

**UNIVERZITET
SINGIDUNUM**

Fakultet za poslovnu informatiku
Danijelova 32, 11000 Beograd

**RAZVOJ I UPRAVLJANJE PROGRAMOM ZAŠTITE ZASNOVANIM NA
MODELU SAZREVANJA PROCESA**

Doktorska disertacija

Mentor:

Prof. Dr Milan Milosavljević

Kandidat:

mr Gojko Grubor, dipl. inž

Beograd, decembar 2007

KATALOGIZACIJA

KOMISIJA

1. Prof. Dr Milan Milosavljević
2. Prof. Dr Milovan Stanišić
3. Prof. Dr Branko Kovačević

ZAHVALNICA

U izradi ovog rada 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 razumevanje koje su mi pružili u periodu teoretskog i istraživačkog rada na disertaciji.

Posebno se zahvaljujem članovima komisije, mentoru **Prof. Dr Milanu Milosavljeviću**, prorektoru Univerziteta Singidunum na inicijativi, punoj podršci, datim sugestijama i ukupnom pozitivnom pristupu i ličnom doprinosu u definisanju forme i sadržaja rada u pripremi, realizaciji i odbrani i **Prof. Dr Milovanu Stanišiću**, rektoru Univerziteta Singidunum na razumevanju potrebe, odobravanju teme, stvaranju opštih uslova za realizaciju disertacije i ukupnom angažovanju u radu ispitne komisije. Izuzetno se zahvaljujem **Prof. Dr Branislavu Kovačeviću**, rektoru Beogradskog univerziteta na angažovanju u radu ispitne komisije, iznetim sugestijama i velikom doprinosu da rad dobije formu i kvalitet na zahtevanom nivou.

Za timski rad u procesu SSAM evaluacije u istraživačkom delu rada, uložene napore i utrošeno vreme zahvaljujem se članovima Tima za evaluaciju *Univerziteta Singidunum* **Dr Mladenu Veinoviću, Časlavu Maksiću, Zoranu Antoniću i Saši Ivanoviću** i pridruženim članovima Tima za evaluaciju, zaposlenim u evaluiranoj organizaciji **Đakonović Miljanu, Đukanović Ani, Jagodić Predragu i Vujnović Marijani**. Posebno se zahvaljujem vlasnicima i menadžerima evaluirane organizacije **Srećku Atanackoviću**, generalnom direktoru i **Mirni Kojić Veljović**, tehničkom direktoru i Sponzoru evaluacije na razumevanju, punoj podršci i strpljenju zbog objektivnih destruktivnih efekata procesa evaluacije na poslovanje organizacije.

Za nesebičnu pomoć u reinženjeringu aplikacije **SSE CMM/SCAMPI Appraisal Assistant**, tehničku obradu rada i iznete sugestije o dizajnu i grafičkim priložima zahvaljujem se Časlavu Maksiću, diplomcu FPI, Univerziteta Singidunum.

ABSTRACT

The systems and processes approaches and structural and object oriented modeling give the best result in designing, development and ICT security practice. The system security processes that transform inputs into outputs and expectedly improve value of the outputs parameters, integrate procedures, tools and skillful and motivated people to perform security practice tasks. The security processes should be continuously evaluated and improved, since owners, managers and common users have generally underdeveloped security awareness and security technologies and experts are relatively expensive. The process oriented standards and models based on CMM (*Capability Maturity Model*), particularly SSE CMM (*System Security Engineering Capability Maturity Model*) have been developed to evaluate quality, and measure progress of process maturity and improvement. Comparative analyses of standards and models correlation, based on *system*, *process* or *environment* approaches, indicate there are number of possibilities to establish more frame for process evaluation and improvement. The CMMs that integrate processes (SSE CMM, CMMI) provide integrated and unique frame to evaluate and improve different processes. The SSE CMM Integrate SSE (11), project-managing (5) and organizational (6) process areas. In the SSE CMM, process performance quality and maturity are measured by specific system and process oriented metric, based on basic (BP) and generic (GP) practices performance and implementation criteria. The SSE CMM metric rates the capability (CL) and maturity (ML) levels into 5 active levels. The SSAM (*System Security Appraisal Method*) based on the SSE CMM model, is specifically developed to perform *verification* type of evaluation that not only *discover* but *verify* objective data of the BP and GP practices performance an implementation. Experimental evaluation of the current ESS processes on three evaluated projects and processes improvement *action plan proposal* confirm declared users acceptability and applicability of the SSE CMM model and the SSAM method to the security processes evaluation and improvement for the optimal security program development, security organization profiling and number of the other ICT security application.

KRATAK SADRŽAJ

Sistemski i procesni pristup, strukturno i objektno orijentisano modelovanje daju najbolje rezultate u projektovanju, razvoju i praksi IKT zaštite. Procesni pristupi, koji transformišu ulazne veličine u izlazne i očekivano povećavaju izlazne vrednosti, integrišu procedure, alate i ljude, motivisane za izvršavanje prakse zaštite, fundamentalni su blokovi za izgradnju sistema zaštite. Procesne zaštite treba neprekidno poboljšavati, zbog generalno slabo razvijene svesti vlasnika, menadžera i korisnika o potrebi zaštite i relativno skupih tehnologije i stručnjaka zaštite. Za evaluaciju kvaliteta i merenje progresivnog sazrevanja i poboljšavanja procesa, razvijeni su procesno orijentisani standardi i modeli na bazi CMM modela procesa, specifično SSE CMM model za procese zaštite. Komparativna analiza komplementarnosti standarda i modela razvijenih na bazi pristupa sistemu, procesu ili okruženju, ukazuje na mogućnost uspostavljanja više okvira za evaluaciju i poboljšavanje procesa. CMM modeli koji integrišu procese (SSE CMM, CMMI) obezbeđuju integrisani i jedinstven okvir za evaluaciju i poboljšavanje različitih procesa. SSE CMM model integriše sistem-inženjerske (11), projektno-upravljačke (5) i organizacione (6) oblasti procesa. Kvalitet izvršavanja i sazrevanja procesa zaštite u SSE CMM modelu, meri se specifičnom metrikom orijetisanom i na sistem zaštite i na procese, na bazi kriterijuma za izvršavanje i implementaciju bazičnih (BP) i generičkih praksi (GP). SSE CMM metrika rangira nivoe kapaciteta (CL) i zrelosti (ML) u 5 aktivnih nivoa. Za evaluaciju procesa zaštite na bazi SSE CMM modela specifično je razvijen SSAM metod verifikacione evaluacije, koji otkriva i verifikuje objektivne dokaze o izvršavanju i implementaciji BP i GP. Eksperimentalna evaluacija tekućih procesa ESS na tri evaluirana projekta i predlog akcionog plana poboljšavanja procesa, potvrđuju korisničku prihvatljivost i deklarisanu primenljivost SSE CMM modela i SSAM metoda evaluacije procesa zaštite za razvoj optimalnog programa zaštite, profilisanje organizacija zaštite i druge brojne aplikacije u oblasti IKT zaštite.

PREGLED TABELARNIH PRIKAZA

Tabela 2.1.1.	Zahtevi za stabilan proces
Tabela 2.3.1.	Uporedivost indikatora nivoa bezbednosti za evaluaciju u relevantnim standardima kvaliteta proizvoda i sistema zaštite
Tabela 2.3.2.	Osnovne karakteristike standarda ISO/IEC 17799
Tabela 2.3.3.	Zbirni pregled metoda za evaluaciju u relevantnim standardima zaštite
Tabela 2.4.1.	CMM modeli, reprezentacije i oblasti primene
Tabela 2.4.2.	Objavljeni modeli sazrevanja procesa zaštite
Tabela 2.4.3.	Razvoj SSE CMM modela
Tabela 2.4.4.	Nivoi kapaciteta-CL i zrelosti-ML procesa SSE CMM modela
Tabela 2.4.5.	Oblasti procesa u tri opšte kategorije SSE CMM
Tabela 2.4.6.	Međizavisnosti OP i GP SSE CMM modela procesa
Tabela 2.4.7.	Broj BP po OP u SSE CMM modelu
Tabela 2.4.8.	Zajedničke karakteristike (CF) po nivoima kapaciteta (CL)
Tabela 2.4.9.	Raspored CF po CL SSE CMM modela
Tabela 2.4.10.	Principi sazrevanja procesa zaštite u SSE CMM modelu
Tabela 2.4.11.	Bezbednosni ciljevi sa atributima primene
Tabela 2.4.12.	Metodi merenja IKT zaštite
Tabela 2.5.1.	Faze procesa SSAM metoda evaluacije
Tabela 2.5.2.	Kvalifikacije i odgovornosti primarnih učesnika u procesu evaluacije
Tabela 2.5.3.	Zahtevi za radno angažovanje u SSAM procesu evaluacije
Tabela 2.5.4.	Neki kriterijumi za izbor projekata za evaluaciju
Tabela 2.6.1.	Aplikativne razlike dve reprezentacije CMMI modela
Tabela 2.6.2.	OP po kategorijama u CL i CM reprezentaciji CMMI modela
Tabela 2.6.3.	Stepen institucionalizacije procesa po GG
Tabela 2.6.4.	Zbirni prikaz GG i pripadajućih GP CMMI v.1.2 modela
Tabela 2.6.5.	Osnovne karakteristike klasa SCAMPI metoda evalua
Tabela 2.6.6.	Kriterijumi za rangiranje CL u kontinualnoj reprezentaciji
Tabela 2.7.1.	Kompatibilnost SSE CMM i ISO/IEC 15504
Tabela 2.7.2.	Komplementarnost SSE CMM, ISO/IEC 17799, ISO/IEC 13335 i NIST
Tabela 2.7.3.	Zbirni pregled metoda za procenu sistema zaštite
Tabela 2.7.4.	Prezentacija uporedivih OP CMMI i SSE CMM modela procesa
Tabela 2.7.5.	Mapiranje ostalih komponenti CMMI i SSE CMM modela
Tabela 2.7.6.	Uporedni pregled SSE CMM i drugih modela IKT zaštite
Tabela 2.7.7.	Mapiranje ISO 9001 prema CMMI modelu procesa
Tabela 2.8.1.	OP P-CMM modela po nivoima zrelosti
Tabela 2.8.2.	Kategorije OP i nivoi zrelosti P-CMM modela
Tabela 2.8.3.	Korelacija kontrola zaštite standarda ISO 17799 i S-vektora
Tabela 2.8.4.	Korelacija OP zaštite SSE CMM standarda i S-vektora
Tabela 2.8.5.	Tipična klasifikacija bezbednosnih zahteva

PREGLED SLIKA I GRAFIČKIH PRIKAZA

Slika 2.1.1.	Tri nivoa sistemskog inženjerstva
Slika 2.1.2.	Izlaz strukturnog modelovanja sistema osnovne IKT zaštite
Slika 2.1.3.	Proces zaštite kao transformator ulaznih parametara u izlazne
Slika 2.1.4.	Generički proces sistema zaštite
Slika 2.1.5.	Proces kao integrator ljudi, metoda i tehnologije
Slika 2.1.6.	Troškovi, prednosti i nedostaci modela procesa
Slika 2.4.1.	Struktura SSE CMM modela sazrevanja procesa zaštite
Slika 2.4.2.	SSE CMM kategorije procesa
Slika 2.4.3.	Međusobni odnosi bezbednosno orijentisanih OP
Slika 2.4.4.	Nivoi kapaciteta procesa zaštite u kontinualnoj prezentaciji
Slika 2.4.5.	Sazrevanje procesa po ML SSE CMM modela
Slika 2.4.6.	Sazrevanje OP po CL u SSE CMM modelu
Slika 2.4.7.	Implementacija SSE CMM nivoa zrelosti SSE procesa
Slika 2.4.8.	Dijagram rasta CL procesa u funkciji porasta troškova
Slika 2.4.9.	Primena SE CMM OP u integrisanim procesima SE za analizu rizika i bezbednosnu garanciju
Slika 2.4.10.	Primena SSE CMM OP u procesu analize rizika
Slika 2.4.11.	SSE CMM OP kao integralni deo ukupnog SE procesa
Slika 2.4.12.	SSE CMM OP za izgradnju argumenata za garantovanu bezbednost
Slika 2.4.13.	Primer profila nivoa kapaciteta OP organizacije za Integraciju sistema
Slika 2.4.14.	Model metrike IKT zaštite
Slika 2.5.1.	Model faza i koraka procesa SSAM evaluacije
Slika 2.5.2.	Princip dostizanja nivoa kapaciteta OP SSE CMM modela
Slika 2.6.1.	Struktura CMMI modela u obe reprezentacije
Slika 2.6.2.	Evolucija nivoa zrelosti i kapaciteta u CMMI modelu
Slika 2.6.3.	Profili rangiranja nivoa zrelosti (a) i kapaciteta (b) OP CMMI modela
Slika 2.6.4.	Komponente CMMI modela
Slika 2.6.5.	Primer CL (GG i GP) profila grupe OP (SG i SP)
Slika 2.6.6.	Faze i procesi SCAMPI metoda evaluacije
Slika 2.7.1.	Razvoj životnog ciklusa politike zaštite
Slika 2.7.2.	Korelacija OP SSE CMM i uključenih članova ISO/IEC 17799 standarda
Slika 2.7.3.	Programi za poboljšavanje procesa
Slika 2.7.4.	Integracija SSE procesa u životni ciklus SE procesa
Slika 2.7.5.	Metod integracije SSE CMM i CMMI procesa
Slika 2.8.1.	Odnosi metoda obezbeđivanja i redukovano modela životnog ciklusa
Slika 2.8.2.	Nivoi i atributi kapaciteta OP P-CMM modela
Slika 2.8.3.	Oblasti procesa P-CMM po nivoima zrelosti
Slika 2.8.4.	Model IDEAL za implementaciju CMMI i SSE CM procesa
Slika 2.8.5.	Razvoj metrike zaštite
Slika 2.8.6.	Odnosi metrike procesa i metrike zaštite
Slika 2.8.7.	Odnosi SSE CMM metrike procesa i metrike zaštite
Slika 2.8.8.	SSE CMM merljivi atributi procesa
Slika 2.8.9.	SSE CMM merljivi atributi sistema zaštite
Slika 2.8.10.	Primena SSE CMM metrika procesa i sistema zaštite
Slika 2.8.11.	Dijagram razvoja metrika zaštite
Slika 2.8.12.	Moguće metrike servisa Kontrole pristupa
Slika 2.8.13.	Odnosi SSE CMM OP i metrika za OP upravljanja rizikom
Slika 2.8.14.	Proces upravljanja web aplikacijom primenom metodologije S-vektora
Slika 4.1.	Model osnovnog metoda istraživanja
Slika 5.1.1.	Referentni profil procesa CA
Slika 5.1.2.	Profil nivoa zrelosti kapaciteta tekućih procesa ESS

SKRAĆENICE KORIŠĆENE U RADU

ARC (<i>Appraisal Requirements for CMMI</i>)	Zahtevi za CMMI evaluaciju
ASE (<i>Assurance Security Evaluation</i>)	Klasa za evaluaciju bezbednosne garancije u CC standardu
AVP	Antivirusni program
BAR	Brza analiza rizika
BP (<i>Basic Practices</i>)	Bazične prakse u CMM i SSE CMM modelima
BS (British standard)	Britanski standard (BS 7799 standard zaštite uključen u ISO/IEC 17799)
BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>)	Nemačka agencija za zaštitu informacija
CA (<i>Certification Authority</i>)	Sertifikaciono telo u sistemu infsatrukture sa javnim ključem.
CBA-IPi (<i>CMM Based Appraisal for Internal Process Improvement</i>)	Evaluacija internih procesa na bazi CMM modela
CC (<i>Common Criteria</i>)	Standard opštih kriterijuma, odnosno, <i>ISO 15408</i> standard za evaluaciju proizvoda i sistema zaštite
CEM (<i>CC Evaluation Methodology</i>)	Metodologija CC evaluacije
CEM (<i>Common Evaluation Methodology</i>)	Opšta metodologije za evaluaciju
CF (<i>Common Features</i>)	Opšte karakteristike u CMM i SSE CMM modelima
CIRT (<i>Computer Incident Response Team</i>)	Interventni tim za odgovore na kompjuterski incident.
CL (<i>Capability Level</i>)	Nivo kapaciteta procesa u CMM modelima procesa
CL (<i>Capability Levels</i>)	Nivoi kapaciteta procesa u CMM i SSE CMM modelima
CMM (<i>Capability Maturity Model</i>)	Model (generički) sazrevanja procesa.
CMMI (<i>Capability Maturity Model Integration</i>)	Integracioni model sazrevanja procesa za proizvodnju, snabdevanje i servise.
CoBIT (<i>Control Objectives for Information and Related Technology</i>)	Kontrolni ciljevi za informacione i odnosne tehnologije
COBRA (<i>Risk Assessment Methodology</i>)	Metodologija za procenu rizika
CPS (<i>Certification Practice Statement</i>)	Izjava o praksi sertifikacije; elemenat politike zaštite PKI.
CTCPEC (<i>Canadian Trusted Computer Product Evaluation Criteria</i>)	Kanadski kriterijumi za evaluaciju proizvoda poverljivih računarskih sistema

DAC (Discret Access Control)	Diskreciona kontrola pristupa sa dodelom prava pristupa na bazi odluke vlasnika sistema
DS	Digitalni sertifikat
DoD (Department of Defence)	Minisatratvo odbrane SAD
DTS (Data Tracking Sheet)	Radna <i>Excel</i> 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
ESS (E-Smart Systems)	Evaluirana organizacija
ETVX (<u>E</u> nt <u>r</u> y C <u>r</u> iteria, <u>T</u> asks, <u>V</u> erification, and <u>e</u> Xit Criteria)	IBM, SEI <i>ETVX</i> format za opis procesa
FIPS (Federal Information Processing Standards)	Standardi procesiranja federalnog IKT sistema SAD
GAISP (General <u>y</u> 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)	<i>Generičke prakse</i> u CMM, SSE CMM i CMMI modelima
KB UBS	Kreditni biro udruženih banaka Srbije.
iCMMI (Integrated Capability Maturity Model)	Integrisani model sazrevanja procesa
IDEAL (Initiating, Diagnosing, Establishing, Acting and Learning)	Model <i>SEI</i> instituta za implementaciju SSE CMM i CMMI procesa.
IEC (International Electronig Committee)	Međunarodni komitet za elektroniku
IKT	Informaciono-komunikacione tehnologije
ISF (International Security Forum)	Međunarodni forum za bezbednost i zaštitu
ISMS (Information Security Management System)	Sistem za upravljanja zaštitom informacija
ISO (International Standardization Organization)	Međunarodna organizacija za standardizaciju
ISSEA (International Systems Security Engineering Association)	Međunarodna asocijacija za sistemsko inženjerstvo zaštite informacija
ITSEC (Information Technology Security Evaluation Criteria)	Kriterijumi za evaluaciju zaštite IKT sistema
ITSEC (Information Technology Security Evaluation Criteria)	Kriterijumi/uputstvo za evaluacije zaštite IKT sistema
ITSEM (Information Technology Security Evaluation Manual)	Uputstvo za evaluaciju zaštite informacija

MAC (Mandatory Access Control)	Obavezna kontrola pristupa
MDD (Method Description Document)	Dokument za opisivanje SCAMPI metod
ML (Maturity level)	Nivo zrelosti procesa u CMM modelima procesa
NDA (Non Disclose Agreement)	Ugovor o neotkrivanju informacija
NIST (National Institute of Standards and Technology,)	Nacionalni institut za standarde i tehnologiju (SAD)
NOSSS (Native Operative System Security Subsystem)	Podrazumevani podsistem zaštite osnovnog operativnog sistema.
OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation)	Metod analize rizika i evaluacije ranjivosti od operativno kritičnih pretnji za imovinu organizacije.
OP (Oblast procesa)	Proces Area u CMM modelima
OS (Operation System)	Operativni sistem računara/mreže
P-CMM (Personal Capability Maturity Model)	Model sazrevanja kompetencije personala
PII (Practice Implementation Indicator)	Indikator implementacije praksi u SCAMPI metodu evaluacije procesa
PIID (PII Description)	Opis identifikatora implementacije prakse u SCAMPI metodu evaluacije
PIP (Process Improvement Program)	Program za poboljšavanje procesa
PKI (Public Key Infrastructure)	Infrastruktura sa javnim ključem; sistem asimetrične kriptografije.
CP (Certificate Policy)	Politika sertifikacije
PP (Protection Profile)	Profil zaštite u CC standardu
RFP (Request for proposal)	Zahtev za predlog, klasa u CC standardu
SAMM (Security Assesment Matirity Model)	Metod evaluacije procesa zaštite na bazi SSE CMM modela.
SSAM PIIID	Opis PII u SSAM metodu evaluacije
SBC (Security By Consensus)	Model sistema zaštite sa konsenzusom
SCE (Software Capability Evaluation)	Evaluacija kapaciteta za razvoj softvera
SE (System Engineering)	Sistemska inženjering ili sistemski pristup,
SE CMM (System Engineering Capability Maturity Model)	Model sazrevanja procesa u sistemskom inženjerstvu

SEI (<i>Software Engineering Institute</i>)	Institut za inženjerstvo softvera, <i>Carnegy Mellon</i> Univerziteta u SAD
SG (<i>Specific Goals</i>)	Specifični cilj u CMMI modelu procesa
SLA (<i>Seciruty Level Agreement</i>)	Sporazum o nivou servisa (zaštite)
SP (<i>Specific Practice</i>)	Specifična praksa u CMMI modelu procesa (kao BP u SSE CMM modelu)
SSE (<i>System Security Engineering</i>)	Sistemska inženjerstvo u oblasti IKT zaštite.
SSE CMM (<i>System Security Capability Maturity Model</i>)	Model i metod sazrevanja procesa zaštite.
ST (<i>Security Target</i>)	Bezbednosni cilj u CC standardu
S-vektor (<i>Security Vector</i>)	Vektor zaštite.
SW CMM (<i>Capability Maturity Model for Software Development</i>)	Model sazrevanja procesa za razvoj softvera
TCB (<i>Trusted Computing Base</i>)	Baza poverljivog računarskog sistema
TCMM (<i>Trusted CMM</i>)	Poverljivi CMM
TCSEC (<i>Trusted Computer System Evaluation Criteria</i>)	Kriterijumi za evaluaciju poverljivog računarskog sistema (SAD standard, tzv. „ <i>Orange book</i> “)
TE (<i>Evaluation team</i>)	Tim za evaluaciju u procesima SSAM i SCAMPI metoda evaluacije
TEMPEST (<i>Transient Electro - Magnetic Pulse Surveillance Technology</i>)	Tehnologija za snimanje tranzijentnih elektro-magnetnih (kompromitujućih) impulsa
TOE (<i>Target of Evaluation</i>)	Cilj (objekat) evaluacije u CC standardu
TSF (<i>Target Security Function</i>)	Bezbednosna funkcija objekta evaluacije u CC standardu
TSM (<i>Trusted Software Methodology</i>)	Metodologija poverljivog softvera
TSP (<i>Target Security Policy</i>)	Politika zaštite objekta evaluacije u CC standardu
TTPS (<i>Trusted Third Party Service</i>)	Servis poverljive treće strane; u oblasti zaštite servis poverljivog provajdera zaštite

SADRŽAJ

Katalogizacija.....	i
Komisija.....	ii
Zahvalnica.....	iii
Abstract.....	iv
Pregled tabelarnih prikaza.....	v
Pregled slika i grafičkih prikaza.....	vi
Skraćenice korišćene u radu.....	vii
1. Uvod.....	1
2. Standardi i modeli kvaliteta procesa zaštite.....	4
2.1. Metodologija sistemskog inženjerstva i procesi zaštite.....	4
2.1.1. Uvod.....	4
2.1.2. Sistemski pristup.....	4
2.1.3. Modelovanje sistema zaštite.....	6
2.1.3.1. Struktirno modelovanje IKT i sistema zaštite.....	6
2.1.3.2. Objektno orijentisani pristup modelovanju sistema zaštite.....	8
2.1.4. Procesni pristup sistemu zaštite.....	10
2.1.5. Modeli procesa najbolje prakse zaštite.....	12
2.1.6. Definisanje standardnog procesa zaštite.....	14
2.2. Poboljšavanje procesa zaštite.....	15
2.2.1. Uvod.....	15
2.2.2. Koncepti poboljšavanja procesa zaštite.....	16
2.2.2.1. Značaj komunikacije za poboljšavanje procesa zaštite.....	17
2.2.3. Struktuirani pristup za poboljšavanje procesa.....	18
2.2.3.1. Evaluacija procesa zaštite.....	18
2.2.3.2. Modeli i okviri za poboljšavanje procesa.....	19
2.3. Pregled standarda kvaliteta proizvoda i sistema zaštite.....	21
2.3.1. Uvod.....	21
2.3.2. Standardi i modeli kvaliteta proizvoda i sistema zaštite.....	22
2.3.2.1. Kriterijumi za evaluaciju poverljivih kompjuterskih sistema.....	23
2.3.2.2. Kriterijumi/uputstvo za evaluaciju zaštite IKT sistema.....	24
2.3.2.3. Opšti kriterijumi za evaluaciju proizvoda i sistema zaštite (CC).....	25
2.3.2.4. Standard za evaluaciju kriptografskih algoritama i modula.....	29
2.3.2.5. Komparativna analiza relevantnih standarda kvaliteta proizvoda i sistema zaštite.....	30
2.3.3. Standard ISO/IEC 17799 za upravljanje zaštitom.....	31
2.4. Modeli sazrevanja procesa zaštite.....	32
2.4.1. Uvod.....	32
2.4.2. Razvoj i struktura generičkog modela sazrevanja procesa.....	33
2.4.3. Model i metod sazrevanja procesa zaštite.....	34
2.4.3.1. Struktura i opis SSE CMM modela.....	35
2.4.3.2. Prednosti i nedostaci SSE CMM modela.....	45
2.4.4. Metrika IKT zaštite i modela sazrevanja procesa zaštite.....	49
2.5. Metodi evaluacije i poboljšavanja procesa zaštite.....	51
2.5.1. Uvod.....	51
2.5.2. Ciljevi i izlazni rezultati evaluacije.....	52
2.5.3. Metod evaluacije primenom modela sazrevanja procesa zaštite.....	52
2.5.4. Uloge i odgovornosti učesnika SSAM procesa evaluacije.....	54
2.5.5. Tipovi SSAM procesa evaluacije.....	55
2.5.6. Promenljivi parametri procesa evaluacije.....	56
2.5.7. Rezultati i izveštavanje SSAM procesa evaluacije.....	58
2.6. Integrirani model i metod evaluacije procesa.....	58
2.6.1. Uvod.....	58

2.6.2.	Struktura CMMI modela.....	59
2.6.3.	Institucionalizacija procesa u CMMI modelu	63
2.6.4.	Osnove SCAMPI metoda evaluacije	64
2.6.5.	Preporuke za primenu SCAMPI v.2.1. metoda evaluacije	68
2.7.	Komplementarnost standarda kvaliteta procesa.....	69
2.7.1.	Uvod	69
2.7.2.	Komplementarnost SSE CMM i drugih standarda zaštite.....	70
2.7.3.	Komplementarnost CMMI i SSE CMM modela procesa	72
2.7.3.1.	Usklađivanje procesa CMMI i SSE CMM modela	75
2.7.3.2.	Komplementarnost CMMI modela i ISO 9000 standarda	76
2.7.3.3.	Komplementarnost CMMI modela i ISO 9000 standarda	78
2.7.3.4.	Komplementarnost CMMI i agilnih metoda za evaluaciju procesa	79
2.8.	Primene modela sazrevanja procesa zaštite	80
2.8.1.	Uvod	80
2.8.2.	Primene SSE CMM modela za razvoj programa zaštite	81
2.8.2.1.	SSE CMM principi za razvoj programa zaštite	81
2.8.2.2.	SSE CMM proces razvoja optimalnog programa zaštite	82
2.8.3.	Primene SSE CMM za profilisanje procesa organizacija u zaštiti	82
2.8.4.	Primena SSE CMM za obezbeđivanje argumenata bezbednosne garancije	83
2.8.5.	Profilisanje kompetencija personala u oblasti zaštite (P-CMM)	84
2.8.5.1.	Struktura P-CMM modela	85
2.8.6.	Komplementarna metrika CC i SSE CMM za razvoj bezbednosnih zahteva.....	87
2.8.6.1.	Razvoj profila zaštite PKI X509 digitalnog sertifikata	88
2.8.7.	Primena SSE CMM metrike za procenu kapaciteta za upravljanje rizikom	89
2.8.7.1.	Razvoj metrike za procenu kapaciteta za upravljanje rizikom.....	89
2.8.8.	Metodologija S-vektora za zaštitu Web aplikacija.....	93
2.9.	Pregled dostupnih istraživanja primena modela sazrevanja procesa zaštite	98
2.9.1.	Uvod	98
2.9.2.	Dostupna istraživanja primene modela sazrevanja procesa zaštite.....	98
3.	Ciljevi istraživanja.....	101
3.1.	Osnovni problemi zaštite informacija.....	101
3.2.	Hipoteze istraživanja.....	102
3.3.	Ciljevi istraživanja	103
4.	Istraživački rad.....	104
4.1.	Predmet i obim istraživanja	104
4.2.	Metodi istraživanja	104
4.3.	Tok izvršavanja projekta ssam evaluacije ESS	105
4.4.	Instrumenti istraživanja	108
4.5.	Uzorkovanje dokaza i izveštavanje o sekundarnim nalazima	108
4.6.	Opis projekta SSAM evaluacije tekućih procesa ESS	109
5.	Analiza rezultata i predlog poboljšavanja procesa ESS.....	112
5.1.	Analiza rezultata evaluacije procesa ESS.....	112
5.1.1.	Izbor željenog profila procesa ESS.....	112
5.1.2.	Analiza rezultata SSAM evaluacije tekućih procesa ESS	113
5.1.3.	Analiza glavnih nalaza SSAM evaluacije ESS	116
5.1.4.	Komparativna analiza referentnog i tekućeg profila procesa ESS.....	118
5.2.	Poboljšavanje tekućih procesa ESS	119
5.2.1.	Praksa poboljšavanja procesa	119
5.2.2.	Akcionni planovi za poboljšavanje procesa ESS.....	120
5.2.2.1.	Uloge u procesu poboljšavanja procesa	121
5.2.2.2.	Tipična infrastruktura procesa Poboljšavanja procesa	122
5.3.	Analiza iskustava iz SSAM procesa evaluacije.....	122
5.3.1.	Odstupanja od SSE CMM modela	122
5.3.2.	Odstupanja od procesa SSAM metoda evaluacije.....	123

5.3.3. Iskustva iz sprovođenja <i>Plana evaluacije tekućih procesa ESS</i>	124
5.3.3.1. <i>Iskustva iz vođenja intervjua</i>	125
5.3.3.2. <i>Sugestije za Sponzora</i>	125
6. Diskusija dobijenih rezultata	126
7. Zaključci	130
8. Ključni termini	133
9. Literatura	139
Prilog 2.1A – Pravila SE razmišljanja	144
Prilog 2.1B – Kriterijumi i uzorci za definisanje i opis procesa	145
Prilog 2.2A – Stabilnost i poboljšavanje stabilnosti procesa zaštite	150
Prilog 2.4A – Kratak opis <i>OP</i> i <i>BP</i> u <i>SSE CMM v.3.0</i> modelu	158
Prilog 2.4B – <i>SSE CMM v.3.0</i> model: pregled oblasti kapaciteta	167
Prilog 2.5A – Primer <i>Upitnika</i> za <i>SSAM</i> evaluaciju	169
Prilog 2.5B – Radna tabela za praćenje podataka (<i>DTS</i>)	172
Prilog 2.5C – Radni dokumenti za praćenje kretanja dokaza	175
Prilog 2.5D – Scenario komunikacija u procesu <i>SSAM</i> evaluacije	177
Prilog 2.6A – Tabela 1. <i>Osnovne karakteristike klase SCAMPI metoda evaluacije</i>	180
– Tabela 2. <i>Procene relevantnih učesnika za SCAMPI intervjuisanje</i>	181
Prilog 2.6B – Primer <i>SCAMPI PIID</i> prema <i>CMMI v. 1.2</i> modelu procesa	182
Prilog 2.8A – <i>SSE CMM</i> kriterijumi za razvoj optimalnog programa zaštite	183
Prilog 2.8B – Razvoj referentnih profila zrelosti <i>OP</i> organizacija zaštite	187
Prilog 2.8C – Kriterijumi za izbor nivoa zrelosti <i>P-CMM</i> kapaciteta	192
Prilog 2.8D – Opis ključnih <i>P-CMM OP</i>	194
Prilog 2.8E – Uspostavljanje <i>PP</i> standardnog <i>PKI X.509 v.3</i> digitalnog sertifikata	198
Prilog 5.1A – <i>Appraisal Assistant</i> generisani rezultati evaluacije	198

1. Uvod

Bezbednosne potrebe savremenih poslovnih sistema informaciono-komunikacionih tehnologija (IKT), određene su njihovim osnovnim karakteristikama: *globalno umrežavanje*, *velika složenost*, *izdavanje beta verzija programa zaštite* i **evolutivni razvoj funkcionalnih i bezbednosnih programa**.

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. Zbog toga, čak i kada se primeni adekvatan pristup zaštite, rezultujući nivo zaštite obično ostaje nepoznat. Proizvodi i sistemi zaštite dolaze na tržište posle dugotrajnog i skupog razvoja, sa evaluacijom ili bez evaluacije u praksi zaštite, 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 rizika IKT sistema. Takođe, korisnici često servise zaštite *poverljivosti*, *integriteta* i *raspoloživosti* informacija, [104], u praksi IKT zaštite, smatraju više teorijskim i „umetničkim“ aktivnostima, a implementiraju ih malobrojni eksperti za zaštitu, najčešće na ličnu inicijativu.

U pogledu operativnog rada i održavanja komponenti i sistema zaštite u praksi zaštite, osnovni zahtev je da svaki korisnik/vlasnik računarskog sistema/mreže bude svestan potrebe zaštite IKT sistema i da neprekidno poboljšava praksu zaštite u krajnje nebezbednom Internet okruženju, [82], i održava operativnost sistema zaštite i garantovani nivo bezbednosti na prihvatljivom nivou rizika, što zahteva *stabilnost*, *ponovljivost*, *efektivnost* i *efikasnost*, odnosno, **zrelost procesa** zaštite.

U savremenim poslovnim IKT sistemima neki oblik podrazumevane zaštite informacija već postoji u samom operativnom sistemu (OS) računara. Podrazumevani sistem zaštite je podsistem zaštite samog operativnog sistema (**NOSSS** - *Native Operative System Security Subsystem*), koji je sastavni deo brojnih, komercijalno raspoloživih platformi (tipa *Windows*, *Linux* i sl.), ali ih u najvećem broju slučajeva krajnji korisnici retko, ili uopšte ne konfigurišu u fazi instalacije OS, pa ova komponenta zaštite računarskog sistema često ostaje nedovoljno i neadekvatno iskorišćena. Takođe, neke oblike upravljačkih i operativno-organizacionih **kontrola zaštite** planiraju i implementiraju administratori sistema i mreža u planu osnovne zaštite informacija i objekata IKT sistema, najčešće, bez definisane *Politike zaštite* i razvoja *Plana zaštite*. Takav rudimentarni sistem zaštite u najgorem slučaju obuhvata mrežnu barijeru (*firewall*), [30] i neki program za antivirusnu zaštitu (AVP), koje projektanti i implementatori IKT sistema planiraju i bez posebnog uključivanja i konsultovanja specijalista zaštite.

Glavne posledice ovako *neformalno izvršavanih procesa* i rešenja savremenih *reaktivnih* sistema zaštite, koji reaguju uglavnom na *poznate* pretnje, su: ne postojanje obavezne i standardima preporučene dokumentacije zaštite (programa, politika, procedura, plana i uputstava zaštite); *ad hoc* rešenja tekućih problema u projektima zaštite; često nepotrebna i redundantna rešenja; preskupa tehnička rešenja sa nedovoljnim efektima ublažavanja realnih faktora bezbednosnog rizika; nemogućnost adekvatnog reagovanja na kompjuterske incidente i vanredne događaje zbog nepostojanja planova i osposobljenih interventnih timova tipa **CIRT** (*Computer Incident Response Team*), [34], [109], ili **CERT** (*Computer Emergency Response Team*), [19], [110] i neadekvatna obuka i obrazovanje u zaštiti, [25]. Međutim, postojanje procesa koji se (neformalno) izvršavaju, osnovna je pretpostavka za primenu klase **modela sazrevanja procesa** - CMM (*Capability Maturity Model*), posebno jedinstvenog modela i metoda sazrevanja procesa zaštite - SSE CMM (*System Security Engineering Capability Maturity Model*), odnosno standarda ISO/IEC 21827 (2002.).

Kompozicija rada obuhvata 9 poglavlja: (1) *UVOD*, (2) *STANDARDI I MODELI KVALITETA PROCESA ZAŠTITE*, (3) *CILJEVI ISTRAŽIVANJA*, (4) *ISTRAŽIVAČKI RAD*, (5) *ANALIZA REZULTATA I PREDLOG POBOLJŠAVANJA TEKUĆIH PROCESA ESS*, (6) *DISKUSIJA DOBIJENIH REZULTATA*, (7) *ZAKLJUČCI*, (8) *KLJUČNI TERMINI* I (9) *LITERATURA*.

POGLAVLJE 2. težišno obuhvata teoretski deo rada kroz 9 potpoglavlja. U **2.1 potpoglavlju** definisani su osnovni elementi metodologije sistemskog inženjerstva: sistem, opšta teorija sistema, sistemski pristup, sistemsko mišljenje i sistemska analiza, kao potencijalni alati u istraživačkom delu rada. U potrebnoj meri opisani su procesno orijentisani strukturni i objektno orijentisani modeli sistema zaštite, a detaljno razmatrani procesni pristup, procesi zaštite i zahtevano poboljšavanje procesa da bi procesi očekivano povećavali izlazne vrednosti. U **potpoglavlju 2.2.** definisani su kvalitet procesa i evaluacija kao nužne pretpostavke svakom poboljšavanju procesa, a detaljnije su opisani ključni atributi improvizovanih, poboljšanih i institucionalizovanih procesa, kao i neformalni pristup poboljšavanju produktivnosti, adaptivnosti i korisničke prihvatljivosti procesa. U **potpoglavlju 2.3** dati su pregled i kratka komparativna analiza standarda i modela kvaliteta proizvoda i sistema zaštite, baziranih na evaluaciji: proizvoda/sistema/ servisa, okruženja i procesa, a sa ciljem otkrivanja kompatibilnih i komplementarnih elemenata. Model i metod sazrevanja procesa zaštite - SSE CMM, razvijen na bazi široko prihvaćenog generičkog modela sazrevanja procesa - CMM, kao dobra osnova za definisanje i poboljšavanje procesa i kapaciteta za generisanje, razvoj, implementaciju, izvršavanje i sazrevanje **11** sistem-inženjerskih (SE), **5** upravljačkih (projektnih) i **6** organizacionih procesa zaštite, sa osnovnim strateškim ciljem da se unapredi inženjering zaštite u dobro definisanu i zrelu-stabilnu, ponovljivu, kontrolisanu i merljivu disciplinu, detaljno je opisan u **potpoglavlju 2.4.** U **potpoglavlju 2.5** ukratko je definisana formalna evaluacija proizvoda i sistema zaštite (Common Criteria-standard ISO/IEC 15408), sa pregledom nekih metoda evaluacije na bazi CMM modela sazrevanja procesa, u odnosu na kriterijume troškova, tačnosti i stepena destrukcije evaluirane organizacije. Detaljno je opisan metod SSAM (Security Assessment Maturity Model) evaluacije procesa zaštite, na bazi SSE CMM modela. Integracioni model sazrevanja procesa CMMI v.1.2 (2006), koji integriše procese za razvoj, akviziciju i davanje servisa i pripadajući SCAMPI metod evaluacije, razmatrani su u **potpoglavlju 2.6.** Komparativna analiza SSE CMM i CMMI modela i SSAM i SCAMPI metoda evaluacije, sa težištem na komplementarnosti ovih modela i metoda evaluacije, kao i na mogućnost primene CMMI modela na procese zaštite, izvršena je u **potpoglavlju 2.7.** Brojne primene SSE CMM modela sazrevanja procesa i SSAM metoda evaluacije u sistem-inženjerskom i procesnom pristupu IKT zaštiti, detaljno su opisane u **potpoglavlju 2.8.** U **potpoglavlju 2.9** dat je pregled dostupnih informacija razmatranih u teoretskom delu rada.

U **POGLAVLJU 3.** uspostavljene su opšta i osnovne hipoteze i definisani sledeći ciljevi istraživanja: *pregled i komparativna analiza standarda kvaliteta procesa, konstruisana i terminološki prilagođena radna dokumenata SSAM metoda i SSE CMM modela, definisan željeni profil procesa evaluirane organizacije-E-Smart Systems (ESS) po zahtevu Sponzora, izmeren tekući profil procesa ESS, analizirani rezultati evaluacije (profil procesa i glavni nalazi) tekućih procesa ESS u odnosu na željeni profil procesa ESS i izrađeni zadaci za dugoročne, kratkoročne i projektne akcione planove za optimalno poboljšavanje tekućih procesa ESS.*

U **POGLAVLJU 4.** detaljno je opisan istraživački deo rada kroz 7 **potpoglavlja**: (1) **Predmet istraživanja**: verifikacija primenljivosti SSE CMM modela i SSAM metoda za evaluaciju i profilisanje tekućih procesa i poboljšavanje kapaciteta za generisanje procesa evaluirane organizacije - ESS; (2) **Metodi istraživanja**: SSE CMM metodologija evaluacije i SSAM metod za primenu te metodologije i inženjerske tehnike *deskriptivnih, eksplorativnih i kauzalnih* istraživanja; (3) **Tok izvršavanja projekta SSAM evaluacije tekućih procesa ESS**: definisan prema toku standardnog procesa SSAM metoda evaluacije i sa radnim dokumentima razvijenim i opisanim u *prilozima* na CD-u koji je sastavni deo rada; (4) **Instrumenti istraživanja**: standardni instrumenti SSAM metoda sa težištem na *atitudinalna i koraborativna merenja*, a kroz radna dokumenata razvijena za potrebe istraživačkog rada: *istraživački upitnik, plan intervjuja, dokumenta za zahtevanje, praćenje, korišćenje, čuvanje i vraćanje dokaza, Excel tabele za*

evidenciju dokaza i za generisanje izveštaja o profilu zrelosti procesa (histogram, tabela, pita dijagram), skale merenja (% račun, kvantitativni brojevi, težinski faktori) i plan evaluacije i istraživačkih merenja; **(5) Uzorkovanje dokaza i izveštavanje o sekundarnim nalazima:** specifično su razvijeni SSAM indikatori implementacije objektivnih dokaza (SSAM PIID), na bazi primera proizvoda rada navedenih u modelu kroz opis bazičnih praksi (BP). Identifikovani su ključni rezultati evaluacije i sekundarni nalazi snage i slabosti organizacije, koji se saopštavaju Sponzoru evaluacije i evaluiranoj organizaciji prema zahtevu Sponzora i **(6) Opis projekta SSAM Evaluacije tekućih procesa ESS:** opisani su osnovni atributi evaluirane organizacije, evaluiranih projekata i procesa evaluacije.

U **POGLAVLJU 5.** detaljno su analizirani rezultati evaluacije tekućih procesa ESS na bazi generisanog profila nivoa zrelosti procesa ESS i glavnih nalaza snage i slabosti organizacije (**potpoglavlje 5.1**). Predlozi *zadataka* dugoročnog, kratkoročnog i projektnog akcionog plana poboljšavanja tekućih procesa ESS, na bazi rezultata SSAM evaluacije, dati su u **potpoglavlju 5.2**, uključujući predlog za primenu **IDEAL** procesa implementacije plana poboljšavanja (**Prilozi 5.2A-5.2.D** na priloženom CD-u) i analizu stečenih iskustava iz primene SSAM metoda evaluacije za praktičnu i teoretsku korekciju novih procesa evaluacije.

U **POGLAVLJU 6.** diskutovani su dobijeni rezultati evaluacije tekućih procesa ESS, a u **POGLAVLJIMA 7., 8. i 9.** dati su **zaključci, ključni termini i literatura.**

2. Standardi i modeli kvaliteta procesa zaštite

2.1. Metodologija sistemskog inženjerstva i procesi zaštite

2.1.1. 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 (kauzalno) povezani pa se njihova svojstva razlikuju od svojstava skupa. Među brojnim definicijama sistema u tehničkoj terminologiji prihvatljiva je sledeća: *sistem je 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*“. Sistem je i „kompleksna matrica sastavnih objekata u interakciji“, koja ima definisane sledeće strukture: **cilja (misije), organizacionu, funkcionalnu, informacionu, komunikacionu i upravljačku**, [7], [8].

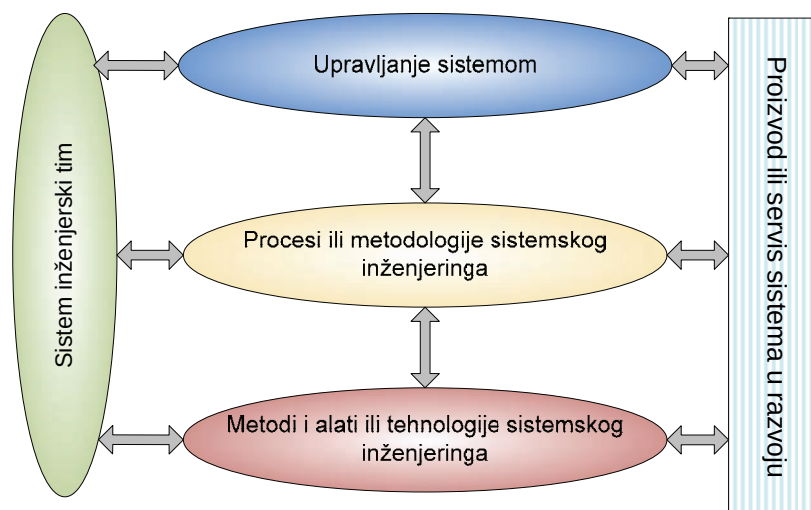
U formi sistema mogu se struktuirati sve situacije, ili kombinacije kompleksnih uticaja brojnih faktora, ili stanja funkcionisanja koja uključuju materijalne, energetske, informacione, vrednosne ili kombinovane tokove. Za proučavanje sistema razvijena je metodologija – **opšta teorija sistema**, gde *teorija* znači konceptualni alat, ili metod u sistemu naučnog znanja. Opšta teorija sistema dovela je do stvaranja **sistemskog inženjerstva**, ili tzv. **sistemskog pristupa**, kojeg karakteriše posmatranje objekata i pojava u dinamičkom odnosu prema sebi i okruženju.

Sistemi kao objekti proučavanja razlikuju se od drugih istraživačkih objekata po kompleksnosti fenomena u različitim disciplinama, uključujući i multidisciplinarnu oblast zaštite informacija, odnosno, IKT sistema. Kompleksnost je, dakle, karakteristika svakog organizovanog skupa pa i sistema zaštite, a podrazumeva da se taj skup sastoji od mnogo **objekata** i njihovih međusobnih veza koje utiču na intersistemsku i ekstrasistemsku dimenziju okruženja. 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.

2.1.2. Sistemski pristup

Sistem, kao meta objekat za istraživanje kompleksnih fenomena, koristi se u teoriji sistema, a **sistemsko inženjerstvo (SE)**, ili **sistemski pristup**, relevantan u tehničkim i brojnim drugim disciplinama, logički je pristup u modelovanju situacija i obezbeđuje efikasnost i efektivnost primene IKT u poslovnim sistemima. Istovremeno, sistemski pristup je struktuirani metod razvoja modela i konceptualnog okvira za analizu i istraživanje date situacije.

Sistemsko inženjerstvo može se definisati kao *tehnologija upravljanja*, koja kontroliše ceo evolutivni proces životnog ciklusa sistema, a rezultira sa *definisanjem, razvojem i implementacijom* visoko kvalitetnog, rentabilnog i na vreme završenog (po planu) sistema, tako da zadovoljava sve potrebe korisnika. SE pokriva razvoj celog sistema, koji može, a ne mora uključivati softver. Pošto se razmatra u okviru inženjeringa sistema, SE uključuje: *upravljanje sistemom, procese sistema i SE metode, alate i tehnologije*. Ova tri nivoa SE ilustrovana su na slici 2.1.1. SE se može posmatrati i kao *tehnologija menadžmenta (TM)*. Dekompozicijom TM na sastavne komponente može se doći do jasne predstave i razumevanja SE.



Sl. 2.1.1.1. Tri nivoa sistemskog inženjerstva

Osnovu SE čine sistemsko mišljenje i sistemsko analiza.

Sistemska mišljenje, kao eksplicitan naučni alat za istraživanje kompleksnosti fenomena i upravljanja problemima realnog sveta, dopunjuje analitičko mišljenje i glavni je faktor strategije dekomponovanja kompleksnih fenomena sistema. Istovremeno je i metod za razmatranje i rešavanje brojnih realnih problema i različitih tipova kompleksnosti. Sistemsko mišljenje fokusira pažnju na *proces*, što zahteva modelovanje, evaluaciju i metod poboljšavanja, kao i na *dinamičke strukture*, što podrazumeva da planirane sisteme treba dizajnirati (projektovati), a ne samo predviđati. Struktura razvoja sistemskog mišljenja, implementirana u modelu sazrevanja procesa, data je u **Prilogu 2.1A**.

Sistemska analiza predstavlja sveobuhvatan pristup problemima i njihovom rešavanju. Metodologijom sistemske analize utvrđuju se performanse sistema, ograničenja, zahtevi za resursima i interakcije sa okruženjem. Osnovne faze sistemske analize su, [8]: *definisane problema, prepoznavanje, definisanje i kvantizacija ciljeva sistema, definisanje i prepoznavanje granica sistema, analiza potreba korisnika, merenje efektivnosti sistema, analiza funkcionisanja sistema, određivanje ograničenja sistema, određivanje alternativnih rešenja i određivanje realnih alternativa (rešenja)*.

Iako precizna definicija **sistemskog inženjerstva u oblasti IKT zaštite - SSE** (System Security Engineering) još uvek ne postoji, jedna od mogućih definicija je: SSE je oblast SE koja primenjuje naučne i inženjerske principe za identifikaciju bezbednosne ranjivosti IKT sistema i smanjenje, ili ublažavanje faktora rizika koji prate te ranjivosti. Ipak, namena i ciljevi SSE dobro su poznati: razumeti bezbednosni rizik, uspostaviti bezbednosne potrebe (zahteve), razviti uputstva i instrukcije za zaštitu, odrediti prihvatljivi nivo rizika i uspostaviti garantovanu bezbednost. SSE prakse (aktivnosti) i procese mogu koristiti i primenjivati brojni entiteti u zaštiti: razvojni inženjeri, proizvođači i snabdevači komponenti zaštite, integratori sistema zaštite i IKT sistema, kupci proizvoda zaštite, organizacije za evaluaciju sistema zaštite, administratori sistema, konsultantske organizacije i organizacije za davanje servisa zaštite – poverljivi provajderi zaštite (TTPS-*Trusted Third Party Service*), [15]. SSE prakse se mogu primenjivati u svim fazama životnog ciklusa proizvoda/sistema zaštite: pre izrade koncepta zaštite, u fazi ispitivanja i definisanja koncepta zaštite, u fazi demonstracije i validacije nivoa zaštite, inženjerskom razvoju i projektovanju, proizvodnji i implementaciji proizvoda/ sistema zaštite, operativnom radu i podršci i u fazi odlaganja sistema zaštite. SSE procesi i prakse obuhvataju brojne komponente sistema zaštite: zaštitu raspoloživosti servisa i aplikacija IKT sistema, zaštitu informacija, mrežnu zaštitu, fizičku zaštitu, personalnu zaštitu, administrativnu zaštitu, zaštitu od KEMZ-a (kompromitujućeg elektro magnetskog zračenja, ili parazitnog zračenja) i zaštitu računarskog sistema.

2.1.3. Modelovanje sistema zaštite

U sistemskoj analizi eksperimentiše se i radi sa **modelima** realnog sistema, koji mogu imati četiri generička tipa: *fizički*, *narativni* (tekstualni, govorni), *grafički* (simbolički) i *matematički* (formalni) model. **Fizički modeli** (n.p.r. automobila) koriste se najčešće u proizvodnji i građevinarstvu; **narativni** (rečima i tekstom) najviše se koriste u svim naučnim disciplinama, a obuhvataju i tzv. *funkcionalne* i *konceptualne logičke* modele; **grafički** se najviše koriste u modelovanju tehničkih sistema, a **matematički** modeli koji su najprecizniji, od jednostavnih do izuzetno kompleksnih, koriste se za modelovanje i simulaciju kritičnih i skupih procesa. 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*“, [24].

U modelovanju IKT i sistema zaštite koriste se narativni, grafički i matematički modeli. U kategoriji narativnih modela najviše su zastupljeni *funkcionalni modeli* (n.p.r. sistema zaštite, procesa upravljanja rizikom i.t.d.), [85]. Grafički modeli u modelovanju tehničkih sistema su brojni (n.p.r. procesa strateškog planiranja zaštite, strateške politike zaštite, procene rizika i.t.d.), [85], [80]. Primena matematičkih modela za kompleksne sisteme zaštite i IKT sisteme neracionalna je, teško izvodljiva, nekoherentna i ne daje najbolje praktične rezultate, [85]. Za potrebe sistem - inženjerske analize IKT i sistema zaštite, bolje rezultate daju *strukturni i objektno orijentisani modeli*, [24].

2.1.3.1. Strukturno modelovanje sistema zaštite

Strukturni model posmatra sistem zaštite (i IKT 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), [24]. U ovoj interpretaciji sistem se posmatra kao koherentna celina tri ključna elementa: ulaznih veličina ili parametara, procesa i izlaznih parametara, čije se interakcije odvijaju u realnom kontekstu (okruženju) koji nameće ograničenja sistema.

Strukturni model zaštićenog (bezbednog) IKT sistema sadrži tri glavne komponente: **skup objekata**, pasivnih i aktivnih komponenti sistema koje se koriste i kojima se pristupa na kontrolisan način; **skup subjekata**, aktivnih komponenti sistema koje koriste i pristupaju objektima i **skup pravila**, na osnovu kojih subjekti koriste i pristupaju objektima, [24]. Strukturni modeli IKT sistema vrše dekompoziciju, odnosno, klasifikaciju i kategorizaciju objekata sistema na skupove objekata, prema definisanim kriterijumima: jedinstvenim bezbednosnim ciljevima, jedinstvenim funkcijama i.t.d., a odbacuju nebitne komponente i tako smanjuju kompleksnost sistema, [85], [24].

Sa aspekta zahteva za *smanjenje kompleksnosti visoko distriburanih sistema OSI modela sa integrisanim sistemom zaštite, iz skupa svih mogućih komponenti IKT sistema, 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, upravljački centar za obradu informacija, udaljeni legalni korisnici sistema, nelegalni korisnici sistema (potencijalni maliciozni napadači), nosioci informacija (magnetski, optički i dr.), izdvojene radne stanice (terminali), tehnika za izradu rezervnih kopija (bekapovanje) i legalni korisnici (ljudi)*, [24].

Primeri strukturnog modelovanja u praksi zaštite su modelovanje: *mehanizma logičke kontrole pristupa i mrežne IKT arhitekture*, [68]. Na primer, strukturno modelovanje mrežne arhitekture obezbeđuje smanjenje kompleksnosti IKT sistema i projektovanog sistema zaštite u četiri koraka:

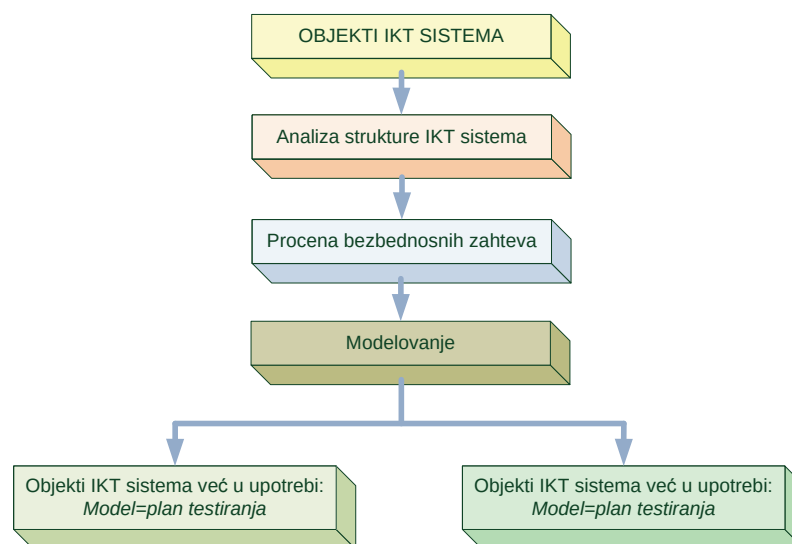
- 1. korak:** analiza mrežnog plana i uklanjanje svake informacije koja nije neophodna za izradu koncepta *sistema osnovne zaštite (security baseline)*;
- 2. korak:** ažuriranje mrežnog plana ili delova plana (ako je podeljen u sekcije) sa stvarnim stanjem topologije mreže;
- 3. korak:** definisanje *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 IKT i sistemima zaštite, nastaju iz najmanje dva razloga, [24]:

1. podele na aktivne (*subjekte*) i pasivne (*objekte*) i
2. 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, [68], prikazan je na Slici 2.1.2.



Sl. 2.1.2. Izlaz strukturnog modelovanja sistema osnovne IKT zaštite

Drugi stereotip u *tradicionalnom pristupu IKT zaštiti* je tretiranje (pod)sistema zaštite operativnog sistema (OS) - **NOSSS** (*Native Operative System Security Subsystem*) kao dominantne komponente zaštite, na koju se izdvajaju znatna sredstva na račun ostalih komponenti sistema realne zaštite. Naime, u savremenim, visoko-distribuiranim IKT sistemima OSI modela višeslojne arhitekture klijent-server tipa, OS ne kontroliše sve *objekte* sa kojima korisnici rade, kao ni aktivnosti samih korisnika koji svoj pristup OS-u registruju i evidentiraju odgovarajućim mehanizmima kontrole pristupa. Na taj način, osnovna bezbednosna funkcija **NOSSS** svodi se na zaštitu prava privilegovanih korisnika (administratora, supervizora i dr.) od napada regularnih korisnika (interno zaposlenih), što je značajno, ali se bezbednost IKT sistema tim merama ne iscrpljuje, [24], [85].

Sledeći pristup je formiranje hardversko-softverskih mehanizama zaštite u vidu sveobuhvatnih servisa zaštite, koji pretpostavljaju ekonomski opravdane zaštitne mere, sinhronizovane sa bezbednosnim potrebama, životnim ciklusom sistema i realnim resursima organizacije, umesto korišćenja samo skupih tehničkih kontrola zaštite. Ove mere treba da uključe različite tehničke i netehničke mere zaštite, jer stepen zaštite informacija od neovlašćenog pristupa i ilegalnih aktivnosti, pored tehničkih kontrola zaštite, zavisi od brojnih upravljačkih i operativno-organizacionih mera, usmerenih na sprečavanje pristupa sistemu i objektima IKT sistema, [24].

Jedan od značajnih problema zaštite informacija u savremenim visoko distribuiranim sistemima je povećanje efikasnosti i kvaliteta upravljanja zaštitom, [24], [64], [97].

Strukturni model, takođe, ne podržava algoritamsku dekompoziciju sistema, kojom se sistem deli na funkcionalne objekte sistema i prikazuje *funkcionalnim modelom*, pošto nije primenljiv u ranoj fazi analize i modelovanja predmetne oblasti, dok algoritam i funkcije dekompozicije još nisu poznati, [24]. 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**, [24], [113], [68].

2.1.3.2. *Objektno orijentisani pristup modelovanju sistema zaštite*

Problem zaštite informacija veoma je složen, jer su složeni i IKT sistem i sistem zaštite. U oblasti zaštite informacija slabo se koriste znanja i iskustva iz *objektno-orijentisanog pristupa* modelovanju IKT sistema, na kojem se zasniva projektovanje savremenih IKT sistema i predstavlja isproban metod za smanjivanje kompleksnosti IKT sistema uključujući i (pod)sistem zaštite. Kao i svaki racionalan metod za smanjivanje kompleksnosti, objektno orijentisani pristup primenjuje princip dekompozicije strukture IKT 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 *disjunktih* (nezavisnih) objekata sa minimalnim brojem međusobnih veza. U narednim fazama dekompozicija se može vršiti i na nižim nivoima apstrakcije. U objektno-orijentisanom pristupu 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 (*enkapsulirani*), a povezivanje objekata dostupno je samo interfejsu, [68].

Za razumevanje pojma **objekta** IKT sistema (ili sistema zaštite) zahteva se razumevanje *klasifikacije i kategorizacije (ili bezbednosne klasifikacije i kategorizacije)* objekata IKT sistema (ili sistema zaštite) i uvođenje pojma **klase objekata**. Generička, **klasifikacija** bilo kojih objekata mora da ima sledeće attribute [40]:

Međusobnu isključivost – sprečava preklapanja, ili klasifikacija objekata u jednu kategoriju isključuje sve ostale kategorije koje su međusobno disjunktne;

3. **Potpunost** – unija svih kategorija obuhvata sve moguće klasifikacije;
4. **Nedvosmislenost** – svaka klasifikacija mora biti jasna i precizna;
5. **Ponovljivost** – svaki proces klasifikacije mora biti ponovljiv i da daje isti rezultat;
6. **Prihvatljivost** – svaka klasifikacija mora biti logična i intuitivna;
7. **Primenljivost** – klasifikacija mora biti primenljiva u različitim sferama istraživanja.

Klasa je apstrakcija skupa stvarnih karakteristika realnog sveta, objedinjenih jednakom *opštom strukturom i ponašanjem*. **Objekat** je elemenat klase, tj. apstrakcija određene stvarnosti. Objekti su aktivni elementi koji imaju unutrašnju strukturu i način ponašanja koji se opisuje tzv. **metodom objekta**. Na 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 moguće posebnim načinom ponašanja.

U sistemu zaštite **bezbednosna klasifikacija** odnosi se na bezbednosne nivoe klase informacionih objekata - *informacija* (n.p.r., *interne, poverljive SP, DT*). Pod **kategorizacijom** podrazumeva se klasifikacija svih objekata IKT sistema u kategorije na koje se mogu primeniti generički atributi klasifikacije, [9]. U kontekstu sistema zaštite, pod **bezbednosnom kategorizacijom** podrazumeva se klasifikacija objekata IKT sistema u kategorije sa jednakim bezbednosnim zahtevima i ciljevima, na koje se mogu primeniti svi navedeni atributi klasifikacije. Prihvatljiv model bezbednosne kategorizacije–**Bk** može se izraziti relacijom, [9], [68]:

$$Bk = (UtP)(UtI)(UtR) = Utmax$$

gde je:

UtP – uticaj pretnji (**V**-visok, **S**-srednji, **N**-nizak) na **poverljivost** informacija,

UtI – uticaj pretnji (**V**-visok, **S**-srednji, **N**-nizak) na **integritet** informacija i

UtR – uticaj pretnji (**V**-visok, **S**-srednji, **N**-nizak) na **raspoloživost** informacija.

Bezbednosnu kategoriju objekta IKT sistema, ili **objekta zaštite** određuje **maksimalni** uticaj pretnji, čime se uzima u obzir najgori slučaj, obezbeđuje najviši stepen zaštite i kompenzuje nizak stepen gradacije uticaja pretnji (**V,S,N**).

Sledeća grupa važnih pojmova objektnog pristupa, koje poseduju komponente klase objekata IKT sistema i sistema zaštite, su *enkapsulacija, nasleđivanje i polimorfizam*, [24], [68]:

- **enkapsulacija** komponenti objekta, osnovni instrument smanjenja kompleksnosti sistema, podrazumeva skraćivanje unutrašnje strukture objekta, detalja realizacije i načina

ponašanja (metoda); smanjuje složenost realizacije, održavajući vidljivim samo značajne interfejsne na datom nivou aproksimacije;

- **nasleđivanje** označava formiranje nove klase objekata na osnovu postojeće sa mogućnošću dodavanja, ili ponovnog određivanja podataka i načina ponašanja; dopušta razvoj komponenti u ranoj fazi razvoja sistema, ne narušavajući integritet složenog objekta (sistema zaštite); važan faktor smanjenja multiplikativnih elemenata realnog sistema, gde se opšta informacija ne duplira, nego se samo ukazuje na postojeće promene; na taj način klasa-potomak postaje koren nove klase-naslednika i
- **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.

Važno je uočiti da nasleđivanje i polimorfizam zajedno daju objektno orijentisanom sistemu sposobnost modularne skalabilnosti (nadogradnje), što je poželjan zahtev za sisteme zaštite. Komponente i sistem zaštite su upravo klasa objekata koji se konstantno modifikuju, zbog promena okruženja (IKT sistema, pretnji i.t.d) i zahtevaju modularnu dograđuju, zbog relativno skupih tehnologija zaštite i čestih izmena.

Grane objekta i nivo dekompozicije (detaljizacije) još su dve bitne karakteristike objekata. Realni objekti po pravilu poseduju nekoliko relativno nezavisnih karakteristika. U modelu objekta takve se karakteristike nazivaju *grane objekta*. Na primer, u sistemu zaštite definisane su tri osnovne grane objekata zaštite: **raspoloživost, integritet i poverljivost informacija**. Tako pojam grane objekta omogućava bolje od polimorfizma, raznolikost aspekata posmatranja i apstrakcije objekata.

Pojam *nivoa dekompozicije* važan je ne samo za vizuelizaciju objekata, nego i za sistematsku analizu složenih objekata, predstavljen 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 $(n-1)$. Objekat sa nivoom detalja 0 smatra se da je atomizovan (nedeljiv). Nivoi detaljizacija variraju kako za objekte tako i za grane objekta, [24].

Veoma rasprostranjena konkretizacija objektno orijentisanog pristupa su *komponente objekta i kontejner*. **Komponenta objekta** može se 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 i objekti IKT sistema koji se štite. Posebno, pojam kontejnera može odrediti granice zone zaštite, ili perimetar zaštite, ili domen zaštite. Komponente objekta raspolažu sa svim karakteristikama objektno orijentisanog pristupa: *enkapsulacija komponenti objekta; nasleđivanje i polimorfizam*, [24].

U objektno orijentisanom modelu za strukturiranje bezbednosnog cilja – razvoja integrisanog sistema zaštite informacija i smanjenje kompleksnosti sistema zaštite, uvode se dva skupa grana objekata, [24], [68]:

skup grana informacionih objekata (objekata zaštite), koga čine raspoloživost, integritet i poverljivost informacija, kao najznačajnijeg objekta IKT i poslovnog sistema. Od svih atributa informacije, ove možemo smatrati relativno nezavisnim i ako su sva tri zaštićena, smatra se da je zaštićen i IKT sistem i

skup grana objekata sistema zaštite (objekata za zaštitu) koga čine upravljačke, organizaciono-operativne i tehničke kontrole sistema zaštite.

U modelovanju i projektovanju sistema zaštite, obe grane objekata razmatraju se sa različitim nivoima detalja. 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 predmetnoj 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 ne menja se, 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 koji se potčinjavaju tim merama zaštite.

Na sve relativno nezavisne grane deluje i princip enkapsulacije, 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). Ortogonalnih skupova nema mnogo: dva skupa sa brojem elemenata od 3-4 daje 12 kombinacija ortogonalnih skupova, što je još uvek prihvatljiv nivo kompleksnosti, [68].

2.1.4. Procesni pristup sistemu zaštite

Kako je u sistemskom pristupu *kvalitet komunikacije i veza sa ostalim sistemima*, važan element svakog sistema, sistem zaštite može se definisati i kao skup *procesa* - p_i koji međusobno komuniciraju, što se u matematičkoj interpretaciji može izraziti relacijom, [12]:

$$P = \{p_1, p_2, \dots, p^n\}$$

Gde se svaki p_i predstavlja skupom: D_i – bezbednosnih događaja, U_i – uslova okruženja (pretnji, bezbednosnih zahteva) i F_{si} – bezbednosnih funkcija koje su rezultat odvijanja procesa zaštite, a koje opisuju međuzavisnost *uslova* (u_i) i *događaja* (d_i) kroz skup *slučajeva* (S). Skup *uslova* (U) i skup *događaja* (D) definišu se formalnim modelom sistema. *Slučaj* (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:

$$(U, S, D, r)$$

gde je:

$U = (u_1, u_2, \dots, u_n)$ – skup uslova,

$P(U) = K$ – skup mogućih kombinacija uslova,

$S = (s_1, s_2, \dots, s_k) \subseteq K$ – skup slučajeva,

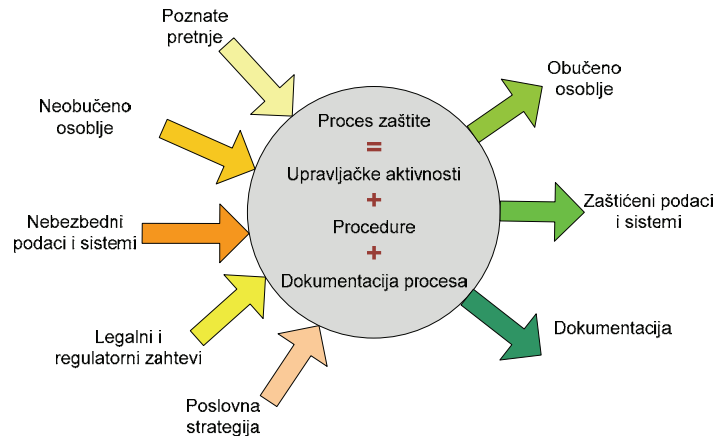
$D = (d_1, d_2, \dots, d_m)$ – skup bezbednosnih događaja,

$r = S'D'S$ – 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*: $K \rightarrow D$.

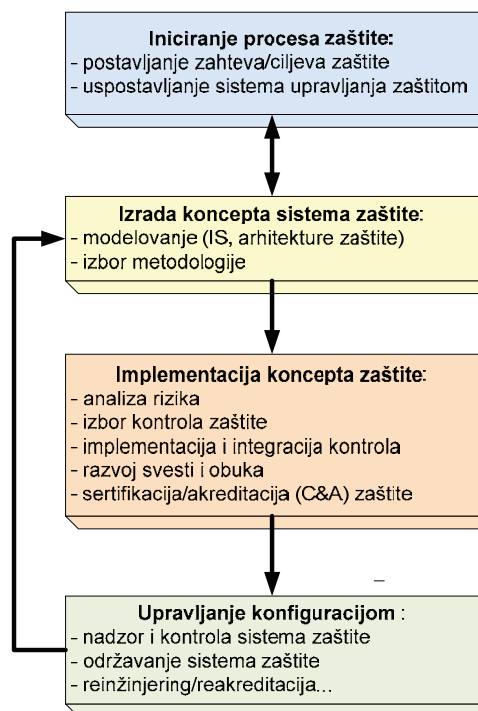
Prvi korak u sistemskom pristupu zaštiti uključuje funkcionalno razlaganje na osnovne elemente sistema: *ulazne veličine*, **procese**, *izlazne veličine* i *okruženje*. Očekuje se da *procesi* koji transformišu ulazne veličine u izlazne povećavaju vrednosti izlaznih veličina i aktivnosti u odnosu na 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**, da se kontrolišu i kvantitativno upravljaju sa krajnjim ciljem predviđanja izlaznih performansi procesa zaštite i uticaja na poslove i misiju organizacije. Efektivno upravljanje procesom zahteva 4 ključne uloge: *sponzora*, *vlasnika*, *menadžera* i *izvršioca* procesa, [26]. **Sponzor**, iskusan menadžer, obezbeđuje smernice i resurse za poboljšavanje procesa. **Vlasnik** obično je izvan procesa, ali je direktno, ili lično odgovoran za ceo proces i treba da pokreće inicijativu za poboljšavanje procesa. **Menadžer** procesa radi unutar procesa i odgovoran je za: diskretne delove procesa, dnevne proizvodne performanse, direktno upravljanje zaposlenim u procesu, odnose sa snabdevačima i obezbeđenje metrike procesa, izveštaja o performansama i ideja za poboljšavanje za vlasnika procesa. **Izvršilac** procesa radi unutar procesa, odgovoran je za specifične isporuke rezultata procesa u skladu sa standardima i obezbeđuje za menadžera procesa metriku procesa, izveštaje o performansama i ideje za poboljšavanje.

Model sistema zaštite u sistemskom pristupu posmatra zaštitu kao **proces** koji transformiše neke ulazne veličine u neke izlazne veličine (Sl.2.1.3). Sistem zaštite se u ovoj interpretaciji posmatra kao *koherentna celina* tri ključna elementa: *ulaznih veličina (parametara)*, *proces* i *izlaznih veličina*, čije se interakcije odvijaju u realnom kontekstu (okruženju) koji nameće ograničenja sistema, [68], [85].



Sl. 2.1.3. Proces zaštite kao transformator ulaznih parametara u izlazne

Ulazne veličine u proces zaštite mogu biti akcije, metode i operacije, odnosno, poznate pretnje, neosposobljeno osoblje, nezaštićeni podaci i IKT sistemi, zakonski i drugi zahtevi, poslovna strategija i dr. **Procesi** su fundamentalni gradivni blokovi sistema zaštite, koji transformišu ulazne veličine u izlazne, objedinjuju upravljačke aktivnosti, sekvencijalno izvršavane aktivnosti, ili praksi zaštite – procedure zaštite i dokumentaciju procesa. Procesi zaštite dodaju novu vrednost i povećavaju kvalitet sistema zaštite. Sve što učinimo 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 (sistem) bilo koje veličine može posmatrati kao *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, politika i dokumentacija zaštite. Generički proces sistema zaštite prikazan je na Sl.2.1.4, [16], [68].

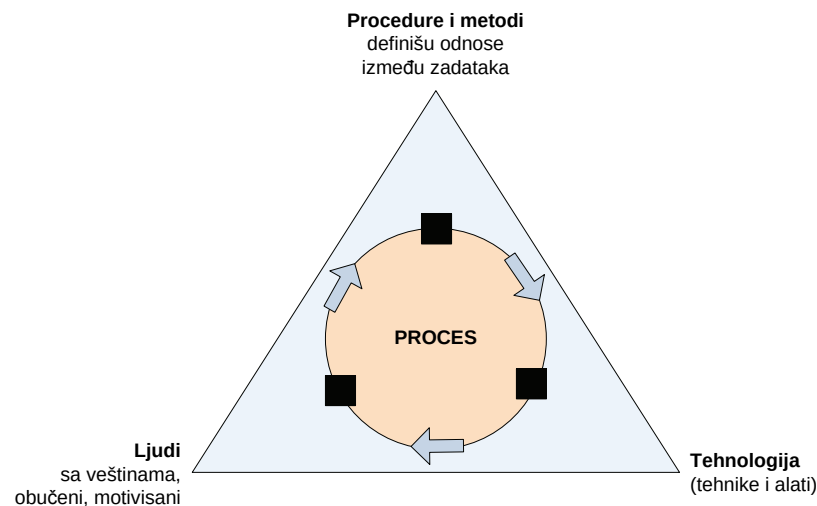


Sl. 2.1.4. Generički proces sistema zaštite

Okruženje sistema zaštite predstavlja **kontekst**, koji određuje namenu IKT sistema sa integrisanim sistemom zaštite u organizaciji – za **opštu podršku**, ili **glavnu aplikaciju**, u odnosu na ograničenja koja nameću poslovi organizacije, struktura IKT sistema, politike i procedure zaštite IKT sistema. Sistem zaštite dobija ulazne podatke iz okruženja u vidu dinamički promenljivih pretnji, bezbednosnih zahteva, kompjuterskog incidenta, vanrednog događaja, a zatim obezbeđuje izlaze i odgovore prema okruženju.

Povećavanje nivoa efikasnosti i efektivnosti procesa u datoj situaciji, ili skupu operacija uobičajena je namena sistemskog pristupa IKT zaštiti. Osnovni alat sistemskog pristupa je **sistemska analiza**, kao *opšta metodologija analize sistema*, ili primena opšte metodologije sistemske analize za izradu matematičkih modela i **evaluaciju** kvaliteta funkcionisanja sistema. U kontekstu sistemskog pristupa i sistemske analize sistema IKT zaštite, dominira inherentni zahtev za **neprekidnim poboljšanjem procesa zaštite**, [8], [68], [67], [27], [87].

Ako se procesi zaštite definišu kao **integrator tri ključna atributa posla: procedura i metoda, tehnika i alata i osposobljenih ljudi** (Sl.2.1.5), onda se neprekidnim poboljšavanjem procesa i *optimalnim troškovima resursa*, [79], može postići najveća produktivnost - efektivnost i efikasnost rada u organizaciji, [20].



Sl. 2.1.5. Proces kao integrator ljudi, metoda i tehnologije

Kako je **kvalitet procesa zaštite** jedna od ključnih determinanti troškova sistema zaštite, vremena isporuke i kvaliteta servisa i mehanizama zaštite i najviše doprinosi produktivnosti organizacije, treba očekivati da organizacije radije usmeravaju pažnju na **poboljšavanje procesa zaštite**, nego na nabavku skupe tehnologije zaštite i angažovanja teško dostupnih i skupih specijalista zaštite. Prvi korak u poboljšavanju procesa zaštite je **evaluacija**, ili procena na bazi određenih kriterijuma. Da bi se procesi zaštite evaluirali i poboljšavali, pretpostavka je da se moraju formalno, ili neformalno izvršavati. Formalno se izvršavaju planirani, dokumentovani, dobro definisani i opisani *standardni procesi*, a neformalno - procesi koji nisu tako dobro definisani i formalno opisani i koji se izvršavaju neregularno.

2.1.5. Modeli procesa najbolje prakse zaštite

Procese najbolje prakse IKT zaštite tretira nekoliko relevantnih međunarodni standarda sa neznatno različitim pristupima: **COBIT** (Control Objectives for Information and Related Technologies), **SSE-CMM** (System Security Engineering - Capability Maturity Model), **OCTAVE** (Operationally Critical Threat, Assets and Vulnerability Evaluation), **BSI - Nemačka** (IT Baseline Protection Model), **ISO/IEC 17799**, **ISO/IEC 15408 ili CC** (Common Criteria for Information Technology Security Evaluation), **ISF** (Best practice v.40).

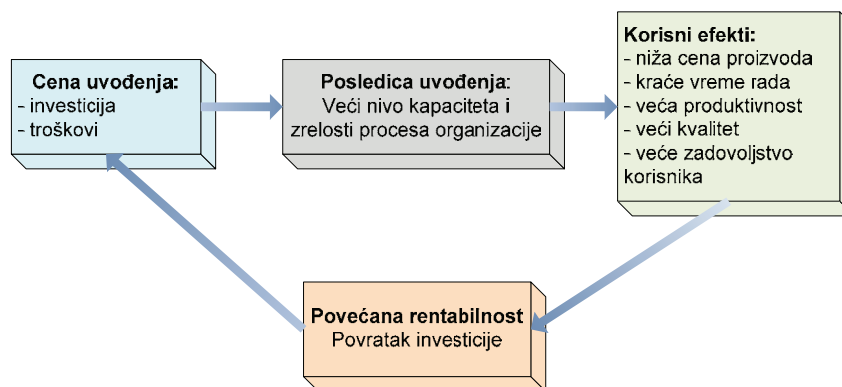
Takođe, postoji više definicija **najbolje i dobre prakse IKT zaštite**, [14], [18], [20], [93], [47], [48], [108], koje sa manjim varijacijama sadrže iste ključne komponente. Prema [108], *proces najbolje prakse IKT zaštite* treba da obuhvata sledeće ključne atribute:

- dokumentovan;
- dostupan;
- usklađen sa opšte prihvaćenim standardima – strateški i taktički, baziran na procesima i metodologiji, vremenski i praktično testiran i obezbeđuju zaštitu prema definisanim ciljevima;
- kontinualno poboljšavan – uključujući stalnu obuku, obrazovanje i sertifikaciju;
- ponovljiv;
- efikasan – rentabilan tj. dobit je veća od troškova;
- skalabilan – nekoliko vitalnih i mnogo trivijalnih rešenja;
- efektivan – vodi do željenog ishoda;
- adaptivan – obuhvata vanredne događaje;
- obezbeđuje indikator progresa i okvire;
- usklađen sa zakonom i regulativama – za legalne potrebe forenzičke analize digitalnih dokaza u slučaju zloupotrebe i kompjuterskog kriminala;
- obuhvata upravljačke, operativno-organizacione i tehničke kontrole zaštite – odnosno, humane, administrativne, tehničke i fizičke aspekte: ljude, procese, procedure, politike, planove, sisteme, mreže, tehnologije i fizičke objekte okruženja i
- obezbeđuje raspoloživost, integritet (uključujući autentičnost i neporecivost) i poverljivost informacija i objekata IKT sistema – u skladu sa objektno orijentisanim pristupom sistemu zaštite.

Model procesa je struktuiran skup praksi koje opisuju karakteristike efektivnih procesa. Efektivnosti praksi uključenih u model iskustveno su potvrđene. Model je dijagnostički alat statusa procesa i **nije proces**. Dakle, sam proces i realan opis procesa uvek se razlikuju od opisa u modelu procesa. Model procesa može se koristiti za, [20]:

- dijagnozu stanja tekućih praksi organizacije sa pripadajućim metodom evaluacije,
- uspostavljanje ciljeva i prioriteta za poboljšavanje procesa,
- uspostavljanje stabilnih i zrelih procesa kroz poboljšavanje projekata i procesa organizacije,
- određivanje početne tačke projekta za poboljšavanja procesa,
- agregaciju iskustava iz primene procesa u organizaciji,
- komunikaciju strateške vizije uobičajenim jezikom organizacije i
- definisanje značaja poboljšavanja procesa za organizaciju.

Primena svakog modela procesa ima svoju *cenu, prednosti i nedostatke* (Sl. 2.1.6). Troškovi primene nekog modela procesa variraju u zavisnosti od brojnih faktora organizacije: ciljeva, veličine, kulture rada, strukture i tipa procesa, [79]. Generalno organizacije sa sistematskom primenom modela procesa rentabilno zatvaraju ciklus i ostvaruju znatan povraćaj investicija, [63], [20].



Sl. 2.1.6. Troškovi, prednosti i nedostaci modela procesa

U familiji brojnih modela procesa su i **modeli sazrevanja procesa** razvijeni na bazi generičkog CMM modela: SwCMM, SE CMM, SSE CMM, CMMI i.t.d. Dakle, u skladu sa definicijom modela procesa, SSE CMM i CMMI nisu procesi; oni **opisuju** karakteristike efektivnih procesa i kao svi modeli samo su korisna aproksimacija realnih procesa, [20].

2.1.6. Definisanje standardnog procesa zaštite

Izrada formalne definicije standardnih i poboljšanih procesa organizacije ključni je korak u kreiranju **dokumentacije procesa**. Opis svakog procesa treba da sadrži, najmanje:

- uloge i odgovornosti ljudi određenih za izvršavanje rada u procesu,
- odgovarajuće alate i opremu koji pomažu ljudima da izvrše svoje radne zadatke i
- procedure i metode koje definišu **kako** se zadaci izvršavaju i međusobne odnose zadataka.

Proces nije jednostavan dijagram toka na najvišem nivou apstrakcije. Na primer životni ciklus sistema nije proces. Alat ili tehnologija takođe nisu procesi. Definicija procesa, dakle, treba da sadrži sekvencijalne korake o tome **šta** treba uraditi i **procedure** koje detaljno opisuju **kako to** treba uraditi.

Organizacija može samo za definisani proces sagledati gde da poboljšava kvalitet, produktivnost, troškove i vreme rada. **Definisan proces je preduslov za poboljšavanje procesa**. Neprekidno i održivo poboljšavanje procesa nije izvodljivo bez definisanja procesa na regularan način. Definisani procesi poboljšavaju komunikaciju i razumevanje **tekućih procesa** i **željenih procesa** kojima se teži. Definisani procesi pomažu kod planiranja i realizacije planova, obezbeđuju kapacitete za izučavanje iskustava i čine lakšom analizu i poboljšavanje standardnih procesa organizacije. Neki proces se smatra definisanim kada je: *dokumentovan (opisan), obuka o procesu izvršena, a proces se dnevno praktično izvršava*. Da bi se izradila dokumentacija procesa, autori moraju dobro razumeti tekući proces i imati viziju o željenom procesu. Kako početi izradu definicije procesa? Dobar metod je, izvršiti dekompoziciju proizvoda/servisa procesa organizacije, prema izlaznim **proizvodima rada procesa**. Ako je, na primer, proizvod rada/servisa procesa organizacije **uspostavljen i funkcionalno opeartivan PKI system**, treba dekomponovati PKI sistem u funkcionalne module: *CA, RA, Direktorijum* i.t.d. Zatim dekomponovati ove module u njihove sastavne komponente: *CA u osnovne module* i.t.d., sve do osnovnih komponenti koje još uvek imaju specifičan proizvod rada. Da bi se izvršio rad za razvoj svakog izlaznog *proizvoda rada*, treba dokumentovati procese za izvršavanje tog rada. Sada se za svaki izlazni proizvod rada do poslednjeg nivoa dekomponovanih modula CA (i drugih komponenti na istom nivou dekompozicije), identifikuju sve *osnovne aktivnosti* (bazične prakse-**BP**) koje treba izvršiti da se taj proizvod rada dobije. Pri tome treba obavezno obuhvatiti logističku podršku organizacije i sve organizacione jedinice, koje na bilo koji način učestvuju u procesu, što uključuje procenu **zadataka** koje treba izvršiti za kompletiranje procesa, **ulaza i izlaza, zavisnosti, uloga i odgovornosti**.

Opis procesa u modelu procesa može biti: *formalan* i *korisnički orijentisan*. **Formalni opis procesa** zahteva tipično uključivanje specijalista zaštite; opis je detaljan i formalizovan i primarno se koristi za razvoj, prilagođavanje i poboljšavanje procesa. Za formalan opis procesa treba poznavati opisne elemente dekompozicije procesa-aktivnosti, kao što su: *namena, izvršioci, ulazne veličine, proizvod rada, kriterijum za početak, kriterijum za uspešno kompletiranje, potreban rad za izvršavanje aktivnosti, sub-prakse* (3-6) koje je potrebno izvršiti za izvršavanje ove aktivnosti, *metrika* za izvršavanje aktivnosti i *prethodna i sledeća aktivnost*.

Korisnički orijentisan opis procesa zahteva uključivanje korisnika procesa (praktičara) koji dnevno koriste procese. Opis je tipično jasan, jednostavan i primarno se koristi za izvršavanje procesa, [28].

