

UNIVERZITET SINGIDUNUM



Departman za poslediplomske studije

Master studije

Branislav Obradović

IMPLEMENTACIJA ERP-a UZ PRIMENU BEZBEDNOSNIH ISO STANDARDA

- Master rad -

Beograd, 2009.

UNIVERZITET SINGIDUNUM



Departman za poslediplomske studije

Master studije

IMPLEMENTACIJA ERP-a UZ PRIMENU BEZBEDNOSNIH ISO STANDARDA

- Master rad -

Mentor:
Prof .dr Milan Milosavljević

Student:
Branislav Obradović
Br. indeksa: M9383/08

UNIVERZITET SINGIDUNUM



Departman za posleddiplomske studije Master studije

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

STUDIJSKI PROGRAM: Savremene informaciono komunikacione tehnologije

Kandidat: Branislav Obradović

Broj indeksa: M9383/08

Tema: IMPLEMENTACIJA ERP-a UZ PRIMENU BEZBEDNOSNIH ISO STANDARDA

Zadatak: Uraditi prikaz primene standarda koji se koriste u oblasti bezbednosti IKT kroz proces implementacije ERP-a u privrednom subjektu.

MENTOR

Prof. dr Milan Milosavljević

SADRŽAJ:

1. Predgovor – organizacije za standardizaciju

2. Uvod

2.1. Definicija standarda i atributi kvaliteta standarda

2.2. Klasifikacija standarda zaštite

3. Predmet standarda

3.1 Sigurnost informacija

3.2 Informacioni resursi koje treba zaštititi

4. Pregled ISO standarda u oblasti IKT

4.1. Pisani i nepisani standardi

4.2. *De facto* i *De jure* standardi

4.3. Vojni standardi iz kojih proizilaze ISO standardi

4.4. Aktuelni ISO standardi i njihova međusobna povezanost

4.5. Standardi koji se ne koriste

4.6. Standardi u razvoju

5. Sigurnosni standardi i programi sertifikacije

6. Prikaz implementacije ERP-a uz primenu bezbednosnih ISO standarda

7. Zaključak

8. Literatura

1. PREDGOVOR – ORGANIZACIJE ZA STANDARDIZACIJU

Organizacija pionir u standardizaciji IKT je britansko nacionalno telo za standardizaciju BSI (engl. *British Standards Institution*) pod čijim okriljem su sredinom devedesetih godina prošlog veka nastali prvi standardi BS 7799-1 i BS 7799-2. Razvoj ovih standarda je od dve hiljadite godine preuzela Međunarodna organizacija za standardizaciju ISO sa Međunarodnom komisijom za elektrotehniku IEC kroz zajednički tehnički komitet (ISO/IEC JTC1) što čini specijalizovani sistem svetske standardizacije. Nacionalna tela koja su članovi organizacija ISO i IEC učestvuju u izradi međunarodnih standarda kroz tehnički komitet da bi se bavili pojedinim poljima tehničkih aktivnosti od zajedničkog interesa. Ostale vladine i nevladine međunarodne organizacije takođe sarađuju sa ISO i IEC. Nacrti međunarodnih standarda koje usvaja ovaj združeni tehnički komitet, izrađuju se u skladu sa pravilima datim u Direktivama ISO/IEC i dostavljaju nacionalnim telima radi glasanja. Za objavljivanje međunarodnog standarda potrebno je da ga odobri 75% nacionalnih tela koja su glasala.

Područje rada ISO/IEC JTC1:

- standardizacija u oblasti informacionih tehnologija
- utvrđivanje, projektovanje i razvoj sistema i alata koji se odnose na preuzimanje, predstavljanje, obradu, sigurnost i zaštitu, prenošenje, međusobno povezivanje, upravljanje, organizovanje, skladištenje i pretraživanje informacija

Do danas su publikovana 2104 dokumenta dok se rad odvija na donošenju 490 novih. U okviru ISO/IEC JTC1 radi stalni komitet SC27 (ISO/IEC JTC1/SC27 "IT Security Technique"), u kome su formirane 3 radne grupe:

- WG 1 Requirements, security and guidelines (moderator BSI),
- WG 2 Security Techniques and mechanisms (moderator IBM),
- WG 3 Security evaluation criteria (moderator SIS),

i 17 potkomiteta od kojih su najznačajniji:

SC 06 - telekomunikacije i razmena informacija među sistemima,

SC 07 - softverski i sistemski inženjering,

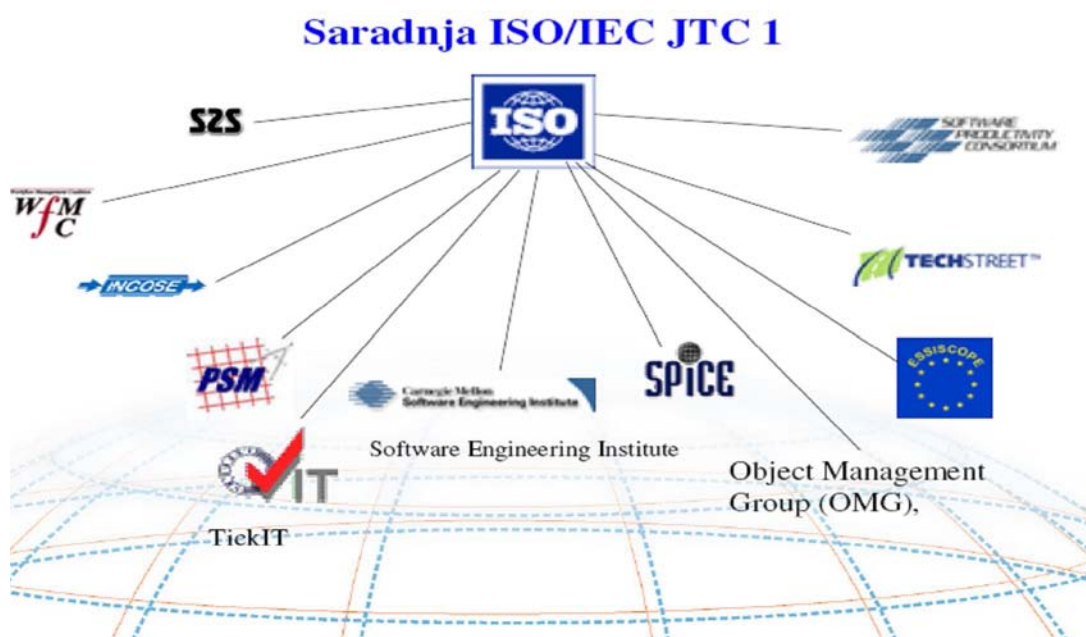
SC 17 - kartice i lična identifikacija,

SC 25 - međusobno povezivanje uređaja za informacione tehnologije,

SC 27 - postupci zaštite u informacionim tehnologijama,

SC 31 - postupci automatizovanog identifikovanja i preuzimanja podataka.

Postoji mogućnost da neki elementi međunarodnih standarda mogu da podležu patentnim pravima. Organizacije ISO i IEC se ne mogu smatrati obaveznim za identifikovanje bilo kojih ili svih takvih patentnih prava. Slika br.1. daje prikaz institucija sa kojima ISO/IEC JTC1 sarađuje pri kreiranju i izradi dokumenata:



Slika br.1.

Osim britanskog nacionalnog tela za standardizaciju *BSI*, standardi sledećih institucija su opšte prihvaćeni kao standardi za bezbednost i zaštitu u pojedinim oblastima IKT:

- National Institute of Standards and Technology (NIST),
- Internet Architecture Board (IAB),
- Internet Engineering Task Force (IETF),
- Internet Engineering Steering Group (IESG),
- Visa i Master Card International,
- American National Standards Institute (ANSI)
- CESG (Communications-Electronics Security Group),
- Information Systems Security (INFOSEC),
- ITU (International Telecommunications Union),
- CISCO,
- OASIS,
- UN/CEFACT, i druge.

U Republici Srbiji poslove u vezi sa donošenjem srpskih standarda i srodnih dokumenata, kao i druge poslove koji su povezani sa standardima i standardizacijom obavlja Institut za standardizaciju republike Srbije. Delatnost Instituta utvrđena je Zakonom o standardizaciji („Službeni list Srbije i Crne Gore”, br. 44/2005), Odlukom o osnivanju Instituta za standardizaciju Srbije („Službeni glasnik Republike Srbije”, br. 16/2007) i Statutom Instituta („Službeni glasnik Republike Srbije”, br. 79/2007), na koji je Vlada Republike Srbije dala saglasnost 2. avgusta 2007. godine („Službeni glasnik Republike Srbije”, br. 73/2007). Prema tim dokumentima, Institut obavlja sledeće poslove:

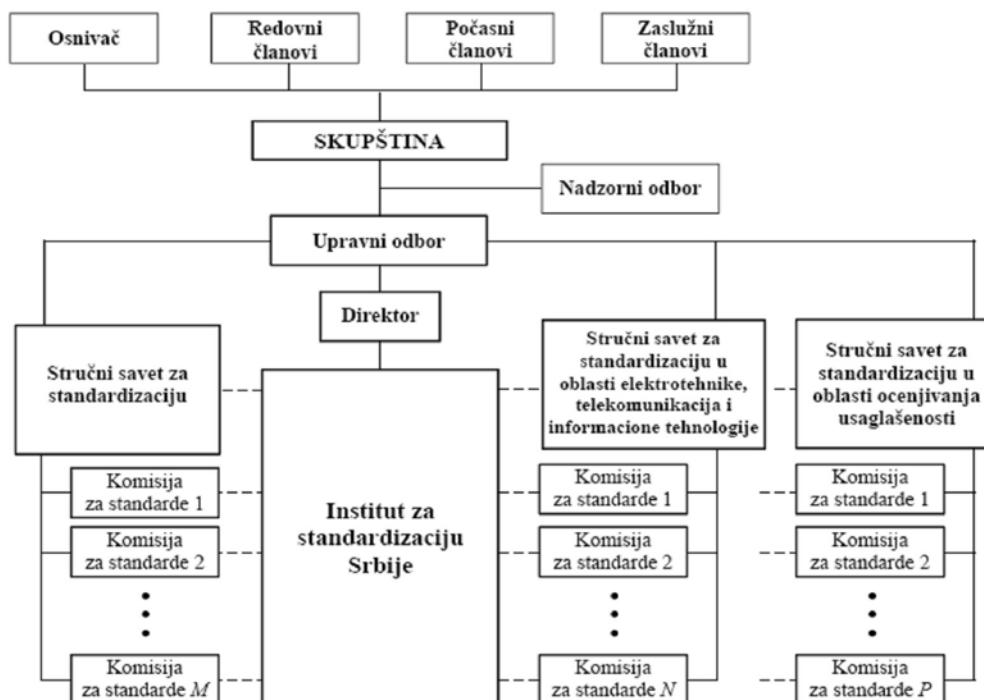
1. donosi, razvija, preispituje, menja, dopunjuje i povlači srpske standarde i srodne dokumente;

2. obezbeđuje usaglašenost srpskih standarda i srodnih dokumenata sa evropskim i međunarodnim standardima i srodnim dokumentima;
3. vodi registar srpskih standarda i srodnih dokumenata, obuhvatajući sve faze razvoja;
4. učestvuje u izradi i preispitivanju evropskih i međunarodnih standarda i srodnih dokumenata koje donose evropske i međunarodne organizacije za standardizaciju u oblastima za koje postoje potrebe i interesi Republike Srbije, a za koje se očekuje preispitivanje ili donošenje srpskih standarda i srodnih dokumenata;
5. sarađuje sa evropskim i međunarodnim organizacijama za standardizaciju i nacionalnim telima za standardizaciju zemalja potpisnica odgovarajućih sporazuma iz oblasti standardizacije;
6. izvršava druge zadatke u skladu sa obavezama iz međunarodnih ugovora u oblasti standardizacije koji obavezuju Republiku Srbiju;
7. obezbeđuje dostupnost javnosti srpskih standarda, srodnih dokumenata, publikacija, kao i standarda i publikacija odgovarajućih evropskih i međunarodnih organizacija i drugih zemalja i vrši njihovu prodaju;
8. daje osnovu za izradu tehničkih propisa;
9. priprema programe i godišnje planove donošenja srpskih standarda;
10. deluje kao informacioni centar, u skladu sa zahtevima predviđenim odgovarajućim međunarodnim sporazumima i obavezama koje proizilaze iz članstva u odgovarajućim evropskim i međunarodnim organizacijama za standardizaciju;
11. predstavlja i zastupa interese Republike Srbije u oblasti standardizacije u evropskim i međunarodnim organizacijama za standardizaciju, kao i u njihovim telima;
12. odobrava upotrebu znaka usaglašenosti sa srpskim standardima i srodnim dokumentima u skladu sa svojim pravilima;
13. promoviše primenu srpskih standarda i srodnih dokumenata;
14. obavlja i druge poslove iz oblasti standardizacije u skladu sa zakonom, aktom o osnivanju i statutom.

Komisije za standarde su osnovna tehnička radna tela u kojima se odvija stručni rad Instituta. Po potrebi, komisije za standarde mogu osnivati potkomisije, radne grupe i druga stalna i povremena tehnička radna tela. Za izradu srpskih standarda i srodnih dokumenata u specifičnim oblastima, Institut može da angažuje specijalizovane organizacije i asocijacije, u skladu sa svojim pravilima.

Sertifikacija sistema menadžmenta kvalitetom (prema standardu SRPS ISO 9001), sistema menadžmenta zaštitom životne sredine (prema standardu SRPS ISO 14001) i drugih sistema menadžmenta (prema standardima OHSAS 18001 i SRPS ISO 22000, odnosno prema standardima sa posebnim zahtevima za primenu standarda SRPS ISO 9001 u pojedinim oblastima, jeste dobrovoljna aktivnost, koju Institut obavlja na zahtev klijenata, na komercijalnoj osnovi. U ranijem periodu sertifikaciju sistema menadžmenta, Institut (u to vreme Zavod za standardizaciju), je obavljao na osnovu Uredbe o unutrašnjoj organizaciji i sistematizaciji radnih mesta u ministarstvima, organizacijama i službama Saveta ministara („Službeni list Srbije i Crne Gore”, br. 25/2003) od 13. juna 2003. godine.

Organi Instituta su: Skupština, Upravni odbor, Nadzorni odbor, direktor i stručni saveti.



Slika br.2 Organizaciona šema Instituta za standardizaciju republike Srbije

2. UVOD

2.1. Definicija standarda

Standard zaštite je usvojen i objavljen dokument koji uspostavlja specifikaciju i procedure dizajnirane da obezbede da dokumenta, materijal, proizvod, metod ili servis zaštite odgovara njegovoj nameni i konzistentno izvršava svoje predviđene funkcije. U praksi standard zaštite sadrži čitav set aranžmana za pokrivanje svih (ili što većeg broja) bezbednosnih zahteva za održavanje rizika na prihvatljivom nivou. U oblasti zaštite, standardi obezbeđuju objektivne mere na koje se konstruktori, inženjeri i prodavci mogu osloniti u razvoju i implementaciji sistema za zaštitu. Standard je glavni alat za poboljšanje kvaliteta i efikasnosti kontrola zaštite apliciranih u IKT sistemu organizacije, i može se koristiti za: povećanje nivoa bezbednosti i zaštite, integrisanje delova standarda u poslovne procese, procenu kvaliteta sistema zaštite, izbor kontrola sistema zaštite, poboljšanje programa obrazovanja, obuku i podizanje svesti o potrebi zaštite.

- **Bitni atributi kvaliteta standarda su da je:**

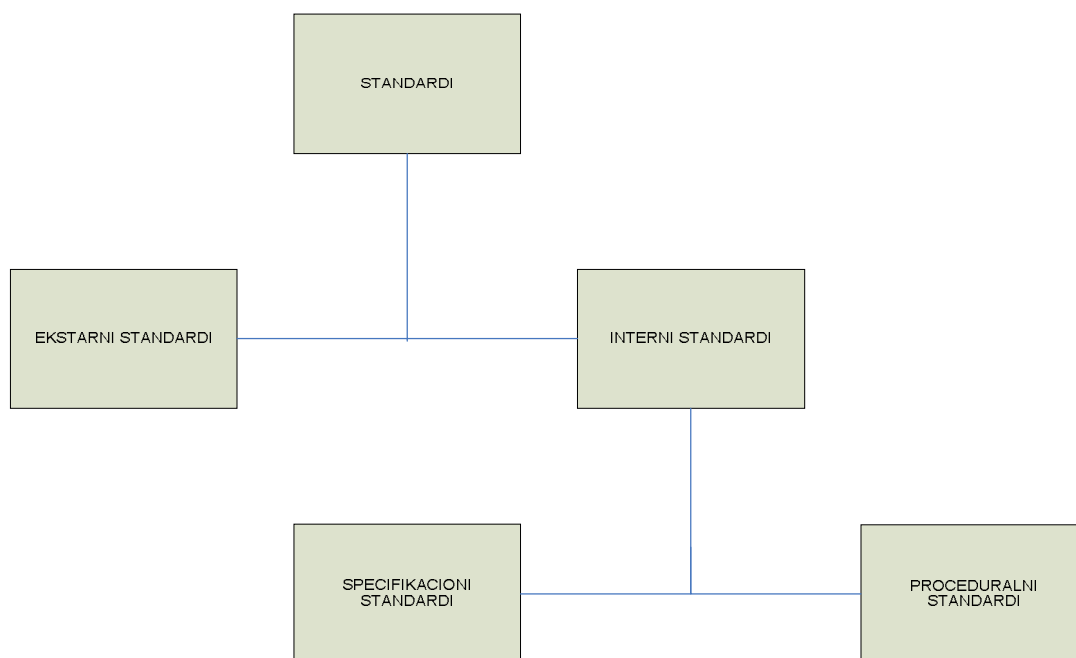
- dokumentovan
- izdat od strane prihvaćenog nacionalnog tela za standardizaciju
- usaglašen sa zakonima i međunarodnim ugovorima
- adekvatan nameni
- rentabilan
- namenjen za zajedničko i ponovno korišćenje
- primena mu je dobrovoljna
- ustanovljen od svih zainteresovanih strana
- sveobuhvatan (tehnoške, procesne i ljudske aktivnosti)

Potreba za standardima i standardizacijom u IKT neophodna je radi:

- definisanja zajedničkog okvira koji će omogućiti da svi koji su uključeni u proces razvoja, projektovanja i upravljanja softverom "govore istim jezikom"
- obezbeđivanja osnove za komunikaciju između IS
- obezbeđivanja preduslova za zajedničko učešće na projektima različitih strana
- obezbeđivanje potrebnog okvira za razvoj i implementaciju softvera definisanog kvaliteta

2.2. Klasifikacija standarda zaštite

U opštem slučaju uobičajena klasifikacija standarda zaštite je na: **eksterne i interne** (slika br.3)



Slika br.3

Eksterni (industrijski) standardi, razvijeni su i šire prihvaćeni. Namenjeni su (ali ne samo) za: upravljanje sistemom zaštite, analizu rizika, obuku, evaluaciju sistema i proizvoda zaštite i specifikaciju i akreditaciju.

Interne standarde organizacije razvijaju samostalno prema svojoj bezbednosnoj politici i potrebama.

Specifikacioni interni standardi definišu sistem osnovne zaštite za datu konfiguraciju IKT sistema. Svaka organizacija definiše ovaj standard na bazi teoretskih razmatranja i izbora osnovnih kontrola zaštite (engl. *Baseline*) iz kataloga kontrola za najbolju praksu zaštite. Ovaj sistem osnovnih kontrola zaštite mora se u fazi razvoja i implementacije dopuniti sa novim kontrolama zaštite specifičnih za sistem i okruženje, a na bazi rezultata analize rizika.

Proceduralni interni standardi su korisni mehanizmi za opisivanje procedura za administraciju zaštite i treba da uključuju samo važne korake bez tehničkih detalja. Uglavnom su generički i nisu specifični za IS (platformu). Detalji se opisuju u tehničkoj dokumentaciji za uređaje/sisteme.

Prednosti eksternih u odnosu na interno razvijene su što obezbeđuju: više testiranja softvera zaštite koji implementiraju ove standarde u praksi, lakše otkrivanje i brže fiksiranje bezbednosnih problema i bržu razmenu iskustva iz prakse zaštite.

3. PREDMET BEZBEDNOSNIH IT STANDARDA

3.1 Sigurnost informacija

Šta se podrazumeva pod sigurnošću informacija?

