa EPG i PAT timovima,

- razvije *politiku organizacije* za svaku OP primenjenog modela procesa,
- kreira okvir za merenja postignutog uspeha i progresa u poboljšanju procesa i
- obezbedi odgovarajuću obuku i alate za podršku (proizvodno okruženje).

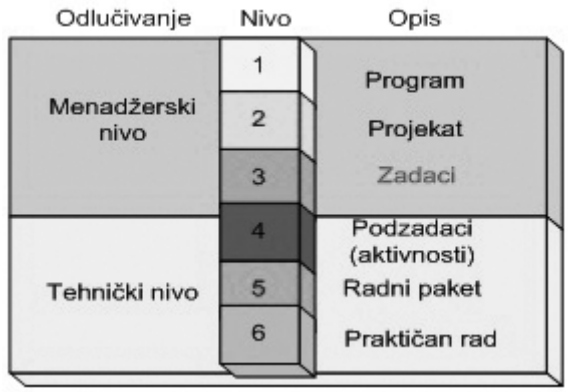
Svi CMM modeli procesa sugerišu *SEI IDEAL Model* za implementacije SSAM i SCAMPI rezultata evaluacije i poboljšanja procesa (videti sliku 10.21).

11.4.3.4 Akcioni planovi za poboljšanje tekućih procesa CAXY

Prema modelima sazrevanja procesa, akcioni plan za poboljšanje procesa razvija se na tri nivoa planiranja: *dugoročnom* (strateškom), *kratkoročnom* (taktičkom) i na nivou *projektnog tima* za realizaciju konkretnog projekta poboljšanja procesa. Za poboljšanje tekućih procesa CAXY razvijena su *tri tipa akcionih planova* za poboljšavanje procesa kroz definisane *faze, zadatke i aktivnosti* koje treba izvršiti:

1. *Strateški plan poboljšanja* ili *program razvoja procesa (PRP) organizacije*, predstavlja okvir za alokaciju resursa, a uključuje razloge i definisane ciljeve poboljšanja.
2. *Akcioni plan poboljšanja procesa (APP)* je taktički, detaljniji, kratkoročni plan koji definiše napore organizacije kroz upravljive zadatke, formirane na bazi rezultata SSAM evaluacije. Naziva se i *plan implementacije ili operativni plan*. *Zadaci* za *APP tekućih procesa CAXY*, detaljno se opisuju u akcionom planu projekta poboljšanja OP. Procesi se opisuju *formalno i detaljno* sa ciljem uspostavljanja standardnih procesa organizacije i formiranja repozitorijuma standardnih procesa organizacije, sa adekvatnom zaštitom i kontrolom pristupa. Primer strukture sadržaja operativnog APP dat je u **Prilogu 11.6.**
3. *Akcioni planovi projektnog tima (PPT)* su vrlo detaljni, a formira ih projektni tim (PT) sa fokusom na to *šta, kako* i *kada* treba da se uradi. PT prioritetno usmerava pažnju na one OP koje su u procesu evaluacije pokazale najveće slabosti. U okviru ovog plana treba definisati *plan potpune komunikacije* u okviru PT, sa drugim PT u organizaciji i spoljnim saradnicima. Dobra komunikacija, sa potpunim razumevanjem značenja razmenjenih poruka, od presudnog je značaja za efikasnost izvršavanja svakog procesa. Uzorak strukture zadataka detaljnog *PPT* za poboljšanje *OP01* sa *CL1 na CL2 i CL3*, kao i nacrt *plana merenja procesa* i primeri potencijalnih *metrika procesa upravljanja bezbednosnim zahtevima na CL 2*, dati su u **Prilogu 11.7.**

Dijagram dekompozicije *programa za razvoj procesa (PRP)*, po nivoima odlučivanja, kroz faze i zadatke do praktične realizacije, prikazan je na slici 11.5. Predlozi akcionih planova za poboljšanje procesa CAXY dati su na nivou *zadataka*, što podrazumeva da u fazi planiranja konkretnih projekata za poboljšanje SSE procesa organizacije, CAXY treba da uspostavi ostale elemente plana projekta: *PT, obim, veličinu i ograničenja, dinamički plan realizacije, kontrolu projekta, faktore rizika projekta, potrebne resurse i druge elemente*.



Slika 11.5 Nivoi dekompozicije programa za razvoj procesa

11.5 ANALIZA ISKUSTAVA IZ SSAM PROCESA EVALUACIJE

11.5.1 Dopuštena odstupanja od SSE CMM modela

Međuzavisnosti određenih OP i GP/BP u modelu (videti tabelu 10.5) doprinose razumevanju uticaja *implementacije* i *institucionalizacije* određenih GP na sazrevanje CL/ML procesa.

Primeri proizvoda rada jedini su indikatori dokaza o implementaciji praksi (BP i GP) procesa prema SSE CMM-u, opisani u samom modelu u okviru opisa BP. U cilju detaljnijeg i preciznijeg dokumentovanja i praćenja potencijalnih *dokaza* izvršavanja, implementacije i institucionalizacije BP i GP SSE CMM-a, izvršena su *prilagođavanja* SSE CMM modela, kroz uvođenje i opis sledećih *termina* i *kategorija*:

1. *Objektivni dokazi* su svi dokazi dobijeni instrumentima SSAM evaluacije, koji objektivno i *koraborativno* (nezavisno od izvora) potvrđuju da su pripadajuće BP i GP izvršavane, implementirane i/ili institucionalizovane.

a. Vrste objektivnih dokaza:

- *direktni dokazi (DD),* opipljivi izlazni rezultati implementiranih praksi, npr. *primer proizvoda rada* naveden u SSE CMM modelu,
- *indirektni dokazi (ID),* posledice ili indikacije implementacije BP i
- *potvrdne izjave (F2F),* usmene/pisane koje podržavaju implementaciju praksi, tj. potvrđene *opservacije* i odgovori na *upitnik* ili *intervju*.

b. Izvori objektivnih dokaza za SSAM evaluaciju mogu biti *instrumenti* metoda:

- *upitnik* u formi ankete, skuplja podatke o imovini procesa organizacije i odražava dokaz o implementaciji praksi prema SSE CMM modelu, npr. projektni dokument;
- *intervju,* struktuiran, po pozivu, dodatni; lidera projekta, praktičara, korisnika;

- *prezentacije,* demonstracije alata, pregledi sastanaka i sl.;
- *neposredna demonstracija korisnika,* praktičara koji izvršavaju procese, dokazuje kvalitet izvršavanja određenih procesa CA, npr. prikazivanje izveštaja o izvršenom procesu na displeju računarskog sistema i sl. i
- *različita dokumenta,* kao što su politika, procedure i planovi implementacije u čvrstoj ili e-formi, tehnička i druga dokumentacija koja ukazuju na implementaciju praksi i OP.

11.5.2. Odstupanja od procesa SSAM metoda evaluacije

- Predlog *plana evaluacije*, izrađen je u prepripremnoj fazi, pre upoznavanja sponzora o detaljima evaluacije i izbora mešovitog TE, čime je značajno skraćen proces evaluacije za period pripreme plana (2 — 6 sedmica), prema SSAM metodu i obimu evaluacije projekata.
- *RF — zahtevi za ponudu evaluacije* nisu specifično razvijani i direktno su uključeni u *plan evaluacije,* zbog nekomercijalnog karaktera evaluacije tekućih procesa CAXY.
- SSAM metod *sugeriše dva posmatrača* u TE — **jednog** iz organizacije evaluatora i **jednog** iz evaluanda, koji se obučavaju za samostalno vođenje procesa evaluacije; na osnovu eksplicitne zainteresovanosti sponzora i tipa procesa evaluacije (*asistirana samo-evaluacija),* povećan je broj posmatrača na **četiri**, pri čemu su svi posmatrači bili zaposleni evaluanda.
- *DTS* dokument nije uključivan u preliminarnu evaluaciju podataka posle administracije *upitnika i intervjua lidera projekta*, ali je revizija i konsolidacija odgovara i priloženih dokaza vršena na bazi analize *afirmativnih odgovora, koraboracije, pokrivanja i kompletnosti* raspoloživih dokaza, posle svake faze administracije odgovora.
- *Zahtevi za dokaze* rukovalac dokaza tražio je na SSAM propisanom formatu za praćenje kretanja dokaza, ali relativno retko, pošto je sponzor obezbedio interni *web* portal u radnoj prostoriji TE, za pristup svim serverima na kojima se čuva elektronska dokumentacija CAXY-a, pa je omogućen neposredan uvid u objektivne i skupljene dokaze svakog člana TE, u fazi sakupljanja i konsolidacije dokaza. Ovakav način verifikacije dokaza za afirmativne iskaze u *upitnicima* i *intervjuima*, ubrzao je proces evaluacije za oko 30% — pet evaluatora i četiri posmatrača za *14 radnih dana* sa četiri efektivna radna sata u proseku, za tri evaluirana projekta, prema tipičnih *20 radnih dana*, za pet evaluatora i jednog posmatrača po osam sati rada dnevno za četiri evaluirana projekta. U procesu evaluacije razvijena su sva zahtevana radna dokumenta TE.
- *Proces SSAM metoda* u celini je izvršen sa svim fazama i koracima, osim u pogledu dinamike rada TE i vremenskog plana, zbog nekomercijalnog karaktera evaluacije i nastojanja TE da minimizira destrukciju rada CAXY-a. TE je isključivo radio u popodnevnim satima, tipično od 14.00 — 18.00 časova, sa jednom do dve pauze od 15 minuta. Na taj način, od tri glavna atributa SSAM procesa evaluacije*: tačnost, destrukcija organizacije i cena,* dva (*destrukcija i cena*), značajno su redukovani.
- *Tačnost SSAM* verifikacionog procesa evaluacije, neznatno je poboljšana uvođenjem preglednih i eksplicitnih DD za afirmativne prakse sa *originalno generisanim SSAM*

PIID dokumentom i striktnim zahtevom za *kooraboraciju, pokrivanje i kompletnost* svakog dokaza, po uzoru na napredniji SCAMPI metod evaluacije, i to u fazi svake konsolidacije dokaza i generisanja preliminarnih i konačnih rezultata i nalaza evaluacije.

- *Broj intervjuisanih praktičara* smanjen je u odnosu na planiranih devet (tri po svakom evaluiranom projektu), na po *jednog* intervjuisanog praktičara sa P1, P2 i P3, zbog efikasne prezentacije dokaza na internom *web portalu* za svaki evaluirani projekat u radnoj prostoriji TE i, posebno, zbog činjenice da sve evaluirane projekte PKI sistema, inženjerski tim CAXY održava i administrira u svim fazama životnog ciklusa sistema sa lokacije evaluacije.
- *Izveštaj o evaluaciji*, uz saglasnost sponzora, nije formalno izrađen i dostavljan sponzoru kao celovit pisani dokument, nego su svi rezultati evaluacije — *profil procesa, glavni nalazi i akcioni plan* u delovima isporučivani sponzoru evaluacije.

11.5.3 Iskustva iz sprovođenja *plana evaluacije tekućih procesa CAXY*

- Iskustvo iz *prve* evaluacije tekućih procesa CAXY u cilju uvođenja sistema kvaliteta i regularnog poboljšanja, značajno je za evaluanda i TE.
- Sve razlike profila pojedinačnih tekućih i željenih OP, identifikovane su i obuhvaćene predlogom *zadataka* za *APP tekućih procesa CAXY*, prema dinamici i resursima CAXY-a.
- Menadžeri i lideri projekata *P1, P2 i P3* intervjuisani su simultano za sve inženjerske (SSE) OP, pošto rade zajedno u svim fazama životnog ciklusa na sva tri evaluirana projekta i imaju višestruke uloge sa pravima pristupa dokazima preko internog *web* portala, što je značajno povećalo efikasnost prikupljanja i verifikacije dokaza.
- Vreme sesije intervjuisanja menadžera i lidera projekta treba povećati do dva sata sa petnaest minuta pauze, umesto standardnih 45 minuta sa 15-minutnom pauzom, što obezbeđuje održavanje suštine intervjua na potrebnom nivou, intenzivnije učešće intervjuisanih i efektivnije sakupljanje dokaza, pošto češći prekidi dovode do gubljenja koncentracije i distribucije pažnje sa predmeta istraživanja.
- Vreme za intervjuisanje praktičara za usklađenost prakse BP i GP datog procesa sa standardima, planom, politikama ili procedurama zaštite, treba povećati na 1.5 čas, zbog njihovog slabijeg razumevanja zahteva procesa evaluacije u celini.
- Preporučuje se pregled internih dokumenata u pripremnoj fazi, pre evaluacije na terenu, što može inicirati menadžer projekta, sponzor ili član TE, zbog preliminarnog uvida u direktne objektivne dokaze u svim fazama SSAM *evaluacije na terenu.*
- *Uloge rukovaoca* dokaza i *člana TE za praćenje dokaza* i realizacije SSAM procesa, spojene su, zbog vremenske fleksibilnosti, nekomercijalnog karaktera evaluacije tipa *asistirana samoevaluacija* i načina sakupljanja dokaza preko *web* portala.

11.5.4 Iskustva iz vođenja intervjua

- U toku intervjua treba intervjuisanim licima dopustiti da donesu sa sobom dokaze (fizička dokumenta, npr.), ili da na mestu intervjuisanja obezbede direktan pristup svim raspoloživim dokazima, identifikovanim u fazi administracije *upitnika.* Interni *web portal* za *on-line* pristup dokazima, obezbeđen u radnoj prostoriji TE gde su intervjuisana sva lica, značajno je povećao efikasnost sakupljanja i konsolidacije svih dokaza.
- Potreban je razmak od najmanje četiri do pet dana između pripremne faze i faze evaluacije na lokaciji, zbog kvalitetne i konzistentne konsolidacije dokaza sakupljenih upitnikom.
- U fazi intervjuisanja lidera projekta i praktičara, zavisno od uloge intervjuisanog, pokazalo se da gotovo redovno treba preformulisati pitanja iz *upitnika*, sa dodatnim razjašnjenjem značenja za konkretnu OP i pripadajuće BP, zbog generičke i uopštene formulacije pitanja u originalnom dokumentu SSAM metoda evaluacije.
- Vreme za dodatni intervju treba uneti u *dinamički plan evaluacije*, pošto se uvek može očekivati neka nekonzistentnost ili potreba za razjašnjavanjem i posle svih intervjua.

11.5.5 Sugestije za sponzora

- Treba praktikovati proveru konzistentnog planiranja i redovnog dokumentovanja izvršavanih aktivnosti (BP) u SSE OP (OP01-OP11), koje se *de facto* uspešno izvršavaju, ali ne ostaju tragovi za uspostavljanje sistema kontrole kvaliteta.
- Treba uspostaviti – planirati i formalno definisati i opisati, *standardne procese organizacije* (OP17) i familiju standardnih procesa organizacije, uključujući i procese za *menadžment bezbednosnog rizika* (OP02-OP05) i dovesti ih najmanje na CL1 u prvim projektima poboljšanja procesa organizacije, a zatim na CL2, bez obzira na željeni profil procesa.
- U dugoročnom planskom periodu, treba stabilisati sve *organizacijske* procese (OP17-OP22) — najmanje na CL2, *projektne* procese (OP12-OP16) — najmanje na CL3, a *inženjerske* procese (OP01-OP11) prema dinamici i raspoloživim resursima CAXY – najmanje na CL3, a OP11 — na CL4.

11.6. REZIME

Glavni ciljevi evaluacija procesa organizacije — efikasno sakupljanje preciznih podataka uz minimalnu destrukciju rada i identifikacija prioriteta procesa za poboljšanje, mogu se dostići na brojne načine i sa različitim stepenom troškova i tačnosti. Većina metoda evaluacije na izlazu ima *nalaze* o slabostima i snazi organizacije i *preporuke* za akcioni plan poboljšanja procesa. *Nalazi* obezbeđuju preciznu sliku o procesima, koristeći neki referentni model procesa kao okvir za evaluaciju. *Preporuke* procesa evaluacije obezbeđuju uputstvo za poboljšanje tekućeg stanja procesa organizacije. Metodi evaluacije na bazi CMM modela su brojni, a u izboru treba razmatrati, najmanje, *tačnost, troškove i stepen destrukcije* poslovanja organizacije.

Na bazi SSE CMM referentnog modela, razvijen je metod evaluacije zrelosti procesa zaštite — *SSAM v.2.0,* koji mogu koristiti brojne organizacije (za *razvoj proizvoda zaštite, provajderi servisa zaštite, integratori sistema zaštite itd.*). Glavne faze procesa SSAM evaluacije su *planiranje, priprema, rad na terenu i izveštavanje*. Relevantne uloge u procesu su *sponzor, tim za evaluaciju (TE), evaluatori, rukovodilac dokaza, članovi TE sa pravom glasa, posmatrači, praktičari, koordinator evaluacije na terenu, menadžment i PR evaluirane organizacije, rukovodilac i praktičari evaluiranog projekta*. Glavni tipovi SSAM evaluacije su *nezavisna evaluacija* i *samoevaluacija* (*asistirana i monitorisana*).

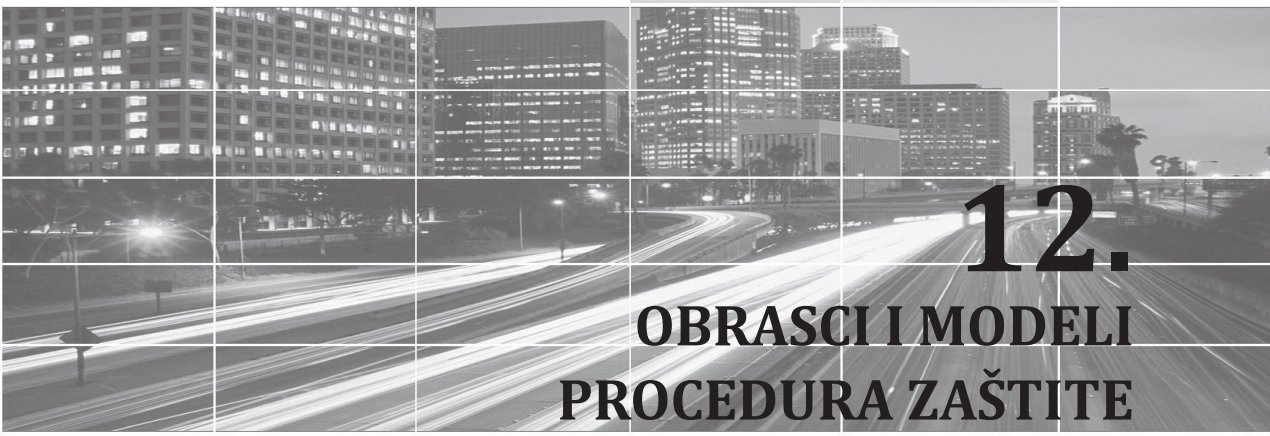
U procesu SSAM evaluacije promenljivi parametri mogu biti *OP, nivoi CL, upitnik, projekat za evaluaciju, intervju, metod izveštavanja, dokazi i odnosi sa koordinatorom rada na terenu.* Rezultate evaluacije, TE definiše konsenzusom prema kriterijumima za verifikaciju dokaza: za CL1 zahteva se 100% izvršavanje BP, a za sve druge — ako je **100%** dostignut prethodni CL, a **80%** tekući CL. Drugi tip kriterijuma je procena, verifikacija i konsolidacija dokaza sa konsenzusom ovlašćenih evaluatora.

U studiji slučaja izvršena je *SSAM asistirana samoevaluacija* tekućih procesa *CAXY* na bazi SSE CMM referentnog modela, sa timom od jednog evaluatora, pet članova sa pravom glasa i četiri posmatrača iz evaluirane organizacije u projektu od dva meseca. Rezultati evaluacije su pokazali glavne prednosti i nedostatke *CAXY* organizacije i ukazali na procese (OP) koje treba akcionim planom obuhvatiti za progresivno poboljšanje, da bi se dostigao profil OP, usaglašen sa referentnim profilom procesa najbolje prakse CA.

11.7 PITANJA ZA PONAVLJANJE

1. Metodologiju za evaluaciju procesa zaštite sadrži:
   a. metod IDEAL
   b. SSE CMM model
   c. metod SSAM
   d. metod 6SIGMA.
2. Glavni ciljevi evaluacije procesa su:
   a. sakupljanje preciznih podatke uz minimalnu destrukciju rada
   b. nalazi o slabostima i snazi organizacije
   c. pomoć u identifikaciji i određivanju prioriteta procesa za poboljšavanje
   d. preporuke za akcioni plan poboljšavanja procesa.
3. Glavne kategorije izlaznih rezultata evaluacije procesa su:
   a. sakupljanje preciznih podatke uz minimalnu destrukciju rada
   b. nalazi o slabostima i snazi organizacije
   c. pomoć u identifikaciji i određivanju prioriteta procesa za poboljšavanje
   d. preporuke za akcioni plan poboljšanja procesa.
4. U izboru metoda evaluacije, zahteva se razmatranje sledećeg skupa faktora:
   a. tipa referentnog modela, troškova i stepena destrukcije poslovanja organizacije
   b. tipa referentnog modela, tačnosti modela i troškova evaluacije
   c. tačnosti modela, troškova i stepena destrukcije poslovanja organizacije
   d. tipa referentnog modela, tačnosti i stepena destrukcije poslovanja organizacije.
5. SSAM metod evaluacije može se koristiti za *evaluaciju procesa* organizacije koja:
   a. razvija proizvode zaštite
   b. obezbeđuje servise zaštite
   c. obezbeđuje tehničke kontrole zaštite
   d. integriše i administrira sisteme zaštite
   e. integriše i administrira IKT sistem
   f. razvija kompetencije specijalista zaštite.
6. Razlozi za izbor nezavisne TTP evaluacije uključuju sledeće:
   a. kompetencije organizacije za ispunjavanje ugovornih obaveza
   b. nezavisnu komparativnu analizu kvalifikacija evaluatora
   c. razumeti sva pitanja koja se odnose na domen zaštite
   d. razumeti razvoj i implementaciju nove prakse zaštite u organizaciji
   e. obezbeđivanje razumevanja i ispunjavanja očekivanja klijenata
   f. obezbeđivanje upravljanja rizikom programa evaluacije
   g. određivanje ukupnih kapaciteta zaštite organizacije
   h. određivanje progresa aktivnosti za poboljšavanje procesa.
7. Razlozi za izbor samoevaluacije uključuju:
   a. kompetencije organizacije za ispunjavanje ugovornih obaveza
   b. nezavisnu komparativnu analizu kvalifikacija snabdevača
   c. razumeti sva pitanja koja se odnose na domen zaštite
   d. razumeti razvoj i implementaciju nove prakse zaštite u organizaciji
   e. obezbeđivanje razumevanja i ispunjavanja očekivanja klijenata
   f. obezbeđivanje upravljanja rizikom izvršavanja programa
   g. određivanje ukupnih kapaciteta zaštite organizacije
   h. određivanje progresa aktivnosti za poboljšanje procesa.
8. Nepromenljivi parametri u procesu planiranja SSAM evaluacije su:
   a. oblasti procesa
   b. SSAM metod
   c. nivoi kapaciteta (CL)
   d. upitnik i projekat za evaluaciju
   e. SSE CMM model.

9. Promenljivi parametri u procesu planiranja SSAM evaluacije su:
   a. metod izveštavanja
   b. dokazi
   c. SSE CMM
   d. OP
   e. projekat za evaluaciju
   f. SSAM.
10. U fazi konsolidacije dokaza TE prihvata sledeće dokaze bez verifikacije:
   a. tipične proizvode rada procesa
   b. popunjene upitnike i rezultate intervjua
   c. opservacije
   d. dnevne redove sastanaka i projektnu dokumentaciju
   e. PPT prezentaciju
   f. ni jedan od navedenih.
11. U fazi konsolidacije dokaza TE prihvata sledeće dokaze sa verifikacijom:
   a. tipične proizvode rada procesa
   b. popunjene upitnike i rezultate intervjua
   c. opservacije
   d. dnevne redove sastanaka i projektnu dokumentaciju
   e. PPT prezentaciju
   f. ni jedan od navedenih.
12. Izveštavanje SSAM procesa evaluacije uključuje:
   a. tipične proizvode rada i posredne artefakte procesa evaluacije
   b. glavne nalaze i izveštaj evaluatora
   c. PPT prezentaciju glavnih rezultata
   d. profil tekućih OP sa nivoima zrelosti kapaciteta (CL).
13. Kriterijumima za verifikaciju dokaza SSAM metoda evaluacije na bazi SSE CMM su:
   a. za CL1 zahteva se 100% izvršavanje BP
   b. za CL2 do CL5 da je 100% dostignut prethodni CL, a 80% tekući CL
   c. za CL1 zahteva se 90% izvršavanje BP
   d. konsolidacija dokaza sa konsenzusom ovlašćenih evaluatora
   e. za CL2 do CL5 da je 50% dostignut prethodni CL, a 90% tekući CL
   f. koraborativnost, pokrivanje i kompletnost dokaza.



12. OBRASCI I MODELI PROCEDURA ZAŠTITE

Po završetku ovog poglavlja studenti će naučiti da samostalno izrade:

- ☑ Proceduru zaštite informacija na bazi uzorka obrasca za dokumentovanje procedure
- ☑ Plan zaštite na bazi generičke strukture procedure za izradu plana zaštite(NIST)
- ☑ Proceduru kontrole pristupa IKT sistemu i informacionoj imovini organizacije
- ☑ Proceduru interne provere ISMS-a

12.1. UZORAK OBRASCA ZA DOKUMENTOVANJE PROCEDURE

Procedura „X“	
R. broj dokumenta:	Datum:
R. broj provere:	Datum:
Opis: (*ime procedure*)	
Ova procedura uključuje…… *Primarni cilj aktivnosti je da….*	
Ulazni kriterijumi/ulazi:....	Izlazni kriterijumi/izlazi:...
Uloge: Ime uloge: *Šta ona/on radi?*	
Imovina: *Standardi, referentni materijal, izlazni proizvodi rada, prethodni opisi procesa…*	

Kratak sadržaj zadataka (Lista glavnih zadataka/koraka procesa): Zadatak 1 Zadatak 2 Zadatak 3 Zadatak 4
KORACI PROCEDURE:
Zadatak 1 ◆ Detalji koraka 1 (aktivnost 1) ◆ Detalji koraka 2 ◆ Detalji koraka 3 ◆ Detalji koraka 4
Zadatak 2 ◆ Detalji koraka 1 ◆ Detalji koraka 2 ◆ Detalji koraka 3 ◆ Detalji koraka 4

12.2 GENERIČKA STRUKTURA PROCEDURE ZA IZRADU *PLANA ZAŠTITE (NIST)*

I. IDENTIFIKACIJA SISTEMA

Datum:

Ime sistema/Naslov: jedinstveni identifikator i kôdni naziv sistema.