Formalni opis procesa sadrži brojne elemente, koje je potrebno dobro definisati da bi korisnik mogao razumeti, upravljati i poboljšavati proces, [97]. **Formalni opis dobro definisanog procesa**

treba da uključi odnosne *politike i standarde* i da sadrže sledeće elemente procesa: *naziv, namenu, obim, ulaze, ulazne kriterijume, aktivnosti, procedure, specifikovane uloge, merenja, validaciju, templejte, izlaze i izlazne kriterijume*, koji su dokumentovani, konzistentni i kompletni. **Naziv** treba biti jednostavan i da sadrži glagol i imenicu, n.p.r., *Dizajnirati novi proizvod*. **Namena** procesa treba da počinje sa „**je da ...**“, n.p.r., „**je da izbac**i novi proizvod na tržište, sa najnovijom tehnologijom i u planiranom roku“. **Obim** procesa definiše precizno gde proces počinje i završava i šta je specifično uključeno, a šta isključeno, n.p.r., „*Proces počinje sa izradom plana projekta, a završava kada korisnici prihvate proizvod; uključuje sve proizvodne faze, ali isključuje dizajn pakovanja*“. **Ulazi** u proces mogu biti opipljivi (n.p.r., pisani podaci), ili verbalni (n.p.r., usmeni zahtev). **Izlazi** procesa mogu biti proizvodi ili servisi, koji treba da odgovaraju prihvaćenim specifikacijama kupca; može biti opipljiv (proizvod), ili neopipljiv (savet). **Kontrole** procesa mogu biti interne – kontrola kvaliteta **validacijom**, ili **procedure** organizacije, ili eksterne – specifikacija zahteva korisnika, zakonska ograničenja, intelektualna svojina i dr. **Resursi** procesa su sve materijalne i nematerijalne stvari koje proces mora imati da bi transformisao ulazne veličine u izlazne, uključujući i ljudske resurse i pripisane **uloge** u procesu.

Većina templejta za opis definisanog procesa uključuju sledeće entitete (tzv. IBM, SEI **ETVX** - *Entry Criteria, Tasks, Verification, and eXit Criteria* format):

1. **Ulazni kriterijumi aktivnosti** (npr., da se izvrši prethodna aktivnost)
2. **Izlazni kriterijumi aktivnosti** (npr., dobijanje proizvoda rada aktivnosti)
3. **Ulaz aktivnosti** (npr., resursi, standard, zahtev)
4. **Izlaz aktivnosti** (npr., očekivani proizvod rada)
5. **Izvršioci aktivnosti** (agenti - *uloge*, član projektnog tima i sl.)
6. **Sledeća aktivnost** (npr., aktivnost čiji početak zavisi od izvršavanja prethodne aktivnosti, ili može početi samo kada se ova aktivnost završi).

Ponekada se **ulazni kriteijumi** i **ulazi**, kao i **izlazni kriterijumi** i **izlazi** kombinuju u jedno, iako u stvari oni nisu isti, jer su *ulazni i izlazni kriterijumi trigeri aktivnosti*, a *ulazi i izlazi su proizvodi rada odnosne aktivnosti*. Većina organizacija u praksi kombinuje ove koncepte u jedinstvene ulazne i izlazne parametre, što nije uvek dobro, jer se teže prate međuzavisnosti aktivnosti koje se odvijaju paralelno u procesu.

U opisu procesa neke organizacije **ETVX** informacije predstavljaju kao dijagram toka sa pratećim tekstom objašnjenja dešavanja u procesu; druge proces predstavljaju kao listu *sekvencijalnih koraka*, a neke proces opisuju tekstualno. Međutim, za opis procesa može se koristiti svaki format koji odgovara kulturi rada organizacije, pod uslovom da je obuhvaćeno najmanje svih 6 **ETVX** komponenti definisanja procesa. Posle opisa i dokumentovanja procesa, mogu se pisati **procedure** koje podržavaju proces, na bazi dokumentovanih koraka procesa. Procedure detaljno opisuju **kako** treba izvršiti korake u procesu. U **Prilogu 2.1B** opisani su ključni kriterijumi i uzorci za definisanje i formalni opis procesa.

2.2. Poboljšavanje procesa zaštite

2.2.1. Uvod

Kvalitet sistema zaštite veoma zavisi od kvaliteta procesa koji se koriste za projektovanje, razvoj i održavanje, [26]. Ova premisa odnosi se podjednako na procese i proizvode zaštite, prema dugogodišnjim iskustvima u proizvodnji, uverenju proizvođača i davaoca usluga širom sveta (tj. ISO standarda). *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*, [20].

Ljudi, procesi i tehnologija glavne su determinante troškova, vremena i kvaliteta proizvoda. Prema kriterijumima kvaliteta procesi mogu biti, [20], [27]:

1. **Improvizovani procesi:** korisnici u praksi (menadžeri i praktičari) čine procese improvizovanim i *ad hock*. Takvi procesi nisu striktno opisani, zahtevani i izvršavani. Izvršavanje procesa mnogo zavisi od sposobnosti i motivacije praktičara koji ih primenjuju. Ograničeno je razumevanje statusa procesa, a proces je generalno nestabilan (nezreo), što znači da organizacija nema vremena za poboljšavanje procesa, jer praktičar mora konstantno da reaguje, ponovo uspostavlja proces i otklanja nekonzistentnosti koje se uvek mogu pojaviti.
2. **Poboljšani procesi:** ovi procesi imaju opis konzistentan načinu na koji se procesi izvršavaju, upravljani su, dokumentovani, definisani i kontinualno poboljšavani. Ove procese eksplicitno podržava menadžment i drugi zaposleni. Procesu su dobro kontrolisani, a ponovljivost procesa se regularno evaluira i nameće. Konstruktivno se koriste merenja procesa i proizvoda rada procesa, a tehnologije se uvode na disciplinovan način. Poboljšavanje procesa je dugotrajan, stratejski zadatak.
3. **Institucionalizovan proces:** neki proces postaje institucionalizovan kada organizacija izgradi infrastrukturu koja obuhvata efektivne, iskoristive i konstantno primenjivane procese. Kultura rada organizacije nasleđuje i prenosi proces. Menadžment podržava i neguje takvu kulturu rada. Institucionalizovani procesi traju duže od ljudi koji su ih definisali i uspostavili

Za poboljšavanje i uspostavljanje stabilnih procesa osnovni zahtev je da su procesi definisani i opisani i da se obezbedi podrška menadžmenta organizacije. Pri tome, uvek treba zagovarati primenu standardnih procesa organizacije, podsticati individualnu inicijativu i nikada ne podcenjivati kritičan značaj ljudskih resursa za izvršavanje svakog procesa. Prva mera za poboljšavanje operativnih procesa je uklanjanje koraka koji ne dodaju novu vrednost procesu i koji mogu samo usporavati dostizanje postavljenih poslovnih ciljeva, [84]. U stabilizaciji procesa potrebno je povećavati produktivnost (efektivnost i efikasnost) procesa, čime se oslobađa vreme za angažovanje pojedinaca i tima na drugim kreativnijim poslovima. Dakle, ne treba slediti proces, stabilisati ga i poboljšavati zbog samih procesa, nego uspostavljati toliko stabilne i zrele procese koji rade tako da podržavaju poslove organizacije i ohrabruju zaposlene da uvek pružaju svoj maksimum.

2.2.2. Koncepti poboljšavanja procesa zaštite

Koristi od poboljšanja (sazrevanja) procesa za organizaciju su brojne, [63]:

- 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 lakše je upravljanje svim promenama i
- povećava se predvidljivost izlaznih performansi procesa.

Poboljšavanje procesa je klasični cilj upravljanja kvalitetom procesa. Kvalitet procesa za nabavku, razvoj, proizvodnju i održavanje komponenti sistema zaštite, veoma utiče na kvalitet sistema zaštite. Za poboljšavanje procesa postoje brojni *formalni* (strukturni) i *neformalni* pristupi i metodi.

Formalni metodi za poboljšavanje procesa su efektivni, sistematični i **strukturni** kroz sledeće korake:

- Razumeti i dokumentovati tekući proces (na primer, kroz *proces evaluacije*);
- Dekomponovati proces u skup sadržanih procedura i pomoćnih mehanizama;
- Odrediti redosled procedura prema prioritetu potrebe za poboljšavanjem;
- Identifikovati željenu situaciju za svaku proceduru/aktivnost procesa;

- Planirati implementaciju kao seriju postupnih (inkrementalnih) poboljšavanja i
- Implementirati i upravljati zavisnostima između procedura.

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

Neformalni metodi i pristupi za poboljšavanje procesa mogu biti vrlo različiti, zavisno od kulture rada organizacije, stručnosti zaposlenih i tipa procesa. Moguće je i korišćenje neke metodologije za poboljšavanje **produktivnosti**, **adaptivnosti** i **korisničke prihvatljivosti**, koje u principu zahtevaju promene operativnih procedura. Međutim, pošto promena operativnih procedura može uključivati značajan bezbednosni rizik, uvek više odgovara **struktuiran** pristup za identifikaciju i modifikaciju slabosti u izvršavanju procesa, [68], [85].

Prvi korak poboljšavanja bilo kojeg procesa je razumevanje tekućeg procesa. Kada se proces potpuno shvati, onda se verifikuje da li je proces 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 poboljšavanje procesa zahteva vreme, primarno se treba koncentrisati na one oblasti procesa koje izazivaju najveće probleme i najteže posledice. Kada se odrede prioriteti poboljšavanja procedura, može početi rad na identifikovanju metoda za poboljšavanje. U slučajevima relativno disjunktne procedura, gde je mala međuzavisnost procedura, poboljšavanje 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, [20], [85].

Planiranje implementacije poboljšavanja kroz seriju **inkrementalnih** koraka opravdano je zbog potencijalnog rizika, [85], [13], [35]. 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 poboljšavanje 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 prenošene poruke.

Primer *formalnog* pristupa poboljšavanju procesa zaštite demonstriran je u istraživačkom projektu rada kroz projekat evaluacije tekućih procesa ESS i predlog zadataka akcionog plana za poboljšavanje tih procesa.

Primer *neformalnog*, praktičnog korisničkog poboljšavanja stabilnosti - *produktivnosti*, *adaptivnosti* i *korisničke prihvatljivosti* procesa i značaja uspešne i potpune komunikacije svih učesnika u svakom, formalnom i neformalnom pristupu poboljšavanju procesa, opisan je u **Prilogu 2.2A**.

2.2.2.1. Značaj komunikacije za poboljšavanje procesa zaštite

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

- procesi zaštite su slabije definisani od procesa IKT sistema, pa je dobra komunikacija neophodna za identifikovanje, razumevanje i definisanje tih procesa,
- kompleksnost IKT sistema dodatno povećavaju još kompleksniji i korisnički teže prihvatljiviji sistemi zaštite, gde se kvalitetna komunikacija javlja kao faktor povećavanja razumevanja, odnosno smanjenja kompleksnosti i
- dobra komunikacija pomaže bolje razumevanje visoko stručne terminologije zaštite, čime se dodatno smanjuje kompleksnost sistema.

Od svih modela zrelosti SSE CMM i CMMI (*Capability Maturity Model Integration*) 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 politika, procedura i procesa, ali je pravi fokus modela na *procesu* i *poboljšavanje procesa*, što uključuje znanja i veštine ljudi, metode koje slede i alate koje koriste za izvršavanje svojih aktivnosti. Za poboljšavanje 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, sama za sebe, ne poboljšava prakse i procese, nego je sredstvo za uspostavljanje *komunikacije* između nameravanih i stvarno implementiranih praksi i procesa. Na taj način element *komunikacije* neposredno utiče na poboljšavanje praksi i procesa.

Razumevanje komponenti uspešne 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, markentiške podatke, teoriju upravljanja, politiku, elemente i izgradnju tima za ublažavanje rizika, planove i brojne druge sadržaje. Poruke koje se odnose na podatke o procesima obuhvataju postavljanje očekivanja, uspostavljanje standarda i referentnih nivoa, definisanje uloga, informisanje, detaljno upoznavanje zadataka i dr. 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 i.t.d. Međutim, bez obzira na formu, svaka kompletirana (uspešno završena) komunikacija ima određene osnovne komponente (Prilog 2.2A).

2.2.3. Struktuirani pristup za poboljšavanje procesa

2.2.3.1. *Evaluacija procesa zaštite*

Ključni alat za postizanje željenih rezultata u formalnom pristupu poboljšavanju procesa je metodologija **evaluacije** (*appraisal*), koju primenjuje osposobljen tim za evaluaciju (TE) na bazi nekog referentnog modela procesa najbolje prakse (n.p.r., SSE CMM, CMMI), [102], [21], [84]. Cilj svake evaluacije, na bazi bilo kojeg modela poboljšavanja 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, koji obuhvata empirijski potvrđene *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 najbolje prakse, to zahteva puno neproduktivnog rada i trošenja resursa organizacije.

Procesno orijentisani modeli i metodi *evaluacije* rezultat su evolucije načina razmišljanja i naučnog mišljenja o poslu, poslovnom sistemu, upravljanju i navikama zaposlenih. **Procesi** su centralni elementi oko kojih su strukturirani tipični poslovi cele **industrijske ere**, u kojoj su finansije stratejski resurs, upravljanje usmereno na ostvarivanje novih vrednosti i nagrađivanje izvršilaca, a struktura zaposlenih - na rad i izvođenje projekata. U nastupajućoj **eri znanja**, poslovi su strukturirani oko **sistema**, gde su SE znanja, objektno orijentisani i procesni pristup od presudnog značaja; gde se upravljanje integriše, a *znanje* postaje neopipljivi strateški resurs i deli se u zajednici zaposlenih i šire, [7], [8].

Evaluacija je prvi korak u procesu identifikovanja stanja tekućih procesa i poboljšavanja procesa. Pojam *evaluacije* (eng. *evaluation*) označava sistematsko prosuđivanje i određivanje *intrinzičnih* (bitnih, primarnih) i/ili *ekstrinzičnih* (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 deskriptivan proces i u osnovi nije evaluativno. Evaluaciju izvode evaluatori, osposobljeni da evaluaciju obave efektivno i efikasno. Evaluacija je proces koji se sastoji od određenog broja faza i koraka i uvek je svrsishodna – ima za cilj stvaranje kognitivnih pretpostavki za efikasno i efektivno odlučivanje i delovanje. Uključuje odgovornosti **evaluatora** i **evaluanda**. 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 namenu i ima očekivani kvalitet. **Verifikacija** je potvrđivanje da proizvod/servis zaštite odražava specifikovane zahteve politika, standarda i/ili korisnika, [7]. U brojnim modelima sazrevanja procesa tipa CMM, za *evaluaciju* se koristi termin *appraisal* koji implicira da evaluaciju obavlja spoljni stručni tim za evaluaciju, osposobljen za primenu referentnog modela i metoda za evaluaciju sa ciljem poboljšavanje procesa, [20], [102].

Za evaluaciju procesa razvijeno je više standarda i modela, od kojih svaki ima određene prednosti i nedostatke.

Prema standardu opštih kriterijuma-CC (*Common Criteria*)- **ISO 15408**, [1], **cilj procesa evaluacije** je da pokaže da sistem ispunjava specifične bezbednosne zahteve pod specifičnim uslovima. Sistem koji to ispunjava naziva se *poverljiv*, a *poverenje* se zasniva na specifičnim *indikatorima objektivnih dokaza* nivoa bezbednosti, koji garantuju da je sistem bezbedan, [18].

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, [49], [56]:

- 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 nivoa 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, tzv. *nivoe poverenja* u sistem zaštite.

Evaluacija podrazumeva nezavisnu i objektivnu procenu i merenja garantovane bezbednosti koju obavljaju nezavisni eksperti – evaluatori. Proces evaluacije može uključivati procenu: *konzistentnosti, kompletnosti, tehničke pouzdanosti i nivoa zaštite od pretnji, administracije sistema zaštite, korisnika, instalacija, dokumentacije zaštite, konfiguracije i korišćenja sistema*, [49].

2.2.3.2. Modeli i okviri za poboljšavanje procesa

Za potrebe formalnog, struktuiranog poboljšavanja procesa, vremenom su razvijeni brojni modeli procesa. Korišćenje nekog modela procesa za poboljšavanje procesa rentabilno je iz više razloga. Pored toga što organizacija može uskladiti svoje procese sa iskustveno dokazanom najboljom praksom, tipično kritičnih procesa za većinu organizacija sa različitim poslovnim profilom, neki modeli sadrže integrisane procese iz više oblasti primene, oblasti procesa koje se mogu prilagođavati ili, ako ih model ne obuhvata, proširivati sa specifičnim ciljevima i praksama procesa organizacije za specifičan kontekst i okruženje (n.p.r., SSE CMM i CMMI modeli integrisanih procesa), [20].

Generalno za evaluaciju i poboljšavanje multidisciplinarnih procesa, kakvi su i procesi zaštite, potrebno je uspostaviti više okvira za evaluaciju i poboljšavanje. Poboljšani procesi povećavaju uniformnost proizvoda, smanjuju ponavljanje rada i grešaka, smanjuju nepotrebno trošenje radne snage, mašinskog rada i materijala, dakle, povećavaju kvalitet izlaznih proizvoda rada sa manjim troškovima ukupnih kapaciteta (resursa). Ostale dobiti od poboljšavanja kvaliteta procesa su niža cena proizvoda, zadovoljniji korisnici i kupci i više rada i zaposlenih zbog konkurentnije pozicije

organizacije na tržištu. Tradicionalne mere za performanse procesa korišćene su za pokazivanje finansijskih performansi, operativne efikasnosti i.t.d. Međutim, ove mere neadekvatno prikazuju progres u promeni ponašanja i efektivnosti rada, kao i u strategiji poboljšavanja procesa.

Razvijeni metodi i procesi evaluacije ugrađeni su u nekoliko okvira za poboljšavanje procesa, pri čemu se metod evaluacije oslanja na referentni model za poboljšavanje procesa (n.p.r., CMMI model pokriva SCAMPI metod evaluacije, SSE CMM model – SSAM metod evaluacije i.t.d.). 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 (n.p.r., upravljanje sporazumom sa snabdevačem). Dakle, zbog ograničenja i usmerenosti okvira za poboljšavanje procesa, u organizacijama su često razvijani i održavani paralelni procesi.

Razvojem integrisanih modela sazrevanja i poboljšavanja procesa tipa SSE CMM, CMMI i iCMMI, koji kombinuju nekoliko okvira procesa za specifične discipline (inženjerske, sistemske, razvoja softvera, nabavke, davanja usluga, zaštite), otvara se mogućnost integracije procesa u organizaciji i smanjuje broj 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 brojnim drugim standardima i modelima za evaluaciju i poboljšavanje procesa, [11], [67], [18], [21], [22], [32], [77].

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 samog sebe, nego – poboljšavanje ukupnih kapaciteta organizacije za ostvarivanje poslovnih ciljeva i misije organizacije. Kvalitet modela procesa raste sa povećavanjem broja oblasti primene i disciplina, kakvi su, na primer, SSE CMM i CMMI modeli, [20].

Generalno, razvoj **integrisanih procesa** koji su usaglašeni za primenu u više disciplina, veoma je kompleksan poduhvat - organizaciono, upravljački i tehnički. Međutim, poboljšavanje procesa koje obezbeđuju integrisani modeli (CMMI tipa), samo po sebi ne implicira postojanje integrisanih procesa. Za prelazak organizacije na višestruko usklađene i integrisane procese potrebno je razviti strategiju deriviranu iz strateških ciljeva organizacije. Ključni koraci u procesu razvoja ove strategije su, [20], [41], [63]:

1. **Kvantifikacija poslovnih ciljeva**, koja pomaže da se odredi obim uključivanja organizacije;
2. **Definisanje višestruko usklađene, integrisane strategije organizacije**, uključujući određivanje vremenskog plana za usklađivanje svake organizacione jedinice sa identifikovanim okvirom za evaluaciju i poboljšavanje procesa;
3. **Analiza rentabiliteta (cost-benefit) strategije**, kojom se rafinira strategija;
4. **Identifikovanje i analiza rizika** koji prati implementaciju strategije i obuhvata preporuke za ublažavanje ovih faktora rizika;
5. **Razvoj plana kolaboracije relevantnih učesnika** u kojem se identifikuju svi relevantni učesnici i način tekuće i periodične komunikacije u organizaciji;
6. **Procena ukupnog rizika** za svaki metod evaluacije koji pokriva multi-disciplinarne i integrisane procese, koji je znatno složeniji od evaluacije procesa jedne discipline. Pored uobičajenih faktora rizika koji prate poboljšavanje procesa, sledeći faktori rizika smatra se da generalno imaju visoku verovatnoću pojavljivanja i visok uticaj:
 - a. **Održavanje učešća i sponzorske podrške menadžmenta** u toku celog procesa od presudne je važnosti, jer se poboljšavanju procesa daje značaj i najviši prioritet;

- b. *Održavanje kolaborativne saradnje članova tima za poboljšanje procesa*, koji pokrivaju različite discipline ili granice okvira, pa može postojati veliki otpor prema integraciji procesa. Potrebno je ove otpore pravilno razumeti i prevazilaziti jačanjem timskog rada i isticanjem prednosti integracije procesa;
- c. *Održavanje finansiranja tokom projekta*, pri čemu se finansijske potrebe deriviraju iz analize rentabiliteta i treba ih pratiti u odnosu na performanse ukupnih napora (rada);
- d. Isticanje značaja podrške menadžera organizacionih jedinica, njihovog učešća u poboljšavanju i integraciji procesa, kroz postavljenje svih napora kao poslovnih ciljeva;
- e. Kreiranje korisničke prihvatljivosti, pošto su korisnici tipično odbojni na promene procesa, posebno ako ne vide dobiti i dodatne vrednosti. Integraciju procesa i poboljšanje korisnici mogu videti "kao promenu radi promene". Isproban metod za dobijanje korisničke prihvatljivosti je uključivanje relevantnih korisnika iz prakse procesa u sve napore integracije i poboljšanja procesa u organizaciji, posebno uz eksplicitnu podršku menadžmenta;
- f. Obezbeđivanje dobre komunikacije i razumevanja između svih organizacionih jedinica, uključivanjem gde god je moguće, većih i iskusnih ljudi u tim za evaluaciju, poboljšavanje i integraciju procesa u organizaciji za ublažavanje ovog faktora rizika i
- g. Obezbeđivanje potrebnih znanja iz više metoda za evaluaciju i poboljšavanje procesa koji postoje u organizaciji, obezbediće bolje razumevanje integrisanog okvira. Ovim se mogu povećati tačnost, skratiti vreme i povećati efektivnost i efikasnost evaluacije, poboljšavanja i integracije procesa, čak i u slučaju angažovanja spoljnih saradnika-eksperata.

Ovi najčešći faktori rizika po intenzitetu, verovatnoći pojave i uticaju, registrovani u tranziciji organizacije sa multidisciplinarnim okvirima za evaluaciju i poboljšavanje procesa na integrisane procese, evaluaciju i poboljšavanje sa jednim metodom, zavise od veličine, geografske distribucije i poslovnih modela organizacije. Ublažavanje faktora rizika vrši se prema planu za ublažavanje faktora rizika, [6], [17], [44], [57], [58], [80], [92], [93], [94].

2.3. Pregled standarda kvaliteta proizvoda i sistema zaštite

2.3.1. Uvod

Nekoliko međunarodnih standardizacionih tela pokazalo je tokom mnogo godina nesumnjiv interes za oblast IKT zaštite: Britanski institut za standarde-**BSI British** (*British Standards Institute*), Nemački agencija za zaštitu informacija - **BSI 1Germany** (*Bundesamt für Sicherheit in der Informationstechnik*), Međunarodna organizacija za standardizaciju - **ISO** (*International Organization for Standardization*), Međunarodna komisija za elektrotehniku - **IEC** (*International Electrotechnical Commission*) i Nacionalni institut za standarde i tehnologiju - **NIST** (*National Institute of Standards and Technology*), [112].

Postoje brojne metodologije za testiranje i garanciju kvaliteta proizvoda i procesa, koje mogu doprineti proizvodnji bezbednih (bez bagova) programskih kôdova i softverskih proizvoda za zaštitu. U Standardu **ISO/IEC 15443** navedene su sve metode i sredstva za kontrolu kvaliteta na bazi **evaluacije**, [27], [28], [49], [50], [51], [53], [54], [76]:

- **proizvoda/sistema/servisa**: *CC/CEM, ITSEC/ITSEM, TCSEC/TPEP, ISO/IEC 9646*-okvir i metodologija za testiranje usaglašenosti, testiranje usklađenosti, testiranje na proboj, *X/Open branding* (softverski proizvodi sa otvorenim izvornim kôdom), personalna garancija i *ISO/IEC 14598* za evaluaciju softverskih proizvoda;

- **okruženja (personal i organizacija):** TCMM, ISO 13407- proces dizajna fokusiran na čoveka i interaktivne sisteme i profesionalna sertifikacija i
- **proces:** SSE-CMM-model i standard sazrevanja procesa zaštite, ISO 9000-3–standard za upravljanje kvalitetom i standard garancije kvaliteta 3.deo, ISO 9001– kvalitet sistema, ISO/IEC 15504-procena procesa za razvoj softvera, CMMI v.1.2- integracioni model sazrevanja procesa, pedigree proizvođača, proizvođačka garancija, deklaracija snabdevača, održavanje nivoa evaluacije, akreditacija sistema zaštite.

Druge tehnike evluacije uključuju evaluacije specijalne namene kao što su kriptografski moduli, za koju se koristi standard FIPS-140-2, [74], [90], [112].

2.3.2. Standardi i modeli kvaliteta proizvoda i sistema zaštite

Od brojnih standarda kvaliteta, relativno mali broj se odnosi na bezbednost IKT sistema. Na primer, **ISO 9000** standard kvaliteta industrijskih proizvoda sadrži neke elemente garancije kvaliteta procesa, primenljive za proizvodnju operativnog i softvera za zaštitu, [54]. Od početka 1980-ih, međunarodna zajednica za zaštitu računara razvijala je kriterijume i metodologije za evaluaciju zaštite IKT proizvoda i sistema. Prvu javnu i široko korišćenu tehniku obezbedili su **Kriterijumi za evaluaciju poverljivog računarskog sistema - TCSEC (Trusted Computer System Evaluation Criteria)**, koje je razvilo ministarstvo odbrane SAD, [76], [90]. Iako su široko primenjivani gotovo dve decenije, TCSEC kriterijumi pretrpeli su brojne kritike, od kojih su najznačajnije: ograničeni obim, problemi sa procesom evaluacije, povezivanje bezbednosne garancije i funkcionalnosti, ne priznavanje evaluacije izvršene u drugoj zemlji, nefleksibilnost u izboru zahteva i dr.

Iako su svi naponi da se proizvodi evaluiraju na bezbednosne karakteristike prihvaćeni kao neophodne funkcije, mnogi eksperti zaštite priznaju da je proces za evaluaciju proizvoda i sertifikaciju sistema zaštite vremenski zahtevan i vrlo skup. Rezultat toga je da proizvodi zaštite dolaze na tržište na jedan od sledećih načina:

1. **kroz dugu i skupu evaluaciju**, tako da poverljivi proizvodi zaštite na tržište dolaze dugo posle potrebe za njima, a sistemi koji su implementirani više ne obuhvataju pretnje za koje su namenjeni, ili
2. **bez evaluacije**, gde se kupci oslanjaju samo na tvrdnje proizvođača o kvalitetu proizvoda zaštite.

Važno je uočiti da su evaluacija poverljivih proizvoda zaštite i sertifikacija sistema zaštite usmerene na pažljivo ispitivanje krajnjeg proizvoda, tj. sistema ili proizvoda i njihove dokumentacije, dok uopšte ne obraćaju pažnju na **procese** koji su uključeni u njihovo kreiranje.

Čini se da je TCSEC standard pokušao da definiše neke procese koji omogućavaju uspostavljanje visoke bezbednosne garancije sistemau, ali zahtevaju testiranje sistema na proboj, korišćenje formalnih matematičkih metoda i upravljanje konfiguracijom. Zato su proizvođači u razvoju bezbednih proizvoda i sistema povećali primenu specifičnih procedura ovog standarda, da bi postigle visok bezbednosni nivo krajnjeg proizvoda. Međutim, ostao je problem što se sve koristi od primene ovih procedura ne mogu postići u *nedisciplinovanom radnom okruženju*. Procesno orijentisani model sazrevanja procesa zaštite – SSE CMM nudi novu paradigmu za obezbeđivanje zaštite i garantovanog nivoa bezbednosti proizvoda i sistema, na bazi garantovanih nivoa zrelosti kapaciteta, tj. na bazi poverenja u zrelost sistem-inženjerske grupe praksi i procesa zaštite, [112].

Razvijene su nove metodologije sa namerom da obuhvate i reše uočene probleme. Najznačajniji su svakako međunarodni **Kriterijumi za evaluaciju zaštite IKT sistema - ITSEC (Information Technology Security Evaluation Criteria)**, [56], [58] razvijeni u Evropi, **Kanadski kriterijumi za evaluaciju proizvoda poverljivih računarskih sistema – CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)** i **Federalni kriterijumi SAD - FIPS (Federal Information Processing Standards)** i **NIST - National Information Standard and Technology**), [74], [75]. Ove

fundamentalne metodologije dovele su do razvoja **Opštih kriterijuma za evaluaciju proizvoda i sistema zaštite** – (CC)¹, prihvaćenih širom sveta, [49].

2.3.2.1. Kriterijumi za evaluaciju poverljivih kompjuterskih sistema

Kriterijumi za evaluaciju poverljivih, ili bezbednih kompjuterskih sistema - **TCSEC** (*Trusted Computer System Evaluation Criteria*), tzv. „*Orange book*“, koje je koristila vlada SAD od 1983-1999, više nisu u upotrebi. Važni koncepti **TCSEC** su, [17], [76]:

- **TCB** (*Trusted Computing Base*), baza poverljivog računarskog sistema i
- **Referentni monitor**, referentni mehanizam za za evaluaciju i validaciju pristupa u slojevitom i složenom sistemu zaštite.

Standard ima težište na zaštiti OS, a *indikator nivoa bezbednosti* klasifikovani su u 7 kategorija:

- **D**: ne prolazi evaluaciju,
- **C1**: obezbeđena diskreciona zaštita,
- **C2**: obezbeđena zaštita sa kontrolom pristupa,
- **B1**: obezbeđena zaštita sa bezbednosnim označavanjem,
- **B2**: obezbeđena struktuirana zaštita,
- **B3**: obezbeđena zaštita izolovanjem domena zaštite i
- **A1**: obezbeđen verifikovan sistem zaštite.

Funkcionalni zahtevi standarda TCSEC obuhvataju :

- Diskreciona kontrola pristupa (DAC);
- Ponovo korišćenje objekata (sadržaje memorijskih i sektora HD ne treba prenositi novim korisnicima);
- Obavezna kontrola pristupa (MAC), zahteva se za klase B1 i više;
- Zaštita na više nivoa (tipa *Bell-LaPadula* modela);
- Bezbednosno označavanje, koje se odnosi na klase B1 na više, MAC i označavanje subjekata i objekata u sistemu zaštite;
- Identifikaciju i autentifikaciju korisnika i entiteta;
- Zahtevi za poverljivost, za B klasu i više i poverljivost između korisnika i poverljivih računarskih sistema (TCB) i
- Zahtevi za kontrolu (*audit*) sistema zaštite.

Zahtevi za garantovanu bezbednost TCSEC standarda obuhvataju:

- *Zahtev za upravljanje konfiguracijom* za klasu B2 i više, sa identifikacijom, odgovarajućim mapiranjem i dokumentacijom konfigurisanih uređaja i podsistema i njihove izvorne kôdove;
- *Zahtev za poverljivu distribuciju informacija*, samo za klasu A1, koji podrazumeva kontrolisan proces od izvornog kôda do isporuke kupcu (korisniku), koji štiti integritet proizvoda/sistema zaštite;
- *Zahtev za arhitekturu sistema*, koji podrazumeva modularnost, minimizaciju složenosti, smanjenje i pojednostavljenje TCB, a počinje sa klasom C1. Klasa B3 mora imati potpuni referentni mehanizam za validaciju;
- *Zahtev za specifikaciju i verifikaciju dizajna*, koji predviđa za: B1 klasu - model neformalne politike zaštite, B2 – model detaljne specifikacije i formalne politike zaštite, B3 – dokazivanje da specifikacija sistema zaštite zadovoljava model klase B3, i za A1 - formalnu detaljnu specifikaciju i mapiranje do izvornog kôda;
- *Zahtev za testiranje*, koji uključuje zahtev za zaštićene kanale na najvišim nivoima bezbednosnih klasa proizvoda/sistema zaštite;

¹ CC kriterijumi su opozvani 2005. godine.

- *Zahtev za dokumentovanje proizvoda/sistema zaštite*, koji podrazumeva izradu *Korisničkog uputstva za zaštitu* i *Priručnika za poverljivi kompjuterski sistem*, i
- *Zahtev za garantovanu bezbednost procesa* za razvoj bezbednog proizvoda/ sistema zaštite.

Prednosti i nedostaci TCSEC standarda:

- Obezbeđuje kreiranje pristupa za analizu dizajna, implementacije, dokumentacije, procesa za razvoj, instalaciju i spoljnu kontrolu (*audit*) sistema zaštite;
- Ograničena primena samo za vladu i vojne potrebe SAD;
- MAC kontrola pristupa, nema toliki značaj za civilne potrebe, koliko za vojnu i policijsku primenu;
- Glavni bezbednosni zahtev je zaštita poverljivosti (tajnosti) podataka i
- Zaštita integriteta i raspoloživosti nije obuhvaćena ovim standardom.

2.3.2.2. *Kriterijumi/uputstvo za evaluaciju zaštite IKT sistema*

Kriterijumi za evaluaciju zaštite IKT sistema - **ITSEC** (*Information Technology Security Evaluation Criteria*) i **Uputstvo za evaluaciju** - **ITSEM** (*Information Technology Security Evaluation Manual*), razvijeni ranih 1990-ih (Francuska, Nemačka, Holandija i V. Britanija), prethodili su standardu **Opšti kriterijumi** - (CC) i **Opšta metodologije za evaluaciju** (CEM-*Common Evaluation Methodology*). **ITSEC** bezbednosna garancija bazirana je na pristupu koji je uveden u poverljivom - **TCSEC**. Međutim, razdvajanje funkcionalnih i bezbednosnih zahteva u **ITSEC** dopušta veću fleksibilnost. Sami bezbednosni zahteva su podeljeni sa dva aspekta: efektivnosti i tačnosti. Procena efektivnosti uključuje razmatranje sledećih aspekata **ciljeva (objekata) evaluacije** - **TOE** (Target of Evaluation), [18]:

- Pogodnosti **TOE** bezbednosnih funkcija koje nameću zaštitu od pretnji za bezbednost **TOE**, identifikovane su u bezbednosnim ciljevima (**ST** –*Security Target*);
- Sposobnosti da se **TOE** bezbednosne funkcije i mehanizmi koji nameću zaštitu, povežu zajedno u integralnu i efektivnu celinu;
- Sposobnosti mehanizama zaštite **TOE** da izdrže direktni napad;
- Mogućnosti kompromitovanja sistema zaštite **TOE** u praksi zaštite, zbog poznatih bezbednosnih ranjivosti u konstrukciji **TOE**;
- Nemogućnosti konfigurisanja, ili korišćenja **TOE** na nebezbedan način, nego na način koji administrator, ili krajnji korisnik smatraju prihvatljivo bezbednim;
- Mogućnosti kompromitovanja sistema zaštite **TOE** u praksi zaštite, zbog poznatih bezbednosnih ranjivosti u operativnom radu **TOE**.

Zahtevi za efektivnost sistema zaštite više usmeravaju pažnju na one aspekte gde evaluator mora koristiti svoja vlastita znanja i iskustva da proceni da li je bezbednosni pristup u evaluiranom IKT proizvodu ili IKT sistemu, racionalan. Zahtevi za tačnost zaštite u **ITSEC** više se odnose na aspekte, koji potvrđuju da su tačne informacije projektanta o zaštiti evaluiranog IKT proizvoda ili sistema.

ITSEM, izgrađen na bazi **ITSEC**, opisuje kako neki **TOE** treba da bude evaluiran u skladu sa ovim kriterijumima. Specifični cilj **ITSEM** je da obezbedi harmonizovan skup metoda za evaluaciju, koje su komplementarne referentnom modelu **ITSEC**.

ITSEC indikatori evaluacije nivoa bezbednosti (E) mogu se ukratko definisati kao:

E0: Neadekvatna bezbednost.

E1: Moraju se sačiniti **ST** i opis arhitekture. Dokumentacija korisnika i administratora je uputstvo za zaštitu **TOE**. **TOE** treba jedinstveno identifikovati i da ima dokumentaciju konfiguracije, isporuke, instalacije i načina rada. Mora se koristiti metod sigurne distribucije. Funkcionalno testiranje treba da obavlja akreditovan evaluator, a nadzor - nadležni organ.

E2: **E1** + mora se generisati neformalna dokumentacija detaljnog dizajna i načina testiranja. Arhitektura pokazuje deljenje **TOE** na primenjene bezbednosne i druge komponente.

Procenjuju se upravljanje konfiguracijom i bezbednost proizvoda. Evidencija kontrole pristupa zahteva se za vreme starta i u toku rada. Evaluators izvršava funkcionalno testiranje i testiranje na proboj pod nadzorom nadležnog organa.

- E3: E2 + treba generisati izvorni kôd, ili hardversku šemu. Mora se potvrditi saglasnost izvornog kôda i detaljnog dizajna i koristiti procedura prihvatanja. Način implementacije treba da bude u skladu sa priznatim standardima. Mora se obezbediti dokaz o ponovljenom testiranju posle korekcije grešaka. Funkcionalna i testiranja na proboj vrše evaluatori.
- E4: E3 + mora se generisati formalni model zaštite i poluformalna specifikacija priimenjenih funkcija, arhitekture i detaljnog dizajna zaštite. Testiranje mora pokazati da je zaštita dovoljna. TOE i alati su pod kontrolom procesa upravljanja konfiguracijom i sa dokumentovanjem opcija kompajliranja. TOE je konfigurisan tako da zadržava bezbedan start i oporavak nakon pada sistema.
- E5: E4 + dizajn arhitekture objašnjava međusobne odnose između primenjenih komponenti zaštite. Treba proizvesti informacije o procesima integracije i biblioteku vremena rada - log datoteku. Upravljanje konfiguracijom je nezavisno od onih koji je razvijaju. Obavezna je identifikacija konfigurisanih bezbednosno relevantnih elemenata TOE sa njihovim međusobnim odnosima.
- E6: E5 + formalni opis arhitekture i primenjenih funkcija zaštite koje treba generisati. Treba dokazati usklađenost formalne specifikacije primenjenih funkcija zaštite kroz izvorni kôd i testiranje. Različite konfiguracije TOE definisane su u terminima formalnog dizajna arhitekture. Svi alati su podvrgnuti kontroli konfiguracije.

Procesi evaluacije prema modelima TCSEC, ITSEC i ITSEM danas nemaju širu praktičnu primenu.

2.3.2.3. Opšti kriterijumi za evaluaciju proizvoda i sistema zaštite (CC)

Standard opštih kriterijuma-**CC** (*Common Criteria*), [18], za evaluaciju proizvoda i sistema zaštite, izradio je konzorcijum NSA (Nacionalnih agencija za bezbednost, SAD) i EU. Pod uticajem Međunarodnog komiteta, **CC standard** je usvojen kao međunarodni standard **ISO/IEC 15408**. Standard su prihvatile sve zemlje EU, Australija, Japan i Rusija, a zamenio je postojeće standarde „Orange Book“ (SAD) i **ITSEC** (EU).

Struktura CC standarda obuhvata 3 dela: Uvod i opšti model, Funkcionalne zahteve i Bezbednosne zahteve. U **CC standard** uključeni su sledeći relevantni standardi:

3. Procedure za registraciju profila zaštite (**IS 15292**),
4. Okvir za bezbednosnu garanciju (**WD 15443**),
5. Uputstvo za izradu profila zaštite (**WD 15446**) i
6. Metodologija za evaluaciju zaštite (**WD 18045**).

CC standard koristi sledeće definisane termine, [12]:

Definicija 182: Politika zaštite (TSP) objekta evaluacije (TOE) je skup pravila koja regulišu kako su objekti upravljani, zaštićeni i distribuirani unutar proizvoda ili sistema. **Definicija 183: Bezbednosna funkcija** objekta evaluacije (TSF) je skup koji sadrži sve hardverske, softverske i firmware (memorijske elemente) proizvoda ili sistema, a koji se koristi za nametanje politike zaštite. TSF je uopšten koncept TCB iz TCSEC standarda.

Definicija 184: Profil zaštite (PP) je skup izjava o bezbednosnim zahtevima za kategorije proizvoda ili sistema, nezavisno od implementacije, koji obuhvata pretnje u specifičnom okruženju i ispunjava specifične potrebe korisnika.

Definicija 185: Bezbednosni cilj (ST) je skup bezbednosnih zahteva i specifikacija kojima proizvod ili sistem teži, a koje treba koristiti kao osnovu za evaluaciju identifikovanog proizvoda ili sistema.

Funkcionalni zahtevi CC standarda:

a) Grupisani su na bazi ispunjenih bezbednosnih ciljeva (**ST**) u **11 klasa**, [68]:

1. identifikacija i autentifikacija,
2. zaštita korisničkih podataka i informacija,
3. zaštita bezbednosnih funkcija - zahtev se odnosi na integritet i kontrolu datih servisa zaštite i mehanizama koji realizuju te servise,
4. upravljanje zaštitom - zahtev se odnosi na upravljanje atributima i parametrima zaštite,
5. kontrola i nadzor sistema zaštite - prijava incidenta, registracija, skladištenje, analiza podataka, ocena ugroženosti TOE, reagovanje na ugrožavanje sistema zaštite,
6. kontrola pristupa objektu evaluacije,
7. zaštita privatnosti - zaštita korisnika od otkrivanja i neovlašćenog korišćenja ličnih podataka,
8. korišćenje objekata IKT sistema - zahtev za raspoloživost informacija,
9. kriptografska podrška - upravljanje kriptografskim ključem,
10. kanali veze - autentifikacija strana koje učestvuju u razmeni podataka,
11. poverljivi kanali veze - za vezu sa servisima zaštite.

b) Funkcionalni zahtevi CC standarda sadrže **66 familija i 135 komponenti**. Na primer:

1. Klasa „Zaštita privatnosti“ sadrži 4 familije funkcionalnih zahteva: (1) Anonimizacija, (2) Pseudonimizacija, (3) Nemogućnost povezivanja podataka sa licem i (4) Tajnost podataka.
2. Klasa „Korišćenje objekata IKT sistema“ sadrži 3 familije zahteva za raspoloživost informacija i servisa IKT sistema: (1) Upravljanje otkazima, (2) Isporuca servisa po prioritetima i (3) Deljenje ili zajedničko korišćenje resursa IKT sistema.

Zahtevi za garantovanu bezbednost (eng. assurance):

a) Imaju sledeće karakteristike:

- namenjeni su za utvrđivanje garantovane bezbednosti ili bezbednosne garancije,
- zasnivaju se na aktivnom ispitivanju (testiranju),
- imaju istu formu kao i funkcionalni zahtevi,
- specifični su po tome što svaki element bezbednosnih zahteva sadrži inherentnu neodređenost (grešku) koja pripada jednom od tri moguća tipa:
 1. uticaju **praktičara** koji ih razrađuje za primenu,
 2. predstavi i sadržaju pojma **uverenja** (poverenja) i
 3. subjektivnom uticaju **evaluatora**.

b) Obuhvaćeni su sa 9 klasa:

1. **razvoj** - zahtev za fazni razvoj bezbednosnih funkcija od izrade specifikacije do detalja implementacije i integracije proizvoda/sistema u IKT sistem,
2. **podrška životnog ciklusa** - zahtevi za modelovanje životnog ciklusa, uključujući redosled otklanjanja nedostataka u zaštiti okruženja,
3. **testiranje** – proizvoda sistema na proboj,
4. **ocena pouzdanosti** - uključujući ocenu **stabilnosti** bezbednosnih funkcija, instalaciju i eksploataciju,
5. **upravljanje konfiguracijom**,
6. **dokumentovanje** - zahtev se odnosi na eksploatacionu dokumentaciju,
7. **bezbednosna garancija** - za podršku u fazi posle sertifikacije,
8. **evaluacija profila zaštite (PP)** i
9. **evaluacija bezbednosnih ciljeva (ST)**.

c) Sadrže **44 familije i 93 komponente**.

Namena CC standarda je za:

- proizvodnju bezbednijih komponenti zaštite;
- evaluaciju bezbednosti softverskih i hardverskih proizvoda zaštite, a često samo dela tih proizvoda;
- evaluaciju *smart* kartica, ali ne i softvera koji one koriste i za
- sertifikaciju postignutog nivoa bezbednosti kod razvijenog proizvoda zaštite.

Primena CC standarda u praksi zaštite zahteva procenu nekoliko elemenata, kao što su: *pretnje, mehanizmi zaštite, testiranje, dokumentacija, instrukcija o bezbednoj primeni, test na mogući proboj, plan za upravljanje verzijama razvoja i projektna dokumentacija.*

Proces CC evaluacije u SAD kontroliše akreditovana laboratorija NIST na osnovu primene metodologije CC evaluacije - *CEM (CC Evaluation Methodology)*, pod komercijalnim uslovima. U svetu postoji svega nekoliko akreditovanih entiteta (agencija) za CC evaluaciju, što je jedna od osnovnih slabosti šire praktične primene ovog metoda evaluacije. Tim za evaluaciju (TE) obezbeđuje evaluaciju profila zaštite (PP) proizvoda i sistema i njihovih bezbednosnih ciljeva (ST). TE tipično ima 4-6 članova (kao i TCSEC). Evaluacija PP izvodi se potpuno u skladu sa CEM dokumentom i u skladu sa usaglašenim planom sa evaluiranim entitetom (*evaluandom*). Kada se PP evaluacija kompletira, TE prezentira nalaze agenciji za CC validaciju, koja odlučuje o validaciji PP evaluacije i dodeljuje *EAL indikatore nivoa bezbednosti*. Evaluacija proizvoda ili sistema je neznatno kompleksnija, zato što sadrži više koraka i zahteva više evaluacionih dokaza. Za ovu evaluaciju organizacija mora obezbediti nacrt bezbednosnih ciljeva proizvoda ili sistema koji se evaluiraju, da bi TE mogao koordinirati projekat sa agencijom za validaciju. Kada se evaluacija kompletira, TE prezentira nalaze agenciji za CC validaciju, koja odlučuje o validaciji nalaza evaluacije i dodeljuje EAL bezbednosne nivoe.

Indikatori evaluacije nivoa bezbednosti - **EAL** (Evaluation Assurance Level) definisani su za 7 nivoa evaluacije, [18], [49]:

EAL 1: (početni) najniži nivo koji obuhvata analizu specifikacija funkcionalnosti, specifikacija interfejsa, eksploatacione dokumentacije i nezavisno testiranje. Primenjuje se kada se pretnje ne smatraju ozbiljnim, a značajan je za projektante u razvoju i potrošače. Testiranje funkcionalnosti je izvršeno. Definiše minimalni nivo bezbednosne garancije na bazi analize funkcija zaštite proizvoda i dizajna interfejsa TOE, onako kako ih prezentiraju projektanti, da bi se razumelo bezbednosno ponašanje. U cilju razumevanja zaštite, obezbeđuje analizu funkcija zaštite na bazi specifikacija funkcionalnosti i interfejsa. Nema validacije kriptozastitnog modula.

EAL 2: *EAL 1* + projekat *TOE* na najvišem nivou apstrakcije, izvršeno nezavisno testiranje, analiza stabilnosti funkcija zaštite i revizija analize ranjivosti sistema. Najviši je bezbednosni nivo koji se može dati bez nametanja dodatnih zadataka projektantima proizvoda zaštite, pored onih za *EAL 1*. Analiza zahteva za funkcionalnost i specifikacija interfejsa vrši se uporedo sa revizijom modela projekta podsistema proizvoda.

EAL 3: *EAL 2* + kontrola okruženja i upravljanje konfiguracijom TOE. Opisuje umeren nivo nezavisno obezbeđene zaštite, odnosno, vrednovane od strane nezavisnog spoljnog entiteta. Ovaj nivo dopušta maksimalnu bezbednosnu garanciju iz faze projektovanja sa nekoliko izmena u procesu testiranja. Maksimalna bezbednosna garancija implicira da je proizvod projektovan sa uključenom zaštitom, umesto implementacije zaštite posle projektovanja. Projektant mora obezbediti dokaze o testiranju, uključujući analizu ranjivosti, koja se zatim selektivno verifikuje. Na ovom nivou prvi put se uključuju elementi evaluacije upravljanja konfiguracijom. Vrš se strukturno testiranje i analiza zaštitnih funkcija korišćenjem specifikacija zahteva za funkcionalnosti i interfejse i projekta podsistema TOE na visokom nivou apstrakcije. Vrš se nezavisno testiranje funkcija zaštite i evidentiraju korisničko testiranje tipa "crne kutije", traženje očiglednih ranjivosti i merenja ispunjavanja bezbednosnih ciljeva (ST).

- EAL 4: *EAL 3* + potpuna specifikacija interfejsa, projekat sistema na nižem nivou apstrakcije (sa više detalja), analiza skupa alternativnih rešenja za realizaciju projekta, primena neformalnog modela politika zaštite, nezavisna analiza ranjivosti i automatizacija upravljanja konfiguracijom. Najviši je nivo bezbednosne garancije koji je izvodljiv za modifikaciju postojećeg proizvoda. Proizvod na ovom nivou je metodički projektovan, testiran i revidiran i obezbeđuje korisniku najviši nivo zaštite na bazi *dobre komercijalne prakse* za razvoj softvera. Korišćenje ove prakse pomaže da se eliminišu uobičajeni problemi u dizajnu i razvoju softvera, koji mogu ugroziti projekat. Ovaj nivo uključuje i nezavisno traženje ranjivosti proizvoda. Vršiti se metodičko testiranje i proveru, a analizu treba podržati testiranjem tipa "*sive kutije*", selektivnom nezavisnom potvrdom rezultata testa projektanta i evidencijom o traženju očiglednih ranjivosti. Zahteva se kontrola razvojnog okruženja i upravljanje konfiguracijom TOE.
- EAL 5: *EAL 4* + primena formalnih modela politike zaštite, poluformalne specifikacije funkcionalnosti i revizije detaljnog projekta sa demonstracijom međusobnih odnosa objekata. Uključena je analiza zaštićenih kanala. Ovaj nivo se ne može lako dostići za komercijalni proizvod, pošto proizvod mora biti namenski projektovan i izrađen sa namerom da se dostigne ovaj nivo. Ovde projektanti moraju primeniti *dobru praksu* izrade komercijalnog softvera i specijalizovane tehnike **sistemskog inženjerstva u oblasti zaštite** (*SSE – Security System Engineering*). Ovaj nivo je pogodan za projektante i korisnike koji zahtevaju visok nivo bezbednosne garancije kroz rigorozni razvoj. Na ovom nivou projektant mora prezentovati specifikacije projekta i kako su funkcionalnosti implementirane u proizvod zaštite.
- EAL 6: *EAL 5* + strukturni model u kojem se mora predstaviti realizacija. Namenjen je za kontekste sa srazmerno visokim rizikom. Obuhvata poluformalnu verifikaciju projekta i testiranje komponenti. Zahteva struktuiranu prezentaciju implementacije. Model i detaljan dizajn proizvoda podvrgavaju se reviziji. Proizvod mora obezbediti visok stepen otpornosti na napad. Ovaj nivo potvrđuje da su u fazi projektovanja implementirani struktuirani procesi razvoja, kontrole razvoja i upravljanje konfiguracijom. Proizvod zaštite je poluformalno dizajniran i testiran. Analiza uključuje svu implementaciju. Bezbednosni nivo podržava modularni i slojeviti pristup dizajnu i prezentaciji strukture implementacije. Nezavisno ispitivanje ranjivosti testiranjem proizvoda na proboj mora osigurati visoku otpornost na napad. Mora se sistematično tražiti tajni kanal i dalje pojačati razvojno okruženje i upravljanje konfiguracijom.
- EAL 7: *EAL 6* + formalna verifikacija projekta *TOE*. Primenjuje se za kontekste sa velikim rizikom. Namenjen je samo za najviši nivo aplikacija zaštite gde visok rizik proboja zaštite opravdava razvoj i troškove zaštite. Ovaj nivo sadrži kompletnu nezavisnu i formalnu reviziju sa fazom verifikacije projekta i testiranjem na proboj. Projektant mora testirati svaku komponentu *TOE* radi otkrivanja očiglednih i neočiglednih ranjivosti, koje zatim kompletno verifikuje nezavisni kontrolor. Ovo je iscrpljujući proces. Formalni model se dopunjava formalnom prezentacijom specifikacije funkcionalnosti i stepena usaglašenosti projekta na niskom nivou apstrakcije. Zahteva se evidencija korisničkog testiranja tipa "*bele kutije*" i kompletne nezavisne potvrde rezultata testiranja projektanta (*developer*). Kompleksnost projekta mora biti minimizirana.

Prednosti i nedostaci CC standarda, [68]:

- podiže nivo i pouzdanost funkcija zaštite koje su implementirane u standardnim proizvodima zaštite - OS, bazama podataka, barijerama, ruterima IDS/IPS,
- značajan za glavne snabdevače proizvoda zaštite i sistema *smart* kartica i za IKT sisteme državnih organa, koji su izloženi visokom riziku, a manje je značajan za ostale kategorije korisnika,
- ne primenjuje objektno orijentisani pristup,
- zahtevi za funkcionalnosti nisu grupisani tako da se može primenjivati atribut nasleđivanja, a funkcionalne komponente nisu međusobno usaglašene,

- sa „bibliotečkim“, a ne objektnim pristupom sužava se krug fiksiranih znanja i usložnjava njihovo korektno korišćenje,
- ne obuhvataju zahteve za arhitekturu, što je posledica primene tradicionalnog modela pristupa „*odozdo na gore*“, što je ozbiljan nedostatak CC standarda,
- tehnologija zaštite nužno se treba podeliti na tehnologiju za zaštitu kritičnih funkcija, među koje spadaju i bezbednosne funkcije,
- bez razmatranja aspekata interfejsa, IKT sistemi ostaju neumreženi i izolovani, a istovremeno važan zadatak zaštite interfejsa mora se rešavati na isti način,
- nema širu primenu, iako je dosta fleksibilan, jer ima veoma kompleksan proces evaluacije i zahteva mnogo vremena,
- u svetu postoji ograničen broj akreditovanih tela sa razvijenim kapacitetima za evaluaciju po ovom standardu,
- usluge ovih tela su skupe i nefleksibilne za širu, transnacionalnu primenu i
- organizacije se pre odlučuju na neprekidno *poboljšavanje* procesa zaštite nego CC evaluaciju proizvoda zaštite.

2.3.2.4. *Standard za evaluaciju kriptografskih algoritama i modula*

Za evaluaciju kriptografskih algoritama i modula razvijen je i najviše se praktično koristi NIST standard **FIPS 140-2**, [74].

Standard FIPS 140-2 (1994-danas) za evaluaciju kriptografskih modula, tj., modula koji implementiraju kriptografske algoritme ili procese, razvile su NSA i NIST (SAD) i Agencija za zaštitu informacija Kanade. Namenjen je samo za evaluaciju kriptomodula, ali i softvera, izvršnih procesora i operativnih sistema koji uključuju kriptomodule. Standard uključuje 4 rastuća indikatora nivoa bezbednosti - **L1, L2, L3 i L4**, a obuhvata sledeće komponente: *osnovni dizajn (projekat), dokumentaciju, uloge, upravljanje kriptografskim ključem, testiranje, fizičku zaštitu od EM interferencija, ublažavanje drugih faktora rizika, tehničku specifikaciju, portove i interfejse, model konačnog broja stanja i druge elemente*.

Ključni kriterijumi zahteva za bezbednosne nivoe kriptomodula su:

Bezbednosni nivo L1:

- Kriptološki algoritam mora biti FIPS sertifikovani algoritam;
- Softverske i memorijske komponente mogu se izvršavati na IKT sistemu za opšte namene sa ne-evaluiranim operativnim sistemom;
- Nema fizičke zaštite veće od one koja se zahteva za objekte IKT sistema u standardnoj upotrebi.

Bezbednosni nivo L2:

- Veća fizička zaštita od regularne: kućište otporno na TEMPEST (*Transient Electro-Magnetic Pulse Surveillance Technology*) prisluškivanje na bazi snimanja kompromitovanog EM zračenja, ili u restriktivnom prostoru, zapečaćenom ili sa bravom otpornom na provalu, [66];
- Autentifikacija operatora za izvršavanje specifičnih servisa na bazi uloga;
- Softverske i memorijske komponente mogu se izvršavati na vešenamenskom sistemu, ali sa OS koji je evaluiran i zadovoljava najmanje EAL2 bezbednosni nivo CC evaluacije. Takođe, mora se koristiti jedan od specifikovanih profila zaštite CC kriterijuma.

Bezbednosni nivo L3:

- Povećana fizička zaštita: toliko da sprečava napadače da pristupe kritičnim bezbednosnim parametrima unutar modula;
- Autentifikacija na bazi identiteta operatera;
- Strogi zahtevi za čitanje i izmenu kritičnih bezbednosnih parametara;

- Softverske i memorijske komponente zahtevaju OS koji je evaluiran i zadovoljava EAL3 bezbednosni nivo CC evaluacije, poverljiv prenosni put i neformalan model politike zaštite. Može se koristiti i ekvivalentni, evaluirani poverljivi OS.

Bezbednosni nivo L4:

- „Zaštitna zona“ oko modula, koja detektuje i odgovara na sve neovlašćene pokušaje fizičkog pristupa, uključujući zaštitu od uticaja okruženja, ili fluktuacija napona i temperatura izvan dozvoljenog opsega modula;
- Softverske i memorijske komponente zahtevaju OS koji je evaluiran i zadovoljava zahteve za funkcionalnosti za bezbednosni nivo L3 i EAL4 bezbednosni nivo CC evaluacije. Može se koristiti i ekvivalentni, evaluirani poverljivi OS.

2.3.2.5. Komparativna analiza relevantnih standarda kvaliteta proizvoda i sistema zaštite

Komparativna analiza kompatibilnosti relevantnih standarda kvaliteta proizvoda i sistema zaštite: TCSEC, ITSEC CC i FIPS -140-2 indicira da su u praksi zaštite svi standardi, [116]:

- prilično nefleksibilni;
- imaju za cilj značajnu procenu nivoa bezbednosti;
- teški i zahtevni za korišćenje u kompleksnim sistemima;
- zahtevaju specifikaciju okruženja u kojem se koriste;
- zahtevaju poverljive i vrlo pažljivo birane administratore;
- korisni su samo ako je cilj **sertifikacija** proizvoda i sistema zaštite i
- imaju slične, ali ne identične *indikatore nivoa bezbednosti*.

U Tabeli 2.3.1 prikazan je odnos *indikatora nivoa bezbednosti* i njihova uporedivost u standardima TCSEC, ITSEC, CC i FIPS -140-2.

Tabela 2.3.1. *Uporedivost indikatora nivoa bezbednosti za evaluaciju u relevantnim standardima kvaliteta proizvoda i sistema zaštite*

TCSEC (1983-1990)	ITSEC	CC (1998-danas)	FIPS 140 (1994-danas)
D	E0	Neme ekvivalent	
Neme ekvivalent	Neme 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	

Tradicionalni industrijski standard za garanciju kvaliteta **ISO-9000/9001**, originalno namenjen za proizvodne organizacije, uz mnogo interpretacija može se primeniti za razvoj i proizvodnju sistemskih, aplikativnih, ili softvera zaštite, [38]. Dok se ISO 9000 sertifikat daje samo organizacijama i kompanijama, modeli sazrevanja procesa (CMMI i SSE-CMM) 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 sertifikat, mora implementirati sistem kvaliteta koji pokriva više oblasti nego što se zahteva u CC standardu za evaluaciju proizvoda i sistema zaštite. Ovaj dodatni napor za dobijanje ISO 9001 sertifikata u većini slučajeva može biti neopravdan.

2.3.3. Standard ISO/IEC 17799 za upravljanje zaštitom

Standardi u IKT zaštiti su brojni, [31], ali mnogi nisu šire prihvaćeni. Najšire prihvaćen standard za upravljanje zaštitom **ISO/IEC 17799** sadrži dva dela, [42], [52]:

1. standard prakse zaštite, za pomoć u implementaciji vlastitog sistema zaštite i
2. **BS 7799** - specifikaciju zahteva za izbor *kontrola zaštite*, koja pomaže organizaciji da definiše bezbednosne zahteve, [14].

ISO/IEC 17799 standard, u suštini predstavlja uputstvo za upravljanje i izbor kontrola zaštite sa instrukcijama **šta** treba raditi u praksi zaštite, ali ne daje odgovore **kako** to treba uraditi. Smatra se kao ISO 9000 za oblast bezbednosti i zaštite IKT sistema, ali nije toliko težak. Usvojili su ga EU, kao i Australija i Novi Zeland (AS/NZS/ ISO/IEC 17799:2000, sa kojim je zamenjen stari AS/NZS 4444, [4]). U većini razvijenih zemalja u svetu usvojeni su nacionalni ekvivalenti ovog standarda, izuzev Severne Amerike. Drugi deo BS 7799 standarda obuhvata implementaciju **upravljačkih, operativnih i tehničkih kontrola zaštite** koje mogu biti: politike, procedure, operativna praksa, organizaciona struktura, ili softversko-hardverske funkcije. Kontrole zaštite u standardu ISO/IEC 17799 definisane su u imperativu. Standard sugeriše **koje** kontrole zaštite treba uključiti u program zaštite, ali ne specificira **kako** ih treba razviti, implementirati i administrirati. Ovo *nije tehnički standard niti zavisi od specifične tehnologije*. Ne obezbeđuje nikakvu metriku za evaluaciju zaštite, ali je kompatibilan i poziva se na sistem bezbednosnih nivoa CC standarda (**EAL**), a može se kombinovati sa metrikom **SSE CMM** modela sazrevanja procesa zaštite u metodologiji vektora zaštite (**S-vektora**), [60].

Standard **ISO/IEC 17799 obavezuje** da se izbor kontrola zaštite vrši na osnovu: *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 neophodnih podataka za pravosudne i forenzičke potrebe, osim uputstva za dokumentaciju zaštite organizacije. Standard usmerava veliku pažnju na definisanje politike zaštite na nivou organizacije sa instrukcijom **šta** dokument treba da sadrži, ali ne nudi detalje **kako** se ta politika razvija. Osnovne karakteristike standarda date su u Tabeli 2.3.2, [68].

Tabela 2.3.2. Osnovne karakteristike standarda ISO/IEC 17799

Struktura	10 glavnih poglavlja, 36 bezbednosnih ciljeva, 127 glavnih kontrola zaštite, nekoliko hiljada uputstava i instrukcija
Poglavljja	Politika zaštite, Organizacija zaštite, Klasifikacija i kontrola objekata (IKT sistema) zaštite, Personalna zaštita, Fizička zaštita i zaštita okruženja, Operativno upravljanje, Kontrola pristupa, Razvoj sistema zaštite i održavanje, Upravljanje nastavljanim poslovanja, Usaglašenost.
Bezbednosni ciljevi (komponente zaštite)	Politika zaštite, Organizacija zaštite, Klasifikacija i kontrola objekata sistema (razmeštaj objekata infrastrukture, snabdevanje strujom, kabliranje, održavanje, izdvojeni objekti, odlaganje i ponovno korišćenje informacionih objekata), Personalna zaštita, Fizička zaštita i zaštita okruženja (bezbedna zona, zaštita opreme IKT sistema, opšta kontrola fizičkog pristupa), Operativno upravljanje, Kontrola pristupa, Razvoj sistema i održavanje, Upravljanje nastavljanim poslovanja, Usaglašenost.

ISO/IEC 17799 (2. Deo, preuzeti BS 7799) je i **katalog dobre prakse zaštite** koju *treba izvršiti* i specificira instrukcije za *sistem upravljanja zaštitom informacija (ISMS)*. Sa **ISMS** organizacija može monitorisati i kontrolisati zaštitu informacija u cilju smanjenja rizika na prihvatljivi nivo i obezbediti da sistem zaštite ispunjava sve normativne zahteve i zahteve organizacije. Zahtevi za **ISMS** obuhvataju sledeće celine: *Obim, Politiku zaštite, Analizu rizika, Izjavu o primenljivosti, Sistem upravljanja razvojem/održavanjem zaštite i Dokumentaciju zaštite*.

U Tabeli 2.3.3 dat je kratak zbirni pregled osnovnih karakteristika *metoda evaluacije* u relevantnim (najviše primenjivanim) standardima kvaliteta proizvoda i sistema zaštite i opšte prihvaćenog standarda ISO/IEC 17799 za upravljanje zaštitom, [38].

Tabela 2.3.3. Zbirni pregled metoda evaluacije u relevantnim standardima 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 procese, i sazrevanje procesa zaštite. Obezbeđuje metodologiju evaluacije (SSAM) nivoa zrelosti procesa i kapaciteta zaštite organizacije.
ISO 17799 (2000-danas)	Uspostavlja uputstvo i opšte principe za upravljanje sistemom IKT zaštite u organizaciji.
ISO/IEC 15408 (CC) (1996-2005)	Predstavlja opšti model za evaluaciju bezbednosnih ciljeva, selekciju i definisanje bezbednosnih zahteva i izradu specifičnih <i>profila zaštite</i> za proizvode i sisteme.

2.4. Modeli sazrevanja procesa zaštite

2.4.1. Uvod

Opšte je prihvaćen princip da se neka aktivnost može dobro upravljati samo ako se može meriti. Osnovu kvaliteta aktivnosti i procesa čini sistem merenja – metrika. Metrika zaštite IKT sistema zahteva dalji istraživački rad. Istraživanja su potvrdila da je merenje u IKT zaštiti važno, ali da se prednosti merenja mogu ostvariti samo kada se metrika primenjuje kao proces, uz korišćenje arhiviranih mernih podataka. Međutim, većina organizacija ne koriste metriku IKT zaštite kao proces, a još manji broj organizacija integriše proces metrike IKT zaštite u sistem kvaliteta i poslovne procese.

Posebnu grupu modela i standarda kvaliteta procesa zaštite čine **procesno orijentisana grupa modela** za merenje nivoa zrelosti i kapaciteta procesa zaštite, razvijena na bazi genričkog CMM (*Capability Maturity Model*) modela, Instituta SEI (*Software Engineering Institute*), *Carnegy Mellon* Univerziteta u SAD, kao što su: SE CMM (*System Engineering Capability Maturity Model*), SW CMM (*Capability Maturity Model for Software Development*), SSE CMM (*System Security Engineering Capability Maturity Model*), iCMM (*Integrated 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, [27], [28], [35], [36], [46], [51].

TCMM (*Trusted Capability Maturity Model*) model, specijalna varijanta CMM, za bezbednosnu procenu softvera u fazi razvoja, baziran na fundamentalnim principima i strukturama generičkog CMM, tipičan je predstavnik standarda za **procenu kvaliteta u odnosu na pretnje iz proizvodnog okruženja**. Poverljivi CMM (**TCMM**) razvijen je ranih 1990-ih kao *Metodologija poverljivog softvera - TSM* (*Trusted Software Methodology*). TSM definiše nivoe poverenja: *nizak* koji ističe otpornost na nenamerne ranjivosti i *visok*, koji dodaje procese za suprostavljanje malicioznim programerima u razvoju softverskih proizvoda. TSM je kasnije harminizovan sa CMM u **TCMM**, koji je orijentisan samo na razvojno okruženje i upravljačke i organizacione aktivnosti, a primenljiv samo za procese i sisteme. Svaki proces koji se odnosi na objekte evaluacije nije obuhvaćen ovim metodom. TCMM nije više u upotrebi.

Generički model CMM (*Capability Maturity Model*) razvijen je na inicijativu NSA (1993-95). CMM model više je usmeren na upravljačke i organizacione procese i aktivnosti. CMM je referentni model zrelih praksi i procesa u specifikovanim disciplinama, koji se koristi za procenu grupnih kapaciteta za izvršavanje te discipline. CMM modeli se razlikuju po, [51]: *disciplini*

(softver, zaštita, sistemi, akvizicija i.t.d); *strukturni* (kontinualna i fazna reprezentacija); *definisanju nivoa zrelosti* (put poboljšavanja procesa) i *definisanju nivoa kapaciteta* procesa (institucionalizacija procesa).

Generički CMM obezbeđuje referentni model zrelih praksi i procesa, pomaže da se identifikuju potencijalne oblasti procesa za poboljšavanje, obezbeđuje definicije na nivou cilja i ključne attribute za specifične procese, definiše karakteristike procesa, ali ne obezbeđuje operativno uputstvo. CMM model procesa obezbeđuje referentni skup **najboljih praksi** koje se mogu koristiti za evaluaciju i poboljšavanje procesa. Takođe, definiše karakteristike procesa i daje obično arhitekturu, ili strukturu procesa. Većina CMM modela procesa imaju dimenzije **nivoa kapaciteta** – CL (*Capability Level*) i/ili **nivoa zrelosti** – ML (*Maturity level*), koji se koriste za evaluaciju i poboljšavanje procesa.

Generički modeli sazrevanja procesa-CMM razvijeni su primarno da, [28]:

- kreiraju sistem merenja *organizacijskih procesa* za životni ciklus sistema, [33],
- identifikuju većinu *projektnih i upravljačkih* praksi i procesa i
- obuhvataju najbolje *inženjerske prakse* za razvoj i upravljanje procesima za proizvodnju softvera, razvoj programa zaštite, profila zaposlenih i organizacija.

Uobičajeno korišćeni tipovi CMM modela, njihove reprezentacije i oblasti primene (OP) sumarno su prikazani u Tabeli 2.4.1, [36].

Tabela 2.4.1. CMM modeli, reprezentacije i oblasti primene

CMM	Reprezentacija	Oblast primene
Sw CMM	Fazna	Razvoj softvera
SE CMM	Kontinualna	Sistemska inženjerstvo
Sw Acquisition CMM	Fazna	Akvizicija softvera
SSE CMM	Kontinualna	Inženjering zaštite
Personal Sw Process	Fazna	Razvoj sw za korisnike (pojdnice)
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
CMMI	Kontinualna/fazna	Razvoj, održavanje, akviziciju, servise

2.4.2. Razvoj i struktura generičkog modela sazrevanja procesa

Na bazi generičkog CMM modela, razvijeni su brojni modeli sazrevanja procesa. Kratak pregled objavljenih modela sazrevanja procesa zaštite sa glavnim karakteristikama prikazan je u Tabeli 2.4.2, [20], [77].

Tabela 2.4.2. Objavljeni modeli sazrevanja procesa zaštite

Model sazrevanja	Opis	Komentar
NIST CSEAT IT Security Maturity Model	Pet nivoa progresivnog sazrevanja: 1. Politika 2. Procedura 3. Implementacija 4. Testiranje 5. Integracija	Fokusiran prema nivoima dokumentacije
Citogrup's Information Security Evaluation Model (CITI-ISEM)	Pet nivoa progresivnog sazrevanja: 1. Uskladenost 2. Prepoznavanje 3. Integracija	Fokusiran prema svesti organizacije o potrebi Zaštite i usvajanju zaštite

Model sazrevanja	Opis	Komentar
	4. Opšta praksa 5. Kontinualno poboljšanje	
CobiT Maturity Model	Pet nivoa progresivnog sazrevanja: 1. Inicijalni/ <i>ad hoc</i> 2. Ponovljiv ali intuitivan 3. Definisan 4. Upravljan i meren 5. Optimizovan	Fokusiran na kontrolu (<i>auditing</i>) specifičnih procedura
P-CMM (Personal Capability Maturity Model)	Pet nivoa progresivnog sazrevanja: 1. Inicijalni 2. Ponovljiv 3. Definisan 4. Upravljan 5. Optimizovan	Fokusiran na sazrevanje kompetencija ljudskih resursa
SSE CMM model i metod	Pet nivoa progresivnog sazrevanja: 1. Neformalno izvršavan 2. Planiran i praćen 3. Dobro definisan 4. Kvantitativno kontrolisan 5. Kontinualno poboljšavan	Fokusiran na SSE procese i dizajn softverskih proizvoda zaštite
CERT/CSO Security Capability Assessment	Pet nivoa progresivnog sazrevanja: 1. Postojeći 2. Ponovljiv 3. Namenjen (određenom licu) 4. Dokumentovan 5. Revidiran i ažuriran Merenja koriste četiri nivoa: 1. Inicijalni 2. Razvojni 3. Uspostavljen 4. Upravljan	Fokusiran na merenja kvaliteta u odnosu na nivoe dokumentovanja

Iz generičkog CMM modela za primenu u oblasti zaštite IKT sistema, izdvojila su se tri relevantna specifična modela:

1. Model sazrevanja procesa u oblasti sistemskog inženjerstva zaštite IKT sistema - **SSE-CMM**, specifično razvijen za razvoj i poboljšavanje procesa zaštite;
2. Integracioni CMM - **CMMI®** i
3. Integrirani CMM – **iCMM**.

Od navedenih modela sazrevanja procesa zaštite, **SSE-CMM** model i metod, razvijen po zahtevu NSA (*Nacionalne bezbednosne agencije SAD*) i DoD (*Ministarstva odbrane SAD*) isključivo za oblast zaštite sa, čak, 11 specifičnih sistem-inženjerskih oblasti procesa za zaštitu IKT sistema, objektivno zaslužuje najveću pažnju.

2.4.3. Model i metod sazrevanja procesa zaštite

Dinamika razvoja *Modela i metoda sazrevanja procesa zaštite* - SSE CMM ilustrovana je u Tabeli 2.4.3, [20].

Tabela 2.4.3. Razvoj SSE CMM modela

Godina objavljivanja	Naziv model
1993	NSA inicirala razvoj CMM za inženjering zaštite
1995	SEI radna grupa CMU razvila SSE CMM
1996	Objavljena SSE CMM v.1.0
1996-98	Pilot projekti SSE CMM u 7 organizacija u SAD

Godina objavljivanja	Naziv model
1999	Objavljena SSE CMM v.2.0 i SSAM (<i>Security System Appraisal Method</i>) metod v.2.0
2002	SSE CMM potvrđen kao standard ISO/IEC 21827
2003	Objavljena SSE CMM v.3.0
2004-05	ISSEA (<i>International Systems Security Engineering Association</i>) podnela zahtev za akreditaciju tela za SSE CMM sertifikaciju lica - <i>ISO/IEC 21827 Apraiser Certification Body for Persons</i>
2004	Usaglašavanje SSE CMM i CMMI v.1.1
2004	Usaglašavanje SSE CMM Apraisal (SSAM) sa CMMI SCAMPI Appraisal – proces u toku
2007	Usaglašavanje SSE CMM i CMMI v.1.2.- proces u toku

Model progresivnog sazrevanja kapaciteta zaštite (SSE-CMM), procesno je orijentisana metodologija za razvoj bezbednog IKT sistema na bazi *organizacijskih* i *upravljačkih* praksi i procesa, u celini preuzetih iz modela SE CMM i originalno razvijenih *sistem-inženjerskih* procesa zaštite (SSE). Model je u SEI institutu razvijen sa ciljem unapređivanja inženjerstva zaštite u definisanu, zrelu i merljivu discipline. **ISSEA**-Međunarodna asocijacija za sistemsko inženjerstvo u oblasti zaštite dalje unapređuje SSE CMM kroz razvoj teorije i prakse, tako da SSE CMM v. 2.0 postaje standard **ISO/IEC 21827**, 2002. godine. Poslednja SSE CMM v. 3.0, objavljena juna 2003, [102], primenjena je kao referentni model za evaluaciju tekućih procesa preduzeća ESS na tri projekta u istraživačkom delu ovog rada.

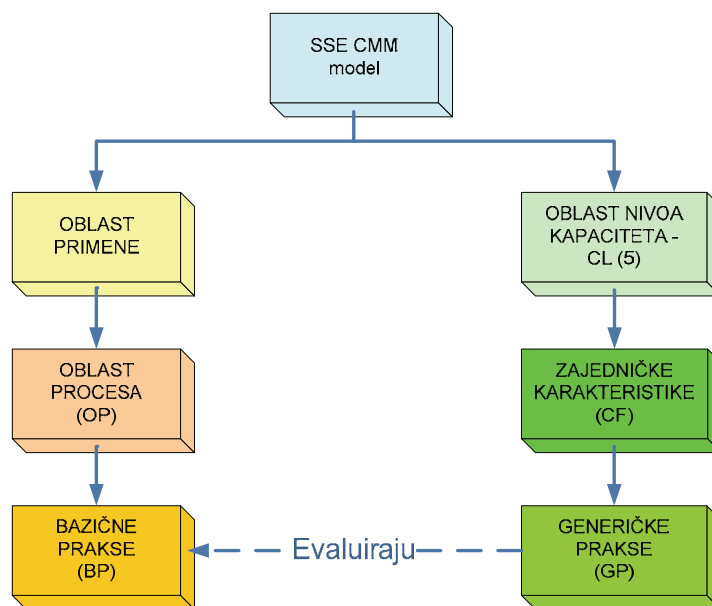
SSE CMM model i standard sadrži dva modula:

1. **SSE CMM v.3.0-model i metod** sazrevanja procesa zaštite i
2. **SSAM v.2.0-metod** evaluacije nivoa kapaciteta i zrelosti procesa, koji koristi **SSE CMM** metodologiju evaluacije kao referentni model, [102].

2.4.3.1. Struktura i opis SSE CMM modela

Struktura SSE-CMM modela organizovana je u dve *dimenzije* (Sl. 2.4.1), [68], [102]:

3. **Dimenzija primene**, koja obuhvata oblast procesa-**OP**: inženjerskih (SSE), upravljačkih (projektnih) i organizacionih i
4. **Dimenzija nivoa kapaciteta** - **CL** (Capability Level) u kontinualnoj reprezentaciji, ili nivoa zrelosti procesa – **ML** (Maturity Level) u faznoj (stepenastoj) reprezentaciji.



Sl. 2.4.1. Struktura SSE CMM modela sazrevanja procesa zaštite

Generalno, oblast procesa definiše **šta** treba da se postigne sa inženjerskim (SSE), projektnim i organizacionim procesima zaštite, a nivoi kapaciteta/zrelosti vrše kategorizaciju **nivoa kvaliteta** postizanja tih ciljeva, odnosno **kako** se dobro ti procesi izvršavaju.

SSE CMM model ima dve reprezentacije *puteva sazrevanja*, ili *poboljšavanja* procesa. „**Reprezentacija**“ CMM modela predstavlja način organizacije, primene i prezentacije komponenti modela i puta sazrevanja procesa, a može biti *kontinualna* i *fazna*. **Kontinualna reprezentacija CMM** odnosi se na progresivno, inkrementalno, ili inovativno, kontinualno poboljšavanje procesa individualnih OP od 0. do 5. *nivoa kapaciteta (CL)*. **Fazna reprezentacija CMM** modela odnosi se na fazno poboljšavanje više, ili svih OP organizacije od 1. do 5. *nivoa zrelosti (ML)* procesa (Tabela 2.4.4).

Tabela 2.4.4. Nivoi kapaciteta-CL i zrelosti-ML procesa SSE CMM modela

Nivo CL/ML	Kontinualna reprezentacija - CL -	Fazna reprezentacija - ML -
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

Dimenzija primene obuhvata tri *kategorije* oblasti procesa (OP), koje su na slici Sl. 2.4.2 prikazane prema nivou uticaja na sazrevanje procesa organizacije:

- *inženjerske ili SSE*: za inženjering i inženjersku analizu procesa, sa najvećim doprinosom za poslove i misiju organizacije,
- *upravljačke*: projektne, za projektovanje, upravljanje projektima i koordinaciju rada na projektu, sa srednjim doprinosom za poslove organizacije i
- *organizacione*: za organizaciju ljudi i procesa koje ti ljudi izvršavaju u projektu, sa najnižim, ali fundamentalnim doprinosom za poslove i misiju organizacije.



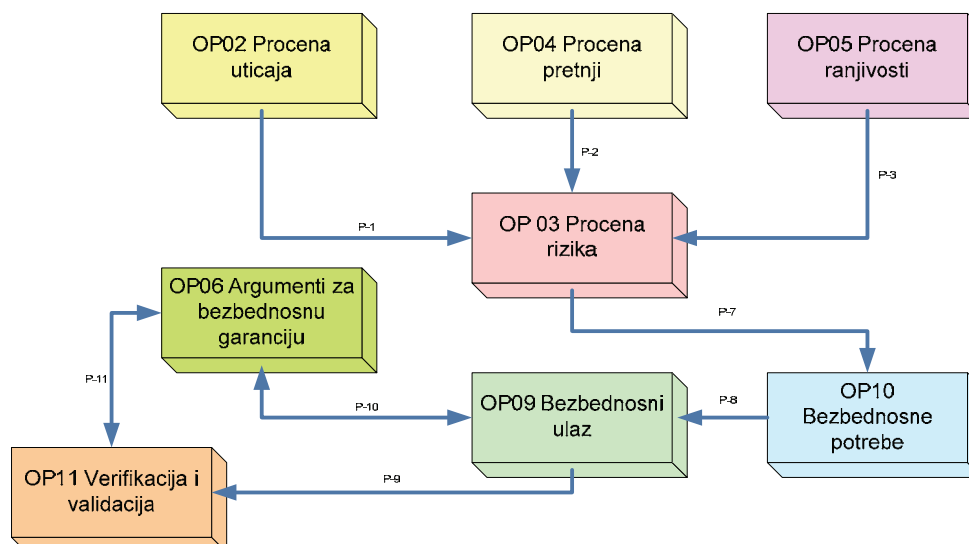
Sl. 2.4.2. SSE CMM kategorije procesa

Model sadrži ukupno 22 OP: **11** originalnih **inženjerskih** (SSE), **5 upravljačkih** (projektnih) i **6 organizacionih** OP. Upravljačke i organizacione OP su u celini nasleđene iz SE-CMM. **Kategorije OP SSE CMM** prikazane su zbirno u Tabeli 2.4.5, [68].

Tabela 2.4.5. 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 snadbevačima
OP07 – Koordinacija sistema zaštite		
OP08 – Nadzor i kontrola sistema zaptite		
OP09 – Obezbeđivanje bezbednosnog nalaza		
OP10 – Specifikacija bezbednosnih potreba		
OP11 – Verifikacija i validacija proizvoda sistema zaštite		

Oblasti procesa (OP) iz sve tri kategorije u suštini su slične. Drugim rečima, sve tri kategorije **OP** u **SSE CMM** modelu treba razmatrati integralno, jer se samo takvim pristupom obezbeđuje progresivno poboljšavanje ukupnih kapaciteta za razvoj programa zaštite. **SSE CMM** obezbeđuje OP za kompletno pokrivanje životnog ciklusa sistema zaštite, odnosno, iste bazične aktivnosti SSE OP primenljive su u svim fazama upotrebe OP. Treba zapaziti da SSE CMM model ne **propisuje** specifične procese, ili aktivnosti, nego **daje opšti model** za formiranje i grupisanje procesa i aktivnosti **najbolje prakse zaštite**. U SSE CMM modelu OP koje se odnose na zaštitu međusobno su zavisne, kao što je prikazano na slici Sl. 2.4.3, [77].



Sl. 2.4.3. Međusobni odnosi bezbednosno orijentisanih OP

Ostale međuzavisnosti OP, kao i OP i GP SSE CMM modela date su u Tabeli 2.4.6. 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 međuzavisnosti može pomoći da se efektivno implementiraju GP. Takođe, neka OP sadrži više BP, koje kada su implementirane mogu, takođe, potpuno implementirati GP, ili generisati proizvod rada koji se koristi za implementaciju GP.

Tabela 2.4.6. Međuzavisnosti OP i GP SSE CMM modela procesa

OP	Zavisi od OP	Zavisi od GP, BP
OP01 – Administracija kontrola zaštite		
OP02 – Procena uticaja	OP03, OP04, OP05, OP09, OP10, OP11	
OP03 – Procena bezbednosnog rizika	OP02, OP04, OP05, OP06, OP09, OP10, BP.04.05, BP.05.03, BP.02.05	
OP04 – Procena pretnji	OP03, OP02, OP05, BP.08.02,	
OP05 – Procena ranjivosti	OP03, OP09, OP10, BP.08.02,	
OP06 – Izgradnja argumenata za bezbednosnu garanciju	OP07	GP 3.3.3
OP07 – Koordinacija zaštite		GP 3.3.1, GP 3.3.2, GP 3.3.3
OP08 – Monitorisanje bezbednosnog stanja	OP03, OP05	
OP09 – Obezbeđivanje bezbednosnog ulaza	OP10	GP 3.3.2
OP10 – Specifikacija bezbednosnih potreba	OP09, OP06, OP07	GP 2.3.2, GP 3.3.3,
OP11 – Verifikacija i validacija zaštite	OP06, OP07, OP15	GP 2.3.2
OP12 – Osiguranje kvaliteta	OP11, OP15	GP 2.3.1
OP13 – Upravljanje konfiguracijom	OP01, OP06, OP10	GP 2.2.2, GP 2.4.1
OP14 – Upravljanje rizikom projekta	OP07, OP15, OP16	
OP15 – Monitorisanje i kontrola tehničkih aktivnosti	OP01, OP08, OP07, OP16	GP 2.4.2

OP	Zavisi od OP	Zavisi od GP, BP
OP16 – Planiranje tehničkih aktivnosti	OP07	GP 2.1.1, GP.2.1.2, GP 2.1.6
OP17 –Definisanje SSE procesa organizacije	OP07	GP 2.1.3, GP 3.1.1, GP 3.1.2
OP18 – Poboljšavanje SSE procesa organizacije	OP17, OP09	GP 2.1.3, GP 5.1.2
OP19 – Upravljanje razvojem proizvodne linije	OP06	GP 5.2.3, GP 5.2.4
OP20 – Upravljanje okruženjem za podršku SSE procesa	OP03, OP06, OP09	GP 2.1.4
OP21 – Obezbeđivanje tekućih znanja i veština	OP09	GP 2.1.5
OP22 – Upravljanje bezbednosnim aspektom sporazuma sa snabdevačima	OP10	

Oblasti procesa (**OP**) u **SSE CMM** modelu opisane su 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 faktički obezbedi zaštitu sistema u operativnom stanju.

Cilj: Kontrole zaštite su propisno primenjene i konfigurisane.

Bazične prakse (BP)

- 1.1.1. Uspostavi kontrolisane odgovornosti za kontrole zaštite i upoznaj sve zaposlene u organizaciji.
- 1.1.2. Upravlja konfiguracijom sistema kontrola zaštite.
- 1.1.3. Upravlja programom za razvoj svesti o potrebi zaštite, obuke i edukacije za sve korisnike i administratore.
- 1.1.4. Upravlja periodičnim održavanjem i administracijom servisa zaštite i kontrolnih mehanizama.

Detaljan, integralni opis OP i BP SSE CMM modela dat je u literaturi, [102]. Skraćeni opis OP i pripadajućih BP SSE CMM v.3.0 modela dat je u **Prilogu 2.4A**.

Bazične prakse - BP (Basic Practices), čije se izvršavanje **obavezno zahteva** za postizanje bezbednosnih ciljeva neke **OP**, čine skup odnosnih, kolektivno izvršavanih osnovnih aktivnosti oblasti procesa. Pri tome nije toliko važno kakvog su kvaliteta **BP**, nego da su samo implementirane da bi se postigla namena **OP** koju **BP** podržavaju. Smatra se da svaka od identifikovanih **BP** doprinosi efektivnom izvršavanju **OP** i zbog toga se **BP** unutar specifične **OP** mora izvršiti. **OP** sakuplja relevantne aktivnosti zaštite u celine koje se mogu implementirati kao odvojeni proces, a u skladu sa zahtevom modela. Model sadrži ukupno 129 BP, od kojih je 61 organizovano u 11 SSE OP, a preostale BP odnose se na projektne i organizacione OP (Tabela 2.4.7), [68].