Bezbednost (engl. *Security*) je stanje sistema u odnosu na okolinu ali i na samog sebe. Bezbednost je stanje u kome su isključeni protivpravni akti, ili ukoliko ovakvi akti i postoje, oni su vrlo retki i protiv njih se preduzimaju energične efikasne sankcije. Bezbednost se u odnosu na suštinu i stvarno značenje može definisati kao *stanje*, organizacija i funkcija.

Sigurnost je stanje, osobina onoga koji je siguran, onoga što je sigurno, u kome nekome ili nečemu ne pretila opasnost, odsutnost opasnosti, bezbednost.

U kontekstu *stanja* sistema prihvata se da sigurnost ima isto značenje kao i bezbednost. Bezbednost se ostvaruje zaštitnim (zaštitom) merama: preventivnim i represivnim (sanacionim) merama.

Prema tome, Zaštita (engl. *Protection*) je skup mera (postupaka) koje imaju za cilj određeni (viši) nivo bezbednosti.

Informacije predstavljaju određenu imovinu, koja kao i druga važna poslovna imovina, za neku organizaciju ima vrednost i otuda je potrebno da se ona odgovarajuće zaštiti. Sigurnošću se informacije štite od širokog opsega pretnji kako bi se osigurao kontinuitet poslovanja, na minimum sveli gubici u poslovanju i na maksimum podigao dobitak od investicija i šansi u poslovanju.

Informacije mogu postojati u mnogo oblika i formi: otšampane ili ispisane na papiru, uskladištene u elektronskom obliku, mogu se slati poštom ili primenom elektronskih sredstava, prikazati na korporacijskom web sajtu, prikazati na filmu, ili izreći u razgovoru. Bilo koji oblik da informacije imaju, ili sredstvo preko kojeg se one zajednički koriste ili na kojem se čuvaju, moraju se odgovarajuće zaštititi.

Sigurnost informacija se karakteriše kao čuvanje sledećih komponenti sigurnosti (Sl. br.3):

- poverljivosti: osiguravanjem da informacije budu na raspolaganju samo onima koji su ovlašćeni da im pristupaju;
- integriteta: samozaštitom tačnosti i celovitosti informacija i metoda za obradu;
- raspoloživosti: osiguravanjem da ovlašćeni korisnici imaju pristup informacijama i pripadajućoj imovini kada im je potrebno,

kao i sprečavanje gubitka **celovitosti** i **raspoloživosti** samih sistema.



Slika br.4

Sigurnost informacija se ostvaruje uvođenjem pogodnog skupa kontrola, koje mogu biti politika, praksa, procedure, organizacione strukture i softverske funkcije. Ove kontrole treba uspostaviti kako bi se u organizaciji osiguralo ispunjavanje specifičnih ciljeva zaštite. Sigurnosne mere uključuju **mehanizme** i **procedure** koje se implementiraju u cilju:

- odvrćanja,
- prevencije,
- detekcije, i
- opravke

od uticaja **incidentnih događaja** a koji deluju na **poverljivost**, **celovitost** i **raspoloživost** podataka i odgovarajućih servisa i resursa uključujući izveštavanje o sigurnosnim incidentima. Sigurnost informacija je ustvari proces upravljanja rizikom. Upravljanje sigurnošću bi trebao da bude deo ukupnog upravljanja rizicima a sigurnost informacija je samo jedan aspekt ukupne sigurnosti organizacije.

- Zašto je potrebna zaštita informacija?

Informacije i postupci podrške, sistemi i mreže, predstavljaju važnu poslovnu imovinu. Poverljivost, integritet i raspoloživost informacija mogu biti od presudne važnosti za održanje na granici konkurentnosti, gotovinskih tokova, isplativosti, pravne usaglašenosti i poslovnog ugleda.

Organizacije i njihovi informacioni sistemi suočavaju se, uz tendenciju porasta, sa pretnjama sigurnosti iz širokog opsega izvora, uključujući prevare uz korišćenje računara, špijuniranje, sabotaze, vandalizme, požare ili poplave. Izvori oštećenja kao što su računarski virusi, kao i napadi probijanja u računare i odbijanja aktiviranja funkcija postali su češći, ambiciozniji i usavršeniji.

Zavisnost od informacionih sistema i usluga znači da su organizacije znatno ranjivije u odnosu na pretnje po sigurnost. Uzajamno povezivanje javnih i privatnih mreža kao i zajedničko korišćenje informacionih resursa otežava ostvarivanje kontrolisanja pristupa informacijama.

Osnovni ciljevi zaštite informacija u nekoj organizaciji su da se obezbedi:

- kontinuitet poslovanja i
- minimiziraju rizici od potencijalnih šteta (havarija)

Ovo se postiže prevencijom incidentnih događaja i redukovanjem njihovog potencijalnog uticaja. Definisanje, implementacija, održavanje i unapređenje koncepta sigurnosti informacija može biti od presudne važnosti za ostvarivanje i održavanje konkurentnosti, dotoka novčanih sredstava i obezbeđenja profitabilnosti, kao i zadovoljenja zakonskih odredbi i osiguranja poslovnog ugleda organizacije. Sigurnost informacija je podjednako važna malim i velikim kao i javnim i privatnim organizacijama. U takvim uslovima oblici centralizovane kontrole nisu delotvorni. Odnosno, primena tehničkih rešenja, odgovarajuće opreme i proizvoda više nije dovoljna da bi osigurala odgovarajuće upravljanje sigurnošću informacija. Sigurnost informacija nije isključivi problem informaciono komunikacionih tehnologija (IKT) već je to "poslovni" problem. Opšte je mišljenje da se primenom odgovarajućih tehnologija rešava samo jedan deo problema sigurnosti informacija. Danas se sigurnost informacija postiže primenom odgovarajućih **kontrola**, koje se odnose na politiku sigurnosti, poslovne procese, procedure, strukturu organizacije i funkcije hardvera i softvera (sistemskog i aplikativnog).

Kontrole važne za organizaciju sa zakonske tačke gledišta su:

- a) zaštita informacija i tajnosti ličnih podataka;
- b) čuvanje organizacionih izveštaja;
- c) poštovanje prava intelektualnog vlasništva.

Kontrole koje u praksi postižu dobre rezultate kod implementacije koncepta sigurnosti informacija su:

- a) sigurnosna politika;
- b) raspodela odgovornosti za sigurnost informacija;
- c) svest o neophodnosti zaštite informacija, obrazovanje i obuka zaposlenih;
- d) ispravno procesiranje podataka u aplikacijama;
- e) upravljanje ranjivostima (slabostima) informacionih resursa;
- f) upravljanje kontinuitetom poslovanja;
- g) upravljanje sigurnosnim incidentima i unapređenje sistema.

Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, preispitivati i unapređivati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahteva organizacije.

3.2 Informacioni resursi koje treba zaštititi

Nezavisno od prirode, informacioni resursi (informacione vrednosti) mogu da imaju jednu ili više sledećih karakteristika:

- Prepoznati su na nivou organizacije kao entitet koji ima vrednost;
- Ne mogu lako da budu zamenjeni bez utroška resursa kao što su: novac, veštine zaposlenih, vreme itd;
- Čine identitet organizacije bez koga poslovanje organizacije može da bude ugroženo.

U tabeli br.1 dat je prikaz informacionih resursa koje je neophodno zaštititi da bi se obezbedili osnovni ciljevi zaštite informacija (kontinuitet poslovanja i minimiziranje rizika od potencijalnih šteta).

Tabela br.1 Kategorije informacionih resursa (vrednosti) koje je neophodno zaštititi

Kategorije informacionih resursa (vrednosti)	Šta se štiti
Informacije	Baze podataka i podaci, dokumenta vezana za sistem, Korisnički priručnici, materijali za obuku, operativne i sistemske procedure, Planovi kontinuiteta, sistem zapisa
Softver	Aplikativni i sistemski, alati za razvoj softvera
Fizički resursi - hardver(kompjuterska oprema)	Kompjuterski uređaji (procesori, monitori, laptopovi, mobilni računari), Komunikacioni uređaji (ruteri, svičevi, modemi, telefoni), Medijumi (trake, diskovi), Ostali tehnički uređaji (sistemi napajanja, hlađenja itd.)
Usluge	Usluge obrade podataka, komunikacione usluge,
Osoblje	Znanje i veštine osoblja (tehničkog, operativnog, marketing).

Pretnje informacionim resursima u nekoj organizaciji predstavljaju:

- Zaposleni,
- Niska svest o potrebi zaštite informacija alata i virusa (korporativna kultura),
- Porast umreženosti i distribuirane obrade podataka,
- Porast složenosti i efektivnosti hakerskih napada,
- E-mail –ovi,
- Požar, poplava, zemljotres itd.

4. PREGLED ISO STANDARDA U OBLASTI IKT

4.1. Pisani i nepisani standardi

Pisani standardi su standardi koje, institucije za standardizaciju ili neki drugi subjekti, propisuju svojim članovima, zainteresovanim subjektima ili drugim organizacijama i subjektima, radi: utvrđivanja određenih normi ponašanja, postizanja određenog kvaliteta proizvoda, vršenja ili obavljanja usluga, određenih proizvodnih i tehnoloških postupaka ili postizanja drugih ciljeva. Korišćenje pisanih standarda može biti dobrovoljno ili propisano zakonima i drugim pravnim uredbama, ili nekim drugim pravnim aktima relevantnim za pripadnike (članove) određenih oblika organizovanja (poslovnih, strukovnih, sportskih...) Nepisani standardi su obično standardi opšte prihvaćeni kao iskustveni standardi ili strukovni standardi i njihova primena je neobavezujuća ali uobičajena u određenim sferama društva ili privrede.

4.2. De facto i De jure standardi

De facto standard je standard (formalni ili neformalni) koji je prihvaćen i koji je dostigao dominantnu poziciju. To je obično proizvod, proces, sistem ili tehnički standard koji je dostigao status neformalnim, opštim prihvatanjem ili tržišnim probojem, i po tradiciji se nastavlja njegovo korišćenje. *De facto* je latinski izraz koji znači „stvarni“ ili „u praksi“ ali nije određen zakonom. Često se koristi kao suprotnost *de jure* standardu koji je standard ustanovljen „po zakonu“. Kada se govori o pravnom aspektu, *de jure* određuje šta zakon propisuje, a *de facto* određuje stvarnost koja se događa u praksi.

4.3. Vojni standardi iz kojih proizilaze ISO standardi

Različite kombinacije nacionalnih i internacionalnih tela za standarde, vladinih organizacija, profesionalnih udruženja i drugih kvazi standardizacionih tela – od kojih svako telo ima uticaj na određeni sektor tržišta – objavili su tokom proteklih godina niz standarda za softver i sisteme, standarda procesa, modela zrelosti, preporučene prakse, uputstava i drugih tipova okvirnih dokumenata. Američko ministarstvo odbrane i američka vojska, objavili su niz standarda koji se odnose na oblast bezbednosti i zaštite IKT. Ovi standardi su kao obaveza nametnuti i drugim armijama članicama NATO pakta i kasnije su prihvaćeni u izvornoj ili prilagođenoj formi za civilnu upotrebu.

- Softverski standardi

US DoD (američko ministarstvo odbrane) je 1994-te objavilo MIL-STD-498 sa ciljem da jednim dokumentom obuhvati zahteve za razvoj softvera (DoD-STD-2167A), kvalitet softvera (DoD-STD-2168), i dokumentaciju (DoD-STD-7935A). Na bazi ovih standarda, združeni komitet IEEE-EIA sa minimalnim izmenama objavio je J-STD-016, koji je opisuje samo procese razvoja softvera.

Objavljivanjem ISO/IEC 12207 (1995) stavljeni su van upotrebe svi gore navedeni Mil-Std. US korisnici standarda su izdali IEEE/EIA 12207 – *Industrijska implementacija ISO/IEC 12207*, koji ima tri dela:

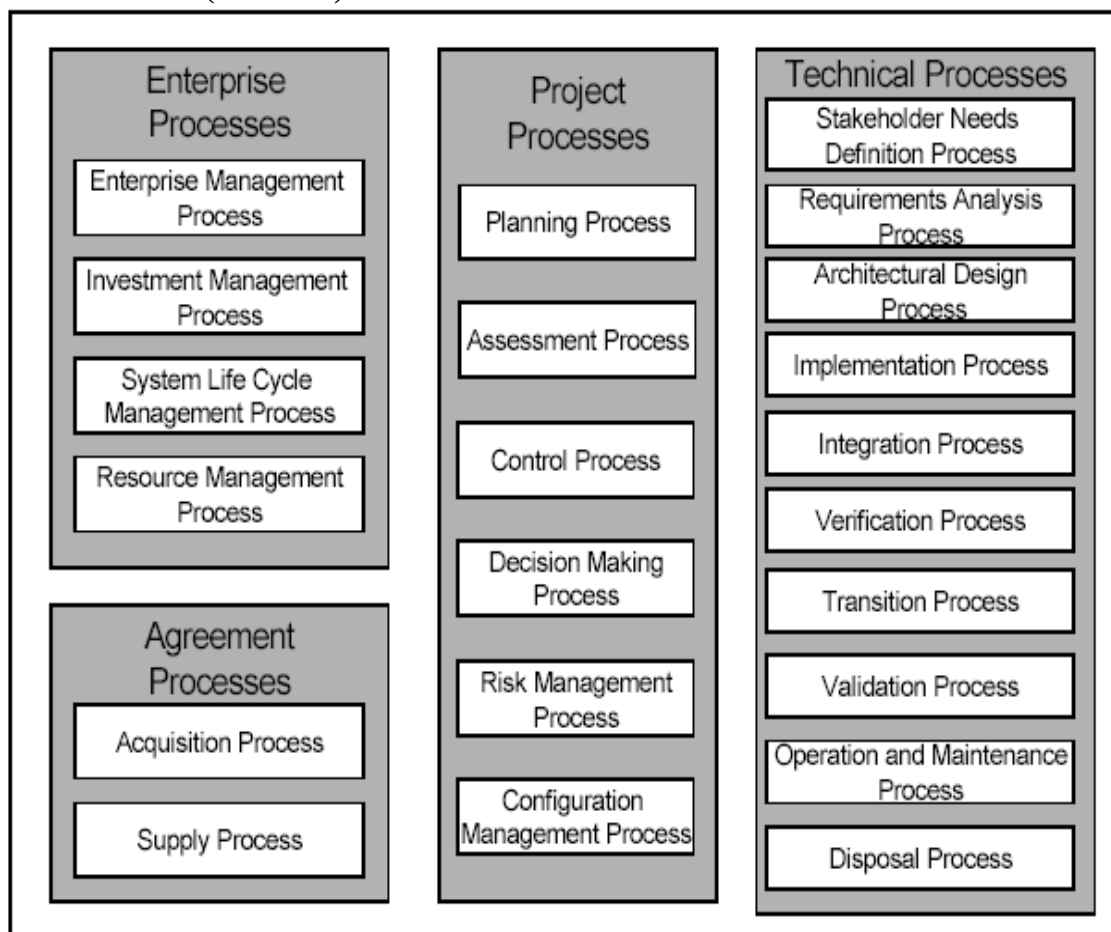
- IEEE/EIA12207.0 – ISO 12207 sa U.S. uvodom i 6 dopunskih appendiksa,
- IEEE/EIA12207.1 – Uputstvo o sadržaju dokumentacije (sumarni pregled sadržaja svakog tipa dokumenta),
- IEEE/EIA12207.2 – Uputstvo sa dodacima, alternativama i pristupima implementaciji, aktivnostima i zadacima ISO 12207.

Potreba da se adresira sigurnost avionskih sistema baziranih na softveru realizovana je kroz RTCA DO-178B, koji opisuje procese planiranja, razvoja, menadžmenta konfiguracijom, obezbeđenja kvaliteta i verifikacije primenjene na softver za različite nivoe sigurnosti.

- Standardi sistem inženjerstva

EIA 632 : 1994 interni standard je bio osnova za dva pravca razvoja, jedan je rezultirao punom verzijom standarda EIA 632:1988, a drugi u razvoj i primenu SECAM-a od strane INCOSE.

Jednovremeno je objavljen IEEE 1220, baziran na MIL-STD 499B i AT&T-System Engineering Manual. Standard definiše četiri grupe procesa razvoja sistemskog softvera. Ovi standardi su poslužili kao osnova za razvoj standarda za procese životnog ciklusa sistema ISO/IEC 15288. (slika br.5.)



Slika br.5 ISO-IEC 15288 procesi životnog ciklusa sistema

Namera je da ovaj standard na visom nivou sumira definicije procesa životnog ciklusa sistema počev od Mil-Std 499:1969, ...

- CMMI – Integrisani modeli zrelosti

Potreba da se da poseban naglasak na sigurnost sistema primorala je Federal Aviation Administration da 1997. izda svoj posebni integrisani CMM, pod nazivom FAA-iCMM.

- Vrednovanje zrelosti i sposobnosti

US Air Force je razvila SDCE-*Software Development Capability Evaluation* fokusirajući se na sposobnosti i slabosti organizacije koja konkuriše za određeni ugovor. Provera pored softverskih oblasti obuhvata i određene sistem inženjering oblasti i tehnološka pitanja u vezi predmetnog projekta

Kada je reč o CMMI, za interne provere namenjen je SCAMPI – *Standard CMMI Assessment Method for Process Improvement*.

- Standardi merenja

DoD i US Army sponzorirali su izradu PSM – *Practical Systems and Software Measurement*, obimnog priručnika koji sadrži smernice koje organizacije mogu koristiti da uspostave odgovarajuće programe merenja. Prvobitna namena bila je merenje softverskih procesa, u verziji 4, objavljenoj 2001, dodate su oblasti sistem inženjeringa i merenje procesa.

1980-tih Motorola je objavila Six Sigma, program inicijalno namenjen povećanju kvaliteta hardverskih sistema, koji sa danas rado primenjuje i na softverske sisteme.

Iako je objava vojnih standarda pokrenula točak istorije primenom ovih standarda i u civilnoj upotrebi, nekoliko verzija MIL-STD 499 objavljenih u 1992 i 1993, industrija nije prihvatila, što je rezultiralo inicijativom da se ukine praksa primene vojnih standarda gde god postoji komercijalna alternativa.

4.4 Aktuelni ISO standardi i njihova međusobna povezanost

Standard ISO/IEC 17799 - Pravila za primenu kod upravljanja zaštitom informacija (*Code of Practice*)

Standard sadrži dva dela:

- Prvi deo - Standard prakse, namenjen da pomogne implementaciju vlastitog sistema zaštite. Standard usmerava definisanje politike zaštite na nivou organizacije sa instrukcijom *šta* dokument treba da sadrži, ali ne nudi detalje *kako* se ta politika razvija i izrađuje.
- Drugi deo - ovog standarda je preuzeti BS7799. To je katalog dobre prakse zaštite koju treba izvršiti i specificira instrukcije za *sistem upravljanja zaštitom informacija* (ISMS). Zahtevi za ISMS obuhvataju: Obim, Politiku zaštite, Analizu rizika, Izjavu o primenljivosti, Sistem upravljanja razvojem/održavanjem zaštite i Dokumentaciju zaštite.

Struktura standarda:

1. Predmet i područje primene
2. Termin i definicije
3. Politika sigurnosti i zaštite
4. Sigurnost i zaštita u organizaciji
5. Klasifikovanje i kontrolisanje imovine
6. Sigurnost (pouzdanost) osoblja
7. Fizička zaštita i sigurnost okruženja

8. Upravljanje radom i komunikacijama
9. Kontrolisanje pristupa
10. Razvoj i održavanje sistema
11. Upravljanje kontinuitetom poslovanja
12. Usaglašenost

U standardima ISO/IEC 17799 i BS7799 - 2.deo usaglašene su (2002.god.) sledeće oblasti – zahtevi za ISMS (tabela br.2): politika zaštite, analiza rizika, Izjava o primenljivosti i sistem upravljanja.