Odgovorna organizacija: naziv organizacije odgovorne za sistem.

Kontakti za informacije: ime osobe(a) ili vlasnika koji imaju informacije o sistemu.

Ime:
Naziv ustanove:
Adresa:
Telefon:
e-mail adresa:

Odgovornost za zaštitu: ime lica odgovornog za zaštitu sistema.

Operativni status sistema: ako je izabran više od jednog statusa, navesti koji deo sistema je pod istim statusom:

- operativni,
- u razvoju,
- u toku je glavna modifikacija (reinženjering).

Generalni opis/namena:

- opisati funkciju ili namenu aplikacija i procesiranih informacija,
- opisati tok procesa aplikacija od ulaza u sistem do izlaza iz sistema i

- navesti organizacije koje koriste sistem (interne i eksterne), tip i datum procesiranja.

Okruženje sistema:

- obezbediti opšti opis tehničkog sistema; uključiti sve faktore okruženja ili tehničke koji zahtevaju posebne mere zaštite (*dial-up*, otvorena mreža — OSI itd.),
- opisati primarne platforme koji se koriste i opisati glavne komponente sistema i
- uključiti sve softvere za zaštitu informacija.

Unutrašnje veze u sistemu/deljenje informacija:

- navesti sve povezane sisteme i identifikatore sistema (ako je prikladno),
- ako neka veza sa spoljnim sistemom nije obuhvaćena planom zaštite, ukratko navesti svaki bezbednosni problem koji treba razmatrati u sistemu zaštite i
- zahteva se potpisivanje sporazuma o saradnji (MoU), pre spajanja sa drugim sistemima i/ili deljenja osetljivih informacija, sa detaljnim opisom pravila ponašanja međusobno povezanih sistema, koji je uključen u *plan zaštite* ili diskutovan u toku planiranja.

Primenljivi zakoni ili regulative koje utiču na sistem:

- navesti svaki zakon ili regulative koji uspostavljaju specifične zahteve za *poverljivost, integritet i raspoloživost (CIA)* informacija u sistemu.

Opšti opis osetljivosti informacija:

- uopšteno opisati informacije koje sistem procesira i potrebu za zaštitnim merama; povezati manipulisane informacije sa svakim od osnovnih atributa zaštite (CIA); za svaku od tri kategorije informacija indicirati kvantitativni (novčani ekvivalent) ili kvalitativni (*visok, srednji, nizak*) merni težinski faktor,
- uključiti izjavu o proceni rizika i veličini štete koja može nastati od gubitka CIA-e informacija.

II. UPRAVLJAČKE KONTROLE ZAŠTITE

Analiza i upravljanje rizikom

- Opisati metodologiju procene rizika korišćenu za identifikaciju pretnji i ranjivosti sistema. Uključiti datum analize rizika. Ako ne postoji analiza rizika, uključiti krajnji datum do kojeg treba završiti procenu rizika.

Pregled kontrola zaštite

- Navesti svaki nezavisni pregled kontrola zaštite u poslednje tri godine.
- Uključiti informacije o tipu izvršene evaluacije kontrole zaštite, evaluatoru, nameni kontrole i preduzetim akcijama na osnovu rezultata provere.

Pravila ponašanja

- Za svaki sistem pojedinačno mora se uspostaviti skup pravila ponašanja u pisanoj formi. Ova pravila treba da budu na raspolaganju svakom korisniku pre dobijanja prava pristupa sistemu. Preporučuje se da pravila sadrže stranicu za potpis korisnika, sa kojim se potvrđuje prihvatanje.
- Pravila ponašanja moraju jasno istaći odgovornosti i očekivana ponašanja svakog pojedinca sa pravom pristupa. Moraju biti navedene posledice za nekonzistentno ponašanje i neusaglašenost, kao i ograničenja za povezivanje sa drugim sistemima.
- Pravila ponašanja u IKT sistemu treba ugraditi u sekciju ili ih priključiti u **Prilog** sekcije.

Planiranje zaštite u toku životnog ciklusa sistema

- Odrediti koja je faza životnog ciklusa sistema, ili dela sistema, u toku. Opisati kako je manipulisana zaštita u tekućoj fazi životnog ciklusa sistema.

Inicijalna faza (pripremna)

- Navesti rezultate procene osetljivosti podataka/informacija sistema.

Faza razvoja/akvizicije

- U toku projektovanja sistema, gde je zahtevana zaštita?
- Gde odgovarajuće kontrole zaštite imaju pridružene procedure za evaluaciju i testiranje, razvijene pre preduzimanja akcije?
- Da li pravna dokumenta (npr. Zahtev za izradu *Predloga sistema zaštite*) uključuju zahteve za zaštitu i procedure za evaluaciju i testiranje?
- Da li zahtevi dopuštaju modernizaciju zahteva za zaštitu kada se identifikuju nove pretnje/ranjivosti i implementiraju nove tehnologije?
- Ako je ovo kupljena komercijalna aplikacija ili aplikacija koja sadrži komercijalno raspoložive komponente, gde su zahtevi za zaštitu uključeni u specifikaciju za nabavku?

Faza implementacije

- Da li su analiza projekta i testiranje sistema provedeni pre postavljanja sistema u rad? Gde su dokumenta o testiranju? Da li je sistem sertifikovan?
- Da li su kontrole zaštite dodavane od razvoja sistema?
- Da li je aplikacija podvrgnuta tehničkoj evaluaciji da bi se uverili da ispunjava zahteve primenljivih zakona, regulativa, politika, uputstava i standarda?
- Uključiti datum sertifikacije i akreditacije. Ako sistem nije još odobren za rad uključiti datum kada će se napraviti zahtev za akreditaciju sistema.

Faza operativnog rada/održavanja

- Plan zaštite dokumentuje aktivnosti u oblasti zaštiti u ovoj fazi.

Faza odlaganja

- Opisati kako se informacije prenose u drugi sistem, arhiviraju, suspenduju ili uništavaju. Navesti kontrole koje se koriste za obezbeđenje poverljivosti informacija.
- Da li su osetljivi podaci šifrovani?
- Kako se informacije brišu i uklanjaju iz sistema?
- Da li su informacije ili mediji uklonjeni, prepisani, demagnetisani ili uništeni?

Ovlašćeno procesiranje

- Obezbediti datum autorizacije, ime i naslov tela koje je autorizovao sistem.
- Ako nije ovlašćeno, navesti datum, ime i titulu menadžera koji zahteva dozvolu za rad.

III. OPERATIVNE KONTROLE

Personalna zaštita

- Da li su sve radne uloge analizirane za dodelu bezbednosnog nivoa?
- Da li je za svakog pojedinca izvršena bezbednosna provera odgovarajuća ulozi?
- Da li je pristup korisnika smanjen na minimum, neophodan za izvršavanje posla?
- Postoji li proces za zahteve, uspostavljanje, izdavanje i zatvaranje korisničkih naloga?
- Da li su kritične uloge podeljene između različitih lica (princip razdvajanja dužnosti)?
- Koji su mehanizmi na raspolaganju za držanje korisnika odgovornim za njihove akcije?
- Koje su prijateljske, a koje neprijateljske procedure za raskid radnog ugovora?

Fizička i zaštita okruženja

- Opisati fizičku zaštitu sistema, zonu u koji se vrši procesiranje informacija (tj. ključeve na radnim stanicama, fizičke barijere oko zgrade i zone procesiranja itd.).
- Uključiti faktore kao što su PPZ, alternativno napajanje (UPSS, agregat), kolaps strukture, curenje vodovodne mreže, intercepcija podataka, mobilne i portabl sisteme.

Proizvodnja, kontrole I/O (ulaz/izlaz)

Opisati kontrole iskorišćene za označavanje, rukovanje, procesiranje, skladištenje i odlaganje U/I informacija i medija, kao i procedura za označavanje i distribuciju informacija i medija, kontrole korišćene za monitorisanje instalacija, ažuriranje kontrola i korišćeni softver. U ovoj sekciji obezbediti nacrt tekuće procedure koja podržava sistem. Primeri ključnih pitanja koja se moraju navesti u ovoj sekciji su:

- Podrška korisnika – postoji li desk za pomoć ili grupa koja daje savete?
- Procedure koje obezbeđuju da neovlašćeni korisnici ne mogu čitati, kopirati, menjati ili ukrasti odštampanu ili elektronsku informaciju.
- Procedure koje obezbeđuju da samo ovlašćeni korisnici uzimaju, primaju ili isporučuju I/U informacije i medije.
- Registrovani kontrolni tragovi za potvrdu ranjivosti I/U informacija.
- Procedure za restrikciju pristupa izlaznim proizvodima.
- Procedure i kontrole koje se koriste za prenos ili slanje medija ili štampanih izlaznih materijala poštom.
- Interno/eksterno označavanje za osetljivost (npr. DT, SP, Pov, Int i dr.) informacija.
- Spoljno označavanje sa specijalnom instrukcijom za rukovanje (npr. identifikatori za log datoteke/imovinu, kontrolisan pristup, specijalne instrukcije za skladištenje, datum izdavanja ili uništavanja).
- Kontrolni trag za nadzor procesa upravljanja objektima IKT sistema.
- Kontrole/procedure za skladištenje medija.
- Procedure za saniranje elektronskih medija za ponovljeno korišćenje.
- Procedure za kontrolisano skladištenje, rukovanje ili uništavanje pokvarenih i rashodovanih medija ili medija koji ne mogu biti efikasno sanirani za dalje korišćenje.
- Procedure za seckanje ili uništavanje na drugi način štampanog materijala.

Planiranje vanrednih događaja

Kratko opisati procedure (*Plan vanrednih događaja*) kojeg treba slediti da se obezbedi nastavak procesiranja kritičnih aplikacija, ako se dogodi katastrofalni incident. Ako postoji formalan *Plan za vanredni događaj* pozvati se na njega i navesti ga u prilogu. Obraditi sledeća pitanja:

- Navesti svaki sporazum o procesu bekapovanja.
- Dokumentovane procedure za bekapovanje sa uključenom frekvencijom (dnevno, sedmično, mesečno) i obimom (potpuno, delimično, diferencirano bekapovanje).
- Lokacija uskladištenih bekapovanih podataka i informacija i generacije održavanih bekapovanih kopija.
- Da li je sačinjen i testiran *Plan za vanredne događaje*? Kako se često plan testira?
- Da li su svi zaposleni osposobljeni za svoje uloge i odgovornosti u odnosu na hitne slučajeve, katastrofu i druge mere iz plana?

Kontrole za održavanje sistemskog hardvera i softvera

- Restrikcije/kontrole lica koja vrše održavanje i popravke.
- Specijalne procedure za popravke i održavanje u vanrednim prilikama.
- Procedure koje se koriste za delove sistema koji se servisiraju na licu mesta i one koji se servisiraju u dislociranom servisu.
- Procedure koje se koriste za kontrolu servisa za održavanja sa daljine, gde se dijagnostičke procedure i održavanje izvršavaju kroz telekomunikacione kanale.
- Kontrola verzija koja omogućava združivanje komponenti sistema sa odgovarajućim verzijama sistema.
- Procedure za testiranje/ili odobravanje komponenti sistema (OS, drugog sistema, korisničkih alata, aplikacija) pre puštanje u rad.
- Analiza uticaja za određivanje efekata predloženih promena postojećih kontrola zaštite, da bi se uključile obuka tehničkog osoblja i korisnika o promenama.
- Da li su podaci testiranja „živi" podaci ili sačinjeni podaci?
- Postoje li politike organizacije protiv ilegalnog korišćenja kopiranog ili šerovanog softvera?

Kontrole integriteta

- Da li je instaliran softver za detekciju i eliminaciju virusa? Ako jeste, postoje li procedure za ažuriranje datoteka definicija virusa, automatskog/ili manuelnog skeniranja virusa, dezinfekcije i karantizacije i izveštavanja?
- Da li sistem koristi rutine za korekcije, tj. *čeksume*, *heš*, registrovanje zbira? Uključiti opis akcija preduzetih za rešavanje bilo koje neusaglašenosti!
- Da li se koristi *kreker*/*čeker* pasvorda?
- Da li aplikacije koriste programe za verifikaciju integriteta za traženje dokaza proboja?
- Da li je u sistemu instaliran mehanizam za kontrolu/sprečavanje upada u sistem (IDPS)?
- Da li se koriste monitoring sistema i analiza sistemskih log datoteka za traženje problema u realnom vremenu, uključujući aktivne napade ili pad sistema?
- Da li je izvršeno testiranje sistema na proboj? Ako jeste, koje procedure postoje?
- Da li se koristi autentifikacija poruka u sistemu da bi se osigurao integritet poruka?

Dokumentacija

Dokumentacija sistema uključuje opis hardvera i softvera, politike, standarde, procedure i dozvole koje se odnose na automatizovan sistem zaštite IKT sistem, bekapovanje i plan vanrednih događaja, kao i procedure za opis korisnika i operatora.

- Navesti dokumentaciju koja postoji za sistem (dokumentacija isporučioca IKT opreme, funkcionalni zahtevi, plan zaštite, korisnička uputstva za programe, dokumenti o rezultatima testova, procedure i plan vanrednih događaja, korisničke procedure, analize i procene rizika, autorizacije za procesiranje itd.).

Svest o potrebi i obuka

- Program razvoja svesti o potrebi zaštite (posteri, propagandni materijal i sl.).
- Vrsta i frekvencija obuke u opštem sistemu obuke za zaposlene i lica po ugovoru.
- Procedure koje obezbeđuju adekvatnu obuku zaposlenih i lica po ugovoru.

Kapaciteti za upravljanje incidentom

- Postoje li procedure za izveštavanje incidenta kojima rukuju specijalisti zaštite?
- Postoje li procedure za prepoznavanje i upravljanje incidentom?
- Ko prima i odgovara na kompjuterski incident?
- Koje preventivne mere su preduzete, npr. IDPS, automatska log datoteka?

IV. TEHNIČKE KONTROLE

Identifikacija i autentifikacija

Opisati metod autentifikacije korisnika (lozinka, token i biometrijski)! Ako se koristi sistem pasvorda (lozinki), obezbediti sledeće specifične informacije:

- minimum maksimum dužine pasvorda,
- dopušten set karaktera,
- vreme zamene pasvorda i obavezne mere,
- broj generacija pasvorda kojima je istekao rok za upotrebu,
- procedure za promenu pasvorda,
- procedure za rukovanje sa izgubljenim pasvordima,
- procedure za rukovanje sa kompromitovanim pasvordima,
- procedure za obuku korisnika,
- indicirati frekvencije promene pasvorda, opisati kako se nameće obaveza promene pasvorda (npr. softverski ili od strane sistem administratora) i identifikovati ko menja pasvorde (korisnici, sistem ili administrator sistema),
- opisati sve biometrijske kontrole koje se koriste, uključiti opis kako su biometrijske kontrole implementirane u sistem,
- opisati sve korišćene token kontrole u sistemu i kako su implementirane,
- opisati nivo nametanja obaveznih mehanizama za kontrolu pristupa,
- opisati kako AC mehanizam podržava ličnu odgovornost i kontrolni trag za proveru,
- opisati tehnike zaštite mehanizma autentifikacije korisnika (npr. pasvord se prenosi i skladišti i šifruje sa jednosmernom *heš* funkcijom za sprečavanje svakog, uključujući i sistem administratora, da čita otvoren tekst pasvorda, pasvord se generiše automatski, pasvord se proverava sa rečnikom i listom potrošenih pasvorda itd.),
- navesti broj nekorektnih pokušaja pristupa koji se može desiti za dati identifikator korisnika ili lokaciju pristupa i opisati akcije preduzete kada ograničenje istekne,
- opisati procedure za verifikaciju da su svi sistemski obezbeđeni administrativni pasvordi podrazumevano podešeni, promenjeni,
- opisati procedure za ograničavanje pristupa skriptu AC sa ugrađenim pasvordom (npr. ovaj skript je zabranjen ili samo dopušten za *batch* aplikacije),
- opisati politiku za autentifikaciju korisnika (npr. *single-sign-on* tehnologije, *host-to-host*, autentifikacioni serveri, *user-to-host* identifikator, identifikator grupe korisnika) i sve kontrole koje to kompenzuju,
- ako se koristi digitalni potpis (DS), tehnologija mora biti usaglašena sa prihvaćenim standardo, opisati svako korišćenje DS-a.

Logička kontrola pristupa

- Diskutovati postojeće kontrole za autorizaciju i restrikciju korisnika i sistema. Opisati karakteristike projektovanog hardvera ili softvera koji dopušta samo autorizovan pristup sistemu, redukuje ovlašćene transakcije i/ili detektuje neovlašćene aktivnosti!
- Kako su prava pristupa dodeljena? Da li su privilegije bazirane na ulogama?
- Opisati sposobnost sistema da uspostavi ACL ili registar!
- Opisati restrikcije pristupa korisnika resursima sistema koji im nisu neophodni za rad!
- Opisati kontrole za detekciju pokušaja neovlašćenih transakcija od strane ovlašćenih/neovlašćenih korisnika! Opisati sve restriktivne mere koje sprečavaju korisnika da pristupi sistemu ili aplikacijama van normalnog radnog vremena!
- Indicirati period neaktivnosti korisnika sistem kada se automatski briše ekran monitora i/ili nakon sistem automatski isključuje neaktivnog korisnika ili zahteva unošenje jedinstvenog pasvorda pre ponovnog povezivanja na sistem ili aplikaciju!
- Ako se koristi šifrovanje za sprečavanje pristupa osetljivim datotekama, indicirati to kao deo sistema ili procedure za aplikaciju AC!
- Opisati faktore za izbor korišćenja ili nekorišćenja *upozorenja* i obezbediti primer korišćenja upozorenja! Ako je prikladno navesti koje institucije/agencije (Ministarstvo pravde, Zavod za intelektualnu svojinu) odobravaju oznake upozorenja!

Kontrolni tragovi

- Da li ova aktivnost podržava odgovornost obezbeđujući tragove akcija korisnika?
- Da li su tragovi za nadzor i proveru dizajnirani i implementirani da registruju odgovarajuće informacije koje mogu pomoći u detekciji upada?
- Da li tragovi za nadzor i proveru uključuju dovoljno informacija za uspostavljanje odgovora na to kada je i ko izazvao događaj? (Tip događaja, kada se događaj desio, koji je korisnik izazvao događaj, koji je program, ili komandu, koristio da inicira događaj?)
- Da li je *on-line* pristup log datotekama za kontrolu striktno nametnut i propisan?
- Da li je poverljivost podataka kontrolnih tragova zaštićena ako, na primer, sadrži personalne informacije o korisnicima?
- Opisati koliko često se kontrolni tragovi analiziraju i da li za to postoji uputstvo?
- Da li odgovarajući administrator na nivou sistema ili nivou aplikacije pregleda i analizira tragove, sledeći poznati problem sistema ili aplikacije, poznatu povredu postojećih zahteva od strane korisnika ili neki neobjašnjiv sistemski ili korisnički problem?

12.3 PROCEDURA KONTROLE PRISTUPA

1. Cilj
2. Obim i namena
3. Rečnik
   3.1. Definicije, termini i skraćenice
   3.2. Uloge
4. Opis procedure
   4.1. Opšte
   4.2. Odgovornosti
   4.3. Postupci
   4.4. Lista aktivnosti
   4.5. Tok rada
   4.6. Opis aktivnosti
      4.6.1. Aktivnost 1. Zahtevanje prava pristupa
      4.6.2. Aktivnost 2. Analiza zahteva
      4.6.3. Aktivnost 3. Analiza zahteva
      4.6.4. Aktivnost 4. Dodela prava
      4.6.5. Aktivnost 5. Zahtevanje ukidanja prava pristupa
      4.6.6. Aktivnost 6. Ukidanje prava pristupa
5. Zapisi
6. Autorizaciona lista
7. Prilozi

1. CILJ

1.1 Definisanje procedure za servis kontrole prava pristupa (AC) informacionoj imovini *XY organizacije*.

2. OBLAST I NAMENA

2.1 *Procedura kontrole pristupa* ukratko navodi način implementacije bezbednosnih ciljeva kontrole pristupa informacionoj imovini *XY organizacije*. Ova procedura primenjuje se na sve legitimne grupe korisnika sistema (zaposlene, saradnike itd.).

3. REČNIK

3.1 Definicije ključnih termina i skraćenica

Matrica pristupa

Definiše tipove korišćenja objekata IKT sistema. Kreira se na osnovu uloga i odgovornosti grupa korisnika u *XY organizaciji*. Predstavlja trenutno bezbednosno stanje sistema.

3.2 Uloge

Administratori: administratori računarskog sistema.

Komercijalisti: zaposleni u sektoru prodaje i marketinga.
Kancelarijski korisnici: zaposleni u administraciji.
Tim za zaštitu (*InfoSec*): zaposleni specijalisti zaštite informacija.
Razvojni inženjeri: zaposleni u proizvodnom sektoru u domenu razvoja.
Sistem inženjeri: zaposleni u proizvodnom sektoru u domenu IKT infrastrukture i zaštite.
Tehnička podrška: zaposleni u sektoru tehničke podrške.
Menadžment: glavni menadžer, izvršni menadžeri, operativni menadžeri.

4. OPIS PROCEDURE

4.1 Opšte

Servis logičke kontrole pristupa je najstariji servis zaštite informacija i neznatno se menjao od prve primene u *mainframe* i *Unix* računarskim sistemima. Ovaj servis integriše mehanizme *identifikacije* korisnika koji pristupa sistemu na bazi korisničkog naloga, verifikacije identiteta ili *autentifikacije* korisnika na bazi nečega što korisnik *ima* (token, PIN i sl.), *zna* (lozinka ili pasvord) ili što *jeste* (otisak prsta, otisak dlana, otisak mrežnjačke oka, boja glasa i drugi biometrijski parametri). Da bi sistem dao pravo pristupa korisniku mora da u bazi korisničkih naloga ima korisnička imena (korisničke profile), a u bazi autentifikacionih podataka identifikacione parametre za referenciranje tekućih podataka. Pojavom mikroprocesorske *smart* kartične tehnologije gde korisnik sve informacije za logički pristup nosi na smart kartici, uključujući šifarski algoritam i ključeve, stvorena je mogućnost konvergencije servisa logičke i fizičke kontrole pristupa informacionim i fizičkim objektima, odnosno korisnik sa istom karticom ulazi na parking zgrade u kojoj radi, u samu zgrdau, zatim u svoju kancelariju i na kraju se loguje na svoj računar.

4.2 Odgovornosti

- *Administrator sistema* zadužen je za otvaranje i gašenje standardnih korisničkih naloga i za sprovođenje politike koju propisuje *Glavni menadžer zaštite informacija*.
- *Glavni menadžer zaštite informacija* vrši proveru AC i sistema zaštite informacija.
- *Menadžer sistema zaštite informacija* nadležan je za otvaranje i gašenje administratorskih naloga i za arhitekturu sistema koja podržava bezbednosne zahteve menadžmenta.
- *Menadžer XY organizacije*, prema poslovnim potrebama i raspoloživim kapacitetima, obezbeđuje angažovanja ljudi na potrebnim radnim mestima, a njihove potrebe za pristup informacijama usklađuju sa prihvatljivim nivoom rizika.
- *Svi zaposleni XY organizacije* su dužni da na svojim radnim stanicama vode računa o bezbednosti informacija i da izveštavaju sve anomalije i incidente u radu sistema.

4.3 Postupci

- U *XY organizaciji*, procesi identifikacije, autentifikacije i autorizacije zasnivaju se na servisu *Aktivnih direktorijuma*. Zaposleni, prema uputstvu za uvođenje novih zaposlenih u radno okruženje, od prvog radnog dana dobijaju korisnički nalog

koji postaje njihov poslovni identitet. Za ovaj identitet se kroz ISO uputstvo vezuju digitalni sertifikati izdati na smart kartici zaposlenog.

- Smart kartica predstavlja standardni način autentifikacije zaposlenih na sve servise u okviru *XY organizacije*. Kartice se vizuelno personalizuju za svakog korisnika i na njima se, na poleđini, štampa osnovno uputstvo za zaposlene.
- Potreba za korisničkim imenom i lozinkom postoji samo za administratorske naloge i naloge za pristup ERP sistemu *XY organizacije*.

Upravljanje pristupom informacionim servisima kontroliše se primenom mehanizama obezbeđenih kroz *Aktivni direktorijum*. Primenom grupnih *polisa* štite se kako same informacije, tako i servisi koji ih obrađuju. Arhitektura zaštite treba da podržava bezbednosne zahteve navedene u *politici zaštite informacija*, ali i garantuje neophodnu raspoloživost informacija. Svaki zaposleni, u skladu sa ulogama i odgovornostima, ima potrebu za određenim nivoom privilegija. Klasifikacija zaposlenih prema pravu pristupa data je u matrici pristupa (tabela 12.1) i listi pristupa (tabela 12.2).

Tabela 12.1 *Matrica pristupa*

GRUPE KORISNIKA	PRAVO PRISTUPA					
	Lokalna radna stanica	Razvojni server	Testni serveri	Produkcioni serveri	VPN pristup	Portali preduzeća
Uprava preduzeća	Admin prava	Bez prava	Bez prava	Bez prava	Korisnička prava	Korisnička prava na svim portalima preduzeća
Razvojni inžinjeri	Admin prava	Admin prava	Admin prava	Bez prava (na specijalan zahtev rukovodioca, samo za određene servise)	Prema poslovnim potrebama	Korisnička prava na portalu razvoja na TFS serveru i eDRMS
Sistem inžinjeri	Admin prava	Admin prava	Admin prava	Admin prava	Prema poslovnim potrebama	Korisnička prava na portalu IZ i Portalu za upravljanje sistemskom dokumentacijom, kao i na eDRMS
Komercijalisti	Admin prava	Bez prava	Bez prava	Bez prava	Bez prava	Korisnička prava na portalu komercijale i eDRMS
Office korisnici	Admin prava	Bez prava	Bez prava	Bez prava	Bez prava	Bez prava osim na eDRMS
Administratori sistema	Admin prava	Admin prava	Admin prava	Admin prava	Admin prava	Admin prava
	Admin prava	Bez prava	Bez prava	Korisnička prava na određenim servisima	Bez prava	Bez prava osim na eDRMS

4.4 Lista aktivnosti

Tabela 12.2 Lista pristupa (ACL)

ID	Aktivnost	Odgovorno lice	Ulazi	Izlazi
1	Zahtevanje prava	Zaposleni preduzeća	Potrebe poslovanja	Usmeno obaveštenje rukovodioca odeljenja o potrebnim pravima
2	Analiza zahteva	Rukovodilac odeljenja	Zahtevana prava, potrebe poslovanja	Usmeno obaveštavanje rukovodioca IKT odeljenja i odeljenja zaštite o potrebnim pravima Ili Obaveštavanje zaposlenog o odbijanju
3	Analiza zahteva	Rukovodilac Odeljenja Infrastrukture i zaštite	Zahtevana prava, potrebe poslovanja, arhitektura sistema	Usmeno izdavanje radnog naloga administratoru Ili Obaveštenje rukovodiocu odeljenja o odbijanju
4	Dodela prava	Administrator sistema	Zahtevana prava, arhitektura sistema	Obaveštavanje zaposlenog o dodeli prava
5	Zahtevanje ukidanja prava	Rukovodilac odeljenja	Potrebe poslovanja	Usmeno obaveštavanje rukovodioca odeljenja zaštite o potrebi ukidanja prava
6	Ukidanje prava	Administrator sistema	Zahtevana prava, arhitektura sistema	Obaveštavanje zaposlenog o ukidanju prava
7				

5. PROCEDURA KONTROLE PRISTUPA

5.1 Tok aktivnosti procedure

Aktivnost 1. Zahtevanje prava pristupa

- Svaki zaposleni, na osnovu trenutnih poslovnih potreba, ima pravo da zahteva pristup dodatnim resursima i dužan je da, usmenim obaveštavanjem rukovodioca svog odeljenja, pokrene proces dodele potrebnih prava pristupa.
- *Matrica pristupa* prikazana u tabeli 13.1 predstavlja opštu arhitekturu privilegija zaposlenih u *organizaciji XY*. Dinamika poslovanja postavlja zahteve za povremenim odstupanjem od ovakve arhitekture.