Tabela 2.4.7. Broj BP po OP u SSE CMM modelu

SSE OP	Broj BP	Projektne i organizacione OP	Broj BP
OP01 – Administracija kontrola zaštite	4	OP12 – Osiguranje sistema kvaliteta	8

SSE OP	Broj BP	Projektne i organizacione OP	Broj BP
OP02 – Procena uticaja	6	OP13 – Upravljanje konfiguracijom	5
OP03 – Procena bezbednosnog rizika	6	OP14 – Upravljanje rizikom	6
OP04 – Procena pretnji	6	OP15 – Monitorisanje tehničkih aktivnosti	6
OP05 – Procena ranjivosti sistema	5	OP16 – Plan tehničkih aktivnosti za razvoja sistema zaštite	10
OP06 – Izgradnja bezbednosne garancije (security assurance)	5	OA17 – Definisanje SE procesa organizacije	4
OP07 – Koordinacija sistema zaštite	4	OA18 – Poboljšavanje SE procesa organizacije	4
OP08 – Nadzor i kontrola sistema zaštite	7	OA19 – Upravljanje razvojnom linijom proizvoda zaštite	5
OP09 – Obezbeđivanje bezbednosnog ulaza	6	OA20 – Upravljanje okruženjem za podršku SE	7
OP10 – Specifikacija bezbednosnih potreba	7	OP21 – Obezbeđenje potrebnih znanja i sposobnosti kadrova	8
OP11 – Verifikacija i validacija proizvoda/sistema zaštite	5	OA22 – Koordinacija bezbednosnih aspekata sa snabdevačem	5
Ukupno BP=129	61		68

Bazična praksa mora se izvršiti u implementiranom procesu (**OP**). Primenjuje su u celokupnom životnom ciklusu sistema i uglavnom se ne preklapa sa drugim **BP**. Generalno, **BP** predstavlja **najbolju praksu zaštite** koju preporučuje međunarodna interesna zajednica u oblasti zaštite. **BP** ne specificira neki poseban metod ili alat, već je preporučena organizacija za izvršavanje aktivnosti u **OP**. Lista **BP** prikazuje se u **opisu OP** u modelu na standardizovan način, sa: *rednim brojem, nazivom, opisom, tipičnim rezultatima (primerom proizvoda rada) i napomenom* kao u sledećem **primeru**:

OP19 - Upravljanje razvojnom linijom proizvoda zaštite:

BP.19.01 Definiši razvoj proizvoda

BP.19.02 Identifikuj tehnologiju novog proizvoda, ili pomoćne strukture koja će omogućiti organizaciji nabavku, razvoj i primenu tehnologije za konkurentnu prednost.

BP.19.03 Napravi neophodne promene u ciklusu razvoja proizvoda 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.

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 raspoloživih tehnologija.

Primer proizvoda rada:

- definicija linije proizvoda zaštite

Napomena:

Definisana linije proizvoda zaštite omogućava efektivniju iskoristivost (ponovno korišćenje) objekata i veći potencijalni povratak investicija.

BP.19.02

Dimenzija kapaciteta (Capability Side) obuhvata tri kategorije atributa procesa:

- generičke prakse (**Generic Practices**)-**GPs**,
- opšte karakteristike (**Common Features**)-**CFs** i
- nivo kapaciteta procesa (**Capability Levels**)-**CLs**

Dok je oblast primene lako razumljiva i intuitivno prihvatljiva, teže je razumeti dimenziju kapaciteta SSE CMM modela, koja definiše **kvalitet izvršavanja OP**. Za lakše shvatanje ove dimenzije modela, potrebno je definisati ključne termine iz standarda **ISO/IEC 21827**, [67]:

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.

Dimenzija kapaciteta SSE CMM modela sadrži ukupno 30 **GP**, koje se izvršavaju kroz izvršavanje BP i **evaluiraju kvalitet** njihovog izvršavanja. GP se grupišu u ukupno 12 **CF**, raspoređenih na 5 **nivoa zrelosti kapaciteta-CL**.

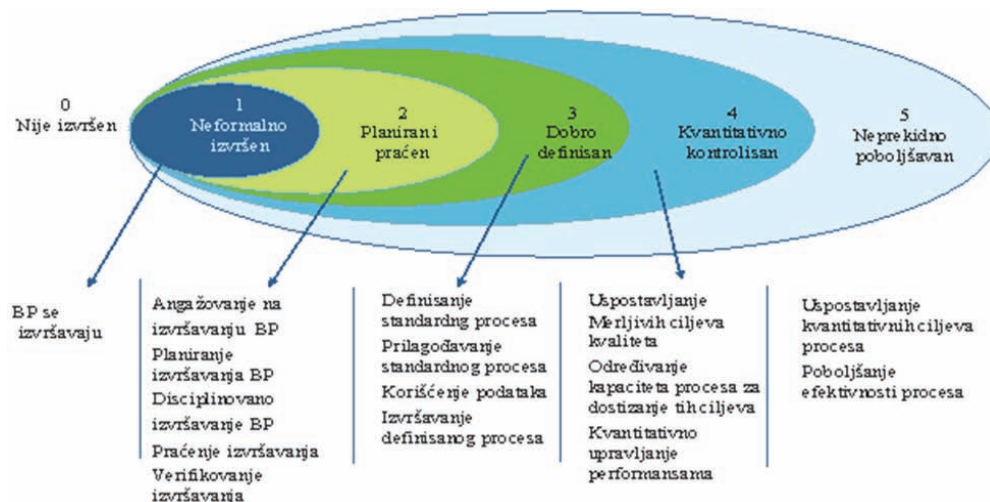
Generičke prakse (GP) predstavljaju izvorne, opšte radnje čije se izvršavanje zahteva u svim procesima (**OP**) u domenu i direktno određuju kapacitete organizacije za izvršavanje procesa, odnosno **kvalitet izvršavanja BP procesa (OP)**. U modelu, **GP** su poredane po **CF** prema svojoj zrelosti, koja raste sa stepenom uvođenja metrike modela. **GP** sa većom zrelosti ukazuje na viši nivo kapaciteta procesa. **GP** moraju biti izvršene u nekoj **OP**, kao deo izvršavanja **BP**, da bi se odgovarajuća **OP** pripisala nekom nivou zrelosti kapaciteta - **CL**. Step implementacije **GP** koristi se za **evaluaciju (appraisal)** i progresivno poboljšavanje procesa. **GP** se grupišu prema opštim karakteristikama u **CF** koje su raspoređene po nivoima kapaciteta (**CL**) od 1. do 5., od kojih svaki **CL** sadrži nekoliko **CF**. **GP** su aktivnosti koje određuju nivo implementacije i institucionalizacije **BP** i koje poboljšavaju kapacitet za izvršavanje svakog procesa u konkretnoj kategoriji **OP**, [68], [102].

Opšte karakteristike-(CF) su svi opšti aspekti procesa, grupisani u logičke oblasti - nivo kapaciteta. **CF** sadrže jednu ili više **GP**. **CF** su sredstvo za kategorizaciju **GP**. Kategorije **CF** su vrlo slične kroz sve **OP**. **CF** se nazivaju **institucionalizacije** zato što osiguravaju da su **OP** efektivne, ponovljive i stabilne i da obezbeđuju potrebnu infrastrukturnu podršku. **CF** su organizovane na 5 (6) aktivnih **nivoa kapaciteta - CL** (1.-5.), s tim da se **0** nivo izostavlja, ili se proces ne izvršava, zavisno od **reprezentacije** komponenti modela. U Tabeli 2.4.8. prikazana je distribucija **CF** po nivoima kapaciteta - **CL**.

Tabela 2.4.8. Zajedničke karakteristike (CF) po nivoima kapaciteta (CL)

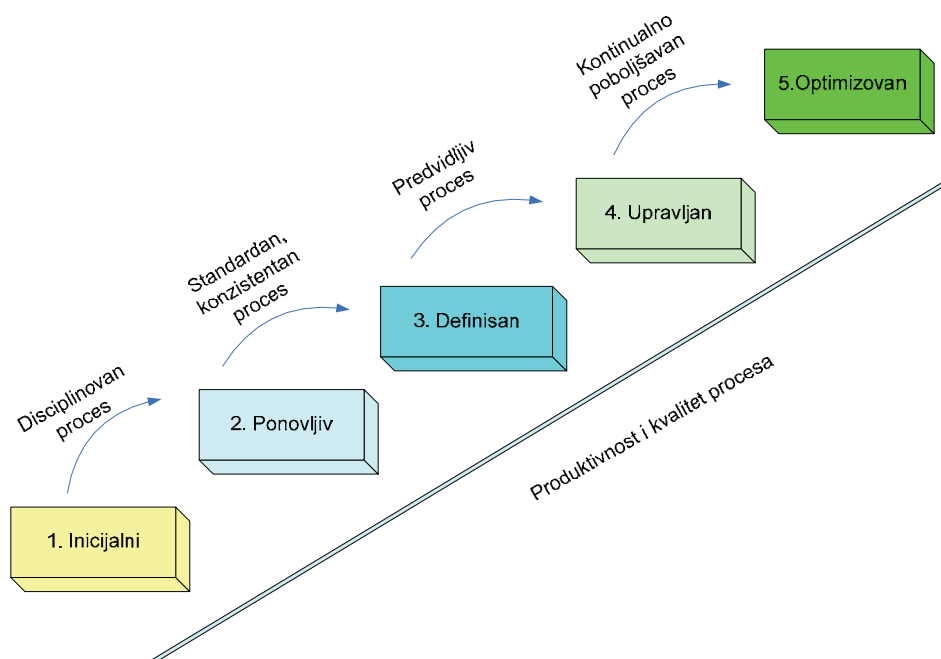
Nivo kapaciteta (CL)	Zajedničke karakteristike (CF)
1.	1.1. BP su izvršene
2.	2.1. Planiranje performansi 2.2. Disciplinovanje aktivnosti 2.3. Verifikacija aktivnosti 2.4. Praćenje aktivnosti
3.	3.1. Definisane standardnog procesa 3.2. Izvršavanje definisanog procesa 3.3. Koordinacija procesa
4.	4.1. Uspostavljanje merljivih ciljeva kvaliteta 4.2. Objektivno upravljanje aktivnostima
5.	5.1. Poboljšanje organizacionih kapaciteta 5.2. Poboljšanje efektivnosti procesa

Grafički model CL sa pripadajućim CF u *kontinualnoj* prezentaciji prikazan je na Sl. 2.4.4, na kojoj je ilustrovan pogresivni rast kapaciteta procesa, [67].



Sl. 2.4.4. Nivoi kapaciteta procesa zaštite u kontinualnoj prezentaciji

Put sazrevanja procesa sa glavnim atributima *ML* u faznoj reprezentaciji SSE CMM modela ilustrovan je na slici Sl.2.4.5.



Sl. 2.4.5. Sazrevanje procesa po ML SSE CMM modela

Detaljniji opis CF, distribuiranih po nivoima kapaciteta (osim 0.) u SSE-CMM modelu i kontinualnoj reprezentaciji prikazan je u Tabeli 2.4.9, [68].

Tabela 2.4.9. Raspored CF po CL SSE CMM modela

CL	CF po nivoima kapaciteta
1	Izvršavan neformalno: CF 1: BP su izvršene –pažnja se usmerava na to da li su organizacije izvršile neki proces zaštite koji uključuje bazične prakse (BP). Ova CF predstavlja postojanje politika zaštite, sistemski specifičnih praksi upravljanja i standarda zaštite.

Primer opisa GP, CF i CL u SSE CMM modelu:

CL1- Izvršen neformalno:

Kratak opis: BP ove OP generalno se izvršavaju. Izvršavanje ovih BP ne mora biti rigorozno planirano i praćeno. Izvršavanje BP zavisi od individualnih znanja, veština i napora. Proizvodi rada OP ispituju se na izvršavanje 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 neki proizvod rada procesa koji se može identifikovati.

Lista CF. Ovaj nivo kapaciteta sadrži sledeće CF:

- **CF 1.1 – BP su izvršene**

CF 1.1 – BPs su izvršene

Kratak opis: GPs ove CF ukazuju jednostavno da se BP ove OP izvršavaju na neki način. Međutim, velika je verovatnoća da konzistentnost, ili izvršavanje i kvalitet proizvedenog rezultata rada ovog procesa mnogo varira, zbog nedostatka implementiranih kontrola.

Lista GP. CF se sastoji od sledećih GPs:

- **GP 1.1.1 – Izvrši proces**

GP 1.1.1 – Izvrši proces

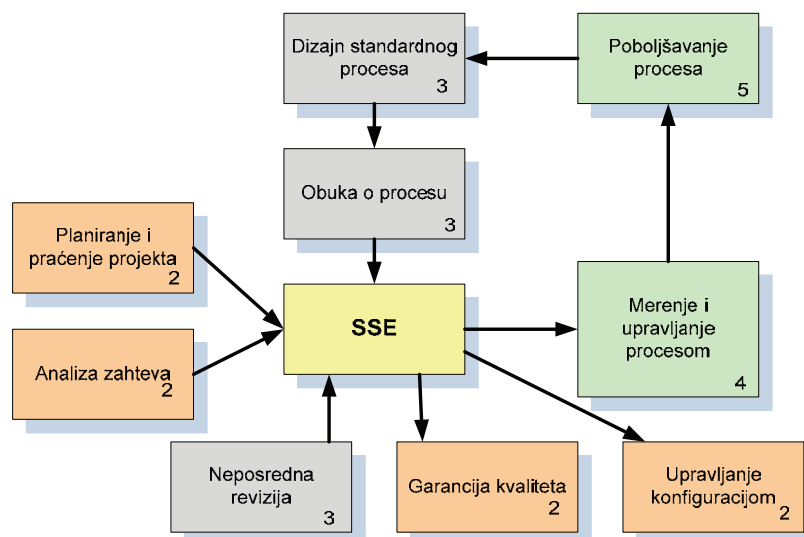
Opis: Izvrši proces koji implementira BP OP tako da obezbedi proizvod rada i/ili servis za klijenta.

Napomena: Proces može biti »neformalni«, a klijent(i) OP mogu biti interni i eksterni za organizaciju.

Skraćeni pregled komponenti oblasti kapaciteta SSE CMM v.3.0 modela dat je u **Prilogu 2.4B**.

Organizacija koja primenjuje SSE CMM model može dostići različite nivoe zrelosti u različitim OP sa dinamikom i resursima koji su na raspolaganju. Model ne zahteva da organizacija dostigne uniformni nivo zrelosti svih OP na jednom nivou da bi se nivo zrelosti nekih OP pomerio na viši nivo, što dopušta organizaciji da se fokusira na one OP koje su relevantne za specifične oblasti poslovanja.

Model obezbeđuje porast sofistikacije izvršavanja i broja izvršavanih GP koje indiciraju dostizanje nivoa zrelosti. Na slici Sl. 2.4.7 prikazano je da organizacija koja dostigne SSE CMM nivo kapaciteta/zrelosti 2. prati i planira projekat, analizira zahteve, obezbeđuje garanciju kvaliteta i upravlja konfiguracijom. Međutim, u skladu sa kriterijumima za SSE CMM nivoe zrelosti, takva organizacija još uvek formalno ne opisuje i ne dizajnira standardni proces, ne izvršava obuku o procesu, merenja i upravljanje procesom. Takođe, organizacija koja dostigne nivo 3. ne meri niti poboljšava procese, [62].



Sl. 2.4.7. Implementacija SSE CMM nivoa zrelosti SSE procesa

Sa porastom nivoa sazrevanja procesa, veliki broj GP se formalizuje, dokumentuje i standardizuje u celoj organizaciji. Na primer, planiranje i praćenje projekta postoji u nekoj formi na nivou 1. i 2., ali na nivou 3. počinje korišćenje procesa organizacije i alata za upravljanje projektima. Na nivou 2., garancija kvaliteta uključuje neformalnu reviziju, dok se na nivou 3. zahteva da je revizija formalizovana i koordinirana sa drugim funkcijama za razvoj i održavanje sistema.

2.4.3.2. Prednosti i nedostaci SSE CMM modela

Glavna prednost primene SSE CMM modela u oblasti zaštite je dobra metrika sazrevanja procesa zaštite. **Glavni principi sazrevanja** procesa i kapaciteta SSE CMM V. 3.0 modela izvedeni su iz opštih, logičkih principa upravljanja projektom (Tabeli 2.4.10).

Tabela 2.4.10. Principi sazrevanja procesa zaštite u SSE CMM modelu

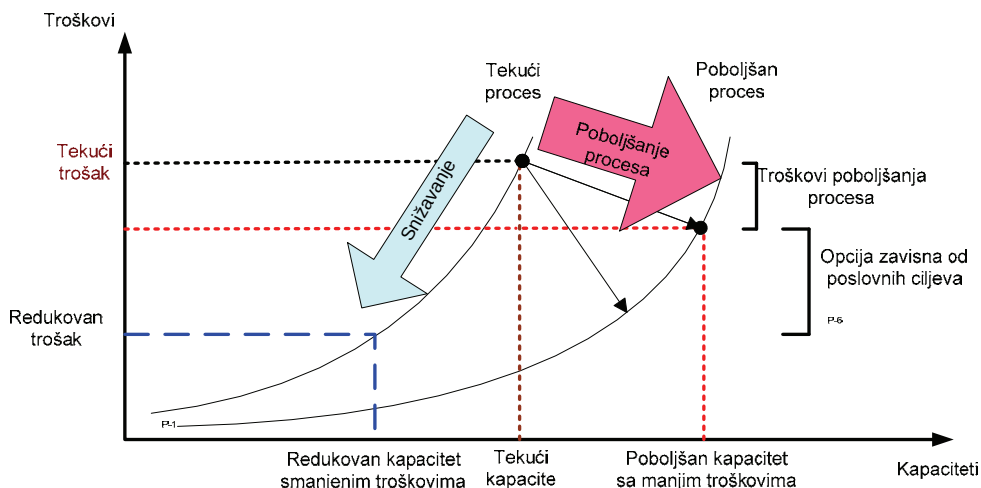
Opšti principi	Principi sazrevanja procesa u SSE CMM modelu
1. Prvo morate nešto uraditi da bi njime upravljali	1. Nivo <i>neformalnog izvršavanja procesa</i> fokusiran je na to da li se uopšte izvršava proces koji sadrži bazične prakse
2. Razumeti šta se događa na projektu (gde su proizvodi-rezultati) pre definisanja procesa u celoj organizaciji	2. Nivo <i>planiran i praćen</i> fokusiran je na definisanje nivoa projekta, planiranje i izvršavanje
3. Koristiti sve najbolje što ste naučili na projektu	3. Nivo <i>dobro definisan</i> fokusiran je na disciplinovano izvršavanje i formiranje standardnih procesa na nivou organizacije od definisanih procesa
4. Ne možete nešto meriti dok ne znate šta je to	4. <i>Metrika</i> . Iako je bitno početi skupljanje i korišćenje osnovnih mernih podataka na projektu što ranije (već na 1. nivou) merenje i korišćenje mernih podataka u celoj organizaciji ne očekuje se sve dok se ne dostigne dobro definisan (3.), a posebno kvantitativno kontrolisan nivo
5. Upravljanje mernim sistemom ima smisla samo kada merite prave stvari	5. Nivo <i>kvantitativno kontrolisan</i> fokusiran je na povezivanje merenja u poslovnim ciljevima organizacije
6. Kultura neprekidnog poboljšavanja zahteva formiranje dobre prakse upravljanja, definisane procese i merljive ciljeve	6. Nivo <i>neprekidnog poboljšavanja</i> dobija podršku od svih inkrementalnih praksi upravljanja na prethodnim nivoima, zatim se pojačava pomakom u razvoju kulture rada koja odražava postignute rezultate

Generalno SSE CMM model i metod može se koristiti za, [83]:

1. **merenje i poboljšavanje zrelosti procesa** zaštite i kapaciteta organizacije za razvoj programa i sistema zaštite,

2. **evaluaciju i profilisanje nivoa zrelosti procesa i kapaciteta zaštite** organizacija u oblasti zaštite i kompetencija zaposlenih, prema generalno prihvaćenim SSE principima, SSE CMM metodologiji i SSAM metodu evaluacije i
3. **obezbeđivanje bezbednosne garancije** (eng. *assurance*) merenjem zrelosti procesa zaštite i usaglašenosti upravljačkih, operativnih i tehničkih kontrola zaštite, čime se povećava poverenje u proizvode/sisteme/servise zaštite.

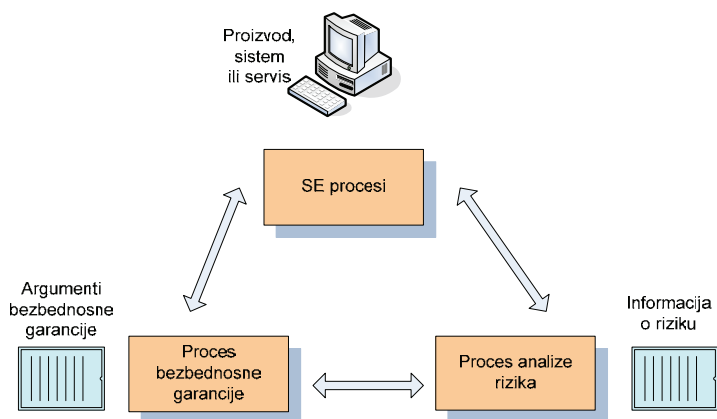
Prednosti izbora i primene SSE CMM modela za poboljšavanje procesa zaštite, grafički su prikazani na dijagramu u slici Sl. 2.4.8, [60].



Sl. 2.4.8. Dijagram rasta CL procesa u funkciji porasta troškova
(Izvor: Merie Whatley, Texas Instruments. Inc.)

Na dijagramu krive zavisnosti *kapaciteti-troškovi* ilustrovan je proces poboljšavanja kapaciteta zaštite uz smanjenje troškova, u odnosu na tekuće kapacitete i troškove. Poboljšavanje procesa inherentno smanjuje troškove, pa se kriva spušta prema osi zavisne varijable (*kapaciteta*), čime se ukupni troškovi smanjuju, uključujući i troškove samog poboljšavanja procesa. Nivo troškova uvek zavisi od poslovnih ciljeva organizacije.

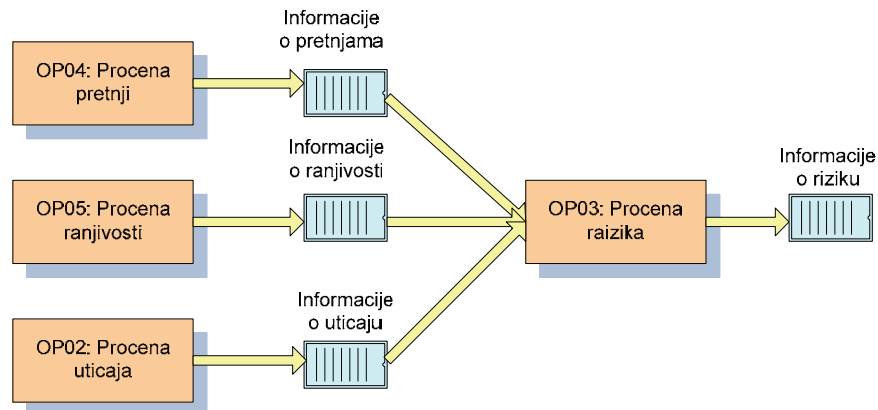
SSE CMM OP mogu se upotrebljavati u različitim procesima primene modela, u kojima učestvuju različite kombinacije OP. Primena SSE CMM OP u **integriranim procesima** sistemskog inženjerstva (SE), analizi rizika i bezbednosne garancije ilustrovana je na slici Sl. 2.4.9., [60]



Sl. 2.4.9. Primena SE CMM OP u integriranim procesima SE za analizu rizika i bezbednosnu garanciju

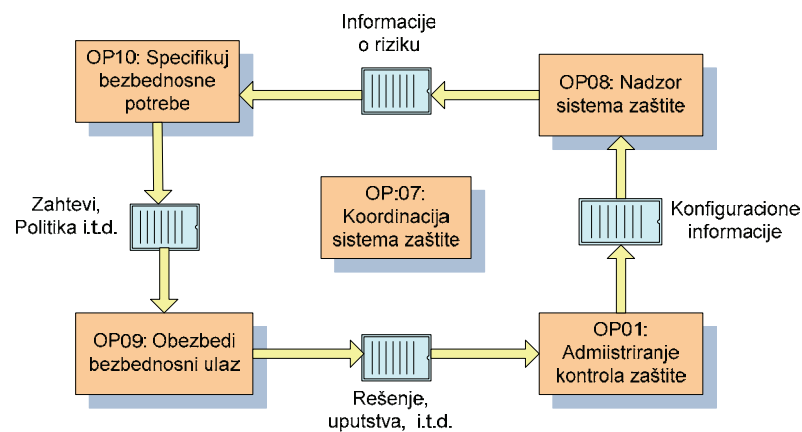
SE aktivnosti su one koje inženjeri zaštite treba da izvrše da bi obezbedili neko rešenje zaštite. Primeri su: definisanje i dostavljanje bezbednosnih zahteva, izrada projekta sistema zaštite na bazi principa zaštite, korišćenje statičkih analitičkih alata, revizija, nadzor i kontrola, bezbedno testiranje i.t.d.

Proces analize rizika obuhvata aktivnosti identifikacije i procene pretnji, ranjivosti i uticaja pretnji na identifikovane ranjivosti, kao najznačajnije aktivnosti u životnom ciklusu sistema zaštite, (Sl. 2.4.10).



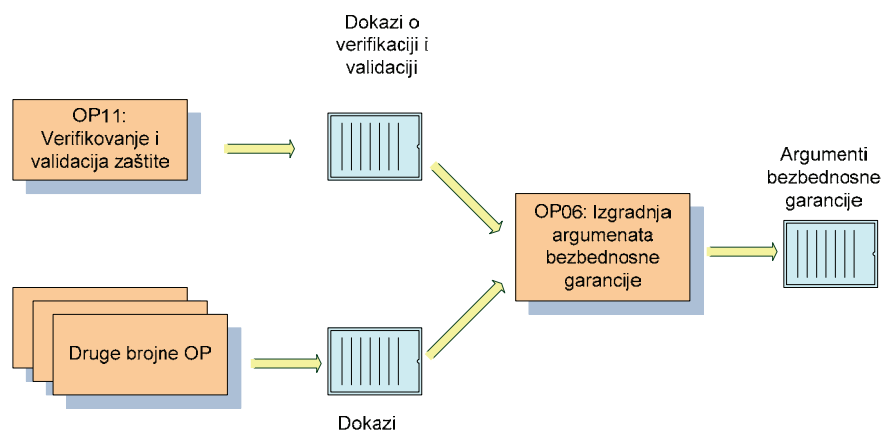
Sl. 2.4.10. Primena SSE CMM OP u procesu analize rizika

U SSE CMM modelu bezbednost sistema je integralni deo ukupnog inženjerskog procesa. Proces **koordinacije sistema zaštite** obuhvata sledeće OP: administriranje sistema zaštite, nadzor i kontrolu, specifikaciju bezbednosnih potreba i obezbeđenje bezbednosnih ulaza (Sl. 2.4.11).



Sl. 2.4.11. SSE CMM OP kao integralni deo ukupnog SE procesa

Aktivnosti za obezbeđivanje bezbednosne garancije uključuju OP za: verifikaciju i validaciju, ekspertsku reviziju, pregled artefakta i evaluaciju u procesu izgradnje argumenata bezbednosne garancije, kao i brojne druge OP sa objektivnim dokazima koji povećavaju poverenje u sistem zaštite (Sl. 2.4.12), [60], [54].



Sl. 2.4.12. SSE CMM OP za izgradnju argumenata za garantovanu bezbednost

Organizaciono upravljačke aktivnosti uključuju: politike organizacije, sponzorstvo i kontrolu menadžmenta, uspostavljanje organizacionih uloga i druge organizacione aktivnosti koje podržavaju bezbednost.

Projektno upravljačke aktivnosti uključuju: planiranje i praćenje projekta, alokaciju resursa i njihovo korišćenje za planiranje, upravljanje i praćenje SSE procesa, bezbednosnu garanciju i identifikaciju rizika.

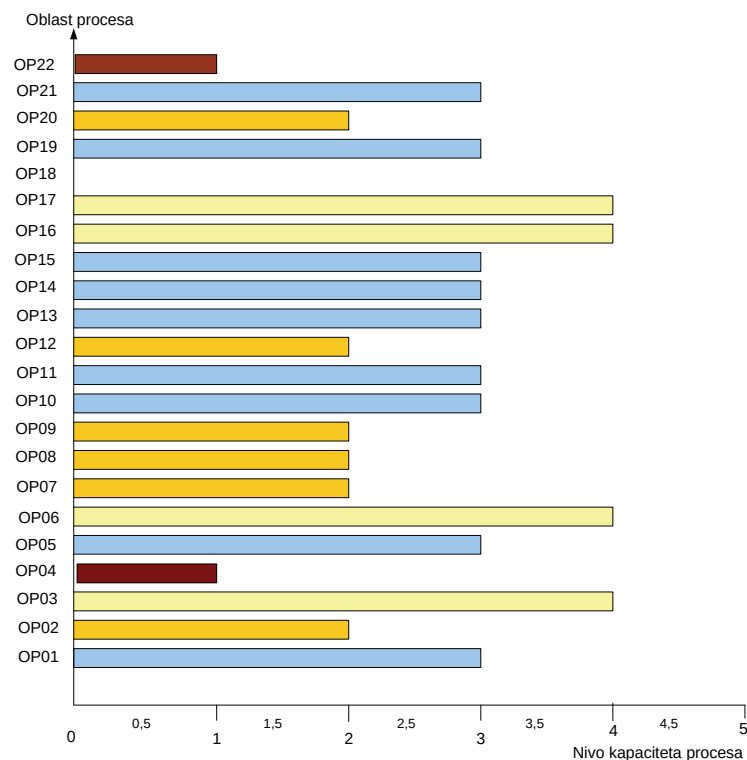
Opšte prednosti primene SSE CMM modela procesa su:

- Uštede koje prate ponovljive i predvidljive prakse i procese koje nastaju zbog manjeg ponavljanja rada;
- Kredit za poboljšavanje stvarnih kapaciteta za izvršavanje procesa, posebno u procesu selekcije snabdevača;
- Fokus na merene kompetencije organizacije (zrelost) i poboljšavanje procesa.

Nedostaci SSE CMM modela proističu iz činjenice da praksa zaštite nema dobro definisane procese kao druge inženjerske discipline, a aktivnosti u zaštiti često se izvršavaju odvojeno od procesa projektovanja i razvoja IKT sistema. Proizvođači hardversko – softverskih komponenti zaštite nemaju, ili ne koriste adekvatnu metriku za procenu SSE kapaciteta tako da ne mogu obezbediti garantovanu bezbednost za svoje proizvode. Takođe, u evaluaciji projekata za razvoj proizvoda/sistema/servisa zaštite često se ističu konačni rezultati, iako se ocene SSE CMM evaluacije odnose na *proces* sa kojima se ti rezultati postižu, [11], [27].

Sam **SSE CMM** model sadrži metodologiju za evaluaciju procesa zaštite, sa ciljem poboljšavanja procesa, pa nije neophodno koristiti **SSAM** (*System Security Appraisal Method*) metod evaluacije, koji je razvijen za specifičnu primenu te metodologije.

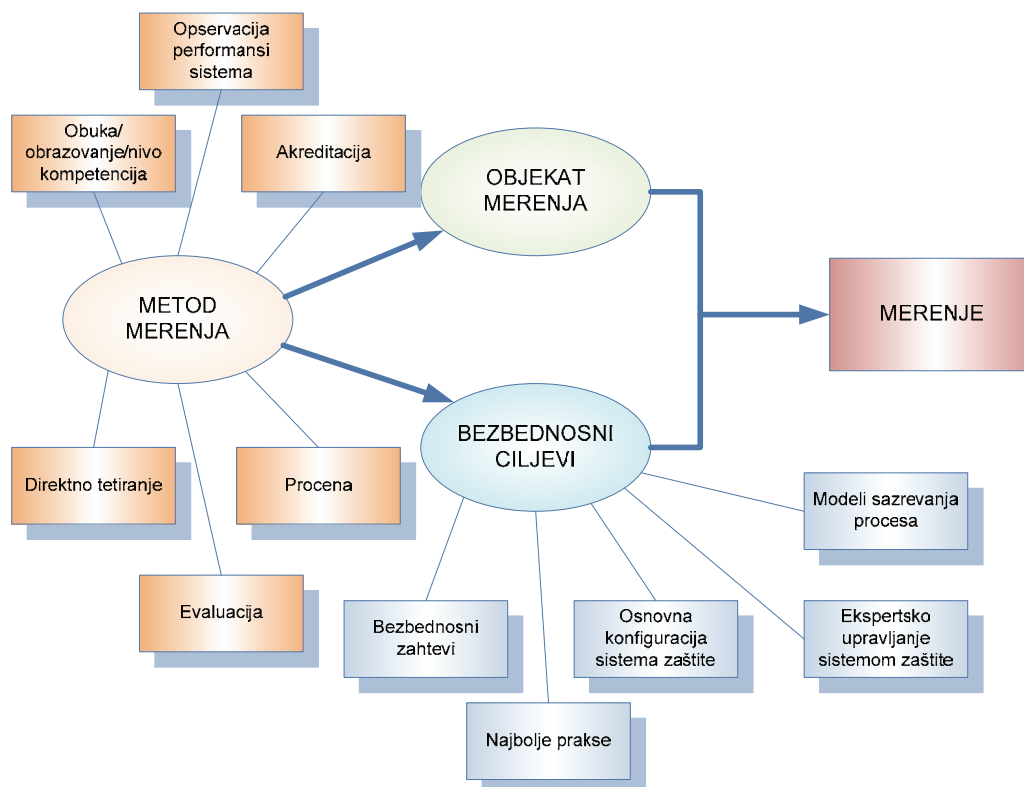
Na slici Sl. 2.4.13 prikazan je primer profila kapaciteta procesa organizacije za *Integraciju sistema* u kome je ilustrovano da su na najvišem nivou one OP koje najviše doprinose ispunjavanju očekivanja kupaca, [37].



Sl. 2.4.13. Primer profila nivoa kapaciteta OP organizacije za Integraciju sistema

2.4.4. Metrika IKT zaštite i modela sazrevanja procesa zaštite

Funkcionalni model metrike IKT zaštite, [91], (Slika 2.4.14) sadrži tri komponente: *objekat merenja*, *bezbednosne ciljeve merenja* (u odnosu na koje se objekti mere) i *metod merenja*.



Sl. 2.4.14 Model metrike IKT zaštite

Objekti merenja IKT zaštite mogu biti sistemi, komponente, politike zaštite, procesi i dr.

Bezbednosni cilj primarno određuje izbor tipa metrike IKT zaštite, a može se odrediti u odnosu na, [98]: *bezbednosne zahteve* (n.p.r., CC standarda), *procesе najbolje prakse* zaštite (n.p.r., ISO/IEC 17799), *osnovnu konfiguraciju* sistema zaštite (n.p.r., BSI Nemačka. *security baselines*), *ekspertska znanja*, tj. upravljanje zaštitom na bazi znanja i iskustava i **modele sazrevanja procesa zaštite** (n.p.r., SSE CMM). U Tabeli 2.4.11 zbirno su prikazani bezbednosni ciljevi sa relevantnim atributima primene.

Tabela 2.4.11. Bezbednosni ciljevi sa atributima primene

Bezbednosni ciljevi	Metod primene	Očekivani rezultati	Primer
Bezbednosni zahtevi	Akcije zaštite upoređuju se sa zahtevima za zaštitu	Sugestije za poboljšavanje	Standardi, CC PP
Najbolje prakse	Date su ili određene procedure zaštite za neke aktivnosti u standardu	Instrukcije za procedure zaštite	Instrukcije za antivirusnu zaštitu
Osnovna konfiguracija zaštite (<i>security baseline</i>)	Kontrola (<i>audit</i>) i procena sistema IKT zaštite organizacije	Minimalni skup potrebnih bezbednosnih akcija	Zahtevane kontrole pristupa
Ekspertska znanja i iskustva	Upravljanje zaštitom na bazi stručnosti i iskustava	Nivo bezbednosti svoje organizacije ili poslovnog partnera	Evaluacija kontrola zaštite
Metodi sazrevanja procesa	Prakse zaštite se ispituju u odnosu na referentni model	Eksplisiti nivo zaštite	SSE CMM

Metodi merenja obuhvataju: direktno testiranje, **evaluaciju**, procenu (rizika, ranjivosti, pretnji); sertifikaciju i akreditaciju; obuku, edukaciju, ocenu nivoa kompetencija i opservaciju performansi sistema (n.p.r., IDS sistema). Metodi merenja sa relevantnim atributima sumarno su prikazani u Tabeli 2.4.12.

Tabela 2.4.12. *Metodi merenja IKT zaštite*

Metod merenja	Kako se primenjuje	Očekivani rezultat	Primer
Direktno testiranje	Stanje sistema se procenjuje testiranjem njegovog kvaliteta	Operativno stanje sistema	Testiranje na proboj
<i>Evaluacija</i>	Bezbednosne mere se upoređuju sa kriterijumima	Uspostavljanje osnovne konfiguracije zaštite, sugestije za poboljšavanje	Kontrola (<i>audit</i>), SSAM evaluacija na bazi SSE CMM modela
Procena	Bezbednosne mere se procenjuju	Određeni prioriteti akcija, sugestije za poboljšavanje	Metodi i tehnike za analizu rizika
Akreditacija	Bezbednosne mere se procenjuju	Izveštaj o sertifikaciji sistema zaštite, sugestije za poboljšavanje	Sertifikat ISO 9000 serije standarda
Obuka, edukacija, nivo kompetencija	Personalno i organizaciono znanje se procenjuje i poboljšava	Izveštaj o sertifikaciji, poboljšavanje u individualnim oblastima	Konferencije, testovi veština, kursevi
Opservacija performansi sistema	Sistem se monitoriše sa tehničkim alatima	Stanje ili kvalitet tehničkih karakteristika u nekom trenutku/periodu	Detektor upada (IDS), merenje opterećenja mrežnog saobraćaja

Problemi metrike IKT zaštite mogu se svrstati u sledeće kategorije:

1. Višeznačnost koncepta „metrike“ u IKT zaštiti, zbog niske objektivnosti rezultata merenja i otežane generalizacije i poređanja;
2. Teškoće u dobijanju kvantitativnih mernih rezultata za objekte IKT zaštite, zbog neobjektivnosti rezultata, teže generalizacije i poređanja;
3. Teškoće u merenju operativnih komponenti zaštite, zbog niske mogućnosti predviđanja stvarnog funkcionisanja sistema zaštite;
4. Prirode same oblasti IKT zaštite, zbog neprekidnog rizika od otkrivanja ranjivosti sistema i problema ubeđivanja menadžmenta u potrebu zaštite.

Procesno orijentisan SSE CMM model, usmeren na oblast zaštite informacija, za merenje SSE, organizacionih i upravljačkih procesa zaštite, koristi **dualnu metriku**, što znači da se obe metrike koraju koristiti istovremeno, [83], [101], [102]:

1. **Specifičnu metriku procesa**, orijentisanu na same procese, koja se može meriti sa:
 - kvantitativno/kvalitativnim dokazima o nivoima zrelosti SSE OP, ili
 - binarnom indikacijom prisustva/odsustva zrelog procesa.
2. **Metriku sistema zaštite**, orijentisanu na rezultate izvršavanja procesa zaštite, koja:
 - obezbeđuje objektivne/subjektivne, kvalitativne/kvantitativne attribute merenja
 - rezultata SSE procesa, kao dokaze efektivnosti tog procesa.

Opšta procedura metričkog sistema SSE CMM modela zrelosti i sazrevanja kapaciteta procesa za razvoj programa zaštite obuhvata sledeće glavne aktivnosti, [83]:

1. Sve merene OP ponderisati težinskim faktorima od 1-5 koji pozicioniraju datu OP na odgovarajući nivo zrelosti (npr. sve OP =3 nalaze se na 3. nivou zrelosti, sve OP=1, na 1. nivou zrelosti i.t.d.), na bazi evaluacije procenta izvršavanja BP i GP date OP prema SSAM kriterijumu.
2. Na svakom nivou izračunati ukupan zbir težinskih faktora svih OP, koji pokazuje nivo zrelosti kapaciteta na datom nivou SSE CMM razvoja procesa zaštite.

3. Razlika između zbira težinskih faktora zrelosti OP na višem nivou u odnosu na niži nivo, pokazuje kvantitativnu meru progresivnog „sazrevanja“ procesa i kapaciteta za razvoj programa zaštite.
4. Izabrati SSE CMM pre-definisani referentni (željeni) profil zrelosti kapaciteta procesa kojem organizacija teži, ili ga odrediti na bazi poslovnih ciljeva i misije organizacije.
5. Posle određenog vremena evaluirati/meriti tekući profil i odrediti **razlike** zrelosti svake/zbira OP na odgovarajućem nivou kapaciteta u referentnom i tekućem profilu, koje indiciraju nivo progresivnog sazrevanja svake/zbira OP i predstavljaju polaznu osnovu za poboljšavanje procesa (OP).

2.5. Metodi evaluacije i poboljšavanja procesa zaštite

2.5.1. Uvod

Formalnu metodologiju za evaluaciju proizvoda i sistema zaštite obezbeđuje **CC standard (ISO 15408)**. **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**). Pozitivno evaluiran sistem naziva se poverljivi (*trusted*) sistem.

Proces evaluacije proizvoda i sistema zaštite prema **CC standardu** obuhvata sledeće korake: pronaći odgovarajući profil zaštite (**PP**) i razviti bezbednosni cilj (**ST**) na bazi tog profila, a ako nema **PP**, koristiti **CC** za direktan razvoj **ST**; evaluirati **ST** u skladu sa klasom za *evaluaciju bezbednosne garancije* (**ASE**) i vrednovati da li je **ST** kompletan, konzistentan i tehnički pouzdan i evaluirati proizvod, ili sistem zaštite prema **ST**, [18].

Formalna metodologija evaluacije obezbeđuje: tehniku merenja na bazi specifičnih bezbednosnih zahteva i dokaze bezbednosne garancije; skup zahteva koji definišu bezbednosnu funkcionalnost za sistem; skup zahteva bezbednosne garancije koji pokazuju da sistem ispunjava svoje funkcionalne zahteve; metodologiju, koja obuhvata funkcionalne i bezbednosne zahteve i nivoe bezbednosne garancije, a kojom se određuje da sistem ispunjava funkcionalne i bezbednosne zahteve na bazi analize dokaza bezbednosne garancije; merenje rezultata koji indiciraju koliko je sistem poverljiv u odnosu na funkcionalne zahteve, što se naziva *nivo poverenja*; nezavisnu, ekspertsku procenu i merenje bezbednosne garancije uključujući procenu konzistentnosti, kompletnosti, tehničke izvodljivosti i adekvatnosti za suzbijanje pretnji za bezbednosne zahteve, kao i procenu administratorskih i korisničkih instalacija i druge dokumentacije koje obezbeđuju informacije o propisnom konfigurisanju, administriranju i korišćenju sistema, [12].

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 u razvoju, evaluatore u fazi testiranja i korisnike u praksi zaštite, [12].

Za evaluaciju i poboljšavanje procesa organizacije postoje brojni metodi, od kojih **CMM** zaslužuju najveću pažnju. **SSE-CMM** metod evaluacije - **SSAM (System Security Appraisal Method)** obezbeđuje evaluaciju kapaciteta i zrelosti **SSE procesa** organizacije prema referentnom **SSE CMM modelu**. **SSAM** metod je primarno namenjen za **TTPS evaluaciju**, ali sadrži uputstvo i za *samo-evaluaciju*: samo-poboljšavanje procesa; bolje razumevanje praksi i implementacije novih praksi; kapaciteta organizacije; indikatora progressa i poboljšavanja i institucionalizacije procesa.

2.5.2. Ciljevi i izlazni rezultati evaluacije

Svaki proces evaluacije ima najmanje dva cilja:

1. efikasno sakupiti precizne podatke uz minimalnu destrukciju rada organizacije 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. *nalazi* o slabostima i snazi organizacije i
2. *preporuke* za akcioni plan poboljšavanja procesa.

Nalazi obezbeđuju preciznu sliku o procesima, koristeći CMM referentni model kao okvir za evaluaciju. **Preporuke** procesa evaluacije mogu da obezbede uputstvo za poboljšavanja tekućeg stanja procesa organizacije, okvir i katalizator za akcije i angažovanost i podršku organizacije; definišu vlasništvo nad rezultatima evaluacije i da olakšaju kontinualno poboljšavanje procesa, [101].

Metodi evaluacije na bazi CMM modela su brojni: SSAM metod evaluacije procesa zaštite, CMMI samo-evaluacija, monitorisana ili asistirana SSAM samo-evaluacija, privremeno profilisanje (SCAMPI B), CMMI mini evaluacija (SCAMPI B i C) i puna SCAMPI A tipa evaluacije [98], [101] i dr.

U izboru metoda evaluacije, sam proces evaluacije zahteva razmatranje najmanje tri faktora: **tačnost**, **troškove** i **stepen destrukcije** normalnog poslovanja organizacije. U Tabeli 2.5.1 data je uporedna analiza glavnih atributa dostupnih metoda evaluacije, [98].

Tabela 2.5.1 Uporedna analiza atributa metoda evaluacije

Tip	Tačnost	Troškovi	Destrukcija
Samo-evaluacija	Niska	Niska	Niska
Asistirana (monitorisana) samo-evaluacija	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, [33].

Tim za evaluaciju (TE) je kritični deo svakog procesa evaluacije. Veličina TE i kvalifikacije članova, uz eventualnu rezervu koordinatora za evaluaciju na terenu, mogu uticati na poverenje sponzora u rezultate evaluacije. Za postizanje ciljeva evaluacije i realizaciju plana evaluacije odgovoran je vodeći evaluator (evaluator 1).

2.5.3. Metod evaluacije primenom modela sazrevanja procesa zaštite

Metod evaluacije 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. Proces SSAM metoda evaluacije može se koristiti za **evaluaciju procesa** organizacije koja: razvija proizvode zaštite, obezbeđuje servise zaštite, integriše i administrira sisteme zaštite, razvija kompetencije specijalista zaštite i drugih zaposlenih. SSAM metod evaluacije obezbeđuje osnovne, tekuće indikatore izvršavanja aktuelnih bazičnih praksi, merenih prema standardima najboljih praksi SSE

CMM modela. Posle evaluacije, organizacija može koristiti SSAM metod **poboljšavanja procesa** za samo-poboljšanje svojih procesa zaštite, ili iznajmiti akreditovanu TTPS organizaciju za ove usluge, [101].

SSAM evaluacija je efektivan alat za selekciju snabdevača proizvoda i usluga, obezbeđujući dobru osnovu za komparativnu procenu kapaciteta potencijalnih snabdevača, kao i informacije koje mogu biti nezamenljive za upravljanje rizikom programa zaštite posle potpisivanja ugovora. Sa dobrom argumentacijom razloga, evaluator može dobiti podršku Sponzora 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 bezbednosnu garanciju, 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 inženjerskih kapaciteta organizacije, za prihvatanje i upravljanje rizikom programa zaštite. Ciljevi evaluacije treba da budu eksplicitno saopšteni u zahtevu za ponudu-RFP (*Request for proposal*), kojeg Sponzor evaluacije dostavlja organizaciji evaluatora, [101].

Zrelost kapaciteta prema SSE CMM, može se pokazati na više načina zavisno od RFP:

1. Ako Sponzor želi da proceni SSE kapacitete organizacije evaluatora, u tom slučaju RFP zahtevi mogu biti uopšteni, zahtevajući da izvođač evaluacije jednostavno komentariše svoje kapacitete za izvršavanje određenog SSAM profilisanja, bez eksplicitnog zahteva za formalnom SSAM evaluacijom.
2. Ako Sponzor želi da izvrši evaluaciju skraćenu po obimu i da samo stekne uvid u zrelost kapaciteta, u RFP se može zahtevati da izvođač u ograničenom obimu odgovori na SSE CMM *Upitnik*, ili da izvođač evaluacije izvrši samo-evaluaciju prema datom SSE CMM profilu i obezbedi rezultate na uvid, kao deo svoje ponude za evaluaciju.
3. RFP može zahtevati da iskusan TTPS **tim za evaluaciju (TE)** kojeg izabere organizacija koja traži ponudu, izvrši evaluaciju kapaciteta izvođača evaluacije, s tim da organizacija snosi troškove barem rada TE.
4. 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 evalaucije.

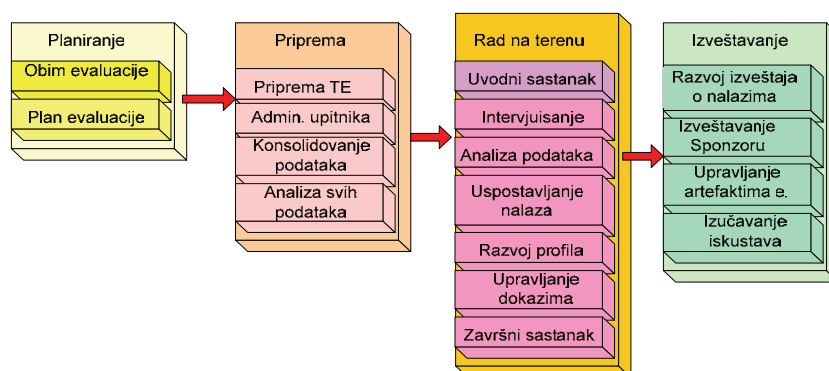
Proces SSAM metoda evaluacije obuhvata 4 faze, (Tabela 2.5.2):

Tabela 2.5.2. Faze procesa SSAM metoda evaluacije

Faza	Opis
1. Planiranje	Upostavlja okvir u kojem će se izvoditi evaluacija procesa, kao i logističku pripremu za fazu (<i>on-site</i>) evaluacije na terenu
2. Pripreme	Priprema TE za evaluaciju na terenu, preliminarno sakupljanje, analiza, konsolidovanje i administracija podataka iz <i>upitnika</i>
3. Rad na terenu	Istraživanje rezultata preliminarne analize podataka i uključivanje korisnika iz prakse evaluiranog entiteta u prikupljanje podataka i validaciju procesa putem <i>intervjua</i>
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, [101] i koristi se kao **radni dokument**. Grafički model procesa SSAM metoda evaluacije sa glavnim koracima u svakoj fazi, prikazan je na Slici 2.5.1. Detaljan opis procesa SSAM metoda evaluacije i model u BPWin CASE alatu dati

su u **Radnim dokumentima (Prilog 1 i 1A)** koji su sastavni deo rada i nalaze se na priloženom CD-u.



Sl. 2.5.1. Model faza i koraka procesa SSAM evaluacije

2.5.4. 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 2.5.3. prikazane su zahtevane kvalifikacije i tipične odgovornosti primarnih učesnika u procesu evaluacije, od kojih neki imaju višestruke funkcije.

Tabela 2.5.3. 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 poboljšavanja Posreduje između evaluatora i koordinatora na lokaciji poboljšavane organizacije	Sposobnost da podrži aktivnosti evaluacije
Tim za evaluaciju (TE)	Sva lica organizacije koja vrši evaluaciju, a učestvuju u aktivnostima evaluacije	Učestvovanje u procesu evaluacije i poboljšavanja procesa	Videti Radna dokumenta, <i>Uputstvo za evaluatore-CD</i>
Evaluatori (Facilitators)	Lideri tima za evaluaciju	Obezbeđivanje korektnog izvršavanja evaluacije Koordinacija aktivnosti sa Sponzorom Razvoj i održavanje plana evaluacije	Videti Radna dokumenta, <i>Uputstvo za evaluatore-CD</i>
Rukovaoc dokaza (2.evaluator)	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	Videti Radna dokumenta, <i>Uputstvo za evaluatore -CD</i>
Posmatrači	Članovi tima za evaluaciju bez prava glasa	Pomažu članovima tima sa pravom glasa i evaluatorima Prikupljaju iskustva iz SSAM evaluacije	Poznavanje SSE CMM modela i SSAM metoda evaluacije i poboljšavanja procesa zaštite
Korisnici procesa na terenu (praktičari)	Svi članovi evaluirane organizacije uključeni u proces evaluacije	Prisustvovanje brifinzima Odgovaranje na pitanja u toku intervjua	Zaposleni u evaluiranoj organizaciji

Organizacija	Opis	Primarna odgovornost	Kvalifikacije
Koordinator evaluacije na terenu	Lice za kontakte iz evaluirane organizacije	Koordinira aktivnosti evaluirane organizacije u toku procesa evaluacije	Poznavanje organizacione strukture, funkcionisanja, politika i procedura evaluirane organizacije Donosioc odluka Upoznat sa procesom SSAM (ako je moguće)
Menadžment	Donosioci odluka na najvišem nivou evaluirane organizacije	Davanje i izražavanje podrške za evaluaciju	Sposobnost da angažuje učešće zaposlenih u procesu evaluacije
PR menadžmenta	Poslove portparola menadžmenta	Obraća se korisnicima na terenu na otvorenim sastancima	Poznavanje izvršnih poslova evaluirane organizacije
Rukovodstvo evaluiranog projekta	Upravlja projektnim aktivnostima i članovima projektnog tima	Popunjavanje SSAM <i>upitnika</i> Prikuplja i daje odgovore na pitanja iz <i>intervjua</i>	Potvrđeno iskustvo iz izvođenja SSE aktivnosti na dokazanom projektu
Praktičari evaluiranog procesa	Član projektnog tima evaluiranog projekta	Odgovara na pitanja iz <i>intervjua</i>	Iskustvo iz podrške, direktne ili indirektna nekom relevantnom projektu zaštite

Tipični zahtevi za radno angažovanje u SSAM procesu evaluacije i poboljšavanju procesa zaštite organizacije na 3-4 projekta prikazani su u Tabeli 2.5.4.

Tabela 2.5.4. Zahtevi za radno angažovanje u SSAM procesu evaluacije

Uloga u evaluaciji	Preporučeni broj ljudi	Angažovanje (čovjek/sati)	Ukupno angažovanje (čovjek/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 primenjivo	1002

2.5.5. Tipovi SSAM procesa evaluacije

Nezavisna TTPS evaluacija je primarna namena SSAM metoda koji sadrži uputstva i za samo-evaluaciju. Evaluaciju obavlja akreditovani poverljivi (TTPS) provajder usluga, a ciljevi evaluacije procesa variraju u skladu sa potrebama **inicijatora evaluacije, ili Sponzora**. Sponzor je organizacija ili pojedinac koji zahteva dobijanje bezbednog proizvoda, sistema, ili servisa i inicira proces evaluacije. Sponzor je odgovoran za uspostavljanje parametara i razloga ciljeva evaluacije, specifikovanje zahteva i obezbeđivanje podrške procesu evaluacije. Mnoge aktivnosti Sponzor može preneti na druge učesnike, pre svega SSAM evaluatore, a TE može mu pomagati u postavljanju zahteva, ciljeva i specifikovanju zahteva za ponudu procesa evaluacije (RFP).

Ciljevi evaluacije utiču na izbor projekata za evaluaciju i informacija za izveštavanje rezultata evaluacije. Razlozi za izbor TTPS evaluacije brojni su, a uključuju:

- kompetentncije organizacije za ispunjavanje ugovornih obaveza,

- nezavisnu komparativnu analizu kvalifikacija snabdevača,
- obezbeđivanje razumevanja i ispunjavanja očekivanja klijenata,
- obezbeđivanje upravljanja rizikom izvršavanja programa i dr.

Samo-evaluacija (*asistirana, monitorisana*) obezbeđuje organizaciji uvid u sopstvene kapacitete za SSE praksu, značajno smanjuje angažovanje resursa i destrukciju suštinskih poslova organizacije, u odnosu na TTPS evaluaciju. Uz dobre razloga za evaluaciju, racionalan obim i plan evaluacije, Sponzor može obezbediti potrebnu podršku i angažovanje cele organizacije. Sponzor postavlja ciljeve evaluacije od kojih zavisi izbor OP za evaluaciju i željenih nivoa kapaciteta, vremena završetka evaluacije, metoda izveštavanja rezultata evaluacije i projekata za evaluaciju. Na primer, ako je primarni cilj evaluacije poboljšavanje kapaciteta organizacije za obezbeđivanje argumenta za bezbednosnu garanciju, proces evaluacije treba da usmeri veću pažnju na kvalitet i kompletnost dokaza, nego u slučaju evaluacije sa ciljem poboljšavanja ukupnih procesa. Tipični ciljevi za samo-evaluaciju 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,
- odrediti progres aktivnosti za poboljšavanje 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 toku integracije sistema, razvoja aplikacija ili proizvoda, ili obezbeđivanja servisa?
- Da li organizacija želi da poboljša svoje SSE prakse i dostigne ponovljivost, neprekidnost, efikasnost i veću bezbednosnu garanciju?
- Da li organizacija želi da uspostavi svoju kompetentnost u izabranoj OP?
- Koji projekti najbolje demonstriraju SSE OP koje treba uključiti u proces evaluacije?

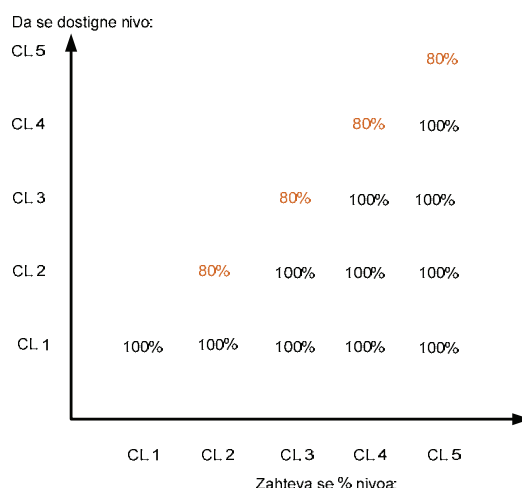
Sponzor, takođe, treba da shvati da neka SSAM evaluacija neće propisati dobre procese, ili naučiti organizaciju kako da poboljša svoje kapacitete za izvršavanje specifičnih procesa, niti da je SSAM evaluacija zamena za evaluaciju proizvoda ili sertifikaciju sistema. Međutim, **SSAM evaluacija može obezbediti važan uvid i uputstvo za budući proces poboljšavanja i može izgraditi dodatne argumente za bezbednosnu garanciju za proizvode i sisteme zaštite**. Sponzor treba da proceni vrednost potencijalnih dobiti od evaluacije, prema njenim troškovima, pre pokretanja zahteva za evaluaciju (RFP).

2.5.6. 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 isključivnje nekih OP modela, iako su sve OP primenljive za SSE praksu, ili prilagođavanje nekih aspekata OP određenim potrebama. Sponzor može ponuditi objektivni dokaz proizvoda rada prakse/procesa koji nije naveden u primerima datih BP u modelu. Terminologija se, takođe, može prilagoditi kulturi rada evaluirane organizacije.

Nivo CL: Sponzor može identifikovati ciljane ili željene nivoe kapaciteta za OP uključene u evaluaciju, ili izabrati pre-definisane 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 nivo kapaciteta (CL). **Kriterijumi za dostizanja CL** definiše SSAM metod evaluacije (Slika 2.5.2), ali Sponzor može tražiti da redefiniše kriterijume na bazi značaja koji pridaje postizanju specifičnog nivoa kapaciteta.



Sl. 2.5.2. Princip dostizanja nivoa kapacitete 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 2.5A**.

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 geografske podatke evaluirane organizacije (udaljenosti, radi troškova putovanja TE), a i ciljevi evaluacije mogu uticati na izbor projekata. Neki kriterijumi za izbor projekata za evaluaciju dati su u Tabeli 2.5.5.

Tabela 2.5.5. Neki kriterijumi za izbor projekata za evaluaciju

Faza	Opis
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 poboljšavanje 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 intervju po različitim projektima treba planirati racionalno, po mogućnosti na istoj lokaciji, zbog troškova. Kontrolna lista za pripremu aktivnosti evaluacije na terenu, koja se koristi kao *pomoćni radni materijal* evaluatora, data je u **Prilogu 4 Radnog materijala** na priloženom CD-u.

Intervju: Za intervjuisanje Sponzor može odrediti lica prema funkciji, nadležnosti, nivou odgovornosti ili drugoj kvalifikaciji. Rukovodstvo projekta, iako može biti sastavljeno od ljudi sa različitim zvanjima, 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 rezultati evaluacije treba da se saopšte; od nesaopštavanja rezultata na kraju faze rada

na terenu, preko uopštene prezentacije rezultata TE svim zaposlenim organizacije, 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 2.5B**.

Odnosi sa koordinatorom rada na terenu: Koordinator rada na terenu je predstavnik evaluirane organizacije i saradnik TE u toku evaluacije na terenu. Sponzor treba da odredi koordinatora koji ima neophodan autoritet za neometan razvoj procesa evaluacije, odgovornog za logističku podršku specifikovanu u *RFP*: obezbeđivanje prostora za rad TE, pristupa objektima, ljudima i dokazima organizacije i snabdevanje TE potrebnim materijalnim resursima tokom procesa evaluacije. Uzorci ostalih radnih dokumenata za praćenje kretanja 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 2.5C**.

2.5.7. Rezultati i izveštavanje SSAM procesa evaluacije

Primarni rezultati SSAM metoda evaluacije procesa su **Glavni nalazi** koje evaluator u ime TE referiše i konačno diskutuje na brifinga Sponzora i ***Izveštaj o evaluaciji***. Brifing za utvrđivanje nalaza uključuje prezentaciju profila nivoa kapaciteta/zrelosti procesa i listu ključnih nalaza procesa/praksi za poboljšavanje. Profil nivoa kapaciteta/zrelosti indicira nivo kapaciteta/zrelosti svake pojedinačne/grupe OP 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 poboljšavanju piše se samo Sponzoru i uključuje dodatne detalje o svakom nalazu, svaki zahtev Sponzora za izveštavanjem i implikacije nalaza na zahteve Sponzora.

Na kraju procesa evaluacije u skladu sa modelom i metodom, vodeći evaluator treba da dostavi referencirane eventualne probleme i iskustava grupi za razvoj SEI instituta, prema formularu za ***Izveštaj evaluatora*** datom u modelu, [102]. U **Prilogu 2.5D** 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, kao i primer direktnih i indirektnih artefakta (tipični proizvodi rada) SSAM metoda evaluacije – **SSAM PIID** dokument, koji je originalno generisan u **Radnim materijalima**, a koji zajedno kompletiraju proces SSAM evaluacije i potrebni **radni materijal**.

2.6. Integrirani model i metod evaluacije procesa

2.6.1. Uvod

Iz generičkog CMM modela razvijena su dva tipa integriranih modela sazrevanja procesa.

Integracioni model sazrevanja procesa–CMMI (CMM Integration), poslednja verzija CMMI 1.2 (25.08. 2006), integriše procese SE CMM i SW CMM i obezbeđuje najbolje prakse za razvoj i

*održavanje, akviziciju i servise, uključujući pomoć organizacijama kod evaluacije i poboljšavanja procesa SCAMPI (Standard CMMI Appraisal Method for Process Improvement) metodom. Model, obezbeđuje i okvir za uvođenje nove discipline, i široko je prihvaćen. U odnosu na ranije CMM modele u CMMI v.1.2 eliminisane su BP i zamenjene sa *specifičnim praksama* (SP). Pojednostavljena je i numeracija komponenti modela, ukinute su CF, a GP više nisu organizovane u CF kao u SSE CMM modelu, nego u *generičke ciljeve* (GG), koji su sekvencijalno numerisani, a izvršavaju se kroz *specifične ciljeve* (SG). Ukupno 22 OP su bitno izmenjene, integrisane i poboljšane sa novim SP, ili napomenama i drugim informativnim komponentama koje dodatno objašnjavaju implementaciju praksi i procesa. Razvijene su tri **konstelacije** modela, za: *razvoj procesa i proizvoda* - **CMMI-DEV** sa 22 OP koja je kompletirana, a za *servise* - **CMMI-SVC** i *akviziciju* - **CMMI-ACQ** u toku su razvoja. U sve tri konstelacije modela zajedničkih je 16 ključnih OP, [20], [63].*

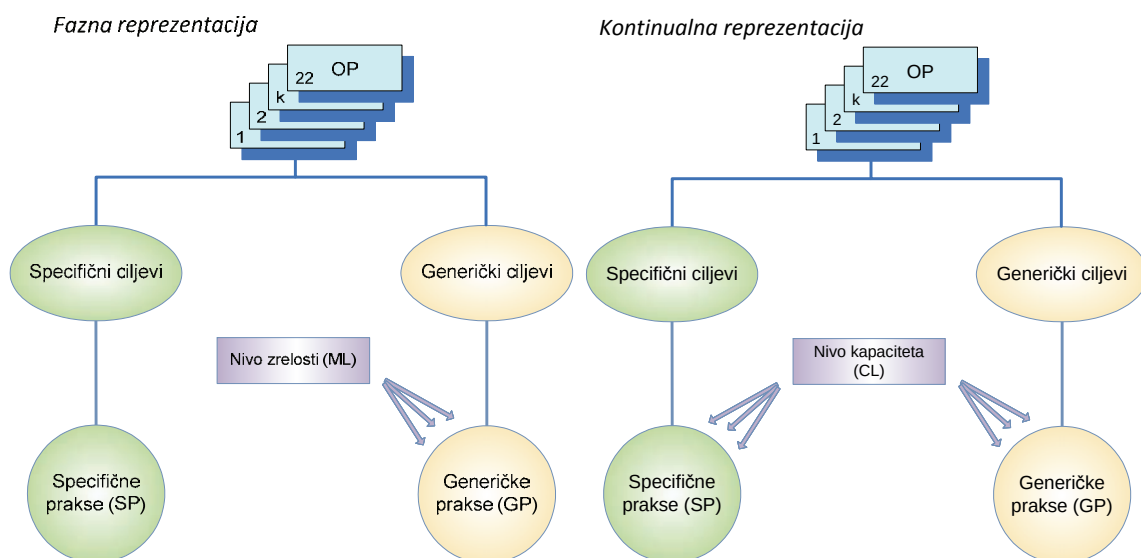
Integrirani model sazrevanja procesa - iCMM (Integrated CMM) obezbeđuje jedinstven model za poboljšavanje procesa velikih organizacija, integrišući brojne kriterijume i standarde, različite po strukturi, formatu, terminima i načinu merenja zrelosti i smanjujući konfuziju kod korisnika, posebno u slučaju korišćenja više od jednog standarda/modela u organizaciji. Model potvrđuje težinu integracije različitih modela u kombinovani program za poboljšavanje procesa. Koristi se u Administraciji federalne avijacije SAD (FAA), [41].

Standardni CMMI metod za evaluaciju i poboljšavanje procesa - SCAMPI 1.2, obuhvata dva ključna dokumenta: **Zahtevi za CMMI evaluaciju -ARC (Appraisal Requirements for CMMI)** koji sadrže zahteve za tri klase metoda evaluacije: A, B i C i **Dokument za opisivanje SCAMPI metoda - MDD (Method Description Document)**, u kojem su opisane klase metoda. CMMI odobrava samo metod klase **A**, dok su metodi klase **B** i **C** manje rigorozni i ispravnije ih je zvati metodama **procene**, a ne evaluacije. SCAMPI A metod se koristiti samo za evaluaciju i poboljšavanje procesa organizacije, a obuhvata tri kategorije komponenti CMMI modela: **zahtevane** (SG i GG), **očekivane** (SP, GP) i **informativne** (subprakse i tipične proizvode rada). Tim za evaluaciju (TE) mora u procesu evaluacije pronaći indikatore *implementacije i institucionalizacije* SP i GP projekta, koji *objektivno* potvrđuju da su SG i GG organizacije zadovoljeni, [99], [100].

2.6.2. Struktura CMMI modela

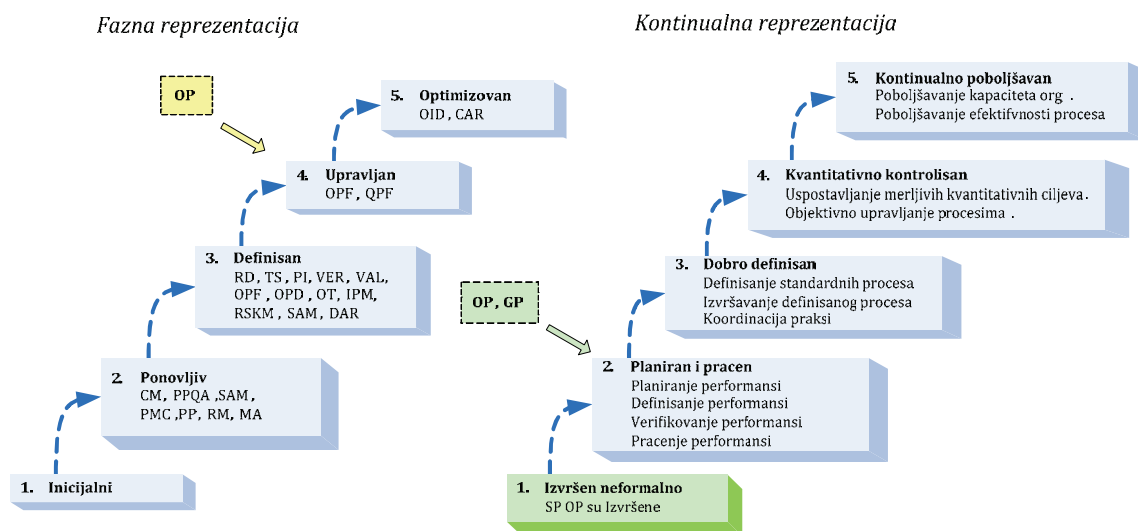
CMMI okvir organizuje komponente u modelima, materijalu za obuku i metodu evaluacije (SCAMPI) i generiše **CMMI Product Suite** - potpunu kolekciju modela, materijala za obuku i metoda evaluacije. Podskup *CMMI Product Suite*, je **CMMI konstelacija** - relevantna za poboljšanje u određenoj oblasti primene - *razvoju, akviziciji i davanju servisa*. CMMI model procesa ima dve reprezentacije: *kontinualnu* i *faznu*.

Reprezentacije CMMI modela, analogna pogledu na skup podataka kojeg obezbeđuje baza podataka, obezbeđuju u suštini isti sadržaj i koriste iste komponente modela, ali su organizovane na različit način i razlikuju se u prva dva nivoa kapaciteta (CL) i zrelosti (ML) procesa, (Sl. 2.6.1), [20].



Sl. 2.6.1. Struktura CMMI modela u obe reprezentacije

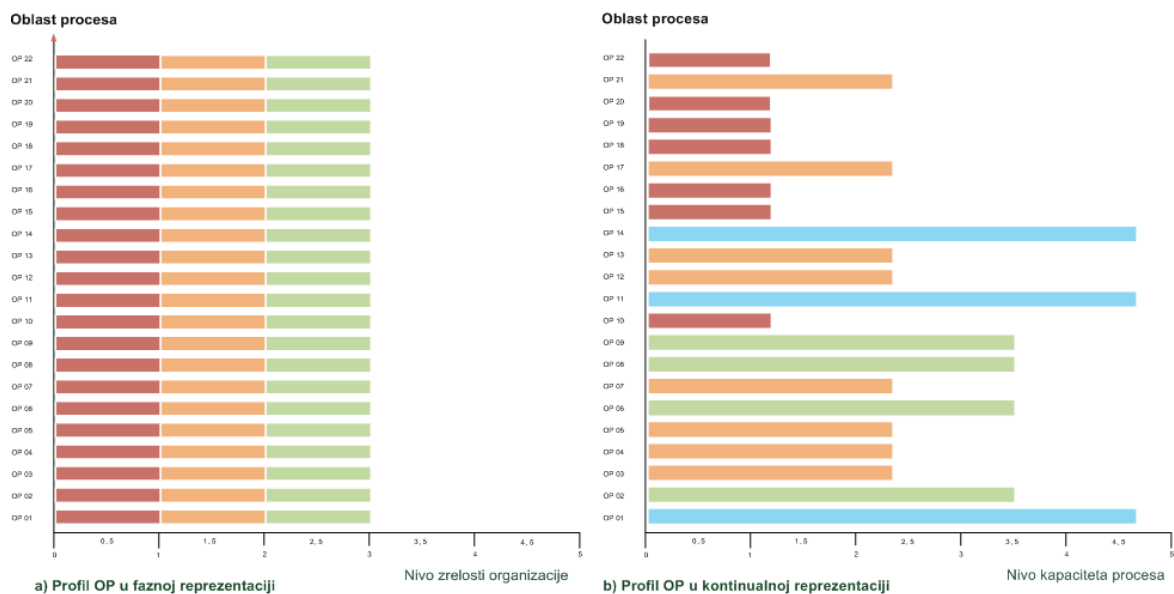
Putevi evolucije nivoa kapaciteta OP u faznoj i kontinualnoj reprezentaciji CMMI modela prikazani su na slici Sl. 2.6.2.



Sl. 2.6.2. Evolucija nivoa zrelosti i kapaciteta u CMMI modelu

Fazna reprezentacija modela koristi se za početno poboljšavanje grupe procesa organizacije, na primer na 1. nivo zrelosti. Svaki *nivo zrelosti* procesa (1-5) obezbeđuje predviđanje opštih izlaza sledećeg projekta. Kontinualna reprezentacija koristi se za progresivno - inkrementalno ili inovativno poboljšavanje izabranih, pojedinačnih OP.

Primer grafičke reprezentacije profila izlaznih nivoa ML OP u faznoj reprezentaciji (a) i nivoa CL OP u kontinualnoj reprezentaciji modela (b) prikazan je na slici Sl. 2.6.3.



Sl. 2.6.3. Profili rangiranja nivoa zrelosti (a) i kapaciteta (b) OP CMMI modela

U faznoj reprezentaciji modela sve OP moraju biti na istom nivou ML pre nego što organizacija može podići OP na sledeći viši nivo zrelosti. U kontinualnoj reprezentaciji modela organizacija može usmeriti aktivnosti i resurse prema OP, koje su bitne za izvršavanje poslovnih cviljeva. Nivoi CL različitih OP mogu međusobno varirati. Aplikativne prednosti i nedostaci obe reprezentacija modela date su u Tabeli 2.6.1, [20].

Tabela 2.6.1. Aplikativne razlike dve reprezentacije CMMI modela

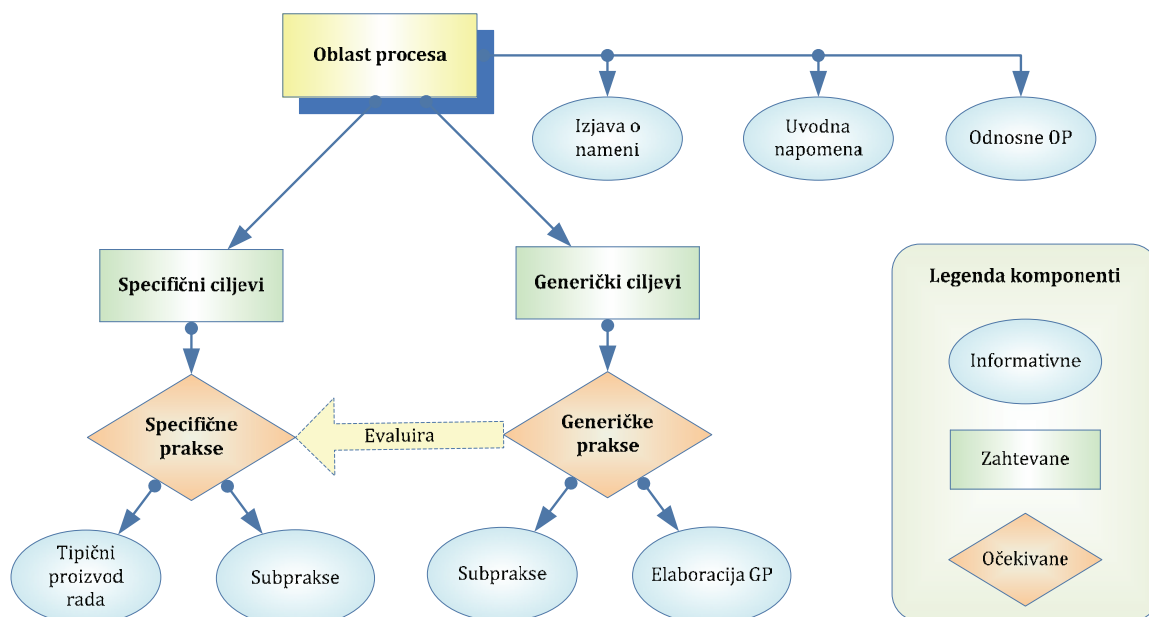
Fazna reprezentacija	Kontinualna reprezentacija
Manje fleksibilan	Fleksibilniji
Obezbeđuje definitivno usmerenje za poboljšanje (sve OP teže 5. nivou zrelosti)	Organizacija može projektovati svoj vlastiti pravac poboljšanja procesa
Primenljiv samo za specifičan tip organizacija	Primenljiv za sve tipove organizacija
Svi procesi su obuhvaćeni na svakom nivou	Proizvoljan broj OP na svakom nivou

Dimenzije CMMI modela čini skup tačaka u dvodimenzionalnoj ravni, odnosno:

- **dimenzija oblasti** procesa ili „šta“ organizacija radi (n.p.r. na **x** osi) i
- **dimenzija kapaciteta** ili „koliko dobro“ izvršava te procese (na **y** osi).

Dimenzija oblasti procesa (OP) je klaster odnosnih specifičnih praksi (SP), koje su glavni gradivni blokovi za uspostavljanje kapaciteta procesa. Svaka OP u CMMI modelu opisana je sa **komponentama modela**: *izjava o nameni*, *uvodna napomena*, *odnosne OP* (koje se odnose na razmatranu OP), *kratak opis specifičnih ciljeva* (SG) i *specifičnih praksi* (SP), *specifične prakse* (SP) po *specifičnim ciljevima* (SG), odnosno SG i SP i *generičke prakse* (GP) po *generičkim ciljevima* (GG), odnosno GG i GP.

Komponente OP grupisane su u tri kategorije: *zahtevane*, *očekivane* i *informativne*. **Zahtevane** komponente **SG i GG** opisuju šta organizacija mora postići da zadovolji neku OP modela i šta mora biti vidljivo implementirano u procesima organizacije. Postizanje specifičnog cilja (SG) koristi se u evaluaciji kao osnova za odlučivanje da li je neka OP zadovoljena. **Očekivane** komponente **SP i GP** opisuju šta organizacija tipično treba implementirati da postigne zahtevane komponente; implementiraju poboljšanja, koriste se u evaluaciji i moraju biti planirane ili implementirane u procesu, pre odluke da su **SG i GG** zadovoljeni. **Informativne** komponente pomažu razumevanje zahtevanih i očekivanih komponenti. Primeri su: *sub-prakse*, *tipičan proizvod rada*, *pojačanja (amplifikations)*, *elaboracija GP*, *naslovi cilja i praksi*, *napomene uz ciljeve i prakse* i *reference*. Komponente CMMI v.1.2 modela prikazane su na slici Sl. 2.6.4, [20].

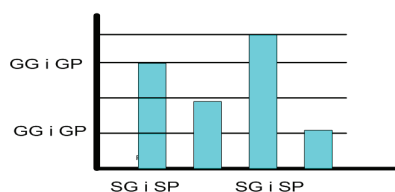


Sl. 2.6.4. Komponente CMMI modela

CMMI model organizuje OP po alfabetskom redosledu. Svaka od 22 OP opisane su u modelu sa svim komponentama modela prikazanim na Sl. 2.6.4. u literaturi [20].

Dimenzija nivoa kapaciteta/zrelosti procesa (CL/ML) je dobro definisani evolucionni put koji opisuje koliko dobro se izvršavaju procesi OP i progres porasta kapaciteta/sazrevanja OP. Model ima 6 CL/ML, ali se 0. nivo nizvršava/izostavlja. Svaki nivo je jedan sloj u temelju za kontinualno poboljšanje procesa. CL/ML su kumulativni, tj. viši nivo CL/ML uključuje attribute nižih nivoa, što znači da u porastu CL/ML ne može biti razmaka.

Generički ciljevi-GG i **generičke prakse-GP** koriste se za realizaciju vrednosti u obe dimenzije (OP i CL) i za evaluaciju procesa. **GG** je uopštena izjava o izlaznom rezultatu kojeg treba dostići sa efektivnom implementacijom pripadajućih GP. **GP** je opis neke akcije koju je neophodno izvršiti da bi se izvršio ključni elemenat (SP) neke OP. GG i GP realizuju dimenziju CL/ML i zato se primenjuju na sve OP (Sl. 2.6.5).



Sl. 2.6.5. Primer CL (GG i GP) profila grupe OP (SG i SP)

Specifični ciljevi (SG) i specifične prakse (SP) realizuju dimenziju procesa modela, pa se zato primenjuju za određene oblasti procesa (OP). Generički ciljevi (GG) i generičke prakse (GP) realizuju dimenziju kapaciteta, pa se zato moraju primeniti na sve OP.

Primer 1: OP-Upravljanje zahtevima (REQM)

SG 1: *Zahtevi su upravljani i identifikovane su nekonzistentnosti sa planovima projekta i proizvodima rada.*

SP 1.4: *Održavanje dvosmernog traga praćenja zahteva.*

Primer 2: OP-Upravljanje zahtevima (REQM)

GG 1: *Implementirani proces postiže specifične ciljeve OP.*

GP 1.1: *Izvršene specifične prakse procesa za upravljanje zahtevima za razvoj proizvoda rada i obezbeđeni servisi za postizanje SG-a OP.*

Oblasti procesa CMMI modela svrstane su u kontinualnoj reprezentaciji (CL) u **kategorije procesa** za: *upravljanje procesom, upravljanje projektom, inženjerstvo i podršku*, a u faznoj reprezentaciji po nivoima zrelosti - ML (Tabela 2.6.2).

Tabela 2.6.2. OP po kategorijama u CL i CM reprezentaciji CMMI modela

Kategorija (CL)	Oblast procesa (OP)	Nivo zrelosti (ML) OP
Upravljanje procesom	Fokusiranje na organizacione procese (OPF)	3
	Definicija organizacionih procesa +IPPD (OPD)	3
	Organizaciona obuka (OT)	3
	Izvršavanje organizacionih procesa (OPP)	4
	Organizacione inovacije i implementacija (OID)	5
Upravljanje projektom	Planiranje projekta (PP)	2
	Kontrola i nadzor projekta (PMC)	2
	Upravljanje sporazumom sa snabdevačem (SAM)	2
	Upravljanje integrisanim projektima + IPPD (IPM)	3
	Upravljanje rizikom (RSKM)	3
	Kvantitativno upravljanje projektom (QPM)	4
Inženjerstvo	Upravljanje zahtevima (REQM)	2
	Razvoj zahteva (RD)	3
	Tehnička rešenja (TS)	3
	Integracija proizvoda (PI)	3
	Verifikacija (VER)	3
	Vrednovanje (VAL)	3
Podrška	Upravljanje konfiguracijom (CM)	2
	Garancija kvaliteta procesa& proizvoda (PPQA)	2
	Merenje i analiza (MA)	2
	Analiza odluka i rešenja (DAR)	3
	Uzročno-posledična analiza i rešenja (CAR)	5

Međusobni odnosi GP i OP, veoma značajni za uzajamno pokrivanje i dopunjavanje, identifikovani su i detaljno opisani u CMMI v.1.2 modelu. Detaljni opis međuzavisnosti GP i OP novi je kvalitet modela, jer doprinosi razumevanju uticaja *implementacije* i *institucionalizacije* određenih GP na sazrevanje nivoa kapaciteta/ zrelosti.

2.6.3. Institucionalizacija procesa u CMMI modelu

Institucionalizacija je koncept koji se najčešće pogrešno interpretira, a od kritičnog je značaja za korišćenje CMMI modela; označava da je proces standardno i duboko ugrađen u organizaciji. Naime, svaka organizacija izgrađuje neku infrastrukturu koja sadrži efektivne, iskoristive i konzistentno primenljive procese. Zavisno od kulture rada, organizacija preuzima te procese u većoj ili manjoj meri, a menadžment treba da neguje i održava tu kulturu rada tako da institucionalizovani procesi traju duže od ljudi koji su ih definisali, uspostavili i institucionalizovali. Sam metod institucionalizacije procesa nije jednostavan, pa je u oceni stepena institucionalizacije procesa, značajnije **kada** se proces smatra institucionalizovanim, nego **koliko** treba da proces postane institucionalizovan. Institucionalizacija je rezultat višekratne implementacije procesa, dok proces ne postane potpuno integrisan i usvojen u organizaciji. Za ocenu institucionalizacije procesa, relevantni su sledeći faktori, [20], [98]:

- raspoloživost procesa i procedura u projektu i organizaciji;
- konzistentnost implementacije procesa i procedura u projektima i organizaciji i
- infrastruktura i povratni mehanizmi za podršku poboljšanja procesa i procedura.

U CMMI modelu GG i GP su gradivni blokovi institucionalizacije i obezbeđuju osnovu za institucionalizaciju procesa organizacije. Koliko kvalitetno i konzistentno su GG i GP izvršene u toj su meri procesi organizacije više institucionalizovani, zato što: doprinose bržoj

institucionalizaciji procesa, pomažu izgradnju infrastrukturne podrške, angažovanje i konzistentnost kroz procese organizacije i primenljive su na sve OP. Stepen institucionalizacije procesa ugrađen je u GG i izražava se imenom procesa koji su pridruženi svakom GG (Tabela 2.6.3).

Tabela 2.6.3. *Stepen institucionalizacije procesa po GG*

Generički cilj i naziv	Progresivno sazrevanje procesa
GG1: Postići specifične ciljeve	Izvršen proces
GG2: Institucionalizuj upravljiv proces	Upravljiv proces
GG3: Institucionalizuj definisan proces	Definisan proces
GG4: Institucionalizuj kvantitativno upravljani proces	Kvantitativno upravljani proces
GG5: Institucionalizuj optimizovan proces	Optimizovan proces

Svaki GG na višem nivou uključuje sva svojstva GG na prethodnom nižem nivou. Na primer, definisan proces uključuje i gradi se na upravljanim procesima i.t.d. U CMMI modelu GG su opisani sa pripadajućim GP. Zbirni prikaz GG i pripadajućih GP koje ukazuju na stepen institucionalizacije dat je u Tabeli 2.6.4, [20].

Tabela 2.6.4. *Zbirni prikaz GG i pripadajućih GP CMMI v.1.2 modela*

Generički ciljevi-GG	Generičke prakse-GP
GG1: Postići specifične ciljeve	GP1: Izvrši specifične prakse
GG2: Institucionalizuj upravljani proces	GP 2.1: Uspostavi politiku organizacije GP 2.2: Planiraj proces GP 2.3: Obezbedi resurse GP 2.4: Pripisi odgovornosti GP 2.5: Obuči korisnike GP 2.6: Upravljaj konfiguracijom GP 2.7: Identifikuj i uključi relevantne učesnike GP 2.8: Monitoriši i kontroliši proces GP 2.9: Objektivno evaluiraj sprovođenje GP 2.10: Revidiraj status sa višim nivoom menadžmenta
GG3: Institucionalizuj definisan proces	GP 3.1: Uspostavi definisan proces GP 3.2: Sakupi informacije o poboljšanju
GG4: Institucionalizuj kvantitativno upravljani proces	GP 4.1: Uspostavi kvantitativne ciljeve za proces GP 4.2: Stabilizuj izvršavanje sub-procesa
GG5: Institucionalizuj optimizovan proces	GP 5.1: Obezbedi kontinualno poboljšanje procesa GP 5.2: Koriguj glavne uzroke problema

Poboljšavanje procesa na bazi CMMI modela pomaže organizaciji da: poboljša zrelost ili kapacitet procesa, uspostavi prioritete i implementira poboljšavanja procesa. Nivoi kapaciteta/zrelosti u CMMI modelu opisuju evolutivni put poboljšavanja procesa organizacije za razvoj i održavanje proizvoda i servisa. CMMI podržava dva puta poboljšavanja procesa: *kontinualni*, koji inkrementalno poboljšava procese po izboru i *fazni*, koji poboljšava skup procesa (OP) sa prethodnog nižeg nivoa zrelosti.