Politika zaštite	Obim, Poverljivost, Integritet, Raspoloživost, Kontrolisana odgovornost Klasifikacija objekata zaštite, Analiza rizika, Normativ.-regul.okvir
Analiza rizika	Procena vrednosti (osetljivosti) objekata IKT sistema, Procena pretnji, Procena ranjivosti, i Procena uticaja faktora rizika
Izjava o primenljivosti	Identifikovanje aktuelnih kontrola zaštite, Razmatranje svih kontrola zaštite (128), uključujući ili isključujući neke od njih na osnovu preliminarnе procene Izbor primenljivih kontrola zaštite na osnovu analize rizika za poslovanje organizacije i informacije.
Upravljanje zaštitom	Regularne kontrolne liste koje kontrolišu da su: Kontrole zaštite - na svom mestu i efektivne, Preostali rizik - na prihvatljivom nivou i Procene vrednosti objekata, pretnji i ranjivosti - validne

Tabela br.2.

Standard ISO 9001:1994

1. Predmet standarda i područje primene

Ovim međunarodnim standardom se specificiraju zahtevi za sistem kvaliteta koji se koristi kada treba da bude pokazana sposobnost isporučioaca da projektuje i isporučuje usaglašen proizvod. Specificirani zahtevi imaju kao primarni cilj postizanje zadovoljenja kupca sprečavanjem neusaglašenosti u svim fazama, od projektovanja do servisiranja. Ovaj međunarodni standard se primenjuje u slučajevima kada se:

- a. zahteva projektovanje, a zahtevi za proizvod su iskazani uglavnom kao performansa ili ih treba utvrditi, i
- b. poverenje u usaglašenost proizvoda može postići odgovarajućim prikazivanjem sposobnosti isporučioaca za projektovanje, razvoj, proizvodnju, ugradnju i servisiranje.

2. Veza sa drugim standardima

Navedeni standard sadrži odredbe koje, putem pozivanja u ovom tekstu, sačinjavaju odredbe ovog međunarodnog standarda. Navedeno izdanje je bilo važeće u vreme štampanja ovog standarda. Svi standardi su podložni reviziji i strane koje ugovaraju na osnovu ovog međunarodnog standarda upućuju se na primenu najnovijeg izdanja dole navedenog standarda. Članice IEC i ISO održavaju registre važećih međunarodnih standarda.

3. Definicije

U ovom međunarodnom standardu se primenjuju definicije date u ISO 8402 i sledeće definicije: 3.1 Proizvod: rezultat aktivnosti ili procesa.

1. Proizvod može da obuhvati uslugu, hardver, procesne proizvode, softver ili njihovu kombinaciju.

2. Proizvod može biti materijalan (npr. sklopovi ili procesni proizvod) ili nematerijalan (npr. znanje ili pojmovi) ili njihova kombinacija.

3.2 Ponuda

3.3 Ugovor

4. Zahtevi za sistem kvaliteta

Najviše rukovodstvo mora da obezbedi da se na odgovarajućim funkcijama i nivoima unutar organizacije utvrde ciljevi kvaliteta, uključujući one potrebne za ispunjavanje zahteva za proizvod. Ciljevi kvaliteta moraju da budu merljivi i usklađeni sa politikom kvaliteta.

4.1 Odgovornost rukovodstva

Rukovodstvo isporučioaca sa izvršnom odgovornošću mora da definiše i dokumentuje svoju politiku kvaliteta, uključujući ciljeve vezane za kvalitet i svoje obaveze u vezi sa kvalitetom. Politika kvaliteta mora da bude u skladu sa poslovnim ciljevima isporučioaca i očekivanjima i potrebama njegovih kupaca. Isporučilac mora da osigura da se ta politika razume, sprovodi i održava na svim nivoima u organizaciji.

4.2 Sistem kvaliteta

4.3 Preispitivanje ugovora

Isporučilac mora da uspostavi i održava dokumentovane postupke za preispitivanje ugovora i za koordinaciju ovih aktivnosti.

4.4 Kontrola projekta

Isporučilac mora uspostaviti i održavati dokumentovane postupke za kontrolu i verifikovanje projekta proizvoda radi osiguranja da su ispunjeni specificirani zahtevi.

4.5 Kontrola dokumenata i podataka

Isporučilac mora da uspostavi i održava dokumentovane postupke za kontrolu svih dokumenata i podataka koji se odnose na zahteve ovog međunarodnog standarda uključujući, u pogodnom obimu, dokumenta spoljnog porekla kao što su standardi i kupčevi crteži.

4.6 Nabavka

Isporučilac mora da uspostavi i održava dokumentovane postupke radi osiguranja da je nabavljeni proizvod usklađen sa specificiranim zahtevima.

4.7 Kontrola isporučenog proizvoda

Isporučilac mora da uspostavi i održava dokumentovane postupke za upravljanje verifikacijom, skladištenjem i održavanjem proizvoda koje dostavlja kupac radi njihove ugradnje u gotove proizvode ili za odgovarajuće aktivnosti u toku izrade. Ako se bilo koji takav proizvod izgubi, ošteti ili je na neki drugi način nepodesan za upotrebu, isporučilac to mora da zapiše i o tome obavesti kupca.

4.8 Identifikacija i sledljivost proizvoda

Kada je to pogodno, isporučilac mora uspostaviti i sprovesti dokumentovane postupke za identifikovanje proizvoda na pogodan način i to od prijema pa tokom svih faza proizvodnje, isporuke i ugradnje.

4.9 Kontrola procesa

Isporučilac mora da identifikuje i planira procese proizvodnje, ugradnje, i servisiranja koji direktno utiču na kvalitet i mora da se osigura da se ti procesi obavljaju pod kontrolisanim uslovima.

4.10 Kontrolisanje (inspekcija) i ispitivanje

Isporučilac mora da uspostavi i održava dokumentovane postupke za aktivnosti kontrolisanja i ispitivanja, radi verifikacije da su ispunjeni utvrđeni zahtevi za proizvod. Zahtevano kontrolisanje i ispitivanje kao i zapisi koji će se sačiniti moraju da budu u skladu sa planom kvaliteta ili dokumentovanim postupcima.

4.11 Kontrolisanje opreme za kontrolisanje, merenje i ispitivanje

Isporučilac mora da uspostavi i održava dokumentovane postupke za kontrolu, kalibraciju i održavanje opreme za kontrolisanje, merenje i ispitivanje (uključujući i ispitni softver), koju on koristi za dokazivanje usaglašenosti proizvoda sa specificiranim zahtevima. Kada se kao pogodni vidovi kontrolisanja koriste ispitni softver ili uporedni etaloni kao što je ispitni hardver, pre upotrebe treba da budu provereni radi dokazivanja da su pogodni za verifikaciju prihvatljivosti proizvoda u upotrebi, tokom proizvodnje, ugradnje ili srevisiranja, a moraju biti proveravani u propisanim intervalima.

4.12 Status kontrolisanja i ispitivanja

Status kontrolisanja i ispitivanja proizvoda mora da se identifikuje na pogodan način koji ukazuje na usaglašenost ili neusaglašenost proizvoda, u odnosu na izvršeno kontrolisanje i ispitivanje.

4.13 Kontrola neusaglašenog proizvoda

Isporučilac mora da uspostavi i održava dokumentovane postupke da bi se sprečila nenamenska upotreba ili ugradnja proizvoda koji nije usaglašen sa utvrđenim zahtevima.

4.14 Korektivne i preventivne mere

Isporučilac mora da uspostavi i održava dokumentovane postupke za sprovođenje korektivnih i preventivnih mera.

4.15 Postupci za rukovanje, skladištenje, pakovanje, čuvanje i isporuku proizvoda

Isporučilac mora da uspostavi i održava dokumentovane postupke za rukovanje, skladištenje, pakovanje, čuvanje i isporuku proizvoda

4.16 Kontrola zapisa o kvalitetu

Isporučilac mora da uspostavi i održava dokumentovane postupke za identifikaciju, prikupljanje, označavanje, pristup, sređivanje, arhiviranje, održavanje i odlaganje zapisa o kvalitetu.

4.17 Interne provere kvaliteta

Isporučilac mora da uspostavi i održava dokumentovane postupke za planiranje i izvršavanje internih provera kvaliteta, radi verifikacije da li su aktivnosti u vezi sa kvalitetom i rezultati koji se na njih odnose u skladu sa planiranim aktivnostima i radi utvrđivanja efektivnosti sistema kvaliteta.

4.18 Obuka

Isporučilac mora da uspostavi i održava dokumentovane postupke za utvrđivanje potreba za obukom i da obezbedi obuku svih zaposlenih na izvršavanju aktivnosti koje utiču na kvalitet. Odgovarajući zapisi o obuci moraju da se održavaju.

4.19 Servisiranje

Ako je servisiranje jedan od utvrđenih zahteva, isporučilac mora da uspostavi i sprovodi dokumentovane postupke za obavljanje, verifikaciju (potvrđivanje) i izveštavanje da servisiranje ispunjava specificovane zahteve.

4.20 Statističke metode

Standard ISO/IEC 9126 - Softverski inženjering i kvalitet softverskih proizvoda:

Prilikom nabavke i implementacije softvera, postoji niz uobičajenih pitanja koja su uvek aktuelna. Neka od njih su: Da li softver raspolože sa zahtevanim funkcijama? Koliko je softver pouzdan? Koliko je softver efikasan? Da li je softver lak za upotrebu?

Ova uobičajena pitanja inicirala su pojavu standarda ISO/IEC 9126. Primena ovog standarda omogućava da se korisnicima olakša vrednovanje softvera:

- prihvatanje međuproizvoda od podgovarača,
- kompletiranje procesa,
- predviđanje i procena kvaliteta,
- prikupljanje informacija o međuproizvodima,
- prihvatanje proizvoda,
- donošenje odluke kada da se objavi proizvod,
- poređenja proizvoda sa uporedivim proizvodima,
- izbor proizvoda između alternativnih,
- ocena pozitivnih i negativnih efekata proizvoda kada se koristi,
- odluka o unapređenju ili zameni proizvoda.

Standard ISO/IEC 9126 sačinjen je u četiri dela koja se odnose na:

- Deo 1: Model kvaliteta
- Deo 2: Eksterne metrike
- Deo 3: Interne metrike
- Deo 4: Metrike kvaliteta u upotrebi

Deo 1: Model kvaliteta

1. *interni kvalitet i eksterni kvalitet* – definiše šest karakteristika, koje se dalje dele na podkarakteristike i grafički su prikazani na slici br.6:



Slika br.6

Deo 2: Eksterne metrike i Deo 3: Interne metrike

Metodologija definisanja metrike u standardima:

1. **Naziv metrike:** metrike u tabeli internih metrika i tabeli eksternih metrika imaju slična imena.
2. **Namena metrike:** pitanje na koje odgovara primena metrike.
3. **Metod primene:** kratak pregled primene.
4. **Merenje, formula i izračunavanje podataka:** Obezbeđuje formulu za merenje i objašnjava značenje korišćenih podataka. U nekim situacijama predloženo je više od jedne formule za metriku.
5. **Interpretacija merene vrednosti:** opseg i željene vrednosti.
6. **Vrsta merne skale:** Vrsta skale koju koristi metrika. Vrste skale koje se koriste su: nominalna skala, redna skala, intervalna skala, proporcionalna skala i apsolutna skala.
7. **Vrsta merenja:** Vrste koje se koriste su: Veličina (npr., veličina funkcije, veličina izvornog koda), Vreme (npr. proteklo vreme, korisnicko vreme), Brojač (npr., broj promena, broj grešaka).
8. **Ulaz za merenje:** Izvorni podaci koji se koriste u merenju.
9. **ISO/IEC 12207 SLCP reference:** Identifikuje procese životnog ciklusa softvera gde je primenljiva metrika.
10. **Ciljna grupa:** Identifikuje korisnike rezultata merenja.

Deo 4: Metrike kvaliteta u upotrebi – Ovaj deo standarda reguliše metrike sledeće četiri karakteristike kvaliteta u upotrebi: efektivnost, produktivnost, bezbednost i zadovoljstvo. Prikazane su na modelu na slici br.7:



Slika br.7

Standard ISO/IEC 14598 – Regulative vrednovanja softverskog proizvoda

Struktura standarda:

1. ISO/IEC 14598-1:1999, Informaciona tehnologija – Vrednovanje softverskog proizvoda
- Deo 1: Opšti pregled
2. ISO/IEC 14598-2:2000, Softverski inženjering – Vrednovanje proizvoda
- Deo 2: Planiranje i upravljanje
3. ISO/IEC 14598-3:2000, Softverski inženjering – Vrednovanje proizvoda
- Deo - 3 - Proces za projektante
 - Namenjen organizacijama koje planiraju da razvijaju novi, ili poboljšavaju postojeći proizvod i nameravaju da izvrše vrednovanje proizvoda koristeći svoje tehničko osoblje
 - Akcenat je na korišćenju indikatora koji mogu predskazati kvalitet krajnjeg proizvoda merenjem međuproizvoda razvijenih tokom životnog ciklusa.
4. ISO/IEC 14598-4:2000, Softverski inženjering – Vrednovanje proizvoda
- Deo - 4 - Proces za naručioce
 - treba da se koristi od strane organizacije koja planira da nabavi ili ponovo koristi postojeći ili prethodno razvijen softverski proizvod
 - može se primeniti u cilju odlučivanja o prihvatanju proizvoda ili izboru proizvoda između alternativnih proizvoda. (Proizvod može biti samostalan, deo sistema, ili deo složenog proizvoda)
5. ISO/IEC 14598-5:2000, Softverski inženjering – Vrednovanje proizvoda
- Deo 5: Proces za ocenjivače
 - Koristi se od strane ocenjivača koji sprovode nezavisno ocenjivanje softverskog proizvoda.
 - Vrednovanje se može izvršavati na zahtev bilo projektanta, nabavljača ili neke treće strane
6. ISO/IEC 14598-6:2000, Softverski inženjering – Vrednovanje proizvoda
- Deo 6: Dokumentovanje modula vrednovanja

Standard ISO/IEC 21827 – SSE CMM v.3 – standard zrelosti kapaciteta

Ovaj standard sadrži dva dela:

1. *SSE CMM* – primena generičkog modela sazrevanja kapaciteta - *CMM (Capability Maturity Model)* u *SSE (Security System Engineering)* sa posebnim osvrtom na razvoj programa zaštite,
2. *SSAM* – metod evaluacije zrelosti kapaciteta ovih procesa, koji koristi *SSE CMM* nivoe sazrevanja kapaciteta za procenu zrelosti procesa, a ne kvaliteta izlaza (proizvoda) tih procesa.

Generički model *CMM* razvio je *Software Engineering Institute (SEI)*, *Carnegie Mellon University (SAD)* za potrebe NSA(1993-1996). *SSE CMM* se u nekim zonama poklapa sa CC standardom za evaluaciju proizvoda i sistema zaštite. *SSE CMM* meri zrelost i kapacitete neke organizacije za izvršavanje procesa zaštite. Model nije toliko fleksibilan kao CC standard, ali ima dobru sistemski i procesno orijentisanu metriku.

Generalno *SSE CMM* standard može se primeniti za: merenje poboljšavanja zrelosti procesa zaštite, evaluaciju zrelosti kapaciteta procesa zaštite i bezbednosnu garanciju (engl. *Assurance*) za zrelost procesa zaštite.

Standard ISO/IEC 15504 – Vrednovanje softverskog procesa

- Istorijat standarda

- *CMM model* - razvijen u SAD za potrebe vojne industrije (preteča standarda ISO/IEC 21827)
- *Trilium* - Kanadske pošte
- *SPICE projekat* - ISO 15504 Vrednovanje softverskog procesa
- *ISO/IEC 15504* ima težnju da bude harmonizovan sa ISO 9000..

- Cilj korišćenja standarda

Opšti poslovni cilj je potsticanje organizacije u poboljšanju kvaliteta proizvoda upotrebljavajući dokaze, konzistentne i pouzdane metode za ocenu stanja procesa i korišćenje rezultata dela jasnog programa poboljšanja. Korišćenje procesa vrednovanja unutar organizacije podstiče:

- kulturu kontinualnog poboljšanja i ustanovljavanje sopstvenog mehanizma za podršku i održavanje te kulture
- inženjerski proces da odgovori poslovnim zahtevima
- optimizaciju resursa

Ovaj standard obezbeđuje okvir za vrednovanje procesa razvoja softverskih proizvoda. Kompatibilan je sa standardom ISO/IEC 21827 iz koga je potekao. Koristi dimenzije procesa, a podržava sve vrste procesa. Na bazi procene specifičnih faza procesa, osnovne oblasti prakse su podeljene na: organizacione, upravljačke, inženjerske, klijentsko – snabdevačke i procese za podršku. Standard ISO/IEC 15504 može se koristiti za:

- Ocenjivanje softverskog procesa
- Poboljšanje softverskog procesa
- Utvrđivanje sposobnosti softverskog procesa

Struktura standarda

1. ISO/IEC DTR 15504-1:2004 Deo 1: Koncept i rečnik
2. ISO/IEC DTR 15504-2 :2003 Deo 2: Funkcionisanje i procena
3. ISO/IEC DTR 15504-3 :2004 Deo 3: Upravljanje funkcionisanjem i procenom
4. ISO/IEC DTR 15504-4 :2004 Deo 4: Upravljanje poboljšanjem performansi i ograničenjima procesa
5. ISO/IEC DTR 15504-5 :2006 Deo 5: Primer Modela za procenu procesa vrednovanja
6. ISO/IEC DTR 15504-6 :2004 Deo 6: Primer Modela sistema za procenu životnog ciklusa

Iskustvo stečeno korišćenjem standarda u praksi dovelo je do pojave još jednog novog dela u strukturi standarda:

7. ISO/IEC DTR 15504-7 :Deo 7: Procena organizacione zrelosti.

Ovaj deo standarda preuzet je iz standarda ISO/IEC 21827 (generički SSE CMM model zrelosti kapaciteta) i određuje 6 nivoa organizacione zrelosti softverskog procesa:

Nivo 0 – Nezreo (nekompletan proces)

- Karakteriše ga neizvršavanje osnovnih postupaka u procesu
- Nije lako identifikovati proizvode ili izlaze procesa
- Sve se aktivnosti izvršavaju ad hok, ne postoji utvrđena procedura

Nivo 1 - Izvršava se neformalno

- Osnovni postupci procesa se generalno izvršavaju
- Performanse se ne planiraju i ne prate i zavise od individualnog znanja i napora – individualni heroizam - bez plana
- Poluproizvodi su identifikovani i nagoveštavaju se performanse.
- Učesnici prepoznaju koje akcije treba izvršiti, i postoji opšti sporazum o tome koje akcije i kada se izvršavaju

Nivo 2 - Planiran i praćen (upravljiv)

- Performanse osnovnih postupaka u procesu su planirane i prate se.
- Performanse se verifikuju po specificiranim procedurama.
- Radni proizvod se povinuje specificiranim standardima i zahtevima.
- Osnovna razlika između 2 i 1 nivoa je da se performance procesa planiraju, da se njima upravlja i da se teži ka dobro definisanim procesima.

Nivo 3 – Dobro definisan i uspostavljen proces

- Osnovni postupci se izvršavaju prema dobro definisanim procesima usklađenim sa usvojenim i prilagođenim verzijama standarda,
- Utvrđen je sekvencijalni i iterativni proces sa drugim procesima
- Zahtevana infrastruktura i radno okruženje za izvršavanje procesa je identifikovano kao deo standardnih procesa
- Unapred su određeni odgovarajući metodi za nadgledanje efikasnosti
- Procesi su dokumentovani.
- Proces je planiran i njime se upravlja, u organizaciji široko rasprostranjenih, standardnih procesa.

Ovaj nivo odgovara ISO9000 sertifikatu kvaliteta

Nivo 4 – Predvidiv i kvantitativno upravljan

- Prikupljaju se i analiziraju detaljna merenja performansi. To dovodi do kvantitativnog razumevanja mogućnosti procesa i stvara mogućnost za predviđanje performansi.
- Performansama se objektivno upravlja.
- Kvalitet radnih proizvoda je kvantifikovan.
- Definisani procesi su kvantitativno razumljivi i kontrolisani.