Aktivnost 2. Analiza zahteva

- Rukovodilac odeljenja obavezan je da po prijemu zahteva analizira opravdanost i ukoliko zaključi da je zahtev bez osnove, obavesti zaposlenog o odbijanju.
- Prihvaćene zahteve rukovodilac odeljenja saopštava menadžeru odeljenja infrastrukture i zaštite.

Aktivnost 3. Analiza zahteva

- *Glavni menadžer zaštite*, uz obavezne konsultacije sa izvršnom menadžerskom strukturom, dužan je da analizira uticaj zahtevane primene prava na bezbednost IKT sistema. Ukoliko dođe do zaključka da zahtevana prava narušavaju bezbednost sistema on odbija zahtev i o tome obaveštava rukovodioca odeljenja. Ukoliko je rukovodilac odeljenja nezadovoljan odlukom, on ima pravo da od glavnog menadžmenta zahteva reviziju odluke. Menadžment zadržava diskreciono pravo da odobri zahtev.
- Ukoliko se kroz analizu pokaže da zahtev za dodelu prava pristupa ne narušava bezbednost sistema, menadžer odeljenja zaštite izdaje usmeni radni nalog administratoru sistema.

Aktivnost 4. Dodela prava pristupa

- *Administrator sistema,* poštujući postojeće procedure, dodeljuje tražena prava zaposlenom i obaveštava zaposlenog o novim pravima.

Aktivnost 5. Zahtevanje ukidanja prava pristupa

- Menadžeri organizacionih jedinica dužni su da vrše periodično preispitivanje poslovnih potreba zaposlenih u svom sektoru i vode računa o nivou privilegija koje su trenutno potrebne. Cilj ovakve periodične provere je održavanje principa minimalnih privilegija. O svakoj uočenoj nepravilnosti (npr. potrebno je ukinuti određena prava) informiše se menadžer odeljenja zaštite koji administratoru sistema delegira zadatak za ukidanja prava pristupa.

Aktivnost 6.Ukidanje prava pristupa

- *Administrator sistema*, poštujući postojeće procedure, sprovodi proces ukidanja prava zaposlenom i obaveštava zaposlenog o novim pravima.

Zapisi

RB	Šifra zapisa	Naziv zapisa	Obrazac
1			
2			

Autorizaciona lista

Na dokument ove procedure primenjuje se autorizacija navedena u katalogu dokumenata za klasu procedura.

RB	Korisnik ili grupa korisnika	Prava
1		☐ Čitanje ☐ Menjanje ☐ Sva prava ☐ Zabrana
2		☐ Čitanje ☐ Menjanje ☐ Sva prava ☐ Zabrana

Prilozi:

12.4 PROCEDURA INTERNE PROVERE ISMS-a

Verzija: 1 – NACRT ~~/ KONAČNI NACRT / ODOBRENO~~
Dokument broj:
Autor: ggrubor@singidunum..ac.rs
Datum objavljivanja: 1.12.2011.
Izmenjeno od strane: _____

Politiku odobrava:	**Datum odobrenja:**

Istorijat dokumenta:

Verzija	Datum	Autor	Opis dorade
1	1.12.2011	Gojko Grubor	Nacrt

1.0 Cilj	1.1 Da se osigura da *organizacija x* stalno posluje u skladu sa određenim propisima, procedurama i eksternim zahtevima kako bi ispunila svoje ciljeve u oblasti informacione bezbednosti. 1.2 Da se osigura identifikovanje i primena poboljšanja u oblasti ISMS-a, kao i da se utvrdi njihova prihvatljivost za ostvarenje ciljeva.
2.0 Obim i namena	Ova procedura obuhvata planiranje, izvršenje, izveštavanje i naknadno praćenje interne ISMS provere i primenjuje se na sve odeljenja koja su deo menadžment sistema bezbednosti informacija u *organizaciji x*.
3.0 Uloge i odgovornosti	3.1 Menadžer za informacionu bezbednost (MIB) ◆ Imenuje glavnog proveravača i tim za proveru. Glavni proveravač može da bude i MIB. ◆ Zajedno sa glavnim proveravačem ispituje korektivne i preventivne aktivnosti i naknadne provere na osnovu dostavljenog izveštaja o unutrašnjoj kontroli. ◆ Rezultate provere čuva poverljivim. 3.2 Glavni proveravač ◆ Priprema *obaveštenje o proveri* kao osnovu za plan provere i kako bi se upoznali svi zaposleni. ◆ Rukovodi aktivnostima interne provere. ◆ Koordinira dinamiku provere sa izvršnim menadžerima. ◆ Planira proveru, priprema radna dokumenta i informiše tim proveravača. ◆ Sjedinjuje sve rezultate i opservacije provere i priprema izveštaj o internoj proveri. ◆ Kritična neslaganja odmah prijavljuje onima nad kojima je provera sprovedena. ◆ Dostavlja rezultate jasno i bez odlaganja onima nad kojima je vršena provera. ◆ Vodi uvodni i završni sastanak.

	3.3 Tim proveravača ◆ Pomaže delatnosti glavnog proveravača. ◆ Vrši proveru koristeći konsolidovanu *kontrolnu listu provere/ obrazac za opservacije*. ◆ Izveštava o neslaganjima i daje preporuke za poboljšanje. ◆ Štiti poverljivost rezultata provere. ◆ U svakom trenutku deluje u skladu sa etičkim normama. 3.4 Proveravani entitet/zaposleni ◆ Primaju izveštaj i odlučuju o o proveri, pokreću i naknadno prate korektivne aktivnosti.
4.0 Procedura	
4.1 Opšte	4.1.1 *Program provere* pravi se tako da sadrži sve zakazane i moguće provere tokom cele kalendarske godine. Ovo uključuje i raspored internih provera, provera dobavljača, provera koje vrše klijenti i nezavisnih provera izvršenih od strane TTP. 4.1.2 Interna provera se planira dva puta godišnje ili po potrebi. 4.1.3 Internu proveru vrši izabrani tim za proveru. 4.1.4 Sve članove tima proveravača imenuje MIB. 4.1.5 Glavni proveravač nadgleda rad tima proveravača. 4.1.6 Obaveštenje o proveri unapred se šalje odeljenima u kojima će biti izvršena provera, barem tri (3) radna dana pre same provere.
4.2 Planiranje i priprema provere	4.2.1 Glavni proveravač priprema godišnji *program provera*, a glavni menadžer ga odobrava. Program je podložan izmenama u skladu sa promenama dinamike provere. 4.2.2 Na osnovu ovog programa glavni proveravač priprema planove pojedinačnih provera. 4.2.3 Glavni proveravač priprema plan provere/obaveštenje, a MIB vrši proveru i odobrava isti. Plan se saopštava ostalim proveravačima i onima koji će biti proveravani i treba da bude fleksibilan kako bi se mogle uneti promene nastale na osnovu informacija prikupljenih tokom provere. Plan obuhvata: ◆ cilj, obim i namenu provere, ◆ odeljenja i odgovorne pojedince, ◆ članove time proveravača, čiji broj zavisi od obima provere, ◆ tip menadžment sistema nad kojim se vrši provera i ◆ datum, mesto, vreme provere i datum objavljivanja izveštaja o proveri.
4.3 Sastanak pre početka provere	Sastanak pre početka provere, na kome učestvuju MIB, glavni proveravač i proveravači, mora da se održi najkasnije jedan dan pre početka provere. Ciljevi sastanka su sledeći: ◆ da se osigura raspoloživost svih neophodnih resursa i ostale logistike koja može da bude potrebna proveravačima i ◆ obim provere verifikuje se na osnovu *Plana provere*.
4.4 Uvodni sastanak	U slučaju da MIB i glavni proveravač to smatraju prikladnim, uvodni sastanak se može održati na dan provere, ali pre početka same provere. Na uvodnom sastanku mogu se razmatrati sledeća pitanja: ◆ cilj i obim provere, ◆ potvrđivanje *Plana provere i* ◆ razjašnjenje svih pitanja pre početka provere.
4.5 Provera	Proveravači vrše unutrašnju proveru koristeći nekoliko kontrolnih lista: ◆ *Kontrolna lista za internu proveru* (*čeklista*) sadrži posebne stavke specifične za organizacionu jedinicu u kojoj se provera sprovodi. Imenovani proveravači odgovorni su da postavljaju pitanja koristeći ovaj obrazac. ◆ *Kontrolna lista sa standardnim zahtevima* sadrži zahteve date u ISO/IEC 27001:2005 standardu. ◆ *Kontrolna lista za neophodne kontrole zaštite* sadrži zahteve za kontrole zaštite date u Aneksu A u ISO/IEC 27001:2005.

4.5 Provera (nastavak)	Rezultati provere prikupljaju se na osnovu intervjua, pregleda dokumentacije i opservacija aktivnosti i uslova u oblastima od interesa i zapisuju se na gore pomenute kontrolne liste. Dokaze koji ukazuju na neslaganja treba zabeležiti ukoliko se čine bitnim, čak i ako nisu pokriveni sadržajem *kontrolnih lista*. Ostale objektivne dokaze i/ili opservacije koje se pozitivno ili negativno mogu odraziti na menadžment sistem bezbednosti informacija treba zabeležiti na predviđenom mestu na kontrolnim listama.
4.6 Izveštaj o proveri	4.6.1 Proveravači moraju da održe sastanak nakon provere sa sledećim dnevnim redom: ◆ Pregled i analiza rezultata. ◆ Konsolidacija svih rezultata uključujući i grupisanje i tabelarno prikazivanje. ◆ Klasifikacija rezultata. ◆ Priprema preporuka i izveštaja o proveri. ◆ Klasifikacija rezultata (videti ispod 4.6.4). ◆ Priprema preporuka i izveštaja o proveri. 4.6.2 Proveravački tim pregleda sve svoje rezultate bilo da ih u izveštaju vode kao neusaglašenosti ili opservacije. Rezultati provere moraju da budu podržani objektivnim dokazima. 4.6.3 Glavni proveravač vrši konsolidaciju svih rezultata za izveštaj o proveri. 4.6.4 Klasifikacija rezultata može biti: ◆ **Glavne neusaglašenosti** se odnose na glavni nedostatak ISMS-a i na situaciju kada jedan ili više zahtevanih elemenata iz ISO 27001 nije primenjen. Neusaglašenosti imaju direktni uticaj na informacionu bezbednost, posebno na očuvanje CIA informacija. ◆ **Manje neusaglašenosti** su manji nedostaci, kada su jedan ili više elemenata ISMS-a samo delimično zadovoljeni i imaju indirektan uticaj na bezbednost informacija. **Primedba:** *Kako glavne, tako i manje neusaglašenosti, zahtevaju da se na odgovarajućem obrascu dokumentuju korektivne akcije.* ◆ **Moguća poboljšanja** su predlog poboljšanja koja proveravana strana može, ali ne mora primeniti. **Primedba:** *mogućnosti za poboljšanja koje se odnose na nedostatke informacione bezbednosti zahtevaju da preventivne akcije budu dokumentovane na odgovarajućem obrascu.* ◆ **Pozitivni rezultati** se odnose na procese i/ili sisteme koji prevazilaze ono što ISMS standard zahteva. ◆ 4.6.5 Glavni proveravač priprema standardni *izveštaj o internoj proveri* koji sadrži sledeće podatke: ◆ referentni broj provere, ◆ datum provere, ◆ proveravački/procesni naziv odeljenja, ◆ naziv proveravanih organizacionih jedinica/procesa i proveravača, ◆ izjava o rezultatima (sve nađene neusaglašenosti), ◆ referenca na ISMS standard, ◆ korektivne i preventivne akcije sa datumom završetka, ◆ naknadna praćenja neusaglašenosti i ◆ potvrda naknadnih aktivnosti. 4.6.6 Proveravači poštuju kodeks ponašanja kada je u pitanju izveštavanje kao što je navedeno u ovom dokumentu. ◆ Izveštaj treba da bude koncizan, ali istinit i prezentovan na konstruktivan način. ◆ Rezultati treba da budu u okviru obima provere i da prikazuju odnose prema korišćenim standardima. ◆ Pojedinačni proveravač ne sme da izveštaj učini pristrasnim.

4.6 Izveštaj o proveri (nastavak)	4.6.7 Glavni proveravač izdaje formalni izveštaj o proveri MIB-u (ukoliko MIB nije glavni proveravač). 4.6.8 Prvobitni izveštaj o proveri održava i kontroliše MIB u skladu sa *Procedurom kontrole podataka***.**
4.7 Završni sastanak	◆ Glavni proveravač predsedava završnim sastankom kome prisustvuju tim proverivača i oni koji su proveravani. ◆ Proveravači ne izveštavaju o svojim saznanjima, opservacijama i preporukama. ◆ Proveravači prvo iznose pozitivne rezultate pa onda navode neusaglašenosti. ◆ Obe strane čuvaju poverljivost izveštaja o internoj proveri. ◆ Razrešavaju se sva pitanja i daju se svi odgovori.
4.8 Naknadne korektivne akcije	4.8.1 Proveravač je odgovoran samo za određivanje neusaglašenosti. 4.8.2 Proveravane strane su odgovorne za ispravku prijavljenih neusaglašenosti. 4.8.3 Odobrene korektivne akcije se zasnivaju na dogovorenom vremenskom periodu. 4.8.4 Glavni proveravač sprovodi naknadnu proveru kako bi proverio primenu korektivnih akcija navedenih u izveštaju o *Neusaglašenostima/korektivnim i preventivnim akcijama* ili u odgovarajućem obrascu. Obično to usledi nakon provere. Učestalost naknadnih kontrola zavisi od rezultata provera. 4.8.5 Glavni proveravač sprovodi drugu naknadnu proveru da bi proverio efektivnost ustanovljenih korektivnih ili preventivnih akcija. Druga naknadna provera se sprovodi između tri (3) i četiri (4) meseca od datuma implementacije nalaza u 4.8.4 proveri. 4.8.6 Glavni proveravač izdaje novi obrazac ako korektivne akcije: - nisu primenjene do predviđenog datuma (vidi 4.8.4), - nisu efektivne (vidi 4.8.5). 4.8.7 U koloni „*Obnovljeno izdanje*“ u obrascu za proveru beleži se bilo koja od situacija iz stavke 4.8.6, ukoliko postane očigledna.
4.9 Naknadno praćenje provere	4.9.1 MIB se sastaje sa proveravačima i preuzima sveukupnu odgovornost za aktivnosti naknadnog praćenja rezultata provere koje se objavljuju u dogovoru sa kontrolisanim odeljenjem/procesom. Aktivnosti naknadnog praćenja ne smatraju se potpunim dok sve korektivne akcije ili mere ne budu sprovedene i dok izveštaj o statusu ne bude podnet glavnom proveravaču.
4.10 Kvalifikacije proverivača	4.10.1 **Lični atributi:** proveravač treba da poseduje sledeće lične atribute kako bi bio sposoban da deluje u skladu sa principima najbolje prakse provere, tj. treba da bude: a) *etičan*, tj. pravičan, istinoljubiv, iskren, pošten i diskretan; b) *otvorenog uma*, tj. voljan da razmotri alternativne ideje; c) *diplomata*, tj. taktičan u odnosu sa ljudima; d) *proniclјiv*, tj. stalno svestan svog fizičkog okruženja i delatnosti; e) *dobar posmatrač*, tj. da instinktivno bude svestan situacija i da iste može i da razume; f) *svestran*, tj. da se prilagođava različitim situacijama; g) *posvećen*, tj. istrajan, fokusiran na ostvarenje ciljeva; h) *odlučan*, tj. da na vreme donosi zaključke zasnovane na logičnom rezonovanju i analizi, i) *samouveren*, tj. da deluje i funkcioniše nezavisno dok istovremeno efikasno sarađuje sa drugima.

4.10 Kvalifikacije proveravača (nastavak)	4.10.2 **Opšte znanje i veštine** koje jedan ISMS proveravač treba da poseduje su iz sledećih oblasti: a) **principi, procedure i tehnike provere:** da bi ih proveravač adekvatno primenjivao tokom različitih provera i da bi bio siguran da se provere sprovode na konzistentan i sistemski način, proveravač bi trebalo da bude sposoban da: ◆ primeni principe, procedure i tehnike provere, ◆ efikasno planira i organizuje posao, ◆ proveru sprovede u predviđenom vremenskom roku, ◆ odredi prioritete i da se fokusira na bitne stvari, ◆ prikupi informacije efektivnim intervjuima, opservacijama i pregledom dokumenata, beležaka i podataka, ◆ razume prikladnost i posledice upotrebe uzornih tehnika prilikom provere, ◆ proveri tačnost prikupljenih informacija, ◆ potvrdi kompletnost i prikladnost dokaza iz provere, potrebnih da podrže rezultate i zaključke provere, ◆ proceni faktore koji mogu da utiču na pouzdanost provere, ◆ koristi radnu dokumentaciju za evidenciju aktivnosti provere, ◆ pripremi izveštaje o proveri, ◆ sačuva poverljivost i bezbednost informacija i ◆ da efikasno prenese poruku, koristeći lične lingvističke veštine ili uz pomoć prevodioca. b) **Menadžment sistem i referentna dokumenta:** da bi proveravač mogao da shvati obim i primeni kriterijum tokom provere, treba da pokriva sledeća znanja i veštine u ovoj oblasti: ◆ interakciju između segmenata menadžment sistema, ◆ ISMS standarde, procedure koje se mogu primeniti ili druga dokumenta koje se mogu koristiti kao kriterijumi za proveru, ◆ uočavanje razlika i prioriteta referentnih dokumenata, ◆ primenu referentnih dokumenata na različite situacije tokom provere i ◆ IKT sisteme i tehnologije za autorizaciju, bezbednost, distribuciju i kontrolu dokumenata, podataka i beležaka. **c)** **Organizacione situacije:** da bi proveravač mogao da shvati operacioni kontekst organizacije, treba da pokriva sledeća znanja i veštine u ovoj oblasti: ◆ veličinu, strukturu, funkcije i odnose u organizaciji, ◆ opšte poslovne procese i srodnu terminologiju i ◆ kulturološke i društvene navike proveravanih entiteta. d) **Relevantni zakoni**, **propisi i ostali zahtevi bitni za organizaciju**: da bi proveravač mogao da bude svestan i da radi u skladu sa propisima koji se primenjuju na organizaciju koja se kontroliše, treba da pokriva sledeća znanja i veštine u ovoj oblasti: ◆ lokalne, regionalne i državne zakone i propise, ◆ ugovore i sporazume, ◆ međunarodne sporazume i konvencije i ◆ ostale zahteve koje organizacija treba da ispuni.

4.11 Kvalifikacije glavnog proveravača	4.11.1 **Opšte znanje i veštine glavnog proveravača ISMS-a** Vođe tima proveravača treba da poseduju dodatno znanje i veštine iz oblasti menadžmenta provere, da bi obezbedio efikasno i efektivno sprovođenje provere i da je sposoban da: ◆ planira proveru i koristi resurse na najefikasniji način, ◆ predstavi tim proveravača proveravanom entitetu, ◆ organizuje i usmerava članove tima proveravača, ◆ usmeri i predvodi proveravače pripravnike, ◆ predvodi proveravački tim u donošenju zaključaka provere, ◆ spreči i reši nastale konflikte i ◆ da pripremi i završi izveštaj o proveri. 4.11.2 **Posebna znanja i veštine ISMS proveravača** Proveravači menadžment sistema bezbednosti informacija treba da poseduju znanje i veštine iz sledećih oblasti: **a) metodi i tehnike koje se odnose na informacionu bezbednost**: da bi proveravač mogao da pregleda menadžment sistem bezbednosti informacija i da bi stekao odgovarajuća saznanja i zaključke o situaciji, treba da pokriva sledeća znanja i veštine u ovoj oblasti: ◆ terminologiju informacione bezbednosti, ◆ principe menadžmenta informacione bezbednosti i njihove primene i ◆ alate za menadžment informacione bezbednosti i njihovu primenu; **b) procesi i proizvodi, uključujući i usluge**: da bi proveravač mogao da shvati tehnološki kontekst u kome se sprovodi provera, treba da pokriva sledeća znanja i veštine u ovoj oblasti: ◆ terminologiju specifičnu za industriju, ◆ tehničke karakteristike procesa i proizvoda uključujući i usluge, kao i procese i prakse specifične za industriju.
5.0 Podaci i dokumenta provere	*Program provere* *Plan provere/obaveštenja* *Kontrolne liste za proveru/obrasci za opservacije* *Kontrolne liste za standardne sistemske zahteve* *Kontrolne liste za zahtevane kontrole zaštite* *Izveštaj o internoj proveri* *Izveštaj o neusaglašenostima/korektivnim i preventivnim akcija* *Izveštaj o naknadnoj proveri*

13.5.1 Preporučena lista pitanja za internu proveru sistema zaštite

Lista obaveznih pitanja koja treba da razmatra tim organizacije za internu proveru sistema zaštite u programu godišnje provere:

- politike fizičke i logičke zaštite,
- odgovornosti i nalozi za nametanje politike zaštite,
- robusnost procesa analize rizika, posebno za ključne objekte zaštite,
- usaglašenost sa politikom kontrole pristupa i upravljanja ovlašćenjima za pristup,
- autentifikacija,
- lista kodiranja i označavanja klasifikovane imovine, konfiguracija sistema zaštite i upravljanje promenama,
- kontrolne sesije protokola zaštite,
- politika zaštite mreža,
- politika pristupa Internetu,
- kriptografske tehnologije za prenos i skladištenje,
- politika daljinskog pristupa mreži.
- jasan sistem administracije procesa i procedura,
- upravljanje kompjuterskim incidentom i izveštavanje,
- sistem internog nadzora i provere,
- kapaciteti za antivirusnu zaštitu i druge DoS (*Denial of Services)* napade,
- bekapovanje,
- održavanje,
- identifikacija informacija i upravljanje informacijama,
- sanacija i arhiviranje medija,
- fizička zaštita,
- personalna zaštita,
- obuka i nivo svesti o potrebi zaštite,
- usklađenost sa primenjivim standardima u zakonima,
- upravljanje vanrednim događajem i kontinuitetom poslovanja.

13.

PRILOZI

PRILOG 6.1: Projektna dokumentacija implementacije ISMS-a

Dokumentacija koja podržava strukturu projekta namenjenog za implementaciju ISMS-a:

- tok procesa implementacije i sertifikacije ISMS-a
- definicija obima ISMS-a
- ISO/IEC 27002 upitnik/Izveštaj o analizi razlika (*Gap Analysis Report*)
- predlog za implementaciju ISMS-a
- plan implementacije ISMS-a
- plan tretmana rizika (kako će biti ublažen preveliki rizik))
- saopštenje o primenljivosti – SOA (*Statement of Applicability*)
- inicijative/dnevni red/odobrenja odeljenja Foruma za zaštitu informacija
- strategija upravljanja rizikom/pristup/metodologija
- ISMS Organizacija (dijagram organizacione strukture ključnih uloga, odgovornosti, linija izveštavanja)
- rečnik termina zaštite informacija (hiperlinkovani *online* dokument)
- smernice i metrika za implementaciju ISMS-a (sa idejama i savetima za implementatore)
- metrika zaštite informacija (skup uzoraka za razmišljanje).

ISMS POLITIKA ZAŠTITE INFORMACIJA

Saopštenja politika zaštite koja pokrivaju različite aspekte informacione bezbednosti (referenca: ISO/IEC 27002 – nije konačna):

- politika bezbednosti informacija (na nivou organizacije),
- politika menadžment sistema zaštite informacija – ISMS politika i
- politika komponente sistema zaštite.

1. Politika kontrole pristupa
2. Politika razvoja svesti o potrebi zaštite i obuka o zaštiti
3. Politika za upravljanje rizikom
4. Politika upravljanja životnim ciklusom sistema zaštite
5. Politika prihvatljivog ponašanja
6. Politika zaštite informacija i podataka na komunikacijama
7. Politika upravljanja vanrednim događajem
8. Politika upravljanja kompjuterskim incidentom
9. Politika sakupljanje i održavanja kontrolnih tragova (*Audit trails*)
10. Politika usaglašenosti i odgovornosti
11. Politika sertifikacije i akreditacije
12. Politika čistog stola i ekrana
13. Politika arhiviranja i zadržavanja podataka
14. Politika klasifikacije informacija
15. Politika odlaganje informacija/medija/opreme
16. Politika zaštite e-poslovanja
17. Politika prihvatljive upotrebe e-pošte
18. Politika procene rizika bezbednosti informacija
19. Politika zaštite laptop (mobilnih) računara
20. Politika mobilnog i rada sa daljine
21. Politika upotrebe iznajmljenih resursa (*outsourcing*)http://www.iso27001security.com/ISO27k_model_policy_on_outsourcing.doc
22. Politika upravljanja pasvordom
23. Politika testiranja sistema na proboj
24. Politika personalne zaštite
25. Politika fizičke zaštite
26. Politika zaštite privatnosti
27. Politika upotrebe licencnog softvera
28. Politika antispam zaštite
29. Politika bekapovanja i oporavka sistema/podataka
30. Politika monitoringa upotrebe sistema
31. Politika pristupa treće strane
32. Politika zaštite od virusa/malicioznih programa itd.