2.6.4. Osnove SCAMPI metoda evaluacije

Glavni principi SCAMPI v. 1.2 metoda evaluacije su, [98]:

1. Upoređuje postojeće procese organizacije prema referentnim u CMMI modelu;
2. Evaluira procese u cilju razumevanja kapaciteta i zrelosti i

3. Odlučuje da li se prakse i procesi izvršavaju na osnovu adekvatnosti dizajna, specifikacije, integracije, implementacije i institucionalizacije praksi i procesa organizacije u odnosu na model.

SCAMPI v. 1.2 metod koristi ostale opšte principe za poboljšavanje procesa organizacije: sponzorstvo glavnog menadžmenta; fokusiranje na poslovne ciljeve; obezbeđenu poverljivost za intervjuisane zaposlene i sakupljene podatke; kolektivni pristup TE procesu evaluacije i fokusiranje na akcioni plan za poboljšavanje procesa.

Za potrebe evaluacije SCAMPI metod koristi *očekivane komponente* - GG, GP i SP CMMI modela, koje određuju obim projekta evaluacije. Zbirni pregled GG (55), GP (189) i SP (826) za potrebe SCAMPI modela evaluacije, [63], [84] ukazuje na težinu problema i obim SCAMPI evaluacije. GG i GP su kritične za proces evaluacije. Subprakse (2-10 po SP) sadrže informativni materijal koristan za razumevanje značenja specifičnih praksi (SP), pa je u procesu evaluacije krajnje nepraktično očekivati sakupljanje dokaza za tako veliki broj subpraksi.

SCAMPI metod evaluacije ne zahteva izričito da proces evaluacije vode ovlašćeni evaluatori, ali se to očekuje da bi se sprečio sukob interesa i zadržao neophodan nivo objektivnosti. SCAMPI A metod evaluacije moraju voditi osposobljeni i (SEI) ovlašćeni *Vodeći SCAMPI evaluatori*. Radni materijal SCAMPI metoda obuhvata: *ARC, MDD, upitnik zrelosti, upitnik za intervju i formulare za evaluaciju*. Rezultat evaluacije procesa obezbeđuje profil nivoa rangiranja zrelosti/kapaciteta procesa organizacije i obuhvata sva pozitivna iskustva iz ranijih modela i metoda evaluacije. SCAMPI metod obezbeđuje detaljnu definiciju metoda (MDD) i uputstvo za implementaciju: jasnu podršku, konzistentnost, ponovljivost i organizovani centar za efikasno korišćenje na terenu, [100].

Strategija poboljšavanja evaluiranih procesa SCAMPI metodom obuhvata:

- **sakupljanje** integrisanih podataka sistemom *upitnika* i neprekidnu konsolidaciju;
- **određivanje prioriteta** za istraživanje *intervjuom*, na bazi podataka iz *upitnika*;
- **analizi usklađenosti** i nivoa pokrivanja praksi organizacije u odnosu na model i
- **verifikaciju** objektivnih dokaza, sakupljenih na lokaciji evaluacije.

Klase SCAMPI metoda evaluacije razlikuje se po stepenu rigoroznosti primene metoda. Klasa A je najzahtevnija u pogledu praćenja SCAMPI metoda i CMMI modela, klasa B je neznatno manje zahtevna i rigorozna, a klasa C najmanje zahtevna i rigorozna. U **Prilogu 2.6A** u Tabeli 1. date su neke očekivane razlike sve tri klase, [100], [118].

Izbor određene klase SCAMPI metoda evaluacije u najvećoj meri zavisi od strategije evaluacije i poboljšavanja procesa organizacije. Moguće su tri strategije:

1. Za iniciranje programa poboljšavanja procesa organizacije koristiti SCAMPI B evaluaciju, identifikovanjem većine slabosti u odnosu na CMMI model i planiranjem procesa poboljšavanja na tim slabostima. Periodično primenjivati SCAMPI C evaluaciju za merenje progressa poboljšavanja procesa u odnosu na plan i za određivanje spremnosti organizacije za narednu evaluaciju klase B ili A.
2. SCAMPI C evaluaciju koristiti na podskupu OP organizacije, zasnivanom na oblasti poslovanja ili veličini projekta. Plan poboljšavanja procesa bazirati na agregaciji otkrivenih slabosti. Pošto je klasa C evaluacije manje detaljna, slabosti pripisati celoj organizaciji, a ne samo podskupu OP u kojem su otkrivene. Posle 6 ili 12 meseci izvršiti evaluacija klase B za procenu progressa poboljšavanja procesa u odnosu na plan evaluacije i odrediti spremnost za evaluaciju klase A.
3. Za inicijalno poboljšavanje procesa organizacije koristiti klasu A evaluacije. Plan poboljšavanja bazirati se na identifikovanim slabostima. Evaluacija klase B može se izvršiti posle 6 ili 12 meseci u odnosu na plan poboljšavanja procesa, da bi se odredila pogodnost za drugu evaluaciju klase A i zvanično rangiranje profila nivoa procesa organizacije.

U većini situacija preporučuje se treća strategija zato što se najveći broj slabosti otkrije u klasi A evaluacije i sa najvećim nivoom poverenja, a organizacija, posebno interni članovi TE, najviše nauči kroz formalni proces evaluacije.

Sakupljanje objektivnih dokaza i aktivnosti SCAMPI v.2.1 evaluacije na četiri projekta SE i SwE procesa na terenu prema CMMI v.1.2 modelu do 3. nivoa zrelosti, treba da traju najviše dve sedmice ili 100 časova. TE u fazi rada na terenu prikuplja koraborativne objektivne dokaze za potvrdu pozitivnih izjava iz preliminarog sakupljanja dokaza o implementaciji praksi kroz sistem upitnika. SCAMPI metod evaluacije specifikuje sledeće tipove objektivnih dokaza koji su indikatori implementacije praksi (PII), [100], [118]:

- **direktne artefakte**, opipljive izlazne rezultate implementiranih praksi, n.p.r., *tipični proizvod rada* naveden u modelu,
- **indirektne artefakte**, posledice ili indikacije implementacije praksi i
- **potvrđne izjave**, usmene/pisane koje podržavaju implementaciju praksi, tj., odgovori na upitnik i intervju.

Prva dva tipa dokaza dolaze iz dokumenata, a potvrđne izjave iz intervjua. TE takođe koristi i zabeleške članova tima, sakupljene za specifične prakse OP **Planiranje projekta**. PII ima dve komponente ili dimenzije: **objektivnost dokaza** i **implementacije praksi**. Komponenta objektivnosti dokaza odnosi se na formu objektivnog dokaza, a komponenta implementacije prakse odnosi se na značaj i dokazujuću vrednost objektivnog dokaza za dokazivanje nivoa implementacije prakse. Inicijalni opis PII (PIID) sadrže direktne i indirektne dokaze – proizvode rada koje priprema organizacija i koji demonstriraju kroz dokumentaciju organizacije kako su CMMI prakse implementirane u organizaciji. Razvoj PIID i priprema za evaluaciju nije trivijalan posao i predstavlja dodatni teret za svaku organizaciju. Primer PIID radnog dokumenta prikazan je u **Prilogu 2.6B**.

Izvori objektivnih dokaza za SCAMPI evaluaciju mogu biti:

- **Instrumenti**: upitnik, anketa, imovina organizacije koja odražava dokaz o implementaciji praksi prema CMMI modelu, npr, tabele mapiranja;
- **Prezentacije**: demonstracije alata, pregledi brifinga i sl.;
- **Dokumenta**: politike, procedure i planovi implementacije, el. dokument i sl.
- **Intervjui**: struktuiran, po pozivu, dodatni; lidera projekta, praktičara, korisnika.

SCAMPI metod takođe ohrabruje formiranje **radnih grupa TE** (mini timova) za nezavisno intervjuisanje, koji imaju ovlašćenja da postižu konsenzus o implementaciji prakse u svakom projektu. Ovo je osnovna razlika od prethodnih metoda evaluacije gde se zahtevalo učešće celog TE u vođenju jednog intervjua.

Vrednovanje objektivnih dokaza vrši se na bazi podataka o implementaciji praksi u procesima organizacije, TE (ili tipično mini tim) pripisuju vrednosti – vrednuju svaki dokaz o meri implementacije prakse CMMI modela. Svaka praksa se karakteriše, uglavnom na bazi procene evaluatora, kao, [98], [118]:

- **PI– potpuno implementirana**: direktni artefakt prezentiran, odgovara i podržan sa indirektnim artefaktom, bez uočenih slabosti, za **>85%-100%** dokaza o izvršavanju SP i GP;
- **ŠI–široko implementirana**: direktni artefakt prezentiran, odgovara i podržan sa indirektnim artefaktom ili potvrđnom izjavom, sa **1** ili nekoliko uočenih slabosti, za **>50%-85%** dokaza o izvršavanju SP i GP;
- **DI–delimično implementirana**: nepostojanje direktnog artefakta, i/ili potvrđne izjave; artefakti i potvrđne izjave indiciraju da su neke prakse implementirane, uočena **1** i više slabosti, za **>15%-50%** dokaza o izvršavanju SP i GP;
- **NI– Neimplementirana**: nije zastupljen ni jedan prethodni slučaj, za **>0%-15%** dokaza o izvršavanju SP i GP.

Karakterizacija oblasti procesa na bazi konsenzusa TE, vrši se agregacijom vrednosti podataka za prakse svakog implementiranog procesa na nivou projekta/organizacione jedinice/organizacije. Na sličan način agregiraju se opservacije o snazi i slabostima praksi procesa i formira se osnova za rangiranje nivoa kapaciteta/zrelosti procesa. Ako je potrebno prosuđivanje TE o implementaciji prakse, odluka se donosi na bazi razmatranja kombinacija karakterizacija dokaza o imlementaciji prakse, razloga za karakterizaciju na nivou implementacije i ozbiljnosti slabosti na nivou agregiranog skupa. Pravila za agregaciju PII na nivou organizacije prikazana su u Tabeli 2.6.5.

Tabela 2.6.5. Pravila za agregaciju vrednosti PII

Uslov	Izlaz	Napomena
Svi <i>X</i> (npr, <i>ŠI</i>)	<i>X</i>	Svi slučajevi implementacije imaju iste karakteristike
Svi (<i>ŠI</i> ili <i>PI</i>)	<i>ŠI</i>	Svi slučajevi implementacije karakterisani su sa <i>ŠI</i> ili <i>PI</i>
Neki <i>DI</i> , nema <i>NI</i>	<i>ŠI</i> ili <i>DI</i>	<i>TE</i> je prosudio i izabrao <i>ŠI</i> ili <i>DI</i> na nivou organizacije
Neki <i>NI</i>	<i>NI</i> , <i>DI</i> , ili <i>ŠI</i>	<i>TE</i> je prosudio i izabrao <i>NI</i> , <i>DI</i> ili <i>ŠI</i> na nivou organizacije

Koncept sakupljanja podataka i rangiranja nivoa OP obuhvata: **koraboraciju**, ili da direktne artefakte podržavajuju indirektni artefakti, ili potvrdne izjave iz različitih izvora dokaza; **pokrivanje**, ili da mora imati dovoljno objektivnih dokaza za implementaciju svake prakse, uvidom da postoji barem jedan slučaj implementacije u **1** projektu, barem **1** SP za svaki slučaj implementacije ili $\geq 50\%$ SP i GP za svaki GG OP i svaki projekat da ima barem po **1** koraborativno potvrđen podatak, i **kompletnost dokaza**, ili da je svaki dokaz o implementaciji dovoljno kompletiran sa prikupljenim podacima za objektivnu kategorizaciju dokaza. **Ispunjavanje GG OP** određuje se na osnovu sposobnosti TE da opiše kako skup agregiranih slabosti utiče na konačno rangiranje i kriterijuma:

- sve SP i GP su ocenjene na nivou organizacije kao *ŠI* ili *PI* i
- agregacija slabosti implementacije SP i GP ne utiče značajno na postizanje GG.

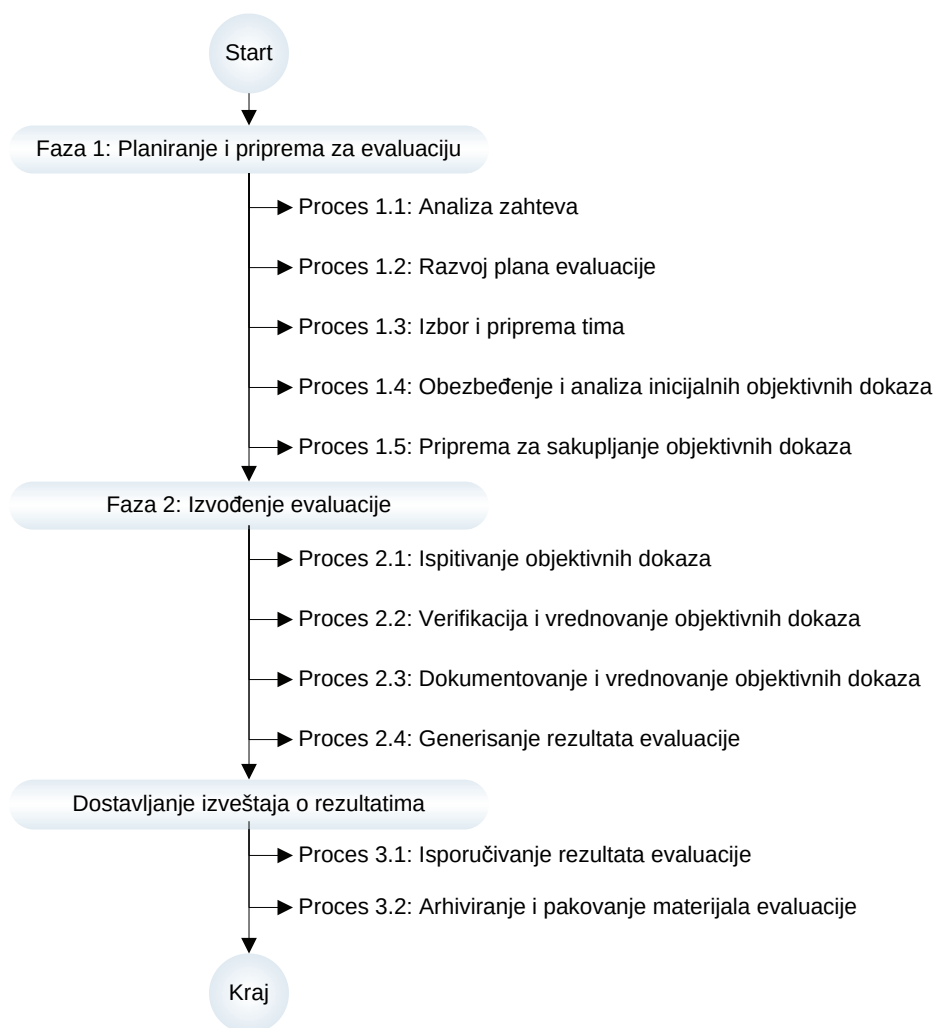
U Tabeli 2.6.6 dati su kriterijumi za rangiranje CL u kontinualnoj reprezentaciji.

Tabela 2.6.6. Kriterijumi za rangiranje CL u kontinualnoj reprezentaciji

CL	Atributi procesa	Rangiranje
1.	Izvršavanje procesa	<i>ŠI</i> ili <i>PI</i>
2.	Izvršavanje procesa	<i>PI</i>
	Upravljanje procesom	<i>ŠI</i> ili <i>PI</i>
	Upravljanje proizvodom rada	<i>ŠI</i> ili <i>PI</i>
3.	Izvršavanje procesa	<i>PI</i>
	Upravljanje procesom	<i>PI</i>
	Upravljanje proizvodom rada	<i>PI</i>
	Definisan proces	<i>ŠI</i> ili <i>PI</i>
	Implementiran proces	<i>ŠI</i> ili <i>PI</i>
4.	Izvršavanje procesa	<i>PI</i>
	Upravljanje procesa	<i>PI</i>
	Upravljanje proizvodom rada	<i>PI</i>
	Definisan proces	<i>PI</i>
	Implementiran proces	<i>PI</i>
	Merenje procesa	<i>ŠI</i> ili <i>PI</i>
	Kontrola procesa	<i>ŠI</i> ili <i>PI</i>

Rezultat SCAMPI evaluacije, pored rangiranja CL/ML nivoa je i generisanje nalaza o **snazi** i **slabostima** procesa organizacije. **Snagu** ukupnih procesa organizacije čine konačni nalazi koji indiciraju najbolje implementirane prakse procesa na nivou organizacije, a **slabosti** su nalazi koji sumiraju propuste u implementaciji praksi, tipično na nivou GG i koji ne doprinose individualnim

projektima organizacije. Proces SCAMPI evaluacije sadrži 3 faze, 11 (pod)procesa i 43 aktivnosti (Sl. 2.6.6).



Sl. 2.6.6. Faze i procesi SKAMPI metoda evaluacije

2.6.5. Preporuke za primenu SCAMPI v.1.2 metoda evaluacije

1. Organizacija treba da obezbede barem dva projekta (obično 4) za evaluaciju, kao izvor objektivnih dokaza koji reprezentativno pokrivaju životni ciklus procesa u organizaciji. Cilj je držati broj evaluiranih projekata što manjim, [20].
2. *Plan evaluacije* treba da uključi intervjuisanje menadžera za: tehnički razvoj, poboljšavanje procesa, obuku, kontrolu kvaliteta i merenja.
3. U proces evaluacije mogu se uključiti i proizvodi koji su delimično u životnom ciklusu proizvoda.
4. Pokrivanje modela određuje se verifikovanjem i vrednovanjem objektivnih dokaza, pregledom artefakata i potvrdnih saopštenja za svaku praksu (SP/GP).
5. Implementacije praksi modela karakterišu se na bazi implementacije SP i GP, a subprakse služe za utvrđivanje stepena implementacije praksi.
6. Tipični proizvodi, amplifikacije discipline i elaboracije GP, uključuju se u ocenu stepena implementacije praksi, gde i kada je to potrebno.
7. Prema proceni SEI, za SCAMPI A evaluaciju 24 OP do 5 nivoa CL/ML, potrebno je za TE od 6 članova 13 dana sa radom od 8 i više časova dnevno.

8. U Tabeli 2. u **Prilogu 2.6A** date su približne procene potrebnog broja relevantnih učesnika koje treba intervjuisati, vremena i broja intervju a i ukupnog vremena za evaluaciju procesa, uključenog u sve tri CMMI modelom obuhvaćene discipline.
9. Cilj CMMI modela je da naknadnih intervju a uopšte nema, ali je dobro planirati po 2 sata za naknadne intervju e, za 4 lica sa ukupno 8 sati rada TE.
10. Vodeći evaluator interpretira CMMI SP i GP prakse kao očekivane, a odluku o tome da li je neka alternativna komponenta prihvatljiva donosi TE konsenzusom,.
11. **Institucionalizaciju** OP u CMMI modelu vodeći evaluator interpretira kao zadovoljenje zahteva GG (generičkih ciljeva).
12. Dokumentovane procedure procesa nisu „očekivane“, niti „zahtevane“ komponente procesa u CMMI. Termini **uspostavi i održavaj** uključuju dokumentaciju i korišćenje komponenti u celoj organizaciji.
14. SAM OP se ne primenjuje na proizvode koji se ne isporučuju za projekat kupca, (n.p.r., neisporučeni razvojni alati), ali se primenjuje na isporučio ca komercijalnih proizvoda, ako se njegov proizvod isporučuje za projekat evaluacije.
16. Minimalan sadržaj *skupa standardnih procesa - OSSP* mora pokriti procese za inženjering, menadžment, podršku SE i organizacione aktivnosti ako se evaluira softver. *Definicija procesa organizacije - OPD* obezbeđuje specifične informacije o definisanju procesa, kako proces može biti definisan i što TE treba da razmatra.
18. Sve procese definisane projektom treba smatrati alternativnim procesima.
19. Za projekte evaluacije koji zahtevaju specijalnu bezbednosnu proveru TE sa Sponzorom potpisuje NDA ugovor, a svi članovi TE imaju bezbednosnu proveru.
20. U modelu ne postoji jedinstvena lista za zahtevane metrike za svaku OP; zahteva se samo dovoljno metrike za potrebe svakog nivoa CL/ML, definisane u okviru procesa, projekta i organizacije, a ne u okviru OP modela.

GP - Sakupljanje informacija za poboljšanje procesa obezbeđuje ulaz u nekoliko praksi OPF i OPD OP. Nema jasne specifikacije minimuma informacija koje treba sakupiti, ali su tipovi sakupljenih informacija definisani u modelu.

2.7. Komplementarnost standarda kvaliteta procesa

2.7.1. Uvod

U praksi zaštite potvrdilo se da gotovo ni jedan model procesa, ili standarda zaštite sam za sebe nije dovoljan za rešavanje većine potencijalnih problema u zaštiti. Međutim, brojni modeli i standardi imaju konzistentne i kompatibilne 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, orijentisanih bilo na sisteme zaštite, procese zaštite ili okruženje, utvrditi prednosti i nedostatke za *konkretne uslove primene i okruženja* i na taj način olakšati korisnicima izbor adekvatnih standarda i modela za rešavanje problema zaštite u realnom kontekstu i okruženju konkretne organizacije, umesto, po pravili najskupljih rešenja „dobrih“ ili „najboljih“ praksi namenjenih za „*tipične organizacije*“ i „*tipična okruženja*“. Sa aspekta kvaliteta procesa zaštite, od posebnog značaja je izbor što bržih, jeftinijih, nedestruktivnih i dovoljno efektivnih metoda za merenje zrelosti, evaluaciju i poboljšavanje procesa IKT zaštite.

Standard **ISO/IEC 15504 - Okvir za merenje procesa**, koji koristi dimenzije procesa i kapaciteta i podržava sve vrste procesa, u velikoj meri je kompatibilan sa SSE CMM modelom. Relevantni standardi za upravljanje sistemom zaštite ISO/IEC 17799, [49], ISO/IEC 13335, [55] i brojni NIST standardi zaštite za federalni IKT sistem SAD, [69] [70], [71], [72], [73], [74], [75] u velikoj meri su kompatibilni sa procesno orijentisanim modelima sazrevanja proces - SSE CMM i CMMI, posebno u oblasti SSE procesa.

2.7.2. Komplementarnost SSE CMM i drugih standarda zaštite

U **standardu ISO/IEC 15504**, na bazi procene specifičnih faza procesa, osnovne oblasti praksi podeljene su na: *organizzazione, upravljачke, inženjerske, klijentsko-slabdevačke i procese za podršku*. Standard specificira 6 nivoa kapaciteta procesa organizacije, [51]:

1. **L0**: nekompletan proces,
2. **L1**: izvršen proces,
3. **L2**: upravljаn proces,
4. **L3**: uspostavljen proces,
5. **L4**: predvidljiv proces i
6. **L5**: optimizovan proces.

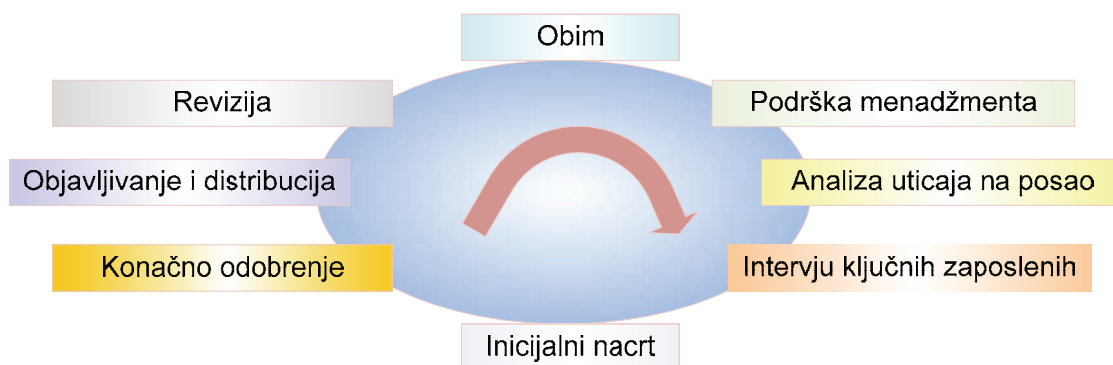
Primenljiv je za: *samo-procenu, nezavisnu, neprekidnu i diskretnu procenu*. Nivo L3 odgovara **ISO 9000** sertifikatu. Kompatibilnost sa **SSE CMM** data je u Tabeli 2.7.1.

Tabela 2.7.1. Kompatibilnost SSE CMM i ISO/IEC 15504

SSE CMM 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: Upravljаn 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 resirse GP 2.1.2: Pripisi odgovornosti GP 2.1.5: Obezbedi obuku	OP 3.2: Atribut resursa procesa
CF 3.3: Kkordiniranje prakse zaštite	Nema direktnog ekvivalenta
Nivo kapaciteta 4: Kvantitativno kontrolisan	Nivo 4: Predvidljiv proces
CF 4.1: Uspostavljenje 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

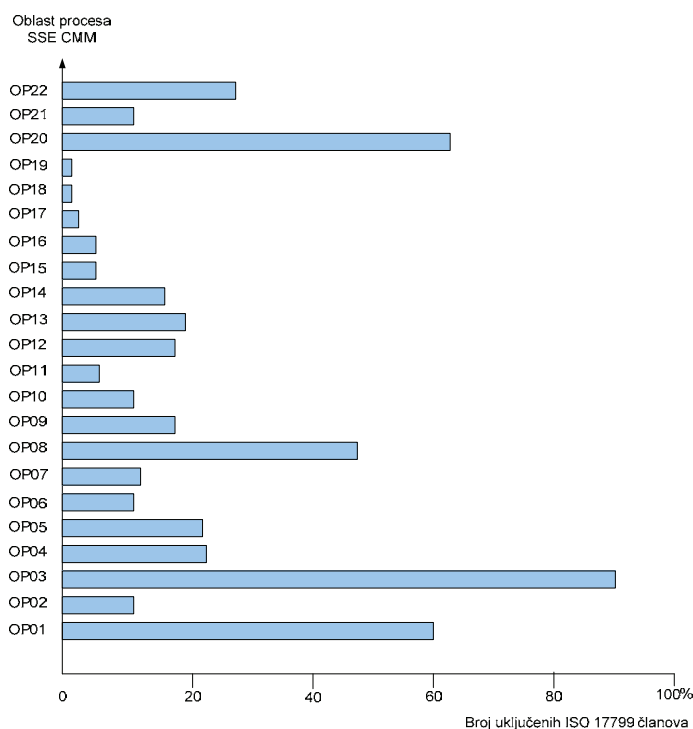
NIST okvir za procenu nivoa bezbednosti federalnog IKT sistema SAD, prevashodno namenjen za razvoj životnog ciklusa politike IKT zaštite, (Sl. 2.7.1), obuhvata pet nivoa efektivnosti programa zaštite,[73], [12]:

1. dokumentovana politika
2. dokumentovane procedure
3. implementirane procedure i kontrole
4. testirane i revidirane procedure i kontrole
5. potpuno integrisane procedure i kontrole zaštite



Sl. 2.7.1. Razvoj životnog ciklusa politike zaštite

ISO/IEC 17799 standard zaštite u kombinaciji sa SSE CMM modelom sazrevanja procesa formira metodologiju vektora zaštite (**S-vektora**) za menadžment zaštite *web* aplikacija, koja je još u fazi razvoja. Najšire prihvaćeni standard za upravljanje zaštitom, ISO/IEC 17799, obuhvata skup upravljačkih, operativnih i tehničkih *kontrola zaštite*, kao i instrukcije o tome **šta** treba uraditi u IKT zaštiti i kako formirati politike zaštite, ali ne sadrži nikakvu metriku zaštite. **SSE CMM** model procesa najbolje prakse zaštite, ne sadrži nikakvu metodologiju niti kontrole zaštite, ali poseduje dobru, sistemski i procesno orijentisanu metriku. U razvoju metodologije S-vektora ova dva standarda pokazala su veliki stepen kompatibilnosti. Na **bar** dijagramu (Sl. 2.7.2) data je procena korelacije OP SSE CMM modela i uključenih članova ISO/IEC 17799 standarda, [10], [42], [104].



Sl. 2.7.2. Korelacija OP SSE CMM i uključenih članova ISO/IEC 17799 standarda

Rezultati jasno indiciraju da su prvih 11 SSE OP SSE CMM modela najbolje pokrivene sa ISO/IEC 17799 standardom, dok su projektna i organizaciona OP slabije pokrivene sa ISO/IEC 17799. Od SSE OP najbolje su pokrivene sa ISO/IEC 17799: *Administriranje kontrola zaštite*, *Koordinacija sistema zaštite* i *Nadzor i kontrola sistema zaštite*. OP – *Obezbeđenje bezbednosnog ulaza* predstavljena je prilično dobro, a OP iz oblasti upravljanja rizikom: *Procena uticaja*, *Procena bezbednosnog rizika*, *Procena 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 koriste ISO/IEC 17799 model imaju povećan

rizik. SSE CMM model sazrevanja procesa zaštite komplementaran je i sa drugim relevantnim standardima zaštite ISO/IEC 13335 i NIST standardima (Tabela 2.7.2), [42], [55], [75].

Tabela 2.7.2. Komplementarnost SSE CMM, ISO/IEC 17799, ISO/IEC 13335 i NIST

SSE CMM	ISO/IEC 17799	ISO/IEC 13335	NIST HANDBOOK
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&A 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

SSE-CMM model sazrevanja procesa zaštite u nekim oblastima poklapa se i sa **CC** standardom (**ISO/IEC 15408**) opštih kriterijuma za evaluaciju proizvoda i sistema zaštite. **SSE CMM** meri zrelost i kapacitete neke organizacije za izvršavanje procesa zaštite, pretpostavljajući da dobar metod sa zrelim procesima i kapacitetima proizvodi dobar proizvod i sistem zaštite. SSE CMM model nije toliko fleksibilan kao **CC** standard, jer ne preporučuje specifičnu metodologiju, kontrole zaštite, ili uputstva za zaštitu, ali zato ima dobru *sistemske* i *procesno orijentisanu* metriku. Kako proces sazreva postaje formalno sve bolje dokumentovan, definisan, merljiv, kontrolisan, ponovljiv i institucionalizovan, odnosno, zreliji i stabilniji, a zbog toga predvidljiviji, ponovljiviji, lakše kontrolisan i efektivniji u pogledu troškova, produktivnosti, kvaliteta i korisničke prihvatljivosti. SSE CMM model meri zrelost procesa, a ne kvaliteta izlaza tih procesa. Kratak pregled ključnih atributa različitih metoda za evaluaciju sistema zaštite prikazan je u Tabeli 2.7.3, [10], [104], [43], [49], [78], [107].

Tabela 2.7.3. Zbirni pregled metoda za procenu sistema zaštite

Kategorija	Metod bezbednosne procene				
	S-vektor	CC	COBRA	OCTAVE	SSE CMM
Status	Istraživanje u toku	Uspostavljen razvojni standard	Dostupan komercijalni proizvod	Dokumentovana metodologija sa raspoloživom obukom	Dokumentovana metodologija sa raspoloživom obukom
Nivo analize	Aplikativni nivo	Nivo tipične systemske komponente (npr., firewall, OS, DBMS), ili bezbednosno specifična aplikacija	Ceo sistem	Ceo sistem	Ceo sistem
Usmerenost	Menadžer-ske potrebe	Ispunjava CC profil zaštite	Najbolja praksa	Najbolja praksa	Najbolja praksa
Zahtevi, pretnje i procena uticaja	Za primenu na bazi upitnika.	Zahtevi u profilu zaštite. Procena uticaja nije uključena	Za ceo sistem. Auto-matizovan alat na bazi ankete i ekspertske sisteme.	Za klasu kritičnih objekata sistema	Nije uključeno
Tehnički kapaciteti (poverljivost, integritet, raspoloživost)	Brojčani poeni za komponente sa odgovarajućim podskupom korišćenim za svaku aplikaciju	Fiksni PP definisan sa CC ili vendor za svaku klasu komponente sistema.	Uključuje podskup tehničkih kapaciteta implementiranih sa infrastrukturom sistema u celini	Kapaciteti za celu infrastrukturu (hardver, OS, mreža)	Samo indirektno: SSE CMM obuhvata procese koji se koriste za implementaciju i podršku tehničkih kapaciteta
Strukturna zaštita	S-vektor uključuje eksplicitne reference prema relevantnim strukturama	Takva struktura može implicitno uticati na EAL nivoe evaluacije komponenti	Nije uključeno	Nije uključeno	Samo indirektno
Proceduralni metodi: razvoj i testiranje	Uključena kao komponenta S-vektora	Uključena u EAL evaluaciju komponenti	Da	Nije uključena	Da
Proceduralni metodi: upravljanje i upotreba	Uključena kao komponenta S-vektora	Nije uključena	Da	Nije uključena	Da
Nezavisno testiranje	Samo u toku istraživačke faze	Koristi rigorozniju metodologiju TTPS evaluacije	Nije uključeno	Nije uključeno	Samo indirektno

2.7.3. Komplementarnost CMMI i SSE CMM modela procesa

Integrirani model sazrevanja CMMI v.1.2 (2006) obuhvata najbolje prakse za oblasti procesa za: **razvoj, održavanje i akviziciju proizvoda i servise**, uključujući SCAMPI v.1.2 metod za evaluaciju nivoa kapaciteta/zrelosti i poboljšavanje procesa, [67].

SSE CMM v.3 (2003) model i metod procesa zaštite, procesno je orijentisana metodologija za razvoj bezbednog IKT sistema i evaluaciju i poboljšavanje procesa zaštite. Za evaluaciju procesa zaštite posebno je razvijen SSAM metod, [101].

CMMI modeli orijentisani su na procese za razvoj, akviziciju proizvoda i davanje servisa, a procese i prakse zaštite ovi modeli obuhvataju *samo* u meri u kojoj to zahteva svaki projekat i to kroz *OP – Upravljanje rizikom*. Dakle, CMMI model i pripadajući SCAMPI metod evaluacije mogu se primeniti na projekte zaštite, ali nedostaju brojne OP za procese zaštite, razvijene specifično u SSE CMM modelu. Odgovarajuće OP i prakse zaštite u CMMI modelu, distribuirane su na više različitih OP SSE CMM modela, što znači da mapiranje OP SSE CMM i CMMI modela (Tabela 2.7.4) nije jednoznačno i nije lako primeniti OP CMMI modela za razvoj i implementaciju praksi zaštite IKT sistema, [67].

Tabela 2.7.4. Prezentacija uporedivih OP CMMI i SSE CMM modela procesa

CMMI	ISO/IEC 21827 (SSE CMM v.3)
Fokusiranje na org procese (CL3)	Definiši organizacioni SSE proces
Definicija org procesa (CL3)	Poboljšaj org SSE proces
Izvršavanje org procesa (CL4)	Upravlaj okruženjem za podršku SE procesa
Org inovacije i implementacija (CL5)	Upravljanje razvojem proizvodne linije
Organizaciona obuka (CL3)	Obezbedi tekuće veštine i znanja
Planiranje projekta (L2)	Planiraj tehničke napore
Kontrola i nadzor projekta (CL2)	Monitoriši i kontroliši tehničke napore
Upravljanje sporazumom sa snabdevačem (CL2)	Koordiniraj sa snabdevačem
Upravljanje integrisanim projektima (CL3)	Koordiniraj bezbednost
Upravljanje rizikom (CL3)	Upravlaj rizikom projekta
Kvantitativno upravljanje projektom (CL4)	Izgradi argumente bezbednosne garancije
Upravljanje zahtevima (CL2)	Specifikuj bezbednosnim potrebama
Razvoj zahteva (CL3)	Obezbedi bezbednosni ulaz
Tehnička rešenja (CL3)	Verifikuj i vrednuj bezbednost
Integracija proizvoda (CL3)	Administriraj kontrole zaštite
Verifikacija (CL3)	Proceni uticaj
Vrednovanje (CL3)	Proceni bezbednosni rizik
	Proceni pretnje
	Proceni ranjivost
	Monitoriši sistem zaštite
Upravljanje konfiguracijom (CL2)	Upravlaj konfiguracijom
Garancija kvaliteta procesa& proizvoda (CL2)	Obezbedi kvalitet
Merenje i analiza (CL2)	
Analiza odluka i rešenja (CL3)	
Uzročno-posledična analiza i rešenja (CL5)	

Neke OP CMMI i SSE CMM modela se u potpunosti poklapaju, ili se poklapaju u velikom stepenu i sa brojnim praksama i procesima.

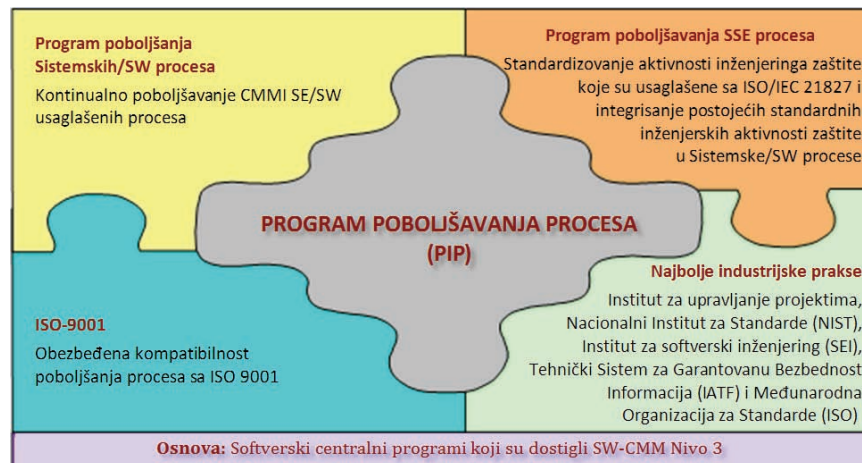
Integracija usklađenih procesa SSE CMM i CMMI v.1.2 modela može obezbediti uspešnu kombinovanu metodu primenljivu u brojnim situacijama:

- **Razvoj procesa:** pomaže uspostavljanje CMMI procesa; SE/SF inženjeri i SSE inženjeri integrišu SSE procese sa sistemskim/softverskim procesima;
- **Implementacija procesa:** inženjer (SSE) procesa zaštite pridružen projektima razvoja sistema/softvera; pomaže implementaciju i institucionalizaciju procesa zaštite u infrastrukturu koju uspostavlja CMMI program;

- **Evaluacija procesa:** bolje dokumentovani i koraborativno potvrđeni objektivni dokazi iz CMMI modela mogu se koristiti u evaluaciji procesa zaštite, u onim OP gde se modeli jednoznačno (ili sa visokim stepenom) preklapaju.

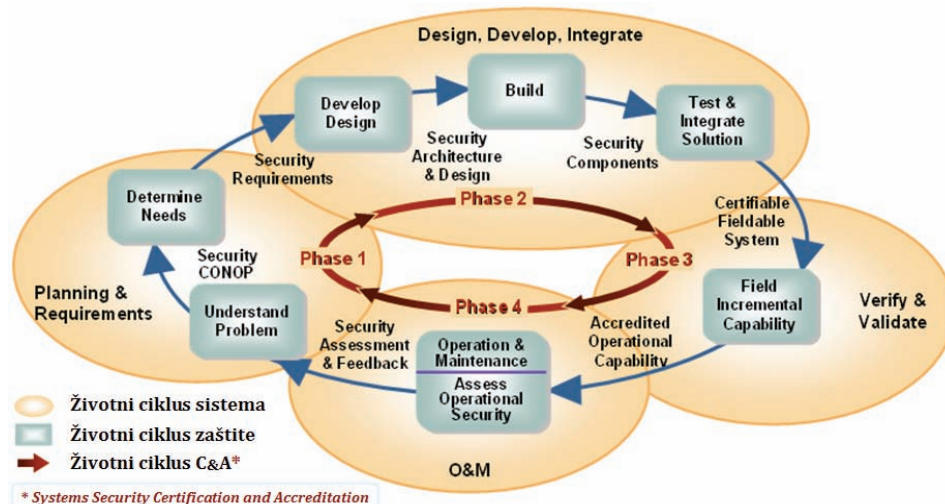
2.7.3.1. Usklađivanje procesa CMMI i SSE CMM modela

Poslovni sistemi sve više zahtevaju primenu CMMI model procesa, jer model obezbeđuje uputstvo i smernice za definisanje, implementaciju i poboljšanje procesa u životnom ciklusu sistema. Brojne organizacije koriste različite standardne za poboljšanje procese – PIP (*Process Improvement Program*) kao dopunu industrijskih standarda kvaliteta proizvoda i procesa (Sl. 2.7.3), [63], [67], [99], [100], [102].



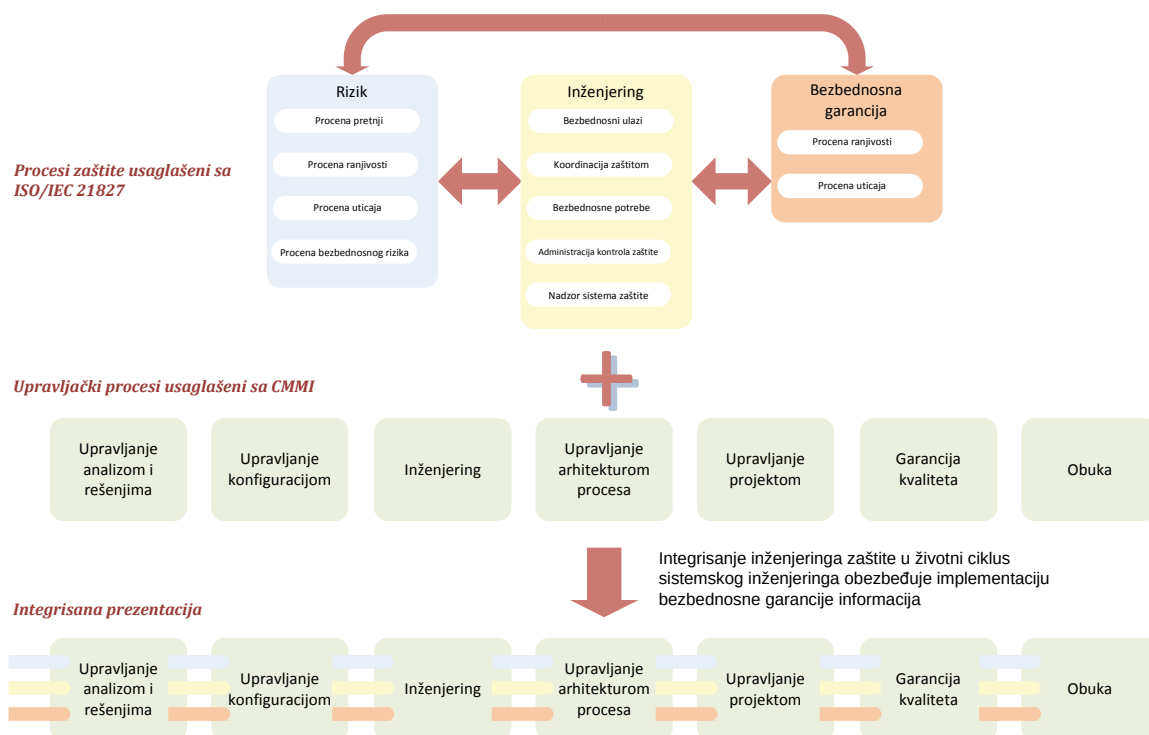
Sl. 2.7.3. Programi za poboljšavanje procesa

Znatno više organizacija koristi CMMI nego SSE CMM model, zbog veće integracije procesa i disciplina i većeg pokrivanja procesa organizacija. Međutim, CMMI tipovi modela imaju ozbiljne propuste u pokrivanju procesa zaštite, gde SSE CMM daje znatno bolje rezultate. U toku 2006/7 sponzori razvoja CMM modela (DoD, NSA i FAA iz SAD) pokrenuli su zahtev da se najbolje prakse zaštite SSE CMM modela kombinuju sa CMMI modelom i integrišu SSE procesi u životni ciklus SE procesa čime se omogućava uspešna implementacija praksi i procesa zaštite informacija CMMI modelom (Sl. 2.7.4).



Sl. 2.7.4. Integracija SSE procesa u životni ciklus SE procesa

Ključni principi metoda integracije međusobno usklađenih procesa SSE CMM i CMMI modela ilustrovani su na slici Sl. 2.7.5.



Sl. 2.7.5. Metod integracije SSE CMM i CMMI procesa

U inicijativi integrisanja procesa i praksi SSE CMM i CMMI modela, predloženo je uključivanje dodatna 4 GG i GP u CMMI specifično namenjene za bezbednost i zaštitu, što je u fazi istraživanja (SEI, NSA, DoD – SAD), [118]. Mapiranje ostalih komponenti CMMI i SSE CMM modela prikazano je u Tabeli 2.7.5.

Tabela 2.7.5. Mapiranje ostalih komponenti CMMI i SSE CMM modela

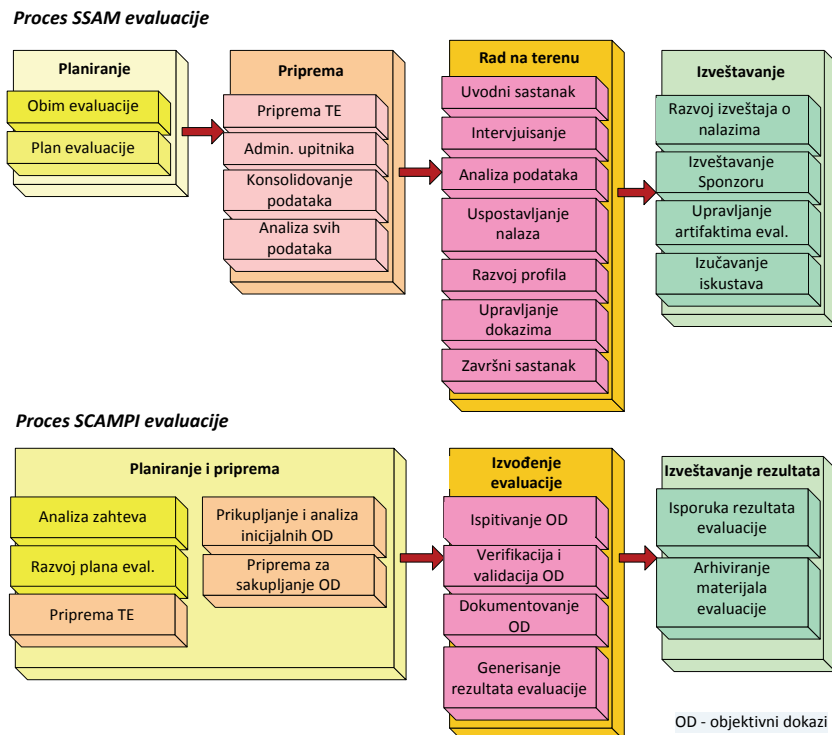
CMMI v.1.2 (2006)	SSE CMM v.3.0 (2003)
Oblast procesa (OP)	Oblast procsa (OP)
Specifična praksa (SP)	Bazična praksa (BP)
Specifični cilj (SG)	Opisan, nije numerisan
Generički cilj (GG)	Nivo kapaciteta (CL)
Nivo kapaciteta/zrelosti (CL/ML)	Nivo kapaciteta/zrelosti (CL/ML)
Uključena u v.1.1, ukinuta u v.1.2	Opšta karakteristika (CF)
Generička praksa (GP)	Generička praksa (GP)
Kontinualna i fazna reprezentacija	Kontinualna i fazna reprezentacija

2.7.3.2. Komplementarnost SSAM i SCAMPI v.1.2 metoda evaluacije

SSAM metod evaluacije namenjen je za evaluaciju i poboljšavanje procesa zaštite u organizaciji, ili projektu i kreiranje/podršku procesa unutar više nivoa strukture organizacije, na bazi referentnog SSE CMM modela procesa zaštite.

SCAMPI v.1.2 metod evaluacije namenjen je za evaluaciju praksi i procesa prema CMMI v.1.2 modelu integrisanih procesa, ali nije dovoljan za evaluaciju procesa zaštite. Međutim, sa predloženim bezbednosnim dodatkom od 4 bezbednosna generička cilja (GG), SCAMPI metod evaluacije moći će se primenjivati za evaluaciju procesa zaštite, što je u fazi ispitivanja (SEI, DoD US), [118].

Procesi SCAMPI i SSAM metoda evaluacije imaju slične izvršne korake, što je prikazano na slici Sl. 2.7.6, [116].



Sl. 2.7.6. Komplementarnost koraka procesa SSAM i SCAMPI metoda evaluacije

Dakle, SSAM metod evaluacije ima za krajnji cilj **poboljšavanje procesa zaštite** prema SSE CMM modelu, a SCAMPI metod evaluacije ima za krajnji cilj **poboljšavanje procesa** za proizvodnju, akviziciju, ili servise prema CMMI modelu sazrevanja procesa. U oba procesa **poboljšavanja procesa** kritična su tri sledeća koraka:

1. Izgradnja jake podrške organizacije i menadžmenta;
2. Uspostavljanje jakog, tehnički kompetentnog TE od relevantnih učesnika i
3. Planiranje poboljšavanja procesa na bazi modela za implementaciju CMM procesa, kao što je IDEAL (*Initiating, Diagnosing, Establishing, Acting and Learning*), SEI instituta, Sigma 6 i sl.

Na program poboljšavanja procesa mogu uticati **tri** tipa izbora:

1. Dela organizacije (projekta, procesa) za poboljšavanje;
2. Modela (SSE CMM, CMMI) za poboljšavanje procesa;
3. Reprezentacije modela: **kontinualne**, **fazne** ili **kombinovane**.

SSE CMM i CMMI modeli opisuju **najbolje prakse**, koje neka organizacija može primeniti u predmetnoj oblasti za postizanje svojih poslovnih ciljeva. Sve OP i prakse koje neki model (SSE CMM/CMMI) obuhvata, svaka organizacija treba da profesionalno proceni u kontekstu svojih uslova, potreba i poslovnih ciljeva. Kad se počne koristiti model (SSE CMM/CMMI) za poboljšavanje procesa, potrebno je da organizacija mapira svoje realne procese sa OP primenjenog modela (SSE CMM/CMMI). Na taj način organizacija u realnom kontekstu procenjuje usklađenost svojih procesa sa OP primenjenog modela i identifikuje procese koje je potrebno poboljšavati.

Kod interpretacije implementiranosti praksi prema modelu, važno je razmotriti ukupan kontekst u kojem se ove prakse primenjuju i odrediti koliko dobro prakse u tom kontekstu zadovoljavaju generičke ciljeve OP modela. Dakle, SSE CMM i CMMI modeli **ne propisuju eksplicitno procese, niti impliciraju da su određeni procesi potpuno adekvatni za svaku organizaciju, ili projekat**. CMM modeli procesa opisuje minimalne kriterijume, neophodne za planiranje i

implementaciju procesa koje organizacija izabere za poboljšavanje, na bazi poslovnih potreba i ciljeva. Zato za adaptaciju specifičnih potreba određene organizacije, CMM modeli procesa namerno koriste izraze kao što su: *relevantni učesnici, kako odgovara i kako je potrebno*, [116].

Kratak uporedni pregled SSE CMM modela sazrevanja procesa zaštite i drugih standarda i modela za poboljšavanje nivoa bezbednosti IKT sistema dat je u Tabeli 2.7.6.

Tabela 2.7.6. *Uporedni pregled SSE CMM i drugih modela IKT zaštite*

Model	Cilj	Pristup	Obim	Status
SSE CMM	Definiše, poboljša i proceni SSE kapacitete	Kontinualni/fazni SSE model sazrevanja i metod evaluacije	SSE organizacije	v.3.0
SE-CMM	Poboljša SE process sistema ili proizvoda	Kontinualni CMM model sazrevanja SE praksi i metod evaluacije	SE organizacije	Videti EIA 731
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 sw 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	Poboljšava bezbednost obezbeđujući višekratno korišćeni profil zaštite (PP) za tehnološke klase	Skup funkcionalnih i bezbednosnih zahteva za zaštitu, sa procesom evaluacije (EAL nivoi)	IKT sistemi	V.2.0
Okvir za merenje procesa zaštite	Poboljšava garantovanu bezbednost sistema, obezbeđujući širok opseg dokaza (argumenata)	Struktuiran pristup za kreiranje argumenta bezbednosne garancije 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 sw i sve druge procese	Sw CMM model i metod evaluacije	SwE organizacije	Svih 9 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 5 delova.

2.7.3.3. Komplementarnost CMMI modela i ISO 9000 standarda

Za evaluaciju usaglašenosti sa ISO 9001, izdato je uputstvo ISO 9000-3 za primenu ISO 9001 standarda za razvoj, snabdevanje i održavanje softvera, čime se izbegla konfuzija i teškoće primene ISO 9001. ISO 9000-3 sadrži 22 člana specijalno napisana za razvoj softvera i mapirana sa aktuelnim ISO 9001 standardom koji sadrži 20 članova. Iako su ovi članovi više specifični za softver, još uvek su dovoljno uopšteni, zahtevaju dalju interpretaciju za primenu i **ne obuhvataju zaštitu IKT sistema**. Treba primetiti da je ISO 9000-3 uputstvo ograničeno na softverske, dok su ISO 9001 i CC primenljivi za hardverske i softverske proizvode i sisteme, [116].

Integrisani modeli procesa u brojnim slučajevima preklapaju se sa elementima ISO 9001:2000 standarda za razvoj, snabdevanje i održavanje softvera (Tabela 2.7.7).

Tabela 2.7.7. Mapiranje ISO 9001 prema CMMI modelu procesa

Sekcija	Naslov u ISO 9001	Generičke prakse, OP CMMI
4	Sistem upravljanja kvalitetom	
4.1	Opšti zahtevi	OPF, OPD
4.2	Zahtevi za dokumentaciju	OPF, OPD, CM, GP 2.6
5	Odgovornost menadžmenta	
5.1	Angažovanje menadžmenta	GP 2.1
5.2	Fokusiranje na kupca	RD, GP 2.7
5.3	Politika kvaliteta	OPF, GP 2.1
5.4	Planiranje	OPF, OPD, OPP, GP 2.2
5.5	Odgovornost, ovlašćenja i komunikacije	GP 2.4
5.6	Revizija upravljanja	OPF, PMC, GP 2.10
6	Upravljanje resursima	
6.1	Obezbeđivanje resursa	GP 2.3
6.2	Ljudski resursi	OT, IPM+IPPD, GP 2.3
6.3	Infrastruktura	IPM+IPPD
6.4	Radno okruženje	IPM+IPPD, PP
7	Realizacija proizvoda	
7.1	Planiranje realizacije proizvoda	OPD, PP, IPM+IPPD, GP 2.2
7.2	Procesi koji se odnose na kupce	REQM, RD, TS, VER
7.3	Dizajniranje i razvoj	PP, PMC, CM, IPM+IPPD, RD,TS, PI, VER,VAL
7.4	Kupovanje	SAM, TS, ISM
7.5	Obezbeđivanje proizvodnje i servisa	RD, TS, PI, VAL, CM
7.6	Kontrola i nadzor mernih uređaja	VER, VAL, MA
8	Merenje, analiza i poboljšavanje	
8.1	Uvod	MA, QPM
8.3	Kontrola neadekvatnosti proizvoda	MA, PMC, PPQA, OPF, OPD, VAL, VER
8.4	Analiza podataka	CM, PMC, MA, RD, QPM, GP 3.2
8.5	Poboljšavanje	PMC, MA, OPF, CAR

Iz Tabele 2.7.7 očigledno je da postoji značajna sličnost između dva modela, ali se vide i elementi sa boljim pokrivanjem i sa više detalja u jednom, ili drugom modelu. Generalno, organizacija čiji procesi zadovoljavaju CMMI model, zadovoljiti će i ISO 9001:2000 standard za ispunjavanja ciljeva i praksi sistema kvaliteta organizacije.

2.7.3.4. Komplementarnost CMMI i agilnih metoda za evaluaciju procesa

Agilni metodi obezbeđuju alate za usmereni razvoj procesa i proizvodnju samo fundamentalnih i najkritičnijih komponenti. Razmišljanja o agilnim procesima počeli su sa bržim promenama na tržištu i zahtevima za brže isporuke proizvoda (n.p.r., softvera), koje korisnici prilagođavaju u toku operativne primene i prakse, nastojeći da pri tome izvrše maksimalno ažuriranje ranjivosti u minimalnom vremenu, [3], [5].

Za razliku od agilnih metoda, svi modeli sazrevanja proocesa (CMM tipa) obezbeđuju **sistematsko poboljšavanje procesa**. Agilne metode pojavile su se kao reakcija na ove, relativno spore sistematske procese poboljšavanja, pokušavajući da naprave kompromis između stanja "bez procesa" i stanja sa "mnogo procesa" i obezbede baš onoliko procesa koliko je potrebno da se dobije razuman balans proizvodnog ciklusa i povratka investicija (investicija/dobit). Proizvođači

smatraju da kraće vreme isporuke nesavršenog proizvoda omogućava da korisnici sami utiču na promenu vrednosnih kriterijuma proizvoda. Naravno, brojne su kritike agilnih metoda za proizvodnju softvera, počevši od toga da je to samo izgovor za uspešno „hakerisanje“ softverskih proizvoda, do toga da takvi proizvodi ne mogu podržati kompleksne arhitekture IKT i sistema zaštite, niti rad sa distribuiranim timovima i slično. Atributi agilne metodologije za proizvodnju softvera uključuju tipično:

- što pre i što češće isporučivati funkcionalan, validan softver,
- meriti progres primarno za funkcionalni softver,
- proizvođači i programeri treba da dnevno rade zajedno,
- podsticati slanje zahteva za izmene,
- kreirati samo-organizujuće timove motivisanih pojedinaca,
- komunicirati ličnim kontaktom,
- izbegavati nebitan rad,
- održavati prihvatljiv korak razvoja,
- neprekidno raditi sa dobrim projektima i
- regularno kontrolisati i podešavati procese.

Generalno, agilni metodi povećavaju individualne napore i interakcije u procesima poboljšavanja proizvoda i primeni softverskih alata. Što projekat postaje složeniji i obimniji, agilni metodi su manje primenljivi i CMM pristupi koji podrazumevaju planski razvoj i isporuku, postaju prihvatljiviji. Ukratko, CMM modeli mogu se primenjivati na veću klasu poslova za proizvodnju softvera. U tom smislu, SSAM i SCAMPI metodi evaluacije, koji se zasnivaju na SSE CMM i CMMI modelima, moraju se prilagoditi za evaluaciju procesa koji koriste agilnu metodologiju razvoja.

2.8. Primene modela sazrevanja procesa zaštite

2.8.1. Uvod

Model sazrevanja procesa zaštite - SSE CMM (ISO/IEC 21827) obezbeđuje uputstvo za definisanje, implementaciju i poboljšavanje **procesa zaštite** u životnom ciklusu sistema. **SSE** procesi obuhvataju tri opšte grupe procesa: **SE procese**, **procese za analizu rizika** i **procese za bezbednosnu garanciju** (*assurance*). SSE CMM definiše zahteve za procese i obezbeđuje *metodologiju* za evaluaciju SSE kapaciteta organizacije, za koju je razvijen poseban *metod* za evaluaciju – SSAM.

Korišćenje SSE CMM modela pomaže organizaciji da izgradi SSE procese u okviru razvoja programa zaštite za životni ciklus sistema. Izgradnja sistema IKT zaštite je tekući proces koji zahteva tekuću analizu pretnji, periodičnu evaluaciju sistema zaštite i stalno poboljšavanje procesa zaštite. SSE CMM model obuhvata SSE aktivnosti koje pokrivaju ceo životni ciklus proizvoda/sistema/servisa zaštite, uključujući za definisanje koncepta sistema zaštite, analizu bezbednosnih zahteva, projektovanje, razvoj, implementaciju i integraciju, operativni rad, održavanje i odlaganje proizvoda/ sistema/servisa zaštite. SSE CMM se može primeniti na proizvođače i provajdere proizvoda/sistema/servisa zaštite, projektante i integratore sistema zaštite, TTPS provajdere zaštite (poverljive organizacije koje obezbeđuju servise zaštite), [108] i SSE rešenja zaštite [37], kao i na sve tipove i veličine organizacija, kao što su komercijalne, državne i akademske.

Bezbednosni ciljevi primene SSE procesa zaštite mogu biti različiti: razumeti bezbednosni rizik; uspostaviti izbalansiran skup bezbednosnih zahteva na bazi identifikovanog rizika; prevesti bezbednosne potrebe u uputstva i politike zaštite; integrisati napore različitih disciplina i specijalnosti; opisati konfiguraciju sistema i operacija; odrediti da li je prihvatljiv operativni

uticaj preostalog rizika; uspostaviti poverenje, ili bezbednosnu garanciju u efektivnost i korektnost kontrola zaštite i dr.

SSE CMM model zahteva da organizacija uspostavi procese na bazi *najbolje prakse zaštite* koju definiše SSE interesna zajednica. Zatim, organizacija meri usklađenost sa SSE CMM nivoima zrelosti i kapaciteta procesa i povećava ih u skladu sa raspoloživim resursima i bezbednosnim potrebama. Dakle, SSE CMM definiše zahteve za *procese za razvoj* sistema zaštite, a ne *nivoa poverenja* kao CC i slični modeli, kao i metodologiju za evaluaciju SSE procesa organizacije, [37].

Cilj svakog projekta primene SSE CMM modela u praksi zaštite je, da unapredi SSE procese organizacije u definisanu, zrelu i merljivu disciplinu. SSE CMM model i njegov SSAM metod evaluacije omogućavaju organizaciji da: usmeri investiranje u SSE alate, obuku, definisanje procesa, upravljanje praksom zaštite i poboljšavanje SSE procesa; meri bezbednosnu garanciju (*assurance*), tj. bezbednost sistema na bazi poverenja u zrelost SSE grupe najboljih praksi zaštite i izabere odgovarajućeg TTPS provajdera zaštite i SSE servisa, kroz evaluaciju nivoa zrelosti i kapaciteta njihovih procesa i pridruženog rizika.

2.8.2. Primena SSE CMM modela za razvoj programa zaštite

U praksi zaštite organizacije, koje primenjuju SSE CMM model, u najvećem broju slučajeva žele da ostvare najviši nivo zrelosti (5.), koji je u većini slučajeva nedostižan i nepotreban za sve OP zaštite. Zbog finansijskih i drugih ograničenja, kao i objektivno nepotrebnog maksimalnog nivoa zrelosti za sve procese zaštite, organizacija može sama, na osnovu analize faktora rizika, izabrati početni nivo razvoja programa zaštite sa tendencijom progresivnog povećavanja nivoa zrelosti i kapaciteta najvažnijih procesa zaštite, dinamiku dostizanja željenog nivoa zrelosti procesa i kapaciteta za razvoj programa zaštite i dostizanje najvišeg nivoa zrelosti samo za OP koje obezbeđuju kritičnu misiju organizacije. Ovaj koncept **redukuje** generički CMM model koji inherentno teži najvišem (5.), nivou zrelosti procesa, [53], [68], [83].

Osnovna prednost primene SSE CCM modela za razvoj programa zaštite je, što organizacija objektivno ne zahteva isti nivo zrelosti za sve procese zaštite, a 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 IKT zaštite obezbeđuje se:

- poverenje da organizacija realizuje program zaštite prema *Planu zaštite*,
- planirani razvoj programa zaštite u granicama raspoloživih resursa organizacije i
- metrika za određivanje adekvatnosti komponente zaštite za specifikovani proces.

2.8.2.1. SSE CMM principi za razvoj programa zaštite

SSE CMM generalno obezbeđuje model za: *kontinuitet, ponovljivost, efikasnost i bezbednosnu garanciju* procesa za razvoj komponenti/sistema zaštite. **Glavni koncept** SSE CMM modela za razvoj programa zaštite obuhvata sledeće elementarne principe, [80]:

- *definisane kriterijume* za merenje zrelosti procesa: način izvršavanja, neprekidni nadzor i kontrola, podrška i ponovljivost merenja,
- *progresivno sazrevanje* procesa i kapaciteta: mereno na 5 nivoa, ne uključujući 0. nivo koji indicira ne-izvršen program zaštite,
- *definisan redosled povećavanja zrelosti* procesa i kapaciteta: bez preskakanja nivoa, a na sledećem nivou uvek je veća zrelost kapaciteta,
- *definisan cilj razvoja* procesa i kapaciteta: uvek teže najvišem 5. nivou zrelosti,
- *definisan odziv* sistema zaštite: brži odziv ostvaruje se na višem nivou zrelosti,
- *definisani prioriteti* i redosled izvršavanja aktivnosti i procesa,
- *merenje progressa sazrevanja* procesa i kapaciteta i

- *komplementarnost sa brojnim uputstvima i standardima zaštite: ISO/IEC 17799, ISO/IEC 13325, NIST SP – uputstva, preporuke i standardi i dr.*

2.8.2.2. SSE CMM proces razvoja optimalnog programa zaštite

Proces SSE CMM razvoja optimalnog programa zaštite odvija se u 3 osnovne faze, [73]:

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 procesa i
- identifikacija indikatora iskoristivih za procenu zrelosti kapaciteta procesa zaštite.

Faza 2: Merenje zrelosti i progresu 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,
- progresivno povećavanje zrelosti procesa do željenog nivoa zrelosti programa zaštite,
- **evaluacija** i procena kvaliteta procesa za razvoj programa zaštite, na bazi:
 - procene stepena implementacije standardizovanih glavnih principa zaštite - GAISP (*Generally Accepted Information Security Principles*), [29],
 - SE i procesnog pristupa planiranju, projektovanju i dokumentovanju zaštite,
 - politika i procedura zaštite razvijenih na osnovu rezultata procene rizika,
 - detaljnog plana upravljačkih, operativnih i tehničkih kontrola zaštite,
 - procedura za vanredne događaje i oporavak IKT sistema i dr.

Faza 3: Realizacija programa zaštite:

- obezbeđivanje opšte podrške menadžmenta,
- razvoj svesti o potrebi zaštite,
- razvoj kapaciteta organizacije za implementaciju procesa zaštite, obezbeđivanjem:
 - potrebnih resursa: vreme, novac, ljudi i alati,
 - politika zaštite, koje usmeravaju izvršioce pri donošenju projektnih odluka,
 - procedura i uputstava baziranih na dobroj praksi zaštite,
 - obuke za sticanje neophodnih veština i znanja iz oblasti zaštite,
 - neprekidnog nadzora i kontrole propisnog izvršavanja rada i
 - nadzora i kontrole kvaliteta servisa zaštite.

SSE CMM model definiše 5 nivoa kapaciteta procesa (CL) za razvoj programa zaštite. Glavni kriterijumi za određivanje nivoa CL programa zaštite IKT sistema organizacije, prema zahtevima SSE CMM modela detaljnije su opisani u **Prilogu 2.8A**.

2.8.3. Primene SSE CMM za profilisanje procesa organizacija u zaštiti

SSE CMM je primenljiv na veliki broj različitih IKT organizacija u kojima programeri, provajderi servisa, integratori sistema, sistem administratori i specijalisti zaštite, koji zahtevaju odgovarajuće metode, prakse i procese rada, mogu imati koristi od primene modela, [37]:

1. **Inženjerske organizacije** - Integratori sistema, Organizacije za razvoj aplikacija, Isporučiocu proizvoda zaštite i Poverljivi provajderi servisa zaštite:
 - uštede u radu zbog primene ponovljivih i predvidljivih procesa i praksi,
 - saznanje o stvarnim kapacitetima procesa, posebno za izbor snabdevača,
 - fokus na merenje zrelosti organizacije i poboljšavanje procesa.
2. **Potrošačke organizacije**, koje nabavljaju proizvode/sisteme/servise zaštite od eksternih/ internih izvora i krajnji korisnici imaju brojne koristi uključujući:
 - jezik i sredstvo za evaluaciju iz standardnih zahteva za ponudu,

- SSAM metod za evaluaciju nivoa kapaciteta/zrelosti snabdevača,
- manji rizik od izbora nekvalifikovanog snabdevača,
- manje nezadovoljstva zbog uniformne evaluacije na bazi standarda i
- predvidljiv, ponovljiv nivo poverenja u proizvode ili servise.

3. **Organizacije za evaluaciju**, sertifikaciju i akreditaciju sistema, evaluatori i procenjivači proizvoda i sistema:

- višestruko iskoristive rezultate i iskustva evaluacije procesa, nezevisno od promena sistema ili proizvoda,
- poverenje u SSE procese i integraciju sa drugim disciplinama i
- veće poverenje u dokaze evaluacije, što smanjuje rad na evaluaciji zaštite.

SSE-CMM model ne sadrži ni jedan *aktuelan* profil organizacije, ali sadrži koncept za razvoj profila procesa organizacije, odnosno, rangiranja nivoa zrelosti kapaciteta OP. Profilisanje procesa organizacije smatra se važnim aspektom primene SSE CMM modela. U tom smislu razvijen je i opisan skup referentnih (željenih) profila procesa ključnih tipova organizacija sa razlozima za izbor CL određenih OP: *organizacije za razvoj proizvoda zaštite, organizacije za integraciju sistema zaštite, organizacije za obezbeđivanje servisa zaštite, standardnog sertifikacionog tela (CA) i korisničke organizacije IKT sistema, (Prilog 2.8B).*

2.8.4. Primena SSE CMM za obezbeđivanje argumenata bezbednosne garancije

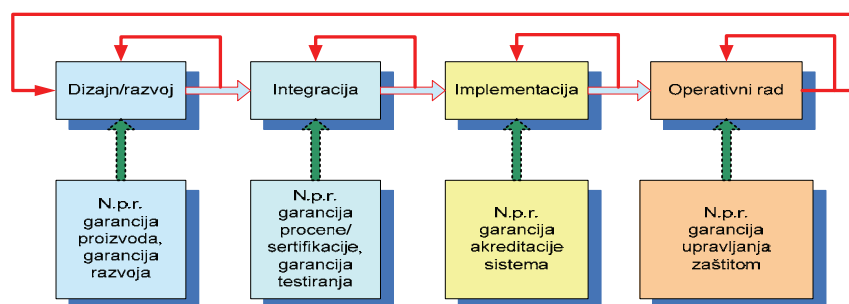
Primenom odgovarajućih aktivnosti i obezbeđivanjem **argumenata bezbednosne garancije** uspostavlja se poverenje da će proizvod/proces/servis/sistema zaštite zadovoljiti svoje bezbednosne ciljeve. Poverenje se stiče revizijom *dokaza bezbednosne garancije* sakupljenih u fazi razvoja, implementacije i iskustava iz operativnog rada proizvoda/ procesa/servisa/sistema zaštite. **Dokazi bezbednosne garancije** često se generišu u formi dokumentacije, razvijene u toku izvršavanja IKT inženjerskih aktivnosti. U izgradnji konzistentnog skupa **argumenata bezbednosne garancije**, vrlo je važno poznavati izvor, bezbednosne zahteve i ciljeve dokaza, pošto različito doprinose izgradnji poverenja. SSE CMM je ne-tradicionalni metod za garanciju kvaliteta bezbednosti IKT sistema, koji dokazuje bezbednosne garancije obezbeđuje na bazi evaluacije nivoa kapaciteta i zrelosti SSE procesa organizacije (CL1-CL5).

Kako u raspoloživoj literaturi nema objavljenih specifičnih saopštenja o tome koji je metod za određivanje bezbednosne garancije proizvoda/procesa/servisa/sistema zaštite najbolji i zašto, izbor metoda treba zasnivati na *politici garantovane bezbednosti* IKT proizvoda/procesa/servisa/sistema organizacije, poslovnim ciljevima i vrsti proizvoda/procesa/servisa/sistema zaštite. Na primer, SSE CMM metod je primenljiv samo za procese, dok je ISO/IEC 15408 (CC) standard primenljiv samo za proizvode/sisteme zaštite. Izabrani metod za određivanje bezbednosne garancije 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 bezbednosne garancije mogu se svrstati u 3 kategorije na bazi, [12]:

1. **evaluacije proizvoda rada**, testiranjem proizvoda/servisa/sistema i njihove zaštite nezavisno od procesa razvoja,
2. **evaluacije procesa** primenjivanih za razvoj, proizvodnju i operativni rad proizvoda rada (komponenti/sistema zaštite) u svim fazama životnog ciklusa i
3. **evaluacije okruženja**, tj. faktora fizičkog okruženja i personala koji doprinose kavalitetu procesa i proizvodnje, ne ispitujući direktno kvalitet procesa/proizvoda.

Metodi za određivanje bezbednosne garancije uključuju brojne nacionalne i međunarodne metode, *de-facto* standarde i druge prihvatljive metodologije koje koriste neki specifikovan i sistematičan pristup. Primer *de-facto* standarda za metod određivanja bezbednosne garancije je SSAM metod evaluacije, dobro dokumentovan, ali ne i šire međunarodno priznat standard. Metodi

za određivanje bezbednosne garancije mogu biti specifični za neku fazu životnog ciklusa, n.p.r., *sertifikacija i akreditacija* sistema zaštite posle implementacije i integracije sistema, ili primenljivi na nekoliko faza životnog ciklusa proizvoda/sistema/servisa/procesa zaštite, kao što su ISO 9000, ISO/IEC 15408 (CC) i SSE CMM. Za postizanja ukupne bezbednosne garancije, u svakoj fazi treba agregirati sakupljene argumente bezbednosne garancije. Obezbeđivanje *inkrementalnog* (Sl.2.8.1) povećavanja dokaza i izgradnje argumenata bezbednosne garancije, primenjuje se do *operativne* faze životnog ciklusa proizvoda/procesa/servisa/sistema zaštite, [60].



Sl. 2.8.1. Odnosi metoda obezbeđivanja garancije i redukovano modela životnog ciklusa

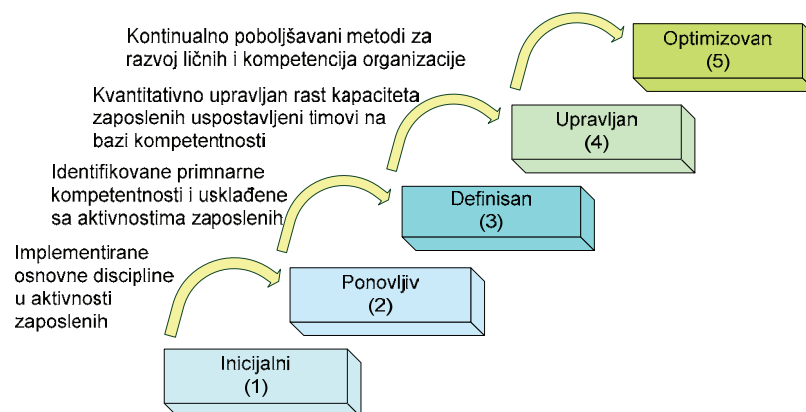
2.8.5. Profilisanje kompetencija personala u oblasti zaštite (P-CMM)

Generički CMM okvir treba prioritarno primenjivati na prakse koje direktno doprinose povećavanju kapaciteta 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 personala zaštite* pravi su kandidat za CMM merenje i poboljšavanje nivoa zrelosti tih procesa. **P-CMM** (*Personal CMM*) model opisuje poboljšavanje kapaciteta za razvoj kompetencija zaposlenih, [23].

P-CMM vodi organizaciju kroz 5 razvojnih nivoa zrelosti praksi i procesa za uspostavljanje i poboljšavanje kompetencija zaposlenih. Dostizanje svakog nivoa zrelosti u P-CMM institucionalizuje nove kapacitete za razvoj kompetencija zaposlenih u zaštiti. Svaki nivo zrelosti obezbeđuje gradivni sloj u osnovi za kontinualno poboljšavanje praksi i procesa za razvoj kompetencija zaposlenih u organizaciji.

P-CMM se može primenjivati za evaluaciju prakse zaposlenih, uputstvo za planiranje i implementaciju poboljšavanja kompetencija zaposlenih i za kontinualno povećanje kapaciteta za razvoj kompetentncija ljudskih resursa u IKT sistemu organizacije. Dugoročni, strateški ciljevi P-CMM mogu biti: *poboljšani kapaciteti organizacije povećavanjem kompetentncija zaposlenih; ljudski kapaciteti su atribut organizacije, a ne pojedinaca; motivacija pojedinaca usklađena sa interesima i ciljevima organizacije i zadržani kritični ljudski resursi, tj. ljudi sa kritičnim znanjima i veštinama.*

P-CMM obuhvata procese (OP) i prakse (BP) u sledećim oblastima: *radno okruženje, komunikacija, popuna radnih mesta (zapošljavanje), obuka, upravljanje performansama, kompenzacija, razvoj kompetentnosti, profesionalni razvoj karijere, izgradnja timskog rada i razvoj kulture rada.* P-CMM kapaciteti poboljšavaju se uspostavljanjem okruženja koje podstiče neprekidno učenje, [45], u kojem organizacija ima kvantitativnu povratnu ocenu o performansama zaposlenih, odnosno, razvija okvir sazrevanja ljudskih kapaciteta za izgradnju takvog radnog okruženja u kojem prakse mogu biti ponovljene, najbolje prakse se mogu brzo preneti na celu grupu zaposlenih, varijacije u izvršavanju najboljih praksi rada su smanjene i prakse se kontinualno poboljšavaju. Na Slici 2.8.2 ilustrovano je 5 nivoa sazrevanja P-CMM procesa sa ključnim atributima, [23].

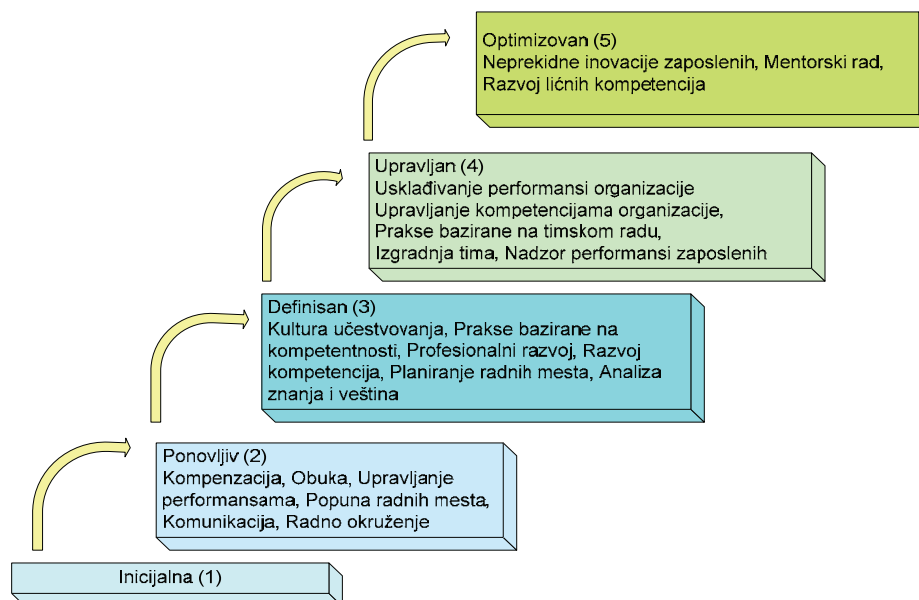


Sl. 2.8.2. Nivoi i atributi kapaciteta OP P-CMM modela

Kriterijumi za izbor nivoa zrelosti P-CMM kapaciteta detaljno su opisani u **Prilogu 2.8C**.

2.8.5.1. Struktura P-CMM modela

Dimenzija OP u P-CMM modelu ilustrovana je na Slici 2.8.3.



Sl. 2.8.3. Oblasti procesa P-CMM po nivoima zrelosti

U Tabeli 2.8.1. navedene su oblasti P-CMM procesa sa osnovnim atributima, detaljnije opisanim u **Prilogu 2.8D**, koje se nalaze na odgovarajućim nivoima zrelosti, [23].

Tabela 2.8.1. OP P-CMM modela po nivoima zrelosti

Nivo zrelosti	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

Nivo zrelosti	Atribut zrelosti	Oblast procesa (OP)
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 ucestvovanja
4.	Upravljeni 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: Instrukтивna obuka
		OP20: Neprekidno inoviranje praksi zaposlenih

Međuzavisnosti OP u P-CMM uspostavljaju četiri kategorije procesa (OP), za: razvoj kapaciteta, izgradnju tima i kulture rada, motivisanje i upravljanje performansama rada i oblikovanje radnog profila zaposlenih. Odnos kategorija OP i nivoa zrelosti (ML) dat je u Tabeli 2.8.2.

Tabela 2.8.2. Kategorije OP i nivoi zrelosti P-CMM modela

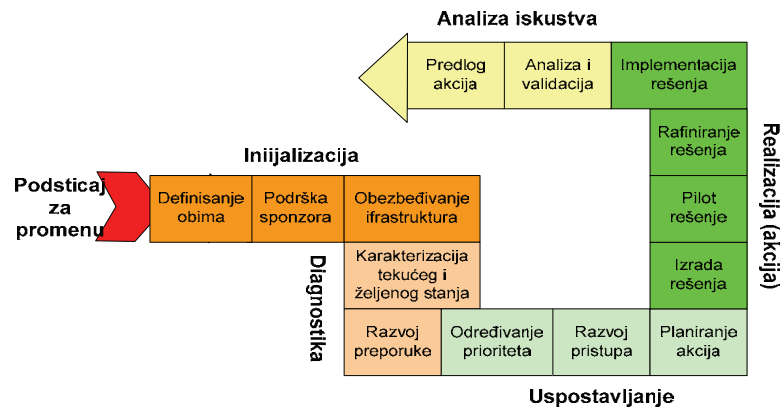
ML	Kategorije procesa			
	Razvoj kapaciteta	Izgradnja tima i kulture rada	Motivisanje i upravljanje performansama rada	Oblikovanje radnog profila zaposlenih
5.	Instruktorska obuka Razvoj ličnih kompetencija	Kontinualno osposobljavanje zaposlenih		
4.	Mentorski rad	Izgradnja tima	Usklađivanje performansi organizacije Razvoj praksi na bazi timskog rada	Upravljanje kompetencijama organizacije
3.	Razvoj kompetencija Analiza znanja i veština	Kultura ucestvovanja	Razvoj praksi na bazi kompetentnosti Profesionalni razvoj	Planiranje ljudskih resursa
2.	Obuka, komunikacija	Komunikacija	Kompenzacija Upravljanje performansama Radno okruženje	Popuna radnih mesta

Dimenzija zrelosti procesa (fazna reprezentacija) P-CMM modela obuhvata 5 CF: angažovanost na izvršavanju praksi, sposobnost izvršavanja praksi, izvršene aktivnosti, merenje i analiza i verifikovanje implementacije.

CF - Izvršene aktivnosti opisuje aktivnosti implementacije, a ostale 4 CF pomažu da se institucionalizuju ove implementacione prakse u kulturu rada organizacije, tako da su efektivne, ponovljive i trajne.

Implementacija programa P-CMM za poboljšanje procesa može se izvršiti prema SEI modelu IDEAL (*I*nitiating, *D*iagnosing, *E*stablishing, *A*cting, *L*earning) koji se u celini može koristiti i

za implementaciju CMMI i SSE CMM praksi i procesa (Sl. 2.8.4), ili nekom drugom modelu za implementaciju procesa, [23], [81].



Sl. 2.8.4. Model IDEAL za implementaciju CMMI i SSE CM procesa

Ulazni parametar u proces implementacije praksi i procesa P-CMM, CMMI, ili SSE CMM modela je neka *inicijativa* za promenu, na osnovu koje se vrši priprema: definiše sadržaj i obim, obezbedi podrška menadžmenta i infrastruktura. U sledećem koraku faze *dijagnostifikovanja* obima implementacije procesa vrši se karakterizacija tekućih i željenih nivoa zrelosti procesa i razvijaju preporuke. U fazi *uspostavljanja* CMMI, ili SSE CMM procesa određuje se profil procesa, razvija pristup (metod) i planiraju aktivnosti za implementaciju. U fazi *realizacije* aktivnosti kreira se rešenje i testira pilot-rešenje sa kojim se rafinira i implementira rešenje. U fazi analize stečenih iskustava implementirano rešenje se analizira, izučavaju se stečena iskustva i daju predlozi za dalje aktivnosti.

2.8.6. Komplementarna metrika CC i SSE CMM za razvoj bezbednosnih zahteva

U procesu razvoja bezbednosnih zahteva za IKT sistem, može se koristiti kvalitativna metrika za dobijanje kvantitativnih informacija koje se, zatim, mogu upotrebiti za evaluaciju i poboljšavanje procesa, posebno za: procenu rizika, ranjivosti sistema i definisanje zaštitnog profila, što je važan aspekt specifikacije bezbednosnih zahteva za sistem. Takvu metriku obezbeđuje kompatibilna kombinacija CC i SSE CMM standarda, koristeći uspostavljeni metod za identifikaciju bezbednosnih funkcija i klasifikaciju bezbednosnih nivoa (EAL) u CC i klasifikaciju nivoa zrelosti kapaciteta u SSE CMM standardu, [54], [38].

Bezbednosni zahtevi mogu se razvijati na bazi bezbednosnih funkcionalnosti komponenti /sistema (CC) i/ili politike zaštite (ISO/IEC 17799). U ovaj razvoj treba uključiti etičke i socijalne aspekte bezbednosti sistema, sadržane u opšte prihvaćenim – GAISP principima zaštite. U svim aspektima zaštite, metrički sistemi doprinose boljem razumevanju procesa i performansi procesa zaštite i bržem odlučivanju za implementaciju *kontrola zaštite*. Metrike zaštite su korisne za identifikaciju i određivanje kritičnih i nekritičnih bezbednosnih parametara, testiranja i usmeravanje napora za evaluaciju sistema i procesa zaštite. Specifikacija bezbednosnih zahteva za proizvod/sistem zaštite prema CC standardu vrši se kroz **profile zaštite (PP)**.

Prema CC, procesi u kojima se analiziraju argumenti bezbednosne garancije za *funkcionalne i bezbednosne* zahteve (EAL), su: evaluacija, testiranje, procena rizika i izrada **PP**. CC standard definiše 7 EAL bezbednosnih nivoa za specifikaciju i evaluaciju proizvoda i sistema zaštite, koji su mera poverenja i indiciraju koliko dobro sistem ispunjava određene bezbednosne ciljeve. Neki autori tvrde da nebezbednost sistema uglavnom dolazi zbog nedovoljnog testiranja, relativno visokih troškova testiranja, ograničenja različitih metoda testiranja i nedostatka harmonizovane metrike zaštite. Razvoj **PP** direktno se odnosi na specifikovanje ciljeva zaštite (ST) i bezbednosnih nivoa (EAL).

Metrike zaštite su važni indikatori nivoa *implementacije* i *institucionalizacije* kontrola zaštite i mogu se koristiti za merenje nivoa zrelosti procesa zaštite i kapaciteta organizacije. Omogućavaju bolje razumevanje performansi, pokrivanja i nivoa odlučivanja različitih procesa i kontrola zaštite, [106]. Ovo je posebno bitno za korisnike sistema IKT zaštite, koji se osim sa problemima tehničkih kontrola zaštite, suočavaju i sa uticajem okruženja i ljudskog faktora.

2.8.6.1. Razvoj profila zaštite PKI X509 digitalnog sertifikata

Za razvoj **PP** za **X.509 digitalni sertifikat**, korisno je upotrebljavati metriku zaštite koja je pogodna za analizu pretnji i faktora rizika, [86].