Nivo 5 - Optimizacija

- Na osnovu poslovnih ciljeva organizacije ustanovljeni su kvantitativni ciljevi poboljšanja efikasnosti procesa iz familije standardnih procesa.
- Omogućeno je neprekidno poboljšanje procesa, nasuprot ovim ciljevima, kvantitativnom povratnom spregom iz izvršavanja definisanih procesa i iz probnih inovativnih ideja i tehnologija.
- Definisani procesi i standardni procesi podvrgavaju se neprestanom prečišćavanju i poboljšanju, na osnovu kvantitativnog razumevanja uticaja izmena u tim procesima.
- Dosadašnja praksa dala je sledeću ocenu organizacione zrelosti softverskog procesa:
 - ✚ smatra se da je 80% organizacija na prvom nivou
 - ✚ postoji samo nekoliko primera projekata i organizacija na nivou 4 i 5
 - ✚ armija USA zahteva da ponuđači budu najmanje na drugom nivou

Standard ISO/IEC FCD 24773 - Sertifikacija profesionalnih inženjera softvera**Razlozi za donošenje standarda**

- U poslednjih nekoliko dekada softverski sistemi su postali kritična komponenta u većini aspekata života
- Sistemi su postali mnogostruko složeni
- Standish Group je 1994 objavila da samo 16% softverskih projekata zadovoljava inicijalno formulisane ciljeve - 31% projekata je obustavljeno pre završetka [Standish].
- Royal Academy of Engineering je objavila da je stanje alarmantno, da značajan broj složenih softvera i IT projekata još ne donosi ekonomsku korist na vreme i u okviru predviđenih troškova i specifikacija.
- Navedeno se pripisuje opštem odsustvu profesionalizma u IT industry. [Royal].
- Standard je napisan kao odgovor potrebama da se izvrši sertifikacija profesionalaca inženjera softvera kako bi se omogućila razmena između različitih zemalja.
- Standard je također odgovor potrebama multinacionalnih organizacija ili naručilaca razvoja softvera za stranim korisnicima (uključujući offshoring) koji zahteva sertifikaciju softverskih inženjera.

Svrha i polje primene standarda

Definiše procese potrebne za **postavljanje, administriranje i održavanje sertifikacione šeme**

Sertifikaciona tela

Definiše uslove koje treba da ispunjava sertifikaciono telo

Standard ISO/IEC TR 19759:2005 – Vodič kroz osnove znanja softverskog inženjeringa (SWEBOK)

Blizu 500 profesionalnih softverskih inženjera iz 41 zemlje, učestvovalo je u realizaciji projekta, zastupajući različita gledišta. Svrha vodiča je da obezbedi konsenzusom potvrđenu karakterizaciju granica discipline softverskog inženjeringa i da obezbedi tematski pristup osnovama znanja podržavajući tu disciplinu.

Standard daje regulative za:

1. Standarde koji mogu biti primenjeni u realizaciji projekata
2. Znanja iz predmetne oblasti u kojoj će softverski inženjer raditi:

Osnovna znanja su podeljena na 10 oblasti: zahtevi softvera, dizajn softvera, konstrukcija softvera, testiranje softvera, održavanje softvera, upravljanje konfiguracijom softvera, upravljanje softver inženjeringom, softver inženjering proces, alati i metode softver inženjeringa, kvalitet softvera

3. Veštine koje softverski inženjer treba da poseduje uključuju:

- a) sposobnost da se primeni znanje i veštine,
- b) sposobnost da efikasno komunicira sa svim zainteresovanim stranama,
- c) sposobnost da identifikuje, formuliše i reši probleme,
- d) sposobnost da efikasno radi kao individua i u timu,
- e) razumevanje uticaja softverskog inženjerskog rada na socijalno, komercijalno, kulturno i druga okruženja u kojima radi.

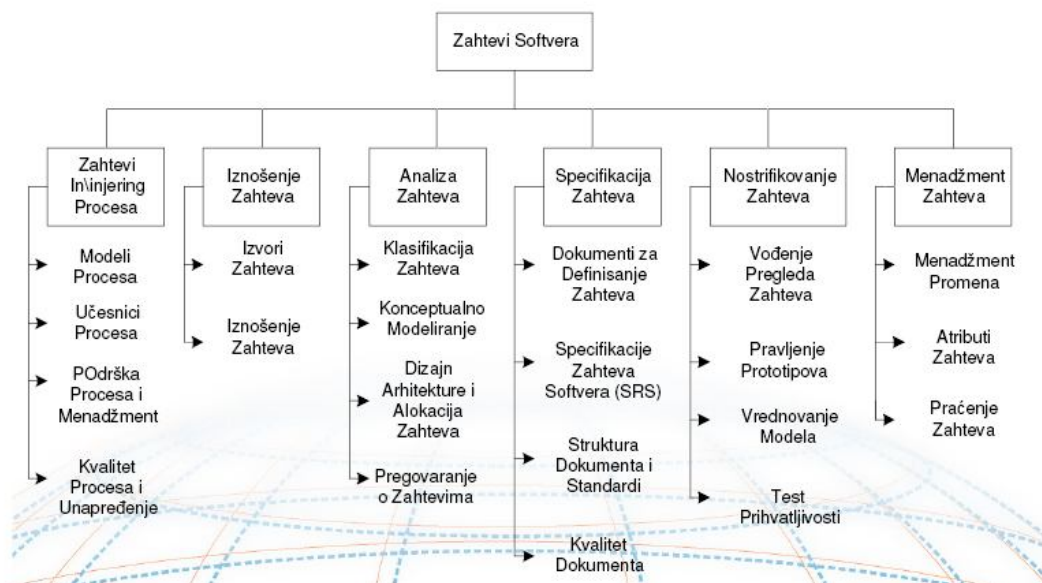
4. Vrednovanje znanja i veština

Znanje i veštine se moraju vrednovati. Sertifikaciono telo treba da:

- znanje i veštine iskaže kroz skup kompetentnosti koje se zahtevaju za sertifikaciju potrebnih znanja i veština,
- obezbedi detalje kako se kompetentnosti mogu dostići i savladati, jer se neke veštine mogu steći samo iskustvom,
- utvrdi način kako će se vršiti vrednovanje: ispitivanje, seminarski izveštaji, intervjui, itd.

5. Etički kodeks i profesionalna praksa

6. Obnavljanje sertifikacije



Slika br.8 Zahtevi softvera

4.5. Bezbednosni standardi koji se ne koriste

Standard COBIT (Control Objectives for Information and Related Technology)

Ovaj standard opisuje metod nadzora i kontrole rizika, koji se javlja korišćenjem IKT sistema za podršku poslovnih procesa. Cobit standard je objavio ITGI (*IT Governance Institut*) organizacije ISACA (*Information Systems Audit and Control Association*). Objavljivanjem standarda BS7799 i NIST *Security Handbook* i sami autori su napustili Cobit standard. Sertifikacija sistema zaštite prema ovom standardu praktično se ne može izvršiti.

Standard ISO/IEC 12207 - Procesi životnog ciklusa softvera

Standard JUS ISO/IEC 12207 identičan je sa međunarodnim standardom ISO/IEC 12207 : 1995, Information technology - Software life cycle processes. Ovaj standard je pripremila Komisija za standarde iz oblasti softverskog inženjeringa KSI 1/07. Standard JUS ISO/IEC 12207 predstavlja prevod sa engleskog na srpski jezik standarda Međunarodne organizacije za standardizaciju ISO.

Rečnik termina međunarodne organizacije za standardizaciju ISO i francuske asocijacije za standardizaciju AFNOR ISO/AFNOR: 1989 primenjuje se za potrebe ovog standarda, pošto nema odgovarajućeg srpskog rečnika.

1. Predmet standarda

Predmet ovog standarda je regulisanje svih aktivnosti vezanih za životni ciklus softvera počevši od nabavke do prestanka njegovog korišćenja (engl. *End of Life*).

2. Veze sa drugim standardima

Sledeći standardi sadrže odredbe koje, putem pozivanja u ovom tekstu, čine odredbe ovog standarda. Navedena izdanja važila su u vreme objavljivanja. Kako svi standardi podležu reviziji, učesnici ugovora zasnovanih na ovom standardu pozvani su da ispituju mogućnost primene najnovijih izdanja niže navedenih standarda. Članice IEC i ISO održavaju registre tekućih važećih međunarodnih standarda.

ISO/AFNOR: 1989, Rečnik računarstva

ISO/IEC 2382-1: 1993, Informaciona tehnologija - Rečnik - Deo 1: Osnovni termini i definicije

ISO/IEC 2382-20: 1990, Informaciona tehnologija - Rečnik - Deo 20: Razvoj sistema

ISO 8402: 1994, Upravljanje kvalitetom i obezbeđenje kvaliteta - Rečnik

ISO 9001: 1994, Sistemi kvaliteta - Model obezbeđenja kvaliteta u projektovanju, razvoju, proizvodnji, ugradnji i servisiranju

ISO/IEC 9126: 1991, Informaciona tehnologija - Vrednovanje softverskih proizvoda - Karakteristike kvaliteta i smernice za njihovu upotrebu

3. Definicije

Za potrebe ovog standarda primenjuju se definicije date u standardima ISO 8402, ISO/IEC 2382-1 i ISO/IEC 2382-20

4. Primena standarda

U ovoj tački dati su procesi iz životnog ciklusa softvera koji se mogu upotrebiti u nabavci, isporučivanju, razvoju, korišćenju i održavanju softverskih proizvoda. Cilj je da se korisnicima standarda obezbedi putokaz tako da se mogu orijentisati u standardima i valjano ih primenjivati.

5. Primarni procesi životnog ciklusa

Primarne procese životnog ciklusa softvera (tačka 5) sačinjava pet procesa koji služe primarnim stranama u toku životnog ciklusa softvera. Primarna strana smatra se ona koja inicira ili obavlja razvoj, korišćenje ili održavanje softverskog proizvoda. Primarne strane su nabavljač, isporučilac, projektant, rukovalac i onaj koji održava softverski proizvod. Primarni procesi su: Proces nabavke, Proces isporuke, Proces razvoja, Proces korišćenja, Proces održavanja

6. Proces podrške u životnom ciklusu

Procese podrške životnog ciklusa softvera (tačka 6) sačinjava osam procesa. Proces podrške podržava drugi proces kao sastavni deo sa posebnim ciljem i doprinosi uspehu i kvalitetu softverskog projekta. Proces podrške se uvodi i izvršava, po potrebi, uz pomoć nekog drugog procesa. Proces podrške su: proces dokumentovanja, proces upravljanja konfiguracijom, proces obezbeđenja kvaliteta, proces verifikacije, proces validacije, proces zajedničkih pregleda, proces provere, proces rešavanja problema

7. Organizacioni procesi životnog ciklusa

Organizacione procese životnog ciklusa softvera (tačka 7) sačinjavaju četiri procesa. Primenu ih organizacija radi uspostavljanja i ostvarivanja osnovne strukture združenih procesa životnog ciklusa i osoblja i neprestanog poboljšavanja strukture i procesa. Tipičan način njihovog korišćenja je izvan oblasti specifičnih projekata i ugovora; međutim, saznanja iz takvih projekata i ugovora doprinose poboljšanju organizacije. Organizacioni procesi su: proces upravljanja, proces infrastrukture, proces poboljšanja, proces obuke

Prilozi

A - Proces prilagođavanja

U ovom prilogu, koji je normativan, definisane su osnovne aktivnosti koje su potrebne za izvođenje prilagođavanja ovog standarda.

B - Smernice za prilagođavanje

Ovaj prilog sadrži kratko uputstvo o prilagođavanju zahteva ovog standarda; u njemu su nabrojani ključni činioci za donošenje odluka o prilagođavanju.

C - Smernice o procesima i organizaciji

U prilogu C prikazani su odnosi između procesa životnog ciklusa i s njima povezanih strana(ka).

Standard ISO/IEC 15408 – Opšti kriterijumi (*Common Criteria*) za evaluaciju proizvoda i sistema zaštite

Standard sadrži tri dela:

- [I] Uvod i opšti model
- [II] Funkcionalni zahtevi
- [III] Bezbednosni zahtevi

U CC standard uključeni su sledeći relevantni standardi:

1. Procedure za registraciju profila zaštite (IS15292),
2. Okvir za bezbednosnu garanciju (WD15443),
3. Uputstvo za izradu profila zaštite (WD15446)
4. Metodologija za evaluaciju zaštite (WD18045)

Opšti kriterijum (*Common Criteria*, CC) rezultat je napora da se naprave kriterijumi za proveru i vrednovanje IKT sigurnosti koji će moći da se koriste u međunarodnoj zajednici. To je svojevrsno ujednačavanje velikog broja različitih izvornih kriterijuma: postojećih evropskih (ITSEC), američkih (TCSEC) i kanadskih kriterijuma (CTCPEC). Standard je zamenio postojeće standarde „*Orange Book*“ (SAD) i *ITSEC*(EU). Zajednički kriterijum razrešava konceptualne i tehničke razlike među izvornim kriterijumima. On doprinosi i razvoju međunarodnog standarda i otvara vrata ka uzajamnom priznavanju rezultata provere i vrednovanja. Opšti kriterijum je sada međunarodni standard (ISO/IEC 15408) za računarsku sigurnost. Utemeljivač ovog standarda je konzorcijum NSA (Nacionalna agencija za bezbednost, SAD) i EU. Pod uticajem Međunarodnog komiteta, standard je usvojen kao međunarodni standard ISO/IEC 15408. Standard su usvojile sve zemlje EU, Australia, Japan i Rusija.

Za razliku od standarda kao što je USA standard FIPS 140, u CC-u se ne daje lista zahteva u pogledu sigurnosti ili funkcionalnosti koje proizvodi moraju da sadrže. Umesto toga, tu se opisuje radni okvir (engl. *Framework*) u kome korisnici računarskih sistema i mreža mogu da specificiraju svoje zahteve; proizvođači (engl. *Vendors*) mogu onda da ih implementiraju i/ili da iznesu stavove i tvrdnje o svojim proizvodima, a laboratorije mogu da provere i evaluiraju proizvode – da provere da li stvarno odgovaraju tim tvrdnjama, odnosno deklaracijama. Drugim rečima, CC obezbeđuje garanciju da će se proces specifikacije, implementacije i evaluacije proizvoda za računarsku sigurnost voditi i sprovesti na rigorozan i standardizovan način, što garantuje određeni nivo kvaliteta proizvoda i usluga u ovoj oblasti.

Značaj standarda je u tome što podiže nivo i pozdanost funkcija zaštite koje su implementirane u standardnim proizvodima zaštite (Operativnim sistemima, bazama podataka, barijerama, ruterima IDS/IPS i dr.). CC standard nema veću primenu iako je dosta fleksibilan, jer ima veoma kompleksan proces evaluacije i zahteva mnogo vremena. U svetu postoji ograničen broj akreditovanih tela i kapaciteta po ovom standardu. Njihove usluge su skupe i nefleksibilne za transnacionalnu primenu. Organizacije se radije odlučuju da ulažu novac na poboljšanje procesa zaštite, nego na njihovu evaluaciju. Standard je značajan za glavne snabdevače proizvoda zaštite i sistema smart kartica, kao i za visoko rizične IKT sisteme državnih organa.

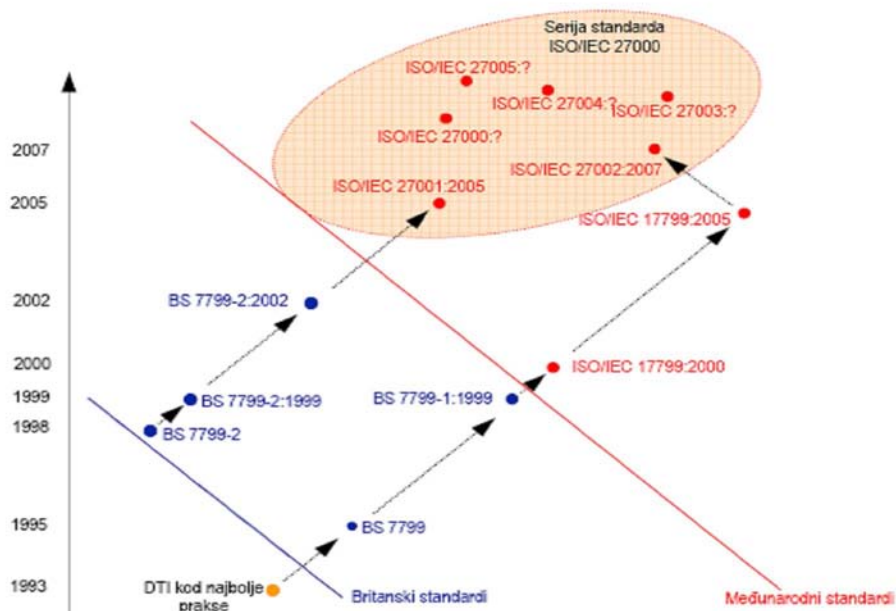
4.6. STANDARDI U RAZVOJU

Stalni komitet SC27 (ISO/IEC JTC1/SC27 "IT Security Technique") pokrenuo je novu seriju standarda ISO/IEC 27000. Ovo je familija standarda o ISMS - sistemu za upravljanje sigurnosti informacija (engl. *Information Security Management System*, ISMS) koja je planirana da se razvije u narednih 5-7 godina. Planirano je da ovu seriju (slika br.9) čine:

- ISO/IEC 27000 ISMS - Osnove i rečnik pojmova
- ISO/IEC 27001 ISMS - Zahtevi
- ISO/IEC 27002 (ISO/IEC 17799 će postati posle 2007 godine) – Kodeks postupaka (dobra praksa) za upravljanje sigurnosti informacija
- ISO/IEC 27003 - ISMS Uputstvo za implementaciju
- ISO/IEC 27004 - Merenja u upravljanju sigurnosti informacija
- ISO/IEC 27005 - Upravljanje rizika sigurnosti informacija

Za sada su objavljena samo dva standarda iz ove serije, ISO/IEC 27001:2005 i ISO/IEC 17799:2005 (slika br. 9). Standard ISO/IEC 17799:2005 definiše kodeks dobre poslovne prakse u oblasti sigurnosti informacija. Bazira se na jedanest sigurnosnih kategorija (poglavlja) koje pokrivaju sve aspekte sigurnosti informacija, i definišu sigurnosne ciljeve i kontrole koje je potrebno sprovesti da bi se ispunili ti ciljevi. Kontrole se definišu kao: način upravljanja rizicima, što podrazumeva politike, procedure, uputstva, organizacione strukture koje mogu da budu administrativne, tehničke, upravljačke ili pravne. Na dobroj poslovnoj praksi koja je definisana u standardu ISO/IEC 17799, razvijan je standard (ISO/IEC 27001) koji definiše zahteve koje menadžment sistem za sigurnost informacija mora da zadovolji i po kome se sprovodi sertifikacija ISMS ako se to zahteva.

Ceo koncept sigurnosti informacija koji je definisan u standardima ISO/IEC 27001 i ISO/IEC 17799 bazira na konceptu upravljanja (menadžmentu) rizicima. Ocena rizika je definisana kao ocena pretnji informacijama (pretnje koje dovode do povrede poverljivosti, integriteta i raspoloživosti informacija) njihovog uticaja na informacije i na ranjivost (slabost) informacija i informacionih sistema kao i verovatnoće njihove pojave.



Slika br.9

Upravljanje (menadžment) rizikom je definisan kao proces identifikacije, kontrole i umanjivanja ili eliminacije sigurnosnih rizika koji mogu da utiču na informacije i informacione sisteme a koji mora da bude finansijski opravdan.

Serija standarda ISO/IEC 27000, odnosno njeni standardi ISO/IEC 27001:2005 i ISO/IEC 17799:2005 (slika br.9) daju jedan harmonizovani pristup upravljanju rizicima kojim su izložene informacione vrednosti u organizaciji kroz razvoj, implementaciju i održavanje menadžment sistema za sigurnost informacija

5. SIGURNOSNI STANDARDI I PROGRAMI CERTIFIKACIJE

U ovom poglavlju su ukratko pobrojani neki od sigurnosnih standarda i programa sertifikacije. Navedeni su neki međunarodni, a takođe i američki standardi i regulacioni propisi. Programi sertifikacije vrlo su značajni u novije vreme jer omogućavaju određeni nivo standardizacije kvaliteta proizvoda i usluga, kao i kadrova koji rade u oblasti sigurnosti.. Naveden je i postupak donošenja Internet standarda i RFC-ova, kao zanimljiv primer procesa *defacto* standardizacije koja je plod entuzijastskog rada profesora i studenata, zatim inženjera i korisnika koji su razvijali prve TCP/IP mreže. Ovaj proces je kasnije formalizovan u okviru institucija.