RELEVANTNI STANDARDI ZAŠTITE

Standard	Namena
ISO/IEC 27001	Smatra se fundamentalnim standardom zaštite informacija jer definiše bazični gradivni i kontrolni ISMS-a; ovaj se standard zaštite sertifikuje.
ISO/IEC 27002 (ISO/IEC 7799)	Ovaj standard daje detaljan opis implementacije kontrola zaštite i aplicira se u fazi implementacija (*PDCA Do* faza) ISO 27001.
ISO/IEC 27003: 2010	Fokusiran na kritične aspekte potrebne za uspešno projektovanje i implementaciju ISMS-a usaglašenu sa ISO/IEC 27001:2005.
ISO/IEC 27004	Obezbeđuje smernice za razvoj i upotrebu metrika i merenja za procenu efektivnosti implementiranog ISM-a i kontrola zaštite specifikovanih u Aneksu A ISO/IEC 27001.
ISO/IEC 27005	Specificira metode za procenu i tretman bezbednosnog rizika i koristi se u PDCA fazi planiranja implementacije ISO/IEC 27001 standarda.

Standard	Namena
BS 7858:2006+ A2:2009	Ovaj standard daje preporuke za bezbednosnu proveru lica za rad u okruženju, gde je vrlo važna bezbednost ljudi, imovine i informacija ili je to u javnom interesu.
BS 25999-1	Daje smernice za implementaciju elemenata kontinuiteta poslovanja.
BS 25999-2	Smatra se fundamentalnim standardom kontinuiteta poslovanja, koji definiše osnove razvoja *sistema menadžmenta kontinuiteta poslovanja* (BCMS). Ovaj se standard zaštite sertifikuje i koristan je u *PDCA Do* fazi za implementaciju zahteva, datih u of Aneksu A, poglavlje 14 (BCM) ISO/IEC 27001 standarda.
ISO/IEC 24762:2008	Međunarodni standard koji daje smernice za servise oporavka informacija i komunikacija posle pada sistema, kao deo BCM-a.
BS 25777:2008	Standard najbolje prakse menadžmenta kontinuiteta IKT sistema, koji podržava ukupne procese menadžmenta kontinuiteta poslovanja (BCM) organizacije.
PD 25111:2010	Smernice za humani aspekt BCM-a, za planiranje strategije razvoja ljudskih resursa i politike za ključne faze aktivnosti posle pad sistema, koje se odnose na neposredne efekte incidenta do oporavka normalnih operacija.
PD 25666:2010	Opšte smernice za BCM simulacije i testiranja ključnih programa za nastavak poslovanja, uključujući i aranžman za IKT sistem.
NIST SP 800-55	Opisuje detaljno kontrole zaštite i merenje njihove efektivnosti.
NIST SP 800-61	Opisuje menadžment kompjuterskog incidenta, kao deo ISMS-a.
COBIT 4.1 (2007)	Opšte prihvaćeni ciljevi kontrola IT-a.
ITIL v.3 (international)	*IT Infrastructure Library* – globalni standard u oblasti menadžmenta servisa koji sadrži sveobuhvatnu javno dostupnu specijalističku dokumentaciju za planiranje resursa i IKT servisima.
ISO/IEC 27031	Smernice za spremnost IKT sistema za kontinuitetet poslovanja; verovatno će zameniti BS25777 standard.
ISO/IEC 27035	Menadžment sistem bezbednosnog incidenta.
ISO 31000:2009	Obezbeđuje principe i generičke smernice za menadžment rizika.
ISO/IEC 38500:2008	Ovaj standard obezbeđuje vodeće principe za direktore organizacija za efektivnu, efikasnu i prihvatljivu upotrebu menadžment procesa IKT sistema u organizaciji, koje mogu kontrolisati specijalisti ili poslovne jedinice organizacije ili TTP.
NFPA 1600	Standard o menadžmentu vanrednih događaja i programa kontinuiteta poslovanja.
PAS 200:2011	Ovaj standard je dizajniran da pomogne organizacije da preduzmu praktične korake za poboljšanje kapaciteta za menadžment kriza i održivi razvoj.

Korisni linkovi:

- International Organization for Standardization
- The British Standards Institution
- National Institute of Standards and Technology - Special Publications (800 Series)

TIPIČNE PROCEDURE ZA ZAŠTITU INFORMACIJA

Dokumentuju procese za implementaciju kontrola zaštite.

- Procedura bekapovanje
- Procena usklađenosti i *provera* procedura (npr. pomoću *CISCO router security audit procedure*)
- Procedura za izveštavanje o incidentu
- Procedura za reviziju logičke kontrole pristupa
- Procedura za upravljanje bezbednosnim zakrpama
- Procedura za administraciju zaštite računarskog sistema
- Procedura za poboljšavanja sistema zaštite
- Procedura za testiranje sistema zaštite
- Korisnička procedura za održavanje sistema zaštite
- Procedure za upravljanje sistemom zaštite
- Smernice za procese upravljanja sa ISMS u celini
- Procedura za korektivne/preventivne akcije
- Procedura za registrovanje i dokumentovanja kontrolnih tragova (revizija dokumenta zaštite, vlasništvo, autorizacije upravljanja, kontrole promena)
- Procedura interne kontrole (*audit*) ISMS
- Materijali za razvoj svesti o potrebi zaštite (posteri, brifinzi, smernice, saveti itd.) po različitim temama zaštite, usmerenim na ciljne grupe
- Uputstvo za *auditing* ISMS
- Procedura za upravljanje rizikom
- Radna tabela za analizu rizika bezbednosti informacija (procena vrednosti imovine, pretnji, ranjivosti i uticaja)
- Pomoćni programski alat za procenu rizika (*Hestia, Cobra, CRAMM* itd.)

OPIS PROFILA ZAPOSLENIH U ZAŠTITI INFORMACIJA (ORGANIZACIJA ISMS-a)

Uloge, odgovornosti, kompetencije itd. za poslove koji se odnose na ISMS

- Uloge za planiranje vanrednog događaja i oporavak sistema
- Vlasnik informacione imovine
- Analitičar informacione bezbednosti
- Projektant sistema zaštite informacija
- Menadžer sistema zaštite informacija (GISO)

- Referent (specijalista) za zaštitu informacija (ISO)
- Specijalista za ispitivanje (testiranje) sistema zaštite
- Proveravač sistema zaštite (*auditor*)
- Administrator sistema zaštite.

OPERATIVNI ARTEFAKTI ISMS-a

Formalne evidencije koje se generišu kao rezultata ISMS.

- Plan kontinuiteta poslovanja (BCP)
- Kontrolna lista za procenu uticaja na poslovanje i sistem izveštavanja
- Plan za oporavak IKT sistema
- Obrasci za izveštavanje o bezbednosnom incident i izveštaji o značajnijim incidentima
- Lista za proveru revizija rešenja dizajna i arhitekture (za razvoj softvera)
- Taksonomije pretnji i ranjivosti/liste za proveru/upitnici/izveštaji

ISMS REGISTRI (EVIDENCIJE)

- Liste ili baze podataka informacione imovine u ISMS
- Registar medija za bekapovanje i arhivu (detaljni spisak traka/diskova/CD/DVD, tipova bekapa, obima bekapovanje – moguće automatizovanog)
- Registar BCP (detalji o svim BCP planovima, sa statusom, vlasništvom, obimom, poslednjim testiranjem itd.)
- Registar/baza podataka inventara informacione imovine
- Registar faktora bezbednosnog rizika (ime rizika, vlasnik rizika, priroda rizika, odluka menadžmenta za redukciju/transfer/izbegavanje/prihvatanje rizika
- Registar incidenata informacione bezbednosti (može se derivirati iz internog portala za pomoć u IKT i servisiranje, iz izveštaja o incidentima logova bezbednosnih događaja i sl.)
- Lista administratorskih, privilegovanih i korisničkih prava pristupa i ovlašćenja.
- Registar licenciranih programa (tip snabdevača, tip licence, uslovi/ograničenja licence, međusobni odnosi vlasnika/menadžera i vendora)
- Lista standardnih programa desktop računara (katalog odobrenih programa)
- Registar zakrpa OS i statusa (antivirusnih programa) AVP (verovatno automatizovan)
- Registar pristupa i konekcija treće strane (bezbednosno informacije).

PRILOG 7.1: Nacrt plana *PDCA faze planiranja*

ISMS dokument *smernice za fazu planiranja* je specifičan za svaku organizaciju i obezbeđuje smernice za organizaciju kod planiranja PDCA *faze planiranja*. Dokument obuhvata detalje o tome šta organizacija smatra relevantnim za fazu planiranja, šta su ciljevi faze planiranja i kako postići te ciljeve. U nastavku je dat nacrt sadržaja smernica za fazu planiranja.

Sadržaj

1. Uvod
- 1.1 Uspostavljanje ISMS-a

2. Obim i granice

3. Organizacija
- 3.1.1 Kontekst (o organizaciji)
- 3.1.2 Lokacija(e)

4. Informaciona imovina
- 4.1 Informacije
- 4.2 Informaciona tehnologija
- 4.3 Humana imovina

5. Saopštenja ISMS politike
- 5.1 Ciljevi
- 5.2 Principi, ograničenja i pretpostavke

6. Zahtevi za usaglašenost
- 6.1 Zakonodavstvo
- 6.2 Regulativa
- 6.3 Ostalo

7. Menadžment rizika – nacrt
- 7.1 Ciljevi menadžmenta rizika
- 7.2 Smernice za menadžment rizika
  - 7.2.1 Ignorisanje rizika
  - 7.2.2 Prihvatanje rizika
  - 7.2.3 Deljenje rizika
  - 7.2.4 Prenošenje rizika
  - 7.2.5 Ublažavanje rizika
- 7.3 Smernice za procenu rizika
  - 7.3.1 Oblast poslovnih funkcija i procesa
  - 7.3.2 Oblast imovine
  - 7.3.3 Oblast pretnji
  - 7.3.4 Oblast ranjivosti

8. Kontrole zaštite
- 8.1 Ciljevi kontrola zaštite
- 8.2 Okvir za menadžment zaštite (SMF)

9. Smernice za odobrenje menadžmenta

10. Smernice za izjavu o primenljivosti (SoA)

PRILOG 7.2: Obrazac sadržaja za ISMS politiku

Obrazac sadržaja za ISMS politiku sadrži delove **xxx** i u < > koji predstavljaju specifičnosti organizacije i koje treba uneti u obrazac.

Obrazac ISMS Politike

ISMS politika *organizacije X*

Zaglavlje politike

	Detalji		
Podneta od	Organizacija X, odeljenje Y, [		
Odobrena od	tima za zaštitu informacija		
Lokacija	lokacija dela distribuirane organizacije na koji se politika odnosi		
Obim politike	[distribuirana organizacija, centrala, odeljenje, web lokacija]		
Broj politike	sadrži jedinstven identifikator kategorije politike i broj u toj kategoriji		
Tip politike	koristi se ako organizacija želi da definiše seriju tipova politike zaštite		
Datum primene	dan, mesec, godina	Verzija	01

SAOPŠTENJA POLITIKE

Poslovni ciljevi politike su da minimiziraju rizik ključnih poslovnih funkcija organizacije X. Ključne poslovne funkcije definišu namenu Organizacije X i izvršavaju one aktivnosti koje ispunjavaju interese relevantnih učesnika u Organizaciji X. Ova politika zaštite obuhvata zaposlene, informacije IT i infrastrukturu koja podržava uspešno izvršavanje ovih ključnih funkcija. Ovu politiku odobrava odbor za menadžersku reviziju <www.orgx.com.>.

Za podršku namene i ciljeva ove politike, ISMS politika zahteva:

- kreiranje okvira za menadžment zaštite – SMF
- definisanje poslovnih pokretača operacija zaštite
- upotrebu SMF za uspostavljanje ciljeva planiranja, implementacije, održavanja, kontrole i provere za minimiziranje rizika organizacije u terminima poverljivosti, integriteta i raspoloživosti
- uspostavljanje kriterijuma za merenje rizika
- uspostavljanje sveobuhvatnog programa menadžmenta usaglašenosti koji, najmanje:
- navodi sve primenljive zahteve za usaglašenost, uključujući zakonske, regulatorne i ugovorne obaveze
- uspostavljanje kriterijuma za merenje nivoa usaglašenosti
- obezbeđivanje formalne procedure za dobijanje menadžerske kontrole i odobrenja za sve inicijative zaštite informacija.

Napomena: *Ova saopštenja na visokom nivou apstrakcije opisuje ISMS politika, koja zahteva formalni menadžment informacione bezbednosti. Postoji više politika koje opisuju detalje menadžment programa bezbednosti informacija. Ove politike uključuju, naprimer*:

- kontinuitet poslovanja,
- svest o potrebi zaštite, obuku i obrazovanje i
- metrike i merenja efektivnosti kontrola zaštite.

NAMENA

Ova politika obuhvata potrebu zaposlenih Organizacije X da osiguraju poverljivost, integritet i raspoloživost ključnih poslovnih funkcija koje podržavaju misiju organizacije X. Takođe, ona minimizira rizik za ključni personal, informacije, IT i infrastrukturu koja podržava ključne poslovne funkcije. Da bi bila efektivna, politika treba da obuhvati i *zaštitu informacija i menadžment sistem zaštite informacija*. Poslovni procesi zahtevaju politiku zaštite informacija i uspostavljanje okvira za razvoj drugih politika, standarda, procedura i prakse zaštite. Drugi zahtev obuhvata formalni menadžment sistem zaštite informacija Organizacije X.

Obime/Primenljivost: Ova politika obuhvata Organizaciju X i primenjuje se na sve zaposlene.

Nivo usaglašenosti: Od svih zaposlenih obuhvaćenih obimom i primenom ove politike, očekuje se da je 100% sprovode.

Posebne okolnosti i izuzeci: Gde nije praktično sprovoditi ovu politiku, zaposleni Organizacije X moraju podneti pisani izveštaj sa opisom okolnosti koje zahtevaju izuzeće. Menadžerska revizija će odrediti opravdanost izuzeća. Menadžment ne prihvata izuzeća za ovu politiku.

Definicije, ključni termini i skraćenice:

Termin	Definicija
SMF	Okvir menadžmenta zaštite obezbeđuje okvir koji pokriva sve bezbednosne potrebe Organizacije X. Osnova za ovaj okvir su standardi ISO/IEC 27001, ISO/IEC 27002, sa dodacima iz NIS i COBIT standarda, ako je potrebno.
Itd.	....

Uloge i odgovornosti u razvoju politike zaštite uključuju:

Uloga	Opis	Detalji
Sponzori	obezbeđuju finansijsku podršku i druge resurse	
Inicijatori	odgovorno lice koje je otpočelo proces	
Projektanti	istraživači i pisci politike	
Podnosioci	formalni snabdevači zahteva kontrolorima; mogu biti inicijatori	
Kontrolori	menadžerski tim za vrednovanje sadržaja politike	
Overavači	formalni tim, često preporučen od proveravača	
Implementatori	primenjuju politiku na poslovne operacije, tehničku infrastrukturu i rešenja	

Uloge i odgovornosti u implementaciji, monitoringu i nametanju politike uključuju:

Uloga	Opis	Tbd
Poslovni menadžment		
Tehnički menadžment		
Data centar		
Menadžment rizika		
Operacije sistema		
Razvoj aplikacija		
Inženjering mreže		
Administracija sistema		
Interna provera		
Pravnik		
Ljudski resursi		

Dokument	izvor	primenljivost
ISO/IEC 27001	ISO	obezbeđuje ISMS okvir
ISO/IEC 27002	ISO	obezbeđuje okvir kontrola zaštite
Zakon xy	TBD	< uneti opis>
Itd.		

Resursi: Nije primenljivo (N/A)

Uputstva, standardi i procedure koje podržavaju		
Tip[1]	opis	link
TBD		

[1]P − procedura, S − standard, U − uputstvo

ISMS POLITIKA *(PRIMER)*

Izjava o nameni obezbeđuje smernicu za donošenje odluke o tome kako nastaviti dalje, u slučaju da se korisnik nađe u situaciji koja nije navedena u politici, proceduri, standardu ili nekom drugom iskustvu. Politika obezbeđuje specifičnosti koje odražavaju najbolju praksu i znanje raspoloživo u vreme pisanja. Namena politike je da ukaže na ponašanje korisnika, ako se suoče sa neizvesnošću.

CILJEVI

Svi zaposleni u *Organizaciji XY* treba da sprovode *ISMS politiku* koja je deo celokupnog sistema ISMS. Namena politike je da zaštiti poverljivost, integritet i raspoloživost informacija organizacije i informacione tehnologije. Poverljivost znači da su informacije dostupne samo onima kojima je dozvoljen pristup. Integritet znači da su informacije tačne i da ništa ne nedostaje. Raspoloživost znači da su informacije ili informaciona tehnologija dostupni za upotrebu na zahtev legalnih korisnika.

POLITIKA

Informaciona imovina *Organizacije XY* je zaštićena na odgovarajući način, nezavisno od vrednosti, pretnji i ranjivosti koje se mogu pojaviti. Da bi postigli taj cilj, izvršni direktor će za taj zadatak obezbediti potrebne finansijske i ljudske resurse. *Organizacije XY* će pratiti regulatorne i zakonodavne zahteve kako bi podržala bezbednosne ciljeve za poverljivost, integritet i raspoloživost informacija i informacionih sistema. Cilj *Organizacije XY* je da sa ovom izjavom politike uspostavi ISMS prema standardu ISO/IEC 27001, koji će sprečiti nedozvoljen pristup, prenos, izmenu, oštećenje i krađu informacione imovine. Svi zaposleni u *Organizaciji XY* dužni su da se upoznaju sa politikom i da je u praksi sprovode. *Organizacija XY* ističe da zaposleni moraju da sprovode ovu politiku i ostale ciljeve, kontrole i smernice. Bilo kakvo kršenje politike zaštite biće ozbiljno razmatrano i istraženo od strane menadžera za bezbednost informacija. *Organizacija XY* će obezbediti obuku za sve zaposlene i periodično sprovoditi procenu rizika da bi utvrdila da li je potrebna dalja akcija. Menadžer za zaštitu informacija ima ulogu da sprovede proces, održava ISMS organizacije i obezbeđuje savete i smernice za implementaciju.

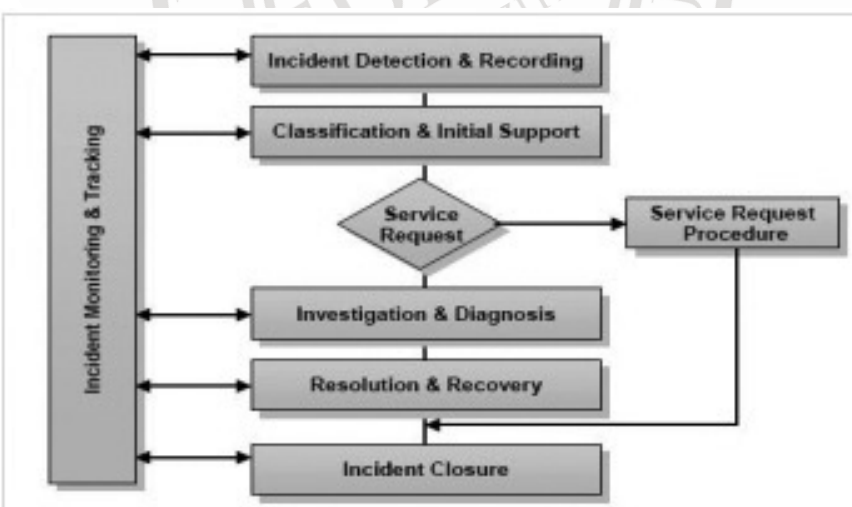
Svi menadžeri organizacije su odgovorni za implementaciju politike u njihovoj oblasti poslovanja i za ponašanje osoblja u skladu sa njom. *Organizacija XY* će pripremiti plan kontinuiteta poslovanja koji će biti održavan i testiran. Periodično, ali ne više od jednom godišnje, ISMS politika će biti revidirana radi potencijalne izmene. Procedure će navesti dodatne događaje koji će aktivirati reviziju politike.

PRILOG 7.3: Prioritetizacija incidenta (P = UT + UR)

Uticaj (Ut)	Zavisi od broja ljudi pogođenih incidentom
1 – Nizak	Jedan korisnik – nisu uključeni izvršni direktori ili njihovo osoblje
2 – Srednji	Više korisnika – uključeni su izvršni direktori ili njihovo osoblje
3 – Visok	Ljudski život, čitava organizacija, odeljenje, zgrada, finansijski sistemi

Urgentnost (Ur)	Zavisi od delovanja događaja na mogućnost nastavljanja rada korisnika. (Ovo ne treba mešati sa mišljenjem onoga ko prijavljuje incident o hitnosti za njegovo rešavanje.)
1 – Niska	Mogućnost nastavljanja rada nije pogoršana (korisnik radi sve funkcije i koristi sve servise)
2 – Srednja	Mogućnost nastavljanja rada je delimično pogoršana (korisnik ne može da radi određene funkcije ili koristi servise)
3 – Visoka	Mogućnost nastavljanja rada je kompletno ugrožena (korisnik je onemogućen da radi bilo koju funkciju ili da koristi servise)

Prioritet (P)	Zavisi od uticaja i urgentnosti. Prioritet određuje koliko brzo treba reagovati na incident
2 – Nizak	Rešiti incident u toku radne nedelje
3 – Srednji	Rešiti incident za 2 radna dana
4 – Visok	Rešiti incident za 4 sata
6 – Urgentan	Odmah reagovati na incident
6 – Vanredan	Postupiti prema odgovarajućoj proceduri za vanredne događaje



Slika P7.3.1. Dijagram toka procesa za određivanje prioriteta incidenata

PRILOG 7.4: Uzorak obrasca za izradu politike zaštite

NAPOMENA: xxx označava mesto gde organizacija unosi svoju specifičnost

Politika <Ime>

Zaglavlje politike

	Detalji		
Podneta od	Organizacija X, odeljenje Y, [		
Odobrena od	tima za zaštitu informacija		
Lokacija	lokacija dela distribuirane organizacije na koji se politika odnosi		
Obim politike	[distribuirana organizacija, centrala, odeljenje, web lokacija]		
Broj politike	sadrži jedinstven identifikator i broj kategorije politike zaštite		
Tip politike	koristi se ako organizacija želi da definiše seriju tipova politike zaštite		
Datum primene	dan, mesec, godina	verzija	01

Saopštenje politike

[Uneti saopštenje (izjavu) politike]

Namena

Ova politika obuhvata xxx i namenjena je svim zaposlenim organizacije X [koji xxx].

Obim/primenljivost

Ova politika obuhvata organizaciju X [centralu, distribuiranu lokaciju, odeljenje, web sajt] i primenjuje se na sve [zaposlene, ugovarače, posetioce itd.].

Nivo usaglašenosti

Očekuje se da sva lica obuhvaćena obimom i primenom [sprovode što je moguće striktnije, 100%, podržavaju duh itd.] ove politike.

Posebne okolnosti i izuzeci

Gde nije primenljivo za xxx, zaposleni Organizacije X moraju xxx i da koristiti zdrav razum da spreče xxx.

Definicije, ključni termini i skraćenice

Termini	**Definicije**

Uloge i odgovornosti

Uloge i odgovornosti u politici zaštite uključuju detalje u sledećoj tabeli:

Uloga	**Opis**	**Detalji**
Sponzori	oni koji obezbeđuju finansijsku podršku	
Inicijatori	oni koji počinju proces i iniciraju izradu politike	
Projektanti (*Developers*)	istraživači i autori izrade politike	
Podnosioci	formalni podnosioci zahteva za proveru	
Proveravači	menadžerski tim za proveru sadržaja politike	
Akreditatori	formalni tim za akreditaciju	
Implementatori	lica koja primenjuju politiku u IKT sistemu i organizaciji	

Dokumentacija za podršku

Dokument	Izvor	Primenljivost

Presedani

Xxx unosi svaki presedan u ovu politiku. Presedan može uključivati iskustvo organizacije, direktno ili indirektno, koje podržava implementaciju, monitoring i nametanje politike.

Sankcije za nesprovođenje

[Uneti xxx sankcije u politiku za slučajeve izveštavanja i eskalacije povrede politike.]

Zapis proverivača

		Proveravač:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis akreditatora:

		Akreditator:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis provere

Verzija	Datum	Opis provere	

Reference: ISO/IEC 27001, ISO/IEC 27002

Resursi

<Lista vendora/proizvoda, web lokacija i drugih resursa koji podržavaju standard >

Procedure, uputstva i standardi koji podržavaju politiku

Tip[1]	Opis	Link
[1] P – procedura, U – smernice, S – standardi		

2. UZORAK OBRASCA ZA IZRADU STANDARDA ZAŠTITE

Standard zaštite <Ime>

Zaglavlje standard

	Detalji		
Podneta od	Organizacija X, odeljenje Y, [		
Odobrena od	tima za zaštitu informacija		
Obim standarda	[distribuirana organizacija, centrala, odeljenje, web lokacija]		
Datum primene	dan, mesec, godina	verzija	01
Komentar	**TBD** – treba da bude urađen		

Namena

[Ovaj standard obuhvata xxx za sve organizacije X] [zaposlene, odeljenja, lokacije] [kojima, koje] xxx.

Standard

Sledeći standard(i) se primenjuju u kontekstu podrške politici zaštite xxx organizacije X:TBD.

Posebne okolnosti i izuzeci

Gde nije primenljivo za xxx, zaposleni Organizacije X moraju xxx i da koristiti zdrav razum da spreče xxx. Izuzeci za ovaj standard su stvarni izuzeci i moraju biti u interesu: izjave o misiji organizacije X, finansijske sigurnosti organizacije X, personalne i javne sigurnosti, kontinuiteta poslovanja i javnog ugleda.

Očekuje se da distribuirani delovi, odeljenja i lokacije organizacije striktno sprovode standard organizacije gde je moguće i usvajaju tehnološke promene kad god je moguće. Sprovođenje standarda promoviše centralizovane kapacitete za podršku (npr. help desk) i unapređuje konkurentsku prednost poslovanja.

Dokumentacija za podršku

Dokument	Izvor	Primenljivost

Zapis proverivača

		Proveravač:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis akreditatora

		Akreditator:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis provere

Verzija	Datum	Opis provere	

Reference: ISO/IEC 27001,ISO/IEC 27002

Resursi: <Lista vendora/proizvoda, *web* lokacija ili drugih resursa za podršku>

3. UZORAK OBRASCA ZA IZRADU PROCEDURE ZAŠTITE

Procedura zaštite <*Ime***>**

Zaglavlje procedure

	Detalji		
Podneta od	Organizacija X, odeljenje Y, [		
Odobrena od	tima za zaštitu informacija		
Obim standarda	[		
Datum primene	dan, mesec, godina	Verzija	01
Komentar	**TBD** – treba da bude urađen		

Namena: *ova procedura obuhvata xxx za celu organizaciju X koja izvršava sledeće poslovne funkcije ili zadatke: xxx, …*

Procedure

<uloga> je odgovorna za xxx koristeći sledeće procedure:

1. korak 1
2. korak 2

Posebne okolnosti i očekivanja

Gde nije primenljivo za xxx, zaposleni organizacije X moraju xxx i koristiti zdrav razum da spreče xxx. Izuzeci procedure su stvarni izuzeci i moraju biti u interesu:

- izjave o misiji organizacije X,
- finansijske sigurnosti organizacije X,
- lične i javne sigurnosti zaposlenih,
- kontinuiteta poslovanja i
- javnog ugleda.