U cilju veće interoperabilnosti federalnog PKI sistema SAD sa drugim PKI sistemima razvijeno je 5 tipova *politika sertifikata* (CP) PKI, koje definiše 5 bezbednosnih nivoa: *rudimentarni, osnovni, srednji i visoki nivo bezbednosti*, [61]. U suštini, ovi nivoi su metrike koje koriste klasifikaciju kritičnih i ne-kritičnih funkcija CP PKI sistema. Prema CC standardu **PP** se definiše kao *"izjava o bezbednosnim zahtevima, nezavisna od implementacije, koja obuhvata pretnje u specifičnom okruženju"*. Ova izjava indicira da je od velikog značaja duboko razumevanje okruženja u kojem se primenjuje objekat evaluacije (TOE). Ovo razumevanje može se postići kroz standardizaciju metrika PP. Standardna metrika SSE CMM može se koristiti za indikaciju dubine CC testiranja specifičnog proizvoda i određivanje EAL nivoa. NIST metodologija metrika zaštite može biti korisna za merenje nivoa zrelosti procesa zaštite organizacije, [106].

Okvir za razvoj PP proizvoda i sistema zaštite, može se uspostaviti primenom različitih postojećih metoda kao što su CC, SSE CMM, model sistema zaštite sa konsenzusom - SBC (*Security By Consensus*) i tehnički model društva. Iako PP mogu varirati u različitim okruženjima, metrike koje se mogu koristiti za merenje različitih parametara mogu se standardizovati. Ključne oblasti procesa u razvoju PP u CC standardu prikazane su u dekomponovanoj CC klasi - *Evaluacija PP*, [99], [49]:

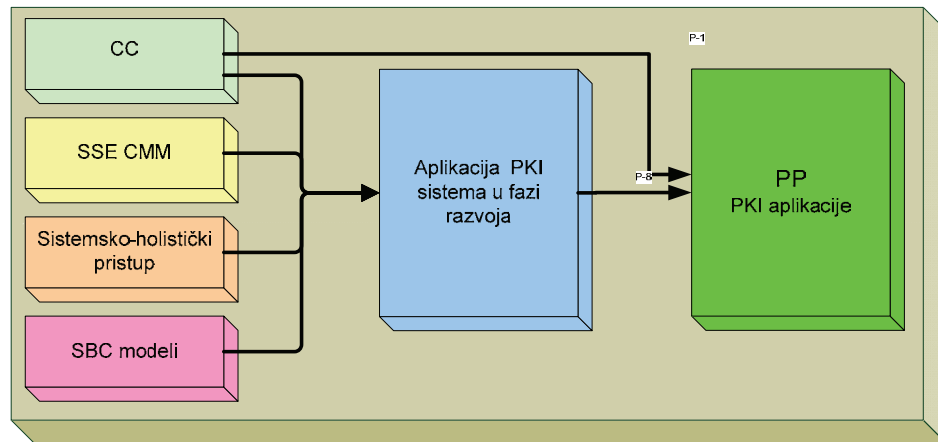
- APE_DES: Opis objekta evaluacije (TOE),
- APE_ENV: Bezbednost okruženja,
- APE_INT: Uvođenje PP,
- APE_OBJ: Bezbednosni ciljevi,
- APE_REQ: IKT bezbednosni zahtevi i
- APE_SRE: Eksplicitno navedeni bezbednosni zahtevi.

Za definisanje i razvoj PP kritične su sledeće oblasti procesa: *identifikacija kritičnih objekata IKT sistema, pregled politika zaštite, upravljanje i procena rizika, procena dopuštenog i nedopuštenog ponašanja u sistemu, procena ponašanja korisnika u prihvatanju sistema, identifikovanje agenata pretnji, analiza pretnji i analiza bezbednosnih funkcija*.

Za identifikovanje *bezbednosnih funkcija* standardnog X.509 sertifikata PKI sistema, može se koristiti CC standard. Pretnje za ove bezbednosne funkcije se identifikuju, a odgovarajuća metrika koristi se za određivanje uticaja tih pretnji. Takođe, za pokrivanje bezbednosnih funkcija treba razviti odgovarajuću metriku. Standardna NIST metrika zaštite [106] i SSE CMM metrika mogu se koristiti za razvoj potrebnih metrika koje se odnose na bezbednosne funkcije i uticaj okruženja, na primer, za procenu svesti zaposlenih o potrebi zaštite, dokumentacije zaštite i drugih procesa koji se odnose na okruženje, [102]. 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*), [104]. Za izučavanje socijalnog aspekta IKT sistema, više odgovaraju metrički sistemi koje obezbeđuje tzv. *Sistemsko-holistički pristup* i model sistema zaštite sa konsenzusom-SBC (*Security By Consensus*), [68].

Na slici Sl. 2.8.5 predstavljen je model okvira za razvoj PP. 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, korisni su za razvoj metrika koje se odnose na obuku u zaštiti, personalnu zaštitu i socijalni aspekt (etičku komponentu) zaštite. Međutim, ovi se modeli mogu koristiti i u drugim aspektima istraživanja bezbednosti i zaštite IKT sistema, [114].



Sl. 2.8.5. Okvir za razvoj profila zaštite (PP)

Ova primena koncepta **PP** za uspostavljanje bezbednosnih zahteva detaljnije je opisana na primeru standardnog X.509 v.3 digitalnog sertifikata u PKI sistemu u **Prilogu 2.8E**, [39], [59], [65].

2.8.7. Primena SSE CMM metrike za procenu kapaciteta za upravljanje rizikom

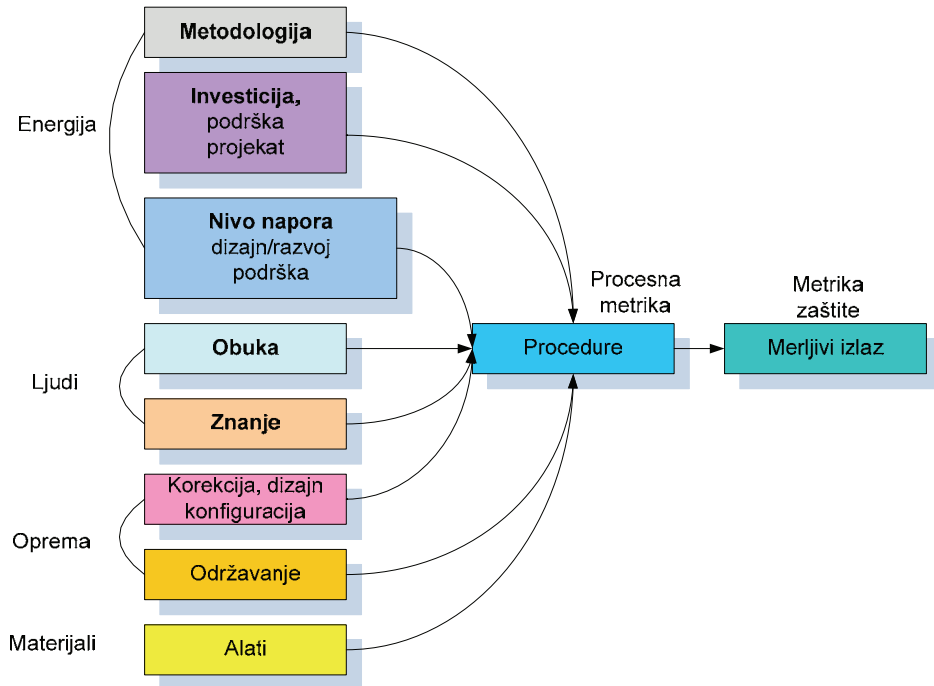
Osnovno pitanje u primeni SSE CMM modela za upravljanje rizikom je „Kako se može znati da primena procesa opisanih u modelu doprinosi većoj bezbednosti sistema, ili operativnih kapaciteta?“ Odgovor na ovo suštinsko pitanje daje inherentna, dualna *metrika procesa* i *metrika sistema zaštite* SSE CMM modela, [62], [102], [115].

Metrika procesa je specifična metrika kvantitativnih/kvalitativnih dokaza nivoa zrelosti za određenu OP, ili binarnih indikatora prisustva ili 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. U praksi zaštite identifikovane su potencijalne grupe korisnika SSE CMM metrike:

- **Rukovodstvo projekta i projektni tim**, za operativno, ili razvojno okruženje, ili poboljšavanje procesa;
- **Menadžment organizacije i izvori finansiranja**, za alokaciju resursa, usmeravanje budžeta i određivanje prioriteta;
- **Šira zajednica**, za razvoj svesti o potrebi zaštite, razvoj konkurentnosti, bolje koordinacije i boljih praksi;
- **Organizacije korisnika**, za nabavku proizvoda i servisa;
- **Konkurentni entiteti**, kao faktor odvratanja onih koji žele konkurisati, ili napasti nečije interese;
- **Snabdevači proizvoda**, za procenu efektivnosti proizvoda zaštite, bazirane na poboljšavanju SSE procesa.

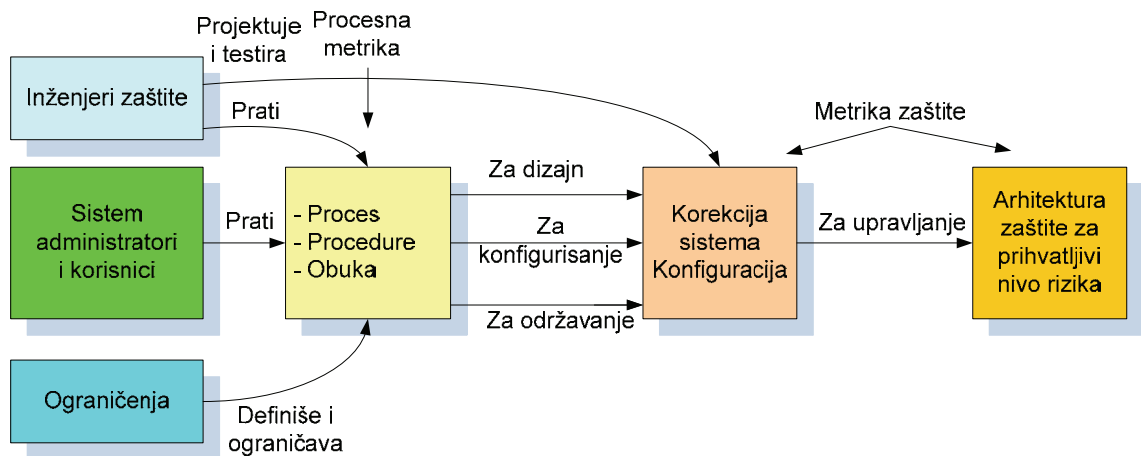
2.8.7.1. Razvoj SSE CMM metrike za procenu kapaciteta za upravljanje rizikom

Svaki proces ima ulazne parametre, ograničenja, aktivnosti i izlazne parametre. Izvršavanje, stabilnost, kapacitet, poboljšavanje i investiranje glavni su faktori za efektivno upravljanje procesom. Na Slici 2.8.6 prikazan je progres od ulaznih parametara procesa i ograničenja do procedura i merljivih izlaznih parametara metrike, [62].



Sl. 2.8.6. Razvoj metrike zaštite

Prvo se ispituje postojanje i izvršavanje svakog proces, bez procene koliko dobro se proces izvršava. Na Slici 2.8.7 prikazan je odnos između SSE CMM metrika, ulaza u SSE proces, procesa koji se izvršava za postizanje SSE ciljeva i performansi procesa zaštite.



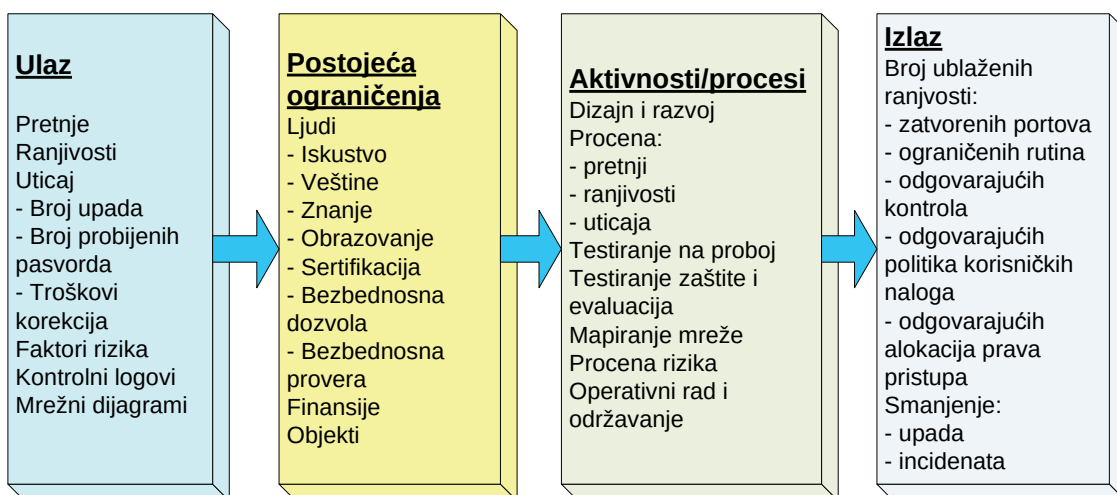
Sl. 2.8.7. Odnosi SSE CMM metrike procesa i metrike zaštite

Primer specifičnih entiteta koji mogu biti mereni u SSE procesu i na koje se metrika procesa može primeniti, prikazan je na Slici 2.8.8.



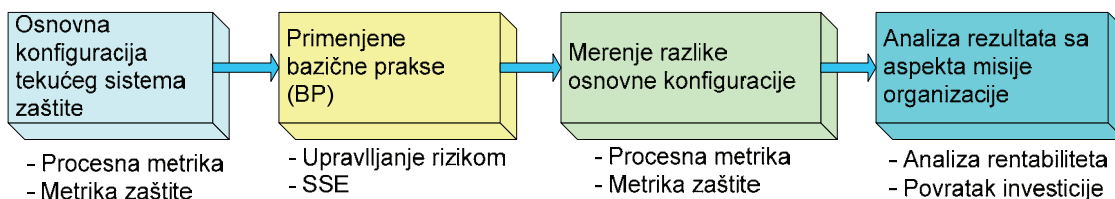
Sl.2.8.8 SSE CMM merljivi atributi procesa

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 zaštite. Primer je prikazan na slici Sl. 2.8.9.



Sl. 2.8.9. SSE CMM merljivi atributi sistema zaštite

Međutim, ni jedna metrika ne može se 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 treba uzeti u obzir da se merenje može izvršiti samo u odnosu na poznate ranjivosti i pretnje i napade iz okruženja. Konačno, metrike se ne mogu koristiti kao 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 organizacije i performansi sistema zaštite (Sl. 2.8.10).

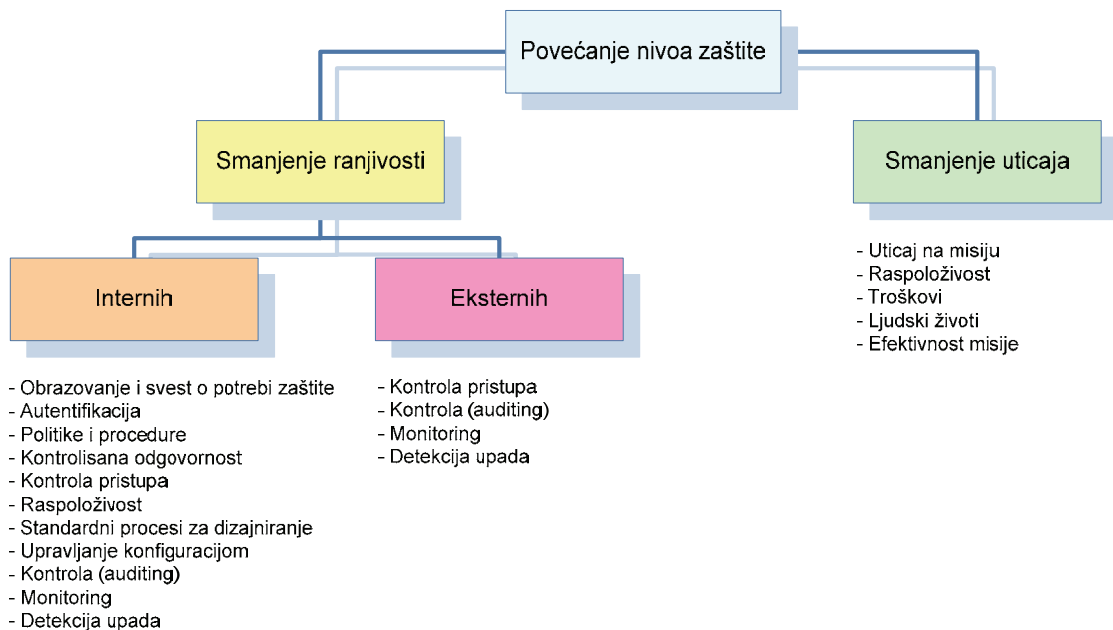


Sl. 2.8.10. Primena SSE CMM metrika procesa i sistema zaštite

Prvi korak je izmeriti osnovnu konfiguraciju sistema zaštite, primenom procesne i systemske metrike. Zatim se izvršavaju BP procesa SSE CMM modela da bi se identifikovale mere zaštite

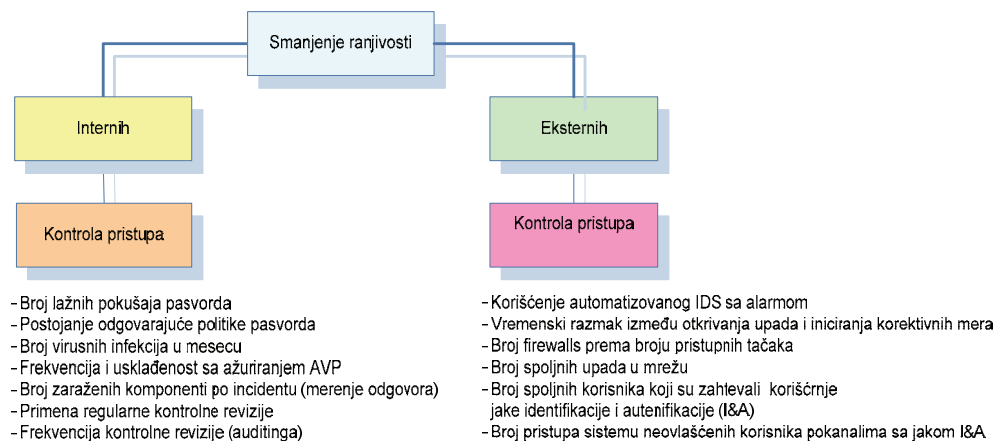
koje dovode do poboljšavanja sistema zaštite organizacije i da bi se te mere implementirale. Posle implementacije preporučenih mera zaštite vrši se druga evaluacija, koja obezbeđuje merenje razlike stanja efektivnosti sistema zaštite "pre" i "posle" primene preporučenih mera zaštite. Na taj način određuje se relativno poboljšavanje nivoa bezbednosti i efektivnosti sistema zaštite. Dobijeni rezultat treba analizirati prema ciljevima i misiji organizacije, odnosno, na bazi analize rentabiliteta ili povratka investicije, da bi se mogli interpretirati rezultati menadžmentu organizacije.

U procesu razvoja metrika zaštite mogu se koristiti brojni metodi. Prihvatljiv pristup za kategorizaciju adekvatne metrike je *odozgo-na dole* (Sl. 2.8.11), gde se metrike razmatraju sa aspekta uputstava, politika, 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.



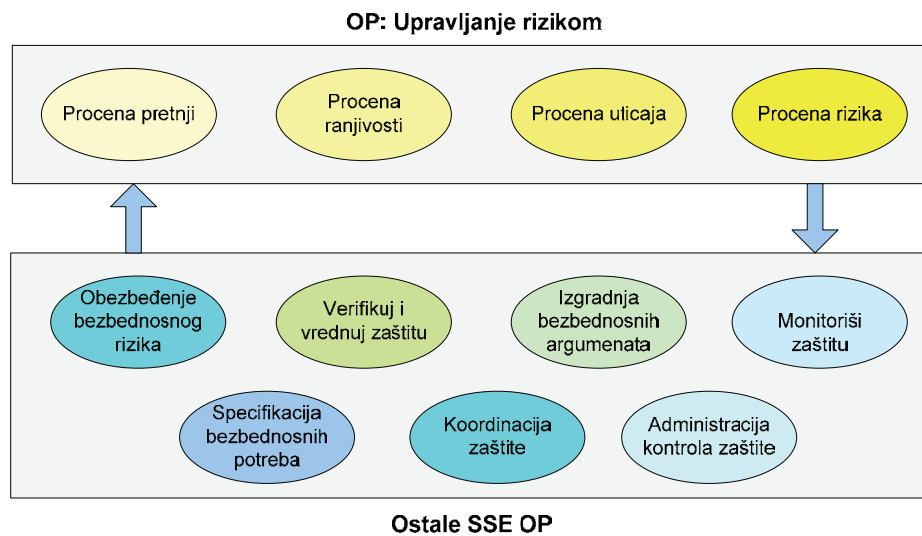
Sl. 2.8.11. Dijagram razvoja metrika zaštite

Na primeru servisa *Kontrole pristupa* na slici Sl. 2.8.12 ilustrovana je dekompozicija dijagrama sa slike Sl. 2.8.11 u skup procesnih i sistemskih metrika. Na Sl. 2.8.12 "korišćenje automatizovanog IDS sa alarmom" i "korišćenje regularne kontrolne revizije" su procesne metrike, a "vremenski razmak između otkrivanja upada i iniciranja korektivnih mera" i "frekvencija kontrolne revizije" predstavljaju metriku sistema zaštite.



Sl. 2.8.12 Moguće metrike servisa *Kontrole pristupa*

Konkretna primer metrike prikazan je na slučaju samo-evaluacije (Sl. 2.8.13) SSE CMM OP za *upravljanje rizikom* za nivo CL3, u odnosu na servise OP i ulogu metrike u tome. U ovom modelu SSE CMM OP delimo u dve grupe: *upravljanje rizikom* i *ostale SSE OP*, sa izostavljanjem brojnih veza između SSE OP.



Sl. 2.8.13. Odnosi SSE CMM OP u modelu metrike za OP upravljanja rizikom

SSE-CMM 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 nivoa kapaciteta. **Kriterijume** za određivanje ranga nivoa kapaciteta (CL) određene OP definišu SSE CMM i SSAM metod evaluacije: OP dostiže 1.CL ako su sve BP **100%** izvršene, nivo 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.

2.8.8. Metodologija S-vektora za zaštitu Web aplikacija

Metodologija S-vektora posebno je namenjena za validaciju sistema zaštite web aplikacija, određivanje prioriteta projekata reinženjeringa postojećeg sistema zaštite web aplikacija i evaluaciju strategije za poboljšavanje i merenje progressa u poboljšavanju sistema zaštite web aplikacija. Koristi metriku ponderisanja, i integriše metodologije tri standarda zaštite, [104], [52], [18] [10]:

4. ISO/IEC 17799, *Code of practice and Security controls*,
5. ISO/IEC 21827 ili model sazrevanja procesa zaštite (**SSE CMM**) i
6. ISO 15408 (CC- opšti kriterijumi za evaluaciju proizvoda zaštite).

Generalno metodologija S-vektora obuhvata **bezbednosne zahteve** za svaku web aplikaciju, koji se mapiraju u željeni, ili **zahtevani vektor** zaštite aplikacija sa željenim težinskim faktorima i **periodičnu procenu** zaštite web aplikacije sa odgovarajućim težinskim faktorom **tekućeg vektora** zaštite aplikacije, koji se upoređuje sa referentnim u zahtevanom vektoru zaštite aplikacije, dajući meru progressa sazrevanja procesa zaštite. U S-vektoru mapirana su tri tipa bezbednosnih zahteva: **tehnički**, **strukturni** i **proceduralni**. **Tehničke komponente** S-vektora, uključujući servise i aplikacije **kriptozaštite** i **jake autentifikacija**, u najvećoj meri korespondiraju zahtevima **CC** standarda. **Strukturne komponente** obuhvataju strukture softvera i dizajna sistema zaštite, obezbeđuju veću bezbednosnu garanciju (*assurance*) servisa zaštite (n.p.r., različiti tipovi automatskih provera kvaliteta programskih kodova) i mogu se aplicirati primenom **ISO/IEC**

17799 i SSE CMM standarda. **Proceduralne komponente**, uključujući procedure za razvoj, implementaciju i upravljanje koje obezbeđuju pouzdanije servise zaštite, obezbeđuju isti standardi. Primeri su metodologija za razvoj programa zaštite (SSE CMM) i politika zaštite (ISO 17799) za upravljanje sistemom zaštite.

U metodologiji S-vektora najbitniji je SSE CMM metrički sistem za kvantitativnu evaluaciju bezbednosnih zahteva i aktuelnih rezultata performansi implementiranog sistema zaštite web aplikacija, odnosno, sistem ponderisanja komponenti S-vektora preuzetih iz ISO/IEC 17799, sa težinskim faktorima i metrikom nivoa zrelosti kapaciteta procesa zaštite, preuzetih iz SSE CMM standarda.

Kontrole i politike zaštite ISO/IEC 17799 standarda mogu se efikasno primeniti za implementaciju S-vektora, ako se definiše sistem težinskih faktora za merenje izvršavanja i kvaliteta njihovog izvršavanja. Kontrole zaštite primarno se odnose na **proceduralne komponente** S-vektora. Matrica *preporučenih* kontrola i korespondirajućih komponenti S-vektora zaštite, prikazana je u Tabeli 2.8.3, [104].

Tabela 2.8.3. Korelacija kontrola zaštite standarda ISO/IEC 17799 i S-vektora

Elementi ISO/IEC 17799	Preporučeno za S-vektor	Korelacija sa komponentama S-vektora		
		Proceduralne	Strukturne	Tehničke
Politika zaštite	X	X		
Organizacione kontrole zaštite	X			
Klasifikacija i kontrola objekata	X			
Personalna zaštita	X			
Fizička zaštita i zaštita okruženja				
Upravljanje komunikacijama				
Kontrola pristupa	X		X	
Razvoj i održavanje sistema	X	X	X	
Upravljanje kontinuitetom poslovanja				
Usaglašenost				

Dakle, S-vektor ne definiše, standardom ISO/IEC 17799 sugerisane politike i kontrole zaštite, nego evaluira postojanje i kvalitet izvršavanja politika i kontrola zaštite.

SSE CMM model i SSAM metod evaluacije nivoa zrelosti kapaciteta procesa, definiše zahteve za procese i procenjuje koliko je proces zreo u metodologiji S-vektora. Moguće je inkorporirati svih 11 SSE OP kao proceduralne komponente u S-vektor, pri čemu se za merenje nivoa kapaciteta procesa i za procenu zrelosti proceduralnih komponenti S-vektora, može koristiti neznatno različita metrika S-vektora, ili originalna metrika SSE CMM modela, bez obzira potiču li komponente iz OP SSE CMM modela, ili ne, [102].

Za izgradnju *okvira za upravljanje* zaštitom web aplikacija, u kojem se administriraju kontrole zaštite u projektu, ili organizaciji, može se primeniti svih 11 SSE u S-vektoru, (Tabela 2.8.4). Preostalih 11 *projektnih i organizacionih* OP, nije u praksi primenjivano za implementaciju u S-vektor (istraživanje je u toku), [104].

Tabela 2.8.4. Korelacija OP zaštite SSE CMM standarda i S-vektora

Oblast procesa zaštite SSE CMM		Preporučeno za S-vektor	Korelacija sa komponentama S-vektora		
			Proceduralne	Strukturne	Tehničke
OP01	Administriranje kontrola zaštite	X	X		
OP02	Procena uticaja	X			
OP03	Procena rizika	X			
OP04	Procena pretnji	X			
OP05	Procena ranjivosti	X			
OP06	Izgradnja argumenata bezbednosne garancije	X			
OP07	Koordinacija zaštite	X		X	
OP08	Monitoring sistema zaštite	X	X	X	
OP09	Obezbeđivanje bezbednosnog ulaza	X			
OP10	Specifikacija bezbednosnih zahteva	X			
OP11	Verifikacija i validacija sistema zaštite	X	X		

SSE CMM OP pomažu da se izgradi okvir za upravljanje, ali ne nudi detalje o tome kako izvršiti ovu praksu. Nivoi kapaciteta koriste se za procenu zrelosti datih procesa. Njihova primenljivost zavisi od ciljeva ponderisanja komponenti S-vektora. Ako je cilj procena kvaliteta izlaza procesa, nivoi zrelosti kapaciteta procesa mogu biti neodgovarajući zato što nisu dizajnirani za ovu namenu. Nivoi zrelosti kapaciteta procesa primenljivi su za S-vektor, ako je cilj ponderisanja komponente, određivanje kvaliteta njenog *praćenja, planiranja, definisanja i kontrolisanja*. *Zahtevani S-vektor bezbednosnih zahteva* ponderiše se sa željenim nivoima kapaciteta. Zatim se mere tekući nivo kapaciteta procesa i ponderiše se *tekući S-vektor*. Nivoi kapaciteta mogu se procenjivati primenom striktno metričke SSE CMM modela, preko SSAM metoda evaluacije, pri čemu se mora znati kako SSAM procenjuje nivo kapaciteta po OP.

Implementacija S-vektora počinje sa određivanjem *zahtevanog S-vektora*, koji se definiše izradom liste ISO/IEC 17799 *kontrola zaštite* relevantnih za *web* aplikaciju. Za ponderisanje kvaliteta svake kontrole koristiti se skala merenja od 5 nivoa (1-5). Za zahtevani S-vektor, svaka izabrana kontrola (čekanirana) dobija *željeni težinski faktor* od 1-5, koji indicira ciljni kvalitet određene kontrole. Zahtevani nivo kvaliteta svake kontrole zaštite određuje se na osnovu referentnih *atributa kvaliteta* SSE CMM modela, koji se pripisuju svakoj kontroli. Prvi se ponderiše *prioritet implementacije*, zatim ostali atribut kontrole zaštite: *definisanost, dokumentovanost, merljivost, ponovljivost i primenljivost*. Procenat, prosta aritmetička sredina, ili druga jedinica težinskih faktora atributa kontrole, određuje **zbirni težinski faktor** kontrole. Kontrole koje imaju vrednost „0“**-ne postoje** i ne treba ih uzimati u obzir za implementaciju, [104].

Tipična strategija za *bezbednosnu klasifikaciju* bezbednosno relevantnih informacija za definisanje nivoa bezbednosti *željenog S-vektora*, koji mora biti dostignut za određenu *web* aplikaciju za **N-niske**, **S-srednje** i **V-visoke** pretnje, prikazana je u Tabeli 2.8.5. U tabeli bezbednosne klase su identifikovane sledećim kôdnim zamenama *bezbednosnih zahteva za web aplikaciju*: **A-najniži**, **B-srednji** i **C-najviši** bezbednosni zahtev za *web* aplikaciju, [10].

Tabela 2.8.5. Tipična klasifikacija bezbednosnih zahteva

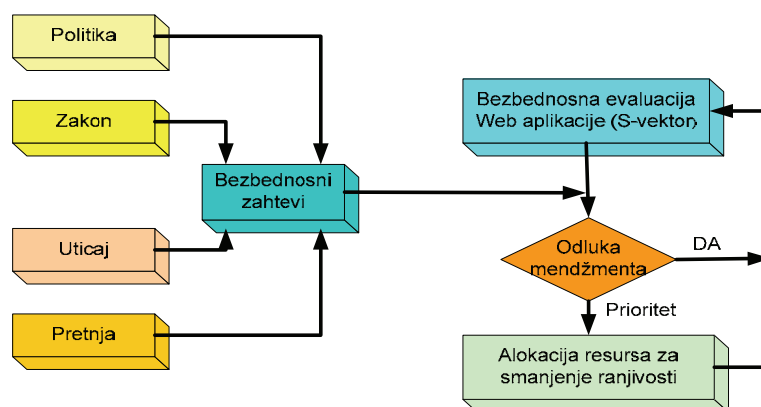
Uticaj	Pretnje			
		N	S	V
	V	B	B	C
	S	B	B	B
	N	A	B	B

Međutim, ako je pretnja za kompromitaciju bezbednosti *web* aplikaciju *najviša-V*, a uticaj takve pretnje izaziva određene slabosti u sistemu zaštite, **nedostaci strategije** su:

- nizak stepen granulacije nivoa bezbednosti ne pokriva sve realne slučajeve kroz većinu zahteva za srednjim nivoom bezbednosti **B**,
- ako nivo zaštite *web* aplikacije padne ispod zahtevanog nivoa **B**, nije jasno koje akcije treba preporučiti i
- pošto malo aplikacija pada u kategorije **A** i **C**, klasifikacija se ne može koristiti za određivanje prioriteta poboljšavanja bezbednosti između većine *web* aplikacija sa **B** bezbednosnim zahtevima.

Praktična vrednost S-vektora je u tome što se za konstrukciju elemenata željenog S-vektora, mogu koristiti informacije bezbednosno relevantne za poslovne procese koje *web* aplikacije podržavaju, uključujući rizik, pretnje, politike i legalne zahteve. Na taj se način tekući bezbednosni težinski faktor S-vektora za *web* aplikaciju, može upoređivati sa željenim težinskim faktorom iz Tabele 2.8.5, a mogu biti obuhvaćeni i elementi koji padnu ispod zahtevanog nivoa. **Prednost mapiranja** tekućih i željenih težinskih faktora S-vektora je što razlika u jednoj koordinati S-vektora identifikuje prirodu slabosti u sistemu zaštite *web* aplikacije, što omogućava menadžmentu da usmeri pažnju i resurse na najkritičnije bezbednosne zahteve. Dakle, elemente S-vektora treba razvijati sa razvojem bezbednosnih zahteva, pošto nema smisla razvijati neki element S-vektora, ako se ne može uspostaviti željeni nivo bezbednosti.

U sistemu upravljanja *web* aplikacijom metodologija S-vektora primenjuje se u skladu sa opštom strukturom sistema za upravljanje *web* aplikacijama, u kojem metod S-vektora ima značajnu ulogu (Slika 2.8.14). Periodična evaluacija *web* aplikacija daje tekući težinski faktor S-vektora svake *web* aplikacije i inicijalni S-vektor nove *web* aplikacije. Bezbednosni elementi, određeni sa 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, [10].



Slika 2.8.14. Proces upravljanja *web* aplikacijom primenom metodologije S-vektora

U toku progresivnog poboljšavanja sistema zaštite, evaluira se postojanje i kvalitet svake izabrane kontrole zaštite. Polukvalitativna metrika tipa 1-5 (analogna akademskoj gradaciji ocena) primenjuje se na svaku evaluiranu kontrolu. Mereni, tekući S-vektor sadrži iste elemente kao

zahtevani S-vektor. Najveći zbirni težinski faktor koji se može dostići u tekućem S-vektoru je zbirni težinski faktor pridruženog zahtevanog S-vektora. Zatim se tekući težinski faktori upoređuju sa zahtevanim i meri se stvarni kvalitet datih kontrola zaštite. Razlika tekućeg i zahtevanog težinskog faktora kontrole zaštite u S-vektoru pokazuje meru zrelosti kontrole zaštite.

Proceduralne komponente S-vektora, mogu se grupisati u grupe i podgrupe, prema obimu i sadržaju. Na primer, sve proceduralne kontrole (grupe) mogu se podeliti u podgrupe kontrola na: *nivou organizacije* i *nivou aplikacija*. Kontrole na nivou organizacije, kao što su: dokument politike zaštite informacija, politika kontrole pristupa, politika barijera i.t.d., mogu se dalje grupisati po sadržaju. Kontrole na nivou aplikacija mogu se grupisati prema aplikacijama. Da bi se lakše poredili, težinski faktori se po volji mogu dodeljivati elementima u podgrupama i grupama i zbirno po grupama i podgrupama.

Efektivnost ponderisanja zavisi od preciznosti definisanja kriterijuma ponderisanja, koji se određuju za svaku proceduralnu kontrolu (upravljačku, organizacionu), pošto su ove mnogo subjektivnije od tehničkih kontrola zaštite. Kriterijumi ponderisanja mogu se prikazati u kontrolnoj (ček) listi. Analitičar zatim može kontrolisati aktuelnu implementaciju pomoću ček liste. U nekim slučajevima kriterijumi ponderisanja mogu biti takvi da jedva specificiraju „postojanje“ kontrole.

Primer: Za ponderisanje ISO/IEC 17799 kontrole zaštite: “*Odvajanje korisničkog od aplikativnog softvera*“, koja se odnosi na klasu *Kontrole Operativnog sistema*, može se pripisati zahtevani težinski faktor „3“, koji predstavlja 3. Nivo CL/ML-*Dobro definisan i implementiran*, kao željeni nivo kvaliteta ove kontrole. Ponderisanje počinje sa određivanjem i pripisivanjem atributa *prioriteta*. Određuje se **kriterijum ponderisanja**: *sve aplikativne datoteke uskladištene su na odvojenoj particiji HD od sistemskih*. Ako su sve systemske datoteke tekućeg S-vektora uskladištene na odvojenoj particiji od aplikativnih datoteka, tekućem S-vektoru treba dodeliti najviši težinski faktor „3“ (zahtevanog S-vektora). Ako su sve systemske i aplikativne datoteke uskladištene na istoj particiji HD dodeljuje se „0“, odnosno, za isti kriterijum ponderisanja za *stepen kvaliteta* kontrole pripisuje se:

- „3“, ako je 100% svih sistemskih i aplikativnih datoteka uskladištene odvojeno;
- „2“, ako je $\geq 75\%$ svih sistemskih i aplikativnih datoteka uskladištene odvojeno;
- „1“, ako je 50%-74% svih sistemskih i aplikativnih datoteka uskladištene odvojeno;
- „0“, ako kontrola nije implementirana (sve datoteke na istoj particiji HD).

Za istu kontrolu zaštite, prema kriterijumu ponderisanja: *obim i sadržaj*, mogu se grupisati u sledeću hijerarhiju: *proceduralne komponente, kontrole na nivou organizacije, kontrole operativnog sistema i odvajanje sistemskih i aplikativnih datoteka*.

Težinski faktori mogu se dodeliti svakoj od ovih grupa. Ukratko, izabrane ISO/IEC 17799 kontrole mogu se koristiti kao proceduralne komponente unutar S-vektora. Kontrole se mogu primeniti na različite sisteme na nivou organizacije, ili na individualne web aplikacije. Zahtevani težinski faktor pripisuje se na bazi relativnog **značaja kontrole zaštite** za organizaciju. U toku SSAM procesa, stvarni težinski faktor određuje se na bazi prethodno definisanih kriterijuma. Stvarni težinski faktor se upoređuje sa ciljanim. Kumulativni težinski faktori mogu se izračunati po grupama i podgrupama kontrola, po želji.

Osnovna prednost metodologije S-vektora je, što omogućava korišćenje dva relevantna standarda - CC i ISO/IEC 17799 koji obezbeđuju specifične kontrole S-vektora, dok SSE CMM model uspostavlja zreo i institucionalizovan okvir za upravljanje programom zaštite web aplikacije. Međutim, da bi se ove kontrole razvile, monitorisale, merile i kontrolisale neka infrastruktura zaštite mora biti već implementirana. Metodologija S-vektora sadrži *tehničke, proceduralne i strukturalne* komponente i zbog toga obezbeđuje sveobuhvatniju procenu bezbednosti web aplikacija nego ISO/IEC 17799, ili SSE CMM model pojedinačno.

Glavni nedostatak metodologije S-vektora je što u potpunosti nisu definisana preklapanja i redundantnosti između ISO/IEC 17799 i SSE CMM standarda, [73], [102], [104]. Za efektivnu implementaciju S-vektora, otvorena pitanja su: definisanje obima S-vektora; izbor rentabilnog

alata za procenu zaštite web aplikacija; implementacija S-vektora bez definisanja administrativnog okvira; definisanje obima potrebne infrastrukture zaštite; definisanje drugih strukturnih komponenti S-vektora (pored proceduralnih) i definisanje kriterijuma za izbor metrike za ponderisanje. Zato je *S-vektor još uvek više strategija nego konzistentna metodologija*. Dalje istraživanje potrebno je za: određivanje elemenata nekog S-vektora, definisanje procesa za mapiranje bezbednosnih zahteva za web aplikaciju u zahtevani S-vektor, definisanje procesa za određivanje težinskog faktora za ponderisanje (S-vektora) za web aplikaciju, razvoj pogodnog načina za menadžere za prezentaciju rezultata ponderisanja i postavljanja željenih težinskih faktora za skup web aplikacija i za procenu performansi metodologije S-vektora.

2.9. Pregled dostupnih istraživanja primena modela sazrevanja procesa zaštite

2.9.1. Uvod

Na osnovu dostupnih podataka, može se zaključiti da *koncept metrike* procesa IKT zaštite, a time i *kvaliteta procesa zaštite*, u velikoj meri nije jednoznačno određen, ali da postoji napor da se postigne jednoznačna kvantitativna, ili kvalitativna vrednost koja opisuje nivo nekih od atributa IKT zaštite. Tehnike merenja i određivanja kvaliteta procesa IKT zaštite, variraju u zavisnosti od bezbednosnih ciljeva i objekata merenja. Postoji nekoliko dostupnih klasifikacija za IKT metriku u odnosu na upotrebu, korisnike, primenjeni metod ili standard (n.p.r., CC, ili SSE CMM). Različite klasifikacije pomažu boljem razumevanju raznovrsnih oblasti primene metrika zaštite. Kada se uspostavlja program metrike, evaluacije i poboljšavanja kvaliteta procesa zaštite, na raspolaganju su brojna uputstva sa nekim zajedničkim karakteristikama, od kojih je najbitnija - *uspostavljanje bezbednosnih ciljeva*, [62], [88], [91].

Ubedljivo najkritičniji problem u metrici IKT zaštite je *neujednačenost terminologije*, kao osnove za uspešnu komunikaciju u projektima zaštite. Takođe postoji potreba za većom i neprekidnom interakcijom i deljenjem znanja između organizacija i nacionalnih interesnih zajednica i profesionalnih agencija za IKT zaštitu. Druga, ništa manje značajna, oblast koja zahteva pažnju, svakako je *razvoj svesti* vlasnika, menadžera i korisnika IKT sistema o potrebi zaštite i obezbeđivanja više resursa i više osposobljenog personala za IKT zaštitu.

Standardi i modeli kvaliteta proizvodnih procesa iz serije ISO 9000 standarda kvaliteta za industrijsku proizvodnju, dobro su poznati, konzistentni, međusobno komplementarni i dostupni u brojnim izvorima. Međutim, *standardi kvaliteta procesa zaštite* IKT sistema nisu obrađeni na istom nivou. Razlozi su brojni, a osnovni je što procesi zaštite informacija nisu tako dobro definisani i što najbolja praksa zaštite nije konzistentno pretočena u opšte prihvaćen i sveobuhvatan standard kvaliteta procesa zaštite. Tako na primer, *najbolju praksu zaštite* obrađuju tri standarda: **ISO/IEC 17799** (2.deo usvojenog BS 7799 standarda), **ISF 4.1.** standard najbolje prakse i **SSE CMM** model sazrevanja najboljih praksi i procesa zaštite. Sva tri standarda na različite i u određenoj meri nekomplementarne načine definišu i tretiraju najbolje prakse i procese zaštite. Brojni istraživači su dali veliki doprinos u otkrivanju kompatibilnosti i komplementarnosti ovih standarda. Rezultat takvih napora su, na primer, primena kompatibilnih elemenata standarda ISO/IEC 17799 i SSE CMM (ISO/IEC 21827) u metodologiji vektora zaštite (S-vektora) za zaštitu web aplikacija, [95], [10], [88], [91], [102], [104], [106], [107].

2.9.2. Dostupna istraživanja primene modela sazrevanja procesa zaštite

U raspoloživim i dostupnim izvorima, pre svega u bazama znanja na Internetu, prve informacije o generičkom modelu sazrevanja procesa zaštite pojavile su se 1995. godine, [11]. Razvoj SSE CMM modela inicirali su NSA i DoD, SAD (1993.), a projekat razvijao i testirao u pilot

projektima u poverljivom okruženju, SEI Institut Univerziteta *Carnegie Mellon*, SAD do 1999. godine, kada su objavljene verzija SSE CMM v.2.0 i SSAM metod (*Security System Appraisal Method*) v.2.0. SSE CMM model je prihvaćen kao ISO/IEC 21827 standard, jedinstven te vrste u svetu, 2002. godine, [53].

SSE CMM model i standard namenjen je primarno za merenje zrelosti i sazrevanje procesa zaštite i kapaciteta za generisanje procesa zaštite. Poslednja verzija SSE CMM v.3.0 modela procesa zaštite objavljena je 2003. godine, kada je model proširen na 22 oblasti procesa (11 inženjerskih, 5 projektnih i 6 organizacijskih), [102], a poslednja verzija SSAM v.2.0 metoda evaluacije, objavljena je 1999. godine, [101].

SSE CMM v.3.0 model dobro je opisan u dokumentu [102], uključujući opise strukture modela – *dimenzije primene* oblasti procesa (OP) i *dimenzije kapaciteta/zrelosti* procesa (CL/ML), bazičnih i generičkih praksi (BP i GP) i opštih karakteristika (CF). Međutim, opis *dualne* - procesne i sistemske *metrike* za merenje zrelosti i progresivnog sazrevanja (poboljšavanja) procesa zaštite, koja je inherentno svojstvo SSE CMM modela, nije adekvatan, celovit i eksplicitan u istom dokumentu. Metriku SSE CMM modela opisali su brojni autori u kontekstu istraživanja različitih aplikacija modela i drugih metoda metrika IKT zaštite. U tom smislu bilo je potrebno istraživati metriku SSE CMM modela kroz brojne autorske radove, [10], [23], [27], [28], [32], [35], [36], [38], kao i razumeti osnovnu prednost ovog modela u odnosu na druge korišćene metode metrika IKT zaštite, a posebno u odnosu na opšte prihvaćeni standard zaštite ISO/IEC 17799, kojem upravo nedostaje bilo kakva metrika IKT zaštite.

SSAM metod evaluacije procesa zaštite, koji se bazira na SSE CMM modelu, dobro je opisan u dokumentu [101], uključujući uzorke ključnih *radnih dokumenata* i toka procesa metoda evaluacije. Međutim, slabije su opisani ukupni kriterijumi i metrika za odlučivanje o validnosti dokaza i podataka o nivou implementacije i institucionalizacije BP i GP, kao i sam proces *verifikacije* tih dokaza i podataka u odnosu na referentni SSE CMM model. U samom dokumentu nije dovoljno istaknuta prednost *verifikacionog tipa* SSAM metoda evaluacije, u odnosu na ranije metode evaluacije procesa, koji samo *otkrivaju*, ali ne i *verifikuju* postojanje dokaza o implementaciji praksi i procesa evaluiranih prema nekom referentnom modelu. Ovaj aspekt kvaliteta SSAM metoda evaluacije nije eksplicitno istaknut u dokumentu SSAM metoda, [101], kao što je taj aspekt istaknut u SCAMPI v.1.2 metodu evaluacije, [98] na bazi CMMI v.1.2 modela, [20]. Zašto metrika svih CMM modela procesa, kao i njena praktična primena, nisu posebno i eksplicitno istaknuti u glavnoj literaturi, pretpostavka je da je ta *veština* namenjena za praktičnu obuku i sertifikaciju SSAM evaluatora od strane akreditovanih SEI instruktora za SSAM evaluaciju. Naime, SSAM metod je primarno namenjen da evaluaciju obavlja SEI akreditovan i osposobljen tim za evaluaciju (od 3-7 članova), od čega najmanje 2 sertifikovana evaluatora po jednom evaluiranom projektu. Međutim, SSAM metod evaluacije procesa zaštite omogućava i samo-evaluaciju, uz dodatni napor pojedinaca u organizaciji koji poznaju neki od ranijih modela i standarda kvaliteta procesa i mogu da shvate proces SSAM evaluacije, način prikupljanja, verifikacije i vrednovanja dokaza o implementaciji BP i GP izabranih OP za evaluaciju, kao i da jezički i semantički prilagode originalnu terminologiju (na engleskom jeziku) i obezbede primenu metoda u realnom kontekstu evaluiranog entiteta.

Razvojem integrisanih CMM modela (iCMM i CMMI) u koje su implementirana sva pozitivna iskustva iz primene CMM klase modela, inicirani su projekti (NSA, DoD SAD, [118]), za usaglašavanje SSE CMM i CMMI v.1.1 (2004), SSAM i SCAMPI *Appraisal* metoda (2005) i SSE CMM i CMMI v. 1.2 (2006), zbog daleko šire primene CMMI modela procesa, koji su intergrirali širu klasu najboljih praksi procesa za *proizvodnju*, *akviziciju* i *servise*, od SSE CMM modela procesa zaštite. Međutim, kako CMMI modeli nemaju nikakve OP za IKT zaštitu, pošto se **OP – Upravljanje rizikom** odnosi na rizik projekta i ne tretira bezbednosni rizik razvijanog/evaluiranog sistema, usaglašavanje je predloženo sa ubacivanjem 4 nova generička cilja (GG) sa pripadajućim OP, GP, SP, SG i drugim komponentama (istraživanje je u toku), namenjena samo za bezbednosni aspekt IKT sistema. Rad na usaglašavanju ova dva modela i pripremi CMMI v.1.2 modela za primenu u oblasti zaštite počeo je početkom 2007. godine u SEI institutu.

Generalno, svi dostupni podaci o klasi razvijenih CMM modela, dovoljni su za razumevanje strukture, toka procesa i osnovnih kriterijuma za primenu modela u nekoj tipičnoj, ali ne i konkretnoj organizaciji i realnom kontekstu, uključujući kulturu rada, nivo i kvalitet komunikacije u realizaciji projekata i nivo zrelosti standardnih procesa odnosno organizacije. Sa tog aspekta, potrebno je *verifikovati primenljivost* modela sazrevanja procesa u realnom projektu i kontekstu aplikacije modela procesa i metoda evaluacije.

Za *verifikaciju primenljivosti* SSE CMM modela sazrevanja procesa zaštite i SSAM metoda evaluacije i poboljšavanja tih procesa u realnom kontekstu, u istraživačkom delu rada izabran je složeni projekat evaluacije i poboljšavanja tekućih procesa za razvoj, implementaciju i održavanje PKI sistema (CA i drugih modula) na bazi *Microsoft* PKI tehnologija i *Windows* platformi, na tri srodna projekta u preduzeću *E.Smart Systems*, Beograd.

3. Ciljevi istraživanja

3.1. Osnovni problemi zaštite informacija

Za postavljanje hipoteza i definisanje ciljeva istraživanja u ovom radu razmatrani su opšte prihvaćena i statistički obrađena brojna teorijska istraživanja i iskustva iz prakse zaštite IKT sistema: FBI, SANU *Institute* i NIST –SAD, FAPSI-Ruska federacija, BSI – Nemačka, BSI – V. Britanija, Australija i Kanada, kao i brojni standardi zaštite, relevantni za predmet istraživanja. Na osnovu prikupljenih informacija i saznanja postavljene su opšta i osnovne hipoteze i definisani ciljevi istraživanja u ovom radu.

Osnovna iskustva, gotovo zajednička za sve razmatrane izvore, svakako su nedovoljno razvijena svest o potrebi zaštite, sporo menjanje te svesti, čak i u informatički razvijenim društvima, alociranje nedovoljnih resursa za zaštitu i nedovoljan broj osposobljenih specijalista IKT zaštite po organizacijama. U prilog tome je i činjenica da je *Svest o potrebi zaštite* definisana kao jedan od 9 fundamentalnih, generalno prihvaćenih principa zaštite (**GAISP** - *Generally Accepted Information Security Principles*), [29], osnovnih gradivnih blokova svake metodologije za razvoj programa i sistema zaštite. Ovom treba dodati i tipično nedovoljan broj stručnih i osposobljenih specijalista zaštite, potpuno posvećenih borbi protiv zloupotreba IKT sistema i na raspolaganju poslovnim sistemima.

Relevantni su problemi i za upravljanje kvalitetom procesa IKT zaštite, kao što su:

- višeznačnost koncepta „*metrike*“ u IKT zaštiti i teškoće u dobijanju kvantitativnih mernih rezultata za objekte IKT zaštite, zbog niske objektivnosti rezultata merenja i problema generalizacije i poređanja mernih rezultata;
- teškoće u merenju operativnih kontrola zaštite, jer je teško predvideti stvarno funkcionisanje sistema zaštite;
- sama priroda oblasti IKT zaštite, gde uvek postoji rizik od otkrivanja i iskorišćavanja ranjivosti sistema, kao i
- konstantan problem ubeđivanja menadžmenta i vlasnika sistema o potrebi zaštite.

Posledice slabog razvoja svesti o potrebi zaštite korisnika, a posebno menadžera i vlasnika sistema brojne su, a glavne su sporo prihvatanje realnih pretnji i implementacija, uglavnom, skupih i najčešće redundantnih **reaktivnih sistema zaštite**, koji reaguju **samo** na *poznate pretnje*. Neadekvatna je i borba protiv zloupotreba IKT sistema i rastućeg kompjuterskog kriminala, u poređenju sa brzinom razvoja IKT sistema i sve novijih i sofisticiranijih tipova pretnji za umrežene sisteme, povezane preko nebezbednog Interneta, [82]. Jedno od skupljih i relativno manje dostupnih rešenja ovog problema je razvoj planiranog, dobro definisanog, dokumentovanog i upravljanog **proaktivnog sistema zaštite**, koji reaguje na *poznate* i *nepoznate pretnje*, [57].

Druga, korisnički prihvatljivija mogućnost usmerena je na dobro definisanje i neprekidno poboljšavanje procesa zaštite. Primenom sistem-inženjerskog i procesnog pristupa, a posebno modela sazrevanja procesa zaštite - SSE CMM modela/metoda, organizacije mogu raspoloživim resursima i sa prihvatljivom dinamikom **razvijati i progresivno poboljšavati procese zaštite do uspostavljanja optimalnog programa zaštite**, [13], [102] i implementirati **sisteme najbolje prakse zaštite** u kombinaciji sa analizom rizika u realnom okruženju [109], [102]. U skladu sa realnim ljudskim, finansijskim, tehnološkim i vremenskim resursima, organizacija sama bira polazni nivo zrelosti procesa zaštite za poboljšavanje, željene (referentne) nivoe profila procesa zaštite kojima teži i dinamiku realizacije pojedinačnih projekata za poboljšavanje individualnih procesa (OP), ili grupe procesa zaštite.

3.2. Hipoteze istraživanja

Polazeći od široko prihvaćenih definicija *procesa zaštite*, kao transformatora ulaznih u izlazne parametre, sa očekivanim povećanjem vrednosti na izlazu i kao integratora *metodologije zaštite*, *tehnologije zaštite* i *osposobljenih ljudi*, motivisanih za izvršavanje procedura i metoda i upotrebu tehnika i alata zaštite, a uzimajući u obzir relativno visoku cenu tehnologija zaštite i nedovoljnu raspoloživost specijalista zaštite, proizilazi da se ovi nedostaci mogu optimalno kompenzovati usmeravanjem pažnje vlasnika sistema na kvalitet i stalno poboljšavanje procesa zaštite. Za određivanje ciljeva istraživanja postavljene su jedna **opšta** i tri **osnovne** hipoteze za istraživanje.

Opšta hipoteza istraživanja: Savremeni IKT sistemi pretežno poseduju **neformalno** izvršavane procese zaštite, gde korisnici slabo planiraju i dokumentuju aktivnosti zaštite, delimično, ili nikakao konfigurišu raspoložive (pod)sisteme zaštite u prirodnom OS računarskog sistema (NOSSS), a od komplementarnih alata zaštite najčešće koriste mrežne barijere (*firewalls*) i antivirusne programe (AVP). Zbog relativno visokih troškova adekvatne tehnologije zaštite i generalno slabo razvijene svesti o potrebi zaštite vlasnika sistema i korisnika, organizacije radije prihvataju svaki model koji omogućava razvoj i implementaciju **optimalnog sistema zaštite** - rentabilnog sa aspekta odnosa troškova i efektivnosti, u odnosu na realne potrebe i raspoložive resurse, a da ne uključuje samo akviziciju skupih tehnologija i retkih i skupih specijalista zaštite. Brojni standardi, modeli i okviri IKT zaštite imaju različite pristupe zaštiti, specifične prednosti i nedostatke, ali vrlo mali broj, ili gotovo ni jedan od njih nije dovoljan sam za sebe za rešavanje svih problema zaštite. Klasa modela za sazrevanja kapaciteta integrisanih inženjerskih, projektnih i organizacijskih procesa (CMM tipa), obezbeđuje mogućnost razvoja optimalnog programa i sistema zaštite sa progresivnim sazrevanjem procesa i kapaciteta za generisanje tih procesa u skladu sa raspoloživim resursima i dinamikom prihvatljivom za organizaciju.

Osnovne hipoteze istraživanja: U klasi CMM modela sazrevanja procesa, SSE CMM model i metod za merenje zrelosti procesa i progresivnog sazrevanja (poboljšavanja) procesa i kapaciteta za izvršavanje procesa zaštite, obezbeđuje metodologiju planiranog, upravljanog, dobro definisanog, kvantitativno kontrolisanog i ponovljivog samo-razvoja procesa optimalnog sistema zaštite. Sa aspekta realne primenljivosti modela sazrevanja procesa - SSE CMM za zaštitu informacija i **predmeta istraživanja** ovog rada, uspostavljene su sledeće osnovne hipoteze:

1. Bilo koja primena SSE CMM modela procesa zaštite zahteva najmanje - da se ti **proces i izvršavaju**, čak i neformalno i *ad hock*. Dakle, praktična primena SSAM metoda za evaluaciju i poboljšavanje tekućih procesa ESS za uspostavljanje **PKI (infrastruktura sa javnim ključem)**, sertifikacionog tela (CA) i drugih modula PKI na bazi SSE CMM modela, zahteva da je **PKI sistem uspostavljen, a PKI moduli operativno funkcionalni**. CA, kao glavni funkcionalni modul PKI sistema integrisanog u IKT sistem poslovnog sistema, minimalno mora imati razvijene i implementirane svoje osnovne funkcionalne module i da se procesi izvršavaju najmanje neformalno, sa nepotpunom dokumentacijom i planiranjem.
2. **Kvalitet procesa zaštite CA**, može se povećavati *optimalno* i *progresivno*, na bazi rezultata SSAM metoda evaluacije i metrike SSE CMM modela za merenje zrelosti procesa i sazrevanja kapaciteta za generisanje tih procesa, u skladu sa **akcionim planom** utvrđenih prioriteta za poboljšavanje procesa i raspoloživim resursima evaluirane organizacije.
3. **Dinamku realizacije** pojedinačnih projekata za otklanjanje SSAM evaluacijom otkrivenih slabosti i **prioritetno poboljšavanje procesa**, ili grupe procesa CA, racionalno je planirati tako da se do najviših nivoa zrelosti (CL3 - CL5) poboljšavaju samo oni procesi (tipično SSE-inženjerske OP) koji proizvode najveću vrednost za organizaciju, što podrazumeva da su organizacijski i projektni procesi dobro planirani i kontrolisani (CL2-CL3).

3.3. Ciljevi istraživanja

Na osnovu razmatranih iskustava iz teorije i prakse zaštite, a na bazi predmeta istraživanja i postavljenih istraživačkih hipoteza, definisani su sledeći **ciljevi istraživanja**:

1. **Izvršeni pregled i komparativna analiza** osnovnih karakteristika, kompatibilnosti i komplementarnosti SSE CMM modela sazrevanja procesa zaštite i drugih relevantnih modela i standarda procesa zaštite (ISO/IEC 17799, ISO 9000/1, CMMI i dr.);
2. **Konstruisana i terminološki prilagođena radna dokumenata** SSAM i SSE CMM modela, za prikupljanje mernih podataka i dokaza za merenje nivoa zrelosti, evaluaciju i poboljšavanje procesa zaštite evaluirane organizacije;
3. **Defnisan željeni profil nivoa zrelosti procesa** evaluirane organizacije na bazi: procesa *najbolje prakse zaštite*, zahteva Sponzora evaluacije, ili preporuke evaluatora;
4. **Evaluiran i izmeren profil tekućih procesa** evaluirane organizacije sa definsanim resursima u planiranom obimu i vremenskom periodu i *verifikovana primenljivost* SSE CMM modela i SSAM metoda evaluacije procesa zaštite;
5. **Analizirani rezultati evaluacije** - *profil procesa i glavni nalazi* tekućih procesa evaluirane organizacije u odnosu na **željeni profil procesa** i

Izrađen akcioni plan projektnih zadataka za optimalno i progresivno poboljšavanje tekućih procesa i dostizanje projektovanog, željenog profila procesa u skladu sa prihvatljivom dinamikom i raspoloživim kapacitetima evaluirane organizacije.

4. Istraživački rad

4.1. Predmet i obim istraživanja

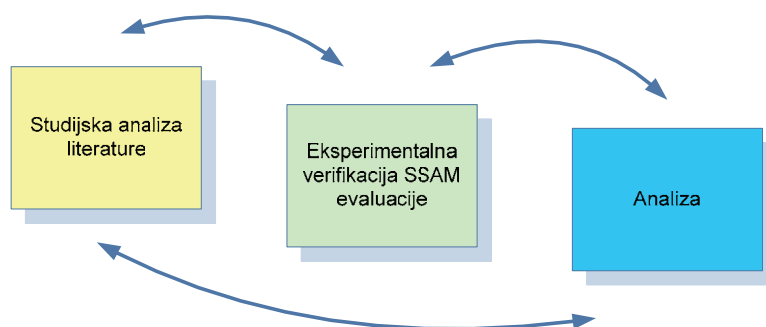
Opšti predmet istraživanja ovog rada je kako se, pod kojim uslovima i sa kolikim resursima, SSE CMM model sazrevanja procesa zaštite (standard ISO/IEC 21827) i metod SSAM evaluacije i poboljšavanja procesa na bazi tog modela, mogu praktično primeniti za razvoj i upravljanje *optimalnog programa* komponenti i sistema zaštite, evaluaciju i poboljšavanje procesa zaštite u realnom kontekstu organizacije i okruženja.

Poseban predmet istraživanja je verifikacija praktične primenljivosti SSE CMM modela i **SSAM** metoda, kroz istraživački zadatak *evaluacije i plana poboljšavanja* tekućih procesa preduzeća *E-Smart Systems (ESS)* sa sedištem u Beogradu, za uspostavljanje PKI sistema (CA i drugih PKI modula). SSAM metod evaluacije primenjuje kriterijum *verifikacije* objektivnih dokaza o izvršavanju, implementaciji i institucionalizaciji bazičnih (BP) i generičkih (GP) praksi procesa zaštite. Evaluacija tekućih procesa **ESS** za uspostavljanje PKI sistema i CA u ovom istraživačkom radu, vrši se sa ciljem poboljšavanja postojećih procesa do uspostavljanja željenog profila nivoa kapaciteta stabilnih procesa kroz predloženi *akcioni plan*.

Obim istraživanja uključuje SSAM evaluaciju tekućih praksi i procesa **ESS** na projektima razvoja, implementacije, integracije i operativne administracije CA PKI sistema: **(P1)-Kreditnog biroa udruženih banaka Srbije (KB UBS)**, **(P2)-Hemofarma** i **(P3)-RZII**, u odnosu na 22 oblasti procesa (OP) SSE CMM modela. Za realizaciju procesa evaluacije formiran je tim za evaluaciju (TE) od pet sertifikovanih **evaluatora sa pravom glasa** sa *Univerziteta Singidunum* i četiri zaposlena u evaluiranoj organizaciji, kao **posmatrača** bez prava glasa u odlučivanju TE. U pred-pripremoj fazi evaluacije, vodeći *evaluator 1* izrađuje nacrt *Plana evaluacije* i priprema druga radna dokumenta, obezbeđuje prihvatanje Sponzora i menadžera evaluiranih projekata, upoznaje sve članove TE i učesnike evaluacije sa osnovnim elementima SSE CMM modela i SSAM metoda evaluacije i priprema ih za fazu evaluacije na lokaciji. Na osnovu rezultata evaluacije, TE izveštava Sponzora i dostavlja **tekući profil** nivoa kapaciteta 22 oblasti procesa, **glavne nalaze** o snazi i slabostima procesa ESS i predlog zadataka **akcionog plana** za poboljšavanje procesa.

4.2. Metodi istraživanja

U istraživačkom procesu i postupku primene SSE CMM modela i SSAM metoda za evaluaciju i profilisanje procesa **ESS**, primarno su korišćeni opisani SSE CMM model i metod procesa i SSAM metod evaluacije na bazi tog modela. Model primenjenog **osnovnog metoda** istraživanja u ovom radu prikazan je na Slici 4.1.



Sl. 4.1. Model osnovnog metoda istraživanja

U okviru opšteg SSAM metoda, korišćene se inženjerske tehnike **deskriptivnih, eksplorativnih i kauzalnih** istraživanja, izabrane na osnovu: kriterijuma prikupljanja metričkih podataka SSAM instrumentima – pozitivnim odgovorima i ponuđenim dokazima iz *upitnika i intervju*; verifikacije objektivnih dokaza (SSAM *PIID*) i nalaza neposrednom opservacijom o implementaciji i institucionalizaciji praksi i procesa, koji potvrđuju nivo zrelosti tekućih procesa. Ove tehnike, pojedinačno i u kombinacijama, primenjujane su u istražnom postupku u sklopu sledećih SE metoda i analiza:

1. Posebnih metoda:

- *desk metoda* za proučavanje stručne SSE CMM i SSAM dokumentacije i prikupljenih metričkih podataka i dokaza o implementaciji praksi i procesa **ESS** i komparativnu analizu iskaza, dokaza i nalaza u cilju otkrivanja nekonzistentnosti, i anomalija u izvršavanju procesa **ESS**,
- *metoda terenskog posmatranja (opservacije)* za prikupljanje metričkih podataka i dokaza,
- *metoda modelovanja procesa SSAM evaluacije* primenom *BPWin CASE* alata,
- *metoda razgovornika - upitnika i intervju* za prikupljanje metričkih podataka za potvrdu implementacije i institucionalizacije praksi i procesa u skladu sa SSE CMM modelom i
- *statističkog metoda* za proračun procenta izvršenih BP, GP i OP i procenu nivoa implementacije i institucionalizacije BP i GP praksi i nivoa zrelosti procesa (OP).

2. Inženjerskih analiza:

- *analiza međusobnog uticaja*, radi otkrivanja anomalija, protivrečnosti i nedoslednosti iskaza anketiranih u *upitnicima i intervjuima*, dokaza i nalaza o kvalitetu izvršavanja BP i GP, u cilju donošenja odluke o nivou zrelosti procesa sa konsenzusom tima za evaluaciju,
- *metod analize rizika projekta* za procenu rizika projekta evaluacije procesa **ESS**,
- *metod funkcionalne analize* za analizu efektivnosti procesa **ESS**,
- *metod korelacione analize* za procenu korelativnosti objektivnih dokaza (porekla iz više izvora), obezbeđenih za afirmativne odgovore u *upitnicima i intervjuima*, u fazi konsolidovanja nalaza i određivanja nivoa zrelosti OP konsenzusom svih članova TE sa pravom glasa.

U okviru opšteg SSAM metoda evaluacije korišćene su grupe kvalitativnih logičkih metoda, kao što su metodi *apstrakcije i konkretizacije, generalizacije i specijalizacije, indukcije i dedukcije*.

4.3. Tok izvršavanja projekta SSAM evaluacije ESS

Istraživački projekat SSAM evaluacije procesa **ESS** izvršen je u celini skladu sa standardnim *procesom SSAM evaluacije*. Faze procesa SSAM evaluacije implementirane su kroz sledeće ključne aktivnosti:

- *identifikacija i definisanje problema*: na uvodnom sastanku sa menadžmentom ESS, kroz inicijalnu procenu stanja procesa u ESS, obima evaluacije, resursa za izvođenje evaluacije, osposobljenosti TE, podrške Sponzora evaluacije, kao i ocenu menadžmenta o ukupnim kapacitetima i zrelosti izvršavanja procesa **ESS**,
- *priprema i planiranje istraživanja*: na uvodnom sastanku pripreme TE; razvojem radnih dokumenata - *upitnika, plana intervju*, za *prikupljanje, obradu i čuvanje objektivnih dokaza* i izborom vremena i lokacije za evaluaciju na terenu,
- *planiranje uzoraka istraživanja*: u dogovoru sa Sponzorom evaluacije o raspoloživosti resursa **ESS**, izboru projekata za evaluaciju, sagovornika, vremena i lokacija za prikupljanje iskaza i objektivnih dokaza,
- *sakupljanje podataka i dokaza*: kroz sakupljanje preliminarne odgovora i dokaza *upitnicima* i evaluaciju na terenu i sakupljanje odgovora i dokaza na istraživačka pitanja kroz *intervjue* rukovodilaca i praktičara mevaluiranih projekata,

- *obrada i analiza* podataka kroz: konsolidovanje i analizu preliminarne dokaza i odgovora na *upitnike*; analizu odgovora i dokaza za istraživačka pitanja sakupljenih kroz *intervjue*; konsolidovanje dokaza i opservacija sakupljenih kroz *upitnike* i *intervjue* u DTS dokumentu; ponderisanje metričkih podataka u fazi donošenja odluka sa konsenzusom TE sa pravom glasa o nivou kapaciteta evaluiranih procesa i glavnim nalazima evaluacije,
- *donošenje odluka i izveštavanje*: na bazi konsolidovanih dokaza i nalaza sa konsenzusom članova TE sa pravom glasa, generiše se izveštaj o nivou kapaciteta evaluiranih procesa i glavnih nalaza u formi pogodnoj za prezentaciju Sponzoru – pita dijagram, tabela ili histogram profila procesa.

Identifikovanje stanja: Opšta ocena menadžmenta ESS je da tekući procesi koje organizacija koristi za uspostavljanje PKI sistema (CA i drugih modula) nisu stabilni i dovoljno zreli, ali da **ESS**, kao poslovni partner *Microsoft*-a, u svakom projektu primenjuju najbolje prakse *Microsoft* (**MS**) PKI tehnologije. Generalno, projektni timovi **ESS** izvršavaju procese regularno po dobijanju zahteva klijenata i sklapanju poslovnog ugovora za razvoj i implementaciju PKI sistema na bazi **MS** PKI tehnologije i Windows platformi, ali u velikoj meri neformalno – sa nedovoljnim planiranjem i dokumentovanjem. Tekući procesi su planirani, a tehničke aktivnosti kontrolisane isključivo na nivou tekućeg projekta, ali se ne koristi u punoj meri sistem indikatora stanja progressa procesa u kontrolnim tačkama (*benchmarking*), ne dokumentuju rezultati kontrole i ne primenjuje se striktno analiza rizika za izvođenje projekta. Procesu su u operativnoj fazi monitorisani i upravljani, kroz izveštavanje korisnika o incidentima u primeni aplikacija i automatizovanim generisanjem izveštaja o stanju sistema i dostavljanjem putem e-mail poruka na server lokalne mreže **ESS**. Međutim, organizacija ne planira i ne vrši regularnu analizu indikatora stanja bezbednosti, iako su obezbeđene metrike za prikupljanje ovih podataka, uključujući i log datoteke događaja u operativnoj primeni aplikacija, koje obuhvataju i bezbednosno relevantne događaje. **Neki** upravljački, operativni, a posebno tehnički procesi zaštite, dokumentovani su u poslovnom sistemu **ESS** kroz detaljne **MS** tehničke procedure i **izvršavaju se na nivou projekta**. Iste procedure se prilagođavaju za sledeći projekat u skladu sa zahtevom organizacije i realnim okruženjem. **ESS** nema formalno definisane, opisane i standardizovane procese organizacije; nema razvijenu familiju standardnih procesa, niti poseban repozitorijum (biblioteku) imovine procesa organizacije. Osnovni problem su ljudski resursi, jer se popuna stručnim kadrovima planira prema zahtevima za projektovanje, razvoj, implementaciju i integraciju PKI sistema na bazi **MS** Windows platformi. Politike zaštite izrađene su na nivou ključnih komponenti PKI sistema, ali nije izrađena politika zaštite na nivou organizacije. Takođe nedostaju politika i sistem za upravljanje dokumentacijom.

Neformalnim izvršavanjem procesa **ESS**, ispunjena je osnovna hipoteza za primenu **SSE CMM** modela procesa zaštite i **SSAM** metoda za evaluaciju tekućih procesa **ESS** na bazi tog modela. **SSE CMM** je prihvaćen, kao dobar model za **definisanje i poboljšavanje kapaciteta** procesa **ESS** za razvoj i implementaciju zrelih inženjerskih, projektnih (upravljačkih) i organizacijskih procesa u **ESS**. Primena **SSE CMM** modela i metoda obezbeđuje **ESS** organizaciji da planira **razvoj optimalnog programa** i implementira **sistem najboljih praksi zaštite**, prema kojem **ESS** sama bira polazni nivo poboljšavanja procesa zaštite, željene nivoe procesa zaštite kojima teži i dinamiku realizacije projekata za poboljšavanje individualnih, ili grupe procesa u skladu sa realnim ljudskim, finansijskim, tehnološkim i vremenskim resursima organizacije.

Projekat **Evaluacije tekućih procesa ESS**, izvršen na tri srodna evaluirana projekta, trajao je od 19.06.–25.07.2007. godine. Za realizaciju projekta razvijeni su **SSAM radni materijali** koji se nalaze na **CD-ROMu** u prilogu rada. **SSAM radni materijali** sadrže četiri foldera: **1. Radna dokumenta**, **2. Administrirani upitnici** i **3. Realizacija SSAM evaluacije ESS procesa**.

U folderu **1. Radna dokumenta** data su sledeća *radna dokumenta* (01-14) metoda evaluacije:

1. Plan evaluacije (uključujući dinamički plan) i prateće priloge – Prilog 1;
2. Proces **SSAM** evaluacije – detaljan opis, Prilog 2 i **BPWin** model toka aktivnosti faza procesa **SSAM** evaluacije - Prilog 2A.

3. SSAM zbirni upitnici za svaku od 22 OP SSE CMM modela za prikupljanje preliminarnih podataka o izvršavanju i kvalitetu izvršavanja - sa dokazima o implementaciji i institucionalizaciji BP i GP praksi procesa ESS, prema SSE CMM modelu procesa, sa procedurom razvoja Upitnika i sugestijama za Izbor sagovornika za Upitnik - Prilog 3;
4. Kontrolna lista zadataka za pripremu procesa evaluacije na terenu, kao pomoćni alata evaluatora dat je u –Prilog 4.
5. Scenario komunikacija u procesu evaluacije –Prilog 5.
6. Elektronski radni dokument (DTS Excel tabela) za elektronsku obradu sakupljenih podataka iz Upitnika i Intervjua i kompjutersko generisanje tekućeg profila procesa ESS – Prilog 7;
7. Uputstvo za popunu DTS tabele – Prilog 7A;
8. SSAM PIID radni dokument – identifikatori implementacije i instiucionalizacije BP i GP praksi – Prilog 8.
9. Pomoćna tabela za evidenciju dokaza (PII) za implementaciju praksi – Prilog 9.
10. Kriterijumi odlučivnja u SSAM metodu evaluacije – Prilog 10.
11. Uputstvo za SSAM evaluaciju – Prilog 11.
12. SSE CMM model sa detaljnim opisom OP i BP - Prilog 12.
13. SSE CMM model sa detaljnim opisom CL, CF i GP - Prilog 13 i
14. SSAM metod evaluacije - Prilog 14.
15. Rezultati *Appraisal Assistant SSE CMM/SCAMPI aplikacije* za interaktivnu, automatizovanu SCAMPI v. 1.2 A tipa evaluaciju procesa zaštite na bazi SSE CMM modela - Prilog 15.

U folderu **2. Administrirani upitnici** dati su administrirani upitnici za 22 pojedinačne OP.

U folderu **3. Realizacija SSAM evaluacije ESS procesa** ostali materijali grupisani su u 4 foldera: 1. *Prilozi plana evaluacije*; 2. *Plan rada tima za evaluaciju*; 3. *Plan intervjuja* i 4. *Rezultati SSAM evaluacije tekućih procesa ESS* i 5. *Predlog zadataka akcionog plana poboljšavanja procesa ESS*.

U **Prilozima plana evaluacije** razvijena su ostala pomoćna radna dokumenta za praćenje realizacije plana evaluacije kao što su: (A) odobravanje TE, (B) odobravanje procesa evaluacije, (C) distribuciona lista materijala evaluacije, (D) promenljivi parametri SSAM evaluacije, (E) gantogram aktivnosti TE, (F) dinamički plan evaluacije, (G) zahtev za potrebne reursrse za rad TE, (H) radni dokument za upravljanje SSAM PII dokazima, (I) kompletirana Excel tabela za evidenciju dokaza, (J) radni dokumenti za praćenje kretanja dokaza, (K) potvrda o izvršenoj evaluaciji procesa ESS i (L) lista priloga plana evaluacije.

U **Planu rada tima za evaluaciju** razvijeni su dnevni planovi rada TE za 14 radnih dana prema dinamičkom planu procesa SSAM evaluacije.

U **Planu intervjuja** data su sva pitanja za istraživanje praćena planom intervjuja i angažovanjem članova TE, posle administracije upitnika, zatim posle intervjuisanja lidera projekata i praktičara i na kraju pitanja za razjašnjavanje kroz dodatni intervju.

U **Rezultatima SSAM evaluacije tekućih procesa ESS** date su DTS radna tabela za profilisanje procesa, preliminarni rezultati SSAM evaluacije procesa ESS, profil nivoa zrelosti tekućih procesa ESS i konačni nalazi SSAM evaluacije.

U **Predlogu zadataka akcionog plana poboljšavanja procesa ESS** date su predlog projekata za dugoročni akcion plan, predlog zadataka za kratkoročni akcioni plan, predlog zadataka za akcioni plan projektnog tima i opis faza i koraka procesa IDEAL za implementaciju plana poboljšavanja procesa. Akcioni planovi su definisani kroz zadatke i aktivnosti, bez konkretnog vremenskog plana, sastava projektnih timova, uloga i odgovornosti i drugih potrebnih resursa za definisanje projekta. Definisani zadaci u planiranim rokovima, obezbeđuju poboljšavanje svih organizacionih OP ESS (OP17-OP22) najmanje na CL2 nivo *planiranih i praćenih* procesa, poboljšavanje projektnih OP (OP12-OP16) najmanje na CL3 nivo *dobro definisanih* procesa i poboljšavanje

inženjerskih OP (OP012-OP11) na željeni nivo zrelosti kapaciteta (CL3 i viši), u skladu sa potrebama, raspoloživim resursima, poslovnim zahtevima i ciljevima ESS.

Radna dokumenta i pomoćni radni materijali, koji podržavaju proces SSAM evaluacije, namenjeni su za bolje razumevanje, efikasnije prikupljanje i analizu podataka i dokaza i donošenje odluka o nalazima i rezultatima evaluacije tekućih procesa **ESS**, a zbog obima nisu direktno uključeni u sadržaj rada.

4.4. Instrumenti istraživanja

Od istraživačkih tehnika korišćena je tehnika merenja i rangiranja nivoa kapaciteta i zrelosti evaluiranih procesa prema:

- kriterijumu realne zrelosti procesa SSAM metoda i SSE CMM modela,
- značaju BP i GP za *evaluiranu organizaciju ESS* i
- funkcionalnoj osetljivosti evaluiranih procesa.

U primenjenim instrumentima istraživanja – *upitnicima* i *intervjuima*, težište je bilo na **atidunalnim merenjima** kvaliteta izvršavanja BP, GP i OP na osnovu *stavova, mišljenja i iskaza* menadžera, projektanata, implementatora i praktičara evaluiranih procesa, kao i na **verifikaciji** objektivnih dokaza - dokumenata zaštite, izveštaja, planova i sl., koji ih podržavaju. Ovi dokazi su posebno značajni za *koraborativno* (iz više izvora) utvrđivanje korelacionih veza između pojedinih afirmativnih izjava, stavova i uverenja, sa jedne i dokaza, nalaza i opservacija o zrelosti izvršavanja, implementacije i institucionalizacije OP (BP i GP) iz različitih izvora, sa druge strane. Verifikacija dokaza odnosi se i na proveru *pokrivenosti* i *kompletnosti* dokaza za sva tri evaluirana projekta.

Za realizaciju **SAMM** procesa evaluacije i merenje kapaciteta procesa **ESS**, razvijena su brojna *radna dokumenta i pomoćni radni materijali*, koji su i instrumenti istraživanja u ovom radu.

4.5. Uzorkovanje dokaza i izveštavanje o sekundarnim nalazima

U SSE CMM modelu procesa zaštite, *Primeri proizvoda rada* bazičnih praksi OP, su evidentni *direktni dokazi* i objektivni indikatori implementacije BP i GP praksi; nabrojani su u modelu u opisu BP, ali bez neophodne numeracije za brže i preciznije praćenje u toku donošenja odluka u procesu konsolidacije dokaza i nalaza. Za potrebe istraživačkog rada originalno je razvijen dokument **SSAM PIID** (*Opis SSAM indikatora implementacije praksi*), prikazan u **Radnim dokumentima, Radni prilozi - Prilog P8. SSAM PIID** je namenjen za bržu i tačniju verifikaciju izvršavanja, implementacije i institucionalizacije praksi i kvantifikaciju prikupljenih metričkih podataka. **SSAM PII** mogu biti: *politike zaštite* organizacije (n .p.r. programska, na nivou IKT sistema i dr.), *primenjeni standardi* zaštite i kvaliteta procesa zaštite, *organizacione procedure* (npr. alokacije resursa, obuke), *planovi projekta zaštite* (npr. upravljanja konfiguracijom, reinženjeringa, planovi projekta uspostavljanja PKI sistema i testiranja funkcionalnosti CA i dr.), *procedure projekta* (npr. za reviziju, razvoj dokumentacije, analizu), *proces implementacije* (npr. projektna dokumentacija) i *kontrolni tragovi* (npr. dnevni red sastanka, stavke akcionog plana, izveštaji, log datoteke).

Ključni rezultat primene SSE CMM modela i SSAM metoda za profilisanje zrelosti procesa **ESS** je profil nivoa kapaciteta tekućih procesa **ESS**, ali je uobičajeno da su to i **sekundarni nalazi** o ključnim slabostima i snazi procesa evaluiranog entiteta. Definiše se tipično **6-7 glavnih nalaza**, što omogućava organizaciji da preciznije odredi prioritete projekata za poboljšavanje procesa koji najefektivnije i najefikasnije otklanjaju otkrivene slabosti i povećavaju proizvodne kapacitete organizacije. Ključni rezultati i sekundarni nalazi saopštavaju se Sponzoru evaluacije i

evaluiranoj organizaciji, na način i u formi koju zahteva Sponzor: pisani izveštaj, multimedijalna prezentacija sa usmenim obrazloženjem i grafičkim prikazima i sl.

4.6. Opis projekta SSAM evaluacije tekućih procesa ESS

- 1) **Organizacija evaluatora:** *Univerzitet Singidunum.*
- 2) **Primenjen metod:** SSAM metoda evaluacije na bazi SSE CMM modela procesa.
- 3) **Evaluairana orgnizacija:** *E-Smart Systems, Blagoja Parovića 28, Beograd, preduzeće za razvoj, implementaciju i održavanje PKI sistema na bazi Microsoft i drugih partnerskih tehnologija i Windows platformi.*
- 4) **Specifičnosti CMM u evaluairanoj orgnizaciji:** Evaluirana organizacija u dosadašnjoj praksi nije sertifikovala, ili na bilo koji način evaluirala, ili procenjivala svoje procese za uspostavljanje PKI sistema – CA i drugih funkcionalnih modula. Organizacija nije uvela sistem kvaliteta procesa i u celini je prihvatila SSE CMM model i standard (ISO/IEC 21827) sazrevanja procesa zaštite i SSAM metod za evaluaciju i poboljšavanje svojih tekućih procesa u ovom projektu. Organizacija je izrazila poseban interes da uključi svoja 4 zaposlena u TE u cilju uspostavljanja sistema kvaliteta i sticanja znanja i iskustava za samo-evaluaciju, uspostavljanje i kontinualno poboljšavanje svojih *standardnih* procesa.

Evaluirana organizacija i Sponzor evaluacije odredili su za SSAM evaluaciju na bazi 22 OP SSE CMM modela, tri tipična projekta koja najbolje reprezentuju tekuće procese ESS:

1. **P1**–PKI sistem i CA Kreditnog biroa udruženih banaka Srbije (KB UBS), Beograd;
 2. **P2**–PKI sistem i CA, fabrike za proizvodnju lekova Hemofarm, Vršac i
 3. **P3**–PKI sistem i CA, Republičkog zavoda za informatiku i Internet (RZII), Beograd.
- 5) **Tip evaluacije:** U fazi planiranja procesa *SSAM evaluacije tekućih procesa ESS* i određivanja obima evaluacije, Sponzor evaluacije je prihvatio da se primeni tip evaluacije: ***asistirana samo-evaluacija***.
- 6) **Tim za evaluaciju (TE):** U TE 5 evaluatora sa *Univerziteta Singidunum* sa CMMI sertifikatom imalo je pravo glasa. Na predlog *evaluatora 1*, Sponzor je prihvatio sugestiju za formiranje mešovitog tima i odredio 4 dodatna člana TE – ***posmatrača***, bez prava glasa i ostale učesnike u procesu evaluacije: *koordinatora za rad na lokaciji, izvršioca, rukovodioca i članove projektnih timova (P1, P2, P3) i praktičare.*
- 7) **Glavne funkcionalnosti evaluirane organizacije:** Prema SSE CMM modelu, ***ESS*** je tip organizacije koja funkcioniše kao: *korisnik sistema zaštite* – administrator CA ESS i faktor povernja svojih korisnika zaštite, *proizvođač komponenti sistema zaštite* - aplikacija za prilagođavanje PKI sistema, alata i sl., *provajder servisa zaštite* – izdavanje digitalnih sertifikata i drugih servisa CA, *integrator sistema* – PKI, CA i drugih modula u IKT sisteme drugih organizacija i *organizacija koja nabavlja nove tehnologije* i proizvode zaštite.

Osnovne funkcionalnosti koje ESS izvršava svojim poslovnim procesima su:

1. Projektuje, razvija, implementira i integriše PKI sisteme - CA i druge module, na bazi *Microsoft* PKI tehnologija i *Windows* platformi, uključujući i smart kartičnu tehnologiju za jaku autentifikaciju, u IKT sisteme državnih institucija, privrednih subjekata i drugih organizacija.
2. Održava, administrira i tehnološki modernizuje, ugovorom preuzete, implementirane PKI sisteme, CA i aplikacije u drugim organizacijama.
3. Administrira CA ESS - izdaje, održava, suspenduje i opoziva digitalne sertifikate korisnika -fizičkih i pravnih lica, kao poverljivi provajder usluga.
4. Prati razvoj *Microsoft* PKI, *smart kartičnih* i drugih relevantnih tehnologija i *Windows* operativnih sistema i primenjuje nova rešenja u svom radu.

8) Namena evaluiranih projekata

Namena evaluiranog projekta P1 je da unapredi i poveća kvalitet poslovanja KB UBS. KB UBS, u operativnom radu od 2004. godine, je nacionalna institucija za praćenje i monitorisanje solventnosti korisnika (građana) svojih klijenata: banaka, različitih fondova, korporacija, preduzeća i potencijalno drugih institucija, kao što su poreske i opštinske službe. Izveštaj KB UBS je osnovni element na bazi kojeg banka donosi odluku o davanju određenih servisa koje građani zahtevaju. *Osnovni funkcionali zahtevi* klijenata za razvoj elektronskog sistema KB UBS su: pristup kreditnom birou preko Internet veze, autentifikacija korisnika i autorizacija za razmenu informacija i XML format izveštavanja i razmene informacija. Projekat održava ESS.

Namena evaluiranog projekta P2 - Implementacija PKI i smart kartične tehnologije u Win 2003 okruženju, implementiranog u IKT sistemu *Hemofarma* u Vršcu i u operativnoj upotrebi od 2005. godine, u prvom redu je podizanje nivoa zaštite u IKT sistemu uvođenjem PKI infrastrukturne komponente zaštite i jake autentifikacije primenom smart kartica. Projekat održava ESS.