SIGURNOSNI STANDARDI

Standard ISO 17799

Standard ISO/IEC 17799 postavlja osnovne i opšte principe za iniciranje, implementaciju, održavanje i unapređenje upravljanja sigurnošću informacija u nekoj organizaciji. Pomenuti principi daju opšte smernice za zajednički prihvaćene ciljeve upravljanja sigurnošću informacija. ISO/IEC 17799:2005 se oslanja na najbolja iskustva upravljanja u sledećim područjima: sigurnosne politike, organizacija sigurnosti informacija, upravljanje vrednostima, sigurnost ljudskih resursa, fizička sigurnost i sigurnost okruženja,

upravljanje komunikacijama i operacijama, kontrola pristupa, akvizicija, razvoj i održavanje informacionih sistema, rešavanje incidenata u oblasti sigurnosti, upravljanje održavanjem kontinuiteta posla, poštovanje propisa i standarda.

Standard ISO/IEC TR 13335

Ovaj standard je razvijen u dve faze. Prva faza bi bio **GMITS** (engl. *Guidelines for the Management of IT Security*), a zatim je 2002.god. prerastao u standard za upravljanje zaštitom informacija i komunikacija **MICTS** (engl. *Management of Information and Communications Technology Security*), kao mogući kandidat za standardizaciju IKT zaštite. Iako je te godine doneta odluka da se umesto termina „IT“ u buduće koristi termin „ICT“, ova odluka u standardu nije konzistentno sprovedena. Standard opisuje procedure za definisanje bezbednosnih ciljeva i kreiranje i implementaciju koncepata IKT zaštite. Sadrži dobro uputstvo za definisanje procesa IKT zaštite, ali nema obezbeđene sertifikacije sistema zaštite na bazi ovog standarda.

Standard ISO/IEC 27001

ISO/IEC 27001:2005 obuhvata sve vrste organizacija (komercijalna preduzeća, državne agencije, neprofitne organizacije). ISO/IEC 27001:2005 specificira zahteve za uspostavljanje, implementaciju, rad, nadzor, pregledanje, održavanje i unapređenje dokumentovanog sistema upravljanja sigurnošću kao delom poslovnih rizika te organizacije. Tu su specificirani zahtevi za implementaciju upravljanja sigurnošću za pojedinačne organizacije i njihove delove.

ISO/IEC 27001:2005 daje mogućnost izbora odgovarajućih sistema upravljanja za zaštitu imovine i stvaranja poverenja kod svih zainteresovanih strana. Primenjiv je na različite tipove i veličine kompanija, organizacija i institucija.

ISO/IEC 27001:2005 je pogodan za nekoliko različitih tipova primene, uključujući sledeće:

- korišćenje u organizacijama pri formulisanju sigurnosnih zahteva i ciljeva
- korišćenje u organizacijama, kao osiguranje da je upravljanje sigurnosnim rizicima efikasno
- korišćenje u organizacijama, kako bi se osiguralo poštovanje zakona i ostalih egulacionih propisa
- korišćenje u nekoj organizaciji, kao okvir procesa za implementaciju i rukovođenje kontrolom, kako bi pojedinačni sigurnosni ciljevi u toj organizaciji bili ispunjeni
- definisanje novih procesa u rukovođenju sigurnošću
- identifikacija i razjašnjenje postojećih procesa upravljanja sigurnošću informacija
- koristi ga rukovodstvo organizacija kako bi se odredio status aktivnosti koje se odnose na upravljanje sigurnošću informacija
- koriste ga interni i eksterni revizori (engl. *Auditor*) organizacije kako bi se odredio stepen poštovanja polisa, direktiva i standarda koje je organizacija prihvatila
- koriste ga organizacije, kako bi poslovnim partnerima i drugim organizacijama s kojima sarađuju – ili iz komercijalnih razloga – obezbedile relevantne informacije o pravilima informacione sigurnosti, direktivama, standardima i procedurama
- implementacija informacione sigurnosti koja omogućava odvijanje posla
- koriste ga organizacije kako bi klijentima dostavile relevantne podatke o sigurnosti informacija.

ISF standard dobre prakse zaštite (V. 4.0 - mart 2003.god.)

Ovaj standard izradila je međunarodna asocijacija *Information Security Forum* (ISF) na osnovu priloga i saradnje sa više od 250 vodećih organizacija u svetu u toku poslednjih 14 godina. Standard se ažurira svake druge godine. Poslednja verzija standarda obuhvata:

- najnovija tehnološka rešenja sistema višeslojne zaštite informacija i IS kao što su:
- detektori upada u sistem (engl. *Intrusion Detection Systems*, IDS),
- mehanizmi za zaštitu privatnosti, zaštitu podataka i informacija i e- pošte,
- podizanje svesti o zaštiti,
- bezbedno korišćenje bežičnih komunikacija i PDA uređaja,
- *Bluetooth* tehnologiju, metodologiju i tehnologiju forenzičke analize softvera, računara i računarske mreže.

Težište standarda je usmereno na poslovne sisteme koji prihvataju da je zaštita informacija ključno pitanje svakog posla. Standard je usaglašen sa standardom za zaštitu ISO/IEC 17799 i obuhvata sledeće aspekte zaštite: upravljanje, kritične operacije, računarske sisteme, računarske mreže, i razvoj sistema zaštite.

Standard EBXML – globalni standard za poslovanje na Internetu

Ovaj standard je naslednik EDI (engl. *Electronic Data Exchange*) standarda. Nastao je kao rezultat rada 300 naučnika u periodu od 1999-2001.god. pod nadzorom OASIS i UN/CEFACT organizacija. ebXML temelji se na nekoliko već šire primenjenih standarda, povezuje ih i dodaje funkcionalnost potrebnu za globalno elektronsko poslovanje. ebXML pomoćnim registrima, modelovanjem poslovnih procesa, XML jezikom za opisivanje strukturiranih dokumenata i drugim komponentama povećava učinak razmene poslovnih dokumenata između učesnika, omogućava pronalaženje poslovnih partnera, integraciju poslovnog znanja među različitim delatnostima i jednostavno povezivanje partnera sa različitim ekonomskih prostora. Standard ebXML ima sledeću strukturu:

- modele poslovnih procesa
- registre i repozitorije
- profile i dogovore o protokolima učesnika
- ebMS za razmenu poruka
- osnovne komponente.

ebXML se oslanja na poslovne procese umesto na fiksne dokumente i na izmenljive osnovne komponente umesto na unapred pripremljene podatke. U praksi to znači, da postoji mogućnost prilagođavanja postupaka i terminologije prema razmerama poslovanja. ebXML u velikom pogledu automatizuje komunikaciju između učesnika, poboljšava i olakšava transakcije.

Procesi, poruke, osnovne komponente i drugi poslovni objekti, koji su potrebni za elektronsko poslovanje, su smešteni u ebXML registrima. Do registra učesnici u transakcijama lako pristupaju, uz upotrebu ebXML. ebXML koristi postojeću Internet infrastrukturu. Podjednako lako ebXML poruke se razmenjuju preko Internet protokola, kao što su HTTP, SMTP, FTP i drugih.

NIST standardi

Odeljenje za računarsku sigurnost američkog Nacionalnog instituta za standarde i tehnologiju (engl. *National Institute of Standards and Technology*, NIST) uključeno je u mnogo različitih projekata. Na primer, kriptografski algoritmi **DES** (engl. *Data Encryption Standard*) i **AES** (engl. *Advanced Encryption Standard*) jesu NIST standardi.

Internet standardi

Poseban, vrlo značajan segment sigurnosti odnosi se na Internet. Mnogi su protokoli iz skupa protokola TCP/IP ili standardizovani ili su u procesu standardizacije. Internet ima sopstvene mehanizme standardizovanja, veoma različite od postupaka koji se primenjuju po standardima ITU-T i ISO. Prema univerzalnom dogovoru, organizacija poznata kao **Internet društvo** (engl. *Internet Society*) bavi se razvojem i publikovanjem ovih standarda. Tri organizacije pod okriljem Internet društva odgovorne su za stvarni rad na ovom području. To su:

1. Internet Architecture Board

(IAB), odgovorna za definiciju celokupne arhitekture Interneta; obezbeđuje rukovođenje, opšte principe i pravce razvoja za IETF. Kada je mreža ARPANET puštena u rad, Ministarstvo odbrane je obrazovalo formalni komitet da je nadgleda. Godine 1983. komitet je preimenovan u **Odbor za aktivnosti na Internetu** (engl. *Internet Activities Board*, IAB) i dodeljena mu je malo šira misija: podsticanje istraživanja da mrežu razvijaju i održavaju Internet u približno istom duhu. Ista skraćenica (IAB) korišćena je i od onda kada je ime Odbora promenjeno u **Odbor za arhitekturu Interneta** (engl. *Internet Architecture Board*).

IAB se okuplja više puta godišnje da razmotri rezultate i da o njima izvesti organizacije koje su ga osnovale i koje ga finansiraju. Kada se ukaže potreba za novim standardom (na primer, za novim algoritmom za rutiranje), članovi IAB-a ga razmatraju, a zatim objavljuju izmene. Izmene su objavljivane u nizu tehničkih izveštaja zvanih **Zahtevi za komentare** (engl. *Request For Comments*, RFC). RFC dokumenti su skladišteni na mreži tako da ih svaki zainteresovani korisnik može preuzeti sa adrese www.ietf.org/rfc. Oni su numerisani hronološki, po redu pojavljivanja i danas ih ima preko 3.000.

2. Internet Engineering Task Force

(IETF), koja se bavi inženjeringom protokola i razvojem Interneta. Do 1989. godine, Internet je tako narastao da opisani neformalni stil rada više nije bio primenljiv. Mnogi proizvođači su već nudili TCP/IP proizvode i nisu želeli da ih menjaju samo zato što šačica istraživača ima "bolju ideju". U leto 1989. godine, IAB je ponovo reorganizovan. Istraživači su prebačeni u **Istraživačke snage Interneta** (engl. *Internet Research Task Force*, *IRTF*) – telo podređeno IAB-u – i paralelno telo **Inženjerske snage Interneta** (engl. *Internet Engineering Task Force*, IETF). IAB su popunili predstavnici organizacija koje nisu više bile samo akademske i istraživačke. U početku je to bila grupa koja se sama obnavljala tako što su posle dvogodišnjeg mandata stari članovi imenovali nove. Kasnije je od osoba zainteresovanih za Internet obrazovano Internet društvo.

Rad IETF-a je podeljen na osam područja, tj. na radne grupe:

- **opšte** (IETF procesi i procedure – na primer, proces za razvoj Internet standarda),
- **aplikacije ili primene** (protokoli zasnovani na Webu, EDI-Internet integracija, LDAP),
- **Internet infrastruktura** (IPv6, PPP proširenja),
- **operacije i upravljanje** (standardi i definicije za mrežne operacije, korišćenje i upravljanje – na primer SNMPv3 i daljinsko nadgledanje mreža),
- **rutiranje** (protokoli za rutiranje, kao što je OSPF),
- **sigurnost** (sigurnosni protokoli i tehnologije, kao što su Kerberos, IPSec, X.509, S/MIME, TLS),
- **transport** (protokoli transportnog nivoa, kao što su IP telefonija NFS, RSVP) i
- **korisničke usluge** (načini da se poboljša kvalitet informacija raspoloživih korisnicima Interneta; na primer, odgovorno korišćenje Interneta, korisničke usluge i dokumenti “vama za informaciju” (engl. *For Your Information*, *FYI documents*)).

Uočavamo da se oblast sigurnosti tretira kao posebno područje, što govori o značaju ove problematike u okviru Interneta.

3. Internet Engineering Steering Group

(IESG), odgovorna za tehničko upravljanje IETF aktivnostima i procesom donošenja Internet standarda. Odluku o tome koji će RFC postati Internet standard, donosi IESG, na predlog IETF-a. Da bi postala standard, specifikacija mora zadovoljiti sledeće kriterijume:

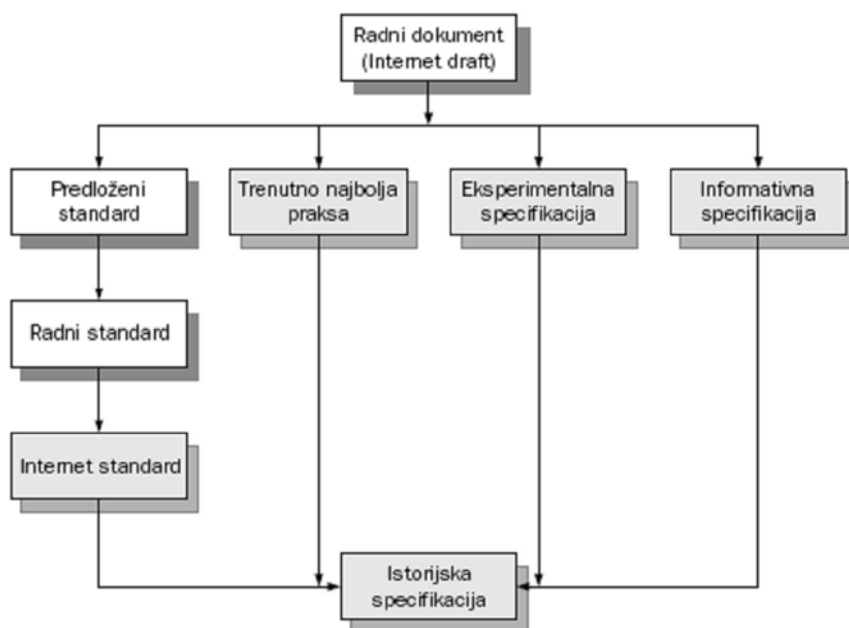
- da bude stabilna i razumljiva,
- da bude tehnički kompletna,
- da ono što specifikacija definiše ima više nezavisnih i interoperativnih implementacija koje su proverene u praksi,
- da ima značajnu javnu podršku,
- da bude prepoznatljiva i korisna u značajnom delu Interneta ili na celom Internetu.

Ključna razlika između ovih kriterijuma i onih koji se koriste kao internacionalni ITU standardi jeste isticanje radnog (operativnog) iskustva, odnosno primene u praksi.

Leva strana slike br.10 prikazuje niz koraka zvanih „standardna staza” (engl. *Standard Track*), kojom prolazi specifikacija da bi postala standard. Ovaj proces je definisan u RFC 2026. Koraci podrazumevaju detaljno ispitivanje i testiranje. U svakom koraku, IETF može preporučiti unapređenje protokola i IESG mora da to ratifikuje. Proces počinje kada IESG odobri objavljivanje Internet nacrt (radnog dokumenta) kao RFC-a sa statusom „predloženi standard” (engl. *Proposed Standard*).

Beli pravougaonici na dijagramu predstavljaju privremena stanja, u kojima se može biti minimalno vreme. Međutim, dokument mora ostati u fazi “predloženi standard” najmanje 6 meseci i u fazi „nacrt standarda” (engl. *Draft Standard*) najmanje 4 meseca kako bi bilo dovoljno vremena za pregled i recenziju dokumenta.

Osenčeni pravougaonici predstavljaju dugoročna stanja u kojima se dokument može zadržati godinama. Da bi specifikacija postala nacrt standarda, moraju postojati najmanje dve nezavisne i interoperabilne implementacije iz kojih je dobijeno adekvatno operativno iskustvo. Kada se ostvari značajno implementaciono i operativno iskustvo, specifikacija se može podići na nivo Internet standarda. U ovoj tački, specifikacija dobija STD broj i RFC broj. Na kraju, specifikacija koja postane zastarela ili prevaziđena dobija istorijski status (engl. *Historic*).



Slika br.10 Nastanak Internet standarda

Svi Internet standardi spadaju u jednu od dve kategorije:

- Tehnička specifikacija (engl. *Technical Specification*, TS). TS definiše protokol, uslugu, proceduru, konvenciju ili format. Gomila Internet standarda su TS-ovi.
- Izjava o primenljivosti (engl. *Applicability Statement*, AS). AS specificira kako i pod kojim okolnostima jedan ili više TS-ova mogu biti primenjeni da podrže određenu Internet mogućnost (engl. *Capability*).

Brojni RFC dokumenti ne postaju Internet standardi. U nekim RFC dokumentima standardizuju se rezultati dogovora, izjave o principima ili zaključci o tome koji je najbolji način da se izvrše određene operacije, kao i o IETF procesnim funkcijama.

Takvi RFC dokumenti sadrže trenutno najbolju praksu (engl. *Best Current Practice*, BCP). Odobranje BCP-ova odvija se isto kao i odobranje predloženih standarda. Za razliku od dokumenata koji prolaze kroz sve etape na stazi standarda, nema trostepenog procesa za BCP; BCP prelazi iz stanja radnog dokumenta u odobreni BCP u jednom koraku. Protokol ili druga specifikacija koja se ne smatra spremnom za standardizaciju, može se objaviti kao eksperimentalni RFC. Posle dodatnog rada, specifikacija može biti ponovo podneta na razmatranje. Ukoliko je specifikacija generalno stabilna, jasna i razumljiva, javno razmatrana i ocenjena povoljno, i ako za nju postoji dovoljan društveni interes i poverenje da bi se smatrala vrednom, RFC će postati predloženi standard.

Posle svega, Informativna specifikacija (engl. *Informational Specification*) objavljuje se kao opšta informacija za Internet zajednicu.

PCI DSS (standard sigurnosti podataka industrije platnih kartica)

Kao odgovor na rastući broj zloupotreba (engl. *Fraud*) u poslovanju na Internetu i uopšte u poslovanju kreditnim i sličnim karticama, nekoliko vodećih svetskih kompanija odlučile su da donesu sigurnosni standard koji bi pomogao da se smanje pronevere i zloupotrebe. Glavni inicijatori **PCI DSS** (engl. *Payment Card Industry Data Security Standard*) standarda jesu Visa i Master Card International. Kasnije su ovaj standard prihvatile i ostale

kompanije koje izdaju kreditne kartice. Doneti su i programi i definisane procedure sertifikacije kojima podležu kompanije koje se bave trgovinom preko Interneta uz primanje uplata kreditnim karticama. Kompanije koje prođu ovu sertifikaciju, imaju kod kompanija koje izdaju platne kartice značajno povoljnije uslove u pogledu provizija i načina refundiranja transakcija koje su posledica pronevera i zloupotreba. Ovaj standard obuhvata 12 područja svrstanih u 6 grupa. To su:

[I] Izgrađivanje i održavanje sigurne mreže

Zahtev 1: Instaliranje i održavanje konfiguracije zaštitne barijere radi zaštite podataka.

Zahtev 2: Ne koristiti podrazumevane vrednosti za lozinke i druge sigurnosne parametre.

[II] Zaštita podataka vlasnika platnih kartica

Zahtev 3: Zaštita uskladištenih podataka.

Zahtev 4: Šifrovanje podataka o karticama i drugih osetljivih informacija koje se prenose preko javnih mreža.

[III] Održavanje programa za rukovanje ranjivostima

Zahtev 5: Korišćenje i redovno ažuriranje antivirusnog softvera.

Zahtev 6: Razvoj i održavanje sigurnosnog sistema i aplikacija.

[IV] Implementacija strogih mera kontrole pristupa

Zahtev 7: Ograničavanje pristupa podacima po poslovnom principu “treba da zna”.

Zahtev 8: Dodela jedinstvene identifikacije svakom licu koje ima pristup računaru.

Zahtev 9: Ograničavanje fizičkog pristupa podacima o vlasnicima kartica.

[V] Redovno nadziranje i testiranje mreže

Zahtev 10: Praćenje i nadzor svih pristupa mrežnim resursima i podacima o vlasnicima kartica.

Zahtev 11: Redovno ispitivanje sigurnosnih sistema i procesa.

[VI] Održavanje politike sigurnosti informacija

Zahtev 12: Održavanje pravila koja se odnose na sigurnost informacija.

PROGRAMI SERTIFIKACIJE

Sigurnost je vrlo osetljivo područje. Mnoge firme i institucije žele da posebnu pažnju posvete proveru i sertifikaciji svojih proizvoda i usluga, kao i kadrova koji rade bilo kao zaposleni, bilo po ugovoru ili onih koji na drugi način (recimo kao poslovni partneri i saradnici) barataju osetljivim informacijama. Primera radi: u procesu ispitivanja mogu se otkriti osetljive informacije o organizaciji. Mnoge firme koje se bave ispitivanjem sigurnosti, trude se da dokažu kako ne zapošljavaju bivše hakere s crnim šeširima i kako se njihovi zaposleni na poslu drže strogih etičkih i moralnih principa.