Dokumentacija za podršku

Dokument	Izvor	Primenljivost

Zapis proverivača

		Proveravač:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis akreditatora

		Akreditator:	
Verzija	**Datum**	**Ime**	**Zvanje**

Zapis provere

Verzija	Datum	Opis provere	

Reference: ISO/IEC 27001, ISO/IEC 27002

Resursi: <Lista vendora/proizvoda, *web* lokacija ili drugih resursa za podršku>

PRILOG 7.5: Primer upitnika za vrednovanje informacione imovine

(*Po uzoru na upitnik za poverljivi računarski sistem.*)

Upitnik je deo uputstva za pripremu koraka analize pretnji i rizika i treba ih modifikovati za svaku konkretnu sredinu i IKT sistem. Kompletiranje upitnika je vitalno pošto svi sledeći koraci u analizi pretnji i rizika koriste ove informacije kao ulazne. Kompletiranje upitnika pomaže u razjašnjavanju detalja IKT sistema i olakšava proces konsultacija sa upravnom strukturom, operativnim i tehničkim osobljem koji pomažu u identifikovanju i proceni vrednosti imovine. Za pitanja na koje se daje odgovor „ DA" treba pripremiti detalje. Dijagram arhitektura sistema i jednostavna taksonomija imovine može se uključiti da pomogne onima koji imaju zadatak da odgovore na pitanja. Izbor načina rada sistema i završni koraci faze pripreme, detaljnije se opisuju u *Uputstvu za upravljanje rizika*. Generalna forma upitnika je primenljiva za postojeći i novi IKT sistem. Međutim, za novi sistem neki odgovori će nužno biti samo prognoze, a neki se ne mogu ni dati.

Opis sistema

Namena:

1. Koje su grupe korisnika u sistemu (organizacije, agencije, odeljenja, odseci, sekcije)?
2. Koja je funkcija sistema?
3. Šta sistem isporučuje?
4. Koji je uticaj na organizaciju ako sistem bude uništen ili ne bude raspoloživ duže vreme?

Funkcionalne karakteristike: aplikacije.

1. Koje procese izvršavaju aplikacije u sistemu (tj. baze podataka, e-pošta itd.)?

Funkcionalne karakteristike: konfiguracija.

1. Koji hardver sistem koristi?
2. Koji OS IKT sistem koristi (*Windows, Novell, NT, Unix, Linux*, …)?
3. Koji se mehanizmi zaštite u OS koriste?
4. Koje su karakteristike zaštite na raspolaganju u OS (tj. koristi poverljiv sistem)?

Funkcionalne karakteristike: komunikacije.

1. Da li sistem ima spoljne veze (tj. LAN, Internet, namenske linije)? Ako ima, opiši svaki!
2. Koji se mehanizmi i protokoli zaštite koriste (tj. *dial-back* modem, Kz, iznajmljene linije)?

PRILOG 7.6: Tipični parovi ranjivost/pretnja (V/T)

Tabela P8.1. *Tipični parovi ranjivost/pretnja*

Ranjivost – V	Pretnja – T koja je može iskoristiti
Okruženja i infrastrukture	
nedostatak fizičke zaštite zgrade, vrata i prozora	krađa
neadekvatne upotreba AC zgradama i sobama	krađa, namerno oštećenje
nestabilna električna mreža	fluktuacija napona napajanja
lokacija u oblasti podložnoj poplavi	poplava
Hardver	
nedostatak šeme periodične zamene (zanavljanja)	kvar medija za skladištenje
osetljivost na varijacije napona napajanja	fluktuacija napona
osetljivost na varijacije temperature	eksterne temperature
osetljivost na vlagu, prašinu, prljavštinu	prašina
osetljivost na EM zračenje	izvori EM zračenja
loše održavanje/pogrešna instalacija medija za skladištenje	greška održavanja
nedovoljno efikasna kontrola upravljanja konfiguracijom	greška operatera
Softver	
nedovoljan/nekompletan profil korisnika	pad softvera
bez ili nedovoljno testiranje softvera	neovlašćena upotreba softvera
komplikovan korisnički interfejs	greška operatera
nedostatak mehanizama I&A	krađa identiteta legitimnih korisnika
nedostatak kontrolnih tragova (*audit trail*)	neovlašćena upotreba softvera
poznata greška (bag) u softveru	neovlašćena upotreba softvera
nezaštićena lista pasvorda	krađa identiteta korisnika
loše upravljanje lozinkom	krađa identiteta korisnika
pogrešna alokacija prava pristupa	neovlašćena upotreba softvera
nekontrolisano preuzimanje i upotreba sw	maliciozni kôdovi
ulogovan posle napuštanja radne stanice	neovlašćena upotreba softvera
nedostatak efektivne kontrole promena	pad softvera
nedostatak dokumentacije	greške operatera
nedostatak rezervnih kopija (bekapa)	maliciozni programi ili požar
odlaganje/upotreba medija bez saniranja	zloupotreba podataka i informacija
omogućen nepotreban servis	upotreba neovlašćenog softvera

Ranjivost – V	Pretnja – T koja je može iskoristiti
nezreo ili novi softver	nekompetentno testiranje
široko distribuirani softver	gubitak integriteta u procesu distribucije
Komunikacije	
nezaštićene komunikacione linije	prisluškivanje – oticanje informacija
loše spajanje kablova	infiltracija u komunikacione linije
nedostatak I&A pošiljaoca i primaoca	krađa identiteta korisnika
otvoren prenos pasvorda	mrežni pristup ilegalnog korisnika
nedostatak dokaza o slanju i prijemu poruka	poricanje transakcije
dial–up linije	mrežni pristup ilegalnog korisnika
nezaštićen prenos osetljivih informacija	prisluškivanje
neadekvatno upravljanje mrežom	preopterećenje saobraćaja
nezaštićene konekcija javne mreže	neovlašćeno korišćenje softvera
nebezbedna mrežna arhitektura	upad u mrežu
Dokumentacija	
nezaštićeno skladište	krađa
nebriga kod odlaganja	krađa
nekontrolisano kopiranje	krađa
Personal	
odsustvo zaposlenih	nedostatak radnika
nekontrolisanje rada od strane obezbeđenja	krađa
nedovoljna bezbednosna obuka	greška operativnog osoblja
nedostatak svesti o potrebi zaštite	greške korisnika
nekorektno korišćenje softvera i hardvera	greška operativnog osoblja
nedostatak mehanizama za monitorisanje	neovlašćeno korišćenje softvera
nedostatak politike za zaštitu prenosa podataka	neovlašćeno korišćenje RM
neadekvatna procedura za prijem radnika	namerna šteta
Proceduralne	
nedostatak ovlašćenja za procesiranje informacija	namerno oštećenje
nedostatak procesa za ovlašćenje pristupa javnim inform.	korupcija podataka
nedostatak procesa za reviziju (superviziju) prava pristupa	neovlašćeni pristup
nedostatak procedure za kontrolu ISMS dokumentacije	korupcija podataka
nedostatak formalne procedure za registraciju korisnika	neovlašćeni pristup

Ranjivost – V	Pretnja – T koja je može iskoristiti
nedostatak kontrole inventara imovine	krađa
nedostatak politike upotrebe mobilnog računara	krađa
nedostatak formalne procedure supervizije ISMS zapisa	korupcija podataka
nedostatak politike „čist sto i čist ekran“	krađa informacija
nedostatak/nedovoljna zaštita od kupaca i/ili TTP	neovlašćeni pristup
nedostatak/nedovoljna zaštita od zaposlenih	krađa i prevara
nedostatak planova za kontinuitet poslovanja	tehnički kvarovi
nedostatak propisne alokacije odgovornosti u zaštiti	poricanje transakcija
nedostatak procedure za identifikaciju i procenu rizika	neovlašćeni pristup IKTS
nedostatak politike upotrebe e–pošte	pogrešno rutiranje poruka
nedostatak procedura za rukovanje klasifikovanih inform.	greške korisnika
nedostatak procedure za zaštitu intelektualne svojine	krađa informacija
nedostatak procedure za izveštaje o slabostima zaštite	ilegalna upotreba RM
nedostatak procedure za uvođenje softvera u OS	greška operatera
nedostatak procedure za kontrolu promena	greška u održavanju
nedostatak regularnog *auditing–a*	neovlašćeni pristup
nedostatak regularne revizije upravljanja	zloupotreba resursa
nedostatak mehanizama za nadzor proboja sistema	namerna oštećenja
nedostatak odgovornosti u zaštiti u opisu posla	greška korisnika
nedostatak evidencija grešaka u log datotekama	neovlašćena upotreba softvera
nedostatak evidencija grešaka u log datotekama	greške operatera
nedostatak definisanih procesa za upravljanje incidentom	krađa informacija
Opšte ranjivosti poslovnih aplikacija za procesiranje	
nekorektno podešavanje parametara	korisnička greška
primena aplikativnih programa na pogrešne podatke	neraspoloživost podataka
nemogućnost izrade izveštaja o upravljanju	neovlašćeni pristup
netačni podaci	korisnička greška
Opšte primenljive ranjivosti	
greška u jednoj tački	pad komunikacionog servisa
neadekvatan servis za održavanje	kvar hardvera
nepropisno projektovan i loš rad sa sistemom zaštite	intercepcija i prisluškivanje veza

PRILOG 7.7: Uzorak *izveštaja o proceni rizika* (NIST *template*)

KRATAK SADRŽAJ

I. Uputstvo

Namena

Obim analize rizika

Opisati komponente sistema, elemente, korisnike, lokaciju i sve druge detalje o sistemu koje treba razmatrati u analizi.

II. Metod analize rizika

Kratko opisati pristup i metodologiju koja je korišćena za analizu rizika, kao što su:

- članovi tima za analizu rizika i drugi odgovorni učesnici,
- metod/tehnika korišćena za prikupljanje informacija i
- razvoj i opis rangiranja atributa rizika i metoda proračuna preostalog rizika.

III. Karakterizacija informacione imovine

Opiši karakteristike sistema – hardvera (računara, servera, rutera i sl.), softvera (aplikacija, OS, protokola), interfejsa sistema (komunikacioni linkovi i sl.), podataka i korisnika! Obezbediti dijagram toka procesa od ulaza do izlaza, da bi se odredio obim napora analize!

IV. Izjava o osetljivosti

Skupiti i navesti spisak potencijalnih ranjivosti koje su primenjive za procenjivani rizik.

V. Izjava o izvorima pretnji

Skupiti i navesti spisak potencijalnih izvora pretnji koje su primenjive za procenjivani rizik.

VI. Rezultati procene rizika

Navesti spisak svih parova (opservacija) pretnje – ranjivosti. Svaki par mora uključiti:

- broj para i kratak opis, npr. opservacija npr.1: sistem korisničkih pasvorda (lozinki) može se probiti pogađanjem ili *krekovanjem*,
- diskusiju o paru pretnja – ranjivost,
- identifikacija postojećih kontrola zaštite za suzbijanje rizika,
- diskusija o verovatnoći incidenata i evaluacija, npr. *V, S ili N* verovatnoća,
- diskusija o uticaju pretnji i evaluacija, npr. *visok, srednji ili nizak* uticaj,
- skala rangiranja rizika i evaluacija, npr. *visok, srednji ili nizak* rizik i
- preporučene kontrole ili alternativne opcije za redukciju rizika.

VII Sumarni sadržaj

Ukupan broj opservacija. Sumiranje opservacija, pridruženih nivoa rizika, preporuke i svi komentari prikazuju se u tabelarnoj formi da se olakša implementacija preporučenih kontrola za vreme procesa ublažavanja rizika.

PRILOG 7.8: Obrazac plana tretmana rizika

Plan tretmana rizika organizacije X
Izjava o primenljivosti (SoA)

Izjava o primenljivosti (SoA)
Legenda (za izabrane kontrole i razloge za izbor kontrola)
LR: legalni zahtevi, **CO**: ugovorne obaveze, **BR/BP**: poslovni zahtevi/usvojene najbolje prakse, **RRA**: resultati procene rizika , **TSE**: do nekog iznosa

Kreiran:
20.11.2011

ISO 27001:2005 Kontrole			Tekuće kontrole	Primedba (opravdanje za isključivanje)	Izabrane kontrole i razlozi za izbor				Primedba (Pregled implementacije)
					LR	CO	BR/BP	RRA	
Član	Sekcija	Control Objective/Control							
Politika zaštite informacija	5.1	Politika zaštite informacija							
	5.1.1	Dokument politike zaštite informacija							
	5.1.2	Revizija politike zaštite informacija							
Organizacija informacione bezbednpsti	6.1	Interna organizacija							
	6.1.1	Angažovanje menadžmenta u zaštiti informacija							
	6.1.2	Koordinacija bezbednosti informacija							
	6.1.3	Alokacija odgovornosti u zaštiti informacija							
	6.1.4	Proces autorizacije za pristup i procesiranje informacija							
	6.1.5	Sporazumi o čuvanju tajnosti							
	6.1.6	Kontakt osoba sa menadžmentom (vlastima)							
	6.1.7	Kontakt osoba sa specijalnim interesnim grupama							
	6.1.8	Nezavisna provera informacione bezbednosti							
	6.2	Spolni saradnici							
	6.2.1	Identifikacija rizika koji se odnosi na spoljne saradnike							
	6.2.2	Bezbednost komunikacije sa kupcima/klijentima							
	6.2.3	Bezbednost sporazuma sa TTP							
Menadžment imovine	7.1	Odgovornost za imovinu							
	7.1.1	Inventar imovine							
	7.1.2	Vlasništvo nad imovinom							
	7.1.3	Prihvatljiva upotreba imovine							
	7.2	Klasifikacija informacione imovine							
	7.2.1	Uputstvo (smernice) za klasifikaciju							
	7.2.2	Označavanje i rukovanje sa informacijama							
Personalna zaštita	8.1	Provere pre zaposlenja							
	8.1.1	Uloge i odgovornisti							
	8.1.2	Bezbednosna provera							
	8.1.3	Zahtevi i uslovi zapošljavanja							
	8.2	Provere u toku zaposlenja							
	8.2.1	Odgovornost menadžmenta							
	8.2.2	Razvoj svesti, obuka i obrazovanje u zaštiti							
	8.2.3	Disciplinski proces i mere							
	8.3	Raskid ili promena posla							
	8.3.1	Odgovornost kod raskida polsa							
	8.3.2	Povratak imovine							
	8.3.3	Uklanjanje prava pristupa							

Napomena: *SoA može biti i odvojen dokument; ako je tako, treba referencirati SoA dokument, radije nego ga kopirati u plan tretmana rizika.*

U primeru SoA dokumenta date su četiri informacione imovine:
politika zaštite, organizacija informacione bezbednosti, menadžment imovine i personalna zaštita.

PRILOG 7.9: Uzorak *Izjave o primenljivosti* (SoA)

Napomena: *SoA može biti i odvojen dokument; ako je tako treba referencirati SoA dokument, u plan tretmana rizika, radije nego ga tamo kopirati.*

Legenda za izabrane kontrole i razloge za izbor kontrola:

LR: legalni zahtevi, CO: ugovorne obaveze, BR/BP: poslovni zahtevi/usvojene najbolje prakse, RRA: rezultati procene rizika, TSE: do neke mere.

U primeru SoA dokumenta date su četiri informacione imovine: *politika zaštite, organizacija informacione bezbednosti i menadžment imovine i personalna zaštita.*

Izjava o primenljivosti (SoA)

Legenda (za izabrane kontrole i razloge za izbor kontrola):
LR: legalni zahtevi, **CO**: ugovorne obaveze, **BR/BP**: poslovni zahtevi/usvojene najbolje prakse, **RRA**: resultati procene rizika , **TSE**: do nekog iznosa

Kreiran: 20.11.2011

ISO 27001:2005 Kontrole			Tekuće kontrole	Primedba (opravdanje za isključivanje)	Izabrane kontrole i razlozi za izbor				Primedba (Pregled implementacije)
					LR	CO	BR/BP	RRA	
Član	Sekcija	Control Objective/Control							
Politika zaštite informacija	5.1	Politika zaštite informacija							
	5.1.1	Dokument politike zaštite informacija							
	5.1.2	Revizija politike zaštite informacija							
Organizacija informacione bezbednpsti	6.1	Interna organizacija							
	6.1.1	Angažovanje menadžmenta u zaštiti informacija							
	6.1.2	Koordinacija bezbednosti informacija							
	6.1.3	Alokacija odgovornosti u zaštiti informacija							
	6.1.4	Proces autorizacije za pristup i procesiranje informacija							
	6.1.5	Sporazumi o čuvanju tajnosti							
	6.1.6	Kontakt osoba sa menadžmentom (vlastima)							
	6.1.7	Kontakt osoba sa specijalnim interesnim grupama							
	6.1.8	Nezavisna provera informacione bezbednosti							
	6.2	Spoljni saradnici							
	6.2.1	Identifikacija rizika koji se odnosi na spoljne saradnike							
	6.2.2	Bezbednost kominkacije sa kupcima/klijentima							
	6.2.3	Bezbednost sporazuma sa TTP							
Menadžment imovine	7.1	Odgovornost za imovinu							
	7.1.1	Inventar imovine							
	7.1.2	Vlasništvo nad imovinom							
	7.1.3	Prihvatljiva upotreba imovine							
	7.2	Klasifikacija informacione imovine							
	7.2.1	Uputstvo (smernice) za klasifikaciju							
	7.2.2	Označavanje i rukovanje sa informacijama							
Personalna zaštita	8.1	Provere pre zaposlenja							
	8.1.1	Uloge i odgovornosti							
	8.1.2	Bezbednosna provera							
	8.1.3	Zahtevi i uslovi zapošljavanja							
	8.2	Provere u toku zaposlenja							
	8.2.1	Odgovornost menadžmenta							
	8.2.2	Razvoj svesti, obuka i obrazovanje u zaštiti							
	8.2.3	Disciplinski proces i mere							
	8.3	Raskid ili promena posla							
	8.3.1	Odgovornost kod raskida posla							
	8.3.2	Povraćaj imovine							
	8.3.3	Uklanjanje prava pristupa							

PRILOG 8.1: Inicijalna priprema implementacije ISMS-a

Uključite u nacrt dokumenta seriju *čeklisti* (kontrolnih lista) koje učesnicima prenose obim napora sa metrikom progresa. Korisne su sledeće *čekliste:*

***Čeklista* ISMS ulaza:**

- npr., ISO 27001 i ISO 27002,
- zahtev za usaglašenost,
- poslovni pokretači (BD),
- rezultati analize rizika.

***Čeklista* aktivnosti, formulisana prema PDCA modelu;**

Plan implementacija ISMS-a*:*

- definišite obim ISMS,
- definišite ISMS politiku,
- definišite politiku zaštite informacija (verovatno u ISMS politici),
- definišite pristup proceni rizika,
- identifikujte rizik,
- analizirajte faktore rizika u kontekstu poslovnih ciljeva i interesa relevantnih učesnika,
- navedite opcije tretmana rizika,
- izaberite ciljeve kontrola zaštite,
- generišite SoA dokument,
- definišite metrike i merenja za podešavanje performansi kontrola zaštite!

Do

- Definišite i implementirajte plan tretmana rizika!
- Implementirajte kontrole zaštite iz faze planiranja!
- Implementirajte program razvoja svesti o potrebi zaštite!
- Uspostavite ISMS operacije!
- Implementirajte infrastrukturu za odgovor na incident!
- Definišite merenja performansi!

Check

- Monitorišite i proveravajte politiku, standarde, procedure i prakse!
- Proverite efektivnost operacija zaštite koristeći metrike i merenja (objektivne faktore efektivnosti)!
- Identifikujte poboljšanja ISMS!

Act

- Implementirajte ISMS poboljšanja!
- Inicirajte PDCA ciklus da prilagodite poboljšanja!

Čeklista ISMS izlaza:

- dokumenta
  - ISMS politika,
  - politika zaštite informacija,
  - proces menadžmenta procene rizika,
  - SoA dokument;
- *servisi*
  - menadžment kontinuiteta poslovanja,
  - odgovor na incident,
  - itd.
- *organizacione promene*
  - Navedite svaku poslovnu jedinicu i poslovne funkcije i sumirajte neophodne akcije da ih prilagodite za efektivni menadžment rizika!
- *komunikacije*
  - Uspostavite komunikacioni protokol takav da direktive dolaze od lica sa ovlašćenjima!

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG 8.2: Projekat poboljšanja procesa

Obrazac definicije projekta obezbeđuje detalje za planiranje, izvršavanje i isporuku projekta. Eksplicitno definisanje ciljeva, obima, pretpostavki, izlaza, uloga i odgovornosti i kriterijuma uspeha promoviše menadžment očekivanja i uspešnog ishoda projekta. Svaki projekat računa na izvršavanje više zadataka od zvanično definisanih u ugovoru. Dodavanje novih servisa je dobra poslovna praksa. Međutim, izvršavanje dodatnih servisa, a da ključni rezultati i kontrolne tačke projekta nisu zadovoljeni, nije dobra praksa. Precizna artikulacija očekivanja u formalnom dokumentu definicije projekta osigurava sinergiju svih relevantnih učesnika o tome šta čini kompletiranje i završetak projekta. Definicija projekta nije nužno zamena za ugovor, izveštaj o radu ili odgovor na zahtev za ponudu. Definicija projekta je češće dodatak ovim dokumentima. Čak i pored zvaničnog ugovora, definicija projekta razjašnjava zadatke i rafinira nejasne termine ugovora za akcije. Sledeći obrazac projekta zahteva unos specifičnosti svake organizacije u < >.

< Ime projekta > <Datum>

Definicija projekta [*Template*] za < Ime projekta >

Saopštenje o nameni projekta

Ovaj dokument sumira zadatke, obim, uloge, odgovornosti, izlazne rezultate i kontrolne tačke.

< Ime projekta >.

Tabela P8.2.1 *Prihvatanje definicije projekta*

Prihvatanje dokumenta
Overavač: < Ime>
Titula: < Titula >
Datum: < dan, mesec, godina>
Potpis: < potpis<

Tabela P8.2 *Promena istorije*

Verzija definicije projekta br.	Datum izdavanja	Opis
1	dan, mesec, godina	

Sadržaj

Ciljevi

Navedite koncizno ciljeve koji uključuju izlazne rezultate, servise ili druge rezultate projekta u narativnoj formi ili u bulitima.

Obim

- Navedite obim projekta u terminima:
- izlazni rezultati, servisi ili drugi rezultati,
- opis svake stavke,
- ko je odgovoran,
- kriterijum za procenu uspešnog kompletiranja projekta.

Pretpostavke

Jasno navedite pretpostavke u odnosu na ciljeve i obim projekta. Koristite sledeće kategorije za specifikaciju pretpostavki:

- Poslovne funkcije

U obimu:

< buliti definicija pretpostavki u obimu>

Izvan obima:

< buliti definicija pretpostavki izvan obima>

Na primer: *poslovne funkcije:*

u obimu:

centar za operacije zaštite je lociran na < adresi>.

izvan obima:

ovo ne uključuje centar za mrežne operacije na istoj lokaciji. Svaka poslovna funkcija koja eksplicitno nije navedena da je u obimu je izvan obima. Navedite opštu izjavu koja obuhvata sve funkcije izvan obima, slično standardnom pravilu *firewalls* „sve što nije eksplicitno dozvoljeno – to je zabranjeno".

Opšte pretpostavke

Organizacija X će obezbediti pristup svim sajtovima, IT i drugim oblastima navedenim u izjavi o obimu projekta. Zaposleni *Organizacije X* će sarađivati i davati blagovremeno sve potrebne podatke. Svi parametri moraju biti blagovremeno navedeni.

Projektni tim

Tabela P8.2.2 *Projektni tim*

Organizacija	Uloga	Član tima	Kontaktne informacije	Komentar
	menadžer projekta	< ime >	< e-mail, tel. >	
	specijalista zaštite			
	mMenadžer usaglašenosti			
	itd.			

Nacrt plana projekta

Obezbedite faze i akcije plana projekta po stavkama. Ovo nije plan projekta, nego opis plana projekta sa uopštenim detaljima. Međutim, ovaj dokument definiše projekat i zahteva formalni potpis. Opšti nacrt projekta uključuje sledeće:

1. *Inicijacija projekta*:
   a. izbor menadžera projekta
   b. identifikacija uloga i odgovornosti
   c. izbor članova tima.

2. *Otkrivanje informacija*:
   a. pre posete lokaciji
   b. poseta lokaciji
   c. posle posete lokaciji.
3. *Analiza*:
   a. < lista aktivnosti i kontrolne tačke>
4. Generisanje izveštaja:
   a. < lista izveštaja>; ovi rezultati će biti isporučeni.
5. *Distribucija izveštaja*:
   a. definišite komunikacioni protokol
   b. distribuirajte protokol.
6. *Projekt kompletiran*:
   a. obezbedite potpis.

Sve stavke iz plana projekta mogu se konvertovati u tabelarnu formu liste akcija:

Tabela P8.2.3 *Lista akcija*

Ko	Isporuka/Kontrolne tačke	Akcija	Opis

Procena rizika

U sledećoj tabeli predstavljeni su faktori potencijalnog rizika za projekat i rešenja.

Tabela P8.2.4 *Faktori rizika za projekat i rešenja*

Rizik	Efekat	Uticaj	Ublažavanje

Kontrolne tačke projekta

1. Obezbedite opis kontrolnih tačaka koji može uključiti:
   a. isporuku definicije projekta
   b. potpisivanje definicije projekta
   c. revizija plana projekta
   d. osnove plana projekta.