Namena evaluiranog projekta P3 - Model interne računarske mreže na MS platformi, implementiranog u RZII i u operativnoj upotrebi od jula 2006. godine, primarno je da se u IKT sistemu RZII obezbede *sve raspoložive funkcionalnosti* i nivo zaštite, koje MS tehnologije omogućavaju. Projekat održava ESS.

9) Proces SSAM evaluacije

Istraživačkim projektom SSAM evaluacije obuhvaćeni su tekući procesi **ESS** u odnosu na 22 OP SSE CMM modela, koji su formalno ili neformalno izvršavani ili implementirani u projektima **P1, P2 i P3**. Za evaluaciju procesa **ESS** striktno su primenjeni **proces** i **metod SSAM evaluacije** i **SSE CMM model** referentnih procesa. Dopusnene izmene metoda i modela i druga prilagođavanja opisana su u **poglavlju 5.3**.

Od početka pripremne faze procesa SSAM evaluacije (19.06.2007), TE je dobio posebnu prostoriju za rad u objektima ESS sa svim zahtevanim materijalnim resursima i opremom, u skladu sa SSAM metodom evaluacije. Već na uvodnom sastanku menadžment ESS je odredio sve učesnike procesa SSAM evaluacije iz **ESS- Sponzora, Koordinatora za rad na terenu, članove TE-posmatrača (4), lidere evaluiranih projekata i praktičare** za intervju i obezbedio njihovo učešće na pripremnom sastanku za upoznavanje svih učesnika projekta evaluacije sa ključnim elementima SSE CMM modela, SSAM metoda i specifičnostima evaluacije procesa ESS (25.06.2007). Predlog *Plana evaluacije*, pripremljen u pre-pripremoj fazi, usaglašen je sa Sponzorom i ažuriran po obimu evaluacije u toku administracije *upitnika*, tako što su izabrani projekti za evaluaciju **P2 i P3**, pored već određenog projekta **P1** (KB UBS). Prva revizija administriranih upitnika i konsolidacija dokaza TE sa liderima projekta **P1**, pokazala je da svi tekući procesi ESS nisu reprezentativno predstavljeni u projektu **P1** i, na osnovu pokrivanja, koraborativnosti i kompletnosti priloženih dokaza, ne daju ni približno realnu sliku o nivou zrelosti procesa i kapaciteta za generisanje procesa ESS, kao ni o stepenu institucionalizacije procesa. Naime, ESS kao strateški partner, u svom radu dominantno koristi tehnologije, standarde, politike i procedure procesa najbolje prakse *Microsoft-a* i drugih partnera, koje sa potrebnim odstupanjima i prilagođavanjima modifikuje od projekta do projekta, pa jedan projekat nije reprezentativan uzorak tekućih procesa ESS. Zato su pored planiranog **P1** projekta za evaluaciju izabrani projekti **P2 i P3**, približno istog tipa – *za razvoj, projektovanje, implementaciju i održavanje PKI sistema, CA i drugih modula na bazi Microsoft PKI tehnologije i Windows platformi* u drugim organizacijama, koji se izvršavaju tekućim procesima i kapacitetima ESS, na bazi specifičnih zahteva korisnika.

Za **verifikaciju elektronskih dokumenata**, kao objektivnih dokaza za implementaciju, izvršavanje i institucionalizaciju BP i GP praksi procesa **ESS** na tri evaluirana projekta, u radnoj prostoriji TE instaliran je interni **web portal** organizacije, tako da su članovi TE mogli neposredno zahtevati dokaze i direktnom *on line* opservacijom steći uvid u svaki elektronski dokument, koji se može prihvatiti kao dokaz za pozitivne odgovore iz *upitnika* i *intervjua*. Dokazi su dostavljani na dokumentovani zahtev rukovoca dokaza (evaluator 2) za određenim dokazima. Fizičke dokaze–

dokumenta u papirnoj formi dostavljao je koordinator rada na lokaciji, na dokumentovani zahtev rukovaoca dokaza, lično, ili preko članova TE – posmatrača (zaposlenih u ESS). Korišćenje dokaza u radu TE, rukovaoc dokaza je dokumentovao u standardnom formatu za praćenje traga kretanja dokaza. Svi zahtevani dokazi dostavljani su isti, ili sledeći dan, korišćeni za verifikaciju afirmativne izjave i vraćeni koordinatoru evaluacije na terenu neposredno posle korišćenja. Za intervjuisanje praktičara (administratora i operatera) na evaluiranim projektima, Sponzor je obezbedio direktan kontakt i sve potrebne uslove za intervjuisanje u radnoj prostoriji TE. TE je konsolidovao dokaze na grupnim sastancima sa konsenzusom članova TE sa pravom glasa, koristeći *Excel tabelu za evidenciju dokaza* i *SSAM PIID radne dokumente*, kao izvor direktnih indikatora implementacije BP i GP praksi prema SSE CMM modelu u procesima ESS, korišćenim za implementaciju evaluiranih projekata. *Excel tabela za evidenciju dokaza* korišćena je i za proveru tačnosti SSAM metoda evaluacije, generisanjem slučajnih uzoraka profila zrelosti pojedinačnih OP i upoređivanjem sa profilom OP generisanim DTS tabelom. Na ovaj način moguće je utvrditi eventualne greške evaluatora u administraciji *upitnika* i *intervjua* i konsolidaciji dokaza u ove dve tabele. *Excel tabela za evidenciju dokaza* obezbeđuje evidenciju direktnih i indirektnih elektronskih dokaza, što omogućava analitičku verifikaciju *koraborativnosti*, *pokrivanja* i *kompletnosti* dokaza, pored obezbeđene direktne opservaciju dokaza svim članovima TE i na internom *web* portalu u radnoj prostoriji TE, i uvida u fizička dokumenta, dostavljana po zahtevu.

Tačnost metoda SSAM evaluacije verifikovana je i sa modifikovanom aplikacijom *Appraisal Assistant*, koja je originalno razvijena za evaluaciju SCAMPI v.1.2 A tipa na bazi CMMI v.1.2 referentnog modela procesa i potencijalno drugih referentnih modela CMM tipa. Aplikacija originalno ne uključuje referentni SSE CMM model, pa se ne može koristiti za SCAMPI evaluaciju procesa zaštite. Modifikacija aplikacije obezbedila je uključivanje SSE CMM modela, terminološko i jezičko prilagođavanje srpskom jeziku i kulturi rada. Na taj način aplikacija se može koristiti kao interaktivni programski alat za SCAMPI evaluaciju procesa zaštite na bazi SSE CMM modela, čime se koriste sve prednosti i veća preciznost poslednje verzije SCAMPI metoda evaluacije procesa.

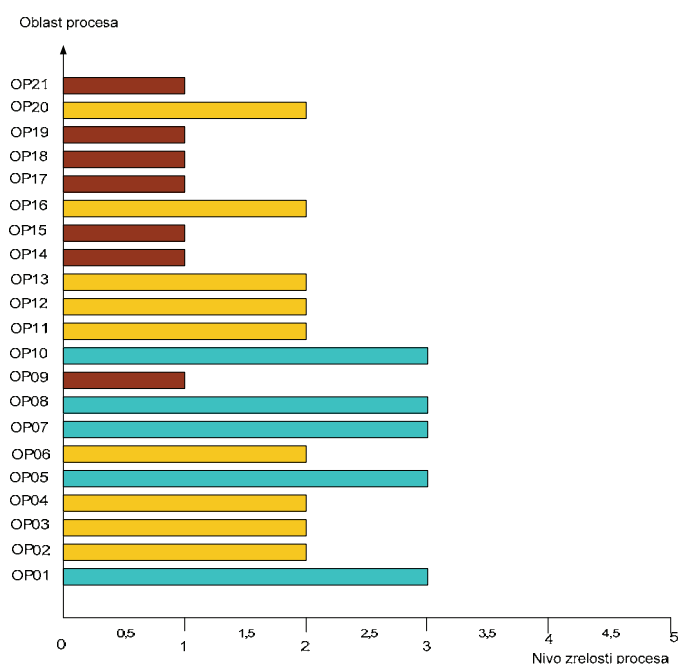
5. Analiza rezultata i predlog poboljšavanja procesa ESS

5.1. Analiza rezultata evaluacije procesa ESS

5.1.1. Izbor željenog profila procesa ESS

U cilju evaluacije i progresivnog poboljšavanja tekućih procesa **ESS**, evaluirana organizacija izabrala je za žljeni profil procesa CA, referentni profil *najbolje prakse procesa* standardnog CA prema SSE CMM modelu, bez dodatnih modifikacija.

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 davanja servisa, autentifikuje digitalne sertifikate, pa tek onda opslužuje specifične klijente. U toku su brojne diskusije o adekvatnoj politici i praksama koju CA treba da sprovede, ili da su obavezne za tipična CA. Međutim, bez obzira na politike i prakse koje CA treba da sprovede 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 Sl. 5.1.1. generički je, izrađen na bazi *najboljih praksi* zaštite 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 CL4) od potčinjenih CA. SSE CMM poseduje ove mogućnosti i potrebnu fleksibilnost.



Sl. 5.1.1. Referentni profil procesa CA

Dovođenje inženjerskih procesa (SSE) na CL3 nivo kapaciteta najefektivnije se može postići dovođenjem projektnih OP na CL2 nivo zrelosti, 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 poboljšavanje organizacionih procesa. Izvršavanjem organizacionih OP dobiju se neophodni resursi koje koriste inženjerske OP za poboljšavanje na CL3 nivo zrelosti. Ovi resursi uključuju standardne SE procese organizacije za podršku i stečena SE znanja i veštine.

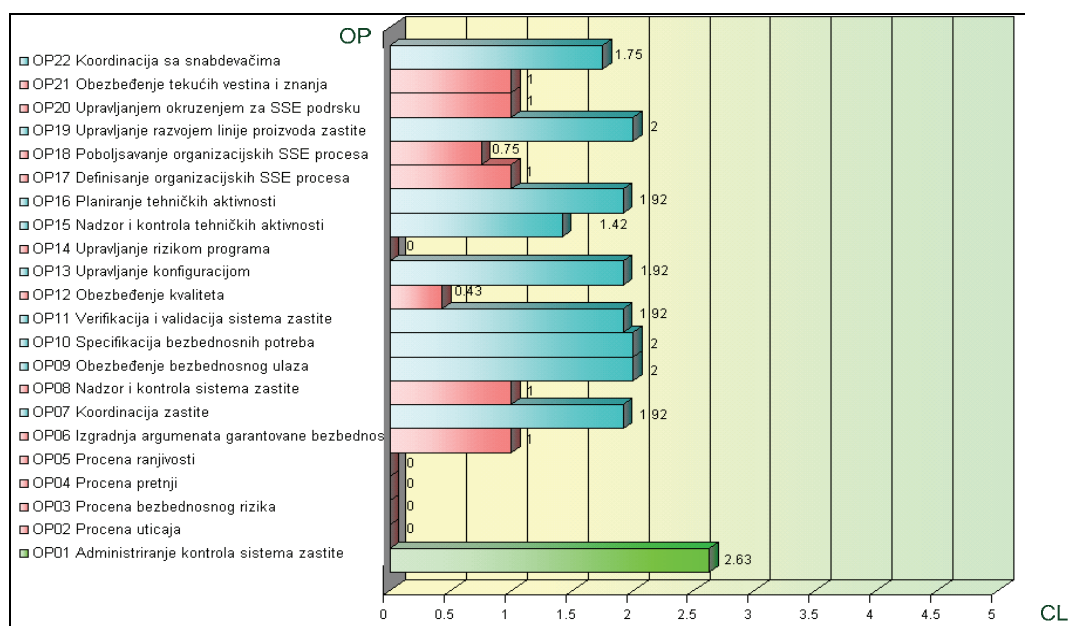
Organizacija koja unapređuje program rada treba da prema značaju odredi prioritete izvršavanja OP u odnosu na postavljene ciljeve i da nastoji da najpre poboljšava kapacitete u tim OP. Smatra se da OP01, OP05, OP07, OP08 i OP10 zaslužuju najveću pažnju i samim tim treba da budu na najvišem nivou zrelosti kapaciteta. Ove OP CA organizacija treba da **regularno** koristi, pa moraju biti dobro dokumentovane i definisane. Smatra se da je dobro definisan i implementiran (CL3) nivo zrelosti procesa sasvim odgovarajući, pošto su ove OP fokusirane na *administraciju kontrola zaštite, procenu ranjivosti sistema, koordinaciju zaštite, nadzor i kontrolu sistema zaštite i specifikaciju bezbednosnih potreba*.

Grupa OP iz SSE OP02, OP03, OP04, OP06 i OP11, koje se odnose na *procenu uticaja, procena bezbednosnog rizika, procena pretnji, izgradnju argumenata za bezbednosnu garanciju (assurance) i verifikaciju i validaciju*, smatraju se važnim, ali ne zahtevaju isti nivo zrelosti kapaciteta kao prethodna grupa OP, zato što se smatra da CA organizacija ove procese koristi **periodično**, pa je za ove OP dovoljno da budu dobro planirane i kontrolisane (CL2). Na istom nivou zrelosti (CL2) mogu biti i projektne OP12 i OP13 koje se odnose na *osiguranje sistema kvaliteta i upravljanje konfiguracijom*. OP16 i OP20 iz kategorije organizacionih procesa, koje *planiraju tehničke napore i upravljaju okruženjem za podršku SSE procesa*, istog su značaja za CA i treba da se nalaze na CL2 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: *definisanje standardnih SSE procesa 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 kada je potrebno važno za ovaj profil.

5.1.2. Analiza rezultata SSAM evaluacije tekućih procesa ESS

Na bazi konsolidovanih dokaza iz *upitnika, intervju* rukovodstva projekata (LP1, LP2, LP3) i praktičara (PP1, PP2, PP3), analize pokrivanja, koraborativnosti i kompletnosti sakupljenih dokaza u kompletiranoj *Excel tabeli za evidentiranje dokaza*, otklanjanja nekonzistentnosti i razjašnavanja poslednjih pitanja kroz naknadni intervju, izvršena je transformacija podataka o dokazima u binarnu formu (**1, 0, ?**) u DTS tabeli (**Radni prilozi, PRILOG 7**) za praćenje kretanja dokaza i automatski je generisan profil nivoa kapaciteta tekućih procesa (OP) ESS prikazan na slici Sl. 5.1.2.



Sl. 5.1.2. Profil nivoa zrelosti kapaciteta tekućih procesa ESS

Profil nivoa zrelosti kapaciteta tekućih procesa ESS u velikoj meri se podudara sa glavnim nalazima snage i slabosti organizacije, otkrivenim u evaluiranim projektima.

Od inženjerskih (SSE) OP, u **OP01- Administracija sistema zaštite**, ESS 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. ESS, takođe, administrira i sopstveni CA i ima iskustvo u uspostavljanja i održavanju najmanje 10 CA sa arhitekturom na jednom i tri nivoa u različitim organizacijama. Proces administracije dobro je planiran i kontrolisan i dokumentovan pretežno kroz MS standardne politike i *tehničke* procedure, koje su prilagođene sa brojnim aplikacijama i konkretnim rešenjima razvijenim u ESS za različite projekte i zahteve organizacija. Ova OP ima tendenciju da brzo postane *dobro definisani* i standardni proces organizacije - institucionalizovan na CL3, sa solidnom metrikom, pod uslovom da se definiše i formalno opiše kao standardni proces ESS (OP17) i familiju standardnih procesa za *Administraciju PKI sistema na bazi MS tehnologija i Windows platformi*, koja uključuje, pored standardnih tehničkih MS procedura i operativne i upravljačke procedure razvijene u praksi ESS. U oblastima procesa za upravljanje bezbednosnim rizikom (OP2-OP5) ESS menadžment i projektni timovi imaju visoko razvijenu svest o potrebi razvoja sopstvene metodologije za upravljanje bezbednosnim rizikom, što je dokumentovano u najmanje dva relevantna dokumenta organizacije -organizaciona struktura i planovi rada. Međutim, ove procese ESS koristi krajnje neformalno, po eksplicitnom zahtevu korisnika, pošto smatra da je procena i upravljanje rizikom u realnom okruženju ugovorna obaveza korisnika. Pored toga, koristeći MS tehnologiju i procese najbolje prakse PKI, ESS ceni da su svi relevantni faktori bezbednosnog rizika podrazumevano ublaženi striktnom implementacijom PKI u skladu sa MS standardnim politikama i procedurama, pa nije neophodno vršiti analizu rizika u konkretnom projektu i okruženju, jer se ne očekuje otkrivanje novih značajnijih faktora rizika. ESS nigde ne planira i formalno ne kontroliše sakupljanje argumenata za garantovanu bezbednost (OP06). U procesu administracije i monitorisanja PKI sistema u skladu sa MS procedurama i preuzetom ugovornom obavezom za održavanje sistema, ESS sakuplja brojne metričke podatke i indikatore garantovane bezbednosti, koje, međutim, ne arhivira i ne analizira za potrebe definisanja argumenata garantovane bezbednosti. Procena TE je da ESS ovu OP neformalno izvršava (CL1), pošto primenjuje MS tehnologiju i najbolju praksu PKI, koje *podrazumevano garantuje* nivo bezbednosti naveden u MS standardnim politikama i procedurama. *OP 07-Koordinacija sistema zaštite OP08–monitorisanje sistema zaštite, OP09-Obezbeđivanje bezbednosnih ulaza i OP10-Obezbeđivanje bezbednosnih potreba*, 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 (13), indirektan su dokaz da projektni timovi ESS 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 sve aktivnosti planiraju za svaki projekat, ali ne jednako striktno i formalno na svim projektima. Osnovni instrument planiranja *MS Project* menadžer i *OneNote* ne koristi se podjednako i sa svim potencijalnim opcijama na svakom evaluiranom projektu. *OP11–Verifikacija i validacija sistema zaštite* uslovno je na drugom nivou zrelosti kapaciteta (CL2), ali nije institucionalizovana na svim projektima ESS. ESS projektni timovi 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, ESS 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, ESS može sa tekućim rigiroznim tehničkim testiranjem PKI rešenja u laboratorijskom (verifikacija) i produkcionom (validacija) okruženju relativno brzo izgraditi komercijalno rentabilan proces za formalnu *sertifikaciju i akreditaciju PKI sistema*.

Upravljačke (projektne) OP uglavnom se izvršavaju regularno po zahtevu korisnika i ugovorenim projektu, ali se ovi procesi formalno slabo planiraju i nedovoljno rigorozno kontrolišu. *OP12 - Osiguranje sistema kvaliteta* izvršava se sa svega 30% i to u odnosu na *kvalitet proizvoda* - tehničkog rešenja PKI, dok se *kvalitet procesa* za implementaciju i održavanje ovih rešenja uopšte ne izvršava. Uvođenjem sistema kvaliteta procesa, ovim procesom evaluacije i formalnim planiranjem aktivnosti ove OP, ESS može dovesti ovu OP sa malo troškova i napora na CL2, odnosno, CL3. U *OP13 - Upravljanje konfiguracijom* - sve ugovorom preuzete obaveze za održavanje i administraciju implementiranih rešenja PKI sistema u drugim organizacijama, ESS izvršava planski i kontrolisano (CL2), izuzev formalnog planiranja procesa monitorisanja i praćenja metričkih indikatora statusa procesa upravljanja konfiguracijom PKI sistema (GP2.4.1). Izvršavanje *OP14 - Upravljanje rizikom projekta* zanemarljivo je u radu projektnih timova ESS, 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 ESS (2004), što ukazuje na postojanje potrebnih znanja i veština. Proces *nadzora i kontrole tehničkih rešenja zaštite (OP15)* izvršava se na svim evaluiranim projektima u skladu sa ugovornim obavezama. ESS 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 monitorisanje i održavanje implementiranih tehničkih rešenja PKI sistema. *OP 16 - Plan tehničkih aktivnosti razvoja sistema zaštite* 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 6 organizacionih OP, ESS formalno planira i izvršava (na CL2) samo dve oblasti procesa: *OP19-Upravljanje razvojem proizvodne linije zaštite* i *OP22-Koordinacija bezbednosnih aspekata sa snabdevačima*. ESS 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 poboljšavanje procesa, ESS je dobrim delom izvršila i *OP18-Poboljšavanje standardnih procesa*, pri čemu se podrazumeva da su tekući standardni procesi ESS, ustvari, adaptirani MS procesi najbolje prakse PKI. ESS neformalno (na CL1), bez formalnog plana i praćenja, *upravlja razvojnim okruženjem za podršku inženjerskih procesa - OP20*. *OP 22 - Koordinacija bezbednosnih aspekata sa snabdevačima* sa kojima ESS ima partnerske odnose, izvršava se

regularno i u velikoj meri formalno (oko 60% GP na CL2). Međutim, ne planiraju se i ne kontrolišu indikatori izvršavanja ove OP koji uvode metriku, potrebnu za kvantitativno praćenje na višim nivoima zrelosti procesa.

5.1.3. Analiza glavnih nalaza SSAM evaluacije tekućih procesa ESS

U procesu SSAM evaluacije **ESS** na evaluiranim projektima **P1, P2 i P3** identifikovani su sledeći **glavni nalazi**:

Glavne slabosti:

1. U **Sektoru infrastrukture i zaštite** (defacto odeljenju) **ESS** organizacije jedan zaposleni pokriva više uloga u životnom ciklusu evaluiranih projekata, odnosno u toku: planiranja, projektovanja, laboratorijskog ispitivanja, implementacije pilot projekta - testiranja u produkcionom okruženju i fazi održavanja komponenti sistema zaštite - modula PKI sistema. Ova činjenica bitno utiče na formalizaciju aktivnosti, za koju zaposleni pored kreativnog rada nemaju vremena, odnosno za formalno planiranje aktivnosti u planu projekta, dokumentovanje dnevnih redova značajnijih radnih sastanaka, dokumentovanje analiza izveštaja, arhiviranje i dokumentovanje rezultata analize indikatora stanja procesa i sl. Na taj način **ova slabost je opšta prepreka za podizanje svih OP na viši nivo**
2. **Tekući procesi** koje ESS primenjuje u radu na tekućim projektima **nisu** eksplicitno **definisani i opisani** 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 u IKT sistemima klijenata, na bazi Microsoft tehnologija i Windows platformi. Imovina (objekti) standardnih procesa distribuirani su na više projekata i u različitim dokumentima i nisu adekvatno dokumentovani i sistematizovani u određenu biblioteku (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. **ESS** 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 management, 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 podizanja 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 politika zaštite ESS, koju bi ESS Odeljenje sistema bezbednosti trebalo izraditi, prema preporukama standarda ISO/IEC 17799. Ovim bi se stvorile pretpostavke za uspostavljanje OP za upravljanje bezbednosnim rizikom (**OP02-OP05**) i **uklonila opšta prepreka za poboljšavanje više inženjerskih (SSE) OP za sakupljanje argumenata za garantovanu bezbednost na veće nivoe zrelosti**.
4. **Metrike PKI sistema zaštite** nisu eksplicitno planirane i dokumentovane. Ne postoji eksplicitna izjava u razvijenim politikama komponenti sistema o uvođenju i korišćenju systemske i procesne metrike za stvaranje argumenata garantovane bezbednosti, predviđanje performansi procesa i kontinualno poboljšavanje procesa. Iako se brojni metrički podaci sakupljaju u izvršavanju standardnih procedura, ne vrši se regularna analiza sakupljenih indikatora o bezbednosnom stanju sistema. Filtrirani bezbednosno

relevantni log podaci (**P1**) prenose se nezaštićenim linijama, ali su predajna i prijemna strana pod stalnim nadzorom ESS, što organizacija smatra pogodnom zaštitom u postojećim uslovima. **Ova slabosti je opšta prepreka za implementaciju i institucionalizaciju GP na CL2 i CL3 za sve inženjerske (SSE) OP.**

5. **Oblasti procesa** (OP02, OP03, OP04, OP05) za upravljanje **bezbednosnim rizikom** ne izvršavaju se, neformalno ni ad hock, nisu eksplicitno planirane, ni dokumentovane na bilo koji način. ESS ne koristi ni jednu formalnu ili neformalnu metodu za analizu rizika, procenu ranjivosti, procenu pretnji i procenu uticaja (iskoristivost) pretnji na identifikovane ranjivosti sistema, poslove i ugled organizacije. Implementaciju PKI sistema ESS 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. **Ne postojanje i ne izvršavanje procesa upravljanja bezbednosnim rizikom, za organizaciju tipa ESS, može se smatrati najvećom slabosti i opštom preprekom za podizanje ovih SSE OP na viši, najmanje CL3 nivo zrelosti.**
6. **OP06** - Izgradnja argumenta bezbednosne garancije formalno se ne planira i ne izvršava u celini. Međutim, BP koje generišu argumente bezbednosne garancije neformalno se izvršavaju u okviru izvršavanja standardnih MS procedura laboratorijskog ispitivanja, pilot testiranja PKI sistema u realnom okruženju i monitorisanja operativnog 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 ESS stekla veće poverenje klijenata i postigla konkurentsku prednost na tržištu.**
7. **Koordinacija aktivnosti inženjerskih grupa** na projektima zaštite (**OP07, BP07.01-07.04**) 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 defacto 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.**
8. **ESS nema razvijen sistem kontrole kvaliteta** u organizaciji. **Sistem kvaliteta proizvoda** (modula PKI) obuhvaćen je delimično ispitivanjima modula PKI sa ciljem potvrđivanja navedenih funkcionalnosti i otklanjanja uočenih nedostataka i defekata u fazi testiranja uzoraka za pripremu projekta, laboratorijskog ispitivanja za ugovoreni projekat i testiranja u produkcionom okruženju. Sva ova ispitivanja kvaliteta proizvoda i PKI tehnologije, ESS ne izvršava u odnosu na neki standardni model kvaliteta, što znači da organizacija formalno nije uvela sistem kvaliteta proizvoda. Međutim, pošto ESS koristi MS proizvode i tehnologiju koja podržava najbolje PKI prakse, **sistem kvaliteta proizvoda** nije ni neophodan. Međutim, **sistem kvaliteta procesa zaštite** ima daleko veći značaj za ESS, sa aspekta poslovnih ciljeva i misije, potrebe formalnog definisanja i opisivanja standardnih procesa i familije standardnih procesa organizacije, kao i stalnog poboljšavanja (sazrevanja) tih procesa. Procesom asistiranje SSAM samo-evaluacije tekućih procesa, na bazi referentnog SSE CMM modela procesa zaštite, ESS uvodi prvu fazu sistema kvaliteta procesa u svoju organizaciju. **Slabosti u izvršavanju BP12.04-12.08 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 ESS obezbeđuje potrebne metričke podatke za brojne SSE OP i sa malo napora, formalnim dokumentovanjem,**

regularnom analizom i korišćenjem rezultata analize za upravljanje procesima, može poboljšati sve OP na više nivoie zrelosti.

2. Razvijene su politike zaštite relevantnih komponenti sistema (8) koje pokrivaju sve bitne oblasti projektovanja, implementacije, integracije i održavanja PKI sistema na baz MS PKI tehnologija i MS Windows platformi u evaluiranim projektima. Opisane su ključne procedure u skladu sa MS dokumentacijom. **Postojeće politike zaštite komponenti sistema zaštite (PKI), dobar su uvod u uspostavljanje i kompletiranje politika ostalih komponenti zaštite IKT sistema ESS organizacije (n.p.r., fizičke, personalne, firewels, kontrole pristupa, pasvorda i sl.).**
3. Iako se metrika procesa ne planira, na nivou procesa praktično se u okviru aktivnosti testiranja uzoraka, laboratorijskog ispitivanja, ispitivanja u produkcionim uslovima, monitorisanja operativnog rada i korisničkog izveštavanja 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 incidentima sistema i (3) *korisničko izveštavanje* o incidentima u sistemu. Generalno, u procesu monitorisanja brojni metrički podaci se sakupljaju automatizovanim sistemima, ili fizičkim opservacijama (izveštajima korisnika). **Ovakva praksa je dobra osnova za opšte povećavanje kvaliteta izvršavanja BP, odnosno, uvođenje metrike na CL2, CL3 i višim nivoima zrelosti SSE OP.**
4. Sa neznatnim naporom i veoma rentabilno, dobro osposobljeni timovi ESS mogu poboljšati formalno dokumentovanje i analizu sakupljenih metričkih podataka i podići specifično OP11-verifikaciju i validaciju tehničkih rešenja na viši nivo zrelosti kapaciteta, čak i na CL3, pošto projektni timovi izvršavaju gotovo sve prakse ove OP na zavidnom nivou kvaliteta, ali ih formalno ne dokumentuju i analiziraju. **Ovu OP ESS perspektivno može vrlo brzo i rentabilno podići na CL4, čime bi organizacija bila osposobljena i za komercijalnu sertifikaciju i akreditaciju PKI rešenja.**

Dodatna verifikacija tačnosti SSE CMM modela i rezultata SSAM metoda evaluacije procesa zaštite izvršena je i sa aplikacijom **SSE CMM/SCAMPI Appraisal Assistant**, koja je originalno namenjena za CMMI model procesa u SCAMPI metod evaluacije. Reinženjeringom aplikacije implementiran je SSE CMM referentni model na programskom nivou, a iskorišćene originalne prednosti SCAMPI v.1.2 (2006) metoda evaluacije u odnosu na SSAM metod (1999) evaluacije. Sakupljeni dokazi o izvršavanju, implementaciji i institucionalizaciji praksi importovani su iz radne tabele za *Evidenciju dokaza* u aplikaciju i obrađeni prema SCAMPI kriterijumima pokrivanja koraboracije i kompletnosti i drugim kriterijumima za konsolidaciju dokaza. Implementacija nekih modela sazrevanja proces u aplikaciju omogućena je samom aplikacijom, ali ne i SSE CMM modela. Implementacija SSE CMM modela i standarda sazrevanja procesa zaštite u aplikaciju nije bila trivijalan posao i zahtevala je intervenciju u programskom kodu. Praktično je SSE CMM model u celini ugrađen u bazu podataka aplikacije, što je omogućilo da se evaluacija tekućih procesa ESS izvrši i prema SCAMPI metodu evaluacije, koji ima prednosti u odnosu na SSAM metod evaluacije, jer karakterizaciju prikupljenih dokaza vrši kroz višekratnu verifikaciju, omogućava izvesnije ocene i ostavlja manje prostora za odluke TE. Takođe, aplikacija na bazi SCAMPI metoda evaluacije, ima neuporedivo veće mogućnosti izveštavanja i generisanja različitih varijanti rezultata evaluacije, u odnosu na SSAM proces evaluacije. **SSE CMM/SCAMPI Appraisal Assistant** aplikacija, između ostalih rezultata, generiše i objektivne argumente za ocenu snage i slabosti evaluirane organizacije. Neki rezultati evaluacije tekućih procesa ESS ilustrovani su u **Prilogu 5.1A**.

5.1.4. Komparativna analiza referentnog i tekućeg profila procesa ESS

Komparativna (*gap*) analiza nivoa zrelosti tekućeg i željenog profila nivoa kapaciteta OP CA, direktno ukazuje na prioritetne akcije ESS za poboljšavanje tekućih procesa. Rezultati ove analize identifikuju OP za prioritetno poboljšavanje i planiranje projekata akcionog plana. Međutim, kod odlučivanja o prioritetu poboljšavanja tekućih procesa ESS, treba uzeti u obzir činjenicu da je za

svaku organizaciju rentabilnije poboljšavati najpre sve organizacione OP (OP17-OP22) najmanje na CL1, ili CL2 – nivo planiranih, kontrolisanih i ponovljivih procesa, a zatim poboljšavati projektne OP (OP12-OP16) najmanje na isti, ili viši nivo dobro definisanih procesa - CL3. Poboljšani organizacijski i projektni procesi stvaraju osnovu za efikasno i mnogo efektivnije poboljšavanje inženjerskih OP (OP01-OP11) na željeni nivo zrelosti, a prema dinamici i raspoloživim resursima organizacije. Generalno, na najviše nivoe zrelosti treba poboljšavati one OP koje proizvode najveću vrednost za organizaciju i koje se koriste regularno i svakodnevno. Na bazi ovakvog pristupa i rezultata kompartivne analize tekućeg i željenog (CA) profila OP, optimalan je sledeći redosled akcija za poboljšavanje procesa ESS, kroz **proizvoljan broj projekata** i sa **projektnim zadacima** definisanim u predlogu akcionog plana:

1. **Orgnizacione OP:** OP17 i OP18 na CL1 i OP20 na CL2;
2. **Projektne OP:** OP12 na CL2, OP13 na CL2, OP14 i OP15 stabilisati na CL1;
3. **Inženjerske (SSE) OP:** OP01, OP05, OP07, OP08 i OP10 stabilisati na CL3, OP02, OP03, OP04, OP06 i OP11 na CL2.

5.2. Poboljšavanje tekućih procesa ESS

5.2.1. Praksa poboljšavanja procesa

Poboljšavanje procesa zahteva intenzivno angažovanje svih kapaciteta organizacije, pa se broj **procesa** za poboljšavanje 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 poboljšavanja procesa, ili **6SIGMA** metodologiju od 6 koraka: izbor, razumevanje, performanse, revizija, izmene i implementacija izmena procesa, ili neku drugu koju korisnik izabere kao odgovarajuću.

Za pokretanja aktivnosti poboljšavanja procesa korisno je razmotriti sledeća pitanja:

1. **Motiv** – koji kritični elemenat posla zahteva poboljšavanje procesa?
2. **Model** – koji referentni model najbolje odgovara praksi i procesima organizacije?
3. **Metod** – kako se može brzo i efektivno identifikovati prilika za poboljšavanje procesa?
4. **Upravljanje promenama** – koji faktori utiču na efektivnost uvedenih promena?
5. **Merenja** – koji su kritični faktori za uspostavljanje programa merenja?

Svaki **program poboljšavanja procesa** treba da se zasniva na poslovnim, ili drugim potrebama organizacije i da je deo strateških zahteva. Dakle, motiv za pokretanje programa poboljšavanja procesa mora imati realno uporište u zahtevima i potrebama organizacije.

Model procesa igra važnu ulogu u poboljšavanju 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:

1. Terminologiju i konstrukcije koje pomažu organizaciji da razume sva pitanja o procesima;
2. Standard za poređenje i indikatore za evaluaciju efektivnosti procesa;
3. Uputstvo za investiranje u poboljšavanje 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 procesa, za šta treba dobar poslovni razlog.

U izboru referentnog modela za poboljšavanje procesa, prvo treba definisati *oblast* poslovanja i oblast procesa koji su relevantni 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.

Sledeće pitanje je izbor reprezentacije modela koja najbolje odgovara ciljevima poboljšavanja procesa. Ako je cilj poboljšavanje nekoliko procesa treba koristiti kontinualnu reprezentaciju, a ako je cilj dobro definisan put poboljšavanja grupe procesa treba izabrati faznu reprezentaciju CMM modela (SSE CMM, ili CMMI).

U izboru tipa CMM modela za poboljšavanje procesa ne treba pažnju obraćati na nivoe kapaciteta/zrelosti procesa. Glavni cilj treba da bude da se proces poboljša i treba izabrati model koji najbolje pokriva kritične procese i koristiti ga za identifikaciju procesa koje treba poboljšavati.

- Posle izbora modela procesa za poboljšavanje kritičnih procesa organizacije, potrebno je odlučiti kako će organizacija evaluirati usaglašenost svojih praksi i procesa sa parametrima modela. Postoje tri osnovna razloga za evaluaciju procesa:
- *identifikacija tekućih procesa sa ciljem poboljšavanja procesa,*
- evaluacija rizika za performanse procesa organizacije i
- sertifikacija nivoa zrelosti kapaciteta procesa.

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 samo-evaluacije, privremenog profilisanja i mini evaluacije do evaluacije osposobljenog tima na bazi CMM modela, kao što su SSAM i SCAMPI 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 poboljšavanja procesa. Proces poboljšavanja 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 poboljšavanja na bazi rezultata evaluacije. *Inovativna poboljšavanja* obično su inicirana spolja uvođenjem nove tehnologije. *Inkrementalna poboljšavanja* inicirana su internom evaluacijom procesa organizacije sa ciljem poboljšavanja i prilagođavanja definisanih procesa. Poboljšavanje standardnog procesa otklanja uobičajene uzroke varijacija procesa u toku izvršavanja. Poboljšavanje tekućih OP ESS na bazi predloženih *zadataka akcionih planova*, treba zasnivati na inkrementalnim poboljšavanjima dokumentovanim u GP 5.2.2 i 5.2.3 za svaku poboljšavanu OP sa ciljevima uspostavljenim u GP 5.1.1.

5.2.2. Akcioni planovi za poboljšavanje tekućih procesa ESS

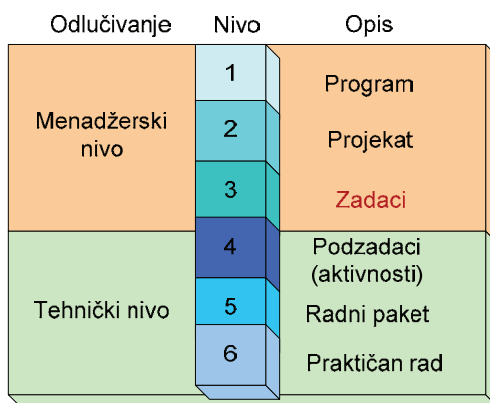
Prema modelima sazrevanja procesa, akcioni plan za poboljšavanje procesa razvija se na tri nivoa planiranja: *dugoročnom* (strateškom), *kratkoročnom* (taktičkom) i na nivou *projektnog tima* za realizaciju konkretnog projekta za poboljšavanje procesa. Za poboljšavanje tekućih procesa ESS razvijena su **tri tipa akcionih planova** za poboljšavanje procesa kroz definisane *faze, zadatke i aktivnosti* koje treba izvršiti:

1. **Strateški plan poboljšavanja procesa (PPP):** sveobuhvatni dugoročni plan, ili **program razvoja procesa organizacije**, koji predstavlja sveobuhvatni okvir za alokaciju resursa, uključuje razloge za izvođenje programa za poboljšavanje procesa i definisane ciljeva

poboljšavanja (CD, 3. *Realizacija SSAM evaluacije*, 4. *Predlog akcionog plana poboljšavanja procesa*, **Prilog 5.2A**).

2. **Akcionni plan poboljšavanja procesa (APP):** taktički, kratkoročni plan, mnogo detaljniji, koji definiše napore cele organizacije kroz upravljive zadatke, formirane na bazi rezultata SSAM evaluacije; ovaj se plan naziva i *plan implementacije ili operativni plan*. **Zadaci** za *Akcionni plan poboljšavanja tekućih procesa ESS* na CL1, u odnosu na 22 OP SSE CMM modela i uzorak za izradu kompletnog akcionog plana dati su na CD-u, 3. *Realizacija SSAM evaluacije*, 4. *Predlog akcionog plana poboljšavanja procesa* u **Prilogu 5.2B**.
3. **Akcionni planovi projektne grupe (PPT):** vrlo su detaljni, formira ih projektni tim (PT) sa fokusom na to *šta, kako i kada* PT treba da uradi. PT prioritetno usmerava pažnju na one OP koje su u procesu evaluacije pokazale najveće slabosti. U okviru ovog plana treba definisati *plan komunikacija* u okviru projektne grupe, sa drugim grupama u organizaciji i sa spoljnim saradnicima. Dobra komunikacija, sa uzajamnim potpunim razumevanjem značenja razmenjenih poruka, od presudnog je značaja za efikasnost izvršavanja svakog procesa. Uzorak strukture zadataka detaljnog **akcionog plana PT** za poboljšavanje procesa, primer zadataka **akcionog plana PT za poboljšavanje OP01- Administracija sistema zaštite 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 na CD, 3. *Realizacija SSAM evaluacije*, *Predlog akcionog plana poboljšavanja procesa* u **Prilogu 5.2C**.

Dijagram dekompozicije **programa za razvoj procesa**, po nivoima odlučivanja, kroz faze i zadatke do praktične realizacije, prikazan je na slici 5.1.3. Predlozi akcionih planova za poboljšavanje procesa ESS dati su na nivou **zadataka**, što podrazumeva da u fazi planiranja konkretnih projekata za poboljšavanje SSE procesa organizacije, ESS treba da uspostavi ostale elemente plana projekta: projektni tim, obim, veličinu i ograničenja, dinamički plan realizacije, kontrolu projekta, faktore rizika projekta i potrebne materijalne i finansijske resurse i druge elemente.



Sl. 5.1.3. Nivoi dekompozicije programa za razvoj procesa

5.2.2.1. Uloge u procesu poboljšavanja procesa

Generičke uloge (pojedinci ili grupe) u procesu *poboljšavanja procesa*, prema CMMI modelu procesa, su:

- **Sponzor PPP:** lice iz organizacije odgovorno za nadgledanje i kontrolu celokupnih aktivnosti za poboljšavanje procesa; generalno ima ovlašćenja za alokaciju finansijskih sredstava i radnog tima za poboljšavanje procesa; uobičajeno je na nivou direktora ili većem.
- **Lice za odnose sa javnošću:** ovo lice (tipično **direktor marketinga**), predstavlja organizaciju po pitanju svih aktivnosti vezanih za poboljšavanje procesa. Može, a ne mora biti istovremeno i lider **inženjerse projektne grupe (tima) –EPG** za realizaciju

projekta poboljšavanja procesa; promoviše ideje, pristupe za rešavanje i rezultate poboljšavanja procesa.

- **Rukovodstvo inženjerske procesne grupe (EPG):** ovo lice/a rukovodi/e i revidira/ju rad članova inženjerske procesne grupe, dodeljuje/u zadatke članovima EPG, nadzire/u njihov rad i planira/ju dnevne aktivnosti EPG.
- **Članovi EPG:** ova lica su članovi EPG i odgovorna su da *obezbede* izradu i striktno sprovođenje dokumentacije za poboljšavanje procesa i generisanje metrike za praćenje poboljšavanja procesa; oni rukovode pojedinačnim *grupama za implementaciju procesa*, ili *akcionim procesnim timovima (PAT)*.
- **Akcionim timovi za implementaciju procesa (PATs):** ovi timovi generišu dokumentaciju za poboljšavanje procesa – politike, opise procesa, procedure, akcione planove i planove za realizaciju zadataka akcionih timova.
- **Spoljni saradnik:** obično 1 ili 2 lica koji su spoljni konsultanti angažovani za pomoć u uspostavljanju planova, vođenju i monitorisanju progressa u poboljšavanju procesa organizacije; unose iskustva i znanja iz poboljšavanja procesa u drugim organizacijama.

Ove se uloge, zavisno od tipa i veličine organizacije, mogu prilagođavati, integrisati i objedinjavati u jednom licu/grupi, gde je potrebno i odgovara.

5.2.2.2. Tipična infrastruktura procesa za Poboljšavanje procesa

Rukovodstvo EPG tipično treba da razvije i uključi sledeće infrastrukturne komponente za uspešnu realizaciju nekog projekta *poboljšavanja procesa*:

- uspostavi, ili stabilise mehanizme komunikacije u celoj organizaciji za efikasnu koordinaciju svih učesnika,
- uspostavi i popuni **Inženjerski projektni tim (EPG)**, **Upravni odbor projekta (Steering Committee)** i **Izvršni odbor projekta (Executive Board)**,
- uspostavi i održava *Entitet (lice/a) za kontrolu konfiguracije-CCB (Configuration Control Board)*, odgovoran za upravljanje (izradu i održavanje) dokumentacijom procesa organizacije (n.p.r., DMS - Document Management System),
- razvije proceduru CCB kontrole dokumentacije za poboljšavanje procesa,
- kreira mehanizme za prezentaciju ideja i postavljanje zahteva za poboljšavanje procesa inženjerskom procesnom timu (EPG) i akcionom timu implementatora (PAT),
- razvije **politike organizacije** za svaku **oblast procesa (OP)** primenjenog modela procesa, za koji se organizacija opredeli (npr. SSE CMM, CMMI i dr.)
- kreira okvir za merenja postignutog uspeha i progressa u poboljšavanju procesa,
- obezbedi odgovarajuću obuku i podršku,
- evaluiira i obezbedi odgovarajuće alate za podršku (proizvodno okruženje).

Svi CMM modeli procesa sugerišu **SEI IDEAL Model** za implementacije SSAM i SCAMPI rezultata evaluacije i poboljšavanje procesa. Faze i koraci **IDEAL** procesa za implementaciju *Akcionog plana za poboljšavanje procesa* prikazane su na priloženom CD, **3. Realizacija SSAM evaluacije**, *Predlog akcionog plana poboljšavanja procesa* u **Prilogu 5.2D**.

5.3. Analiza iskustava iz SSAM procesa evaluacije

5.3.1. Odstupanja od SSE CMM modela

Međuzavisnosti određenih OP i GP/BP u modelu su distribuirano opisane kroz napomene u opisu BP, odnosno OP. Tabela prikaz (p.p. 2.4, Tabela 2.4.6) ovih međuzavisnosti daje bolji pregled i doprinosi razumevanju uticaja *implementacije* i *institucionalizacije* određenih GP na sazrevanje nivoa kapaciteta/zrelosti SSE CMM modela.

Primeri proizvoda rada jedini su indikatori dokaza o implementaciji praksi (BP i GP) procesa prema SSE CMM modelu, 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 modela, izvršena su **prilagođavanja** SSE CMM modela, kroz uvođenje i opis sledećih termina i kategorija:

1. **Objektivni dokaz:** svi dokazi dobijeni instrumentima SSAM evaluacije, koji objektivno i nesumnjivo, nezavisno od izvora ukazuju i potvrđuju da su pripadajuće BP i GP izvršavane, implementirane i/ili institucionalizovane.
2. **Vrste objektivnih dokaza:**
 - **direktni dokazi (DD)**, opipljive izlazne rezultate implementiranih praksi, n.p.r., *Primer proizvoda rada* naveden u SSE CMM modelu,
 - **indirektni dokazi (ID)**, posledice ili indikacije implementacije praksi i
 - **potvrđne izjave (F2F)**, usmene/pisane koje podržavaju implementaciju praksi, tj., potvrđene opservacije i odgovori na upitnik, ili intervju.
3. **Izvora objektivnih dokaza** za SSAM evaluaciju mogu biti **instrumenti** metoda:
 - **Upitnik:** anketa, podaci o imovini procesa organizacije, koja 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 brifinga i sl.;
 - **Neposredna demonstracija korisnika:** praktičara koji izvršavaju procese, koja dokazuje kvalitet izvršavanja određenih procesa CA, ukoliko ih mogu na bilo koji način dokumentovati, n.p.r., neposredan printing izveštaja o izvršenom procesu na displeju računarskog sistema i sl. i različita
 - **Dokumenta:** politike, procedure i planovi implementacije u čvrstoj kopiji, ili kao elektronski dokument, tehnička dokumentacija i druga zvanična dokumenta koja se odnose na evaluirane projekte, a ukazuju na implementaciju praksi i procesa.

5.3.2. Odstupanja od procesa SSAM metoda evaluacije

- *Plan evaluacije* (predlog) izređen je u pre-pripremnoj fazi, pre upoznavanja Sponzora o detaljima evaluacije i izbora mešovitog tima za evaluaciju. Tako je sam process evaluacije značajno skraćen za period potreban za pripremu plana evaluacije od 2-6 sedmica, prema SSAM metodu i obimu evaluiranih projekata;
- *RFP- zahtevi za ponudu evaluacije* nisu specifično razvijani i direktno su uključeni u *Plan evaluacije*, zbog nekomercijalnog karaktera evaluacije tekućih procesa ESS.
- SSAM metod *sugeriše 2 posmatrača* u TE: **1** iz organizacije evaluatora i **1** iz evaluirane organizacije, koji se obučava za samostalno vođenje procesa evaluacije. Na osnovu eksplicitne zainteresovanosti Sponzora i tipa procesa evaluacije - *asistirana samo-evaluacija*, povećan je broj posmatrača na **4**, pri čemu su svi posmatrači zaposleni iz evaluirane organizacije.
- *DTS* radni dokument nije uključivan u preliminarnu evaluaciju podataka posle administracije *upitnika i intervju lidera projekta*, ali je revizija i konsolidacija odgovora i priloženih dokaza vršena na bazi analize afirmativnih odgovora i *koraboracije, pokrivanja i kompletnosti* raspoloživih dokaza, posle svake faze – administracije odgovora na upitnike i intervju.
- *Zahtevi za dokaze* rukovodilac dokaza tražio je na SSAM propisanom formatu za praćenje kretanja dokaza, ali relativno retko, pošto je Sponzor obezbedio interni *web* portal u radnoj prostotriji TE, za pristup svim serverima na kojima se čuva elektronska dokumentacija ESS, pa je omogućena neposredna opservacija dokaza i uvid u 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%: 5 evaluatora i 4 posmatrača za 14 radnih dana sa 4 efektivna radna sata u

proseku, za 3 evaluirana projekta, prema tipičnih 20 radnih dana, za 5 evaluatora i 1 posmatrača po 8 sati rada dnevno za 4 evaluirana projekta. Svi radni dokumenti TE razvijeni u procesu evaluacije priloženi su na CD-u radnih materijala u prilogu rada.

- *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 organizacije. 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 organizacije i cena*), značajno su poboljšani u procesu evaluacije tekućih procesa ESS.
- *Tačnost SSAM* verifikacionog i visoko-preciznog procesa evaluacije, neznatno je poboljšana uvođenjem preglednih i eksplicitnih direktnih dokaza za afirmativne prakse sa generisanim *SSAM PIID dokumentom* i striktnog zahtevanja *koraboracije, pokrivanja i kompletnosti* svakog dokaza po uzoru na SCAMPI metod evaluacije, u fazi svake konsolidacije dokaza i generisanja preliminarne i konačnih rezultata i nalaza evaluacije.
- *Broj intervjuisanah praktičara* smanjen je u odnosu na planiranih 9 (3 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 ESS održava i administrira u svim fazama životnog ciklusa sistema.
- *Izveštaj o evaluaciji*, uz saglasnost Sponzora, nije formalno izrađen i dostavljan Sponzoru kao celovit pisani dokument, nego su svi rezultati evaluacije u delovima isporučeni Sponzoru evaluacije: profil procesa, glavni nalazi i akcioni plan.

5.3.3. Iskustva iz sprovođenja Plana evaluacije tekućih procesa ESS

- Iskustvo dobijeno iz **prve** evaluacije procesa u cilju uvođenja sistema kvaliteta i regularnog poboljšavanja tekućih procesa organizacije ESS u celini je vrlo značajno i produktivno za evaluiranu organizaciju i TE. Identifikovane su snaga organizacije – *primena MS i drugih partnerskih standardnih procesa najboljih praksi, kao standardnih procesa organizacije* i glavne slabosti organizacije – *nedovoljno formalno dokumentovanje praksi i procesa, nepostojanje definisanih relevantnih standardnih procesa i familije standardnih procesa organizacije i slabo korišćenje metrike i rezultata merenja za poboljšavanje praksi i procesa*.
- Sve razlike profila pojedinačnih tekućih i željenih OP, identifikovane su i obuhvaćene predlogom **zadataka** za *Akcioni plani poboljšavanja tekućih procesa ESS* (za 22 OP) na prvi nivo zrelosti kapaciteta procesa (CL1) i progresivno poboljšavanje na CL2 i CL3, prema dinamici i raspoloživosti resursa ESS.
- Menadžeri i lideri projekata *P1, P2 i P3* intervjuisani su simultano za sve inženjerske (SSE) OP, pošto kao jedinstvena inženjerska grupa rade zajedno u svim fazama životnog ciklusa na sva tri evaluirana projekta i imaju podeljene i višestruke uloge sa individualnim pravima pristupa dokazima preko internog *web portala*. Ovakav pristup značajno je povećao efikasnost prikupljanja dokaza, kao i verifikaciju njihovog pokrivanja, koraboracije i kompletnosti na sva tri projekta.
- Vreme sesije intervjuisanja menadžera i lidera projekta treba povećati do 2 sata sa 15 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 intervjuisanih i distribucije pažnje sa fokusiranog predmeta istraživanja.
- Vreme za intervjuisanje praktičara za OP u kojima je istraživana usklađenost prakse izvršavanja BP i GP datog procesa sa standardima, planom, politikama ili procedurama zaštite, treba povećati na 1.5 čas, zbog slabijeg razumevanja zahteva procesa evaluacije u celini. Planiran broj intervjuisanih praktičara po zahtevu Sponzora, smanjen je sa 9 na 3 - 1

po projektu, zbog toga što inženjerski tim ESS praktično održava sisteme na sva tri evaluirana projekta, čime je obezbeđeno *pokrivanje* dokaza.

- Preporučuje se pregled internih dokumenata u pripremnoj fazi, pre početka SSAM procesa evaluacije na terenu, što može inicirati menadžer projekta, Sponzor, ili član TE koji zahteva dokaze, zbog preliminarne uvida u direktne objektivne dokaze i povećanja efikasnosti sakupljanja i konsolidacije dokaza u svim fazama SSAM evaluacije na terenu.
- Uloge rukovaoca dokaza i člana TE zaduženog za praćenje vremena realizacije koraka u fazama SSAM procesa bile su spojene, zbog vremenske fleksibilnosti, nekomercijalnog karaktera evaluacije tipa *asistirana samo-evaluacija* i načina sakupljanja dokaza preko instaliranog internog web portala.
- Modifikovana *SSE CMM/SCAMPI Appraisal Assistant* aplikacija, korišćena u istraživačkom projektu evaluacije za dodatnu verifikaciju tačnosti SSAM metoda evaluacije, potvrdila je visoku tačnost SSAM evaluacije, ako se metod striktno primeni, ali i meru u kojoj se mogu povećati tačnost i efikasnost procesa evaluacije primenom aplikacije sa SSE CMM referentnim modelom i SCAMPI metodom za evaluaciju procesa zaštite. Aplikacija nije primarno korišćena za evaluaciju tekućih procesa ESS u istraživačkom projektu, da bi se mogao korektno verifikovati SSAM metod, razvijen specifično za evaluaciju procesa zaštite na bazi SSE CMM modela procesa. Rezultati *SSE CMM/SCAMPI Appraisal Assistant* aplikacije dati su na priloženom **CD-Radni materijali, 4.Rezultati SSE CMM SCAMPI Appraisal Assistant aplikacije.**

5.3.3.1. Iskustva iz vođenja intervjua

- U toku vođenja intervjua treba intervjuisanim licima dopustiti da donesu sa sobom dokaze (fizička dokumenta, na primer), 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 4-5 dana između pripremne faze i faze evaluacije na lokaciji, zbog kvalitetne i konzistentne konsolidacije dokaza i odgovora sakupljenih u fazi administracije upitnika.
- 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.

5.3.3.2. Sugestije za Sponzora

- Treba praktikovati proveru konzistentnog planiranja i redovnog dokumentovanja izvršanih aktivnosti (BP) u inženjerskim OP (OP01-OP11), koje se *defacto* uspešno izvršavaju, ali ne ostaju tragovi za sistem kontrole kvaliteta.
- Treba uspostaviti – planirati i formalno definisati i opisati *standardne procese organizacije* (OP17) i familiju standardnih procesa organizacije, uključujući i procese za *upravljanje bezbednosnim rizikom* (OP02-OP05), najmanje na CL1 u prvim projektima poboljšavanja tekućih procesa organizacije, a zatim na CL2, bez obzira na izabrani željeni profil procesa.

U narednom dugoročnom (strateškom) 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 ESS – najmanje na CL3, ili na CL4 (OP11).

6. Diskusija dobijenih rezultata

1. *U sistemskom pristupu zaštiti, procesi* su fundamentalni gradivni blokovi sistema zaštite, transformišu ulazne veličine u izlazne i integrišu *procedure i metode, tehnike i alate* i *osposobljene i motivisane ljude* za izvršavanje rada. Prema kriterijumima kvaliteta procesi mogu biti: **improvizovani** - neformalno i *ad hock* izvršavani, slabo opisani i zahtevani, zavisni od sposobnosti i motivacije praktičara i bez vremena za poboljšavanje, zbog potrebe konstantnog reagovanja, ponavljanog uspostavljanja procesa i otklanjanja čestih nekonzistentnosti; **poboljšani (stabilni)** – opisani konzistentno načinu izvršavanja, upravljani, dokumentovani, definisani i kontinualno poboljšavani, sa konstruktivnom upotrebom metrike procesa i proizvoda rada procesa i disciplinovanom uvođenjem tehnologije; **institucionalizovani** - sa izgrađenom infrastrukturom organizacije za podršku efektivnih, iskoristivih i konstantno primenjivanih procesa u svim projektima; procesi se nasleđuju i prenose u kulturu rada organizacije, povećavajući vrednosti izlaznog rada, zbog očekivanog sinergijskog delovanja komponenti zaštite, što nije uvek slučaj, pa je **potrebno da se neprekidno poboljšavaju**.
2. Proces može postati **stabilan-zreo** i ponovljiv samo neprekidnim poboljšavanjem. Za održavanje stabilnosti procesa zaštite zahteva se održavanje njihove *produktivnosti, adaptivnosti i korisničke prihvatljivosti*. Prvi korak u poboljšavanju procesa je **evaluacija**, ili objektivno procenjivanje **stepena i kvaliteta** izvršavanja, implementacije i institucionalizacije praksi (BP i GP) i procesa evaluirane organizacije u odnosu na primenjeni referentni model procesa (SSE CMM, ili neki drugi). Efektivno upravljanje procesom zahteva u prvom redu da je proces formalno *opisan* i dobro *definisan*. Opis procesa u modelu procesa može biti: *formalan* i *korisnički orijentisan*. **Formalni opis procesa** zahteva tipično uključivanje specijalista zaštite; opis je detaljan i formalizovan i primarno se koristi za **razvoj, prilagođavanje i poboljšavanje** procesa. Za formalni opis procesa, potrebno je dobro opisati osnovne elemente dekompozicije procesa - aktivnosti (prakse): *namena, izvršioci, ulazne veličine potrebne za izvršavanje, proizvod rada, kriterijum za početak, kriterijum za uspešno kompletiranje, potreban rad za izvršavanje, sub-prakse (3-6) koje je potrebno izvršiti, metriku za izvršavanje i prethodne i sledeće aktivnost*. **Korisnički orijentisan opis procesa** zahteva uključivanje praktičara koji dnevno koriste procese i tipično je jednostavan, jasan i koristi se primarno za **izvršavanje procesa**. **Dobro definisan** proces zahteva jasno definisane uloge: *sponzora, vlasnika, menadžera i izvršioca* procesa i treba da sadrži: *naziv, namenu, obim, ulaz, izlaz, kontrolu i resurse*.
3. Ključni **alat za poboljšavanje procesa** je objektivna i nezavisna metodologija ekspertске **evaluacije (appraisal)** za identifikovanje i poboljšavanje stanja tekućih procesa. Evaluacija je uvek svrsishodan proces stvaranja kognitivnih pretpostavki za efikasno i efektivno poboljšavanje, a vrši je osposobljen tim za evaluaciju (TE) na bazi referentnog modela procesa. Generalno, za evaluaciju i poboljšavanje tipično multidisciplinarnih procesa zaštite, potrebno je uspostaviti više okvira i koristiti više **referentnih modela**, što se može izbeći primenom **procesno orijentisanih** modela **integriranih procesa** kao što su SSE CMM i CMMI. Metodi evaluacije i poboljšavanja procesa na bazi ovih modela zasnivaju se na **verifikaciji** koraborativnosti, pokrivanja i kompletnosti objektivnih dokaza izvršavanja, implementacije i institucionalizacije praksi procesa, što predstavlja znatno viši kvalitet od ranijih metoda evaluacije procesa samo na bazi **otkrivanja** dokaza.
4. **SSAM v.2.0 metod evaluacije** procesa zaštite na bazi SSE CMM v.3.0 modela sazrevanja procesa, posebno je razvijen da obezbedi *proces* izvršavanja metodologije evaluacije koju SSE CMM model inherentno sadrži. Svaki SSAM proces evaluacije ima najmanje dva cilja: (1) sakupiti precizne i objektivne podatke o izvršavanju, implementaciji i institucionalizaciji praksi i procesa zaštite uz minimalnu destrukciju svakodnevnog rada

organizacije i (2) odrediti prioritete poboljšavanja procesa, koji se mogu dostići na brojne načine i sa različitim stepenom troškova i tačnosti. Ciljevi evaluacije procesa mogu varirati u skladu sa potrebama *inicijatora evaluacije ili Sponzora* i može biti poboljšavanje svih OP na jedan nivo zrelosti, ili pojedinačnih OP na specifičan nivo zrelosti kapaciteta. U ovoj **prvoj** evaluaciji kvaliteta procesa, Sponzor evaluacije izabrao je da se izvrši evaluacija *tekućih procesa ESS* organizacije u odnosu na 22 OP SSE CMM modela. Kao i većina metoda evaluacije, SSAM evaluacija ima dve glavne kategorije izlaznih rezultata: *nalazi* o slabostima i snazi organizacije, *profil procesa i preporuke* za akcioni plan poboljšavanja procesa. Sponzor je zahtevao izradu profila tekućih procesa **ESS**, određivanje glavnih nalaza o snazi i slabostima organizacije i izradu akcionih planova za poboljšavanje procesa u odnosu na referentni profil CA.

5. **Ukupni naponi TE na projektu SSAM evaluacije tekućih procesa ESS** u istraživačkom delu rada, potvrdili su da je proces SSAM metoda evaluacije sistematičan, precizan i vremenski zahtevan. Prema iskustvima Instituta SEI iz realne primene procesa SSAM evaluacije, za rentabilnu, najmanje destruktivnu i što tačniju evaluaciju 22 OP na 3-4 projekta, zahteva se rad 2 iskusna evaluatora, 3 člana TE i 2 posmatrača, od oko 20 dana sa 8-časovnim radom svakog evaluatora ili 160 sati/evaluatoru. TE *Univerziteta Singidunum* od 5 članova i 4 posmatrača iz evaluirane organizacije (**ESS**) izvršio je u potpunosti sve 4 faze i korake standardnog proces evaluacije za ukupno 14 radnih dana, prosečno sa 4 radna sata, što čini angažovanje od 56 sati/evaluatora, ili za oko 30% manje vremena. Metod SSAM evaluacije u *procesu evaluacije* detaljno opisuje dopuštene promene određenih parametara, zavisno od veličine i tipa evaluirane organizacije, stava i odnosa Sponzora evaluacije i osposobljenosti i iskustva evaluatora, ali je fleksibilan i za druge vrste planiranih i kontrolisanih prilagođavanja, što je u dobroj meri iskorišćeno u istraživačkom projektu evaluacije ESS procesa. Sponzor evaluacije **ESS** tekućih procesa, zahtevao je rad TE *striktno usaglašen* sa procesom SSAM metoda evaluacije, sa krajnje *objektivnom procenom* svakog ponuđenog dokaza–sagledavanjem *pokrivanja, koraborativnosti i kompletnosti* svakog dokaza i maksimalnim angažovanjem zaposlenih ESS u radu TE. Iako je SSAM metod primarno namenjen za nezavisnu TTPS evaluaciju, koju izvršava osposobljen i neutralan tim evaluatora, metod sadrži uputstvo i za *samo-evaluaciju*, koja omogućava određena prilagođavanja i maksimalno učešće zaposlenih evaluirane organizacije u procesu evaluacije.
6. **Profil nivoa kapaciteta tekućih procesa ESS** u velikoj meri se podudara sa glavnim nalazima snage i slabosti organizacije, otkrivenih u evaluiranim projektima. Neočekivani nalazi, neformalnog, ili nikakvog izvršavanja procesa za upravljanje *bezbednosnim rizikom* (OP02-OP05) i OP17 - *Definisanih standardnih procesa*, mogu se objasniti oslanjanjem ESS na *najbolju praksu* MS procesa i PKI tehnologija i drugih partnerskih tehnologija, koje podrazumevaju da se svi relevantni faktori bezbednosnog rizika podrazumevano ublažavaju striktnom implementacijom PKI u skladu sa MS dobro definisanim standardnim politikama i procedurama, pa da nije neophodno vršiti analizu rizika u konkretnom projektu i okruženju, jer se ne očekuje otkrivanje novih značajnijih faktora rizika, niti je potrebno posebno definisati standardne procese organizacije. Međutim, ESS ima u organizacionoj strukturi odeljenje za *Bezbednost IKT sistema* i generalno visoko razvijenu svest o potrebi zaštite, posluje kao organizacija koja implementira PKI infrastrukturnu komponentu zaštite, ubeđuje klijentske organizacije u potrebu zaštite, ali istovremeno *nema razvijenu sopstvenu metodologiju za upravljanje bezbednosnim rizikom*. Standard ISO/IEC 17799 preporučuje da se najbolja praksa zaštite primenjuje u kombinaciji sa analizom bezbednosnog rizika u realnom okruženju, što optimalno prilagođava najbolje prakse zaštite specifičnim potrebama konkretne orgnizacije. Takođe, ESS prioritetno treba da definiše i opiše generičke *standardne procese*, koji uključuju pored standardnih tehničkih MS procedura i operativne i upravljačke procedure razvijene u praksi ESS, kao i familiju standirdnih procesa ESS, umesto da se od projekta do projekta prilagođavaju standardne MS tehničke procedure koje opisuju primenjene PKI tehnologije. Više tekućih procesa ESS (OP08, OP11, OP13, OP14, OP15 i P19) obezbeđuje solidne metričke podatke koji se, međutim, ne koriste u

dovoljnoj meri za analizu stanja, ili predviđanje performansi procesa. Sa neznatnim naporom i rentabilno, dobro osposobljeni timovi ESS mogu poboljšati formalno dokumentovanje i analizu sakupljenih metričkih podataka i podići ove OP na viši nivo zrelosti kapaciteta, čak i na CL3. Ovo se posebno odnosi na *OP11-verifikaciju i validaciju* tehničkih rešenja, u kojoj projektni timovi izvršavaju gotovo sve prakse na zavidnom nivou kvaliteta, ali ih formalno ne dokumentuju i analiziraju. Ovu OP ESS perspektivno može vrlo brzo i rentabilno podići na CL4, čime bi organizacija bila osposobljena i za komercijalnu *sertifikaciju i akreditaciju* PKI rešenja.

7. **Rezultati istraživanja** u projektu *evaluacije procesa ESS* nedvosmisleno potvrđuju da se SSE CMM model može koristiti za *merenje, evaluaciju i poboljšavanje* zrelosti izvršanih i implementiranih procesa zaštite i kapaciteta za generisanje tih procesa, što je i primarna namena modela. Međutim, SSE CMM model i SSAM metod mogu se jednako efikasno koristiti i za *razvoj procesa za upravljanje programom zaštite i komponentama programa zaštite*. Glavna **prednost** primene SSE CMM modela u oblasti zaštite je *dualna metrika* sazrevanja procesa zaštite: *specifična metrika procesa*, orijentisana na same procese i *metrika sistema zaštite*, orijentisana na rezultate procesa zaštite. Glavni **nedostaci** primene SSE CMM modela su slabije definisani procesi zaštite od drugih inženjerskih disciplina, nedovršeno usklađivanje OP modela sa drugim modelima najboljih praksi zaštite (ISO/IEC 17799), razvoj procesa zaštite odvojen od procesa razvoja IKT sistema, neadekvatno korišćenje *metrike procesa* za evaluaciju inženjerskih kapaciteta procesa za razvoj i proizvodnju komponenti zaštite, gde se često ističu konačni rezultati u procesu SSAM evaluacije, iako se ocene evaluacije odnose na *proces* sa kojima se ti rezultati postižu, kao i relativno nedovoljan broj argumenata garantovane bezbednosti, pošto model ne *propisuje* eksplicitno procese zaštite u realnom okruženju.
8. **Odstupanja od standardnog procesa SSAM evaluacije** u projektu evaluacije tekućih procesa *ESS*, izvršena u cilju što veće tačnosti evaluacije i što manje destrukcije tekućih poslova *ESS*, odnose se na metodom dopuštena prilagođavanja i fleksibilno prilagođavanje vremena sastanaka i rada TE na pripremi učesnika, administraciji instrumenata evaluacije (*upitnika, intervju*), konsolidovanju nalaza i dokaza i izradi izveštaja. Tako je TE radio u popodnevnim satima, tipično od 14 -18 časova, nije radio intenzivno 8 i više radnih sati u jednom danu i nije u kompaktnom vremenskom periodu kompletirao proces evaluacije, pre svega zbog nekomercijalnog karaktera projekta evaluacije *ESS*, velike podrške menadžmenta *ESS* procesu evaluacije i želje da se evaluacija procesa izvrši što kvalitetnije.
9. **Kriterijumi za odlučivanje evaluatora** o stepenu izvršavanja, implementacije ili institucionalizacije u SSAM metodu evaluacije izraženi su eksplicitno i kvantitativno, ali zahtevaju u velikoj meri **prosudivanje evaluatora**. Iako sve ove kriterijume definiše SSAM metod, Sponzor ih može redefinisati na bazi značaja koji pridaje postizanju specifičnog CL, ali u procesu evaluacije ESS procesa nije bilo takvih zahteva. Stepenu izvršavanja GP, koje se izvršavaju zajedno sa BP i opisuju kvalitet izvršavanja BP, na CL2- CL5 ukazuje na stepen implementacije i institucionalizacije procesa na odgovarajućem CL, odnosno stepen sazrevanja (kvaliteta) procesa organizacije primenjivanih na svim projektima. Za ocenu izvršavanja GP, pored afirmativnih izjava i direktnih dokaza *-proizvoda rada BP iz SSAM PIID dokumenta*, u *Excel tabeli za evidenciju dokaza* sakupljani su dokazujući podaci iz različitih izvora – direktni i indirektni dokazi, neposredne opservacije i izjave praktičara koje se na bilo koji način mogu dokumentovati, a koji svi zajedno *koraborativno* potvrđuju objektivnost dokaza, njegovu *kompletnost* (dnevni red sastanaka, e-mail poruke i sl.) i *pokrivanje-zasupljenost* u evaluiranim projektima. Ovakav pristup verifikaciji dokaza obezbeđuje, pored profilisanja nivoa kapaciteta OP na bazi podataka iz DTS tabele, *dodatnu proveru tačnosti SSAM metoda*, slučajnim izborom OP i generisanjem kontrolnog profila na bazi *Excel tabele za evidenciju dokaza*. Ovu kontrolnu opciju originalni SSAM metod ne sadrži. *Excel tabela za evidenciju dokaza*, takođe, evidentno ukazuje u kojoj meri je SSAM metod evaluacije sistematičan, vremenski zahtevan i destruktivan za tekuće

poslovanje organizacije, kao i na eventualne greške u evidentiranju i konsolidovanju podataka. Modifikovana *Appraisal Assistant SSE CMMI/SCAMPI* aplikacija, koja dodatno povećava efikasnost i tačnost evaluacije, korišćenjem prednosti SCAMPI metoda na bazi SSE CMM modela procesa zaštite, u istraživačkom projektu rada korišćena je za verifikaciju tačnosti rezultata SSAM evaluacije.

10. ***Istraživački projekat SSAM evaluacije tekućih procesa ESS***, potvrdio je hipotezu da u praksi zaštite gotovo ni jedan model/standard procesa zaštite nije dovoljan sam po sebi za rešavanje svih potencijalnih problema u zaštiti. ESS je u osnovi organizacija u oblasti IKT zaštite, koja razvija, projektuje, implementira, integriše i održava PKI sisteme na bazi MS PKI tehnologije i Windows platformi, u klijentskim organizacijama. Međutim, ESS je istovremeno i poverljivi provajder usluga zaštite kao CA za brojne korisnike, proizvođač komponenti zaštite (izrada brojnih aplikacija, personalizacija smart kartica za jaku autentifikaciju korisnika i dr.), kao i nabavljač tehnologija zaštite, kroz partnerske odnose sa više snabdevača i vendora. Rezultati SSAM evaluacije tekućih procesa ESS, potvrđuju da SSE CMM model integrisanih procesa ***u velikoj meri odgovara profilu poslovanja i kulturi rada ESS organizacije***, u kojoj su svi zaposleni orijentisani na razvojne, funkcionalne i bezbednosne aspekte PKI infrastrukturne komponente zaštite.
11. ***SSE CMM/SCAMPI Appraisal Assistant*** aplikacija razvijena reinženjeringom originalne *CMM/SCAMPI Appraisal Assistant* aplikacije (SEI), omogućila je dodatnu verifikaciju tačnosti SSAM metoda evaluacije, kao i generisanje raznovrsnih i kombinovanih argumenata iz rezultata evaluacije tekućih procesa ESS, koji značajno povećavaju tačnost i objektivnost evaluacije, kao i efikasnost korišćenja rezultata evaluacije.

7. Zaključci

1. **Dostupni**, brojni pristupi za poboljšavanje prakse IKT zaštite, sa pretežno deskriptivnim opisom funkcionalnih modela, ističu najčešće prednosti izabranog pristupa sa prenaplašenim značajem *tehnoloških rešenja* (kriptografski pristup), ili suvišnim oslanjanjem na *proceduralne komponente* (CRAMM, OCTAVE, BAR i druge metode analize rizika), ili na *upravljačke kontrole* zaštite (ISO/IEC 13335 i ISO/IEC 17799), ili samo na jedan standard zaštite. Nedostaci svakog pristupa, iako korektno navedeni, najčešće ostaju u senci, jer ih korisnici prihvataju kao „nužno zlo“ primenjene metodologije za koju se odlučuje.
2. **Sistemska-inženjerski, objektno-orijentisani i procesni pristup** IKT zaštiti, predstavlja najpotpuniji okvir za sveobuhvatni i najmanje kompleksan, struktuiran pristup teoriji i praksi bezbednosti i zaštite IKT sistema. Ovaj rad je najvećim delom fokusiran na **procesne zaštite**, kao fundamentalne blokove za sistem-inženjerski i objektno-orijentisani pristup razvoju, implementaciji i održavanju programa i sistema zaštite. Značaj fokusiranja ovog rada na *procesne zaštite* treba posmatrati u uslovima relativno slabije razvijenih procesa zaštite u odnosu na standardne proizvodno-industrijske, ili procese za proizvodnju softvera. Procesi zaštite su u radu razmatrani sistematično i celovito, počevši od formalnih definicija i relevantnih opisa, preko kompleksnih modela za evaluaciju i poboljšavanje procesa zaštite, do postizanja atributa zrelih-stabilnih, ponovljivih, upravljivih i optimalnih (adaptivnih) procesa, primenom modela sazrevanja procesa zaštite - SSE CMM.
3. **Standardi zaštite** su neophodni za konzistentnu praksu IKT zaštite, kao baze znanja, referentne instrukcije za uspostavljanje dokumentacije zaštite, interoperabilnost IKT sistema i sakupljanje i održavanje podataka za legalne potrebe *digitalne forenzike* u slučaju zloupotreba i kompjuterskog kriminala. Modelovanje i modeli su neizbežni elementi *sistenskog inženjerstva zaštite* (SSE) i alati za projektovanje adekvatnih i rentabilnih sistema zaštite. Standardi i modeli su brojni i različito orijentisani, ali pojedinačno nedovoljno dobro pokrivaju svu složenu problematiku i procese zaštite. Korisnici su često prinuđeni da primenjuju više standarda, modela i okvira za uspostavljanje, implementaciju, održavanje i poboljšavanje procesa zaštite. *SSE CMM model sazrevanja integrisanih procesa zaštite* (SSE, projektnih i organizacijskih) omogućava smanjenje broja potrebnih standarda i modela, pokrivajući sasvim dobro većinu procesa organizacija, koje na bilo koji način uključuju oblast zaštite IKT sistema.
4. **Specifičan doprinos rada** je i *fokusirana, priručnička forma komparativne analize* sa identifikacijom kompatibilnih i komplementarnih elemenata strukture relevantnih standarda i modela *najboljih praksi* zaštite (ISO/IEC 13335, ISO/IEC 17799, ISO/IEC 15408 ili CC, ISO/IEC 21827 ili SSE CMM, NIST, COBRA, OCTAVE, ISF 4.0 i drugi) i isticanjem prednosti modela integrisanih procesa (SSE CMM, CMML,...). Ovo može omogućiti menadžerima, specijalistima i korisnicima direktan uvid u prednosti i nedostatke relevantnih standarda i modela i lakši izbor adekvatnih standarda i modela, ili njihovih kombinacija, koje najviše odgovaraju standardnim procesima, kulturi rada i bezbednosnom okruženju konkretne organizacije.
5. **Standardi i modeli kvaliteta** proizvodnih, industrijskih procesa dobro su definisani, razvijeni i pokriveni serijom IS 9000 standarda, ali nisu u celini primenljivi za procese zaštite. Na bazi generičkog modela za merenje sazrevanja i kontrolu kvaliteta procesa (CMM-Capability Maturity Model) razvijeno je više tipova **procesno orijentisanih** modela, od kojih je **SSE CMM** model integrisanih *inženjerskih (SSE), projektnih i organizacionih* procesa za merenje sazrevanja (poboljšavajna) *najboljih praksi i procesa zaštite, jedinstven* i usvojen kao ISO/IEC 21827 standard zaštite 2002. godine. U radu su detaljno opisani SSE CMM model i brojne mogućnosti primene u oblasti IKT zaštite, a

primenljivost modela verifikovana je u istraživačkom projektu rada, kroz SSAM evaluaciju tekućih procesa organizacije ESS, sa visokim stepenom tačnosti i korisničke prihvatljivosti.

6. **Evaluacija tekućih procesa ESS za uspostavljanje PKI i CA** na 3 evaluirana projekta sa ciljem poboljšavanja procesa, argumentovano je razmatrana, detaljno analizirana i *eksperimentalno potvrđena* u istraživačkom projektu. Istaknut je značaj i kvalitet *verifikacionog tipa* SSAM metoda evaluacije, koji proces evaluacije zasniva na verifikaciji *koraborativnosti, pokrivanja i kompletnosti* objektivnih dokaza o izvršavanju, implementaciji i institucionalizaciji praksi i procesa u odnosu na referentni SSE CMM model. Obim razvijenih radnih materijala, angažovanja TE, evidentiranog broja dokaza i rezultata evaluacije dobijenih u istraživačkom delu rada, nesumnjivo potvrđuju da je SSAM metod evaluacije *sistematičan, vremenski zahtevan, tačan i umereno destruktivan* za poslove organizacije. Međutim, obezbeđivanjem *on-line* uvida u dokaze na internom *web portalu* u radnoj prostoriji TE, sakupljanjem dokaza u *Excel tabeli za evidenciju dokaza* i konsolidovanje pokrivanja, koraborativnosti i kompletnosti dokaza, kao i obezbeđivanjem intervjua u radnoj prostoriji TE, **tačnost metoda može se dodatno proveriti i povećati. Vreme rada i destruktivnost procesa evaluacije može se značajno smanjiti**, dobrom pripremom TE u pre-pripremnoj fazi i izradom predloga *Plana evaluacije* i drugih radnih materijala.
7. **Poseban doprinos rada je prilagođavanje i poboljšanje** referentnog SSE CMM modela (v.3.0, 2003.) i SSAM metoda evaluacije (v.2.0, 1999.) u delu koji evaluatoru obezbeđuje *bržu, precizniju i jeftiniju evaluaciju* praksi i procesa zaštite. Razvijen je radni dokument **SSAM PIID** u kojem su eksplicitno numerisani ciljevi oblasti procesa (OP), a **primeri proizvoda rada** bazičnih praksi (BP) u opisu OP, eksplicitno su **definisani kao direktni objektivni dokazi** izvršavanja, implementacije i institucionalizacije praksi i procesa zaštite. Uvođenjem izmena parametara koje SSAM metod dopušta i navedenih **prilagođavanja** SSE CMM modela i SSAM metoda kroz **novi** radni dokumenat, iskorišćene su prednosti poslednje verzije SCAMPI v.1.2 (2006) metoda evaluacije, na bazi referentnog CMMI v.1.2 (2006) modela integrisanih procesa, koji, međutim, nije dovoljno kompletiran sa neophodnim praksama i procesima zaštite za primenu u sistem-inženjerskoj praksi IKT zaštite.
8. **Specifičan doprinos razvoju SSAM metoda** je generisanje i način upotrebe originalno razvijene *Excel tabele za evidenciju* i sakupljanje dokazujućih podataka iz različitih (*koraborativnih*) izvora dokaza: direktnih i indirektnih, neposrednih opservacija i izjava praktičara koje se na bilo koji način mogu dokumentovati. Na ovaj način obezbeđuje se direktan pregled *koraborativnosti, kompletnosti i pokrivanja* dokaza u evaluiranim projektima, olakšava se verifikacija dokaza u procesu konsolidovanja DTS tabele i obezbeđuje *dodatna provera tačnosti SSAM metoda*, koju originalni metod ne predviđa. Ova tabela evidentno potvrđuje u kojoj meri je SSAM metod evaluacije sistematičan, vremenski zahtevan i destruktivan za tekuće poslovanje organizacije.
9. **Značajan doprinos** razvoju SSAM metoda evaluacije, predstavlja i programski modifikovana, jezički i terminološki prilagođena našem jeziku i kulturi rada **SSE CMMI/SCAMPI Appraisal Assitant** aplikacija za SCAMPI evaluaciju procesa zaštite na bazi **SSE CMM** modela. Originalna aplikacija namenjena je prevashodno, kao interaktivni programski alat evaluatora, za SCAMPI v.1.2 evaluaciju na bazi CMMI v.1.2 modela integrisanih procesa, bez mogućnosti trivijalne implementacije SSE CMM modela. Reinženjeringom aplikacije i odgovarajućom intervencijom u programskom kodu u aplikaciju je implementiran SSE CMM model, čime je omogućena primena SCAMPI metoda za evaluaciju procesa zaštite. Primena modifikovane **SSE CMM/SCAMPI Appraisal Assitant** aplikacije, koja koristi sve prednosti SCAMPI v.1.2 (2006) metoda evaluacije procesa, obezbeđuje interaktivni alat za efikasniji rad TE, povećava tačnost i efikasnost procesa evaluacije u odnosu na SSAM v.2.0 (1999) metod evaluacije.
10. **Praktični doprinosi rada za evaluiranu organizaciju – ESS** su glavni nalazi snage i slabosti, *profil nivoa kapaciteta tekućih procesa* i predlog zadataka za *akcione planove* za poboljšavanje procesa na bazi rezultata i glavnih nalaza SSAM evaluacije, kao i

osposobljavanje članova tima za evaluaciju iz redova zaposlenih - *posmatrača*, za definisanje i formalni opis standardnih procesa, dokumentovanje praksi i procesa i primenu SSE CMM modela i SSAM metoda evaluacije za samo-evaluaciju i konstantno poboljšavanje procesa ESS.

11. **Doprinos rada** je i uspostavljeni *radni materijal* za evaluaciju tekućih procesa ESS – ukupno 80 radnih dokumenata, uključujući i programsku aplikaciju, terminološki i semantički prilagođenih srpskom jeziku i kulturi rada, sa kompleksnim opisom toka procesa evaluacije i *procedura evaluacije* razvijenih u istraživačkom delu rada, SSAM uputstvima za rad Sponzora i evaluatora, diskusijom i analizom rezultata, koji zajedno obezbeđuju svojevrsno *operativno uputstvo* za praktičnu primenu SSE CMM modela i SSAM metoda evaluacije. Naime, **SSE CMM** obezbeđuje referentni model *najboljih*, zrelih praksi i procesa zaštite, pomaže da se identifikuju potencijalne oblasti procesa za poboljšavanje, obezbeđuje definicije na nivou bezbednosnih ciljeva i ključne atribute za identifikaciju specifičnih bazičnih praksi (BP) i procesa (OP) i definisanje karakteristika procesa, ali *ne obezbeđuje operativno uputstvo za praktičnu primenu*.

8. Ključni termini

Agilni metod razvoja proizvoda: Obezbeđuje sredstva za usmereni razvoj i proizvodnju procesa sa njihovim fundamentalnim i najkritičnijim komponentama; nastali su sa bržim promenama na tržištu i zahtevima za brže isporuke proizvoda (n.p.r., softvera), koje korisnici popravljaju u toku operativne primene i prakse, nastojeći da pri tome izvrše maksimalno ažuriranje ranjivosti u minimalnom vremenu.

Argument bezbednosne garancije (*assurance argument*): Skup struktuiranih izjava, tvrdnji, dokumenata koji potvrđuju garantovanu bezbednost, a kojeg podržavaju objektivni dokazi i rezultati koji jasno pokazuju da su zahtevi za garantovanu bezbednost zadovoljeni.

Bazična praksa (BP): Mora se izvršiti u implementiranom procesu (**OP**) SSE CMM modela u životnom ciklusu sistema i uglavnom se ne preklapa sa drugim **BP**; generalno predstavlja *najbolje prakse zaštite*; prikazuje se u opisu OP u modelu na standardizovan način sa: *rednim brojem, nazivom, opisom, tipičnim rezultatima (primerom proizvoda rada) i napomenom*.

Bezbednosna garancija (*security assurance*): Izvršavanje odgovarajućih aktivnosti, ili procesa u cilju postizanja poverenja da proizvod/sistem/servis/proces zaštite postiže bezbednosne ciljeve; osnova za poverenje da neki entitet postiže svoje bezbednosne ciljeve [ISO/IEC 15408–1]

Bezbednosna kategorizacija: Klasifikacija objekata IKT sistema u kategorije sa jednakim bezbednosnim zahtevima i ciljevima.

Direktni artefakti: Opipljivi izlazni rezultati implementiranih praksi, n.p.r., tipični proizvod rada navedeni u CMMI modelu procesa.

Dokument za opisivanje SCAMPI metoda (*MDD-Method Description Document*): Dokument opisuje sve tri klase metoda i odobrava samo **A** metod SCAMPI evaluacije koju izvršava osposobljen tim za evaluaciju.

Dokumenta: Dokumentacija procesa - politike organizacije, procedure i planovi implementacije; može biti tvrda kopija, elektronski dokument, HTML i sl.

Evaluacija (*evaluation*): Sistematsko prosuđivanje i određivanje primarnih i/ili sekundarnih vrednosti nekog evaluiranog entiteta (*evaluanda*) - cilja, misije, strategije, projekta, programa, procesa, organizacije i sl.; uvek je svrsishodna – ima za cilj stvaranje kognitivnih pretpostavki za efikasno i efektivno odlučivanje i delovanje; *evaluacija (appraisal)* implicira da evaluaciju obavlja nezavisni stručni tim za evaluaciju, osposobljen za primenu referentnog modela i metoda za evaluaciju i poboljšavanje procesa.

Garancija kvaliteta procesa: Evaluacija, ili provera kvaliteta rada i sprovođenja procesa, ispravnosti, rigoroznosti, efikasnosti i efektivnosti kontrole kvaliteta, ispunjavanja ciljeva organizacije procesom i stepena uticaja procesa na kvalitet proizvoda/srvisa u životnom ciklusu.

Generalno prihvaćeni principi zaštite informacija (*GAISP-Generally Accepted Information Security Principles*): Osnovni gradivni blokovi na kojima se zasnivaju procesi upravljanja sistemom zaštite; odnose se na fizičke, tehničke i administrativne komponente sistema zaštite, a dele u tri kategorije - *opšte, funkcionalne i potpune (detaljne) principe zaštite*, u kojim se principi zaštite sakupljaju, komentarišu i organizuju. Opšti principi odnose se na upravljanje, funkcionalni – na operativno upravljanje, a potpuni - na praksu zaštite i specijaliste zaštite; u širem smislu uključuju *principe, standarde, konvencije i mehanizme i protokole zaštite*.