Kao dodatna garancija pouzdanosti i poslovnosti ovih firmi, postoje sertifikati o stepenu poverenja, pouzdanosti i usklađenosti sa industrijskim standardima i najboljom praksom i procedurama, koje izdaju profesionalne i vladine (državne) institucije. U ovu svrhu su, pored standarda, uvedeni i brojni programi sertifikacija koje mogu propisivati vladine i zakonodavne agencije i/ili institucije, zatim profesionalne grupe i udruženja, a takođe i pojedini proizvođači opreme ili davaoci usluga. Evo nekih organizacija za sertifikaciju:

CISSP *Certified Information Systems Security Professional*

(CISSP®) sertifikacija daje profesionalcima u oblasti sigurnosti objektivno merilo kompetencije, kao i globalno priznat standard u pogledu dostignuća u ovoj oblasti. CISSP uverenje pokazuje kompetenciju u 10 domena (ISC) CISSP® CBK®. Ovo uverenje su akreditovalе organizacije ANSI i ISO (ISO 17024:2003) u polju informacione sigurnosti. CISSP uverenje, tj. sertifikat, potreban je rukovodiocima srednjeg i višeg nivoa koji nameravaju da budu ili su već na položajima CISO (*Chief Information Security Officer*), CSO (*Chief Security Officer*) ili SSE (*Senior Security Engineer*).

CHECK, CESC

U Velikoj Britaniji, glavni standard/akreditacija je CHECK šema koju administrira CESC (Communications-Electronics Security Group, deo GCHQ-a). Ovaj standard je obavezan preduslov za zapošljavanje u svim vladinim institucijama (centralnim, lokalnim, policijskim snagama itd.), i u mnogim komercijalnim „blue chip” organizacijama. Organizacije potpisnici ove šeme dužne su da održavaju stroge etičke norme, a od nosilaca sertifikata se automatski zahteva da imaju najmanje SC nivo sigurnosne provere (engl. *SC level security clearance*).

GIAC *Global Information Assurance Certification*

GIAC je osnovan 1999. godine, kako bi se proveravale realne i praktične veštine profesionalaca u oblasti IT sigurnosti i izdavao sertifikat o tome. Sertifikat GIAC je svojevrsno jemstvo da ovlašćena osoba ima praktična znanja i veštine koje se mogu primeniti u ključnim oblastima računarske sigurnosti. GIAC trenutno nudi sertifikovanje za 18 specifičnih tipova poslovnih odgovornosti koje odražavaju tekuću praksu informacione sigurnosti. GIAC je jedinstven po tome što meri pojedine specifične oblasti znanja umesto opštih znanja u oblasti informatičke sigurnosti.

GIAC sertifikacije su klasifikovane u 5 osnovnih područja: Security Administration (administriranje sigurnosti), Management (upravljanje), Operations (operacije), Legal (pravni aspekti), Audit (nadzor). Postoji nekoliko nivoa sertifikacije: srebrna, zlatna i platinasta (engl. *Silver, Gold, Platinum*).

CCSP - Cisco Certified Security Professional

CCSP sertifikacija je potvrda posedovanja naprednih znanja i veština koje su potrebne da se Cisco mreže učine sigurnim. Profesionalac u oblasti računarskih mreža koji ima sertifikat CCSP, vlada veštinama potrebnim za upravljanje mrežnim infrastrukturama, zaštitu produktivnosti i smanjivanje troškova. U CCSP kurikulumu (engl. *Curriculum*) naglašava se upravljanje VPN mrežama, Cisco Adaptive Security Device Manager (ASDM), PIX firewall, Adaptive Security Appliance (ASA), Intrusion Prevention Systems (IPS), Cisco Security Agent (CSA) kao i tehnike kojima se ove tehnologije kombinuju u jedinstvena i integrisana mrežna rešenja.

INFOSEC *Information Systems Security Professional Recognition*

Namena INFOSEC instrukcije je da ustanovi minimalni standard za obučavanje profesionalaca za sigurnost informacionih sistema (INFOSEC) i to u oblasti telekomunikacija i automatizovanih informacionih sistema.

NSTISSD 501 (*National Security Telecommunications and Information Systems Security Directive No.501*), **američka direktiva** sadrži zahtev da sva federalna ministarstva i agencije sprovedu programe obuke za INFOSEC profesionalce. Kao što je definisano u NSTISSD 501, INFOSEC profesionalac je osoba koja je odgovorna za pregled/nadzor ili rukovođenje, za nacionalne sigurnosne sisteme tokom određenih faza životnog ciklusa.

Direktiva 501 implementira se kroz zajednički rad odeljenja i agencija koje su obavezne da zadovolje INFOSEC obrazovne zahteve na najbolji i najefikasniji način. Ova instrukcija je prva u seriji standarda koji definišu minimum obuke i obrazovanja; ona treba da pomogne ministarstvima i agencijama da postignu i zadovolje zahteve u ovim područjima. Instrukcija važi kako za njihove zaposlene, tako i za saradnike po ugovoru (engl. *Contractors*).

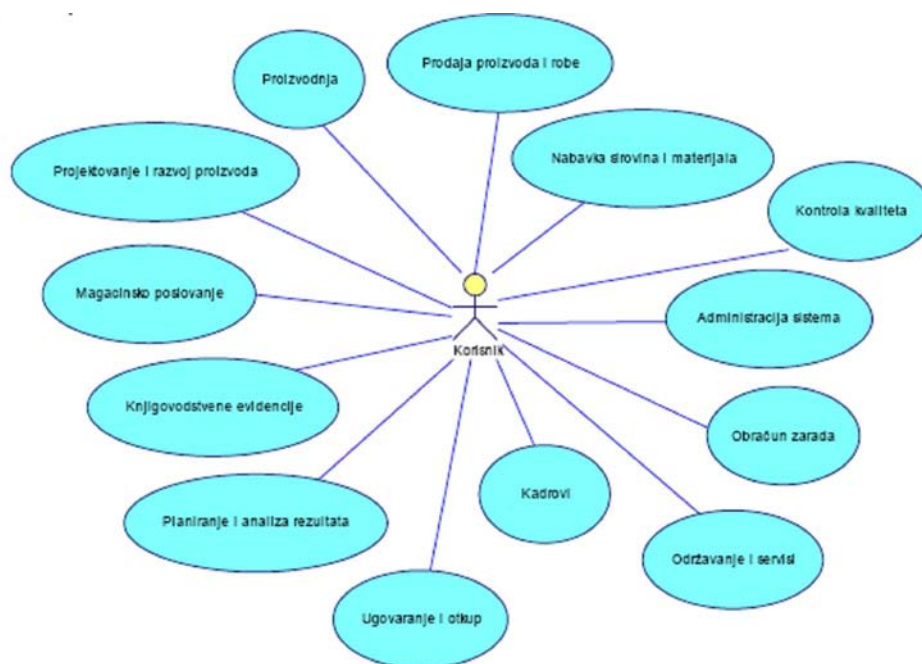
6. Prikaz implementacije ERP-a uz primenu bezbednosnih ISO standarda

Istorijski razvoj ERP-a

Početak upravljanja resursima i potrebama je razvijanje MRP (engl. *Material Requirements Planning*) kompjuterizovanih sistema koji su imali zadatak da upravljaju sistemom za planiranje proizvodnje i unapređuju poslovanje kontrole zaliha.

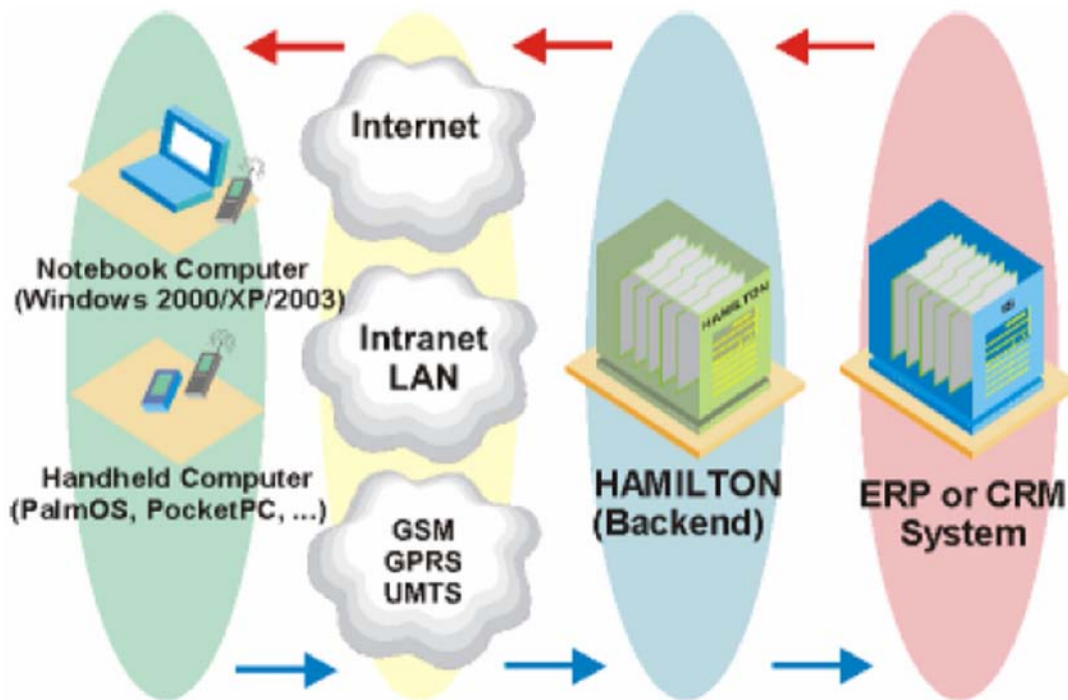
U drugoj fazi je razvijen MRP II (engl. *Manufacturing Resource Planing*) sistem koji obuhvata i module za podršku poslovnim funkcijama: praćenja proizvodnje u toku, nabavke, obračuna troškova, knjigovodstva kupaca i dobavljača.

Prema zahtevima savremenog poslovanja došlo je do stvaranja nove generacije poslovnih rešenja – ERP sistema koji uspevaju da dodatnim modulima za finansije, prodaju i distribuciju proizvoda, upravljanje ljudskim resursima (engl. *Human Resources Management*) (Sl.br.11) objedine sve oblasti poslovanja i samim tim povećaju efikasnost i produktivnost rada kompanija kroz efikasnu obradu strukturiranih podataka i integrisani su tako da mogu da zadovolje opšte poslovne potrebe integrisanog i umreženog preduzeća. Daljim razvojem ERP sistemi su se razvili u ERP II ili proširene ERP sisteme fokusirane na Internet orijentisana rešenja. Ovakva rešenja, koja omogućuju pristup resursima sistema sa bilo kog mesta i bilo kada, doprinose tome da se u ERP sisteme integrišu novi moduli, kao što su SCM (*Supply Chain Management*), CSM (*Customer Relationship Management*), Sales Force Automation (*SFA*), Advanced Planning and Scheduling (*APS*), Business Intelligence (*BI*) i e-Business mogućnosti.



Slika br.11 Use case dijagram jednog ERP sistema

Na slici 12 je prikaz Hamilton SFA softverskog rešenja (proširenje SAP-a), koje se može koristiti na različitim tipovima mobilnih uređaja radi povećanja efikasnosti prodaje.



Slika br.12 Hamilton SFA softversko rešenje kompatibilno sa ERP-om

6.1. Nabavka ERP-a

- Odluka o pokretanju nabavke

Vlasnik ili rukovodstvo kompanije, u zavisnosti od vlasničke strukture, na inicijativu zaposlenih u sektoru (službi) za IKT, donosi odluku o izboru dobavljača po pozivu ili javnim oglašavanjem, za izradu Studije izvodljivosti uvođenja novog informacionog sistema i izradi Idejnog projekta uvođenja ERP paketa. Radi izbora kvalitetnog dobavljača, uslove u konkursnoj dokumentaciji postaviti tako da ponude mogu podneti samo ozbiljne firme, zastupnici svetski priznatih proizvođača softvera, koji garantuju kvalitet svojim kapacitetima, referencama na tržištu, stečenim ugledom u branši i **sertifikatima koji su garancija kvaliteta ponuđača:**

- posedovanje međunarodno priznatog sertifikata kvaliteta ISO 9001:1994 (ISO 8402) – kojim se specificiraju zahtevi za sistem kvaliteta koji se koristi kada treba da bude pokazana sposobnost isporučioaca da projektuje i isporučuje usaglašen proizvod i da to dokumentuje odgovarajućim sertifikatom.

Kao garanciju kvaliteta i stručnosti personala, neophodno je zahtevati da potencijalni dobavljač u ponudi dostavi i strukovne sertifikate svojih stručnjaka i to:

- sertifikate firme *Microsoft* – (ako ERP radi na *Microsoft* platformi) da ponudjač zapošljava dovoljan broj *Microsoft* sertifikovanih sistem administratora MCSA (engl. *Microsoft Certified System Administrator*) i dovoljan broj *Microsoft* sertifikovanih sistem inženjera MCSE (engl. *Microsoft Certified System Engineer*) – ako ERP radi na platformi nekog drugog proizvođača prilažu se odgovarajući sertifikati tog proizvođača

- sertifikate da ponuđač zapošljava dovoljan broj sertifikovanih inženjera i tehničara za održavanje opreme koja se nudi uz softver, izdate od edukacionih centara firme proizvođača opreme (npr. Hewlett Packard sertifikati)
- sertifikate da ponuđač zapošljava dovoljan broj sertifikovanih stručnjaka za implementaciju i održavanje komunikacione opreme koja je predmet nabavke (npr. CCSP - Cisco Certified Security Professional)

Ovi sertifikati su potvrda posedovanja naprednih znanja i veština personala ponuđača, koje su potrebne da bi se izvršila dobra postavka temelja ERP-a – instalacija i konfigurisanje server room-a ili mainframe računara i mrežne infrastrukture, i time u startu postavio dobar **temelj sigurnosti informacionog sistema** i firme.

- Izrada studije izvodljivosti (engl. *Feasibility Study*)

Pozvani ponuđač, ili ponuđači prijavljeni na konkurs, pre nego što pristupe izradi Idejnog projekta, snimaju postojeće poslovne procese u svim poslovnim funkcijama kompanije i pristupaju izradi Studije izvodljivosti uvođenja ERP-a. Cilj ovih istraživanja je da se utvrdi spremnost kompanije da prihvati savremeni informacioni sistem podržan savremenom informacionom tehnologijom. Kroz ove aktivnosti utvrđuju se i eventualne prepreke koje treba ukloniti pre nego što se pristupi bilo kakvoj aktivnosti na projektovanju informacionog sistema. Posebno se ispituju sledeće sposobnosti kompanije po poslovnim funkcijama i u celini: opšta, organizaciona, kadrovska, finansijska. Sačinjene studije izvodljivosti, ponuđač(i) prezentiraju naručiocu.

- Izrada idejnog rešenja (projekta)

Nakon predstavljanja Studije izvodljivosti ponuđači pristupaju, izradi Idejnog projekta, kroz koji naručiocu prezentiraju softver koji nude i svoje viđenje novog informacionog sistema u kompaniji naručiocu. Izrada Idejnog projekta ima dva cilja:

- donošenje odluke o izgradnji integralnog informacionog sistema,
- donošenje odluke o troškovima i organizaciji informacionog sistema.

Kroz Idejni projekat preciziraju se sve informacije neophodne za donošenje ovih odluka. Idejni projekat je osnova za izradu Glavnog (izvršnog) projekta.

- Odluka o nabavci

Nakon završetka prezentacija(e) svih ponuđača, vlasnik kompanije ili top menadžment, na osnovu prezentiranih Idejnih rešenja, sagledava svoje potrebe, mogućnosti i ponudena rešenja i donosi Odluku o izboru dobavljača i izradi Glavnog projekta i kupovini ERP-a.

- Ugovor

Po izboru najbolje ponude, sačinjava se Ugovor o izradi Glavnog projekta i nabavci ERP paketa. Ugovor reguliše sva međusobna prava i obaveze obe strane, rok za izradu Glavnog projekta, rokove uvođenja pojedinačnih modula ERP-a, isporuka izvornih (engl. *Source*) verzija aplikativnog softvera, cene licenci sistemskog i aplikativnog softvera i njihove instalacije, rokove isporuke i instalacije, obuku korisnika, cene hardvera, rok isporuke i hladnog starta (engl. *Cold start*), cene konsultantskih usluga, valutu, rokove i način plaćanja, penale za neispunjene obaveze, garanciju (predmet garancije, dužinu trajanja garancije, vrstu garancije), kao i posebne stavke za koje naručilac ili ponuđač insistiraju da budu sastavni deo ugovora. Kao prilog ovog ugovora ili zasebno, sačinjava se ugovor o paušalnom održavanju koji osim specifikacije stavki održavanja, cena na mesečnom nivou i valute plaćanja, sadrži i garantovano vreme odziva na intervenciju i garantovano vreme popravke hardvera ili otklanjanja softverskog problema.

6.2. Izrada glavnog projekta

Kada ugovor stupi na snagu, izabrani dobavljač pristupa izradi Glavnog projekta. Glavni projekat je zasnovan na idejnom projektu, mnogo je detaljniji i precizniji od Idejnog projekta, stim, što naručilac može pismenim putem izneti svoje primedbe na Idejni projekat i sa ponuđačem ugovoriti da se neki delovi projekta izmene u meri koja ne narušava osnovnu ideju projekta.

6.3. Prestrojavanje kompanije

Shodno Glavnom projektu tj. "filozofiji" ERP-a, kompanija mora biti spremna da:

- organizaciju i poslovanje prilagodi Glavnom projektu ERP-a koji nabavlja. Neophodno je izraditi i sprovesti u praksi novu sistematizaciju radnih mesta. Ovo je jedan od najosetljivijih poslova jer se u praksi pokazalo da svaki ERP iziskuje dosta kadrovskih promena. Dolazi do:

- pojave tehnoloških viškova (obično radna snaga niske kvalifikacije),
- promene opisa poslova na postojećim radnim mestima (usložavanje poslova) a time i do promene vrednovanja poslova po radnim mestima,
- potrebe za zapošljavanjem novih visokoobrazovanih kadrova,
- potrebe za premeštanjem "bezbednosno nepodobnih" kadrova na radna mesta koja nisu u dodiru sa poslovima vezanim za ERP,
- potrebe za otvaranjem novih radnih mesta koja do uvođenja ERP-a nisu postojala,
- potrebe za informatičkim opismenjavanjem, dodatnim informatičkim edukovanjem i sertifikacijom (ECDL sertifikati) korisnika, odnosno dodatno doškolovanje i strukovna sertifikacija informatičara profesionalaca,
- pri uvođenju ERP-a obezbedi primenu bezbednosnih ISO standarda i time zaštiti svoju intelektualnu i materijalnu svojinu,
- uvođenjem novog ERP paketa istovremeno uvede ili poboljša postojeći TQM i IMS i time pripremi kompaniju za ravnopravnu utakmicu kvaliteta na domaćem i međunarodnom tržištu dobijanjem sertifikata sistema kvaliteta,
- pri uvođenju ERP-a obezbedi nesmetani paralelni rad postojećeg i novog poslovno informacionog sistema, do momenta potpunog prelaska na novi ERP. To je faza u toku koje se proverava i kontroliše kvalitet i pripremljenost novog ERP-a za optimalni rad.

6.4. Donošenje odluke o formiranju tima za uvođenje ERP-a i zaštitu podataka

Rukovodstvo kompanije donosi odluku o:

- formiranju glavnog tima za uvođenje ERP-a,
- formiranju podtimova za uvođenje ERP-a u svakoj poslovnoj funkciji,
- formiranju rukovodnog foruma za zaštitu informacija,
- odobravanju dokumenta o politici sigurnosti podataka (engl. *Security Policy*),
- primeni pravila prakse za upravljanje sigurnošću informacija pri uvođenju ERP-a (standard JUS ISO/IEC 17799),
- primeni ISF standarda dobre prakse zaštite,
- primeni ebXML globalnog standarda za poslovanje na internetu.

Glavni tim za uvođenje ERP-a

Za članove glavnog tima za uvođenje ERP-a imenuju se:

- vođa projekta - uobičajeno rukovodilac sektora za IKT, i članovi:
- članovi rukovodnog foruma za zaštitu informacija,
- vođe podtimova za uvođenje ERP-a iz svih poslovnih funkcija,
- lice odgovorno za uvođenje sistema kvaliteta i sertifikaciju u kompaniji,
- članovi iz sektora za IKT: rukovodioci službi za sistemski softver, implementaciju ERP-a, mreže i komunikacije, podršku IKT, lice zaduženo za ustanovljavanje šifarskog sistema, lice zaduženo za uvođenje bezbednosnih standarda u IKT.