PRILOG 10.1: SSE CMM v.3.0 model: DIMENZIJA NIVOA KAPACITETA (CL)

CL	CF (Zajedničke karakteristike)	Atributi
1	1.1. BP se izvršavaju	*zvršavane neformalno*
2	2.1. Planiranje performansi 2.2. Disciplinovanje performansi 2.3. Verifikovanje performansi 2.4. Praćenje performansi	*planirane i praćene*
3	3.1. Definisanje standardnog procesa 3.2. Izvršavanje definisanog procesa 3.3. Koordinacija procesa	*dobro definisan*
4	4.1. Uspostavljanje merljivih ciljeva kvaliteta 4.2. Objektivno upravljanje performansama	*kvantitativno kontrolisan*
5	5.1. Poboljšavanje kapaciteta organizacije 5.2. Poboljšavanje efektivnosti procesa	*kontinualno poboljšavan*

CF (Zajedničke karakteristike)	GP (Generičke prakse)
CL1	
1.1 – BP se izvršavaju	1.1.1 – izvrši proces
CL2	
2.1 – Planiranje performansi	2.1.1 – alociraj resurse 2.1.2 – pripiši odgovornosti 2.1.3 – dokumentuj proces 2.1.4 – obezbedi alate 2.1.5 – obezbedi obuku 2.1.6 –planiraj proces
2.2 – Disciplinovanje performansi	2.2.1 – koristi planove, standarde i procedure 2.2.2 – upravljaj konfiguracijom
2.3 – Verifikovanje performansi	2.3.1 – verifikuj usklađenost procesa 2.3.2 – kontroliši proizvode rada
2.4 – Praćenje performansi	2.4.1 – prati sa merenjem 2.4.2 – preduzimaj korektivne akcije
CL3	
3.1 – Definisanje standardnog procesa	3.1.1 – standardizuj proces 3.1.2 – formiraj standardni proces
3.2 – Izvršavanje definisanog procesa	3.2.1 – koristi dobro definisan proces 3.2.2 – izvrši reviziju defekata 3.2.3 – koristi dobro definisane podatke
3.3 – Koordinacija procesa	3.3.1 – koordinacija unutar grupe 3.3.2 – koordinacija između grupa 3.3.3 – koordinacija sa spoljnim grupama
CL4	
4.1 – Uspostavljanje merljivih ciljeva kvaliteta	4.1.1 – uspostavi ciljeve kvaliteta
4.2 – Objektivno upravljanje performansama (izvršavanjem OP)	4.2.1 – odredi kapacitet procesa 4.2.2 – koristi kapacitet procesa
CL5	
5.1 – Poboljšavanje kapaciteta organizacije	5.1.1 – uspostavi ciljeve efektivnosti procesa 5.1.2 – kontinualno poboljšavaj standardni proces
5.2 – Poboljšavanje efektivnosti procesa	5.2.1 – izvrši uzročno-posledičnu analizu 5.2.2 – eliminiši uzroke defekata 5.2.3 – kontinualno poboljšavaj definisani proces

PRILOG 10.2: SSE CMM kriterijumi za razvoj optimalnog programa zaštite

CL 1 – Dokumentovan i neformalno izvršan program zaštite organizacije prema SSE CMM modelu, ima formalno objavljen *Program* i *Plan zaštite* koji zadovoljavaju sledeće kriterijume:

Kriterijumi za CL 1	Da/Ne
a. **Dokumentacija programa zaštite.** - Sadrži sveobuhvatan i detaljan *Plan zaštite* koji pokriva svu ključnu imovinu. - Odobren *Plan zaštite* obuhvata *politiku zaštite*, *menadžment rizika* itd. - *Plan zaštite* identifikuje vlasnika imovine i odgovornosti za upravljanje imovinom.	
b. **Uspostavljanje strukture za menadžment zaštite.** - Formiran centralni tim za menadžment programa zaštite. - Program zaštite sadrži ovlašćeno, nezavisno i stručno telo za menadžment. - Imenovan je glavni menadžer zaštite i ima odgovarajuću subordinaciju.	
c. **Definisanje odgovornosti za zaštitu**. - Definisane su i jasno pripisane odgovornosti za zaštitu i očekivano ponašanje za sve relevantne učesnike u sistemu zaštite.	
d. **Upravljanje rizikom**. - Integralni deo programa i politike zaštite, - regularna i periodična procena rizika i ranjivosti i - monitorisanje efikasnosti realizacije Programa zaštite.	

CL 2: Kompletiran, planiran i kontrolisan program nasleđuje i kompletira kriterijume CL 1 +

Kriterijumi za CL 2	Da/Ne
a. **Dokument Programa zaštite**. - Sadrži detaljan i odobren *Plan zaštite*, koji pokriva svu ključnu imovinu, politiku zaštite, menadžment rizika , pregled kontrola zaštite itd., identifikuje vlasnike informacija i odgovornosti.	
b**. Uspostavljanje strukture za menadžment zaštite**. - Generalno formira se centralni tim za menadžment zaštite. - Program zaštite sadrži ovlašćeno, nezavisno i stručno telo za menadžment zaštite. - Imenovan je glavni menadžer zaštite i ima odgovarajuću subordinaciju.	
c. **Definisanje odgovornosti.** - Pripisane su kontrolisane odgovornosti za zaštitu i očekivano ponašanje za sve relevantne učesnike.	
d. . **Upravljanje rizikom**. - Integralni deo programa i politike zaštite, regularna i periodična procena rizika i ranjivosti i monitorisanje efikasnosti realizacije programa zaštite.	
e. **Akreditacija *plana zaštite*.** - *Plan zaštite* je odobren od strane menadžmenta i obuhvata sve IKT sisteme.	

CL3: Implementiran, dobro definisan program zaštite obuhvata formalne procedure za implementaciju koje promovišu ponovljivost i potpuno razumevanje implementacije programa zaštite. Program zaštite je na CL 3 ako zadovoljava sve kriterijume sa CL 2, sadrži pisane procedure zaštite i ispunjava sledeće kriterijume:

Kriterijumi za CL3	Da/Ne
a. **Razvoj svesti o potrebi.** - Vlasnik i korisnici svesni potrebe za donošenje i implementaciju politike zaštite. - Distribuirana *politika zaštite,* pravila i očekivana ponašanja svim u IKT sistemu. - Od korisnika se zahteva da potpišu izjavu o prihvatanju odgovornosti za zaštitu.	
b. **Provera i kontrola zaštite**. - Rutinski koristi automatske alate za monitorisanje sistema zaštite. - Uspostavljene politike pregleda sistemskih *log* datoteka, testiranja na proboj sistema, interne i eksterne provere i nadzora.	
c. Upravljanje zaštitom u toku životnog ciklusa sistema. - Razmatrati zaštitu u svakoj fazi životnog ciklusa IKT sistema.	
d. Uspostavljanje procedure za akreditaciju i sertifikaciju. - Zvanično telo formalno autorizuju operacije (rad) sistema i menadžment rizika.	
e. **Implementacija efikasne, bezbednosno orjentisane politike personalne zaštite.** - Precizno identifikuje potrebne veštine i uključuje opis radnog mesta. - Razvija i implementira procedure prekida posla i premeštaja. - Izvršava periodičnu bezbednosnu proveru za svakog zaposlenog. - Obezbeđuje adekvatnu obuku i ekspertska znanja iz oblasti zaštite. - Dokumentuje i monitoriše obuku i profesionalno stručno usavršavanje zaposlenih.	
f. Implementacija politike fizičke zaštite i zaštite od uticaja okruženja. - Razvoj i implementacija procedura za fizičku zaštitu IKT sistema.	
g. Implementacija politike zaštite za informatičku podršku i funkcionisanje. - Razvoj i implementacija procedura za podršku krajnjim korisnicima.	
h. Implementacija politike za vanredne događaje (VD). - Zahteva razvoj, testiranje i ažuriranje plana za VD za sve IKT sisteme.	
i. Dokumentovanje specifičnih kontrola zaštite i operativnih procedura. - Dokumentacija uključuje specifikacije isporučioca opreme, korisnička uputstva, procedure za evaluaciju i proceduru za akreditaciju i sertifikaciju.	
j. Obuka zaposlenih iz oblasti zaštite. - Plan, implementacija, održavanje i evaluacija efikasne obuke i program za razvoj svesti o potrebi zaštite dizajniran za razne vrste poslovnih funkcija.	
k. Implementacija kapaciteta za upravljanje kompjuterskim incidentom. - Uspostavlja kapacitet za upravljanje kompjuterskim incidentom koji obezbeđuju forenzičku analizu digitalnih dokaza. - Obezbeđuje antivirusne programe, tim i sredstava za izveštavanje o incidentima. - Obezbeđuje informacije o ranjivostima sistema i savete za njihovo otklanjanje.	
l. Kontrola pristupa IKT sistemima. - Razvija i implementira politiku i procedure autentifikacije i autorizacije. - Uspostavlja politiku kontrole pristupa.	
m. Implementacija politike za registrovanje tragova za nadzor i proveru. - Razvoj procedura za registrovanje tragova za proveru sistema zaštite (*audit*), - Registrovanje, pregled i analizu tragova za istragu kompjuterskog incidenta. - Obezbeđuje zaštitu kontrolnih informacija od neovlašćenog pristupa.	

CL4: Verifikovan i kvantitativno upravljan program zaštite precizno određuje vrednost specifičnih kapaciteta za zaštitu, vrednuje podatke i informacije na najvišem nivou i štiti ih od gubitaka, oštećenja, izmene i neraspoloživosti, u skladu sa njihovom vrednosti i obezbeđuje integrisani menadžment sistem zaštite. CL4 zahteva aktivno uključivanje u vlasnika/menadžera procesa za izvršavanje poslova i misije organizacije. Smatra se da je program zaštite najmanje na CL 4, ako zadovoljava sve kriterijume sa CL 3 i ispunjava sledeće:

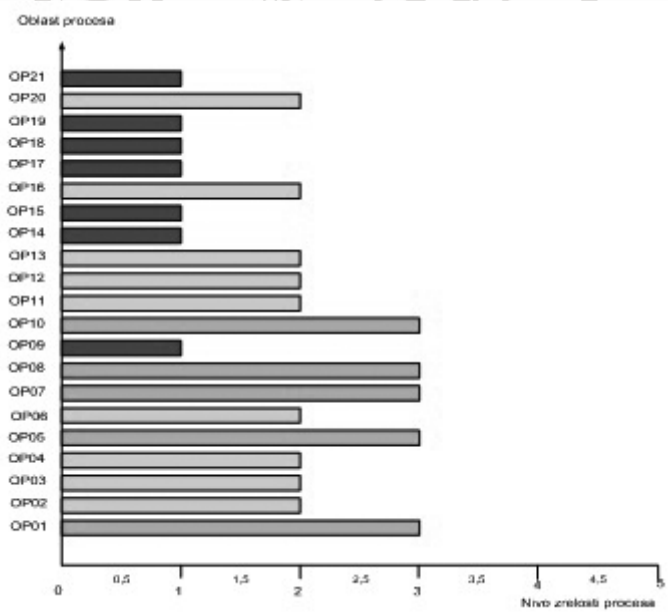
Kriterijumi za CL4	Da/Ne
a. Razumeti vrednost informacija i uticaj gubitaka na misiju organizacije.	
b. Odrediti kako nebezbednost u IKT sistemu može uticati na misiju organizacije.	
c. Porediti troškove sistema zaštite sa troškovima posledica uticaja na misiju.	
d. Obezbediti da su troškovi kapaciteta za rad barem jednaki troškovima zaštite.	
e. Izložiti i promovisati proaktivan stav prema zaštiti u celoj organizaciji.	
f. Praktikovati odbranu po dubini – zaštita, detekcija, suzbijanje i aktivan odgovor.	
g. Posmatrati sistem zaštite kao sredstvo za ostvarivanje misije organizacije.	
h. Analizirati sistem mera za evaluaciju efikasnosti zaštite.	
i. Izveštavati o identifikovanim ranjivostima i preduzimati korektivne akcije.	
j. Precizno meriti i određivati poboljšanje kapaciteta misije organizacije.	
k. Precizno meriti i određivati troškove implementacije sistema zaštite.	

CL5: Optimalan i sveobuhvatan program zaštite kontinualno poboljšava rentabilnost mera zaštite i donosi odluke na bazi preciznih znanja o dobiti i troškovima implementacije sistema zaštite. Na ovom nivou programa zaštite, sistem zaštite se posmatra *kao integralni deo misije organizacije*, a akvizicija i implementacija sistema zaštite su neophodni troškovi poslovanja.

Kriterijumi za CL5	Da/Ne
a. Rentabilne mere derivirane sa četvrtog nivoa pretočiti u odluku za poboljšanje zaštite.	
b. Demonstrirati da je zaštita IKT sistema integralni deo poslova organizacije.	
c. Razumeti i upravljati ranjivostima sistem zaštite.	
d. Kontinualno reevaluirati pretnje i adaptivno uračunavati promene okruženja.	
e. Po potrebi identifikovati dodatne ili rentabilnije alternativne mere zaštite.	
f. Realizovati i identifikovati ostvarene koristi od sistema zaštite.	

PRILOG 10.3: Razvoj referentnog profila op standardnog CA

Sertifikaciono telo (CA) servisira povezivanje matematičkih parova privatnog i javnog ključa sa pridruženim entitetima u *infrastrukturi javnog ključa* (PKI). Na neki način CA izvršava slične servise kao i servisna organizacija, ali se razlikuje po tome što servisira širu zajednicu korisnika i što pre autentifikuje digitalne sertifikate, pa tek onda opslužuje specifične klijente. U toku su brojne diskusije o adekvatnoj politici i praksama koju CA treba da sprovode ili da su obavezne za tipična CA. Međutim, bez obzira na politike i prakse koje CA treba da sprovode jeste i uvek će biti vrlo važno da se sačuva i održava bezbednost i poverenje korisnika u CA, kao poverljivog provajdera servisa zaštite – TTPS. SSE-CMM model pruža prednost zato što ne formuliše poseban proces kojeg treba slediti, prepuštajući to samoj organizaciji, ali obavezuje da se zrelost korišćenog procesa upoređuje sa odgovarajućim procesom najbolje prakse zaštite iz modela, čak i ako se realni proces razlikuje od njega. Ovaj aspekt SSE CMM modela veoma je važan, pošto mreža CA raste i povećava se nivo međusertifikacija. Referentni profil OP standardnog CA prikazan na slici P10.4.1 generički je i primenljiv na sve tipove CA. Međutim, očekuje se da u hijerarhijskoj organizaciji CA, *rut* CA na nacionalnom nivou bude na višem nivou zrelosti procesa i kapaciteta (barem 4.) od potčinjenih CA. SSE CMM poseduje ove mogućnosti i potrebnu fleksibilnost.



Slika P10.4.1 Profil procesa CA

Dovođenje inženjerskih procesa (SSE) na 3. nivo kapaciteta najefektivnije se može postići dovođenjem projektnih OP na 2. nivo zrelosti, a organizacionih OP na 1. nivo zrelosti. Planiranje, nadzor i praćenje projektnih OP na nivou projekta obezbeđuje kontrolu kvaliteta,

upravljanje konfiguracijom, upravljanje rizikom i planiranje, što je neophodno za obezbeđivanje podataka za poboljšavanje organizacionih procesa. Izvršavanjem organizacionih OP dobiju se neophodni resursi koje koriste inženjerske OP na 3. nivou zrelosti. Ovi resursi uključuju standardne SE procese organizacije, podršku i stečena SE znanja i veštine.

Organizacija koja unapređuje program rada treba da prema značaju odredi prioritete izvršavanja OP u odnosu na postavljene ciljeve i da nastoji da najpre poboljšava kapacitete u tim OP. OP01, OP05, OP07, OP08 i OP10 smatra se da zaslužuju najveću pažnju i samim tim treba da budu na najvišem nivou zrelosti kapaciteta. Ove OP moraju biti dobro dokumentovane i organizacija treba da ih regularno koristi. Smatra se da je dobro definisan i implementiran treći nivo zrelosti procesa sasvim odgovarajući, pošto se ove OP fokusiraju na *administraciju kontrola zaštite, procenu ranjivosti sistema, koordiniranje zaštite, nadzor i kontrolu sistema zaštite i specifikaciju bezbednosnih potreba*.

OP02, OP03, OP04, OP06 **i** OP11 iz SSE grupe OP odnose se na *procenu uticaja (pretnji na poslovni sistem), procena bezbednosnog rizika, procena pretnji, izgradnju argumenata za bezbednosnu garanciju (assurance) i verifikaciju i validaciju*. Ove se OP smatraju važnim, ali ne zahtevaju isti nivo zrelosti kapaciteta kao prethodna grupa OP. Za ove OP dovoljno je da budu dobro dokumentovane. U istu srednju grupu (drugi nivo zrelosti) svrstavaju se i projektne OP12 i OP 13 koje se odnose na *osiguranje sistema kvaliteta i upravljanje konfiguracijom*. OP iz oblasti organizacione grupe OP16 i OP20 koje *planiraju tehničke napore i upravljanje podrškom SSE procesa* istog su značaja i nalaze se na drugom nivou zrelosti procesa. Smatra se da CA organizacija periodično koristi ove procese (na drugom nivou zrelosti procesa).

Preostala OP09 iz SSE grupe, koja definiše *obezbeđenje bezbednosnog ulaza*, kao i OP15 iz projektne grupe, koja definiše *nadzor i kontrolu tehničkih napora* i OP17, OP18, OP19 i OP21 iz organizacione grupe, koje definišu: *SSE procese organizacije, poboljšavanje SSE procesa organizacije, upravljanje razvojem proizvodne linije i obezbeđenje tekućih znanja i veština* iz *oblasti zaštite*, svrstane su na najniži nivo zrelosti za ovaj profil, pošto je verovatnije da se ove OP ređe koriste pa će se na višim nivoima zrelosti postići manja dobit za organizaciju, iako je izvršavanja ovih aktivnosti važno za ovaj profil.

PRILOG 10.4: Primer *plana im*plementacije poboljšanja procesa

		Uvod
	1.1	Rezultati SSAM evaluacije procesa organizacije
	1.2	Oblasti procesa od interesa za poboljšavanje
	1.3	Struktura inženjerskog tima za poboljšavanje procesa (EPG)
	1.4	Struktura akcionog tima za implementaciju procesa (PAT)
1.0	1.5	Entitet za kontrolu konfiguracije i upravljanje dokumentacijom (CCB)
	1.6	Kontrola (garancija) kvaliteta (*Quality Assurance*)
	1.7	Dinamički (vremenski) plan
	1.8	Alati
	1.9	Faktori rizika
	1.10	Revizije i odobrenja
		Faza projektovanja (dizajniranja)
	2.1	Generisanje akcionog plana projektnog tima (PAT)
	2.2	Revizija, modifikacija i odobravanje akcionog plana PAT
2.0	2.3	Generisanje *Akcionog plana* EPG
	2.4	Revizija, modifikacija i odobrenje *Akcionog plana*
	2.5	Pripisivanje uloga prema akcionom planu
	2.6	Izvršavanja rada po planu (politike, procedure, standardi)
	2.7	Razvoj metrika i tehnika merenja
	2.8	Razvoj zahtevanog materijala za obuku
	2.9	Praćenje statusa implementacije poboljšavanja procesa
	2.10	Revizija i preporuka alata za reviziju
	2.11	Podrška, revizija i monitorisanje rada
	2.12	Ažuriranje akcionih planova EPG
	2.13	Prisustvovanje sastancima/podrška EPG
		Faza pilot projekta
	3.1	Izbor pilot projekata
	3.2	Dokumentovanje kriterijuma za uspeh i tehnika merenja
	3.3	Orijentisanje i obuka članova projektnog tima o konceptu poboljšavanja procesa (npr. SSE CMM ili CMMI)
	3.4	Orijentisanje i obuka članova projektnog tima o procesima i procedurama
3.0	3.5	Izvođenje (izvršavanje) pilot projekata
	3.6	Monitorisanje pilot projekata
	3.7	Analiza rezultata iz pilot projekata
	3.8	Mere uspeha (benčmarking)
	3.9	Obezbeđivanje izučavanja iskustava
	3.10	Ažuriranje procedura i sistema standardnih procesa organizacije ako je potrebno

4.0		**Faza implementacije**
	4.1	Izbor jednog ili više projekata
	4.2	Dokumentovanje kriterijuma uspeha i tehnika merenja
	4.3	Orijentisanje i obuka članova projektnog tima o konceptu poboljšavanja procesa (npr. modeli procesa SSE CMM ili CMMI)
	4.4	Orijentisanje i obuka članova projektnog tima u procedurama
	4.5	Pomoć u implementaciji ako je potrebna
	4.6	Monitorisanje i merenje uspeha
	4.7	Obezbeđivanje izučavanja iskustava
	4.8	Ažuriranje procedura i sistema standardnih procesa organizacije ako je potrebno
	4.9	Implementacija procesa iz više projekata ako je potrebno
	4.10	Potpisivanje i odobravanje kompletiranja PATs
5.0.		**Kontrola i monitoring**

NAPOMENA:

Angažovanje svih učesnika koji izvršavaju proces bitno je za kreiranje iskoristivog opisa procesa. Procesi u nekoj organizaciji ili na nekom projektu ne treba da odgovaraju jedan na jedan sa procesima (OP) opisanim u modelu. Zbog toga pokrivanje neke OP sa procesom organizacije može biti opisano na više načina, tj. kroz politike, standarde i/ili procedure, a opis procesa može obuhvatiti više od jedne OP.

PRILOG 11.1: Primer *UPITNIKA* za SSAM evaluaciju

OP 09 – Obezbeđivanje bezbednosnog ulaza

CL1: Bazične prakse

Komentar: Da li su dole identifikovane BP **izvršavane** kao deo vašeg projekta? Napominjem da lično ne morate biti uključeni u izvršavanje BP; dovoljno je da znate ko je izvršava. Za svako pitanje sa pozitivnim odgovorom, navedite dokaz koji podržava odgovor.

Bazična praksa (BP)	DA	NE	Ne znam	DOKAZ
09.01. Rad sa projektantom, razvojnim inženjerom i korisnicima da se stekne uverenje da odgovarajuća strana shvata sve potrebne ulazne bezbednosne informacije.	+			Dokument: *Plan zaštite, br. evid. 123/4-2003. god.*
09.02. Određena bezbednosna ograničenja i razmatranja potrebna za donošenje kvalitetnih inženjerskih izbora.				
09.03. Identifikovana alternativna rešenja za zaštitu koja se odnose na inženjerske probleme.				
09.04. Analizirani i određeni prioriteti inženjerskih alternative, koristeći bezbednosna ograničenja i razmatranja.				
09.05. Obezbeđena odgovarajuća uputstva za zaštitu za druge inženjerske grupe.				
09.06. Obezbeđena odgovarajuća uputstva za zaštitu za korisnike operativnog sistema i administratore.				

CL 2: Planiran i praćen

Da li oni koji izvršavaju BP-e ***OP Administriranje kontrola zaštite*** takođe izvršavaju neku od sledećih funkcija? Za svaku tvrdnju sa pozitivnim odgovorom navedite dokaz koji ga podržava.

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
2.1.1 Alocirani adekvatni resurs (uključujući ljude) za izvršavanje OP				
2.1.2 Pripisane odgovornosti za zavoj proizvoda rada, i/ili servisa OP				
2.1.3 Dokumentovan metod izvršavanja OP u politikama, standardima i/ili procedurama, uključujući merenja koja treba izvršiti				
2.1.4 Obezbeđeni odgovarajući alati za podršku izvršavanja OP				
2.1.5 Obezbeđeno da su pojedinci koji izvršavaju proces odgovarajuće obučeni kako da izvršavaju proces				
2.1.6 Izrađen plan izvršavanja procesa				
2.2.1 Sprovedeni dokumentovani planovi, politike, standardi i/ili procedure				
2.2.2 Proizvod zaštite (rada) podvrgnut kontroli verzije, ili odgovarajućem procesu upravljanju konfiguracijom				
2.3.1 Verifikovana usaglašenosti procesa sa primenljivim politikama, standardima i/ili procedurama				
2.3.2 Verifikovana usaglašenosti proizvoda zaštite (rada) sa primenljivim standardima i/ili zahtevima				
2.4.1 Praćen status procesa u skladu sa planom korišćenjem sistema merenja				
2.4.2 Preduzete odgovarajuće korektivne akcije kada proces značajno odstupa od plana				

CL 3: Dobro definisan

Da li oni koji su uključeni u upravljanje procesima na bazi BP-si ***OP Administriranje kontrola zaštite*** izvršavaju neku od sledećih funkcija? Za svaku tvrdnju sa pozitivnim odgovorom navedite dokaz koji ga podržava.

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
3.1.1 Dokumentovan standardni proces ili familija procesa u definicijama standarda organizacije koji opisuje kako implementirati BP-e OP				
3.1.2 Izrađena definicija standardnog procesa organizacije za potrebe specifične upotrebe				
3.2.1 Sprovedena izrađena verzija definicije standardnog procesa organizacije				
3.2.2 Izvršena revizija defekata odgovarajućih proizvoda zaštite (rada)				
3.2.3 Korišćenje podataka o izvršavanju definisanog procesa za upravljanje definisanim procesom				

3.3.1 Koordinisana komunikacija unutar bezbednosnih inženjerskih grupa				
3.3.2 Koordinisana komunikacija između različitih grupa u okviru projekta/organizacije				
3.3.3 Koordinisana komunikacija sa spoljnim grupama učesnika u projektu				

CL 4: Kvantitativno kontrolisan

Da li je sledeće vidljivo ili na raspolaganju onima koji koriste procese ***Administracije kontrola zaštite*** organizacije? Za tvrdnju sa potvrdnim odgovorom navesti dokaz koji ga podržava.

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
4.1.1 Uspostavljeni ciljevi merenja kvaliteta za proizvode zaštite (rada) familije standardnih procesa organizacije				
4.2.1 Kvantitativno određen nivo zrelosti kapaciteta procesa za definisani proces				
4.2.2 Preduzete odgovarajuće korektivne akcije ako se definisani proces ne izvršava unutar nivoa zrelosti kapaciteta procesa				

CL 5: Kontinualno poboljšavan

Da li su sledeće karakteristike vidljive u procesima ***OP Administracije kontrola zaštite*** organizacije? Za svaku tvrdnju sa pozitivnim odgovorom navedite dokaz koji ga podržava.

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
5.1.1 Uspostavljeni kvantitativni ciljevi za poboljšavanje efektivnosti familije standardnih procesa organizacije, na bazi poslovnih ciljeva organizacije i tekućeg nivoa zrelosti kapaciteta procesa				
5.1.2. Kontinualno poboljšavani standardni procesi promenom familije standardnih procesa organizacije radi poboljšavanja njihove efektivnosti				
5.2.1 Izvršavanje uobičajene analize defekata				
5.2.2 Selektivno eliminisanje uzroka defekata u definisanom procesu				
5.2.3 Kontinualno poboljšavanje izvršavanja definisanog procesa, implementacijom svih promena u definisani proces radi povećanja njegove efektivnosti				
5.2.4 Kontinualno poboljšavanje OP izmenom definicije standardnog procesa organizacije, radi povećanja njegove efektivnosti				

PRILOG 11.2: Kontrolna lista za pripremu aktivnosti faze evaluacije na terenu

Kontrolna lista se koristi kao ***pomoćni alat*** za SSAM evaluatore u fazi pripreme za evaluaciju na terenu. U tabeli su opisani glavni događaji koji se moraju kompletirati pre početka faze rada na terenu. Vremenski okviri su približni i zavise od iskustva TE i odnose se na početak faze rada na terenu, a ne koliko vremena treba da se ovi zadaci izvrše.