Generičke prakse (GP): Predstavljaju izvorne, opšte radnje koje se izvršavaju u svim procesima (**OP**) u domenu, a koje određuju kapacitete organizacije za izvršavanje procesa, odnosno **kvalitet izvršavanja BP** procesa; u modelu su poredane po opštim karakteristikama (**CF**) prema zrelosti, tako da **GP** sa većom zrelosti ukazuje na viši nivo kapaciteta procesa; moraju biti izvršene u

nekoj **OP**, kao deo izvršavanja **BP**, da bi se odgovarajuća **OP** pripisala nekom nivou kapaciteta/zrelosti (**CL/ML**); stepen implementacije i institucionalizacije **GP** koristi se za **evaluaciju** (*appraisal*) i progresivno poboljšavanje procesa.

Indikatori implementacije praksi (PII): SCAMPI metod evaluacije na bazi CMMI modela procesa specifikuje sledeće tipove indikatora implementacije praksi modela *direktne artefakte*, *indirektne artefakte*, *potvrđne izjave*.

Indirektne artefakti: Posledice ili indikacije implementacije praksi navedenih u CMMI modelu procesa.

Instrumenti CMM: Upitnik, anketa, imovina procesa orgnizacije koja odražava dokaz o implementaciji praksi prema CMMI i SSE CMM modelima procesa; radna dokumenta SCAMPI i SSAM metoda evaluacije za prikupljanje dokaza o implementaciji praksi.

Intervju: Struktuiran plan razgovora sa poznavaoacima evaluiranih procesa - liderima projekta, praktičarima, korisnicima za prikupljanje dokaza i razjašnjavanje nejasnih pitanja iz *Upitnika* u procesima SCAMPI i SSAM metoda evaluacije; može biti po pozivu, ili dodatni.

Izvršavanje procesa: Mera stvarnih rezultata procesa na određenom projektu koji mogu, a ne morju pasti unutar očekivanog opsega.

Kapacitet procesa: Odnosi se na potencijale resursa organizacije; opseg u kojem se očekuje izvršavanje procesa organizacije, koji se mogu postići kada se proces sledi i izvršava; predviđa buduće izlazne rezultate projekta.

Kategorije komponenti CMMI modela: Model obuhvata tri kategorije komponenti *zahtevane-specifični ciljevi* (SG) i *generički ciljevi* (GG), *očekivane-specifične prake* (SP) i *generičke prakse* (GP) i *informativne-subprakse* i tipični proizvodi rada. U procesu evaluacije tim za evaluaciju (TE) pronalazi indikatore *implementacije* i *institucionalizacije* specifičnih i generičkih praksi (SP i GP) projekta koji *objektivno* potvrđuju da su specifični i generički ciljevi organizacije zadovoljeni.

Kolaboracija: U konteksti SSAM i SCAMPI evaluacije opisuje zajednički rad TE na konsolidovanju dokaza o implementaciji praksi i procesa preme referentnom modelu. Uključuje i donošenje odluka TE sa konsenzusom.

Kontrola kvaliteta: Evaluacija ili provera kvaliteta proizvoda i životnog ciklusa proizvoda.

Kontrola zaštite: Krajnja klasifikacija mehanizama zaštite, koja implicira da svaki mehanizam (servis, sistem) zaštite ima punu vrednost samo ako se može *kontrolisati*; tipično neka funkcija dizajna sistema koja se odnosi na: *tehničke mehanizme zaštite* i kibernetičku kontrolnu-povratnu spregu, kao što su mehanizmi za identifikaciju i autentifikaciju, uređaji za fizičku kontrolu pristupa (video nadzor, protivprovalni senzori i sl.), kriptografski mehanizmi, neki IDS/IPS i.t.d.; *raspoloživu dokumentaciju zaštite* -zakone, standarde, uputstva i.t.d., i *operativne prakse* - fizičko kretanje ljudi kroz računski centar i njihove operativne i upravljačke aktivnosti; poseduju dva osnovna atributa: *robustnost* (otpornost na napade) i *adaptivnost* (*fleksibilnost* i *skalabilnost*).

Koraboracija: U kontekstu SSAM i SCAMPI metoda evaluacije označava obezbeđivanje dokaza za istu praksu iz različitih izvora.

Kvantitativno upravljanje: Upravljanje na bazi brojeva i drugih statističkih podataka.

Menadžment: Uključuje interakciju organizacije sa okruženjem i omogućava organizaciji da bolje kontroliše svoje okruženje u cilju uspešnijeg postizanja misije i ciljeva.

Menadžment tehnologije: Uključuje interakciju *tehnologije*, *organizacije* koja skuplja i koristi tehnologiju i *okruženja*.

Merenje u zaštiti: Obezbeđuje jednokratni uvid u specifične merne parametre komponente/sistema zaštite, predstavljen sa brojevima, težinskim faktorima, ili binarnim saopštenjima.

Metrika zaštite: Višekratna merenja tokom vremena, sa upoređivanjem dva, ili više merenja prema pre-definisanim osnovnim sistemima merenja, čime se obezbeđuje sredstvo za interpretaciju sakupljenih merenih podataka.

Metod bezbednosne garancije (*assurance method*): Priznata specifikacija za dobijanje ponovljivih rezultata bezbednosne garancije (garantovane bezbednosti).

Metod evaluacije procesa zaštite (*SSAM-System Security Appraisal Method*): Metod evaluacije razvijen za specifičnu primenu SSE CMM metodologije za evaluaciju procesa zaštite; koristi SSE CMM referentni model procesa, a izvršava ga osposobljen tim za evaluaciju.

Metod evaluacije za poboljšavanje procesa (*SCAMPI - Standard CMMI Appraisal Method for Process Improvement*): Metod evaluacije na bazi CMMI modela procesa; obuhvata dva ključna dokumenta: **Zahtevi za CMMI evaluaciju - ARC** (*Appraisal Requirements for CMMI*) koji sadrže zahteve za tri klase metoda evaluacije: A, B i C i Dokument za opis SCAMPI metoda – **MDD** (*Method Description Document*).

Metodi za merenja nivoa zaštićenosti informacija: U praksi zaštite razvijene su brojne metode - analiza rizika, kontrola (*auditing*), sertifikacija, merenje upada u sistem (IDS/IPS), nadzor performansi sistema zaštite (mrežni skeneri), testiranje sistema na proboj (simulacija malicioznih napada) i.t.d.

Metrički sistem zaštite: Skup kriterijuma, parametara, merenih podataka i jedinica za izražavanje rezultata merenja, koji uobičajeno podrazumeva procese **evaluacije** (*auditing*, analiza ranjivosti, testiranje na proboj) i/ili **monitoringa** performansi servisa zaštite (tehnički sistem metrike, log datoteke); u praksi zaštite najčešće se primenjuju - snaga kriptografskog algoritma, kvalitativna metrika (npr. uticaja: *nizak, srednji, visok*); kvantitativna metrika (*cost - benefit*), metrika softverskog inženjerstva (SwE), detekcija anomalija (IDS/IPS), srednje vreme napada, intervju, metrika poslovnih procesa, metrika kontrole sistema zaštite (*auditing*) i **SSE-CMM dualna metrika sazrevanja procesa zaštite**; razvijena su tri tipa metričkih sistema zaštite, za merenje: (1) *kvaliteta implementacije politika zaštite*, (2) *efektivnosti i efikasnosti servisa zaštite* i (3) *uticaja bezbednosno relevantnih događaja na poslove i misiju organizacije*.

Metrika zaštite: Višekratno merenje u dužem vremenskom periodu ili sredstvo za interpretaciju agregiranih podataka merenja (merenih podataka) na višem nivou (organizacije); zahtevani mereni podaci moraju biti dostupni, a razmatrani procesi merljivi, konzistentni, stabilni i ponovljivi; mora obezbediti kvantitativne *merne jedinice*, uporedive od jednog do drugog merenja i primenljive za analizu i praćenje promena korišćenjem istih referentnih merenih vrednosti - **procenatni račun, srednja vrednost i apsolutni brojevi**; monitoriše stepen postizanja taktičkih (*goals*) i strateških (*objectives*) ciljeva zaštite: kvantifikovanjem nivoa implementacije, efektivnosti i efikasnosti kontrola zaštite, analizom adekvatnosti procesa i kontrola zaštite i identifikovanjem mogućih akcija za njihovo poboljšavanje.

Model sazrevanja procesa (*CMM- Capability Maturity Model*): Model procesa usmeren na upravljačke i organizacione procese i aktivnosti; referentni model zrelih praksi i procesa u specifikovanim disciplinama za procenu grupnih kapaciteta za izvršavanje te discipline.

Model sazrevanja procesa zaštite (*SSE CMM-System Security Engineering Capability Maturity Model*): Model i metod sazrevanja sistem-inženjerskih procesa zaštite, specifično razvijen za razvoj i poboljšavanje procesa zaštite; sadrži metodologiju za evaluaciju i poboljšavanje procesa zaštite i posebno razvijen metod (SSAM) za primenu te metodologije.

Najbolje prakse (*Best practices*): Najbolje prakse zaštite su one koje su dokumentovane, dostupne, efektivne, adekvatne i široko prihvataju strategije, planove, taktike, procese, metodologije, aktivnosti i pristupe koje su razvila ekspertska tela, a izvršava ih adekvatno osposobljeno osoblje u skladu sa postojećim zakonima i regulativama i koje su vremenom pokazale kroz istraživanje, evaluaciju i praksu, da su efikasne u obezbeđivanju racionalnog nivoa zaštite željenog izlaza i koje se neprekidno revidiraju i poboljšavaju u skladu sa potrebama.

Nivo kapaciteta/zrelosti (CL/ML): dimenzija kapaciteta procesa (OP) koja vrši kategorizaciju *nivoa kvaliteta* postizanja ciljeva OP; definiše **kako** se dobro procesi izvršavaju kroz stepen implementacije i institucionalizacije generičkih praksi-GP i opštih karakteristika-CF (SSE CMM), ili GP i generičkih ciljeva-GG (CMMI).

Objekti merenja: U sistemu zaštite informacija objekti merenja mogu biti *organizacija proizvod* (planiran, u razvoju, u radu), *tehnički sistem* (hardver, softver, komunikaciona infrastruktura), objekti sistema i sl.

Objektivni dokazi implementacije praksi: Dokazi koji su objektivni (postoje i mogu se verifikovati), a potvrđuju da su prakse i procesi SSE CMM i CMMI modela imlementirani u projektu/organizaciji.

Oblast procesa (OP): Osnovna komponenta dimenzije primene svih CMM modela procesa; generalno definiše **šta** treba da se postigne sa inženjerskim (SSE), projektnim i organizacionim procesima; sadrži bazične prakse (BP) koje se u jednoj OP moraju izvršavati, da bi se OP smatrala izvršenom; SSE CMM model sadrži ukupno 22 OP-11 originalnih *inženjerskih* (SSE) i 5 *upravljačkih* (projektnih) i 6 *organizacionih* OP koje su u celini nasleđene iz SE-CMM; u modelu su opisane u standardnom formatu sa: *rednim brojem, nazivom, ciljem, kratkim opisom sadržaja i opisom BP*.

Ocenjivanje: Poređenje opservirane vrednosti sa standardnom; ocena je količnik opservirane i standardne vrednosti.

Opšte karakteristike (CF): Svi opšti aspekti procesa, grupisani u logičke oblasti - nivoa kapaciteta; sadrže jednu ili više **GP** i kategorizuju **GP**; kategorije **CF** su vrlo slične kroz sve **OP**; nazivaju se *institucionalizacija* zato što osiguravaju da su **OP** efektivne, ponovljive i stabilne i da obezbeđuju potrebnu infrastrukturnu podršku; organizovane su na 5 aktivnih *nivoa kapaciteta* - **CL** (1-5).

Performansa procesa: Mera aktuelnih rezultata postignutih izvršavanjem procesa. (isto-izvršavanje procesa).

Potvrdne izjave: Usmene, ili pisane izjave lidera projekta, menadžera i drugih praktičara, koje potvrđuju, ili podržavaju implementaciju praksi, tj., odgovori na upitnike i intervju.

Prezentacije rezultata evaluacije: Demonstracije alata SCAMPI i SSAM metoda evaluacije, pregledi brifinga, izveštavanje rezultata evaluacije i sl.

Pristup (approach): Metod koji se koristi, ili koraci koji se preduzimaju u pripremi za rešavanje nekog zadatka, ili problema.

Procena bezbednosne garancije (assurance assessment): Verifikacija i registrovanje svih tipova i količina argumenata bezbednosne garancije koji postoje za neki proizvod/ sistem/servis/proces zaštite u životnom ciklusu.

Proces zaštite: Sekvencijalno izvršavanje aktivnosti zaštite radi ostvarivanja jedinstvenog bezbednosnog cilja, ima početak i kraj i definisane ostale resurse; transformator ulaznih veličina u sistem zaštite u izlazne, objedinjujući upravljačke aktivnosti, procedure zaštite - sekvencijalno izvršavane aktivnosti, ili praksi zaštite i dokumentaciju procesa; integrator tri ključna atributa prakse zaštite - procedura i metoda koje definišu zadatke, tehnika i alata i osposobljenih ljudi motivisanih za izvršavanje zadataka.

Profil nivoa kapaciteta/zrelosti procesa: Rezultat SSAM/SCAMPI metoda evaluacije nivoa zrelosti/kapaciteta procesa, prikazan u reprezentaciji bar dijagrama.

Proizvod rada procesa: Bilo koji artefakt kojeg proces proizvede, kao što su elektronske datoteke, papirna dokumenta, deo proizvoda, servisi, procesi, specifikacije i profakture. Primeri procesa koji se mogu smatrati proizvodom rada uključuju proizvodni proces, proces obuke i proces za odlaganje proizvoda. Ključna razlika između proizvoda rada i komponente proizvoda je u tome što se proizvod rada ne mora više procesirati, ili je deo konačnog proizvoda.

Projekat: Upravljiv skup međusobno povezanih resursa, koji obezbeđuje isporuku jednog ili više proizvoda kupcima ili krajnjim korisnicima.

Reprezentacija CMM modela: Predstavlja organizaciju, način primene i prezentacije komponenti CMM modela i put sazrevanja procesa; može biti *kontinualna (CL)* - progresivno, inkrementalno, ili inovativno, kontinualno poboljšavanje procesa individualnih OP i *fazna (ML)* - poboljšavanje procesa organizacije kroz više OP.

Sertifikacija (Certification): Procedura zaštite koja obezbeđuje sveobuhvatnu *evaluaciju* tehničkih i ne-tehničkih komponenti sistema zaštite; uspostavlja *meru u kojoj* određeni projekat i implementacija sistema zaštite ispunjavaju specifikovane bezbednosne zahteve; obezbeđuje *dokaz* o usklađenosti sa bezbednosnim zahtevima; obezbeđuje *podatke* za akreditaciju sistema zaštite.

Sistem: 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.

Sistemska analiza: Sveobuhvatan pristup problemima i njihovom rešavanju sa utvrđivanjem performansi sistema, ograničenja, zahteva za resursima i interakcije sa okruženjem.

Sistemska inženjerstvo u IKT zaštiti (SSE): Elemenat sistemskog inženjerstva (SE) koji primenjuje naučne i inženjerske principe za identifikaciju bezbednosne ranjivosti IKT sistema i smanjenje, ili ublažavanje faktora rizika koji prate te ranjivosti.

Sistemska pristup (sistemska inženjering): Posmatranje objekata i pojava u dinamičkom odnosu prema sebi i okruženju; relevantan u tehničkim i brojnim drugim disciplinama; logički pristup za modelovanje situacija; obezbeđuje efikasnost i efektivnost primene IKT u poslovnim sistemima; struktuirani metod razvoja modela i konceptualnog okvira za analizu i istraživanje date situacije; čine ga *sistemska mišljenje* i *sistemska analiza*.

Sistemska mišljenje: Eksplicitan naučni alat za istraživanje kompleksnosti fenomena i upravljanja problemima realnog sveta, dopunjuje analitičko mišljenje i glavni je faktor strategije dekomponovanja kompleksnih fenomena sistema; metod za razmatranje i rešavanje brojnih realnih problema i različitih tipova kompleksnosti; fokusira pažnju na *proces* - modelovanje, evaluaciju i poboljšavanje i *dinamičke strukture* - projektovanje planiranih sistema.

Stabilan proces: Proces koji ispunjava najmanje tri osnovna atributa: *produktivnost, adaptivnost i korisničku prihvatljivost*; zreo proces – planiran, praćen i kontrolisan, dobro definisan, kvantitativno upravljan i optimizovan (adaptivno poboljšavan).

Standardi zaštite: Pomažu korisnicima da prevedu (kodiraju) zahteve za zaštitu sa nivoa normativa u bezbednosne zahteve na nivou politika zaštite; *smanjuju kompleksnost* sistema zaštite u procesu upravljanja, obezbeđuju izradu *standardne dokumentacije, interoperabilnost* sistema zaštite i formiranje *baze znanja* iz oblasti zaštite.

Strategija zaštite: Obezbeđuje osnovni okvir za pomeranje nivoa bezbednosti IKT sistema sa jednog (nižeg) nivoa bezbednosti na drugi (viši) nivo bezbednosti; uključuje *inicijative*, koje sadrže skup *projekata* zaštite raspoređenih po prioritetima izvršavanja u *akcionom planu* za izvršavanje inicijativa i projekata i indikatore progressa razvoja strategije (*benčmarking sistem*) za praćenje stanja progressa u razvoju strategije zaštite.

Tehnologija: Organizacija, aplikacija i isporuka naučnih znanja i drugih formi znanja za poboljšavanje poslovanja klijentskih grupa, koja uključuje tehnika i alate, ali se u osnovi može smatrati ljudskom aktivnosti.

Uputstva za zaštitu: Precizne instrukcije za upravljanje sistemom zaštite, koje ne obavezuju korisnike da ih striktno sprovode za razliku od zakona i standarda zaštite.

Vrednovanje (validacija): Potvrđivanje ispunjavanja namene proizvoda/servisa zaštite.

Verifikacija: Potvrđivanje da proizvod/servis zaštite odražava specifikovane zahteve.

Zahtevi za CMMI evaluaciju (*ARC-Appraisal Requirements for CMMI*): Dokument opisuje zahteve za tri klase metoda evaluacije - A, B i C, koji postavljaju pravila za definisanje svake klase metoda evaluacije.

Zrelost procesa: Mera u kojoj je proces eksplicitno planiran, definisan, upravljani, merljiv, kontrolisan, ponovljiv i efektivan (isto: *stabilnost*).

9. 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) American National Standards Institute-ANSI: *Electronic Standards Store*, <http://webstore.ansi.org/ansidocstore/default.asp>, avgust 2003.
- 3) Anderson D. J., *Schrageheim E., Agile Management for Software Engineering: Applying the Theory of Constraints for Business Results*, Prentice Hall, 2003.
- 4) Australasian Police Education Standards Council Inc.(APESC), *Training Package: User Guide for the Policing Profession*, www.apesc.org, 2001.
- 5) B. Boehm and Turner, R., *Principles Behind the Agile Manifesto*, Pearson Education, Boston, MA, www.agilealliance.org/principles.htm, 2003.
- 6) Bahan C, *The Disaster Recovery Plan*, <http://www.sans.org>, 2003.
- 7) Banjanin K.M., *Metodologija inženjeringa –inženjerske analize i mreže znanja*, DIS PUBLIC, Beograd, 2006
- 8) Banjanin K.M., *Naučno istraživačka metodologija*, DIS PUBLIC, Beograd, 2006.
- 9) 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.
- 10) Barton R., Hery J. W., Liu Peng, *An S-vector for Web Application Security Management*, Penn State University, PA, rbarton@psu.edu, 2004.
- 11) Bate R., and all, *A Systems Engineering Capability Maturity Model V.1.1*, Software Engineering Institute, www.sei.cmu.edu, US DoD, 1995.
- 12) Bishop M., *Introduction to Computer Security, Chapter 18: Evaluating Systems* Wesley and Sons, November 1, 2004.
- 13) Bjork Fredrik, *Security Scandinavian Style-Interpreting the practice of managing information security in organizations*, Stockholm University, Rozal Institute of Technology, 2001.
- 14) British Standards Institution, *BS 7799-2—Code of Practice for Information Security Management*, <http://www.bsi.org>, <http://www.iso.org>, 1999.
- 15) 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.
- 16) BSI (Federalni IS Nemačke), *IT Baseline Protection Manual*, <http://www.bsi.bund.de/gshb>, juli 2005.
- 17) Carrol M.J., *Computer Security*, Butterworth-Heinemann, 1997.
- 18) CCIMB-99-031, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, Version 2.1, <http://www.commoncriteria.org>, 1999.
- 19) CERT, <http://www.cert.org/advisories>, 2003.
- 20) Chrissis M. B., Konrad M., Shrum S., *CMMI v.1.2, Guide for process integration and product improvement*, Second Edition, SEI, Addison-Wesley, 2006.
- 21) COBIT, *Cobit-Control Objectives for Information and Related technologies*, <http://www.ITgovernance.org>, <http://www.isaca.org/cobit>, 2000.
- 22) CRAMM, <http://www.crammusergroup.org.uk>, 2004
- 23) Curtis B.I, Hefley E. W., Miller S., *People Capability Maturity ModelSM*, CM SEI, www.sei.cmu.edu, 1995.

- 24) Domarev V.V., *Защита информации и безопасность компьютерных систем*, <http://www.security.ukrnet.net/>, 1997.
- 25) Dorothea E. de Zafra, Sadie I. P., *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST SP 800-16, <http://www.nist.gov/publications>, 1998.
- 26) DTI- Department of Trade and industry, *Process understanding and improvement*, www.dti.gov.uk/quality/process, 2006.
- 27) Ferraiolo Karen & Sachs Joel E., *Distinguishing Security Engineering Process Areas by Maturity Levels*, USA Columbia, ferraiolo@md.arca.com, sachs@interramp.com, 1996.
- 28) Ferraiolo Karen M., *Considerations for Re-architecting the SEI CMM and Building Engineering CMMs*, Arca Systems, Inc., ferraiolo@arca.va.com, 1995.
- 29) GAISP – *Generally Accepted Information Security Principles*, <http://www.gaisp.org>, 2003.
- 30) Gary Smith: *A brief Taxonomy of Firewalls-great Walls of Fire*, SANS Institute, <http://www.sans.org/rr/firewall/taxonomy.php>, 18 maj 2001.
- 31) Gaskell Gary, *Information Security Standards*, http://www.nist.gov/publications/public_affairs/standards.htm, 2001
- 32) Glenn Fourie, *The evolution of the information Security mindset: a hypothesis of Stages of individual and enterprise Security maturation*, www.sans.com, 2002.
- 33) Grance T., Hash J., Stevens M., *Security Considerations in the Information System Development Life Cycle*, NIST SP 800-64, <http://csrc.nist.gov/publications/nistpubs/800-64/sp800-64.pdf>, juni 2004.
- 34) Grance T., Kent K., Kim B., *Computer Security Incident Handling Guide*, NIST SP 800-61, <http://www.nist.gov/publications>, January 2004.
- 35) Hefner Rick Ph.D, and Monroe W., *System Security Engineering Capability Maturity Model*, TRW, CA, rick.hefner@trw.com, 1997.
- 36) Hefner R., Ph.D, *Lessons Learned with the Systems Security Engineering Capability Maturity Model*, rick.hefner@trw.com, 2000.
- 37) Hopkinson J. P., *System security engineering capability maturity model - Organization profiles*, EWA-Canada, John.Hopkinson@sympatico.ca, 2003.
- 38) Hopkinson John P., *The Relationship Between The SSE CMM and IT Security Guidance*, EWA-Canada, John.Hopkinson@sympatico.ca, 1999.
- 39) Housley R. i dr., *Internet X509 Public Key Infrastructure: Certificate and CRLProfile (RFC 2459)*, <http://www.ietf.org/rfc/rfc2459.txt>, 2002.
- 40) Howard D., J., *An Analysis of Security Incidents on the Internet 1989-1998*, Thesis for the degree of doctor of philisophy, Carnegie Mellon University, http://www.cert.org/incident_notes/index.html, 1997.
- 41) Ibrahim L., *Enterprise Process Improvement*, US Federal Aviation Administration, Business Process Management Conference Washington DC , linda.ibrahim@faa.gov, 19.09. 2006
- 42) IEC/ISO 17799 Security Standard overview, <http://www.securityauditor.net/iso17799/what.htm>, 2005.
- 43) *Introduction to the OCTAVE® Approach*, <http://www.cert.org/octave>, 2005.
- 44) ISACA, *IS Auditing Procedure: Security Assessment Penetration Testing and Vulnerability Analysis*, Document #8, <http://www.isaca.org>, 2004.
- 45) ISACA, *Standards for Information Systems Control Professionals*, <http://www.isaca.org>, 1999.

- 46) ISACA, *System Security Engineering - Capability Maturity Model*, Round Table, <http://www.isaca.org>, 20 October 2001.
- 47) ISF, *The Standard for Good Practice for Information Security*, <http://www.isf.org>, V.3.0., 2003.
- 48) ISF, *The Standard for Good Practice for Information Security*, <http://www.isf.org>, V.4.0., 2006.
- 49) ISO/IEC 15408, *Common Criteria for IT Evaluation User Guide*, <http://csrc.nist.gov/cc/info/infolist.htm>.
- 50) ISO/IEC 15443, *Information Technology-Security Techniques*, <http://www.iso.15443.org>, 2000.
- 51) ISO/IEC 15504 (CMM), <http://www.iso.15504.org>, 2000.
- 52) ISO/IEC 17799:2000, *Information Technology – Code of practice for information security management*, <http://www.iso.org>, 2005.
- 53) ISO/IEC 21827 (SSE CMM), *System Security Engineering Capability Maturity Model*, <http://www.iso.21827.org>, 2002.
- 54) ISO/IEC JTC 1/SC 27, ISO/IEC TR 15443-1: 2004, *Information technology - Security techniques – A framework for IT security assurance - Part 1: Overview and framework*, <http://www.iso.15443-1.org>, 2004.
- 55) ISO/IEC 13335 - *Guidelines for the management of IT Security*, <http://www.iso.13335.org>, 2003.
- 56) ISO/IEC 15408 - *Common Criteria/ITSEC*, <http://www.iso.15408.org>, 2003.
- 57) ISS, *Dynamic Threat Protection™ : A New Definition for Information Security*, <http://www.iss.org>, 2005.
- 58) *IT Baseline Protection Manual*, <http://www.bsi.bund.de/qshb>, juli 2000.
- 59) ITU-T Recommendation X.509, *Information Technology – Open system Interconnection – The directory: Public key and attribute certificate frameworks*, <http://www.itu.x509.org>, 2002.
- 60) Joshi J., *IS 2620: Developing Secure Systems, Secure Software Development Models/ Methods*, <http://www.sis.pitt.edu/~jjoshi/courses/IS2620/Spring07/>, Jan. 16, 2007
- 61) Kelm S., *The PKI page*, <http://www.pki-page.org>, 2004.
- 62) Kormos C., & all, *Using security metrics to assess risk management capabilities*, NSA, Arc Systems, Booz, Allen & Hamilton, Inc., ckormos@radium.ncsc.mil, 2005.
- 63) Kulpa K. M., & Johnson A.K., *Interpreting the CMMI: A Process Improvement Approach*, Auerbach Publications, 2003.
- 64) 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.
- 65) Lyons-Burke K., *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, NIST Special Publication 800-25, <http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf>, 2000.
- 66) Markus G. K., *Compromising emanations: eavesdropping risks of computer displays*, December 2003.
- 67) McLean, *Mature and Secure: Creating a CMMI® and ISO/IEC 21827 Compliant Process Improvement Program*, Booz, Alen, Hamilton, VA April 11, 2006.
- 68) Milosavljević M., Grubor G., *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, 2006.
- 69) NIST SP 800-14, *Generally Accepted Principles and Practices for Security*, <http://csrc.nist.gov/publications/nistpubs/800-14/sp800-14.pdf>, 2002.
- 70) NIST SP 800-3, *Establishing a Computer Incident Response Capability*, <http://www.nist.gov/publications>, 1999.

- 71) NIST SP 800-53, *Recommended Security Controls For Federal IS*, <http://csrc.nist.gov/publications/nistpubs/800-53/sp800-53.pdf>, 2004.
- 72) NIST SP 800-61, *Computer Security Incident Handling Guide*, <http://csrc.nist.gov/publications/nistpubs/index.html>, 2004.
- 73) NIST, *Federal information technology security framework*, National Institute of Standards and Technology, Gaithersburg, MD, http://www.cio.gov/documents/federal_it_security_assessment_framework.html, 2000.
- 74) NIST, *FIPS 140-2 pulikacija*, <http://www.itl.nist.gov/fipspubs>, 2003.
- 75) NIST, *Standards*, http://www.nist.gov/publications/public_affairs/standards.htm, avgust 2003.
- 76) NIST, *Trusted Computer System Evaluation Criteria*, <http://www.radium.ncsc.mil/tpep>, 1999.
- 77) NIXU, *Evaluating and managing security*, www.nixu.com, 2005.
- 78) OCTAVE methods and criteria, <http://www.cert.org/octave>, 2005.
- 79) Orlandi E., *The Cost of Security*, The Carnahan Conference on Security Technology, IEEE Press, New York, 1991.
- 80) Ozier W., *Risk Analysis and Assessment, Handbook of Informaton Security Management 1999*, CRC Press, Boca Raton, Florida, 1999.
- 81) Pankaj G., *CS497 – Security engineering and software engineering*, Indian Institute of Technology, Kanpur, India, e-mail: [pankajgo]@cse.iitk.ac.in, 2005.
- 82) Petrović R. S., *Kompjuterski kriminal II Izdanje*, MUP R. Srbije, 2001.
- 83) 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.
- 84) Phillips M., CMMI Program Manager, *CMMI V1.1 and Appraisal Tutorial*, Sponsored by the U.S. Department of Defense, Carnegie Mellon University, 2004.
- 85) Purser S., *A practical guide to managing information security*, Artech House, Boston, London, www.artechhouse.com, 2005.
- 86) RFC 3280 (X.509), <http://www.icann.rfceditorc.org>, 2005.
- 87) [Richard B. Waina, P.E. Ph.D](http://www.mdmaturity.com), *Five critical questions in process improvement Part II*, www.mdmaturity.com, 2006.
- 88) 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.
- 89) RSA Data Security Conference, *Functional Model TTPS S2101/03 v.1.1*, San Jose, CA, <http://www.solutioncentre.nl>, 1999.
- 90) Russel D. & Gangemi G.T. sr., *Computer Security Basics*, O'Reilly and Ass., 1995.
- 91) Sademies A., *Process approach to information security metrics in Finish industry and state institutions*, VTT Electronics Publications 544, <http://www.vti.fi/inf/pdf>, ESPOO, 2004.
- 92) Ruth A., Hudson K., *Sertificat Security +*, MicrosoftCo., CET Beograd, 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) Schneier B., *Secrets and lies: Digital security in a networked world*, www.schneier.com, 2000.
- 98) SEI, *Appraisal Method for Process Improvement (SCAMPISM) A, Version 1.2: Method Definition Document*, SCAMPI Upgrade Team, www.sei.cmu.edu, August 2006.
- 99) SEI, *CMMI ARC: Appraisal Requirements for CMMI*, <http://www.sei.cmu.edu/publications/documents/01.reports/01tr034>, 2007.
- 100) SEI, *CMMI MDD: Method Description Document*, <http://www.sei.cmu.edu/publications/documents/01.reports/01tr034>, 2007.
- 101) SEI, *SSAM: SSE Capability Maturity Model Appraisal Method Version 2.0*, www.sei.cmu.edu, april 16, 1999.
- 102) SEI, *Systems Security Engineering Capability Maturity Model®, SSE-CMM® Model Description Document, Version 3.0*, www.sei.cmu.edu, June 15, 2003.
- 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) USA CERT, www.uscert.org, 2005.
- 112) Van Wyk K. R., Graff G.M., *Survey and Analysis of Related Standards* webmaster@securecoding.org. 2003.
- 113) Wendy B., Moshel B., *UML i Rational Rose 2002*, Kompjuter biblioteka, Beograd, 2005.
- 114) Williams R. J., Ferraiolo K. M., *P³I – Protection Profile Process Improvement*, Arca Systems, Inc., <http://www.arcasystems.com>, 2003.
- 115) 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.
- 116) Zadjura J., *An Introduction to Certification and Accreditation v. 1.4*, SANS Institute, <http://www.sans.org>, 2003.
- 117) Zahran Dr S., *Software Process Improvement*, Addison-Wesley, NY, 2005.
- 118) 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.

Pravila SE razmišljanja

Ako sistem inženjeri ne primenjuju strogo SE discipline u razvoju i upravljanju proizvodnjom, problemi se ne uočavaju u inicijalnoj fazi, ali se javljaju kada organizacija pokušava da razvije i implementira akcioni plan. **Sistemska razmišljanje** je okvir za razumevanje međuzavisnosti i ponovljivosti, sposobnost uočavanja obrasca promena, disciplina koja obezbeđuje viđenje celine sistema, umesto statičkih i izolovanih objekata sistema. Sistemska razmišljanje je značajno za uspešan razvoj proizvoda i poboljšavanje procesa, a polazi od toga da je važna međuzavisnost objekata sistema, koji se odnose na opštu namenu sistema. Može se reći da je sistemska razmišljanje *peta* disciplina za učenje organizacije pored četiri tradicionalne: (1) upravljanje ljudskim resursima, (2) mentalni model opšteg tržišta i konkurentskog odnosa, (3) opšta vizija za budućnost organizacije i (4) osposobljavanje timskog rada.

U koncept sistem inženjerskog razmišljanja ugrađena su sledeća iskustva:

- kratkoročna poboljšavanja često dovode do dugoročnih problema,
- laka rešenja mogu biti nikakva rešenja uopšte,
- brza rešenja, posebno na nivou simptoma, često dovode do većih problema,
- uzroci i posledice nisu nužno blisko povezani ni u vremenu ni u prostoru, pa rešenja implementirana lako i na brzinu mogu imati negativan uticaj znatno kasnije,
- ceo sistem, uključujući organizaciju i njeno okruženje moraju se razmatrati zajedno.

Pravila sistenskog razmišljanja primenjiva na svakodnevne poslove mogu se sabrati u sledeća:

1. U svim fazama projekta i u toku životnog ciklusa sistema sistem inženjeri moraju uzeti u obzir (razvoj zahteva):
 - viziju, ciljeve i zadatke organizacije,
 - zahteve i želje korisnika,
 - problem i potrebe korisnika koje sistem treba da reši.
2. Treba sagledati celinu, kao i interakciju između elemenata sistema. Iterativno i rekurzivno razmišljanje mora zemeniti tradicionalno linearno razmišljanje (razvoj zahteva i tehnička rešenje);
3. Člнови projekta uvek treba da traže sinergiju i relativnu prednost koju daje integracija podsistema (n.p.r. sistema zaštite) u sistem (tehnička rešenja i integracija proizvoda);
4. Rešenja uvek nisu inženjerska pa treba uzeti u obzir:
 - poslovne i ekonomske troškove,
 - višekratno korišćenje proizvoda i razvijene infrastrukture,
 - organizacione, upravljačke, političke i personalne faktore.
 - Sistem inženjeri treba da razmatraju sistem sa što je više moguće različitih aspekata.
5. Sistem inženjeri i menadžeri projekta uvek treba da uzmu u obzir razvoj zahteva i tehničkih rešenja:
 - analizu električnih rešenja,
 - analizu mehaničkih rešenja,
 - analizu uticaja okruženja,
 - analizu garancije kvaliteta (quality assurance),
 - analizu kvalitativnih faktora kao što su pouzdanost, isplativost, mogućnost održivanja i testiranja.
6. Planiranje logističkih zahteva treba evaluirati tako da zadovoljavaju sve faze razvoja sistema uključujući za razvoj zahteva i tehničkih rešenja:

- rezervne delove,
 - infrastrukturu za podršku,
 - logističku podršku,
 - servise,
 - nivo održavanja,
 - tehničku dokumentaciju.
7. Kada se pojavi potreba za modifikacijom sistema, uvek treba uzeti u obzir (razvoj zahteva-tehnička rešenja-upravljanje zahtevima):
 - inženjerske i neinženjerske implikacije,
 - efekti forme, adekvatnosti i funkcija,
 - odgovore sistema na promene,
 - potrebe, teškoće i stav onih koji moraju pratiti modifikaciju (korisnička prihvatljivost promena).
 8. Svaki problem mora imati više od jednog mogućeg izvođačkog (radnog) rešenja (tehnička rešenja):
 - sve moguće alternative treba ispitati i uporediti jednu prema drugoj sa kvantitativnom ili kvalitativnom metrikom,
 - u svakoj fazi treba razmatrati isplativost i tehničko ekonomsku analizu rentabiliteta (troškovi-efektivnost).
 9. Sistem inženjeri treba da podstiču i traže promene koje uvode značajna poboljšavanja sa minimalnim naporima.
 10. Procesi koji daju slabe i postepene rezultate treba ozbiljno uzeti u razmatranje (razvoj i inovacije organizacije).
 11. Poznata rešenja nisu uvek pogodna za rešavanje tekućeg problema. Svako raspoloživo rešenje treba razmatrati zajedno sa rizikom, zavisnostima i ograničenjima koja su inherentna za sistem u razvoju (treba da postane generička praksa).
 12. Rizik razvoja mora se uzeti u obzir kroz ceo ciklus razvoja proizvoda (planiranje projekta-upravljanje rizikom).
 13. Nemoguće je voditi projekat bez upravljanja, kontrole projekta i kontrole konfiguracije:
 - kontrola,
 - upravljanje konfiguracijom,
 - kontrolne tačke (milestone),
 - upravljanje,
 - metodi planiranja vremena (planiranje projekta).
 14. Krajnji korisnik se mora smatrati glavnim delom sistema (razvoj zahteva i planiranje projekta).
 15. Sistem inženjersko razmišljanje zahteva integraciju ekspertskih znanja i veština iz više disciplina i ispitivanje sa više aspekata, tražeći timski rad za pokrivanje ovih perspektiva (upravljanje integrisanim projektom, razvoj integrisanog procesa i proizvoda i integrisani tim).
 16. Izbor partnera i podgovarača je kritičan faktor. Ne treba ulaziti u partnerstvo sve dok partner nije spreman da deli jednako rizik, uspeh i profit (upravljanje sporazumom sa snabdevačem).
 17. Ograničite odgovornosti pripisane spoljnim faktorima, pošto one povećavaju zavisnost od njih (sporazum sa snabdevačima-komercijalno kupljen softve).
 18. Kod izbora komponenti za proizvodnju treba uzeti u obzir vreme koje proizvod ima od trenutka proizvodnje do nabavke.
 19. Sistem inženjersko razmišljanje uključuje i verovatnoću i statistiku kada se definiše specifikacija sistema, određuju ciljevi projekta, troškovi i performanse (analiza odluka i rešenja).

Kriterijumi i uzorci za definisanje i opis procesa

1. Kriterijumi za definisanje procesa: pitanja i dogovori za sastavne komponente

1. *Ulazni kriterijumi aktivnosti*

P: Kada ova aktivnost može početi?

Opiši uslove pod kojim aktivnost može startovati.

O: Upisati stanje aktivnosti.

Primeri: Odobrena izjava o radu, definisane odgovornosti za kreiranje *Plana projekta*,
odobren *Plan testiranja*.

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 među-proizvodi rada koriste za ulaz u ovu aktivnost?

*Ulaz je međuveza ili link između date aktivnosti i njenog rezultata rada. Ulazi su
proizvodi rada-rezultati prethodnih aktivnosti, koje opisivana aktivnost koristi.*

O: Ime rezultatnog proizvoda rada.

Primeri: izjava o izvršenom radu, odobrena alokacija zahteva.

4. *Izlaz aktivnosti*

P: Šta su rezultati ili proizvodi rada proizvedeni sa ovom aktivnosti?

*Izlaz je međuveza ili link između date aktivnosti i njenog rezultata rada. Izlazi su rezultati
proizvedeni sa opisivanom aktivnosti.*

O: Ime rezultatnog proizvoda rada.

Primeri: deo programskog koda, procedura testa, specifikacija projekta (dizajna),
odobrena *Izjava o izvršenom radu*.

5. *Izvršioci aktivnosti*

P: Ko izvršava ovu aktivnost?

*Ovo je međuveza ili link između date aktivnosti i izvršioca te aktivnosti. To je
organizaciona jedinica, uloga-zaposleni, 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 i.t.d.

6. Sledeća aktivnost

P: Koja je sledeća aktivnost?

Tok aktivnosti je uslovna međuveza ili link između dve aktivnosti. Tok aktivnosti definiše redosled izvršavanja aktivnosti i generalno zavisi od izlaznih kriterijuma.

O: Proizvedeni rezultat.

Primeri: finalni proizvod rada aktivnost, ili među-proizvod koji vodi u sledeću aktivnost.

2. Uzorci za definisanje i opis procesa i procedura

2.1. Uzorak opisa procesa: kratka verzija

Proces: Upravljanje bezbednosnim zahtevima	
Akcija	Odgovornost
Dobijanje radnog zahteva od kupca	Stariji menadžer (SM), Menadžer projekta (PM)
Revizija radnog zahteva	PM
Izrada inicijalnog plana budžeta/procene rada/potrebnog vremena	PM
Inicijalno planiranje	PM, projektni tim (PT)
Zahtevi na konceptualnom nivou	PM, PT, kupac
Identifikovanje faktora rizika i dokumentovanje	PM
Nacrt specifikacije zahteva	PM, PT
Tehnička revizija	PM, PT, predstavnik sistema kvaliteta (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
Odobranje i potpisivanje	Kupac, QA, PM, SM, EPG
Osnovna specifikacija zahteva	PM, CCB, EPG
Procena, praćenje i unošenje promena	PM, CCB, QA, EPG, kupac, PT

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

Engineering Process Group (EPG) – SE tim za implementaciju

Senior Management (SM) - Stariji menadžer

2.2. Uzorak opisa procesa: duga verzija

Proces: Upravljanje zahtevima

Sadržaj

1. Uvod
 - 1.1. Namena
 - 1.2. Obim
 - 1.3. Upravljanje promenama
 - 1.4. Uloge i odgovornosti
2. 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 kriteriumi/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. Uključenost (angažovanost) glavnog menadžmenta
 - 2.3.4.2. Uključenost projekt menadžera (PM)
 - 2.3.4.3. Uključenost predstavnika sistema kvaliteta (QA)
 - 2.3.4.4. Revizija proizvoda
 - 2.3.4.5. Revizija menadžmenta
 - 2.3.4.6. Revizija kupaca
3. Resursi i finansiranje
4. Merenja
5. Obuka
6. Referentna dokumenta
7. Izmena istorije (iskustvenih podataka)

2.3. Uzorak: *opis procedure*

Templejt procedure	
R. broj 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	

Templejt procedure	
R. broj dokumenta:	Datum:
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	
Nastavak...	

Stabilnost i poboljšavanje stabilnosti procesa zaštite

1. Korisnički zahtevi za stabilnost procesa zaštite

Iskustva iz prakse zaštite ključni su ulazni parametri za poboljšavanje procesa zaštite. Ipak, praksa je potvrdila da mnogi procesi zaštite ne proizvode očekivane rezultate i pored primene solidne metodologije. Drugim rečima, procesi zahtevaju stalni nadzor i poboljšavanje. Samo neprekidno poboljšavan proces može postati zreo i ponovljiv, odnosno, stabilan. U oblasti zaštite IKT sistema, da bi proces bio stabilan zahteva se ispunjavanje i održavanje najmanje tri osnovna atributa: *produktivnost, adaptivnost i korisničku prihvatljivost* procesa, [68], [85]:

Zahtevi za stabilan proces	PRODUKTIVNOST: (efektivnost) procesa zahteva da dizajn procesa mora rezultirati sa visokim nivoom produktivnosti.
	ADAPTIVNOST: zahteva da je proces sposoban da se prilagodi promenama okruženja, odnosno da dizajn procesa mora ugraditi zahteve za fleksibilnost i skalabilnost.
	KORISNIČKA PRIHVATLJIVOST: podrazumeva da dizajn procesa mora zadovoljiti zahteve krajnjih korisnika i da proces bude u skladu sa kulturom organizacije

1.1. Produktivnost

Produktivnost ili efektivnost procesa je najkritičniji elemenat procesa i ako proces ne ispuni očekivane rezultate smatra se neuspešnim (neizvršenim). Uzroci smanjenja produktivnosti procesa mogu biti različiti, ali se mogu svrstati u četiri opše 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 i ako ne obezbeđuje optimalan odgovor za smanjenje ukupnog rizika. Drugim rečima, od male je koristi implementirati ekstremno ambiciozne kontrole zaštite u jednoj oblasti, ako se ostave ranjivosti u drugim oblastima.

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. Nerealna očekivanja zaposlenih, koja premašuju kapacitete tima za administraciju korisničkih naloga, dovode do blokiranja servisa zbog nemogućnosti pravovremenog rešavanja svih zahteva. U ovim uslovima zaposleni mogu kontaktirati administratora za zaštitu/sistem, koji troši svoje vreme da reši njihove zahteve i dalje degradira isti servis.

3. Neefikasni kontrolni mehanizmi. Kontrolni mehanizmi mogu brzo zastariti i postati neefikasni, ako se regularno ne nadgledaju (nadziru). Na primer, digitalno potpisan e-mail ne dodaje novu vrednost dokumentu, sve dok ovlašćena strana u transakciji ne verifikuje potpis.

4. Slabo dizajniran tok procesa zaštite i neodgovarajuće pripisivanje odgovornosti često je uzrok problema u procesima zaštite. Na primer, često se u praksi greši kada se nekom menadžeru organizacije pripiše odgovornost za odobravanje zahteva za bezbednosno relevantne promene

konfiguracije sistema, a poznato je da oni retko redovno i na vreme izvršavaju taktičke i operativne zadatke.

Poboljšavanje produktivnosti: Produktivnost procesa može se definisati kao mera u kojoj se očekivani izlaz može postići sa fiksnim skupom resursa. Što je veća produktivnost, proizvodi se veći izlazni rezultat. Glavni faktori koji utiču na produktivnost procesa su **efektivnost, efikasnost i ponovljivost**, što se može izraziti sa, [68], [85]:

P (produktivnost) = f (Efektivnost, Efikasnost, Ponovljivost)

Gde **P = f(x)** označava da **P** zavisi od **x**, a ne predstavlja preciznu matematičku 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. Poboljšavanjem proizvodnog ciklusa (smanjenjem perioda ponavljanja) smanjuje se kašnjenje između prijema ulaznih parametara i proizvodnje izlaznih rezultata.

Sva tri atributa stabilnosti procesa međuzavisna su. Na primer, nema smisla tvrditi da je neki proces efikasan, a da nije efektivan.

Poboljšavanje efektivnosti procesa je sinonim za uklanjanje svake aktivnosti koja ne dodaje vrednost datom procesu. Striktno govoreći, ovo 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, otvoreno je pitanje koji se nivo dokumentacije i opisa procesa zahteva za smanjenje rizika na optimalan način. Slično je i sa definisanjem sastavnih komponenti sistema zaštite, ili procenom nivoa osposobljenosti u zaštiti.

Što se tiče dokumentacije procesa zaštite, treba koristiti formalizovane opise procedura kao pomoćnu dokumentaciju i njih održavati ažurnim. To podrazumeva da svaki put za svaku promenu ne treba raditi novu dokumentaciju za dati proces zaštite.

Pre implementacije specifičnih kontrola zaštite za smanjenje rizika treba razmotriti sve opcije. Ako su procedure kontrole skupe prihvatljiva opcija je da se rizik prihvati ili prenese na poverljivog provajdera zaštite (TTPS – *Trusted Third Party Service*), [15].

Prvi korak u poboljšavanju efektivnosti postojećih procedura zaštite je da se proverí da li se rizik smanjuje na odgovarajući način i na prihvatljivi nivo.

Organizacije mogu implementirati program/sistem zaštite na osnovu, [68], [85]:

- politike zaštite i/ili
- najbolje prakse zaštite i/ili
- analize tekućeg rizika.

Organizacije koje implementiraju program/sistem zaštite na osnovu politike ili najbolje prakse zaštite, mogu poboljšavati efektivnost procedura na opisani način. Međutim, implementacija najbolje prakse zaštite nije uvek **optimalna**, jer je najbolja praksa namenjena za najviši nivo zaštite i implementaciju maksimalnih kontrola zaštite za neku tipičnu organizaciju i ne mora biti adekvatna za konkretni kontekst date organizacije. Većina korisnika želi rešenje zaštite sa što manjim troškovima, što postaje mera optimalnosti programa/sistema zaštite, [79].

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 dizajniranju procesa. Primeri organizacionih metoda za povećavanje efikasnosti procesa zaštite su:

- postavljanje realističkih bezbednosnih ciljeva,
- praćenje korisničkih očekivanja,
- određivanje prioriteta poboljšavanja,
- smanjenje zavisnosti od skupa specifičnih veština i
- određivanje adekvatnosti pripisanih odgovornosti.

Postavljanje realističkih ciljeva i postizanje sporazuma o nivou servisa zaštite (*SLA-Security Level Agreement*), [88], u slučaju korišćenja usluga TTPS provajdera zaštite, [88], sa korisnicima, poboljšava efikasnost eliminisanjem nepotrebnog praćenja ponašanja krajnjih korisnika. Umesto toga administratori mogu posvetiti više vremena ključnom procesu, a manje vremena za rad sa nezadovoljnim korisnicima. Kada se definišu ciljevi i uspostave nivoi servisa zaštite, tada ima smisla planirati akcije za ekstremne situacije, kao što je privremeno odsustvo nekoliko administratora u isto vreme. Jedan način rešavanja ovog problema je određivanje prioriteta za izvršavanje aktivnosti i definisanje bezbednog načina rada (*safe mod*), koji usmerava na izvršavanje najvažnijih servisa. *SLA* treba da obezbedi pod kojim se uslovima ovaj mod rada uvodi i kako se uvodi. Određivanje prioriteta za izvršavanje procedura koje sadrži proces, pomaže da se obezbedi optimalno korišćenje raspoloživih resursa. Zato je određivanje prioriteta - tehnika organizacionog poboljšavanja, pošto se odnosi na interaktivni rad ljudi na izvršavanju procedura. Korišćenje resursa nije u pitanju u normalnim uslovima rada, ali postaje važno pitanje u uslovima povećanog obima aktivnosti, ili kada nema dovoljno resursa. Na isti način unutar procedura moguće je odrediti prioritete za izvršavanja aktivnosti. Na primer, u uslovima velike potražnje obično pomaže da se prioritetnije izvršavaju zahtevi za proizvodnjom umesto razvojem.

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 korišćenjem različitih alata za dobijanje istih ili boljih rezultata. Ovo se uglavnom postiže automatizovanjem manuelnih procesa i može se koristiti za značajno povećanje efikasnosti 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 skraćuje vreme potrebno da se izvrše aktivnosti - počnu i završe. Zato je poboljšavanje ciklusa ekvivalentno bržem izvršavanju procedure i predstavlja povećanje produktivnosti. Ovo poboljšavanje posebno je važno u proizvodnoj industriji gde duži ciklusi isporuke dovode do nezadovoljstva kupaca, povećanja troškova i.t.d. U sistemu zaštite smanjenje ciklusa procedure najvažniji je instrument za povećanje zadovoljstva korisnika. Ovo ne važi samo za rutinske administrativne procese nego i za procese za razvoj i nabavku operativnog i zaštitnog softvera.

Ako proceduru smatramo sekvencijalnim izvršavanjem bazičnih praksi (aktivnosti, zadataka), možemo poboljšavati vreme ciklusa, uklanjanjem praksi koje ne povećavaju vrednost, bržim izvršavanjem praksi, ili smanjenjem kašnjenja između zadataka. Prvi faktor je diskutovan u povećanju efikasnosti procesa. Povećavanje brzine izvršavanja može se postići automatizacijom, ili povećavanjem resursa čime se, međutim, povećavaju proizvodni troškovi.

1.2. Adaptivnost procesa

Adaptivnost je značajan atribut procesa zaštite, koji se izvršavaju u uslovima brojnih promena okruženja (pretnji, tehnologija i dr.) sa sledećim posledicama:

- dizajn procesa reflektuje specifične, a ne generičke zahteve;
- nedovoljno se koriste uloge i odgovornosti u izvršavanju procesa zaštite;
- nedovoljno se obraća pažnja na kompenzujuće (univerzalne) kontrole zaštite, koje se mogu koristiti za kompenzaciju ranjivosti bilo gde u sistemu zaštite (n.p.r., antivirusni program);
- ne ugrađuju se potencijalni (realno očekivani) novi zahtevi u dizajn procesa, koji obezbeđuju elemente *proaktivne* zaštite.

Iako većina procedura kontrola zaštite odgovara generičkim zahtevima, u praksi se često dobro uklapaju u realni kontekst. Tipičan primer je zahtev za procedure za kontrolu vanrednog događaja, koji se mogu pojaviti za određenu aplikaciju. Takođe, ako su procedure dizajnirane za specifičan sistem, malo je verovatno da će imati koristi od kompenzacionih kontrola razvijenih na drugom mestu u arhitekturi sistema zaštite.

Procedure koje koriste koncept uloga fleksibilnije su od onih koje reflektuju organizacionu strukturu. Ovo je važno za veće organizacije gde su promene česte. Dizajniranje procedura i kontrola zaštite za individualni IKT sistem, ne uzimajući u obzir arhitekturu, značajno redukuje mogućnost korišćenja kompenzacionih kontrola zaštite.

Poboljšavanje adaptivnosti procesa: Adaptivost procesa je sposobnost procesa da se prilagođava promenama okruženja –pretnji, tehnologija, zahteva. Sposobnost adaptacije procesa određuju njegova *fleksibilnost* i *skalabilnost*. Fleksibilnost je sposobnost asimilacije novih funkcionalnih zahteva, a skalabilnost - sposobnost da proces može prihvatiti povećan obim zahteva, [68], [85]:

Adaptivnost = f(fleksibilnost, skalabilnost)

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. Dalje, kontrola toka između procedura treba da bude što je moguće više standardizovana, što uključuje minimizaciju izuzetnih slučajeva koje treba rešavati. U IKT sistemu proceduralne korake koji se oslanjaju na funkcionalnost posebnih sistema treba zameniti 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 logova i upravljanje ranjivostima, potencijalno treba izvršavati na stotinama i više platformi.

Važne tehnike za upravljanje skalabilnosti su određivanje prioriteta izvršavanja i isporuke rezultata i upravljanje gradacijom. Obe ove tehnike obezbeđuju skalabilnost po nekoj ceni. U prvom slučaju, skalabilnije procedure koncentrišu se na one rezultate koji najviše dodaju novu vrednost. ***Na 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 rizika za više sistema po cenu ignorisanja ranjivosti od faktora *niskog* uticaja rizika, [85], [107].

Slična argumentacija primenjuje se kada se menja granulacija kontrolnih mera sa ciljem povećavanja skalabilnosti. Mehanizmi za kontrolu pristupa klasični su primer u ovoj oblasti. Održavanjem granularnih prava pristupa za milione datoteka i stotine zaposlenih jasno da nije lako izvodljivo. Zbog toga se i korisnici koji pristupaju objektima IKT sistema i objekti kojima

korisnici pristupaju, u većini sistema svrastavaju 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 izvršavanje stvarne kontrole 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.

1.3. Korisnička prihvatljivost

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. Procesi koji ne uzimaju u obzir zahteve učesnika u komunikaciji, izvršioca i korisnika verovatno će biti brzo zapostavljeni i odbačeni.

Dizajn procesa sa aspekta korisničke prihvatljivosti uključuje sledeće relevantne faktore:

1. Kompleksnost: Smanjenje kompleksnosti IKT sistema i sistema zaštite, dovodi do boljeg razumevanja, a razumevanjem problema zaštite - isti se bolje rešavaju.

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, na primer, administriranje barijera (*firewalls*). Korisnici mogu postići razumevanje sintakse i semantike složenijih procesa, ali za razumevanje normalnog ponašanja tih procesa, kao i za upravljanje rizikom za te procese zahtevaju se ekspertski znanja.

3. Psihološka prihvatljivost: Osnovni psihološki problem je što rutinski zadaci, kao što su brojne procedure zaštite, teško motivišu korisnike da ih korektno i konzistentno izvršavaju.

Poboljšavanje korisničke prihvatljivosti: Na korisničku prihvatljivost utiče niz različitih faktora, uključujući mnoge već spomenute. **Na primer,** zaposleni verovatno neće biti motivisani da učestvuju u procesu koji je očigledno neefikasan i mogu biti frustrirani kada su procesi neefektivni. Na korisničko prihvatanje procedura jako utiču kulturološka iskustva, nivo razumevanja i psihološki faktori, [68], [85].

Korisnička prihvatljivost = f(kulturološki uticaj, kompleksnost, psihološki uticaj)

Kulturološki uticaj poznato je da ima glavni uticaj na korisničku prihvatljivost promena svake vrste. Primeri ovog fenomena su brojna propala udruživanja organizacija zbog nemogućnosti prevazilaženja kulturoloških razlika.

Moćna tehnika za uvođenje značajnijih promena je ona koja dopušta da zaposleni sami vode proces promena. Osnovna ideja je da se onima koji izvršavaju tekuću proceduru obezbedi pomoć u identifikovanju zahteva 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. 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 izvršavanja procedura i da izbegnu drastične promene.

Smanjenje kompleksnosti je važno za poboljšavanje procesa u dve odvojene oblasti:

- dizajniranju samog procesa i
- načinu komunikacije postavljenih ciljeva i samog dizajna procesa zaposlenim.

Naime, nije teško shvatiti zašto se već 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 dizajna procesa. U praksi, kod određivanja kompleksnosti odlični rezultati postižu se sledeći zdravu logiku. Na primer, broj tačaka odlučivanja u proceduri dobra je indikacija kompleksnosti – više tačaka znači veću kompleksnost.

Nažalost čak i kada su procesi dobro dizajnirani, savremena tehnika za zaštitu informacija nije lako razumljiva za neupućene, a eksperti zaštite koriste složeni rečnik za opisivanje problema i rešenja u zaštiti. Deo problema kompleksnosti je i način na koji se informacije prenose korisnicima. Izbegavanje stručnih izraza i održavanje kratke, konkretne i jasne dokumentacije mnogo doprinose smanjenju kompleksnosti same dokumentacije zaštite. Jednostavni alati kao što su dijagrami toka i ček liste mnogo pomažu u ovoj oblasti, posebno kada ih prate objašnjenja i primeri koji su poznati prosečnim korisnicima.

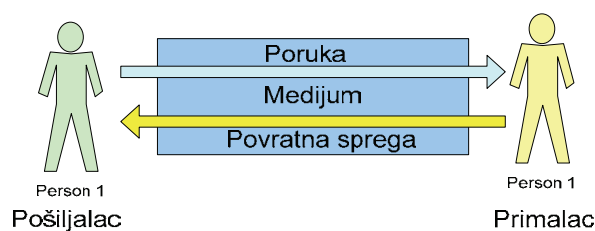
Uticaj psiholoških faktora određuje meru u kojoj se ljudi vežu za dobijene zadatke. Psihološki faktori su brojni, uključujući sposobnost ljudi za izvršavanje zadataka i meru u kojoj zadatke smatraju interesantnim. Ako je sposobnost izvršavanja zadataka nekog pojedinca znatno iznad ili ispod zahtevanog nivoa, motivacija će verovatno opasti. U prvom slučaju nedostatak motivacije nastaje zbog stalnih neuspeha da se postigne zahtevani standard izvršavanja procesa, a u poslednjem slučaju zbog nedostatka izazova za izvršavanje tog procesa. Aktivno upravljanje radnim zadacima obezbeđuje da zaposleni dobiju zadatke koji su u opsegu njihovih 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 planira obuka i obrazovanje u zaštiti. Korisna tehnika je i rotiranje uloga članova tima za izvršavanje zadataka.

U svakom pristupu poboljšavanju procesa od posebnog značaja je kvalitetana, uspešno završena dvosmerna komunikacija svih učesnika u procesu. Svaka kompletirana (uspešno završena) komunikacija ima određene osnovne komponente.

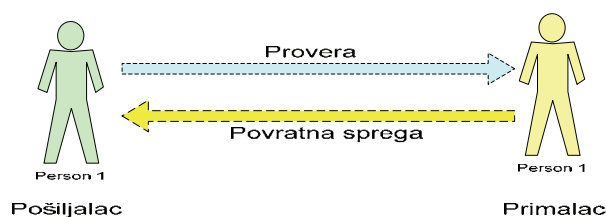
1.4. Osnovne komponente komunikacije

Kompletirana komunikacija uključuje zatvorenu petlju koja sadrži nekoliko ključnih elemenata. Osnovni elementi su **pošiljalac, poruka, prenosni medijum (ili medij), primaoc i povratna veza** (Sl.1). Ako bilo koji od ovih elemenata nije efektivan, nije potpuna komunikacija i prenose se samo fragmenti podataka.



Sl. 1. Zatvorena petlja komunikacije

Pre, za vreme i ponekad umesto prenosa formalne poruke, pošiljalac i primalac se angažuju u interakciji koja uspostavlja pripremnu fazu (proveru) za razmenu glavnih poruka (Sl. 2).



Sl. 2. Interakcija za razmenu poruka

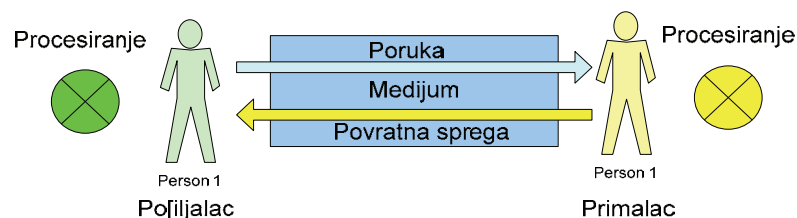
Provera može uključivati kontakt očima, neki ritual kao što je rukovanje, tehničku aktivnost kao što je mašinsko rukovanje (tipa *Kerberos* autentifikacionog protokola, modema, faks mašina, telefonske konekcije i.t.d.). Iako se u društvenom kontekstu ova interakcija smatra prenosom poruka, ona to nije, 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 potrebe za efikasnošću, kreiranjem kontrolnih tragova, minimizacijom distorzija, ili nekog drugog kriterijuma. Može postojati i neopipljiv razlog, pošto izbor medija može stvoriti percepciju o kritičnosti poruka, tačnosti i relevantnosti, odnosno kreirati elemente poruka. Izbor medija treba da se izvrši kada pošiljalac uspostavi nameru komunikacije i treba uzeti 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 (šifruje) beznačajne ili pogreške informacije.

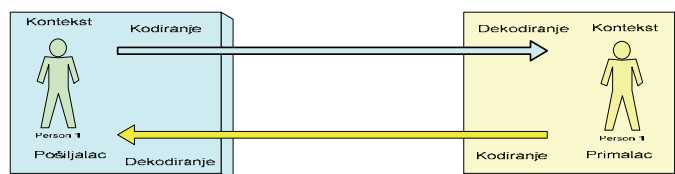
Za netrivialne transakcije, pošiljalac ne može pretpostavljati da je poslata poruka adekvatna za dostizanje željenog odredišta. Poruke često uključuju zahteve za potvrdu o prijemu ili druge odgovore primaoca. Uloga primaoca uključuje dekodiranje (interpretaciju) poruke i neku formu procesiranja. Mnogo puta, 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 enkodira i prenosi odgovor pošiljaocu. Kada originalni primalac dekodira i procesira odgovor, komunikaciona petlja je kompletirana (Sl. 3). 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.



Sl. 3. Kompletirana komunikaciona petlja

Aktivnosti komunikacione petlje događaju se u *kontekstu*, koji često nije isti za primaoca i pošiljaoca (Sl. 4). Na primer, mnogi nesporazumi potiču u toku interakcije pojedinca sa različitim nivoa odgovornosti, a drugi između ljudi različitih specijalnosti. Ove grupe imaju različite kontekste (kompetencije i referentne okvire) koji mogu izazvati stvarne komunikacijske probleme.



Sl. 4. 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, različiteih procesa, jezika, nacionalnosti i religija.

Takođe, savremeni termin „upravljanje znanjem“ stvara pogrešnu koncepciju da znanje može biti lako uskladišteno i prenošeno. Često mislimo da prenosimo znanje, a ustvari, prenosimo podatke, zato što se pravo znanje ili značenje nalazi među ljudima, a ne u rečima ili slikama koje koristimo u komunikaciji. Dakle, oni koji iniciraju komunikaciju moraju razumeti kompletnu komunikacionu petlju i 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 odnosna 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 opsega, mogu uticati i drugi faktori, kao što su rukovanje modema, kašljanje, kontakt očima, glasovne poruke, e-mail i sl.. Za uspešnu komunikaciju poruke i povratna sprega moraju stizati nepromenjeni. Zato nastojimo da minimiziramo distorzije u mediju i učesnicima. Kod elektronskih poruka proverava se integritet podataka. U govornoj komunikaciji možemo pitati da li nas sagovornig čuje, ili tražiti da se poruka ponovi. Rizik od distorzije poruka raste kada se poruke prenose posrdno, 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 konfliktnan. 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.

Kratak opis OP i BP u SSE CMM v.3.0 modelu

Oblast inženjerskih (SSE) procesa

OP 01- Administriranje kontrola zaštite

Cilj: Kontrole zaštite su propisno konfigurisane i korišćene.

Kratak opis: Namena ove OP je da obezbedi da je namenjen i planiran nivo zaštite u fazi razvoja i projektovanja postignut u operativnom radu sistema.

BP 01.01. Uspostaviti odgovornosti i kontrolisane odgovornosti

BP 01.02. Upravlјati konfiguracijom kontrola sistema zaštite

BP 01.03 Upravlјati svešću o potrebi zaštite

BP 01.04. Upravlјati servisima i kontrolnim mehanizmima zaštite

OP 02-Procena uticaja (faktora rizika)

Cilj: Identifikovan i okarakterisan bezbednosni uticaj faktora rizika na sistem.

Kratak opis: Namena ove OP je da identifikuje relevantne bezbednosne uticaje na sistem i da proceni verovatnoću tih uticaja. Uticaji mogu biti opipljivi (materijalni), kao što je gubitak imovine ili finansijski gubitak, ili neopipljivi, kao što su gubitak ugleda ili poverenja klijenata. *BP 02.01 Identifikovati, analizirati i odrediti prioritete operacija, poslova ili kapaciteta misije koje podržava informacioni sistem*

BP 02.02 Identifikovati i okarakterisati objekte (imovinu) sistema koji podržavaju ključne operativne kapacitete, ili bezbednosne ciljeve sistema

BP 02.03 Izabrati metriku uticaja koju treba koristiti za ovu procenu

BP 02.04 Identifikovati međusobne odnose između izabranih metrika za ovu procenu i metrike za konverziju faktora ako se zahteva

BP 02.05 Identifikovati i okarakterisati uticaje

BP 02.06 Monitorisati tekuće promene uticaja.

OP 03 – Procena bezbednosnog rizika

Cilj: Razumeti bezbednosni rizik koji prati rad sistema u definisanom okruženju.

Kratak opis: Namena ove OP je da identifikuje faktore bezbednosnog rizika za sistem u definisanom okruženju. OP je usmerena na procenu faktora rizika, na bazi procena ranjivosti kapaciteta i imovine na potencijalne pretnje. Specifično ove aktivnosti uključuju identifikovanje i procenu verovatnoće da će neka *pretnja iskoristiti identifikovanu ranjivost (tzv. izloženosti)*. Izloženost se odnosi na kombinaciju prtnji, ranjivosti i uticaja koji može izazvati značajne štete u sistemu i organizaciji. Ovaj skup aktivnosti može se izvršavati u bilo koje vreme u životnom ciklusu sistema u cilju podrške razvoja, održavanja ili funkcionisanja sistema u poznatom okruženju.

BP 03.01 Izabrati metode, tehnike i kriterijume sa kojima se analizira, procenjuje i upoređuje bezbednosni rizik za sistem u definisanom okruženju

BP 03.02 Identifikovati izloženost (pretnja/ranjivost/uticaj).

BP 03.03 Proceniti rizik pridružen verovatnoći događanja neke pretnje (iskoristivosti).

BP 03.04 Proceniti ukupnu neodređenost rizika za izloženosti sistema

BP 03.05 Poređati faktore rizika po prioritetu značaja i uticaja.

BP 03.06 Monitorisati tekuće promene faktora rizika i njihovih karakteristika

OP 04 – Procena pretnji

Cilj: Identifikovane ranjivosti sistema i određeno njihovo potencijalno iskorišćenje.

Kratak opis: Namena ove OP je da identifikuje kombinovane bezbednosne pretnje, njihova svojstva i karakteristike.

BP 04.01 Identifikovati primenljive pretnje koje potiču iz prirodnih izvora

BP04.02 Identifikovati primenljive slučajne i namerne pretnje koje potiču od humanih/veštačkih izvora

BP 04.03 Identifikovati odgovarajuće jedinice merenja i primenljive opsege u specifikovanom okruženju

BP 04.04 Proceniti kapacitet i motivaciju agenata pretnji za pretnje koje potiču iz humanih/veštačkih izvora

BP 04.05 Proceniti verovatnoću pojave događaja pretnje

BP 04.06 Monitorisati tekuepromene faktora pretnji (rizika) i njihovih promena

OP 05- Procena ranjivosti sistema

Cilj: Razumeti ranjivosti sistema zaštite.

Kratak opis: Namena ove OP je da identifikuje i okarakterise bezbednosne ranjivosti sistema. OP uključuje analizu objekata (imovine) sistema, definišući speifične ranjivosti svakog objekta i obezbeđujući procenu ukupne ranjivosti sistema. Termini koji se koriste u proceni rizika i ranjivosti koriste se različito u različitim kontekstima. U ovom modelu *ranjivost* se odnosi na aspekte sistema koje neka potencijalna pretnja može iskoristiti za namenu koja nije predviđena, kao što su propusti u dizajnu, bezbednosne rupe, ili greške u implementaciji sistema. Ove ranjivosti su nezavisne od bilo kojeg određenog slučaja pretnje ili napada. Ovaj skup aktivnosti može se izvršavati u bilo koje vreme u životnom ciklusu sistema u cilju podrške razvoja, održavanja ili funkcionisanja sistema u poznatom okruženju.

BP 05.01 Izabрати metod, tehnike i kriterijume.

BP 05.02 Identifikovati ranjivosti sistema zaštite.

BP 05.03 Sakupiti podatke o svojstvima ranjivostima.

BP 05.04 Proceniti ranjivosti sistema i agregirati specifične ranjivosti

BP 05.05 Monitorisati tekuće promene u primenljivim ranjivostima

OP 06 – Izgradnja dokaza za bezbednosnu garanciju (garantovanu bezbednost)

Cilj: Obezbeđeno da procesi generišu dokaze da su zadovoljene bezbednosne potrebe organizacije

Kratak opis: Namena ove OP je da jasno prenese da su bezbednosne potrebe korisnika ispunjene. Argument bezbednosne garancije je skup navedenih ciljeva bezbednosne garancije koje podržava kombinacija dokaza garantovene bezbednosti, deriviranih iz brojnih izvora i nivoa apstrakcije. Ovaj proces uključuje identifikovanje i definisanje zahteva za garantovanu bezbednost; aktivnosti za proizvodnju i analizu dokaza i dodatnih aktivnosti potrebnih za dokazivanje zahteva bezbednosne garancije. Osim toga, dokazi sakupljeni u ovim aktivnostima sakupljaju se, pakuju i pripremaju za prezentaciju.

BP 06.01 Identifikovati ciljeve bezbednosne garancije

BP 06.02 Definisati strategiju ostvarivanja bezbednosne garancije za ispunjavanje ciljeva bezbednosne garancije

BP 06.03 Identifikovati i kontrolisati dokaze bezbednosne garancije

BP 06.04 Izvršiti analizu dokaza bezbednosne garancije

BP 06.05 Obezbediti argumente za bezbednosnu garanciju koji pokazuju da su ispunjeni zahtevi korisnika za bezbednosnu garanciju

OP 07 – Koordinacija zaštite

Cilj:

- Postignuta svest o potrebi i uključivanju svih članova projektnog tima u aktivnosti SSE programa zaštite do mere potrebne za izvršavanje dodeljenih funkcija.
- Sve odluke i preporuke koje se odnose na program zaštite prenesene su svim učesnicima i koordinirane.

Kratak opis: Namena ove OP je da obezbedi da su svi učesnici svesni i angažovano uključeni u SSE aktivnosti. Ove aktivnosti su kritične zato što se SSE aktivnosti ne mogu izolovano uspešno izvršavati. Ova koordinacija uključuje održavanje otvorene komunikacije između svih učesnika projekta i spoljnih grupa. Različiti mehanizmi, uključujući memorandume, dokumenta, e-mails, sastanke i radne grupe, mogu se koristiti za koordinaciju i komunikaciju SSE odluka i preporuka ovih učesnika.

BP 07.01. Definirati ciljeve koordinacije i međusobne odnose SSE procesa

BP 07.02. Identifikovati mehanizme za koordinaciju SSE procesa

BP 07.03. Obezbediti što lakšu koordinaciju SSE procesa

BP 07.04. Koristiti identifikovani mehanizam za koordinaciju odluka i preporuka koje se odnose na zaštitu

OP 08 – Nadzor i kontrola sistema zaštite

Cilj:

- Detektovani i praćeni interni i eksterni bezbednosno relevantni događaji.
- Odgovori na incidente u skladu sa politikom zaštite.
- Identifikovane i upravljane promene operativnog bezbednosnog okruženja u skladu sa politikom zaštite.

Kratak opis: Namena ove OP je da osigura da su identifikovani i javljeni svi proboji, pokušaji proboja ili greške koje mogu potencijalno dovesti do proboja sistema zaštite. Monitoriše se interno i eksterno okruženje sistema na sve faktore koji mogu uticati na bezbednost sistema.

BP 08.01. Analizirati evidenciju o događaju radi određivanja uzroka događaja, načina odvijanja i verovatnoće ponavljanja

BP 08.02. Monitorisati promene pretnji, ranjivosti, uticaja, rizika i okruženja

BP 08.03. Identifikovati bezbednosno relevantne incidente

BP 08.04 Monitorisati performanse i funkcionalnu efektivnost kontrola sistema zaštite

BP 08.05. Revidirati sistem zaštite i identifikovati neophodne promene

BP 08.06. Upravljanje odgovorom na bezbednosno relevantne incidente

BP 08.07 Obezbediti adekvatnu zaštitu artefakta koji se odnose na monitoring sistema zaštite

OP 09– Obezbeđivanje bezbednosnih ulaza

Cilj:

- Pregledane, analizirane i razrešene bezbednosne implikacije svih aspekte sistema u skladu sa bezbednosnim ciljevima.

- Obezbeđena adekvatna znanja i razumevanja zaštite svih članova projektnog tima, tako da mogu izvršavati svoje funkcije.
- Rešenja reflektuju obezbeđene bezbednosne ulaze.

Kratak opis: Namena ove OP je da obezbedi arhitekta sistema, projektante, implementatore, ili korisnike sa bezbednosnim informacijama koje su im potrebne. Ove informacije uključuju arhitekturu sistema zaštite, projekat ili alternativna rešenja implementacije zaštite i uputstva zaštite. Bezbednosne ulaze razvijaju, analiziraju, obezbeđuju i koordinišu odgovarajući članovi organizacije, na bazi bezbednosnih potreba koje su identifikovane u OP 10 – *Specifikacija bezbednosnih potreba*.

BP 09.01 Raditi sa dizajnerima, implementatorima i korisnicima radi obezbeđenja razumevanja potreba za bezbednosnim ulazom.

BP 09.02 Odrediti bezbednosna ograničenja i razmatranja koja su potrebna za kvalitetan inženjerski izbor.

BP 09.03 Identifikovati alternativna rešenja za inženjerske probleme zaštite.

BP 09.04 Analizirati i odrediti prioritete inženjerskih alternativa koristeći bezbednosna ograničenja i razmatranja.

BP 09.05 Obezbediti instrukcije koje se odnose na bezbednost sistema za druge inženjerske grupe.

BP 09.06 Obezbediti uputstva koja se odnose na zaštitu za operativne korisnike sistema i administratore.

OP 10 – Specifikacija bezbednosnih potreba

Cilj: Svi učesnici na koje se odnosi, uključujući i korisnike, postigli opšte razumevanje bezbednosnih potreba.

Kratak opis: Namena ove OP je da eksplicitno identifikuje potrebe koje se odnose na bezbednost sistema. OP uključuje definisanje osnovne konfiguracije zaštite sistema (*security baseline*) da bi se zadovoljili svi legalni zahtevi, zahtevi politike zaštite i organizacijski bezbednosni zahtevi. Ove se potrebe prilagođavaju, na bazi realnog operativnog bezbednosnog konteksta sistema, tekućeg sistema zaštite i okruženja organizacije i identifikovan je skup bezbednosnih ciljeva. Definisan je skup bezbednosnih zahteva za sistem, koji postaje osnovna konfiguracija sistema zaštite, nakon akreditacije vlasnika sistema.

BP 10.01 Razumeti sve bezbednosne potrebe kupaca

BP 10.02 Identifikovati zakone, politike, standarde, spoljne uticaje i ograničenja koja su okvir za upravljanje sistemom.

BP 10.03 Identifikovati namenu i bezbednosno okruženje (kontekst) sistema.

BP 10.04 Definirati koncept sistema zaštite.

BP 10.05 Identifikovati opšte bezbednosne ciljeve koji definišu bezbednost sistema.

BP 10.06 Definirati konzistentan skup izjava (politika) koje definišu zaštitu koju treba implementirati u sistem.

BP 10.07 Obezbediti sporazum da specifikovani bezbednosni zahtevi ispunjavaju potrebe korisnika.

OP 11 – Verifikacija i validacija (akreditacija i sertifikacija) sistema zaštite

Cilj:

- Obezbeđeno da rešenja zaštite zadovoljavaju bezbednosne zahteve.
- Obezbeđeno da rešenja zaštite zadovoljavaju operativne bezbednosne potrebe korisnika.

Kratak opis: Namena ove OP je da obezbedi verifikaciju i validaciju rešenja zaštite u odnosu na bezbednosne aspekte. Rešenja se verifikuju prema bezbednosnim zahtevima, arhitekturi i dizajnu, na osnovu opservacija, demonstracije, analize i testiranja. Rešenja se vrednuju prema operativnim bezbednosnim potrebama i zahtevima korisnika.

BP 11.01 Identifikovati rešenja zaštite koja treba verifikovati i vrednovati.

BP 11.02 Definirati pristup i nivo rigoroznosti za verifikaciju i validaciju svakog rešenja zaštite.

BP 11.03 Verifikovati rešenje koje implementira prethodne zahteve za zaštitu

BP 11.04 Vrednovati rešenje pokazujući da zadovoljava prethodne potrebe korisnika i ispunjava operativne bezbednosne ciljeve korisnika.

BP 11.05 Evidentirati rezultate verifikacije i validacije za druge inženjerske grupe

Oblasti procesa za upravljanje projektom

OP. 12: Osiguranje kvaliteta

Cilj:

- Definisan i izmerin proces kontrole kvaliteta.
- Postignut očekivani kvalitet rezultata procesa.

Kratak opis: Namena ove OP je da obuhvati ne samo kvalitet sistema nego i procesa koji se koriste za generisanje sistema i stepen u kome projekat sledi definisani proces. Osnovni koncept ove OP je da se visoko-kvalitetan sistem može konzistentno izgraditi samo ako postoji neki proces koji neprekidno meri i poboljšava kvalitet. Osim toga taj se proces mora izvršavati u svim fazama životnog ciklusa sistema. Ključni aspekti procesa koji se zahtevaju za razvoj visoko-kvalitetnih sistema su merenje, analiza i korektivne akcije.

BP12.01 Identifikovati zahteve za kvalitet za svaki proizvod rada.

BP 12.02 Obezbediti da definisani SSE proces odgovara za sve faze ž/c sistema

BP 12.03 Evaluirati kvalitet proizvoda rada prema zahtevima za kvalitetom proizvoda rada.

BP 12.04 Meriti kvalitet SSE procesa korišćenih u projektu zaštite.

BP 12.05 Analizirati merenja kvaliteta radi razvoja preporuka za poboljšavanje kvaliteta ili korektivne akcije, ako odgovara.

BP 12.06 Obezbediti učešće zaposlenih u identifikovanju i izveštavanju pitanja značajnih za kontrolu kvaliteta sistema zaštite.

BP 12.07 Inicirati aktivnosti koje obuhvataju identifikovana pitanja kvaliteta ili mogućnosti poboljšavanja

BP 12.08 Uspostaviti mehanizam ili skup mehanizama za detekciju potreba za korektivnim akcijama procesa ili proizvoda zaštite.

OP.13. Upravljanje konfiguracijom

Cilj: Kontrolisano održavanje konfiguracije sistema

Opis: Namena aktivnosti upravljanja konfiguracijom je da se održavaju podaci o statusu identifikovanih jedinica konfiguracije i za analizu i kontrolu promena sistema i njegovih jedinica konfiguracije. Upravljanje konfiguracijom sistema uključuje obezbeđenje preciznih podataka o tekućoj konfiguraciji i statusu projekatata i korisnika. Ova OP je primenjiva na sve radne procese koji se mogu obuhvatiti sa upravljanjem konfiguracije. Primer elemenata koji obuhvaćenih upravljanjem konfiguracijom su hardver i softver, projektni principi, zahtevi, datoteke podataka o proizvodima ili studija o trgovini.

BP 13.01 Odlučiti i izabrati odgovarajući metod za upravljanje konfiguracijom.

BP 13.02 Identifikovati nedeljive jedinice za upravljanje konfiguracijom.

BP 13.03 Održavati repozitorijum osnovne konfiguracije proizvoda rada (baseline).

BP 13.04 Kontrolisati promene, radi uspostavljanja jedinica konfiguracije.

BP 13.05 Komunicirati (preneti) odnosnim grupama status podataka o konfiguraciji, predložene promene i pristupne informacije.

OP. 14: Upravljanje rizikom projekta

Cilj: Identifikovani, shvaćeni i ublaženi faktori rizika projekta za implementaciju programa zaštite.

Bezbednosna razmatranja: Ova OP se odnosi na faktore rizika uspešnog kompletiranja SSE projekta zaštite, obuhvatajući pitanja koja se odnose na troškove i vremenski plan. Inženjerske OP (OP02, OP03, OP04 i OP05) obuhvataju aktivnosti za procenu i ublažavanje **bezbednosnog rizika**, određujući da li je operativni uticaj preostalog bezbednosnog rizika prihvatljiv. Rezultati aktivnosti za procenu i ublažavanje bezbednosnog rizika mogu obezbediti ulaz i uticati na aktivnosti upravljanja projektnim rizikom. Da se obezbedi obuhvatanje bezbednosnog rizika treba uzeti u obzir OP07 – *Koordinacija sistema zaštite*.

Kratak opis: Namena ove OP je da identifikuje, proceni, monitoriše i ublaži faktore rizika za uspešno postizanje SSE procesa i ukupnih tehničkih napora. Ova OP se odnosi na i odvija neprekidno u toku svih faza životnog ciklusa sistema. Slično kao OP16 i OP15, ova OP obuhvata i SSE aktivnosti i ukupne tehničke napore na projektu, pošto se SSE aktivnosti u projektu ne mogu smatrati uspešnim, ako nisu uspešni ukupni tehnički napori.

BP 14.01 Razviti plan za aktivnosti upravljanja rizikom koji je osnova za identifikovanje, procenu, ublažavanje i monitorisanje rizika za životni ciklus projekta.

BP 14.02 Identifikovati faktore rizika projekta na osnovu ispitivanja ciljeva projekta u odnosu na alternativna rešenja i ograničenja i identifikovati šta sve može krenuti pogrešnim putem.

BP 14.03 Proceniti faktore rizika i odrediti verovatnoću događanja i posledice realizacije.

BP 14.04 Obezbediti formalnu prihvatljivost procene rizika projekta.

BP 14.05 Implementirati aktivnosti za ublažavanje rizika.

BP 14.06 Monitorisati aktivnosti za ublažavanje rizika, radi obezbeđivanja željenih rezultata.

OP 15. Kontrola i nadzor tehničkih aktivnosti

Cilj: Kontrolisane i neprekidno monitorisane tehničke aktivnosti.

Kratak opis: Namena ove OP je da se obezbedi adekvatna vidljivost aktuelnog progressa i rizika. Neprekidan nadzor obezbeđuje preduzimanje blagovremenih korektivnih akcija kada izvršavanje procesa odstupa značajno od planiranih. Tehnički procesi uključuju usmeravanje, praćenje i reviziju rezultata i postignutog stanja projekta, tehničkih aktivnosti, rizika u odnosu na procenjeni preostali rizik, statusa komunikacija i planova revizije.

BP 15.01 Usmeriti tehničke napore u skladu sa planom upravljanja tehničkim rešenjima.

BP 15.02 Pratiti aktuelno korišćenje resursa prema planu upravljanja tehničkim rešenjima.

BP 15.03 Pratiti performanse prema uspostavljenim tehničkim parametrima.

BP 15.04 Pregledati i revidirati performanse prema planovima za upravljanje tehničkim rešenjima.

BP 15.05 Analizirati pitanja koja su rezultat praćenja i revizije tehničkih parametara za određivanje korektivnih akcija.

BP 15.06 Preduzimati korektivne akcije kada aktuelni rezultati odstupaju od planova.

OP 16: Planiranje tehničkih aktivnosti

Cilj: Planirani svi aspekti tehničkih aktivnosti za realizaciju procesa.

Kratak opis: Namena ovog procesa je uspostavljanje plana za obezbeđivanje vremenskog rasporeda izvršavanja aktivnosti, praćenje i pregovaranje o prirodi i obimu tehničkih aktivnosti uključenih u sve faze životnog ciklusa - razvoj sistema, funkcionisanje, održavanje i odlaganje. Aktivnosti SSE moraju biti integrisane u kompleksni plan tehničkih poslova za celokupni projekat. Planiranje tehničkih poslova uključuje procenu rada kojeg treba izvršiti u fazi razvoja, obezbeđivanjem neophodnog angažovanja radnih timova i definisanjem plana za izvršavanje tog rada.

BP 16.01 Identifikovati resurse kritične za uspeh tehničkog projekta

BP 16.02 Proceniti (evaluirati) faktore koji utiču na nivo i tehničku izvodljivost projekta.

BP 16.03 Proceniti troškove za sve tehničke resurse koje projekat zahteva.

BP 16.04 Odrediti tehnički proces koji će biti korišćen u projektu.

BP 16.05 Identifikovati tehničke aktivnosti za ceo životni ciklus projekta.

BP 16.06 Definirati specifične procese za efektivnu interakciju sa korisnicima i snabdevačima.

BP 16.07 Razviti plan tehničkih aktivnosti za ce ž/c projekta.

BP 16.08 Ustanoviti tehničke parametre sa granicama za projekat i sistem.

BP 16.09 Koristiti informacije sakupljene u fazi planiranja, razvoja plana upravljanja tehničkim projektom, koji služi kao baza za praćenje ostalih aspekata projekta i SSE napora.

BP 16.10 Revidirati plan upravljanja tehničkim projektom sa svim odnosnim grupama i pojedincima i obezbediti angažovanje.

Oblast organizacionih procesa

OP 17: Definisanje (inženjerskih) SSE procesa organizacije

Cilj: Definirani standardni SSE procesi organizacije.

Kratak opis: Namena je kreiranje i upravljanje standardnim SSE procesima organizacije, koji mogu sukcesivno biti kreirani u projektu da bi se formirali jedinstveni procesi koji će pratiti razvoj sistema/proizvoda. Definisanje SSE procesa organizacije uključuje definisanje, razvoj i dokumentovanje objekata (imovine) SSE procesa. Objekti SSE procesa uključuju fragmente procesa, dokumentaciju koja se odnosi na procese, arhitekturu procesa, pravila i alate za izradu procesa i merenje procesa.