Vođa projekta određuje i koordinira aktivnosti i zaduženja članova tima, određuje potrebe za konsultantskim uslugama i termine konsultacija, analizira postignute rezultate, razmenjuje iskustva sa članovima tima i periodično podnosi izveštaj vlasniku ili organu upravljanja o rezultatima i aktivnostima na uvođenju ERP-a, i po potrebi zahteva njihovo angažovanje na otklanjanju uskih grla.

Rukovodni forum za zaštitu informacija

Ova grupa unapređuje sigurnost unutar sopstvene organizacije odgovarajućim obavezivanjem i adekvatnim resursima. Forum može biti deo nekog postojećeg rukovodnog tela. Takav forum tipično preduzima sledeće:

- A. preispituje, odobrava i koordinira politiku sigurnosti i zaštite informacija i ukupne obaveze i odgovornosti,
- B. nadgleda znatnije izmene u izloženosti informacione imovine većim pretnjama,
- C. odobrava značajnije inicijative za poboljšanje sigurnosti informacija,
- D. uvodi, usaglašava i unapređuje kontrole za zaštitu informacija,
- E. obezbeđuje i osigurava da zaštita bude deo postupka planiranja informacija,
- F. preispituje incidente narušavanja sigurnosti.

Za sve aktivnosti u vezi sa sigurnošću informacija, obavezuje se i snosi odgovornost (samo) jedan rukovodilac.

Dokument Politika sigurnosti (engl. *Security Policy*)

Kao minimum dokument treba da odredi:

- a) vlasnika politike sigurnosti koji je zadužen za njeno održavanje i preispitivanje u skladu sa utvrđenim postupkom preispitivanja;
- b) definiciju sigurnosti informacija, njenih ukupnih ciljeva i područja primene kao i značaj sigurnosti kao mehanizma koji omogućuje zajedničko korišćenje informacija;
- c) izjava o namerama rukovodstva, sa podrškom ciljevima i principima zaštite informacija;
- d) kratko objašnjenje politike zaštite, principa, kriterijuma i zahteva za usaglašenost sa posebnim značajem za organizaciju sa:
 - 1) zakonskim i ugovornim zahtevima;
 - 2) zahtevima za školovanje u pogledu zaštite;
 - 3) ažurnim otkrivanjem i sprečavanjem virusa i drugih zloćudnih softvera;
 - 4) upravljanjem kontinuitetom poslovanja;
 - 5) posledicama kršenja politike zaštite;
- e) definicijama opštih i posebnih obaveza za upravljanje zaštitom informacija, uključujući izveštavanje o incidentima narušavanja sigurnosti;

f) dokumentacijom kojom se podržava politika.

Ovu politiku treba distribuirati korisnicima unutar organizacije u odgovarajućoj formi, koja je dostupna i razumljiva namenjenom čitaocu.

U dokumentu se moraju unapred predvideti periodična preispitivanja:

- a) efikasnosti politike, koja se pokazuje prirodom, brojem i uticajem zapisanih incidenata narušavanja sigurnosti,
- b) troškova i uticaja kontrolisanja na efikasnost poslovanja,
- c) učinka izmena u tehnologiji.

Takvo preispitivanje može se sprovesti funkcijom interne provere, angažovanjem nezavisnog rukovodioca ili organizacije treće strane koja je specijalizovana za takva preispitivanja, čiji kandidati imaju odgovarajuća znanja i iskustvo.

6.5 Obezbeđenje ambijentalnih i tehničkih uslova i fizička zaštita sektora za IKT

Rukovodni forum za zaštitu osigurava fizičku zaštitu sektora za IKT da bi se sprečilo neovlašćeno pristupanje, oštećivanje i smetanja u poslovnim prostorijama i na informacijama. Sačinjava se projekat zaštićenog područja koji treba da predvidi mogućnost oštećenja usled požara, poplave, eksplozije, socijalnih nemira i drugih oblika prirodnih nesreća ili ljudskog faktora. U projektu se uzimaju u obzir odgovarajući zdravstveni i bezbednosni propisi i standardi. Za smeštanje kritične i osetljive opreme za obradu informacija obezbeđuje se osigurani prostor, zaštićen u definisanom sigurnosnom prečniku, sa odgovarajućim sigurnosnim pregradama i kontrolom ulaska. Fizički je zaštićen od neovlašćenog pristupanja, oštećivanja i smetanja. Obezbeđuje se zaštita primerena identifikovanim rizicima.

Fizička zaštita se ostvaruje uspostavljanjem sigurnosnih krugova oko službenih prostorija i opreme za obradu informacija (nešto što predstavlja sazidanu prepreku, npr. zid, ulazna vrata sa kontrolom ulaska pomoću kartice ili prijavnica sa osobljem), a svaki od sigurnosnih krugova povećava zaštitu koja se pruža. Mesto i čvrstina svake prepreke zavisi od rezultata procene rizika. Rukovodni forum definiše sledeće smernice i kontrole:

- a) Uspostavlja obaveze i odgovornosti kao i procedure za rad i upravljanje celokupnom opremom za obradu informacija. Ovo obuhvata izradu odgovarajućih uputstava za rad i postupanje u slučaju incidenata.
- b) Definiše sigurnosni krug - ne sme da ima prekide kroz koje bi se lako mogao ostvariti upad. Zgrade treba da su nenametljive i da što je moguće manje ukazuju na svoju namenu, bez vidljivih oznaka izvan ili unutar zgrade, koje bi ukazivale na prisutnost aktivnosti obrade informacija. Spoljni zidovi oko mesta treba da su od čvrste konstrukcije a sva spoljna vrata odgovarajuće zaštititi protiv neovlašćenog pristupa: kontrolnim mehanizmima, šipkama, alarmima, bravama. Ključnu opremu postaviti tako da se izbegne javni pristup.
- c) Zaštićeno područje štiti se kontrolisanjem ulaznja. Pristup osetljivim informacijama, i opremi za obradu informacija, kontroliše se i ograničava samo na ovlašćene osobe. Osoblje mora da nosi neki oblik vidljive identifikacije. Posetioци zaštićenih područja se nadgledaju ili pretražuju a datum i vreme njihovog dolaska i odlaska se evidentira.
- d) Fizičke prepreke postavljaju se tako da se protežu od stvarnog poda do stvarnog plafona.
- e) Na sva protivpožarna pregradna vrata u sigurnosnom krugu postavlja se alarm i obezbeđuje se zatvaranje udarom.

- f) Oprema za obradu informacija kojom upravlja kompanija mora se odvojiti fizički od one kojom upravljaju treće strane.
- g) Imenici i spiskovi telefona u kojima su navedena mesta na kojima se nalazi osetljiva oprema za obradu informacija, ne smeju biti javno dostupni.
- h) Opasne ili zapaljive materije moraju da se skladište na bezbednom rastojanju od zaštićenog područja. U zaštićenim područjima, bez potrebe se ne skladište velike količine papira.
- i) Oprema za povratak na prethodno stanje i medijumi za čuvanje kopija moraju da se skladište na bezbednoj lokaciji da bi se izbeglo oštećenje usled nesreće na glavnom mestu.
- j) Osoblju treće strane za uslužnu podršku treba ograničiti pristup zaštićenom području ili osetljivoj opremi za obradu informacija. Ovakav pristup treba odobriti i treba ga nadgledati.
- k) Nije dozvoljena upotreba fotoaparata, video, audio ili drugih uređaja za zapisivanje, osim odobrenih.
- l) Opremu i uređaje treba fizički zaštititi od pretnji njihovoj sigurnosti i opasnosti iz okoline radi smanjenja rizika neovlašćenog pristupa podacima, gubitka i oštećenja. Za zaštitu od opasnosti ili neovlašćenog pristupa, kao i samozaštitu sredstava za podršku, uvesti posebne kontrole, kao nad električnim napajanjem i kablovskom infrastrukturom.
- m) Ustanoviti obaveznu evidenciju unošenja i iznošenja opreme, i uvesti kontrole kako bi se smanjio rizik potencijalnih pretnji koje obuhvataju: krađu, požar, eksplozive, dim, poplavu (ili prekid u snabdevanju vodom), prašinu, vibracije, hemijske uticaje, smetnje u električnom napajanju, elektromagnetska zračenja.
- n) Zabranjeno je konzumiranje hrane i pića, kao i pušenje u blizini opreme za obradu informacija.

Napajanje električnom energijom, klimatizacija i uređaj za samogašenje požara

Napisati i primeniti procedure za reagovanje u vanrednim situacijama. Zaštititi sve uređaje od nestanka struje i drugih anomalija obezbeđenjem neprekidnog napajanje u skladu sa proizvođačkim specifikacijama za opremu, prema sledećim opcijama:

- a) instalirati višestruke vodove kako bi se izbegao otkaz u jednoj tački napajanja;
- b) napajanje obezbediti preko uređaja za neprekidno napajanje (UPS);
- c) obezbediti rezervni električni generator i dovoljno pogonskog goriva;
- d) napajanje klima uređaja povezati preko UPS-a;
- e) u blizini izlaza za slučaj opasnosti postaviti prekidače napajanja kako bi se olakšalo isključivanje u vanrednim situacijama;
- f) postaviti panik svetlo za slučaj nestanka struje;
- g) na zgradu postaviti zaštitu od atmosferskih pražnjenja a na sve spoljne komunikacione vodove ugraditi zaštitne filtre;
- h) u server salu postaviti uređaj za samogašenje požara sa javljačima, povezati ga u jedinstveni sistem PPZ i napisati proceduru reagovanja u vanrednim situacijama;
- i) koristiti optičke kablove i zaštititi kablove napajanja i telekomunikacione kablove od prisluškivanja, oštećenja i neovlašćenog priključenja na njih, postavljanjem podzemnih, oklopljenih (engl. *Shielded*) kablova i razdvojiti ih na bezbednu udaljenost zbog elektromagnetnih smetnji;

- j) napisati procedure za korišćenje svih oblika ličnih računara, elektronskih rokovnika, mobilnih telefona, papirne ili druge forme, koje se drže na radu kod kuće ili koje se transportuju izvan normalnog mesta rada;
- k) napisati proceduru za postupak i sprovesti kontrolu sprovođenja pri odbacivanju ili rashodu uređaja koji sadrže medijume za čuvanje podataka;
- l) sprovesti politiku praznog stola i praznog ekrana i zabraniti iznošenje softvera u privatne svrhe.

6.6. Selekcija osoblja za rad u službi za IKT i ključnim tačkama IS kod korisnika

Obzirom da najnovija istraživanja pokazuju da čak 85% napada na bezbednost IS potiče od unutrašnjeg faktora (zaposleni u IKT i korisnici unutar kompanije), ovo je jedan od najbitnijih preduslova bezbednog funkcionisanja IS. Da bi se predupredili i smanjili rizici nastali delovanjem ljudskog faktora, obaveze i odgovornosti u pogledu sigurnosti i zaštite treba da se navedu još u ranim fazama koje su sadržane u radnim ugovorima, a nadgledaju se prilikom prijema pojedinaca u radni odnos.

- Selekcija profesionalnog osoblja za rad u IKT

Profesionalci za rad u IKT treba da zadovolje nekoliko bitnih preduslova pri prijemu u radni odnos:

1. odgovarajuće stručno zvanje (potvrđivanje iskazanih akademskih i profesionalnih kvalifikacija)
2. zdravstvenu pogodnost (za bezbednosno najodgovornija radna mesta traže se lica koja poseduju posebne psihičke sposobnosti)
3. provera (potpunosti i tačnosti) kretanja u zaposlenju
4. raspoloživost zadovoljavajućih referenci o karakteru, npr. jedna poslovna i jedna lična
5. uverenje da nisu osuđivani ili pod istragom
6. po mogućstvu posedovanje strukovnih sertifikata

Kao deo polaznih termina i uslova zapošljavanja, zaposleni treba da potpišu sporazum o poverljivosti ili obavezi čuvanja poslovne tajne. Uslovi zapošljavanja treba da iskazuju da se odgovornosti protežu i izvan prostorija organizacije i van radnog vremena, npr. u slučaju rada kod kuće, a po potrebi, radi zaštite od konkurencije i određeni vremenski period nakon odlaska iz kompanije. Za rad u službi za implementaciju ERP-a, treba izbeći da se u sektor za IKT prime stručnjaci iz pojedinih poslovnih funkcija (zbog dobrog poznavanja problematike poslova) koji nisu informatičari profesionalci, zbog sprečavanja stvaranja bezbednosno kritičnog mesta u sistemu zaštite. Praksa je pokazala da takve osobe skoro nikada ne prihvataju informatičku struku kao svoju, olako shvataju pretnje i brigu za sigurnost informacija, i ostaju sentimentalno vezani za posao i kolege sa kojima su ranije radili u drugom okruženju, i lako im „izlaze u susret“ pri rešavanju problema vezanih za IS.

- Selekcija korisnika za rad na informatičkoj opremi na ključnim tačkama IS

Na radna mesta po poslovnim funkcijama, za rad na informatičkoj opremi na ključnim tačkama IS (radna mesta koja po funkciji imaju ovlašćenja da ažuriraju podatke u IS ili puštaju i koriste izveštaje koji sadrže poverljive podatke) treba birati osobe koje:

1. nisu osuđivane ili pod istragom
2. poseduju dovoljno informatičkog znanja (ECDL sertifikat) i tehničke kulture za obavljanje predmetnog posla
3. su svojim odnosom prema radu i ponašanjem potvrdili odanost kompaniji

- Obuka korisnika

Pre davanja odobrenja za pristupanje informacijama ili servisima, kako bi se na minimum sveli mogući rizici u vezi sigurnosti, i da se osigura da korisnici budu svesni pretnji i brige za sigurnost informacija, kao i da budu opremljeni za podršku politici sigurnosti u organizaciji tokom svog normalnog rada, treba da završe obuku o procedurama zaštite i ispravnom korišćenju sredstava za obradu informacija. Sve zaposlene i ugovarače treba upoznati sa procedurama izveštavanja o raznim tipovima incidenata (proboj zaštite, pretnja, slabost ili zloćudno funkcionisanje) koji mogu imati uticaj na sigurnost imovine organizacije. Od njih treba zahtevati da zapisuju i izveštavaju o:

- svakom uočenom incidentu ili sumnjivom događanju što je pre moguće preko naznačene tačke za kontakt. Uspostaviti proceduru zvaničnog izveštavanja, zajedno sa procedurom za odziv na incidente, isticanjem akcija koje treba preduzeti po prijemu izveštaja o incidentu.
- svakom uočenom ili sumnjivom slabljenju sigurnosti ili pretnjama, sistemu ili uslugama.
- zloćudnim funkcijama softvera.

Sva znanja i iskustva iz incidentnih situacija posebno klasifikovati i akumulirati radi iskustvenog korišćenja.

- Postupak disciplinskog kažnjavanja

Uvesti zvaničan postupak kažnjavanja za zaposlene koji krše politiku i procedure zaštite u kompaniji. (Takav postupak služi za odvratanje zaposlenih koji bi mogli biti skloni da se ne pridržavaju postupaka zaštite.)

6.7. Upravljanje radom i komunikacijama

Da se osigura ispravan i siguran rad opreme za obradu informacija i zadovoljavajuće kontrolisanje svih izmena na uređajima, softveru ili u postupcima, treba uspostaviti obaveze i odgovornosti kao i procedure za rad i upravljanje celokupnom opremom za obradu informacija. Procedure za rad utvrđene politikom zaštite treba da se dokumentuju i održavaju. Treba uspostaviti periodičnu proveru procedura i njihovog poštovanja od strane internih proverivača zaduženih za uvođenje sistema TQM. Sa radnim procedurama treba postupati kao sa zvaničnim dokumentima, a izmene treba da odobri rukovodstvo. Moraju se pripremiti dokumentovane procedure za aktivnosti održavanja reda u sistemu zajedno sa pripadajućom opremom za obradu informacija i komunikacije, kao što su procedure za: pokretanje sistema i završetak rada, izrade rezervnih kopija, održavanje uređaja, upravljanje i bezbednost u prostoru sa računarima i sa poštom.

Treba izvršiti izradu odgovarajućih uputstava za rad i postupanje u slučaju incidenata.

- Izmene na programima

Izmene na operativnim programima rade se na pismeni zahtev (koji se čuva u arhivi) sa obrazloženjem podnosioca, odobrava ih nadležni rukovodilac, i podležu strogoj kontroli. Izmene u operativnom okruženju utiču na aplikativne programe. Zato, treba objediniti postupke za kontrolu izmena na operativnom i aplikativnom delu softvera. Procedurom propisati obavezu vođenja dnevnika rada koji je šifriran, potpisan od strane nadređenog rukovodioca i sadrži:

- a) identifikovanje i zapisivanje znatnijih izmena;
- b) procenjivanje mogućih posledica takvih izmena;
- c) postupak zvaničnog odobravanja predloženih izmena;
- d) informisanje svih odgovarajućih osoba o detaljima izmena;

e) procedure utvrđivanja obaveza za obustavljanje i oporavak od neuspešnih izmena

- Procedure za postupanje pri incidentima

Treba uspostaviti obaveze i odgovornosti za postupanje pri incidentima kako bi se osigurao brz, efikasan i uređeni odziv na incidente ugrožavanja sigurnosti. Treba predvideti sledeće kontrole:

a) Treba uspostaviti procedure kako bi se obuhvatili svi mogući tipovi incidenata, uključujući:

- 1) otkaze informacionog sistema i gubitak usluga;
- 2) odbijanje usluga;
- 3) greške koje nastanu od nekompletnih ili netačnih poslovnih podataka;
- 4) kršenje poverljivosti.

b) Pored normalnih planova za nepredviđene slučajeve (projektovanih za oporavak sistema ili servisa što je pre moguće) procedure treba takođe da obuhvate:

- 1) analizu i identifikovanje uzroka incidenata;
- 2) planiranje i ugradnju popravki da bi se sprečilo ponavljanje, ako je potrebno;
- 3) prikupljanje tragova za proveru i sličnih dokaza;
- 4) komuniciranje sa onima na koje je to uticalo ili su učestvovali u oporavku od incidenta;
- 5) izveštavanje odgovarajućih nadležnih o preduzetoj akciji.

c) Tragove za proveru i slične dokaze treba prikupljati i odgovarajuće zaštititi, radi:

- 1) interne analize problema;
- 2) korišćenja kao dokaza u vezi mogućeg kršenja ugovora, kršenja zakonskih obaveza ili u slučaju građanskih ili krivičnih procesa, npr. u vezi zakona o zloupotrebi računara ili zaštite podataka;
- 3) pregovaranja o naknadi od isporučilaca softvera i usluga.

d) Akcije za oporavak od proboja zaštite i otkaza ispravnih sistema treba pažljivo i zvanično kontrolisati. Procedure treba da osiguraju da:

- 1) samo jasno identifikovano i ovlašćeno osoblje ima dozvolu za pristup aktivnim sistemima i podacima;
- 2) sve preduzete hitne akcije budu detaljno dokumentovane;
- 3) o svim hitnim akcijama bude izvešteno rukovodstvo i da se one preispituju na jedan uređen način;
- 4) integritet poslovnih sistema i kontrola bude potvrđen uz minimalno kašnjenje.

- Razdvajanje zaduženja

Razdvajanje zaduženja je metoda za smanjivanje rizika od slučajnih i namernih zloupotreba sistema. Treba uraditi razdvajanje upravljanja i izvršenja određenih zaduženja ili područja odgovornosti, kako bi se smanjile povoljne prilike za neovlašćeno menjanje ili zloupotrebu informacija ili usluga. Zaduženja treba podeliti tako da nijedan pojedinac ne bude u stanju da počini prevaru u području pojedinačne odgovornosti a da ne bude otkriven. Inicijativu za neko događanje treba razdvojiti od njegovog odobravanja. Treba predvideti sledeće kontrole:

- a) Razdvojiti aktivnosti kod kojih je za prevaru potreban tajni dogovor, npr. povećanje porudžbine, od verifikovanja da je roba primljena.
- b) Za sprečavanje tajnih dogovora, treba napraviti takvu kontrolu da bude angažovano dvoje ili više ljudi, i time sniziti opasnost od zavere.