√	Zadatak	Opis	Odgovornost	Vreme
	Postaviti parametre i definisati granice evaluacije	Sastanci/diskusija da se upravlja očekivanjima u kojima su definisani namena, ciljevi, parametri i ciljevi evaluacije.	evaluator, sponzor	1 − 1,5 mesec
	Uspostavi zahteve za rukovanje osetljivim/ vlasničkim materijalima	Nacrt/odobrenje/potpisivanje svakog neophodnog NDA sporazuma kao i uspostavljanje procedura za skladištenje i odlaganje dokaza koje TE sakupi.	evaluator, sponzor	1 − 1,5 mesec
	Inicijalni sporazum	Odobrenje/potpisivanje sporazuma između evaluatora i Sponzora, koje obuhvata namenu, ciljeve, parametre i objekte evaluacije kako je uspostavljeno u 2.1.1 i 2.1.2 i verifikovanje lica koje će primiti podatke po završetku evaluacije.	evaluator, sponzor	1 − 1,5 mesec
	Uspostavi TE	Izabrati članove TE na bazi kvalifikacija/ standarda postavljenih u SSAM metodu i obezbediti ih sa kompletnim kopijama SSE CMM i SSAM.	evaluator sponzor	1 − 1,5 mesec
	Izabrati projekte za evaluaciju	Rad sa koordinatorom za rad na terenu da se potvrdi raspoloživost projektnog tima, učesnika i menadžera evaluanda i TE; uspostavljanje plana evaluacije koji uključuje pripremu, rad na terenu i fazu posle evaluacije, sa datumima podnošenja i završetka poslednjeg zadatka.	sponzor	1 mesec
	Logistika	Obezbediti odgovarajući radni prostor za rad TE. Potrebno je imati na raspolaganju nekoliko sala za sastanke, različitih veličina za različiti broj učesnika, uključujući najveće sastanke uvodni i završni, 3-4 manje sobe za intervjuisanje projektnog tima i korisnika iz prakse i salu za rad TE. Za rad TE potrebno je obezbediti računarski sistem sa periferijskim uređajima (printer, skener, projektor), kopir mašinu i faks aparat. Poželjno je imati računarski sistem u svakoj prostoriji za intervjuisanje i šire radne sastanke. Po zahtevu TE treba obezbediti ostali sitan pribor potreban za rad TE (markere, krede, tablu, beležnice, papir za štampanje i sl.). U ovoj aktivnosti identifikuje se eventualna pratnja članova TE u toku rada na terenu u evaluiranoj organizaciji, kao i drugi zahtevi koje može postaviti sponzor.	koordinator za rad na terenu, evaluator	2 − 4 sedmice

	Priprema TE	Revizija SSAM sa članovima TE da se obezbedi dobro poznavanje metodologije koja se koristi u procesu evaluacije i razumevanje uloga u izvođenju te evaluacije.	evaluator, TE	1 mesec
	Prilagođavanje upitnika za evaluaciju	Na bazi ciljeva evaluacije, prilagoditi SSE CMM upitnik koji treba da bude kompletiran od strane projektnog tima ESS za razvoj PKI sistema.	evaluator, TE	1 mesec
	Priprema *laptop* računara	Svaki član TE treba da ima na svom računaru za evaluaciju kopije svih kompletiranih upitnika, opise svakog projekta, spisak članova projektnog tima organizacije i ostalih učesnika, kao i kopije SSE CMM i SSAM i prilagođen upitnik za razgovor.	evaluator	7 dana
	Administracija upitnika	Na grupnom sastanku članovi projektnog tima dobiju upitnik na koji na licu mesta odgovaraju.	evaluator, koordinator za rad na terenu, projektni tim za razvoj PKI	2 – 3 dana

PRILOG 11.3: Radna tabela za praćenje podataka (DTS)

Da bi se olakšala analiza odgovora na SSAM upitnik odgovori treba da budu konsolidovani i prebačeni u elektronski tabelarni mehanizam za praćenje – **DTS** (*Data Tracking Sheet*), tipično Excel tabelu. Ova tabela koristi evaluatoru da prepoznaju obrazac i nekonzistentnosti u odgovorima kako u pojedinačnim projektima, tako i u celoj organizaciji. **DTS** predstavlja alat za konsolidovanje odgovora na *Upitnik* i iz *Intervjua* i daje ukupnu sliku prakse sistema zaštite organizacije. TE ***analizira*** DTS i dokaze koji podržavaju odgovore na *upitnik* i *intervijue*. Analiza uključuje traženje neusklađenosti, nekonzistentnosti i neadekvatnosti u odgovorima i navedenim dokazima. Iako ima nekih automatskih proračuna u DTS, sve ulazne podatke treba da kontroliše TE. Struktura DTS dopušta dodavanje informacija od strane onih koji ih obezbeđuju. Cilj da TE može ispravno odrediti da li su odgovori indikator individualnog znanja ili odražavaju istinski nivo kapaciteta organizacije.

Kratak opis: DTS izrađen u *Exce* tabeli ima četiri glavne sekcije (tabela 11.3.1):

OPs

Odgovori na pitanja *(iz pripremne i faze rada na terenu)*

Odgovori na intervjue *(iz jednog ili više projekata – tri)*

Prihvatanje dokaza *(sa konsenzusom TE)*

Tabela 11.3.1 *Uzorak DTS*

OP	Odgovori na upitnik						Odgovori intervjua			Prihvatanje dokaza	Konačno rangiranje
	Pripremna faza/ faza na terenu						Faza rada na terenu(P1 – P6)				
	O1	**O2**	**O3**	**O1**	**O2**	**O3**	L1	L2	L3		
OP01											**100%**
BP	1	1	1	1	1	1	1	1	1	1	100%
…..	1	0	1	0	?	?				0	
GP	1	1	1	1	1	0	1	1	1	1	87%
….											
OP02	1	0	0	0	1	?	1	0	1	1	**50%**
BP											
…..											
GP											
….											

Svaka od ovih sekcija dalje se dekomponuje u nekoliko podsekcija (***radni dokument*** DTS).

OP: sve OP obuhvaćene u SSAM procesu navedene su u krajnje levoj koloni DTS. Svaka ***BP*** i ***GP*** su navedene u individualnim redovima. ***GP*** su navedene za svaku ***OP***.

Odgovori na *upitnike*: kolone odgovora na pitanja koriste se za registraciju odgovora dobijenih na *upitnik* od zaposlenih u organizaciji čiji se kapaciteti poboljšavaju i obezbeđuje preliminarni pogled na profil nivoa rangiranja procesa organizacije, koji TE pokazuje koliko je organizacija blizu da dostigne određeni referentni nivo zrelosti/kapaciteta procesa. Sekcija *Odgovora na upitnik,* DTS deli u ***dve podsekcije***: ***pripremnu fazu*** i ***fazu na terenu.*** Očekuje se da organizacija u celini ili individualni projekti uključeni u evaluaciju, generišu ***odgovor***e na pitanja iz upitnika u toku *pripremne faze* tako da su kolone označene sa ***O1, O2 i O3***. U toku *Faze na terenu* odgovori na *upitnik* odnose se na odgovore rukovodilaca (*project leads*) individualnih projekata rezultate, tako da su kolone odgovora označene sa ***L1, L2, i L3***. U fazi rada na terenu vrši se intervjuisanje rukovodilaca projekata, a rezultati upisuju u kolone ***L1I, L2I,*** Rezultati intervjuisanja praktičara po projektima (do šest) upisuju se u kolonama ***P1.1 – P1.6; P2.1 – P2.6; P3.1 – P3.6*** po pojedinačnim projektima (tri).

Upisivanje odgovora iz upitnika iz *pripremne* i *faze na terenu* u DTS vrši se na sledeći način:

- ***DA* = 1,**
- ***NE* = 0,**
- ***Ne znam* i *prazno* =?.**

***Preliminarno rangiranje nivoa*:** kriterijumi za proračun su:

- procenat (%) odnosno ≥ 50% odgovora *DA* od ukupnog broja odgovora *DA* i *NE*,
- *prazni* i *Ne znam* odgovori se ne uzimaju u proračun,
- ovo je startna pozicija za analizu rezultata intervjua.

Upisivanje odgovora iz intervjua vrši se u isti obrazac DTS za praćenje i administraciju podataka iz sve tri faze intervjua*:*

1. ***rukovodstva projekta*** (*Project Lead),*
2. ***praktičara*** (*Practitioner)* i
3. ***naknadnih intervjua*** *(Follow-Up*).

Kao i odgovore na *upitnik* i odgovore iz *intervjue* prate davaoci odgovora, u DTS grupisani po projektima, ali se podaci razlikuju značajno od onih iz *upitnika*. Namena intervjua sa *rukovodstvom projekta* i *praktičarima* je da ***verifikuje*** ne samo da li se SSE procesi praktično primenjuju u organizaciji, nego i da postoji dokaz koji potvrđuje ovu tvrdnju.

Upisivanje odgovora iz intervjua**:** Za ***verifikaciju***, odgovori intervjua prate se i upisuju u DTS u skladu sa dokazima koje intervjuisani obezbedi. TE jednoznačno označava sve ***dokaze*** sa alfa-numeričkim identifikatorima. Dokaz se u DTS unosi sa:

1 – dokaz za kojeg tim smatra da ima ***dokaznu vrednost*** i da je ***relevantan za BP/ GP***;

0 **–** ako se potvrdi da navedeni dokaz ne postoji, ili se pokaže da nije relevantan, ili intervjuisani koji izvršava odnosnu BP ili GP nije sposoban da odgovori na pitanje;

prazno **–** ako intervjuisani nije pitan odgovarajuća ćelija ostaje prazna.

Prihvatanje dokaza**:** TE analizira sve obezbeđene ***dokaze*** i razmatra kako ih organizacija koristi. Na osnovu prihvaćenih dokaza TE određuje konačan rang zrelosti organizacije.

Prolazi/otpada**:** Neki dokaz *prolazi* (TE ***prihvata***) ili otpada na osnovu odluke članova TE sa pravom glasa sa konsenzusom, kojom se određuje da li su obezbeđeni dokazi dovoljni da se organizaciji dodeli kredit za *implementaciju* neke BP ili GP.

Evidentiranje prihvatanja dokaza**:**

- **za BPs i GPs** gde se obezbeđeni dokazi smatraju ***dovoljnim*** za odgovarajuće dokazivanje, u odgovarajuću ćeliju koja potvrđuje usaglašenost unosi se identifikator:**„1“**;
- **za BPs i GPs** gde se smatra da su obezbeđeni dokazi ***nedovoljni*** ili ***nema*** dokaza upisuje se identifikator: „**0“**;
- **za BPs i GPs** za koje u intervjuu nije postavljeno pitanje, a pripadajuće BPs i GPs imaju određen dokaz „**0“**, upisati **„0“** u odgovarajuću ćeliju;
- **za BPs i GPs** gde nije postavljeno pitanje u intervjuu, a ni jedna pripadajuća BPs ili GPs nema određen dokaz sa „0“, ostaviti „**praznu“** odgovarajuću ćeliju.

Konačno rangiranje: konačan profil rangiranja nivoa zrelosti kapaciteta organizacije sa DTS *Excel* tabelom, automatski se računa za svaku OP na svakom CL, na bazi SSAM kriterijuma.

SSAM kriterijumi za određivanje ranga nivoa kapaciteta (CL) određene OP:

- OP dostiže 1.CL ako su sve BP ***100% izvršene***;
- OP dostiže 2. – 5.CL ako je OP sa prethodnog CL 100% izvršena, a ***najmanje 80% OP*** sa tekućeg CL;
- minimalno ***50% dokaza*** za izvršavanje BP/GP mora biti dokumentovano da se OP smatra izvršenom na nekom CL.

PRILOG 11.4: Radni dokumenti za praćenje kretanja dokaza

Zbog značaja ***identifikacije, sakupljanja, korišćenja i odlaganja*** dokaza za evaluaciju zrelosti/ kapaciteta procesa zaštite, razvijena su četiri **radna dokumenta** (alata) za pomoć u radu i praćenju kretanja dokaznog materijala:

1. ***formular za zahtevanje dokaza*** (*Evidence Request Form);*
2. ***tabela za praćenje zahteva za dokaze*** (*Evidence Request Tracking Sheet*);
3. ***tabela za praćenje korišćenja dokaza*** (*Evidence Use Tracking Sheet)*;
4. ***tabela za praćenje odlaganja dokaza*** (*Evidence Disposal Tracking Sheet*).

Na kraju procesa evaluacije zrelosti/kapaciteta ***formular za zahtevanje dokaza*** može se uništiti, a popunjene **tabele za praćenje** moraju biti prosleđene sponzoru evaluirane organizacije.

Formular za zahtevanje dokaza: ovaj formular koristi SSAM TE da zahteva dokumenta od ovlašćenog koordinatora na radnoj lokaciji. Za održavanje poverljivosti učesnika i članova SSAM tima, ovaj formular ne identifikuje ko je identifikovao postojanje određenog dela dokaza ili ko je od članova SSAM tima zahtevao dokaze.

Formular za zahtevanje dokaza

Posednik dokaza: _____
Koordinator rada: _____
Datum zahteva: _____
Format dokaza: _____
Naziv dokaza: _____
Opis dokaza: _____
Datum prijema: _____

Dokaz	Naziv	Opis	Član SSAM tima	Datum/ vreme zahteva	Datum/ vreme prijema	Datum/vreme povratka
1	SSE CMM priručnik	interpretacija SSE CMM od ***XYZ*** organizacije	član SSAM tima	1.03.2006 u 12.00 h	1.03.2006 u 12.30 č	1.04.2006 u 2.30 č

Tabela za praćenje zahteva za dokaz: Ova radna tabela koristi se u vezi sa obrascem za *Zahtev za dokaze* i omogućava posedniku dokaza da prati usaglašenost organizacije u SSAM procesu sa svim zahtevima za dokaz.

Član SSAM tima	OP	BP/CL	Član projektnog tima	Tip	Naziv	Opis	Datum prijema	Dokaz (broj)
član tima	OP1	BP1	PL 1	dokument	priručnik za SSE CMM	interpretacija SSE CMM od XYZ organizacije	1.04. 2006.	1

Tabela za praćenje korišćenja dokaza: popunjava je član SSAM tima za korišćenje svakog pojedinačnog dokaza.

Dokaz (broj)	Naziv	Opis	Datum/ vreme uništenja	Sredstvo	Datum/ vreme upućivanja organizaciji	Sredstvo	Datum/ Vreme prijema u organizaciji
1	Priručnik za SSE CMM	interpretacija SSE CMM od XYZ organizacije	nije raspoloživo	nije raspoloživo			
2	Zabeleške SSAM tima	interne zabeleške tima u toku sastanaka		spaljena vreća			

Tabela za praćenje odlaganja dokaza: U ovu tabelu unose se podaci o odlaganju dokaza i privremenih proizvoda rada SSAM tima.

PRILOG 11.5: Scenario komunikacija u procesu SSAM evaluacije

1. UVODNI SASTANAK

Dnevni red

1. Uvod u projekat evaluacije
2. Obim projekta u okviru evaluirane organizacije
3. Plan rada
4. Osnovna pravila rada u procesu evaluacije
5. Komunikacija u procesu evaluacije.

Uvod u projekat evaluacije:

- dobrodošlica predstavnika evaluirane organizacije i sponzora evaluacije,
- kontekst evaluacije,
- učesnici evaluirane organizacije (imena, članova i koordinatora rada na terenu),…

Cilj procesa evaluacije:

- profil tekućih procesa CA i akcioni plan poboljšavanja.
- Obim evaluacije:
- primenljivost SSE CMM modela (tip projekta, oblasti procesa),
- ciljni projekat evaluacije (CA PKI; nabrojati projekte koji će biti evaluirani),

- ciljni nivo kapaciteta za izabrane oblasti procesa (OP),
- ciljni procesi za evaluaciju (lista OP koje treba evaluirati),
- korišćenje SSE CMM modela i SSAM metoda (samoevaluacija i poboljšanje procesa),
- organizaciona jedinica za evaluaciju (CA PKI *Univerziteta Singidunum i)*
- izveštavanje (brifinzi – ko i zašto, konačni nalazi – ko i zašto).

Tim za evaluaciju:

- evaluatori,
- koordinator rada na terenu,
- član tima za evaluaciju,
- posmatrači (članovi TE bez prava glasa)…

Upoznavanje sa SSE CMM modelom

- Šta je SSE CMM metodologija evaluacije? (Metod koji se koristi za merenje kapaciteta procesa SSE funkcija organizacije.)
- Šta je SSAM metod evaluacije? (Proces za izvršavanje SSE CMM evaluacije.)
- Kako se tipično mogu izvršavati (***interna samo-evaluacija i identifikacija oblasti za poboljšavanje),*** evaluacija TTPS provajdera usluga (izbor snabdevača)?

Ciljevi evaluacije za evaluiranu organizaciju:

- primarni ciljevi evaluacije (nabrojati),
- prednosti za evaluiranu organizaciju (rezultati pilot projekta evaluacije – profil rangiranja nivoa kapaciteta procesa, nalazi),
- indikacija usaglašenosti sa modelom ….

Proces evaluacije – koristiti opis procesa evaluacije iz osnovnog radnog dokumenta [101].

Poverljivost – osnovno pravilo: *evaluacija zavisi od iskrenosti i otvorenosti diskusija u procesu evaluacije, zahteva da:*

- nijedan projekat ili pojedinac ne mogu biti imenovani u nalazima,
- TE ne može diskutovati ili komentarisati proces evaluacije izvan samog procesa,
- TE ne može prenositi drugim licima informacije koje čuju u procesu evaluacije.

Dinamički plan – u skladu sa dinamičkim planom, planirati vreme održavanja:

- uvodnog sastanka,
- prikupljanja odgovora na *upitnik,*
- intervjuisanja rukovodstva projekta za uspostavljanje CA*XY,*
- intervjuisanja praktičara,
- prezentacije nalaza sponzoru.

Pravila prezentacije nalaza:

- nijedan medij za prezentaciju nalaza ne može se izneti iz zgrade *CAXY,*
- upravljanje sa podacima sakupljenim u procesu evaluacije odobrava sponzor,
- svi učesnici u procesu evaluacije treba da rade prema NDA sporazumu.

Dnevni red sastanka za prezentaciju nalaza:

1. Informacije o procesu evaluacije (cilj, značaj učešća članova evaluirane organizacije,...)
2. Profil rangiranja procesa
3. Nalazi
4. Akcioni plan za poboljšavanje procesa.

Nalazi procesa evaluacije:

- ***sinteza nalaza*** na bazi: odgovora iz *upitnika i intervjua*, dokaza, iskustva i znanja TE,
- ***proces razvoja nalaza***: prikupljanje inicijalnih ulaznih podataka iz brojnih i različitih izvora, analiza podataka, određivanje prioriteta nalaza i predstavljanje,
- ***kriterijumi*** za definisanje ključnih nalaza: samo elementi koji se potencijalno mogu preporučiti i da TE odluke donosi ***konsenzusom.***

Rezultati evaluacije: *profil rangiranja nivoa kapaciteta procesa prikazanih prema* SSE CMM referentnom modelu: bar–dijagram, pita–dijagram ili tabela.

Prezentacija akcionog plana za poboljšavanje OP CA na bazi nalaza.

Završna reč Sponzora.

2. PRIMER OPISA DIREKTNIH (ARTEFAKTA) DOKAZA SSAM METODA EVALUACIJE – PIID:

OP – oblast procesa**; SG –** specifični ciljevi**; BP –** bazične prakse**; PR –** proizvod rada.

OP	SG	BP	Pitanje: Postoje li direktni (DE) i indirektni (ID) dokazi	DA/NE
01	Administriranje kontrola zaštite			
	1.1	Kontrole zaštite su propisno konfigurisane i korišćene		
		01.01.	***Uspostavi odgovornosti i kontrolisane odgovornosti*** PR: Dijagram organizacione strukture u zaštiti PR: Plan/politika zaštite koji opisuje uloge u zaštiti PR: Plan/politika zaštite koji opisuje opšte odgovornosti u zaštiti PR: Dokument zaštite koji opisuje kontrolisane odgovornosti u zaštiti PR: Dokument zaštite koji opisuje autorizacije u zaštiti	
		01.02.	***Upravljaj konfiguracijom kontrola sistema zaštite:.*** PR: Evidencija svih ažuriranja softvera PR: Evidencija svih problema u distribuciji PR: Konfiguracija sistema zaštite PR: Promene konfiguracije sistema zaštite PR: Evidencija svih potvrđenih ažuriranja PR: Periodični zbir distribucije poverljivog softvera PR: Bezbednosne promene projektne dokumentacije PR: Implementacija kontrola zaštite PR: Pregled sistema zaštite PR: Odlaganje kontrola zaštite i plan tranzicije	
		01.03.	***Upravljaj svešću o potrebi zaštite*** PR: Korisnički pregled materijala za obuku o zaštiti PR: Log evidencija obuke i razvoja svesti o potrebi zaštite PR: Periodična procena kompetencija korisnika u odnosu na bezbednost PR: Evidencija o materijalu za obuku, razvoj svesti i edukaciju	
		01.04.	***Upravljaj servisima i kontrolnim mehanizmima zaštite.*** PR: Održavanje administrativnog loga PR: Periodično održavanje i pregledi administracije zaštite PR: Greške u administriranju i održavanju PR: Izuzeća u administraciji i održavanju PR: Liste osetljivosti informacija PR: Liste o osetljivosti medija PR: Evidencija o saniranju, deklasifikaciji i odlaganju medija	

PRILOG 11.6: Projekat za razvoj i poboljšavanje *OP18 SSE CMM*

Cilj: *planirati i implementirati proces poboljšavanja standardnih SSE procesa.*

Zadatak 1:

Na bazi dokumentovanih rezultata SSAM (SSE CMM) evaluacije tekućih procesa ESS analizirati i shvatiti rezultate evaluacije:

- analizirati profil zrelosti kapaciteta procesa (OP01 – OP22),
- analizirati stvarne performanse tekućih procesa (neformalno izvršavanje, slabo planiranje, dokumentovanje i analiza rezultata),
- analizirati nalaze o snazi i slabostima i
- izvršiti *gap* analizu profila evaluiranih, tekućih i željenih procesa.

Zadatak 2:

Izraditi akcioni plan projektne grupe za poboljšavanje procesa (1 ili grupe OP) organizacije na bazi analize uticaja potencijalnog poboljšavanja na postizanje ciljeva procesa, raspoloživih resursa i prema dinamici koja odgovara CAXY.

- Planirati i dokumentovati poboljšavanje procesa u saopštenju politike zaštite CAXY i planu projekta poboljšavanja procesa.
- Planirati i dokumentovati (u politici i planu) uobičajenu analizu defekata i odstupanja performansi procesa od planiranih i očekivanih.
- Planirati i dokumentovati metod implementacije poboljšavanja procesa u politici i/ili procedurama, uključujući merenja koja treba izvršiti za praćenje (tipa IDEAL, 6 OMEGA i sl.) .

Zadatak 3:

Izvršiti i dokumentovati promene standardnih SSE procesa ESS u cilju održavanja željenog poboljšavanja.

- Redefinisati i dokumentovati standardni proces sa izvršenim poboljšavanjem.
- Revidirati (po potrebi) uputstvo za poboljšavanje procesa.

Zadatak 4:

Upoznati sve učesnike projekta i druge grupe (ako je potrebno) o izvršenom poboljšavanju standardnih SSE procesa.

- Izraditi i dokumentovati listu poboljšanih elemenata/procesa sa opisom razloga za poboljšavanje i promena na standardnim SSE procesima.
- Izraditi i dokumentovati plan projekta za implementaciju promena (poboljšanja) standardnih SSE procesa.
- Za razvoj i poboljšavanje ove OP kao *ulazne kriterijume* treba uzeti i procese *definisanja standardnog procesa – OP17* i *obezbeđivanja bezbednosnih ulaza – OP09*.

PRILOG 11.7: Uzorak: Akcioni plan projektnog tima za poboljšanje procesa

Uvod – glavni rezultati izvršene evaluacije (pregleda, provere)

1. Cilj/obim
   - 1.1 Izjava o identifikovanju problema
   - 1.2 Vizija rešenja problema posle uspešnog izvršavanja plana
   - 1.3 Izjava o dugoročnom (strateškom) cilju poboljšavanja procesa
2. Ulazni kriterijumi
   - 2.1 Sponzor projekta odobrava i obezbeđuje proces poboljšanja
3. Glavni ulazni parametri
   - 3.1 Relevantne informacije iz procesa evaluacije (profil OP/slabosti)
   - 3.2 Relevantni tekući rad (projekat/zadaci/pilot projekat/poboljšavanje OP i rezultati)
4. Kratak sadržaj pristupa
   - 4.1 Koraci/zadaci za OP (bazirani na praksama)
   - 4.2 Kratkoročni scenario (vremenski plan za implementaciju)
5. Glavni izlazni parametri
6. Izlazni kriterijumi

Detaljni plan

7. Programerska pitanja
   - 7.1 Ograničenja
   - 7.2 Pretpostavke/zavisnosti
   - 7.3 Faktori rizika
   - 7.4 Alternative
8. Dinamički plan
   - 8.1 Koraci faza poboljšanja procesa
   - 8.2 Dijagram projekta poboljšavanja procesa (PERT/GANTT)
9. Zahtevani resursi
   - 9.1 Ljudi (ko/koliko radnih sati)
   - 9.2 Obuka
   - 9.3 Računarski/tehnološki resursi
   - 9.4 Ostalo
   - 9.5 Plan upravljanja

10. Provere (revizije) projekta (kontrolne tačke)

- 10.1 Neposredne opservacije
- 10.2 Revizije upravljanja projektom
- 10.3 Druge vrste revizije
- 10.4 Kriterijumi merenja progresa projekta (*benčmarking*)

11. Plan marketinga/implementacije/obuke

Nacrt plana procesa merenja progresa projekta:

I Uvod (namena, obim)
II Organizaciona i projektna pitanja
III Opšti pristup merenjima
IV Pristup za metrike upravljanja projektom
V Pristup za tehničke metrike
VI Pristup za uvođenje metrika u organizaciju
VII Skupljanje i korišćenje metrika
VIII Uloge i odgovornosti
IX Plan komunikacije/povratnih informacija
X Lista merenja

Primeri metrike za CL 2: metrike procesa *Upravljanja bezbednosnim zahtevima:*

1. osetljivost (nepredvidljivost) zahteva – procenat izmene zahteva
2. broj zahteva po tipu ili statusu – definisani, revidirani, odobreni i implementirani
3. kumulativan broj izmena alociranih zahteva, uključujući ukupan broj predloženih, tekućih, odobrenih i ugrađenih izmena u osnovnim konfiguracijama objekata sistema
4. odnos broja zahteva za izmene po mesecu, u poređenju sa originalnim brojem zahteva dostavljenih za dati projekat
5. utrošeno vreme, rad i novac za implementaciju zahtevanih promena
6. broj i veličina zahtevanih izmena posle završetka faze podnošenja zahteva
7. troškovi implementacije zahteva za promene
8. broj zahteva za promene prema ukupnom broju zahteva za promene u toku životnog ciklusa projekta
9. broj prihvaćenih, ali neimplementiranih zahteva za promene
10. broj zahteva za promene i dodatke osnovnoj konfiguraciji (*baseline*).