BP 17.01 Uspostavi ciljeve za SSE proces organizacije na bazi poslovnih ciljeva organizacije.

BP 17.02 Sakupiti i održavati imovinu SSE procesa organizacije.

BP 17.03 Razviti dobro definisan standardni SSE proces organizacije.

BP 17.04 Definirati uputstva za prilagođavanje standardnih SSE procesa za primenu u projektu za razvoj projektom definisanog procesa.

OP 18: Poboljšavanje (tehničkih, inženjerskih) SSE procesa organizacije

Cilj: Planirano i implementirano poboljšavanje SSE procesa do standardnih i stabilnih procesa.

Kratak opis: Namena ove OP je dobijanje komparativne prednosti kontinualnim poboljšavanjem efektivnosti i efikasnosti standardnih SSE procesa koje organizacija koristi. Uključuje razvoj i razumevanje procesa organizacije u kontekstu poslovnih ciljeva organizacije, analizu izvršavanja procesa i eksplicitno planiranje i poboljšavanje ovih procesa.

BP 18.01 Evaluirati postojeće procese koji se izvršavaju u organizaciji, radi shvatanja njihove snage i slabosti.

BP 18.02 Planirati poboljšavanja procesa organizacije na bazi analize uticaja potencijalnog poboljšavanja na postizanje ciljeva procesa.

BP 18.03 Promeniti standardni SE proces organizacije da odražava ciljno poboljšavanje.

BP 18.04 Komunicirati (preneti) poboljšavanje procesa na postojeći projekat i druge odnosne grupe ako je prikladno.

OA 19: Upravljanje razvojem proizvodne linije

Cilj: Proizvodne linije se razvijaju u pravcu postavljenih ciljeva.

Kratak opis: Namena ove OP je uvođenje servisa, opreme i novih tehnologija da bi se postigla optimalna dobit u razvoju procesa proizvoda/sistema, troškovima, vremenu i izvršavanju u toku planiranog vremena, kako se i proizvodna linija razvija u pravcu konačnih ciljeva. Organizacija prvo mora odrediti razvoj proizvoda, zatim treba da odluči kako će projektovati i izraditi ove proizvode, uključujući kritične komponente, rentabilne alate i efikasne i efektivne procese.

BP 19.01 Definirati tipove proizvoda koje treba ponuditi.

BP 19.02 Identifikovati nove proizvodne tehnologije ili infrastrukturu koja omogućava ili pomaže organizaciji da nabavi, razvije i primeni tehnologiju za komparativnu prednost.

BP 19.03 Izvršiti neophodne promene u ciklusu razvoja proizvoda radi podrške razvoja novih proizvoda

BP 19.04 Obezbediti da su na raspolaganju kritične komponente za podršku planiranog razvoja proizvoda

BP 19.05 Uvesti novu tehnologiju u razvoj proizvoda, marketing i proizvodnju.

OA 20: Upravljanje proizvodnim okruženjem za podršku SSE procesa

Cilj: Obezbeđena podrška SSE procesa za maksimalnu efektivnost procesa.

Kratak opis: Namena ove OP je da se obezbedi proizvodno, tehnološko okruženje za podršku SSE procesa, neophodno za razvoj proizvoda/sistema i izvršavanje procesa zaštite. Razvojni i tehnološki procesi uvode se u okruženje sa ciljem minimizacije prekida razvojnih aktivnosti, dok se vrši nadgradnja sa novom tehnologijom. Tehnološke potrebe organizacije se tokom vremena menjaju, a naponi opisani u ovim oblastima procesa moraju po potrebi biti obnavljani.

BP 20.01 Održavati svest o tehnologijama koje podržavaju ciljeve organizacije.

BP 20.02 Odrediti potrebe za proizvodnim okruženjem za podršku SSE procesa organizacije, na bazi potreba organizacije.

BP 20.03 Obezbediti proizvodno okruženje za podršku SSE procesa koje ispunjava zahteve uspostavljene u BP – Odredi potrebe za podršku SSE procesa.

BP 20.04 Prilagoditi proizvodno okruženje za podršku SSE procesa individualnim potrebama projekta

BP 20.05 Uvesti nove tehnologije u proizvodno okruženje za podršku SSE procesa na bazi poslovnih ciljeva i projektnih potreba.

BP 20.06 Održavati proizvodno okruženje za neprekidnu podršku SSE procesa projekata koji od njega zavise

BP 20.07 Monitorisati okruženje za podršku SSE procesa radi potencijalnog poboljšavanja.

OP 21: Obezbeđivanje tekućih znanja i sposobnosti kadrova

Cilj: Organizacija ima neophodne veštine i znanja da postigne projektne i organizacione ciljeve.

Kratki opis: Namena procesa je da se obezbedi da projektni tim ima neophodna projektna (inženjerska) i organizaciona znanja i sposobnosti za postizanje ciljeva projekta i organizacije. Da bi se obezbedila efektivna aplikacija ovih kritičkih resursa koji su predominantno zavisni samo od

ljudi, zahteva se identifikacija znanja i sposobnosti organizacije, kao i specifičnih projektnih ili organizacionih potreba (n.p.r., koje se odnose na nove programe i tehnologije, nove proizvode, procese i politike). Neophodna znanja i sposobnosti mogu se obezbediti sa obukom u organizaciji i sa resursima izvan organizacije. Akvizicija iz spoljnih izvora može uključiti resurse korisnika, privremeno iznajmljivanje, konsultante i proizvođače. Znanje se može obezbediti i angažovanjem eksperata za predmetnu oblast.

BP 21.01 Identifikovati potrebe za poboljšavanjem veština i znanja u celoj organizaciji, koristeći potrebe projekta, strateški plan organizacije i postojeće veštine i instrukcije zaposlenih.

BP 21.02 Evaluirati i izabrati odgovarajući način za obezbeđivanje znanja i veština u odnosu na obuku i druge izvore.

BP 21.03 Obezbediti da su odgovarajuće veštine i znanja na raspolaganju za SSE aktivnosti.

BP 21.04 Prepremiti materijal za obuku na bazi identifikovanih potreba za obuku.

BP 21.05 Obučiti personal tako da imaju veštine i znanja potrebna za izvršavanje svojih pripisanih uloga.

BP 21.06 Proceniti efektivnost obuke za postizanje identifikovanih potreba za obukom.

BP 21.07 Održavati evidenciju o obuci i iskustvima.

BP 21.08 Održavati materijal za obuku u pristupačnom repozitorijumu.

OA 22: Koordinacija bezbednosnih aspekata sa snabdevačima/prodavcima

Cilj: Izabrati i koristiti efektivne snabdevače.

Kratak opis: Namena procesa je da se obuhvate potrebe organizacije za efektivno upravljanje delovima proizvodnog rada koje organizacija obavlja sa spoljnim snabdevačima. Generalno pojam snabdevača se odnosi na identifikovanje organizacija koje razvijaju, proizvode, testiraju, daju logističku podršku i.t.d. nekoj komponenti sistema primarne organizacije, koja zahteva snabdevanje proizvoda/usluga. Snabdevač može biti prodavac (*vendor*) opreme, podizvođač radova, partner i.t.d. Uspešnost odnosa organizacije i snabdevača zavisi od kapaciteta obe organizacije i kvaliteta međusobne komunikacije i razumevanja odnosa i očekivanja.

BP 22.01 Identifikovati potrebne komponente sistema ili servisa koji se moraju obezbediti od strane druge/spoljne organizacije.

BP 22.02 Identifikovati snabdevače koji su pokazali stručnost u identifikovanim oblastima

BP 22.03 Izabrati snabdevače u skladu sa definisanim procesom.

BP 22.04 Obezbediti snabdevače sa adekvatnim potrebama, očekivanjima i merama efektivnosti koje organizacija treba da izvrši za komponente sistema ili servise koje treba isporučiti.

BP 22.05 Održavati blagovremeno dvosmernu komunikaciju sa snabdevačem.

SSE CMM v.3.0 model: *Pregled oblasti kapaciteta*

CL	Atributi
1	Izvršavane neformalno
2	Planirane i praćene
3	Dobro definisan
4	Kvantitativno kontrolisan
5	Kontinualno poboljšavan

CL	CF (Zajedničke karakteristike)
1	1.1. BP se izvršavaju
2	2.1. Planiranje performansi 2.2. Disciplinovanje performansi 2.3. Verifikovanje performansi 2.4. Praćenje performansi
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 performansama OP
5	5.1. Poboljšavanje kapaciteta organizacije 5.2. Poboljšavanje efektivnosti procesa

CF (Zajedničke karakteristike)	GP (Generičke prakse)
1.Nivo zrelosti	
1.1 – BP se izvršavaju	1.1.1 – Izvrši proces
2.Nivo zrelosti	
2.1 - Planiranje performansi	2.1.1 – Alociraj resurse 2.1.2 – Pripisi 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 – Upravlja 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
3.Nivo zrelosti	
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

CF (Zajedničke karakteristike)	GP (Generičke prakse)
3.3 - Koordinacija procesa	3.3.1 – Koordinacija unutar grupe 3.3.2 – Koordinacija između grupa 3.3.3 – Koordinacija sa spoljnim grupama
4.Nivo zrelosti	
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
5.Nivo zrelosti	
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

Primer *UPITNIKA* za SSAM evaluaciju

OP 09 - Obezbeđivanje bezbednosnog ulaza

1.CL: 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.				

2. CL: Planiran i praćen

Da li oni koji izvršavaju BP-e *OP Administriranje kontrola zaštite* takođe izvršavaju neku od sledećih funkcija? Za svako pitanje 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				

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
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?				

3. CL: 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 svako pitanje 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?				

4.CL: Kvantitativno kontrolisan

Da li je sledeće vidljivo ili na raspolaganju onima koji koriste procese *Administriranja kontrola zaštite* organizacije? Za svako pitanje sa pozitivnim odgovorom navedite 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?				

5.CL: Kontinualno poboljšavan

Da li su sledeće karakteristike vidljive u procesima *OP Administriranje kontrola zaštite* organizacije? Za svako pitanje 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				

Generička praksa (GP)	DA	NE	Ne znam	DOKAZ
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?				

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 *Intervijua* i daje ukupnu sliku prakse sistema zaštite organizacije. TE **analizira** DTS i dokazuje 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 Excel Tabeli ima 4 glavne sekcije (T. 1):

1. OPs
2. Odgovori na pitanja (iz pripremne i faze rada na terenu)
3. Odgovori na intervijue (iz 1 ili više projekata-3)
4. Prihvatanje dokaza (sa konsenzusom TE)

OP	Odgovori na upitnik						Odgovori intervijua			Prihvatanje dokaza	Konačno rangiranje
	Pripremna faza/ faza na terenu						Faza rada na terenu(P6)				
	01	02	03	01	02	03	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											
....											

T. 1. Uzorak DTS

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 preliminarne 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 **odgovore** 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 6) upisuju se u kolonama **P1.1-P1.6; P2.1-P2.6; P3.1-P3.6** po pojedinačnim projektima (3).

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 $\geq 50\%$ 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 inetrvjua** (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 alfanumeričkim 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 **dokazae** 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:

1. **Za BPs i GPs** gde se obezbeđeni dokazi smatraju **dovoljnim** za odgovarajuće dokazivanje, u odgovarajuću ćeliju koja potvrđuje usaglašenost unosi se identifikator: „**1**“
2. **Za BPs i GPs** gde se smatra da su obezbeđeni dokazi **nedovoljni** ili **nema** dokaza upisuje se identifikator: „**0**“.
3. **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.
4. **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.

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 prosledene 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: _____

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.

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 č	1.03.2006 u 12.30 č	1.04.2006 u 2.30 č

Tabela za praćenje korišćenja dokaza: Popunjava je član SSAM tima za korišćenje svakog pojedinačnog dokaza.

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 odlaganja dokaza: U ovu Tabelu unose se podaci o odlaganju dokaza i privremenih proizvoda rada SSAM tima.

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			

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 (samo evaluacija i samo poboljšavanje procesa)
- Organizaciona jedinica za evaluaciju (CA PKI *Univerziteta Singidunum*)
- 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 inženjerskih bezbednosnih 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:

- ni jedan projekat ili pojedinac ne mogu biti imenovani u nalazima,
- TE ne može diskutovati ili komentarisati proces evaluacije izvan samog procesa,
- TE ne može prenositi drugi licima informacije koje čuju u procesu evaluacije (odgovori na pitanja i intervju)

Dinamički plan

U skladu sa dinamičkim planom, planirati vreme održavanja:

- Uvodnog sastanka,
- Prikupljanja odgovora na *Upitnik*,
- Intervjuisanja rukovodstva projekta za uspostavljanje CA ESS,
- Intervjuisanja praktičara,
- Prezentacije nalaza Sponzoru.

Pravila prezentacije nalaza

- Ni jedan medij za prezentaciju nalaza ne može se izneti iz zgrade ESS,
- Upravljanje sa podacima sakupljenim u procesu evaluacije odobrava Sponzor,
- Svi učsnici u procesu evaluacije treba da rade prema NDA sporazumu.

Dnevni red sastanka za prezentaciju nalaza:

- Informacije o procesu evaluacije (cilj, značaj učešća članova evaluirane organizacije,...),
- Profil rangiranja procesa
- Nalazi,
- 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 evalaucije - 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 odgovornosti u zaštiti? PR: Dokument zaštite koji opisuje kontrolisane odgovornosti u zaštiti? PR: Dokument zaštite koji opisuje autorizacije u zaštiti?	
		01.02.	Upravlja 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.	Upravlja 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 edukaciji?	
		01.04.	Upravlja servisima i kontrolnim mehanizmima zaštite. PR: Održavanje administrativnog loga? PR: Periodično održavanje i pregledi administracije zaštite? PR: Greške u administriranju i održavanju? PR: Izzužeca u administraciji i održavanju? PR: Liste osetljivosti informacija? PR: Liste o osetljivosti medija? PR: Evidencija o saniranju, deklasifikaciji i odlaganju medija?	

Tabela 1. Osnovne karakteristike klasa SCAMPI metoda evaluacije

Atributi	Klasa A	Klasa B	Klasa C
Način upotrebe	rigorozno i detaljno ispitivanje procesa, osnova za aktivnosti poboljšanja	inicijalna evaluacija, inkrementalna (delimična) samo-evaluacija	brz uvid, inkrementalna evaluacija
Prednosti	potpuno pokrivanje snage i slabosti svake evaluirane OP; robusnost metoda sa konzistentnim i ponovljivim rrezultatima; obezbeđuje objektivan uvid; kompatibilan sa 15504.	organizacija ima uvid u sopstvene kapacitete, obezbeđuje startnu poziciju ili fokus na oblast koja zahteva najveću pažnju, promoviše prihvatanje metoda	jeftina, kratko traje, brz odziv
Nedostaci	zahteva značajne resurse	ne ističe dubinu pokrivanja i rigirozne primene ne može se koristiti za rangiranje nivoa	manje prihvatanje metoda i rezultata evaluacije; nije dovoljno detaljna za finu korekciju plana poboljšanja procesa
Sponzor	glavni menadžer organizacione jedinice	svaki menadžer	svaki interni menadžer
Sastav TE	spoljni ili unutrašnji	spoljni ili unutrašnji	spoljni ili unutrašnji
Veličina TE	4-10 lica + lider TE	1-6 lica+ lider TE	1-2 lica+ lider TE
Kvalifikacije TE	iskusni	umereno iskusni	umereno iskusan
Zahtevi za lidera TE	vodeći evaluator	vodeći evaluator, ili lice iskusno u primeni metoda	lice obučeno za primenu metoda

Tabela 2. *Procene relevantnih učesnika za SCAMPI intervjuisanje*

Uloga	Procenjen broj intervjua	Sati po intervjuu	Broj intervjuisanih po intervjuu	Procejeno ukupno sati
Menadžer projekta	4	2	1	8
Grupa za merenje (pretpostavlja odvojenu grupu)	2	1,5	4	12
Grupa srednjih menadžera	2	2	4	16
Grupa za obuku	1	2	3	6
Podnosioci zahteva	1	2	4	8
Predstavnici razvoja	1	2	4	8
Grupa za testiranje	1	2	4	8
Grupa za integraciju	1	2	4	8
Grupa za poboljšavanje procesa (posebna)	1	2	4	16
Grupa za kontrolu kvaliteta	2	2	4	16
Grupa snabdevača	1	2	4	8
Grpa za alate	1	2	3	6
Ukupno procenjeno	18	28	43	120

Primer SCAMPI PIID prema CMMI v. 1.2 modelu procesa

Ovaj **radni dokument** obezbeđuje početnu poziciju za identifikovanje **direktnih** i **indirektnih** dokaza za svaki SG i SP u modelu. Važno je razumeti da su ovi proizvodi rada rezultati izvršavanja praksi i procesa definisanih u projektu/organiaciji i izabranih za evaluaciju. U ovom **Radnom dokumentu** za svaku SG i SP dati su primeri **direktnih** i **indirektnih** dokaza. Svaki TE sakuplja, konsoliduje i priprema specifične direktne i indirektne dokaze koji se zahtevaju za neku evaluaciju. U nekom slučaju nekoliko dokaza može postojati u jednom dokumentu i obrnuto. Ključni kriterijum za izbor dokaza je da ga generiše evaluirani proces i da zadovoljava potrebe organizacije. Drugim rečima dokazi moraju objektivno odražavati SG i SP evaluiranih procesa.

Primer direktnih i indirektnih artefakta SCAMPI v.1.2 metoda evalaucije za OP: CAR (Analiza uzroka i rešavanje problema)

OP	SG	SP	Pitanje: Postoje li direktni (DE) i indirektni (ID) dokazi	DA/NE
CAR		Kauzalna analiza i rešavanje problema		
	1	Odrediti uzroke defekata: Koreni uzroka defekata i drugih problema su sistematično određeni		
		1.1.	Izbor podataka o defektima za analizu: Izaberi defekte i druge probleme za analizu DE: Podaci i problemi o defektima izabrani za dalju analizu? DE: Izveštaji krajnjih kupaca, koisknika o defektima? DE: Izveštaji otkriveni revizijom i testiranjem? ID: Dnevni red sa sastanka o selekciji defektnih podataka?	
	.	1.2.	Analiza uzroka: Izvrši kauzalnu analizu izabranih defekata i drugih problema i predloži akcije za otklanjanje. DE: Rezltati analize defekata? DE: Rezultati analize problema? DE: Predlozi korektivnih akcija? ID: Dnevni red sastanka o analizi defektnih podataka ili problema? ID: Status predloga za korektivne akcije?	
	2	Otkloniti uzroke defekata: Koren uzroka i drugih problema sistematski su tertirani da se spreči njihov budući uticaj.		
		2.1.	Implementacija predloga akcija: Implementiraj izabrane akcija iz predloga razvijenih u kauzalnoj analizi. DE: Lista predloga korektivnih akcija izabranih za implementaciju? DE: Kompletirane (izvršene) korektivne akcije? DE: Lista predloga za poboljšavanje? DE: Opis implementacije akcija? ID: Dnevni red sastanaka o selekciji akcija? ID: Agende o reviziji korektivniha akcija ili odobrenjima te revizije?	
		2.2.	Evaluacija efekata promena: Evaluacija efekata promena u performansama procesa. DE: Merenja performansi i promena u performansama? DE: Merenja efektivnosti korektivnih akcija? ID: Rezultati procene efektivnosti korigovanih procesa? ID: Zapisnik o ažuriranju razvoja procesa ili druge evidencije?	
		2.3.	Evidencija podataka: Evidentiraj podatke analize i rešenja za upotrebu u projektima i organizaciji DE: Zapisnici ili izveštaji o kauzalnoj analizi? ID: Dnevni red sastanka o registrovanju rezultata analize? ID: Odobrenje za poboljšavanje procesa?	

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 sve glavne objekte i operacije. - Odobren Plan zaštite obuhvata politiku zaštite, upravljanje rizikom, procenu pretnji/ranjivosti, pregled kontrola zaštite, pravila ponašanja, kontrolu pristupa i nadzor i kontrolu sistema zaštite. - Plan zaštite identifikuje ko je vlasnik IKT objekata i ko je odgovoran za upravljanje objektima.	
b. Uspostavljanje strukture za upravljanje zaštitom. - Formiran „centralni entitet za upravljanje programom zaštite“. - Program zaštite sadrži ovlašćeno, nezavisno i stručno telo za upravljanje zaštitom. - Glavni rukovodilac zaštite imenovan je na najvišem nivou i ima odgovarajuću subordinaciju.	
c. Definisanje odgovornosti za zaštitu. Definisane su i jasno pripisane odgovornosti za zaštitu i očekivano ponašanje za: (1) vlasnike IKT objekata i korisnike, (2) upravnu strukturu IKT objekata i osoblje za procesiranje, (3) najvišu upravnu strukturu i (4) administratore i specijaliste 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 zaštite sadrži kriterijume u suštini iste kao i za CL 1, razlika je samo u kompletnosti kriterijuma za CL 2.

Kriterijumi za CL 2	Da/Ne
a. Dokument Programa zaštite. - Sadrži detaljan i odobren Plan zaštite, koji pokriva sve glavne objekte i operacije organizacije, - Plan obuhvata Politiku zaštite, Upravljanje rizikom, pregled kontrola zaštite, pravila ponašanja, upravljanje životnim ciklusom, autorizaciju procesa, personalnu i fizičku zaštitu, hw/sw podršku, plan za vanredne događaje i incidente, dokumentaciju, obuku, odgovore, kontrolu pristupa i audit - Plan zaštite identifikuje ko je vlasnik IKT objekata i ko je odgovoran za upravljanje objektima.	
b. Uspostavljanje strukture za upravljanja zaštitom. - Generalno formira se „centralni entitet za upravljanje programom zaštite“, - Program zaštite sadrži ovlašćeno, nezavisno i stručno telo za upravljanje zaštitom. - Glavni rukovodilac zaštite imenovan je na najvišem nivou i ima odgovarajuću subordinaciju.	
c. Definisanje odgovornosti. Pripisane su kontrolisane odgovornosti za zaštitu i očekivano ponašanje za: vlasnike IKT objekata i korisnike, upravnu strukturu IKT objekata i osoblje za procesiranje, najvišu upravnu strukturu i administratore i specijaliste zaštite.	
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 upravne strukture, savremen i obuhvata sve sisteme za opštu podršku i glavne aplikacije organizacije.	

CL3: Implementiran, dobro definisan program zaštite obuhvata formalne procedure za implementaciju koje promovišu ponovljivost realizacije programa zaštite i obezbeđuju osnovu za jasnu, preciznu i potpuno razumljivu implementaciju programa zaštite. Program (ili deo) zaštite organizacije smatra se da je na CL 3 ako, pored zadovoljavanja svih kriterijuma sa CL 2, sadrži pisane procedure zaštite i ispunjava sledeće kriterijume.

Kriterijumi za 3. nivo	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 u sistemu i aplikacijama svim korisnicima na koje se odnosi. - Od korisnika se zahteva da periodično potpisuju izjavu kojom potvrđuju svoju svest o potrebi i prihvatanje odgovornosti za zaštitu.	
b. Revizija i kontrola zaštite. - Rutinski koristi automatske alate za monitorisanje sistema zaštite. - Uspostavljene politika pregleda sistemskih log datoteka, testiranje na proboj sistema, interna i eksterna kontrola i nadzor.	
c. Upravljanje zaštitom u toku životnog ciklusa sistema. Razmatrati zaštitu u svakoj fazi životnog ciklusa IKT sistema: inicijacija (planiranje i priprema), razvoj/akvizicija, implementacija, funkcionalni rad i odlaganje (rashodovanje).	
d. Uspostavljanje procedure za akreditaciju i sertifikaciju. Zvanični upravni organ formalno autorizuje operacije (rad) sistema i upravljanje rizikom.	
e. Implementacija efikasne, bezbednosno orjentisane kadrovske politike. - 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 da zaposleni imaju 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 objekata u kojima su smešteni digitalni objekti, osoblja u objektima i IKT objekata.	
g. Implementacija politike zaštite za informatičku podršku i funkcionisanje. Razvoj i implementacija procedura za podršku korisnicima, izvršnog novog softvera, korišćenje pomoćnih alata OS, upravljanje licencama, bekapovanje i standardno logovanje.	
h. Implementacija politike za vanredne situacije. Zahteva razvoj, testiranje i ažuriranje plana za vanredne događaje za sve glavne aplikacije i opštu podršku sistema.	
i. Dokumentovanje specifičnih kontrola sistema zaštite i operativnih procedura. Dokumentacija uključuje specifikacije isporučioća hardversko softverske i druge 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 sa karakteristikama koje sugerišu zvanični organi istrage kompjuterskog kriminala, - Obezbeđuje korišćenje hw/sw tehnika i alata za forenzičku akviziciju i analizu digitalnih dokaza, - Obezbeđuje korišćenje softvera za identifikaciju virusa, razumevanje sastava i obuke tima za intervencije, sredstava za brzo centralizovano izveštavanje o incidentima, - Obezbeđuje distribuciju upozorenja o ranjivostima sistema i saveta za preduzimanje aktivnosti za njihovo brzo otklanjanje.	
l. Kontrola pristupa IKT objektima. - Razvija i implementira politiku identifikacije, autorizacije i autentifikacije i procedure za kontrolu pristupa objektima IKT sistema.	

Kriterijumi za 3. nivo	Da/Ne
- Uspostavlja politiku identifikacije korisnika, pokušaja logovanja, lozinki, ACL (kontrolne liste pristupa), mehanizama kriptozastite, uređaja za zaštitu portova i barijera (firewalls) i dr.	
m. Implementacija politike za registrovanje tragova za nadzor i kontrolu (audit). - Razvoj procedura za registrovanje tragova za kontrolu funkcionisanja sistema zaštite (audit), - Registrovanje, pregled i analizu tragova za istragu kompjuterskog incidenta, - Obezbeđuje zaštitu kontrolnih informacija od neovlašćenog pristupa.	

CL 4: Verifikovan i kvantitativno upravljani program zaštite organizacije imaju kada su sposobne da precizno odrede vrednost specifičnih kapaciteta za zaštitu, što je bitno za implementaciju rentabilnog (efikasnog i ekonomski opravdanog) – **optimalnog programa** zaštite. Ove organizacije vrednuju podatke i informacije na najvišem nivou i štite ih od gubitaka, oštećenja, izmene i neraspoloživosti, u skladu sa njihovom vrednosti. Na ovom nivou organizacije obezbeđuju integrisano upravljanje sistemom zaštite i sposobne su da odrede da li će specifični kapaciteti sistema zaštite omogućiti takve kapacitete za obavljanje misije, koji imaju troškove najmanje jednake troškovima implementacije sistema zaštite. Dostizanje CL 4 zahteva aktivno uključivanje u program zaštite vlasnika/najviše upravne strukture procesa za izvršavanje poslova i misije organizacije. Program zaštite neke organizacije smatra se da je najmanje na CL 4, ako zadovoljava sve kriterijume sa CL 3 i ispunjava sledeće kriterijume:

Kriterijumi za 4. nivo	Da/Ne
a. Razumeti vrednost informacija i uticaja gubitaka, oštećenja i neraspoloživosti informacija na misiju organizacije.	
b. Odrediti kako nebezbednost u IKT može uticati na misiju organizacije, merenjem rentabilnosti mera zaštite i uticaja programa zaštite.	
c. Porediti troškove sistema zaštite sa troškovima posledica uticaja na misiju, ako mere zaštite nisu implementirane.	
d. Obezbediti da su troškovi kapaciteta za ostvarivanje misije barem jednaki troškovima implementacije mera i metoda 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, koja u suprotnom može biti ugrožena brojnim faktorima rizika.	
h. Analizirati sistem mera za evaluaciju efikasnosti zaštite.	
i. Vodi pozitivno izveštavanje o identifikovanim ranjivostima i preduzima preventivne i korektivne aktivnosti.	
j. Precizno meri i određuje poboljšanje kapaciteta misije organizacije, koju obezbeđuju date mere i metode zaštite	
k. Precizno meri i određuje troškove implementacije sistema zaštite.	

CL 5: Optimalan (adaptivan) i sveobuhvatan program zaštite poboljšava kontinualno rentabilnost mera zaštite i donosi odluke na bazi preciznih znanja o dobiti i troškovima implementacije sistema zaštite, koje uključuju: poboljšavanje programa zaštite, poboljšavanje procedura programa zaštite, poboljšavanje mera i metoda sistema zaštite, dodavanje novih mera i metoda zaštite, integrisanje sistema zaštite u IKT infrastrukturu i uključivanje u IKT arhitekturu i poboljšavanje procesa za ostvarivanje misije i aktivnosti za upravljanje rizikom. Na ovom nivou programa zaštite, sistem zaštite se posmatra **kao integralni deo misije organizacije**, a akvizicija i implementacija sistema zaštite uzimaju se kao neophodni troškovi poslovanja, što se postiže sa:

- Razumevanjem i postavljanjem sistema zaštite kao faktora koji obezbeđuje efikasnije ostvarivanje misije organizacije, obezbeđujući poboljšanje misije IKT sistema sa boljim sistemom zaštite,

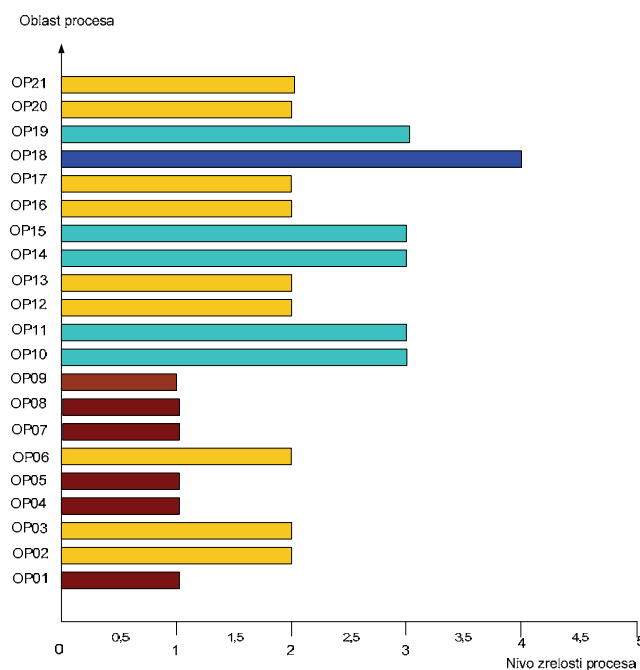
- Postavljanjem vlasnika misije kao aktivnog učesnika programa zaštite,
- Obezbeđivanjem velikog opsega opcija za odluke o poboljšavanju kapaciteta za ostvarivanje misije sa poboljšavanjem sistema zaštite,
- Obezbeđivanjem korektnog upravljanja rizikom (očekuje se na svim nivoima okvira), tj. izbora što niže cene implementacije sistema zaštite za redukciju što većeg broja faktora rizika na niži nivo.

Kriterijumi za 5. nivo	Da/Ne
a. Primeniti rentabilne mere derivirane sa 4. nivoa i pretočiti u odluku za postizanje poboljšanja programa zaštite.	
b. Demonstrirati da je zaštita IKT objekata integralni deo poslova organizacije.	
c. Razumeti i upravljati ranjivostima sistem zaštite.	
d. Kontinualno re-evaluirati 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.	

Razvoj referentnih profila zrelosti OP organizacija zaštite

1. Razvoj referentnog profila zrelosti OP organizacije za razvoj proizvode zaštite

SSE-CMM profil za organizaciju koja razvija proizvode zaštite prikazan je na Sl. 2.9.1.

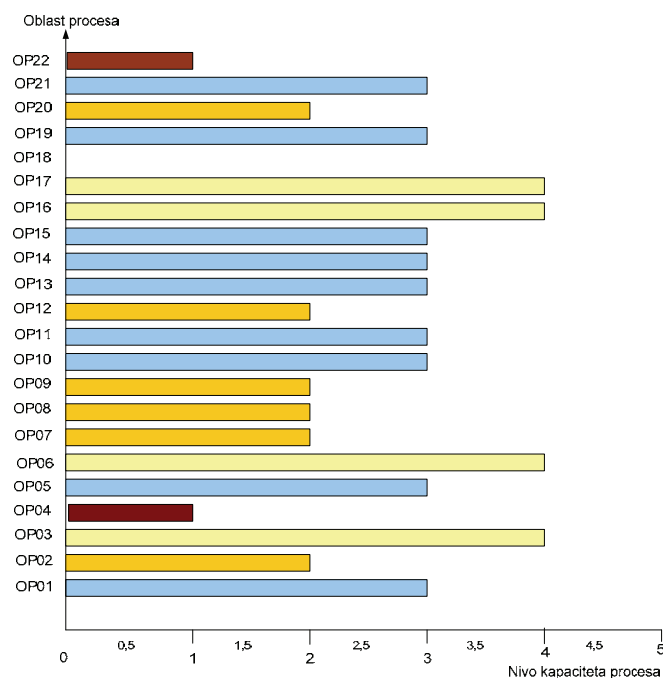


Sl. 2.9.1. Profil za organizaciju koja razvija proizvode zaštite

Kao što se vidi OP koje se odnose na aktivnosti razvoja proizvoda stavljene su na najviši nivo zrelosti, dobro definisanih i implementiranih procesa, kako se i očekuje. SSE OP generalno su pripisane nižim nivoima zrelosti, iako su važne aktivnosti, ali nisu glavne aktivnosti organizacije i nisu stalno u upotrebi. Međutim, ako organizacija samo proizvodi proizvode zaštite onda inženjerskim (SSE) OP treba pripisati viši nivo zrelosti. Izuzetak od ovog su OP02, OP03, OP06 i OP10. U ovom slučaju OP se fokusiraju na identifikovanje ranjivosti proizvoda, obezbeđuju bezbednosni ulaz za proizvod i verifikuju korektnost implementacije zaštite. Ove OP su, u slučaju proizvoda zaštite, veoma važne, posebno sa aspekta kupaca. OP06 je uključena kao bezbednosna garancija koja se odnosi na poverenje kupca u bezbednosni kvalitet kupljenog proizvoda zaštite. Za snabdvača proizvoda zaštite važno je da obezbede poverenje kupaca u svoje proizvode.

2. Razvoj referentnog profila OP organizacije za integraciju sistema zaštite

Profil za organizaciju koja integriše sisteme zaštite u IKT sisteme prikazan je na slici Sl. 2.9.2. Profil je nezavisan od načina integracije sistema i stepena specijalizacije organizacije za integraciju sistema zaštite.



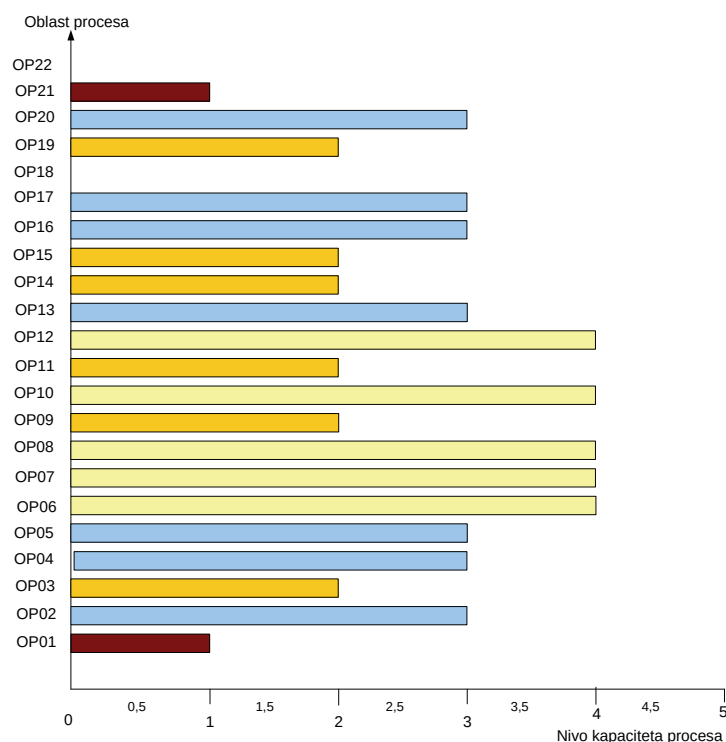
Sl. 2.9. 2. Profil organizacije za integraciju sistema

U ovom slučaju najviši nivo zrelosti zahteva se za one OP koje najznačajnije doprinose ispunjavanju očekivanja kupaca. Dakle, najveća pažnja je usmerena na OP16 i OP17 koje se odnose na zrelost SSE procesa organizacije, kao i na OP06 - *Izgradnja argumenata bezbednosne garancije*, koja obezbeđuje poverenje kupca i konačno na OP03 koja vrednuje i verifikuje da su bezbednosni zahtevi ispunjeni. Sve druge OP su pripisane umerenim nivoima zrelosti sa pretpostavkom da se kupci konačno oslanjaju na rezultate integracije, pa ovi rezultati moraju biti adekvatno obezbeđeni i pouzdani. OP se ne primenjuju samo na rezultate preduzetih procesa nego i na okruženje u kojem se vrši integracija, a koje nije bezbedno, pa se može uneti ranjivost u procesu integracije. Jedini izuzetak od ovog opšteg pristupa je OP04-*Procena pretnji*. U ovom slučaju pretpostavlja se da je ova aktivnost više funkcija konačnog proizvoda u operativnom okruženju, pa je dovoljno da je samo planirana i dokumentovana. Dakle, izvršiće je kupac u okruženju krajnjeg korisnika proizvoda zaštite.

3. Razvoj referentnog profila OP organizacije za servisiranje zaštite

Organizacija za servisiranje izvršava neki poseban skup funkcija u ime ugovorne organizacije. Profil OP ovakve organizacije prikazan je na slici Sl. 2.9.3. Pošto se ovakve organizacije obično specijalizuju u određeni tip servisnih funkcija, one mogu izvršavati ove funkcije mnogo efektivnije i jeftinije nego individualne organizacije. Servisna organizacija normalno izvršava isti skup funkcija za više drugih organizacija. Tradicionalno shvatanje rada servisnih organizacija u IKT se menja. U većini slučajeva podrazumeva se da servisna organizacija ima odgovornost za najveći deo, ako ne sve operacije IKT sistema organizacije, što značajno povećava zavisnost klijenata od servisne organizacije, ali i zahteve za većim poverenjem u kvalitet dobijenih usluga. Poverenje mora postojati između servisne organizacije i klijenata, posebno da će informacije iz klijentskih organizacija biti zaštićene od otkrivanja i korupcije i da će usluge biti izvršene u odgovarajućem vremenskom okviru. Ima mnogo primera organizacija koje se mogu svrstati u ovu grupu uključujući snabdevače objekata za oporavak sistema posle vanrednog događaja ili kompjuterskog incidenta (opremanje vruće i hladne lokacije), banke, organizacije za verifikaciju kredita, tradicionalne servisne organizacije za IKT podršku, računovodstvene organizacije i.t.d. Dakle, OP koje zahtevaju najviši nivo zrelosti su one koje osiguravaju separaciju i zaštitu i obezbeđuju argumente bezbednosne garancije klijentskoj organizaciji, odnosno OP06, OP07, OP08, OP10 i OP12. OP01 se smatra da je od malog značaja pošto zadatak identifikovanja

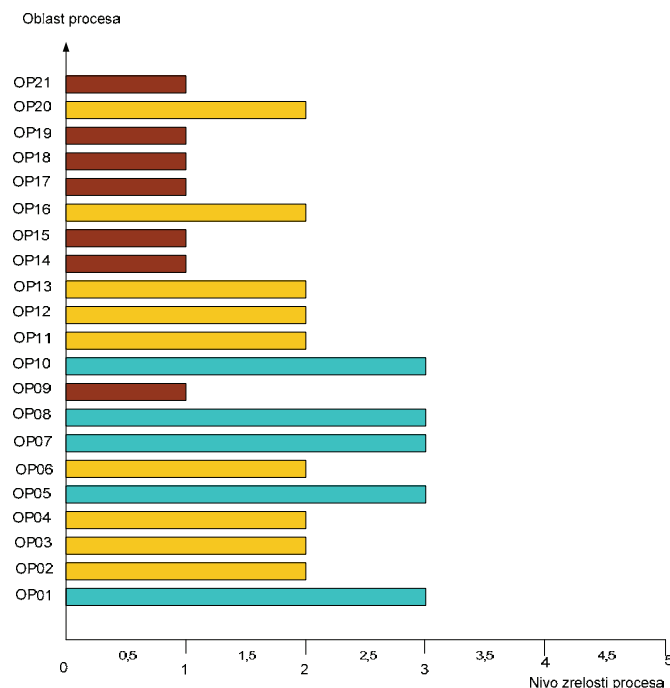
bezbednosnih potreba izvršava klijentska organizacija i prenosi ga servisnoj organizaciji. OP22 - *Koordinacija sa snabdevačem* kao i OP18 - *Poboljšavanje SSE procesa organizacije* smatraju se relativno beznačajnim u ovom slučaju, pa se ne koriste. Sve druge OP smatraju se umereno važne i potrebne su da u nekoliko slučajeva podrže OP na višim nivoima zrelosti.



SL. 2.9.3. *Profil servisne organizacije u IKT*

4. Razvoj referentnog profila OP standardnog sertifikacionog tela

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 sprovede, ili da su obavezne za tipična CA. Međutim, bez obzira na politike i prakse koje CA treba da sprovede 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 SL. 2.9.4 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.



Sl. 2.9.4. 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.

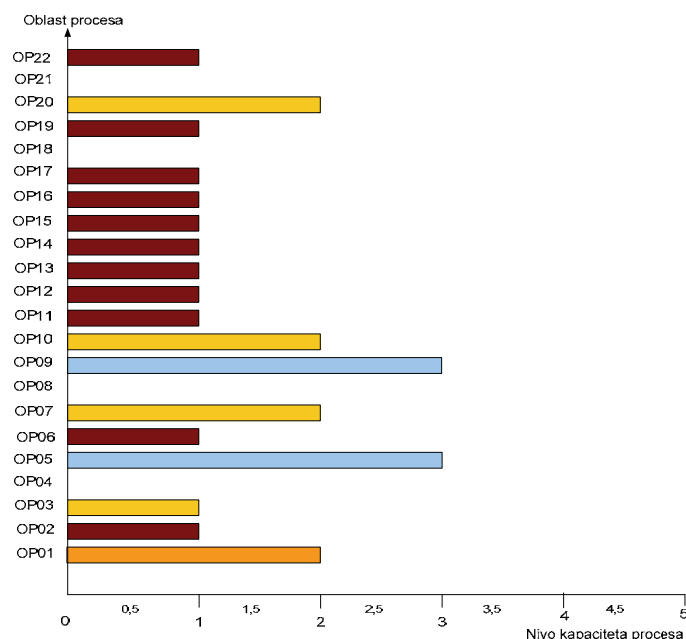
Organizacija koja unapređuje program rada treba da prema značaju odredi prioritete izvršavanja OP u odnosu na postavljene ciljeve i da nastoji da najpre poboljšava kapacitete u tim OP. OP01, OP05, OP07, OP08 i OP10 smatra se da zaslužuju najveću pažnju i samim tim treba da budu na najvišem nivou zrelosti kapaciteta. Ove OP moraju biti dobro dokumentovane i organizacija treba da ih regularno koristi. Smatra se da je dobro definisan i implementiran 3. 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 (2. 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 2. nivou zrelosti procesa. Smatra se da CA organizacija periodično koristi ove procese (na 2. 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 tekucih 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.

5. Razvoj referentnog profila OP korisničke organizacije IKT sistema

Organizacija koja koristi IKT sistem može biti svaka organizacija koja koristi IKT sistem za opštu podršku poslovnih procesa, glavnu aplikaciju, ili pomoć u upravljanju delom ili svim operacijama u organizaciji. To praktično znači da u ovu kategoriju spada ogroman broj savremenih organizacija. Svaka organizacija ima informacije koje zahtevaju određeni stepen zaštite. Zahtev za zaštitu može se odnositi na zaštitu poverljivosti, integriteta, ili raspoloživosti i kombinaciju ovih zahteva. Potrebe za zaštitom informacija zahtevaju da organizacije koriste zrelije procese za zaštitu, bilo iz sopstevnih resursa ili od TTPS provajdera zaštite. U suprotnom, organizacija se izlaže značajnom riziku za tekuće operacije. Profil zrelosti procesa korisničke organizacije prikazan je na slici Sl. 2.9.5.



Sl. 2.9.5. Profil IKT korisničke organizacije

Imajući ovo na umu procenjuje se da OP09 – *Koordinacija zaštite* i OP05 – *Procena operativnog rizika* zahtevaju najviše nivo zrelosti. Njih blisko prate OP01, OP07, OP08, OP10 i OP20 koje se sve zahtevaju za obezbeđivanje podrške tekuće efektivnosti sistema zaštite koju organizacija uspostavi. Ostale OP smatra se da ne moraju biti na istom nivou zrelosti. Mogu se pripisati SSE aktivnostima koje korisničke organizacije ređe izvršavaju, a mogu se dobiti i od TTPS provajdera zaštite. OP04, OP18 i OP21 smatraju se neprimenljivim u opštem slučaju zbog njihove visoko specijalizovane prirode.

Gornji primeri referentnih (željenih) profila predstavljaju uopštene modele primenljive za sve navedene tipove organizacija, ali se podrazumeva da svaka konkretna organizacija prilagodi model profila sopstvenim potrebama i okruženju. Najbolje je da takvu vrstu prilagođenja modela svojim potrebama, organizacija radi uz pomoć eksperta za primenu SSE CMM modela evaluacije (SSAM), posebno da se izbegnu problemi sa međuzavisnostima OP. Naime, iako je namera modela da sve OP budu što više nezavisne, neizbežna je određena međuzavisnost OP i ovaj se aspekt mora uzeti u obzir.

Kriterijumi za izbor nivoa zrelosti P-CMM kapaciteta

Nivo 1: Inicijalni nivo zrelosti: Performanse aktivnosti zaposlenih su nekonzistentne. Organizacija tipično obezbeđuje alate za evaluaciju kvaliteta rada, ali malo uputstava i obuke za izvršavanje aktivnosti koje ti alati podržavaju. Menadžeri nisu osposobljeni za izvršavanje najvećeg broja aktivnosti svojih zaposlenih, tako da su im kapaciteti za upravljanje svedene na lične sposobnosti i stečena iskustva. Oni ne poseduju kapacitete za sistematski razvoj konkurentnih sposobnosti (kompetentnosti) svojih zaposlenih. Zaposleni na ovom nivou ne shvataju svoj rad ozbiljno, jer ne veruju da njihove praktične aktivnosti imaju veliki uticaj na stvarni rad i da doprinose razvoju organizacije. Zaposleni ne usklađuju lične inicijative sa ciljevima organizacije i misle da su bolji radni uslovi u drugoj organizaciji. Odlaskom osposobljenih pojedinaca iz bilo kojeg razloga, nije moguće poboljšavati znanja i veštine u organizaciju u dužem vremenskom periodu.

Nivo 2: Ponovljivi procesi: Primarni ciljevi su da se eliminišu problemi koji sprečavaju ljude da efektivno izvršavaju svoje radne zadatke i da se uspostavi osnov za radnu praksu koja se kontinualno može poboljšavati u procesu razvoja ljudskih resursa. Najčešći problemi koji sprečavaju efektivan rad uključuju: rasipanje pažnje u okruženju, nejasni ciljevi rada, nedostatak relevantnih znanja i veština, loša komunikacija.

Organizacija se u politici (rada, zaštite i sl.) obavezuje na razvoj ljudskih resursa. Svi zaposleni imaju odgovornosti koje lično prihvataju i efektivno primenjuju prakse rada. Ozbiljnim shvatanjem svojih radnih odgovornosti, zaposleni počinju razvijati ponovljive metode za izvršavanje specifičnih aktivnosti, kao što su intervjuisanja i uspostavljanje kriterijuma kvaliteta rada. Zaposleni vide veću konzistentnost u rezultatima rada svoje grupe, mada su moguće individualne varijacije između grupa zbog korišćenja različitih metoda. Na bazi politike organizacije, organizacione jedinice izrađuju planove rada za implementaciju radne prakse i ispunjavanje svojih odgovornosti.

Nivo 3 – Definisani procesi: Organizacije na nivou ponovljivih procesa izvršavaju bazične prakse zaposlenih, ali postoje nekonzistentnosti u načinu izvršavanja na nivou cele organizacione jedinice. Takođe, na ovom nivou organizacije ne standardizuju najbolje radne prakse, zato što ne mogu identifikovati potrebna opšta znanja i veštine i najbolje prakse za njihov razvoj u celoj organizacionoj jedinici. Zato je organizacija motivisana da dostigne definisani nivo, da bi ostvarila strategijsku komparativnu prednost zahvaljujući suštinskoj kompetentnosti zaposlenih. Na definisanom nivou, organizacija počinje da prilagođava radne prakse zaposlenih prema specifičnoj prirodi svog poslovanja. Komparativnom analizom zahtevanih veština za zaposlene i poslovnih funkcija koje izvršava, organizacija identifikuje suštinske kompetentnosti koje se zahtevaju za izvršavanje poslovnih ciljeva. Zatim, organizacija usvaja radne prakse za razvoj specifičnih znanja i veština, koje čine ove suštinske kompetentnosti. Organizacija identifikuje najbolje prakse za razvoj kompetentnosti i aktivnosti svojih zaposlenih, ili onih iz drugih organizacija i prilagođava ih kao osnovu za razvoj radne prakse svojih zaposlenih. Organizacija analizira svoje poslovne procese radi određivanja suštinske kompetencije i znanja i veština koji čine te kompetencije. Zatim, razvija dugoročne i kratkoročne planove za razvoj kompetencija zaposlenih. Definiše se program za razvoj ključnih kompetencija, kao i strategije za individualno profesionalno usavršavanje pojedinaca. Organizacija analizira prakse svojih zaposlenih, da bi identifikovala ključne kompetentnosti i primenila proces poboljšanja.

Opšta kultura rada organizacije može se razviti na ovom nivou zrelosti, zato što se organizacija usmerava na razvoj skupa ključnih kompetencija. Ova kultura rada pridaje značaj izgradnji i rastu kapaciteta za razvoj ključnih kompetentnosti zaposlenih u organizaciji, a svi zaposleni dele odgovornost za to. Ova se kultura rada može poboljšati stvaranjem takvog okruženja gde su svi zaposleni učesnici procesa razvoja kompetencija u domenu svog rada. Na ovom nivou kapaciteta

zaposleni poseduju osnovna znanja i veštine za izvršavanje ključnih poslovnih funkcija organizacije. Znanja i veštine u ključnim kompetencijama organizacije uglavnom su ravnomerno raspoređeni u organizaciji. Organizacija je poboljšala svoje sposobnosti da predvidi performanse radnih aktivnosti na bazi stečenih znanja i veština zaposlenih. Organizacija uspostavlja osnovu za kontinualni razvoj znanja i veština.

Nivo 4 – Upravljeni procesi: Organizacija preduzima prve korake za izvlačenje stratejskih prednosti iz upravljanja procesima za razvoj ključnih kompetentnosti zaposlenih. Postavlja kvantitativne ciljeve za rast ključnih kompetencija i usklađivanje performansi pojedinaca, timova, radnih jedinica i na nivou cele organizacije. Ove mere uspostavljaju kvantitativnu osnovu za evaluaciju trenda razvoja kapaciteta zaposlenih. Nastoji se postići maksimalna efektivnost od primene ovih kompetencija kroz razvoj timova koji integrišu komplementarna znanja i veštine. Na 3. nivou zrelosti ovakav tim se razvija samo tamo gde uslovi rada podržavaju njihovo funkcionisanje. Na ovom nivou zrelosti kapaciteta, aktivnosti za izgradnju timskog rada izvršavaju se sa ciljem poboljšavanja efektivnosti ovih timova. Primenjene na timski rad, radne prakse zaposlenih prilagođavaju se prema referentnim praksama P-CMM modela. Timu i pojedincima su na raspolaganju mentori za pružanje lične pomoći u znanjima i veštinama i davanje potrebnih instrukcija. Takođe, mentori prenose zaposlenim sublimirana znanja i iskustva stečena u celoj organizaciji.

Razvoj OP organizacije u svakoj ključnoj kompetentnosti kvantitativno je upravljan. Podaci na nivou ključnih kompetencija organizacije analiziraju se radi određivanja trendova i zrelosti kapaciteta. Ovi trendovi razvoja kompetencija koriste se za evaluaciju efektivnosti praksi koje se odnose na rast kompetentnosti zaposlenih. Ovi se trendovi rasta prate, mere i upoređuju sa skupom ciljeva u dugoročnim i kratkoročnim planovima. Kapaciteti zaposlenih na ovom nivou su prdvidljivi, zato što su tekući kapaciteti kvantitativno mere. Organizacija je razvila mehanizam za efektivnu implementaciju kompetentnosti kroz kompetentne visoko efikasne timove. Dakle, ovaj nivo kapaciteta zaposlenih obezbeđuje organizaciju sa važnim prediktorom trendova razvoja poslovnih kapaciteta.

Nivo 5 – Optimizovani procesi: Na ovom nivou pažnja se neprekidno usmerava na poboljšavanje individualnih kompetentnosti i pronalaženje inovativnih načina za podizanje motivacije i kapaciteta zaposlenih. Organizacija podržava individualne napore za neprekidni razvoj ličnih kompetencija. Obezbeđeni su instruktori za dalji razvoj personalnih i timskih kompetencija. Podaci o efektivnsoti praksi zaposlenih koriste se za identifikovanje potreba za inovaciju praksi zaposlenih ili tehnologija. Inovativne prakse i tehnologije se evaluiraju, a one koje najviše obećavaju testiraju se u istraživačkom pilot projektu. Uspesna inovacija se zatim implementira u celoj organizaciji. Kapaciteti zaposlenih na ovom nivou neprekidno se poboljšavaju zato što se neprekidno poboljšavaju njihove prakse kroz *inovativno* ili *inkrementalno* poboljšavanje. Kultura rada na ovom nivou je takva u kojoj svi zaposleni teže da povećaju lična, timska i organizaciona znanja, veštine i motivacije, da ciljem poboljšavanja ukupnih performansi organizacije.

Opis ključnih P-CMM OP

Ključne OP na CL 2: Ponovljivi procesi

Fokusirane su na uspostavljanje osnovnih praksi zaposlenih i eliminisanje problema koji koče radne performanse. Ključne OP su opisane u nastavku:

OP1: Radno okruženje je dizajnirano da uspostavi i održava radne uslove koji dopuštaju pojedincima da se koncentrišu na svoje zadatke, bez nepotrebne i neodgovarajuće destrukcije pažnje. Obezbeđuje postojanje odgovarajućeg radnog okruženja koje je usklađeno sa primenljivim zakonima i regulativama, gde je učinjeno poboljšanje performansi, uklonjene prepreke za performanse i da su destrukcije minimizovane.

OP2: Komunikacija dizajnirana je da uspostavi društveno okruženje koje podržava efektivnu interakciju i osigura da zaposleni imaju veštine da dele informacije i efektivno koordiniraju aktivnosti. Komunikacija uključuje uspostavljanje efektivnih komunikacionih mehanizama odozgo - na dole i odozdo - na gore u organizaciji i osiguranje da svi pojedinci imaju neophodne komunikacione veštine za izvršavanje zadataka, efektivnu koordinaciju, efikasno vođenje sastanaka i rešavanje problema.

OP3: Popuna radnih mesta dizajnirana je da uspostavi i koristi formalni proces sa kojim se regrutuju, biraju i uvode u poslove organizacije talentovani pojedinci. Rekrutovanje uključuje identifikovanje znanja i veština koje se zahtevaju za otvorene poslove, motivisanje svih pojedinaca da traže kvalifikovane kandidate, oglašavanje raspoloživih poslova i pregled efektivnosti napora regrutovanja. Selekcija uključuje razvoj liste kvalifikovanih kandidata, definisanje kriterijuma i strategije za izbor, identifikovanje kvalifikovanih kandidata i detaljnu proveru kvalifikovanih kandidata i izbor najboljih kandidata. Uvođenje u posao uključuje prijem izabranih kandidata, upoznavanje sa organizacijom i obezbeđivanje uspešne tranzicije na nove poslove.

OP4: Upravljanje performansama dizajniran je za uspostavljanje kriterijuma za merenje performansi organizacionih jedinica i pojedinaca za obezbeđivanje povratnih informacija i neprekidno poboljšavanje performansi. Upravljanje performansama uključuje uspostavljanje objektivnih kriterijuma za evaluaciju performansi organizacionih jedinica i pojedinaca, regularnu diskusiju i identifikovanje potreba za razvojem, sistematsko obuhvaćanje problema i nagrađivanje izvanrednih rezultata.

OP5: Obuka je dizajnirana da osigura da svi pojedinci imaju zahtevane veštine za izvršavanje svojih zadataka. Obuka uključuje identifikovanje zahtevanih veština za izvršavanje kritičnih zadataka, identifikovanje potreba za obukom za svaku jedinicu i obezbeđivanje neophodne obuke.

OP6: Kompenzacija je dizajnirana da obezbedi sve pojedince sa nadoknadom i beneficijama na bazi njihovog doprinosa i povećanja vrednosti za organizaciju. Kompenzacija uključuje razvoj dokumentovane strategije za kompenzacije, razvoj plana za administraciju kompenzacija i periodično prilagođavanje kompenzacija na bazi performansi.

Ključne OP na CL 3: Definisani procesi

Ključne OP na nivou definisanih procesa obuhvataju organizaciona pitanja, pošto organizacija prilagođava svoje definisane prakse zaposlenih prema ključnim kompetencijama koje se zahtevaju u poslovnom okruženju.

OP7: Analiza znanja i veština dizajnirana je za identifikaciju znanja i veština potrebnih za izvršavanje ključnih poslovnih procesa, tako da se mogu razvijati i koristiti kao baza za praksu zaposlenih. Analiza znanja i veština uključuje identifikovanje poslovnih procesa u kojima organizacija mora održavati kompetencije, razvoj profila znanja i veština potrebnih za

izvršavanje ovih poslovnih funkcija, održavanje inventara znanja i vještina i identifikovanje budućih potreba za znanjima i vješinama.

OP8: Planiranje sistematizacije je dizajnirana za koordinaciju aktivnosti zaposlenih sa tekućim i planiranim poslovnim potrebama na nivou organizacije i organizacionih jedinica. Planiranje sistematizacije zaposlenih uključuje razvoj strateškog plana koji postavlja ciljeve na nivou organizacije za razvoj kompetencija i aktivnosti zaposlenih i razvoj kratkoročnih planova za vođenje aktivnosti zaposlenih u svakoj organizacionoj jedinici.

OP9: Razvoj kompetentnosti je dizajnirana da konstantno poboljšava kapacitete zaposlenih za izvršavanje zadataka i odgovornosti. Ključne kompetencije definisane u OP 7 i OP8 obezbeđuju osnovu za program razvoja i obuke organizacije. Razvoj kompetencija uključuje uspostavljanje obuke i drugih razvojnih programa u svakoj od ključnih kompetencija organizacije. Razvojne aktivnosti su dizajnirane da podignu nivo znanja i vještina u u tekućim i novo-prihvaćenim kompetencijama organizacije.

OP10: Profesionalni razvoj dizajniran je da osigura da su svi pojedinci motivisani i imaju priliku za razvoj novih vještina koje poboljšavaju njihove sposobnosti za postizanje ciljeva karijere. Razvoj karijere uključuje diskusiju opcija karijera sa svakim pojedincem, razvoj plana za personalni razvoj, praćenje progressa prema tom planu, identifikovanje mogućnosti za obuku i pravljenje zadataka koji poboljšavaju ciljeve karijere.

OP11: Prakse za procenu kompetentnosti dizajnirane su da osiguraju da su sve prakse zaposlenih zasnovane delom na razvoju znanja i vještina zaposlenih. Ova OP uključuje zapošljavanje na bazi potreba za znanjima i vješinama, metoda izbora na proceni znanja i vještina kandidata, procene izvršavanja poslova na bazi zadataka i uloga i kompenzacije zaposlenih barem delom na bazi povećanja znanja i vještina.

OP12: Kultura učestvovanja dizajniran je da osigura tok informacija u organizaciji, ugradnju znanja pojedinaca u proces odlučivanja i da obezbedi njihovo angažovanje. Uspostavljanje kulture učestvovanja postavlja osnovu za izgradnju tima sa visokim performansama. Kultura učestvovanja uključuje uspostavljanje efektivne komunikacije između svih nivoa organizacije, traženje ulaza od pojedinaca, uključivanje pojedinaca u odlučivanje i angažovanje i komunikaciju odluka tim pojedincima.

Ključne OP na CL 4: Upravljeni procesi

Ključne OP na ovom nivou usmerene su na izgradnju kompetentnog tima i uspostavljanje kvantitativne metrike za razumevanje trendova u razvoju znanja i vještina i usklađivanje performansi na različitim nivoima organizacije. Analiza pet ključnih OP na ovom nivou zrelosti veoma su međuzavisne.

OP13: Mentorsko vođenje dizajnirano je za korišćenje iskustva zaposlenih organizacije za obezbeđivanje podrške i instrukcija drugim pojedincima i grupama. Ovo može uključivati razvoj znanja i vještina, poboljšavanje performansi, snalaženje u teškim situacijama i formiranje odluka o profesionalnom razvoju. Mentorsko praćenje uključuje postavljanje ciljeva, selekciju i osposobljavanje odgovarajućih mentora, dodeljivanje mentorima pojedinaca i grupa, uspostavljanje odnosa među mentorima i evaluaciju efektivnosti programa mentorskog praćenja.

OP14: Izgradnja tima dizajnirana je da iskoristi prilike za kreiranje timova koji maksimalno integrišu različita znanja i vještine za izvršavanje poslovnih funkcija. Izgradnja tima uključuje usklađivanje potencijalnih sposobnosti članova tima za zahtevana znanja i vještine, obučavanje novih članova u vješinama tima, definisanje ciljeva za performanse tima, prilagođavanje standardnih procesa za korišćenje u radu i periodičnu reviziju performansi tima.

OP15: Prakse za izbor kompetentnosti tima dizajnirana je za prilagođavanje praksi zaposlenih organizacije za podršku razvoja, motivacije i funkcionisanja tima. Prakse bazirane na timskom radu uključuju obezbeđivanje da radno okruženje podržava funkcije tima, postavlja kriterijume

performansi i revizije performansi tima, uključujući članove tima u aktivnosti performansi zaposlenih i reflektujući kriterijume tima na odluke o kompenzaciji pojedinaca.

OP16: Upravljanje kompetencijama organizacije dizajnirana je da poveća kapacitete organizacije u ključnim kompetencijama i da odredi efektivnost aktivnosti u razvoju tih kompetencija u postizanju ciljeva rasta specifičnih kompetencija. Ova OP uključuje postavljanje merljivih ciljeva rasta ključnih kompetencija organizacije, definisanje i sakupljanje relevantnih podataka, analizu uticaja aktivnosti razvoja kompetencija na postizanje tih ciljeva i korišćenje rezultata za upravljanje aktivnostima poboljšavanja kompetencija.

OP17: Usklađivanje performansi organizacije dizajnirana je da poboljša usklađivanje rezultata performansi na nivou pojedinaca, tima, organizacione jedinice i organizacije sa odgovarajućim ciljevima i kvantitativnom procenom efektivnosti praksi zaposlenih na postizanju tih usklađivanja. Ova OP uključuje uspostavljanje merljivih ciljeva za usklađivanje performansi na nivou pojedinaca, organizacionih jedinica i organizacije, definisanje podataka i analizu, sakupljanje podataka, analizu trenda ispunjavanja ciljeva, delovanje na izuzetne nalaze, analizu uticaja praksi koje se odnose na ljude na usklađivanje performansi i izveštavanje rezultata.

Ključne OP na CL 5: Optimizovani procesi

Oblast ključnih procesa (sadrži 3 OP) na ovom nivou pokriva pitanja koja moraju obuhvatiti i pojedinci i organizacije u kontinualnom poboljšavanju svojih kapaciteta.

OP18: Razvoj personalne kompetentnosti dizajnirana je da obezbedi osnovu za profesionalni samorazvoj. Razvoj ličnih kompetencija sastoji se od dobrovoljnog programa za neprekidno poboljšavanje individualnih radnih procesa. Ovaj program uključuje razvoj ciljeva i planova za lične radne aktivnosti, uspostavljanje i korišćenje definisanih personalnih procesa, merenje i analizu efektivnosti ovih personalnih procesa i njihovo poboljšavanje.

OP19: Instrukтивna obuka dizajnirana je da obezbedi ekspertsku pomoć za povećanje performansi pojedinaca i tima. Instruktori se blisko angažuju sa pojedincima i timovima u razvoju veština koje poboljšavaju performanse procesa rada. Instrukтивna obuka uključuje izbor odgovarajućeg instruktora, analizu podataka o personalnim ili timskim performansama.

OP20: Neprekidno inoviranje praksi zaposlenih dizajnirana je da identifikuje i evaluiira poboljšane prakse zaposlenih i tehnologije i najbolje implementira u celoj organizaciji. Ova OP uključuje uspostavljanje mehanizma za predlaganje poboljšavanja aktivnosti zaposlenih, identifikovanje potreba za novim praksama i tehnologijama i implementacije u organizaciji onih koje donose najveće benefite.

Kategorije kapaciteta OP P-CMM

Razvoj sposobnosti — Napor za razvoj sposobnosti (kapaciteta) zaposlenih u organizaciji počinju na nivou *Ponovljivih procesa* sa identifikovanjem trenutnih potreba za obukom zaposlenih u svakoj organizacionoj jedinici. Oralne i pismene komunikacione sposobnosti poboljšavaju se kroz obuku iz komunikacija. Na nivou *Definisanih procesa* organizacije sistematičnije gleda na znanja i veštine koje se zahtevaju za izvršavanje poslovnih procesa organizacije (*Analiza znanja i veština*) i identifikuje ključne kompetencije. Organizacija takode, uspostavlja program razvoja ovih kompetencija za celu organizaciju (*Razvoj kompetencija*). Na nivou *Upravljanih procesa* obezbeđeni su mentori za vođenje pojedinaca ili timova u razvoju svojih kompetencija (*Mentorsko vođenje*). Konačno na nivou *Opimalnih procesa*, zaposleni mogu inicirati individualni program za razvoj svojih kompetencija (*Razvoj personalnih kompetencija*), a instruktori su obezbeđeni za one koji žele pomoć (*Instruktorsku obuku*). Trend sazrevanja razvoja kompetencija zaposlenih počinje sa identifikovanjem tekućih potreba za obukom u nekoj organizacionoj jedinici, a završava sa identifikacijom ključnih kompetencija koje je organizacija razvila, a zatim se vraća na pojedince koji su sposobni da uspostave svoj program za profesionalni razvoj.

Izgradnja timova i kulture rada — Naponi za poboljšavanje načina na koji su zaposleni organizovani i sarađuju u organizaciji počinju na nivou *Ponovljivih procesa* sa fokusom na poboljšavanje formalnih i inter-personalnih komunikacija u organizaciji (*Komunikacije*). Na nivou *Definisanih procesa* organizacija razvija kulturu učestvovanja povećanjem uključivanja zaposlenih u odlučivanje koje utiče na njihov rad (*Kultura učestvovanja*). Na nivou *Upravljanjih procesa* organizacija počinje izgradnju visoko efektivnih timova na bazi kompetencija i obezbeđuje ih sa odgovarajućim nivoom autonomije (*Izgradnja tima*). Na nivou *Optimalnih procesa* organizacija neprekidno traga za inovacijama da poboljša kulturu rada ili funkcionisanje tima (*Kontinualno inoviranje zaposlenih*). Trend sazrevanja u izgradnji timova i kulture počinje sa uspostavljanjem osnovnih komunikacionih veština, rastu do razvoja kulture učestvovanja i nastavljaju u formalnu izgradnju tima i neprekidno poboljšavanje kapaciteta tima.

Motivacija i upravljanje performansama — Fokus na motivaciju i upravljanje performansama počinje na nivou *Ponovljivih procesa* sa uspostavljanjem okruženja koje ima adekvatne resurse i koje izvršavanje poslova (performanse) ne sprečavaju niti ometaju (*Radno okruženje*). Diskusija o poboljšavanju performansi održava se periodično, upravljaju se neprihvatljive performanse rada, a obezbeđena su priznanja za izuzetne performanse (*Upravljanje performansama*). Osnovni sistem kompenzacija i beneficija definiše se na ovom nivou, a njegova administracija delimično je povezana za radne performanse (*Kompenzacija*). Na nivou *definisanih procesa* radne prakse zaposlenih uspostavljene na nivou *Ponovljivih procesa* prilagođavaju se da motivišu razvoj ključnih kompetencija (*Prakse bazirane na kompetencijama*). Organizacije takođe uspostavljaju skup prilika za razvoj lične karijere, dizajniran da motiviše zaposlene i nagradi one koji razvijaju dodatne veštine (*Razvoj karijere*). Na nivou *Upravljanjih procesa* prakse zaposlenih ponovo se prilagođavaju, ovaj put za korišćenje u timu formiranom na bazi kompetencija (*Prakse na bazi tima*). Organizacije takođe postavljaju i prate ciljeve za prilagođavanje performansi na nivou pojedinca, tima, organizacione jedinice i organizacije (*Prilagođavanje performansi organizacije*). Na nivou *Optimalnih procesa* organizacija traga za inovativnim praksama i tehnologijama zaposlenih koje dalje mogu motivisati ili poboljšati razvoj kompetencija ili radne performanse (*Neprekidno inoviranje zaposlenih*). Trend sazrevanja u motivisanju i upravljanju performansama počinje sa uspostavljanjem upravljanja bazičnim performansama i kompenzacionim praksama, zatim poboljšavanjem ovih praksi kroz njihovo prilagođavanje do razvoja kompetencija i izgradnje tima, a zatim traženjem konstantnih izvora inoviranja tih praksi.

Popuna radnih mesta — Ovaj napor za postizanje poslovnih potreba počinje na nivou *Ponovljivih procesa* sa uspostavljanjem osnovnih praksi za regrutovanje, izbor kandidata za posao i orijektisanjem ljudi na nove zadatke (*Popuna radnih mesta*). Na nivou *Definisanih procesa* organizacija počinje razvijati strateške i kratkoročne planove za obezbeđenje ključnih kompetencija koje su potrebne za tekuće i nove poslovne zahteve (*Planiranje popune radnih mesta*). Na nivou *Upravljanjih procesa* organizacija postavlja i prati ciljeve za razvoj znanja i veština u svakoj ključnoj kompetenciji (*Upravljanje kompetencijama organizacije*). Na nivou *Optimalnih procesa* organizacija traga za inovativnim praksama ili tehnologijama da pomogne popunu svojih radnih mesta (*Neprekidno inoviranje zaposlenih*). Trend sazrevanja u popuni radnih mesta počinje sa uspostavljanjem osnovnih praksi, rasta do razvoja planova za razvoj zapošljavanja, postavlja i prati ciljeve za razvoj kompetencija zaposlenih, a zatim traži konstantne izvore inovacija tih kompetencija.

Uspostavljanje *pofila zaštite* standardnog PKI X.509 V.3 digitalnog sertifikata

1. Identifikacija kritičnih objekata

U procesu razvoja profila zaštite (**PP**), pre analize pretnji mora se izvršiti identifikacija kritičnih objekata koje želimo zaštititi. *IKT sistem* koji procesira, skladišti i prenosi informacije sadrži informacione, hardverske i softverske objekte, ljude i neku pristupnu tačku hostu klijenta, serveru i.t.d. Generalno, na najvišem nivou apstrakcije IKT sistema, kritični objekti se mogu kategorizovati u sledeće kategorije: **informacije, softver, hardver, sistemi i ljude**. *Informacije* uključuju dokumentaciju, poslovne planove, projektne planove, baze podataka o kupcima/klijentima, personalne podatke i finansijske informacije koje se koriste za ispunjavanje misije organizacije. *Softverski objekti* sadrže systemske i aplikativne programe i servise, kao što su OS, baze podataka, systemske i mrežne programe, poslovne aplikativne programe i korisničke aplikacije. *Hardver* sadrži fizičke objekte IKT sistema, kao što su radne stanice, serveri, printeri, mrežni uređaji i fizički mediji za prenos i.t.d. Objekat *IKT sistema* obuhvata hardver, softver, komunikacionu infrastrukturu, ljude i njihove međusobne veze. Objekat *ljudskih resursa* u oblasti zaštite obuhvata dobro osposobljene, vešte i iskusne specijaliste zaštite.

2. Metrike za procenu pretnji i rizika

Ove metrike mogu se koristiti za indikaciju nivoa intenziteta uticaja nekog napada u slučaju da se određena bezbednosna funkcija ne izvrši. U odnosu na posledice napada za organizaciju, metrika klasifikuje bezbednosne nivoe na *rudimentarni, bazični, srednji* i *visoki* nivo posledice uticaja napada (Tabeli 1), što je važno za proces razvoja PP za indikaciju bezbednosnih funkcija na koje objekat evaluacije (OE) mora usmeriti veću pažnju, kao i za verifikaciju samog PP, [62], [114].

Tabela 1. *Metrike za klasifikaciju uticaja kompromitacije bezbednosnih funkcija*

Br.	Bezbednosni nivo	Primenljivost za određivanje prioriteta bezbednosnih funkcija
1	Rudimentarni	Bezbednosne funkcije klasifikovane na ovom nivou obezbeđuju servis zaštite integriteta podataka
2	Bazični	Bezbednosne funkcije klasifikovane na ovom nivou su one koje uključuju objekte za ublažavanje pretnji za kompromitaciju podataka
3	Srednji	Bezbednosne funkcije klasifikovane na ovom nivou su one koje uključuju objekte za ublažavanje pretnji, koje mogu uzrokovati kompromitacija podataka, lažni pristup podacima i maliciozni korisnici
4	Visok	Ovaj nivo primenljiv je na bezbednosne funkcije čije nefunkcionisanje može izazvati velike posledice za organizaciju

Dakle, u procesu razvoja bezbednosnih zahteva za IKT sistem koristi se kvalitativna metrika za dobijanje kvantitativnih informacija koje se mogu koristiti za poboljšavanje procesa evaluacije, posebno: rizika i ranjivosti, profila zaštite i testiranja sistema.

3. Familije zaštite i komponente strukture PKI

U Tabeli 2. sumirani su primeri mapiranja CC bezbednosno funkcionalnih klasa prema bezbednosno funkcionalnim komponentama primenjenim u PKI sistemu, što je važan korak u procesu razvoja PP PKI. CC bezbednosne funkcije korisne su zato što pomažu evaluatoru da shvati, definiše i eventualno odredi adekvatne bezbednosne funkcije na bazi uticaja napada na sistem kompromitacijom određene funkcije, [18]. [114].

Tabela 2. Pokrivanje bezbednosno funkcionalnih komponenti aplikacija PKI sistema sa CC bezbednosno funkcionalnim klasama

Struktura komponenti bezbednosnih funkcija primenjenih u PKI sistemu (RFC 3280)	Korespondirajuće familija CC bezbednosnih funkcija
Potpis	Povezivanje korisnika i subjekta (FIA_USB)
Ime izdavača	Identifikacija korisnika (FIA_UID)
Ime subjekta	Identifikacija korisnika (FIA_UID)
Period validnosti	Istek roka bezbednosnog atributa (FMT_SAE)
Jedinstveni ID izdavača	Identifikacija korisnika (FIA_UID)
Jedinstveni ID subjekta	Identifikacija korisnika (FIA_UID)
Korišćenje ključa	Politika kontrole pristupa (FDP_ACC)
Politika sertifikacije	Politika kontrole pristupa (FDP_ACC)
Alternativno ime subjekta	Identifikacija korisnika (FIA_UID)
Alternativno ime izdavača	Identifikacija korisnika (FIA_UID)
Ograničenja politike	Politika kontrole pristupa (FDP_ACC)
Prošireno korišćenje ključa	Politika kontrole pristupa (FDP_ACC)
Sprečavanje neke politike	Politika kontrole pristupa (FDP_ACC)
Distribuciona tačka CRL	Opoziv (FMT_REV)
Sertifikaciona lista koja treba da se potpiše	Autentifikacija korisnika (FIAT_UAU)
Potpis CRL	Autentifikacija korisnika (FIAT_UAU)
Sadašnje ažuriranje CRL	Istek roka bezbednosnog atributa (FMT_SAE)
Sledeće ažuriranje CRL	Istek roka bezbednosnog atributa (FMT_SAE)
Opozvani sertifikat	Opoziv (FMT_REV)
Pogrešan podatak CRL	Istek roka bezbednosnog atributa (FMT_SAE)

4. Analiza pretnji

Organizacije mogu obezbediti servise zaštite, ili proizvode zaštite, ili jedno i drugo od poverljivih snabdevača. Međutim, osim servisa i proizvoda zaštite, poslovni sistemi imaju treću ključnu komponentu, a to je **upravljanje**, uključujući i upravljanje sistemom zaštite. U procesu analize pretnji, upravljanje ljudima, informacijama i drugim reusrsima je bitan faktor uspeha u svakoj organizaciji. U Tabeli 3 predstavljeni su neki od IKT objekata, kritičnih informacionih objekata i potencijalnih pretnji za identifikovane objekte. Proces analize pretnji značajan je za razumevanje *objekata zaštite*, tj. onoga što organizacija štiti, ili želi da zaštiti, [114].

Tabela 3. Analiza pretnji

Ključni posao	Opis	Objekti IKT	Značajni informacijski objekti	Pretnje
Servisi	Može uključiti poslovni ili tehnički konsalting Razvoj kompetencija i javnog servisa i.t.d.	Ljudi, hardver, softver, informacije, sistemi	Patenti, autorska prava, trgovačke tajne, zaštitni znak, projekat, poslovni plan, upravljačke informacije, informacije o kupcima	Gubitak, modifikacija, otkrivanje, oštećenje, prekid
Proizvodi	Može uključiti sisteme, prenosne puteve i računarske mreže	Ljudi, hardver, softver, informacije, sistemi	Patenti, autorska prava, trgovačke tajne, zaštitni znak, projekat, informacije o kupcima	Gubitak, modifikacija, otkrivanje, oštećenje, prekid
Upravljačke funkcije	Upravljačke informacije	Ljudi, hardver, softver, informacije, sistemi	Poslovni/strategijski plan, finansijski IS, plate, informacije o snabdevačima, komunikacije org., partneri, ljudski resursi, informacije/baze klijenata	Gubitak, modifikacija, otkrivanje, oštećenje, prekid

U Tabeli 4 predstavljeni su *agenti pretnji* – izvršioci napada, čije razumevanje je od presudnog značaja za razvoj strategije za suzbijanje pretnji. Najopasniji agent pretnji za bezbednost IKT sistema je ljudski faktor, kojeg treba primarno analizirati u svakoj proceni pretnji. Za analizu ovog faktora pretnji korisni su sistemsko-holistički i SBC modeli, korisni za razvoj PP koji obuhvata bezbednosne probleme okruženja.

Tabela 4. Agenti pretnje

Agent pretnje	Definicija
Čovek	Ljudi mogu biti pretnja neovlašćeno pristupajući mreži (logički ili fizički), slučajno ili namerno
Kvar sistema	Pretnje se odnose na IKT sistem organizacije. Primeri su defekti hardvera i softvera, odbijanje servisa (DOS napadi), maliciozni kodovi, virusi, trojanci i drugi problemi koji se odnose na sistem, kao što su preplavlivanje bafera, problem određenosti u generatoru slučajnog niza brojeva i.t.d.
Vanredni događaj	Pretnje u ovoj klasi su izvan uticaja i kontrole organizacije, a uključuju, prirodne katastrofe (zemljotres, grom i sl.), terorizam, kvarove vodovoda, el. napajanja i sl.

5. Mapiranje i prioritizacija faktora rizika za digitalni sertifikat

U Tabeli 5 predstavljeni su neki primeri metričkog mapiranja SSE CMM OP02: *Procena uticaja faktora rizika* za digitalni sertifikat (DS) i verovatnoće njihove pojave. Ako je verovatnoća pojave rizičnih događaja *visoka* i uticaj rizika *visok*, takav faktor rizika mora se smatrati *kritičnim* i mora se planirati visok bezbednosni nivo funkcija zaštite za ublažavanje tog rizika. Prioriteti ublažavanja rizika mogu se odrediti grupisanjem faktora rizika u grupu **glavnih** (ključnih, kritičnih) sa visokom verovatnoćom pojave i visokim uticajem i **sekundarnih**, ili nisko-prioritetnih faktora rizika sa niskom verovatnoćom i uticajem. U periodu važnosti DS uticaj rizika je katastrofalan i verovatnoća je *visoka*, zato što se u toku vremena teško može predvideti kada verifikacija DS neće uspeti. Uticaj je katastrofalan zato što DS, koji se koristi izvan perioda važnosti znači zloupotrebu i kompromitaciju poverljivosti. Ako su kodiranja imena izdavača DS i subjekta izvršena propisno, rizik od verovatnoće događanja ovog incidenta je minimalan, [114].

Tabela 5. OP02: Procena faktora rizika za DS-mapiranje i prioritetizacija

Faktori rizika za digitalni sertifikat	Uticaj rizika				Verovatnoća rizika		
(Primeri iz RFC 3280)	Metrika				Metrika		
	Nesreća	Značajno	Malo	Beznačajno	V	S	N
Greška u verifikaciji potpisa	X					X	
Greška u verifikaciji imena izdavača	X						X
Greška u verifikaciji imena subjekta	X						X
Greška u verifikaciji perioda validnosti	X				X		
Greška u verifikaciji jedinstvenog ID izdavača		X					X
Greška u verifikaciji jedinstvenog ID subjekta		X					X
Greška u verifikaciji identifikatora ključa CA		X					X
Greška u verifikaciji identifikatora ključeva subjekata		X					X

6. Bezbednosne funkcije, servisi zaštite i bezbednosni nivoi

U Tabeli 6, [114], sumirane su neke bezbednosne funkcije PKI aplikacija DS, kritične za procesiranje DS u skladu sa bezbednosnim ciljem. Bezbednosne funkcije su bazirane na [86] i PKIX2002, [2] i identifikovane korišćenjem metrike CC standarda. Pripisivanje EAL nivoa bezbednosnim funkcijama X.509 DS zavisi od okruženja, ili PKI aplikacije koja verifikuje DS. EAL nivoi se mogu razlikovati u zavisnosti od oblasti primene DS u: finansijama, obrazovnoj ustanovi, ili drugom okruženju. Međutim, indikatori nivoa bezbednosti-EAL za *verifikaciju digitalnog potpisa, ime izdavača (CA), ime subjekta i period validnosti DS, jedinstveni ID izdavača i subjekta i verifikacija politike sertifikacije (CP)*, **kritični su** faktori za validnost DS. EAL se koriste za verifikaciju povezanosti subjekta i DS, koja je presudna za međusobno poverenje korisnika u PKI sistemu. Preporučljivo je da se bezbednost ovih funkcija održava na **visokom** nivou u svim aplikacijama i okruženjima PKI sistema.

Tabela 6. Zavisnost servisa zaštite od bezbednosnih funkcija i nivoa bezbednosti

Br.	Bezbednosne funkcije aplikacija PKI sistema	Pretnja za servis zaštite						Bezb.nivo (EAL)			
		I	P	A	R	AC	N	B	O	S	V
1	Verifikacija serijskog broja sertifikata								X		
2	Verifikacija potpisa	X	X	X		X	X				X
3	Verifikacija imena izdavača	X	X	X		X	X				X
4	Verifikacija imena subjekta	X	X	X		X	X				X
5	Verifikacija perioda validnosti		X	X		X	X				X
6	Verifikacija jedinstvenog ID izdavača		X	X		X	X				X
7	Verifikacija jedinstvenog ID subjekta		X	X		X	X				X
8	Verifikacija identifikatora ključa CA					X				X	
9	Verifikacija identifikatora ključeva subjekata					X			X		
10	Verifikacija korišćenja ključa		X			X	X			X	
11	Verifikacija politike sertifikacije		X			X	X				X
12	Verifikacija mapiranja politike		X			X	X			X	

Br.	Bezbednosne funkcije aplikacija PKI sistema	Pretnja za servis zaštite						Bezb.nivo (EAL)		
13	Verifikacija alternativnog imena subjekta			X		X	X			X
14	Verifikacija alternativnog imena izdavača			X		X	X			X
15	Ograničenja imena		X				X			X
Legenda: I-integritet, P-poverljivost, A-autentifikacija, R-raspoloživost, AC-kontrola pristupa, N-neporecivost; B-beznačajan, O-osnovni, S-srednji, H, visok										

7. Socijalni i etički aspekti bezbednosti sistema

Ljudi kao kritični objekat IKT sistema, najteži su objekti za upravljanje u procesu zaštite IKT sistema [97]. Pažnju treba usmeriti na etička pitanja, korisničku prihvatljivost i prilagođavanje korisnika sistemu, ili korisničko usvajanje sistema i percepciju korisnika o bezbednosnom riziku u IKT sistemu. Ovi ciljevi mogu se postići korišćenjem instrumenta *Upitnika* i prikupljanjem informacija iz uzorkovanih organizacija (državnih, finansijskih, zdravstvenih i akademskih institucija). Uključivanje sociološko/kulturološkog aspekta u proces razvoja PP, odlučujući je faktor koji čini razliku između sistema u razvijanju i razvijenog IKT sistema. U ovoj evaluaciji kao metrika koristi se *broj ljudi i potrebno vreme*, za postizanje korisničke prihvatljivosti IKT sistema i sistema zaštite. Određena metrika (*procenat*) koristi se za merenje šta ljudi smatraju etičkim, a šta ne-etičkim ponašanjem, ili zloupotrebama i kompjuterskim kriminalom u IKT okruženju.

8. Metrika politika zaštite PKI sistema

U Tabeli 6 prikazane su metrike koje se odnose na politike zaštite u PKI sistemu. U procesu razvoja PP, politika zaštite utiče na postavljanje zahteva za PP. Zbog toga, metrike postojećih politika zaštite treba da se izuči da bi se odredila pogodnost politike kao baze na koju će se PP oslanjati. CC i SSE CMM modeli dokazali su prednosti za razvoj bezbednosnih funkcija i njihovih metrika. Međutim, da bi se izučila sociološka komponenta IKT sistema, sistemsko-holistički pristup i SBC modeli postaju pogodniji. Ovi modeli mogu obuhvatiti prevare i kako i zašto ljudi zloupotrebljavaju, ne veruju, ne razumeju i sl. IKT i sisteme zaštite. Ključna pretpostavka je da metodologija razvoja PP koja se primenjuje na sistem u razvoju i realnom okruženju, proizvodi adekvatniji PP, nego da se koristi PP razvijen za razvijeni sistem i različito okruženje. Uticaj faktora rizika i metrika koja je predstavljena u Tabeli 6, donekle je subjektivna zato što procena da je incident katastrofalan i da će se dogoditi kroz 2, ili 10 godina, zavisi od okruženja, vremena i organizacionih faktora, [114].

Značaj razvoja **standardnih** PP zahteva za PKI digitalni sertifikat time je veći, što se brojne zemlje u kojima su PKI sistemi u razvoju, sve više umrežavaju sa zemljama u kojima su PKI sistemi već razvijeni, pa uspostavljeni ovi zahtevi omogućavaju lakše umrežavanje, dok drugi faktori kao što su zakonski okviri, etički, kriminološki, atidunalni, tehnološki i prihvatljivost korisnika, ostaju vrlo različiti. Standardizovan i široko prihvaćen zahtev za PP PKI sertifikata mogao bi ublažiti, ili ukloniti neke od pomenutih prepreka, koje su posebno vidljive u oblasti transnacionalne istrage kompjuterskog kriminala.