REČNIK TERMINA ISMS-A

ENGLISH	SRPSKI
access control	kontrola pristupa
access control policy	politika kontrole pristupa
access rights	pravo pristupa
accident	nesreća
accidental threat	slučajna prijetnja
accountability	kontrolisana (dokaziva) odgovornost
administrative controls	upravljačke kontrole zaštite
advanced digital signature	napredan elektronski potpis
alternative site	rezervna lokacija
asset	Imovina, resurs
asset inventory	popis imovine (resursa), iventar
attack	napad
audit	provera, revizija
authentication	provera identiteta
authenticity	autentičnost
authorization	ovlašćenje, autorizacija
availability	raspoloživost, dostupnost
awareness programmes	programi razvoja svesti o potrebi zaštite
backup copy	rezervvna kopija; bezbednosna kopija
BCP testing	testiranje plana kontinuiteta poslovanja
best-practice	najbolja praksa, najbolja iskustva
business continuity	kontinuitet poslovanja
business continuity management	upravljanje kontinuitetom poslovanja

business continuity officer/coordinator	rukovodilac za kontinuitet poslovanja
Business Continuity Plan	plan kontinuiteta poslovanja; plan neprekidnosti poslovanja
Business Impact Analysis	analiza uticaja na poslovanje
catastrophic impact	katastrofalan učinak
certification body	certifikaciono telo
Chief Information Security Officer	rukovodilac informacijske bezbednosti
Chief Security Officer	rukovodilac bezbednosti
classified agreement	klasifikova sporazum
classified contract	klasifikovan ugovor
classified information	klasifikovane informacije
complete security check	potpuna bezbednosna provera
confidential	povjerljivo (stepen tajnosti podataka)
confidentiality	poverljivost
confidentiality agreement	sporazum o tajnosti
consent of the subject	pristanak ispitanika
control	*kontrola zaštite*; bezbednosna mera; mera zaštite
control objective	cilj kontrole zaštite
corporate security	korporativna bezbednost
corrective action	korektivna mera; korektivna akcija
corrective controls	korektivne kontrole; popravne mere
cost-effectiveness	isplativost; rentabilnost
Crisis Management Support Team	tim za podršku kriznom menadžmentu
Crisis Management Team	tim za krizni menadžment
Crisis Manager	krizni menadžer
critical activity	kritična aktivnost
critical business process	kritičan poslovni process
critical infrastructure	kritična infrastruktura
cryptographic material	kriptomaterijali
cryptographic techniques	kriptografske tehnike/metode
cryptomaterial	kriptomaterijali
cybercrime	kompjuterski kriminal (kiber kriminal)
data classification level	stepen tajnosti podatka
data protection	zaštita podataka
data recovery	oporavak podataka
data restore	restauracija podataka
detective controls	kontrole otkrivanja

deterrent controls	kontrole odvraćanja
digital certifcate	digitalni sertifikat
digital signature	digitalni potpis
disaster	havarija
disaster recovery plan	plan oporavka nakon havarije
effectiveness	efektivnost (stepen ostvarivanja aktivnosti)
efficiency	efikasnost (rezultati/uloženi resursi)
electronic document	elektronski dokument
electronic record	elektronski zapis
electronic signature	elektronski potpis
employee training	obuka zaposlenih
event	događaj
event scenario	scenario događaja
gap analysis	analiza neusaglašenosti (razlika)
guideline	smernica
hardware	hardver
hot site	vruća lokacija
identification	identifikacija
identity certificate, see alsodigital certificate	digitalni sertifikat
impact	uticaj
impact assessment	procena uticaja
incident	incident; neželjeni događaj
incident management	upravljanje incidentom
incident response plan	plan odziva na incident
information access rights	prava na pristup informacijama
information asset	informaciona imovina (resurs)
information asset management	upravljanje informacionom imovinom
information security	informaciona bezbednost
Information Security Advisor	savetnik za informacionu bezbednost
Information Security Consultant	konsultant za informacionu bezbednost
information security event	događaj informacione bezbednosti
information security incident	incident informacione bezbednosti
information security incident management	upravljanje incidentom informacione bezbednosti
Information Security Management System	sistem upravljanja zaštitom informacija
Information Security Manager	menadžer informacione bezbednosti
information security policy	politika zaštite informacija

information security risk	rizik informacione bezbednosti
information security standard	standard zaštite informacija
information system	informacioni sistem
information system incident	incident u informacionom sistemu
Information System Management Committee	odbor za upravljanje IKTsistemom
information system recovery	oporavak IKTsistema
information system security policy	politika bezbednosti IKT sistema
Information Systems Auditor	revizor IKT sistema
Information Systems Security Professional	stručnjak za bezbednost IKT sistema
infrastructure	infrastruktura
in-house recovery	interni oporavak
integrated security	integralna bezbednost
integrity	integritet, celovitost (podataka/informacija)
intentional threat	namerna pretnja
internal audit	Interna provera; unutarnja revizija
ISMS (information security management system)	menadžment sistem zaštite informacija
Lead Auditor	glavni proveravač (auditor, revizor)
logical controls	logičke kontrole zaštite
loss of classified data	gubitak klasifikovanih podataka
malicious code, see also malware	maliciozni program
malware	malver
management controls	upravljačke kontrole zaštite
management review	menadžerska revizija (provera)
management system	menadžment sistem; sistem upravljanja
mandatory procedures	obvezne procedure
manned security	telesna zaštita
monitoring	monitoring, nadzor, praćenje
nonconformance	neusaglašenost
nonconformity, see also nonconformance	neusaglašenost
non-information related event	ne-informacioni događaj
non-repudiation	neporecivost
organisational controls	organizacione kontrole zaštite
outsourcing	iznajmljivanje usluga (podugovarača)
PDCA Cycle (Plan-Do-Check-Act)	PDCA ciklus (uspostavljanje, implementacija, održavanje, poboljšavanje)
personal data	lični podaci

personal data filing system	zbirka ličnih podataka
Personal Data Protection Act	zakon o zaštiti ličnih podataka
physical controls	fizičke kontrole
physical protection measures	kontrole fizičke zaštite
physical security	fizička bezbednost
physical security incident	incident fizičke bezbednosti
policy	politika
preventative/preventive controls	preventivne kontrole zaštite
preventive action	preventivne akcije
privilege management	odobravanje privilegija
privileged access	privilegovan pristup
procedure	procedura
process	proces, postupak
qualitative risk assessment	kvalitativna procena rizika
quantitative risk assessment	kvantitativna procena rizika
record	zapis
record management	upravljanje zapisima
Recovery Point Objective	ciljna tačka oporavka
recovery time objective	ciljno vrieme oporavka
registration	evidentiranje
reliability	pouzdanost
residual risk	preostali rizik
resilience	otpornost
restricted	ograničeno (stepen tajnosti podatka)
risk	rizik
risk acceptance	prihvatanje rizika
risk analysis	analiza rizika
risk assessment	procena rizika
Risk Assessment Report	izveštaj o proceni rizika
risk assessment tools	alati za procenu rizika
risk avoidance	izbegavanje rizika
risk communication	komunikacija o rizicima
risk criteria	kriterijumi za prihvatanje rizika
risk estimation	vrednovanje rizika
risk evaluation	evaluacija rizika
risk impact	uticaj rizika; posledica rizika

risk management	menadžment (upravljanje) rizika
risk mitigation	ublažavanje rizika
risk monitoring	praćenje rizika
risk probability	verovatnoća rizika
risk reduction	smanjenje rizika
risk transfer	prenos rizika
risk treatment	obrada rizika, tretman rizika
risk treatment plan	plan obrade rizika, plan tretmana rizika
safety	stanje zaštićenosti od šteta, nezgoda i drugih neželjenih događaja, sigurnost
scope	opseg
secret	tajna (stepen tajnosti podatka)
security	stanje zaštićenosti od mogućih napada čija je svrha nanošenje štete/ozleda/gubitaka; bezbednost; zaštita
security accreditation	bezbednosna akreditacija (IKT sistema)
security check	bezbednosna provera
security guard services	servisi telesne zaštite
security incident	bezbednosni incident
security policy	bezbednosna politika
Single Point of Failure	jedinstvena tačka prekida
social engineering	socijalni inženjering
software	softver, program
Statement of Acceptance of the ISMS Documents	Izjava o prihvatljivosti dokumenta ISMS-a
Statement of applicability	Izjava o primenjivosti
surveillance visit of the certification body/ auditor	poseta sertifikacionog tela/proveravača
technical (security) measures; technical controls	tehničke (mere) kontrole zaštite
technical security	tehnička zaštita (hardversko softverski mehanizmi zaštite)
threat	pretnja; ugrožavanje
tolerable period of disruption	tolerantno vreme prekida
top secret	strogo poverljivo
unacceptable risk	neprihvatljiv rizik
unauthorized disclosure (of classified information)	neovlašteno otkrivanje (klasifikovanih informacija)
unavailability	neraspoloživost

unclassified information	neklasifikovane informacije
unwanted event	neželjeni događaj
user privileges	korisnička prava
vital business process	ključni poslovni process
vulnerability	ranjivost
weakness	slabost

Preuzeto sa: http://wiki.iso27001standard.com/index.php?title=Glossary

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

LITERATURA

1. Aizuddin A., *The common criteria ISO/IEC 15408– the insight, some thoughts, questions and issues,* http://www.niap.nist.gov/cc-scheme, 2002.
2. Anderson D. J., Schragenheim E., *Agile Management for Software Engineering: Applying the Theory of Constraints for Business Results,* Prentice Hall, 2003.
3. *AS 13335.1:2003, Australian Standard Information technology – Guidelines for the management of IT Security, 2003.*
4. B. Boehm and Turner, R., *Principles Behind the Agile Manifesto,* Pearson Education, Boston, MA, www.agilealliance.org/principles.htm, 2003.
5. Bahan C, *The Disaster Recovery Plan*, http://www.sans.org, 2003.
6. Banjanin K.M., *Metodologija inženjeringa – inženjerske analize i mreže znanja*, DIS PUBLIC, Beograd, 2006.
7. Barker William C., *Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST SP800-60-1 i 2, http://www.csrc.nist.gov/publications, juni 2004.
8. Barton R., Hery J. W., Liu Peng, *An S-vector for Web Application Security Management*, Penn State University, PA, *rbarton@psu.edu*, 2004.
9. Bate R., and all, *A Systems Engineering Capability Maturity Model V.1.1*, Software Engineering Institute, www.sei.cmu.edu, US DoD, 1995.
10. Bishop M., *Introduction to Computer Security, Chapter 18: Evaluating Systems,* Wesley and Sons, November 1, 2004.
11. Bjork Fredrik, *Security Scandinavian Style-Interpreting the practice of managing information security in organizations*, Stockholm University, Rozal Institute of Technology, 2001.
12. British Standards Institution, *BS 7799-2 — Code of Practice for Information Security Management*, http://www.bsi.org, http://www.iso.org, 1999.
13. Brown, S. Castell, G. Gray, P. Muller, *User Requirements for Trusted Third Party Services, INFOSEC Project Report S2101/01,* Commission of the European Communities, DG XIII, B-6, Oct 1993.
14. BSI (Nemačke), *IT Baseline Protection Manual*, *http://www.bsi.bund.de/gshb*, juli 2005.
15. Carrol M.J., *Computer Security*, Butterworth-Heinemann, 1997.
16. CCIMB-99-031, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, Version 2.1, http://www.commoncriteria.org, 1999.

17. CERT, *http://www.cert.org/advisories*, 2003.
18. Chrissis M. B., Konrad M., Shrum S., *CMMI v.1.2, Guide for process integration and product improvement* , Second Edition, SEI, Addisoon-Wesley, 2007.
19. COBIT, *Cobit-Control Objectives for Information and Related technologies,* http://*www.ITgovernance.org,* http://*www.isaca.org/cobit,* 2000.
20. *CRAMM,* http://www.crammusergroup.org.uk, 2004
21. Curtis B.l, Hefley E. W., Miller S.**,** *People Capability Maturity Model* [SM]**,** CM SEI**,** www.sei.cmu.edu, 1995.
22. Domarev V.V.,*Защита информациии и безопасность компьютерных систем*, http://www.security.ukrnet.net/, 1997.
23. DTI- UK Department of Trade and Industry, *Process understanding and improvement*, www.dti.gov.uk.quality/process, 2006.
24. Ferraiolo Karen & Sachs Joel E., *Distinguishing Security Engineering Process Areas by Maturity Levels*, USA Columbia, ferraiolo@md.arca.com, sachs@interramp.com, 1996.
25. Ferraiolo Karen M.**,** *Considerations for Re-architecting the SEI CMM and Building Engineering CMMs,* Arca Systems, Inc., ferraiolo@arca.va.com, 1995.
26. GAISP – *Generally Accepted Information Security Principles*, http://www.gaisp.org, 2003.
27. Gaskell Gary, *Information Security Standards*, http://www.nist.gov/publications/public_affairs/standards.htm, 2001.
28. GCIO Guidelines, *Information Security Guidelines v.6.0,* www.gcio.com, *2007*.
29. Grance T., Kent K., Kim B., *Computer Security Incident Handling Guide*, NIST SP 800-61, http://www.nist.gov/publications, January 2004.
30. Grubor G., Milosavljević M., *Osnovi zaštite informacija*, Univerzitet Singidunum, 2010.
31. Gutošić H., *Upravljanje kvalitetom ISO 9000 i okolinsko upravljanje ISO 14000*, Sarajevo, 2001.
32. Hefner R., Ph.D, *Lessons Learned with the Systems Security Engineering Capability Maturity Mode*l, rick.hefner@trw.com, 2000.
33. Hefner Rick Ph.D, and Monroe W., *System Security Engineering Capability Maturity Model*, TRW, CA, rick.hefner@trw.com, 1997.
34. Hopkinson J. P., *System security engineering capability maturity model – Organization profiles*, EWA-Canada, John.Hopkinson@sympatico.ca, 2003.
35. Hopkinson John P., *The Relationship Between The SSE CMM and IT Security Guidance,* EWA-Canada, John.Hopkinson@sympatico.ca, 1999.
36. Housley R. i dr., *Internet X509 Public Key Infrastructure: Certificate and CRLProfile (RFC 2459),* http://www.ietf.org/rfc/rfc2459.txt, 2002.
37. http://www.itu.org, *ITU X.800*, 2002.
38. *IEC/ISO 17799:2000 Security Standard overview,* http://www.securityauditor.net/iso17799/what.htm, 2005.
39. Information Security & Business Continuity Academy, *ISO 27001 implementation checklist,* www.iso27001standard.com, 2011.
40. Information Security & Business Continuity Academy, *How to deal with BCM sceptics?*, www.iso27001standard.com, 2011.
41. Information Security & Business Continuity Academy, *ISO 27001 vs. ISO, 27002,* www.iso27001standard.com, 2011.
42. Information Security & Business Continuity Academy, *How to conduct an internal audit according to ISO 27001 and BS 25999-2,* www.iso27001standard.com, 2011.
43. Information Security & Business Continuity Academy, *Is it possible to calculate the Return on Security Investment (ROSI)?,* www.iso27001standard.com, 2011.
44. Information Security & Business Continuity Academy, *BS 25999-2, A leading business continuity standard,* www.iso27001standard.com, 2011.

45. InformationShield, *Using Information Shield publications for ISO/IEC 27001 certification*, www.informationshield.com, 2011.
46. Injac N., *Mala enciklopedija kvalitete – Proces menadžment*, Zagreb, 2004.
47. International Federation of Accountants, *Managing Security of Information*, *www.ifa.org,* 1998.
48. *Introduction to the OCTAVE® Approach*, http://www.cert.org/octave, 2005.
49. ISACA, *IS Auditing Procedure*: *Security Assessment Penetration Testing and Vulnerability Analysis,* Document #8, http://www.isaca.org, 2004.
50. ISACA, *Standards for Information Systems Control Professionals*, http://www.isaca.org, 1999.
51. ISF, *The Standard for Good Practice for Information Security*, http://www.isf.org, V.4.0., 2006.
52. ISO/IEC 13335-1, *Management of information and communications technology security*, www.iso.org, 2004.
53. ISO/IEC 15408, *Common Criteria for IT Evaluation User Guide*, *http://csrc.nist.gov/cc/info/infolist.htm.*
54. ISO/IEC 15443, *Information Technology-Security Techniques,* http://www.iso.15443.org, 2000.
55. ISO/IEC 15504 (CMM), *http://www.iso.15504.org,* 2000.
56. ISO/IEC 27001, *Information Technology – Code of practice for information security management,* http://www.iso.org, 2005.
57. ISO/IEC 27002, *Information Technology – Code of practice for security controls,* http://www.iso.org, 2006.
58. ISO/IEC 27005, *Information Technology – Code of practice for risk management,* http://www.iso.org, 2009.
59. ISO/IEC 27006, *Information Technology – System Security Certification and Acreditation,* http://www.iso.org, 2010.
60. ISO/IEC 21827 (SSE CMM), *System Security Engineering Capability Maturity Model*, http://www.iso.21827.org., 2008.
61. ISO/IEC JTC 1/SC 27, ISO/IEC TR 15443-1: 2004, *Information Technolog–Security Techniques – A framework for IT security assurance – Part 1: Overview and framework*, http://www.iso.15443-1.org, 2004.
62. ISO/IEC 13335 – *Gudelines for the management of IT Security,* http://www.iso.13335.org, 2003.
63. ISO/IEC 15408 – *Common Criteria/ITSEC* , http://www.iso.15408.org, 2003.
64. *IT Baseline Protection Manual***,** *http://www.bsi.bund.de/gshb*, 2000.
65. IT Governance Institute, *COBIT* (*Control Objectives for Information and related Technology*) 3rd Edition, 2000, *www.ITgovernance.org, www.isaca.org.*
66. ITU-T Recommendation X.509, *Information Technology – Open system Interconnection – The directory: Public key and attribute certificate frameworks,*
67. Joshi J., *IS 2620: Developing Secure Systems, Secure Software Development Models/ Methods*, http://www.sis.pitt.edu/~jjoshi/courses/IS2620/Spring07/, Jan. 16, 2007.
68. Kelm S., *The PKI page*, http://www.pkipage.org, 2004.
69. Kormos C., & all, *Using security metrics to assess risk management capabilities,* NSA, Arc Systems, Booz, Allen & Hamilton, Inc., ckormos@radium.ncsc.mil, 2005.
70. Kulpa K. M., & Johnson A.K., *Interpreting the CMMI: A Process Improvement Approach,* Auerbach Publications, 2003.
71. Lee A., Brewer T., *Information security within the system development life cycle,* Jones Computer Security Division Information Technology Laboratory NIST, http://www.itl.nist.gov/, 2004.
72. Locher, Christian, *Methodologies for evaluating information security investments*, 2005.
73. Markus G. K., *Compromising emanations: eavesdropping risks of computer displays*, December 2003.
74. McLean, *Mature and Secure: Creating a CMMI® and ISO/IEC 21827 Compliant*

Process Improvement Program, Booz, Alen, Hamilton, VA April 11, 2006.
75. NIST SP 800-14, *Generally Accepted Principles and Practices for Security*, http://csrc.nist.gov/publications/nistpubs/800-14/sp800-14.pdf, 2002.
76. NIST SP 800-12, *Security Handbook*, http://www.nist.gov/publications, 2003.
77. NIST SP 800-53, *Recommended Security Controls For Federal IS*, http://csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf, 2004.
78. NIST SP 800-61, *Computer Security Incident Handling Guide*, http://csrc.nist.gov/publications/nistpubs/index.html, 2004.
79. NIST, *FIPS 140-2*, http://www.itl.nist.gov/fipspubs, 2003.
80. NIST, *Trusted Computer System Evaluation Criteria*, *http://www.radium.ncsc.mil/tpep,* 1999.
81. *OCTAVE methods and criteria*, http://www.cert.org/octave, 2005.
82. Ozier W., *Risk Analysis and Assessment*, *Handbook of Informaton Security Management 1999,* CRC Press, Boca Raton, Florida, 1999.
83. Pankaj G., *CS497 – Security engineering and software engineering,* Indian Institute of Technology, Kanpur, India, e-mail: [pankajgo]@cse.iitk.ac.in, 2005.
84. Partida A., Andina D., *IT Security Management*, Springer, www.springer.com/series/7818, 2010.
85. Petrović R.S., Čekerevac Z., Grubor G., *Security System Engineering Capability Maturity Model in The ICT Security,* 10. međunarodna naučna konferencija, "Rešavanje kriznih situacija u specifičnim prostorima", Fakultet specijalnog inženjerstva, ŽU, Žilina, Slovačka, 2005.
86. Purser S., *A practical guide to managing information security,* Artech House, Boston, London, www.artechhouse.com, 2005.
87. Registar ISO sertifikata, http://www.iso-27001certificates.com
88. Richard B. Waina, P.E. Ph.D, *Five critical questions in process improvement Part II*, www.mdmaturity.com, 2006.
89. Ross R., Swanson M., &all, *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST SP 800-37, http://www.csrc.nist.gov/publications, 2004.
90. RSA Data Security Conference, *Functional Model TTPS S2101/03* v.1.1, San Jose, CA, http://www.solutioncentre.nl, 1999.
91. Russel D. & Gangemi G.T. sr., *Computer Security Basics*, O'Reilly and Ass., 1995.
92. Sademies A., *Process approach to information security metrics in Finish industry and state institutions,* VTT Elektronics Publications 544, http://www.vti.fi/inf/pdf, ESPOO, 2004.
93. SANS Institute, *Information Security Policy & Best Practices*, http://www.sans.org/policies, 2003.
94. SANS Institute, *Introduction to business continuity planning*, http://www.sans.org, 2002.
95. Savola R., *Measurement of Security in Processes and Products*, www.vitt.ele, 7.04.2005.
96. Schell P.G., McLeod Jr. R., *Management Information Systems,* 9. izdanje, Pearson Prentice Hall, SAD, 2004.
97. SEI, *Appraisal Method for Process Improvement (SCAMPI^{SM}) A, Version 1.2: Method Definition Document,* SCAMPI Upgrade Team, www.sei.cmu.edu, 2006.
98. SEI, *CMMI ARC*: *Appraisal Requirements for CMMI,* http://www.sei.cmu.edu/publications/documents/01.reports/01tr034, 2007.
99. SEI, *CMMI MDD: Method Description Document*, http://www.sei.cmu.edu/publications/documents/01.reports/01tr034, 2007.
100. SEI, *SSAM: SSE Capability Maturity Model Appraisal Method,* Version 2.0, www.sei.cmu.edu, april 16, 1999.
101. SEI, Systems *Security Engineering Capability Maturity Model®, SSE-CMM® Model Description Document,* Version 3.0, www.sei.cmu.edu, 2010.

102. Sigurjon Thor Arnason, Keith D. Willett, *How to Achieve 27001 Certification, Auerbach Publications, London,* www.auerbach-publications.com, 2008.
103. Shawn Presson, *Communication Loops Within the CMMI®*, White Paper, Apogen Services, LLC, www.sei.cmu.edu, 2006.
104. Spears J., Barton R., Hery W., *An Analysis of How ISO 17799 and SSE-CMM Relate to the S-vector Methodology*, http://www.ebrc.psu.edu, avgust 2004.
105. Stoneburner G., *Underlying Technical Models for Information Technology Security Services*, NIST SP 800-33, http://csrc.nist.gov/publications/nistpubs/80033/sp800-33.pdf, decembar 2003.
106. Swanson M., & all, *Security Metrics Guide for Information Technology Systems*, NIST SP 800-55, http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf,, 2003.
107. Swanson M., *Security Self-Assessment Guide for Information Technology Systems*, NIST SP 800-26, http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf, 2001.
108. UK Department of Industry, *A Taxonomic Model of Trusted Third Party Services*, Gamma Secure Systems, Diamond House, Frimley Road, Camberley, 2002.
109. University of Dallas Center of Information Assurance, *Information Assurance Best Practices Definition*, http://gsmweb.udallas.edu, 2007.
110. US Department of Homeland Security, *Federal Computer Incident Response Center: Incident Handling Checklists*, http://www.fedcirc.gov/incidentResponse/ IHchecklists.html, 2003.
111. US Department of Health and Human Services, *Standard HIPAA*, http://www.hhs.gov/ocr/hipaa/finalreg.html, 2011.
112. US General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, www.fas.org/irp/gao/aim96084.htm, 1996.
113. USA CERT, www.uscert.org, 2005.
114. Van Wyk K. R., Graff G.M., *Survey and Analysis of Related Standards*, webmaster@securecoding.org. 2003.
115. Williams R. J., Ferraiolo K. M., *P3I – Protection Profile Process Improvement*, Arca Systems, Inc., http://www.arcasystems.com, 2003.
116. Yngström L., Chaula J. A., Kowalski S., *Security metrics and evaluation of information Systems security*, Department of Computer and Systems Sciences, Stockholm University/ KTH, E-mail: si-jac1, louise2, stewart3}@dsv.s, 2004.
117. Zadjura J., *An Introduction to Certification and Accreditation v. 1.4*, SANS Institute, http://www.sans.org, 2003.
118. Zahran Dr S., *Software Process Improvement*, Addison-Wesley, NY, 2005.
119. Zimmie K.M., *Secure and Mature: Combining SCAMPI CMMI model with an ISO/IEC 21827 (SSE CMM Appraisal or SSAM metod.)*, Booz, Allen & Hamilton, Inc., ckormos@radium.ncsc.mil, 2006.

Na osnovu člana 23. stav 2. tačka 7. Zakona o porezu na dodatu vrednost („Službeni glasnik RS", br. 84/04... i 61/07), Odlukom Senata Univerziteta Singidunum, Beograd, broj 260/07 od 8. juna 2007. godine, ova knjiga je odobrena kao osnovni udžbenik na Univerzitetu.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

007:004.056(075.8)

ГРУБОР, Гојко, 1949-
Projektovanje menadžment sistema zaštite informacija / Gojko Grubor. - Beograd : Univerzitet Singidunum, 2011 (Loznica : Mladost grup). - XX, 375 str. : graf. prikazi, tabele ; 25 cm

Tiraž 300. - Rečnik termina ISMS-a: str. 363-369. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 371-375

ISBN 978-86-7912-398-5

a) Информациона технологија - Безбедност
COBISS.SR-ID 188609804

© 2012.

Sva prava zadržana. Nijedan deo ove publikacije ne može biti reprodukovan u bilo kom vidu i putem bilo kog medija, u delovima ili celini bez prethodne pismene saglasnosti izdavača.