- Razdvajanje opreme za razvoj od opreme za rad

Treba izvršiti međusobno razdvajanje opreme na kojoj se obavljaju razvoj i ispitivanja od one na kojoj se radi i utvrditi nivo razdvajanja između radnog, ispitnog i razvojnog okruženja, kako bi se postiglo razdvajanje prisutnih uloga i time smanjio rizik od slučajnih izmena ili neovlašćenog pristupanja radnom softveru i poslovnim podacima. Pravila za prenošenje softvera iz statusa razvoja u radni status treba definisati i dokumentovati. Treba predvideti sledeće kontrole:

- a) Razvojni i radni softver treba da se, gde je moguće, izvršavaju na različitim računarima, ili u različitim domenima ili direktorijumima.
- b) Aktivnosti razvoja i ispitivanja treba da se što je moguće više razdvoje.
- c) Pomoćni programi za kompilaciju, unošenje izmena i dr. ne bi trebalo da su dostupni sa radnog sistema ako to nije potrebno.
- d) Za radne i ispitne sisteme treba koristiti različite procedure prijavljivanja, kako bi se smanjio rizik od grešaka. Korisnike treba usmeriti da na ovim sistemima koriste različite lozinke a na meniju treba da se prikazuju odgovarajuće poruke za identifikaciju.
- e) Osoblje iz razvoja treba da ima pristup radnim lozinkama samo tamo gde je uspostavljena kontrola izdavanja lozinki za podršku radnim sistemima. Kontrole treba da osiguraju da se posle korišćenja takve lozinke promene.

- Upravljanje izmeštenom opremom

U slučaju angažovanja spoljnog izvođača radi upravljanja opremom za obradu informacija može doći do: kompromitovanja, oštećenja, ili gubljenja podataka kod ugovorne strane. Ove rizike treba identifikovati unapred, a o odgovarajućim kontrolama treba se sporazumeti sa ugovaračem i uneti ih u ugovor. Posebni problemi koje treba uzeti u obzir obuhvataju:

- a) identifikovanje osetljivih ili kritičnih aplikacija koje je bolje zadržati kod kuće;
- b) dobijanje saglasnosti od vlasnika poslovnih softvera;
- c) posledice po planove kontinuiteta poslovanja;
- d) standarde o zaštiti koje treba navesti, kao i postupak za merenje usaglašenosti;
- e) dodela posebnih zaduženja i procedura za efikasno nadgledanje svih odgovarajućih aktivnosti vezanih za zaštitu;
- f) obaveze i postupci za izveštavanje i postupanje sa incidentima u vezi sigurnosti.

- Planiranje sistema

Da bi se na minimum sveli rizici otkaza sistema, smanjio rizik od preopterećenja sistema, i osigurala raspoloživost odgovarajućih kapaciteta i resursa, potrebne kapacitete treba projektovati za budućnost. Ovi planovi treba da uzmu u obzir nove poslove i sistemske potrebe kako za tekuće tako i za projektovane trendove u obradi informacija u organizaciji. Posebnu pažnju zahtevaju glavni računari, jer su mnogo veći troškovi i vreme kod nabavke novih kapaciteta. Rukovodioci službi održavanja treba da nadgledaju korišćenje ključnih sistemskih resursa, i utvrde trendove razvoja, a rukovodstvo treba da koristi ove informacije kako bi otkrilo potencijalna uska grla koja mogu predstavljati pretnju po sigurnost sistema ili korisničkih usluga, i planiraju odgovarajuće aktivnosti za njihovo otklanjanje.

- Prihvatanje sistema

Treba uspostaviti kriterijume za preuzimanje novih informacionih sistema, unapređenja i novih verzija. Rukovodioci treba da osiguraju da se jasno definišu zahtevi i kriterijumi za preuzimanje novih sistema, da se oni prihvate, dokumentuju i ispituju. Treba predvideti sledeće kontrole:

- a) zahtevi za radne karakteristike i kapacitete;
- b) oporavak posle grešaka i procedure ponovnog puštanja u rad, sa planovima za nepredviđene situacije;
- c) priprema i ispitivanje rutinskih radnih procedura prema definisanim kriterijumima;
- d) dogovoreni skup postavljenih kontrola za sigurnost;
- e) postavljene manuelne procedure;
- f) postavke za kontinuitet poslovanja;
- g) dokaz da postavljanje novog sistema neće nepovoljno uticati na postojeće sisteme; posebno u vreme najveće obrade, kao što je to krajem meseca;
- h) dokaz da je uzet u obzir uticaj novog sistema na ukupnu sigurnost organizacije;
- i) obuka za rad ili korišćenje novih sistema.

- Zaštita od zloćudnih softvera

Da bi se obezbedila celovitost i integritet softvera i informacija, potrebne su mere opreza kako bi se sprečilo i otkrilo uvođenje zloćudnih softvera. Zaštita od zloćudnih softvera treba da se zasniva na upućenosti u zaštitu, odgovarajućim kontrolama pristupanja sistemu i izmenama na softveru. Treba predvideti sledeće kontrole:

- a) zvaničnu politiku kojom se zahteva usaglašenost sa licencama za softver i zabranu korišćenja neautorizovanih softvera;
- b) zvaničnu politiku kojom se štiti protiv opasnosti od datoteka i softvera koji se dobijaju sa ili posredstvom spoljnih mreža, ili na bilo kojem drugom medijumu, sa ukazivanjem na zaštitne mere koje treba preduzeti;
- c) ugradnju i redovno ažuriranje softvera za zaštitu i oporavak od virusa i neželjenih poruka;
- d) sprovođenje redovnog preispitivanja sadržaja softvera i podataka u postupcima koji su kritični za poslovnu podršku. Prisutnost bilo kakvih neodobrenih datoteka ili neovlašćenih dopuna mora se zvanično istražiti;
- e) provere, pre korišćenja, prisutnosti virusa u svim datotekama na elektronskim medijumima čije je poreklo nesigurno ili neautorizovano, ili u datotekama koje su primljene preko neproverenih mreža; Ova provera može se sprovoditi na raznim mestima, npr. na serverima za elektronsku poštu, na stonim računarima ili prilikom ulaska na mrežu organizacije;
- f) propisati i primeniti procedure postupanja, obaveze i odgovornosti za rad na zaštiti sistema od virusa, obuci u njihovom korišćenju, izveštavanju i oporavku od napada virusima;
- g) odgovarajuće planove za kontinuitet poslovanja prilikom oporavka od napada virusima, uključujući sve neophodne podatke i postavke sa rezervnom kopijom softvera i sa podacima za oporavak;
- h) procedure za verifikovanje svih informacija o zloćudnim softverima i osiguravanje da su upozoravajući izveštaji informativni i tačni. Koristiti kvalifikovane izvore, proverene časopise, pouzdane lokacije na Internetu i isporučioce antivirusnih softvera. Osoblje treba uputiti u problem pojave lažnih (šaljivih) virusa i šta da sa njima rade nakon prijema.

- Održavanje reda u kući

Za održavanje celovitosti i raspoloživosti funkcija obrade informacija i komunikacija, treba uspostaviti rutinske postupke za sprovođenje dogovorene strategije izrade rezervnih kopija i njihovo pravovremenim isprobavanjem i obnavljanjem, beleženjem događaja i neispravnosti i, nadgledanjem okruženja u kojem se uređaji nalaze.

1. Izrada rezervnih kopija informacija

Rezervne kopije značajnih poslovnih informacija i softvera treba praviti redovno. Treba obezbediti odgovarajuću opremu za rezervne kopije kako bi se osiguralo da se sve značajne poslovne informacije i softveri mogu obnoviti posle nesreće ili otkaza medijuma. Treba predvideti sledeće kontrole:

- a) Minimalni nivo rezervnih kopija informacija, zajedno sa tačnim i kompletnim popisima rezervnih kopija i dokumentovanim postupcima za njihovo obnavljanje, treba čuvati na nekoj udaljenoj lokaciji.
- b) Rezervnim kopijama informacija treba dati odgovarajući nivo fizičke zaštite i zaštite od okruženja koji je saglasan sa kriterijumima koji se primenjuju na glavnoj lokaciji.
- c) Medijume sa rezervnim kopijama treba redovno proveravati, kako bi se osiguralo da se na njih može osloniti u vanrednim situacijama kada je to neophodno.
- d) Procedure za obnavljanje treba redovno proveravati i ispitivati kako bi se osiguralo da su upotrebljive i da se mogu do kraja sprovesti tokom vremena predviđenog radnim postupcima za oporavak. Treba utvrditi trajanje perioda održavanja važnih poslovnih informacija, kao i sve zahteve za trajno održavanje arhiviranih kopija.

2. Dnevnici rada operatera sistema i sistem inženjera

Zaposleno osoblje treba da održava dnevnike svojih aktivnosti. Dnevnici treba da budu: potpisani i overeni od strane nadređenog rukovodioca, sa numerisanim stranicama, valjano obeleženi sa šifrom procedure koja propisuje njihovu formu i da obuhvataju:

- a) datum i dan u nedelji;
- b) hronologiju i vreme izvršenja bitnih sistemskih komandi (podizanje, obaranje ili restart mainframe računara, servera, mreže i printing sistema, podizanje i obaranje baza podataka i mrežnih servisa i protokola) i stručni komentar u vezi preduzetih aktivnosti;
- c) hronologiju i vreme početka i završetka programa i jobova na sistemu;
- d) sistemske greške koje hardver pokazuje i preduzete mere za njihovo ispravljanje;
- e) važne sistemske poruke, kao i poruke vezane za regularnost rada baze podataka i aplikacija;
- f) informacije o administraciji sistema i baze podataka;
- g) potvrdu ispravnog rada sa datotekama podataka i izlazom iz računara;
- h) potpis osobe koja je izvršilac.

Dnevnike rada treba redovno i nezavisno proveravati i upoređivati sa radnim procedurama i po potrebi sa sistemskim log datotekama. Procedurom treba definisati period njihovog čuvanja nakon upotrebe.

- Upravljanje u mrežama

Da bi se osigurala samozaštita informacija u mrežama i zaštita infrastrukture za podršku, treba sprovesti upravljanje sigurnošću i zaštitom u mrežama shodno bezbednosnom ISF standardu dobre prakse zaštite (V. 4.0).

Treba uspostaviti DMZ (demilitarizovanu zonu) u konfiguraciji server sale i u njoj predvideti softverske (npr. Microsoft-ov ISA server) i hardverske (Firewall, IPS i IDS) prepreke upada u mrežu. Treba obezbediti mehanizme za zaštitu privatnosti, zaštitu podataka i

informacija i e-pošte, podizanje svesti o zaštiti, bezbedno korišćenje bežičnih komunikacija i PDA uređaja, metodologiju i tehnologiju forenzičke analize softvera, računara i računarske mreže. Na korisničkoj strani treba ograničiti broj računara sa kojih se pristupa Internetu, definisati za takve radne stanice poseban domen i izvršiti selekciju Internet adresa kojima je moguće pristupati, i prema politici sigurnosti (engl. *Security Policy*) regulisati korišćenje elektronske pošte.

- Kontrolisanje u mrežama

Rukovodioci mreža treba da ugrade kontrole kako bi se osigurala sigurnost podataka u mrežama, kao i zaštita pripadajućih usluga od neovlašćenog pristupa. Treba predvideti sledeće kontrole:

- a) Treba razdvojiti zaduženje za rad mreže od rada računara;
- b) Treba uspostaviti zaduženja i postupke za rad sa udaljenim uređajima, uključujući uređaje kod korisnika;
- c) Treba uspostaviti posebne kontrole za samozaštitu poverljivosti i celovitosti podataka koji prolaze preko javne mreže i kontrole za održanje raspoloživosti mrežnih usluga i priključenih računara;
- d) Aktivnosti upravljanja treba da budu usko koordinisane radi optimizovanja poslovnih usluga i osiguravanja da kontrole budu ujednačeno primenjene kroz infrastrukturu za obradu informacija.

- Postupanje sa medijumima i njihova zaštita

Treba uspostaviti odgovarajuće radne procedure za zaštitu dokumenata, računarskih medijuma (traka, diskova, kaseta), ulazno/izlaznih podataka i sistemske dokumentacije, od oštećenja, krađe i neovlašćenog pristupa.

1. Upravljanje prenosivim računarskim medijumima

Jasno dokumentovati sve procedure i nivoe ovlašćenja treba za postupanje sa prenosivim računarskim medijumima, kao što su trake, diskovi i otštampani izveštaji. Treba predvideti sledeće kontrole:

- a) Prethodni sadržaj svakog medijuma koji će se izneti i ponovo koristiti izvan organizacije, ako više nije potreban, treba da se izbriše.
- b) Za sve medijume koji se iznose iz organizacije treba tražiti odobrenje, a o svim takvim iznošenjima treba sačiniti zapis kako bi se sačuvao trag za proveru.
- c) Sve medijume treba čuvati na bezbednom i zaštićenom mestu, u skladu sa specifikacijama proizvođača.

2. Odbacivanje medijuma

Treba uspostaviti zvanične procedure za sigurnosno odbacivanje medijuma, kada više nisu potrebni, i odbacivati ih na sigurnosan i bezbedan način da ne mogu doći do osoba izvan organizacije. Treba predvideti sledeće kontrole:

- a) Medijume koji sadrže osetljive informacije treba čuvati i odbacivati na sigurnosan i bezbedan način, npr. spaljivanjem ili kidanjem, pražnjenjem podataka ili uništavanjem na uređaju za uništavanje medijuma.
- b) Sledeći oblici medijuma zahtevaju sigurnosno odbacivanje: papirni dokumenti, govorni ili drugi zapisi, listovi indiga, izlazni izveštaji, trake za štampanje sa jednokratnom upotrebom, magnetne trake, zamenljivi diskovi ili kasete, medijumi sa optičkim zapisima (svi oblici), izlistani programi, podaci o ispitivanjima, sistemska dokumentacija.

- c) Odbacivanje osetljivih elemenata treba gde je to moguće zapisivati kako bi se sačuvao trag za proveru.

3. Procedure za postupanje sa informacijama

Procedure za postupanje sa informacijama treba sačiniti tako da budu u skladu sa stepenom njihove poverljivosti u dokumentima, računarskim sistemima, mrežama, mobilnom izračunavanju, mobilnim komunikacijama, pošti, govornim pošiljkama, govornim komunikacijama u opštem smislu, multimedijumima, uređajima poštanskih usluga, korišćenju uređaja za faksimil i svim drugim osetljivim vrstama rada, npr. nepopunjenim čekovima i fakturama. Treba predvideti sledeće kontrole:

- a) rukovanje i stavljanje oznaka na sve medijume;
- b) ograničenja pristupa kako bi se identifikovalo neovlašćeno osoblje;
- c) održavanje zvaničnog zapisa sa podacima o ovlašćenim primaocima;
- d) osiguravanje da ulazni podaci budu kompletni, da se obrada u potpunosti dovrši i da se primeni ocenjivanje validnosti na izlazu;
- e) zaštita od nakupljanja podataka koji čekaju izlaz, na nivou koji je u skladu sa njihovom osetljivošću;
- f) čuvanje medijuma u uslovima koji su u skladu sa specifikacijama proizvođača;
- g) svođenje distribuiranja podataka na minimum;
- h) jasno označavanje svih kopija podataka koje se upućuju ovlašćenom primaocu;
- i) preispitivanje, u redovnim intervalima, spiskova za distribuiranje i spiskova ovlašćenih primalaca.

4. Zaštita sistemske dokumentacije

Sistemska dokumentacija može sadržati niz osetljivih informacija, npr. opise aplikativnih procesa, procedura i postupaka, procedura za dodelu ovlašćenja. Da bi se sistemska dokumentacija zaštitila od neovlašćenog pristupanja treba predvideti sledeće kontrole:

- a) Sistemske dokumentacije treba čuvati pod zaštitom.
- b) Spisak ovlašćenih za pristupanje sistemske dokumentaciji treba da je što uži i treba da ga odobri vlasnik aplikacije.
- c) Sistemska dokumentacija koja se stavlja na javnu mrežu, ili koja se dostavlja preko javne mreže, treba da bude odgovarajuće zaštićena.

5. Razmenjivanje informacija i softvera

Da bi se sprečilo gubljenje, menjanje ili zloupotreba informacija koje se razmenjuju između organizacija, razmenjivanje informacija i softvera među organizacijama treba da bude pod kontrolom, u skladu sa odgovarajućom pravnom podlogom. Treba uspostaviti procedure i kriterijume za zaštitu informacija i medijuma koji su u tranzitu i proceniti posledice na poslovanje i sigurnost pri elektronskoj razmeni podataka, elektronskoj trgovini i elektronskoj pošti. Među organizacijama treba uspostaviti sporazume o razmeni informacija i softvera (ručnoj ili elektronskoj). Sadržaj o zaštiti u takvom sporazumu treba da odražava poslovnu osetljivost takvih informacija. Sporazumi o uslovima sigurnosti i zaštite treba da predvide:

- a) obaveze rukovodstva u pogledu kontrolisanja i izveštavanja o prenosu, otpremi i prijemu;
- b) procedure za izveštavanje pošiljaoca, prenos, otpremu i prijem;
- c) minimalne tehničke kriterijume za pakovanje i prenos;
- d) kriterijume za identifikovanje kurira;
- e) obaveze i odgovornosti u slučaju gubitka podataka;

- f) primenu dogovorenog sistema označavanja osetljivih i kritičnih informacija, uz osiguranje da je značenje oznaka odmah razumljivo i da su te informacije odgovarajuće zaštićene;
- g) vlasništvo nad informacijama i softverom i odgovornost za zaštitu podataka, usklađenost sa pravima za kopiranje softvera i slične detalje;
- h) tehničke standarde za zapisivanje i čitanje informacija i softvera;
- i) sve posebne kontrole koje će možda biti potrebne da bi se zaštitili osetljivi detalji, kao što su šifarski ključevi.

6. *Zaštita medijuma u tranzitu*

Da bi se računarski medijumi zaštitili u toku transporta između lokacija, treba primeniti sledeće kontrole:

- a) Treba koristiti pouzdana sredstva transporta ili kurire. Rukovodstvo treba da dogovori i odobri spisak kurira a treba uvesti i proceduru za proveru identiteta kurira.
- b) Pakovanje treba da je dovoljno otporno da bi se sadržaj zaštitio od fizičkih oštećenja koja mogu da nastanu na putu, u skladu sa specifikacijama proizvođača.
- c) Treba uvesti posebne kontrole, gde je neophodno, kako bi se osetljive informacije zaštitile od neovlašćenog razotkrivanja ili menjanja. Na primer: korišćenje zaključanih kutija, ručno dostavljanje, pakovanje na kojem ostaje trag otvaranja (pokušaja pristupanja), deljenje pošiljke na više isporuka i otprema različitim putevima, primenu digitalnih potpisa i poverljivog šifrovanja.

7. **Sigurnost i zaštita u elektronskoj trgovini**

Elektronsku trgovinu treba organizovati prema ebXML standardu. Razmatranje sigurnosti kod elektronske trgovine treba da uključi sledeće kontrole:

- a) Utvrđivanje verodostojnosti. Koji će nivo poverljivosti biti potreban kupcu i trgovcu za proveru uzajamno izjavljenih identiteta?
- b) Autorizacija. Ko je ovlašćen da uspostavlja cene, izdaje ili potpisuje ključne prodajne dokumente? Kako trgovinski partner može to da sazna?
- c) Postupci ugovaranja i raspisivanja konkursa. Kakvi su zahtevi za poverljivost, celovitost i zaštitu pri otpremi i prijemu ključnih dokumenata i neporicanju ugovora?
- d) Informacije o cenama. Koji nivo poverenja se može staviti pod celovitost oglašenog cenovnika i poverljivost osetljivih dogovora o popustu?
- e) Druge transakcije. Kako se obezbeđuju poverljivost i celovitost porudžbine, detalji plaćanja i adrese isporuke, i potvrda prijema?
- f) Kontrola podobnosti. Koji stepen kontrole podobnosti je odgovarajući da bi se proverila informacija o plaćanju koju dostavi kupac?
- g) Poravnanje. Koja je najpogodnija forma plaćanja da bi se zaštitilo od prevare?
- h) Naručivanje. Kakva je zaštita potrebna da bi se održala poverljivost i celovitost informacija o porudžbini i da bi se izbegao gubitak ili dupliranje transakcije?
- i) Odgovornost. Ko snosi rizik od malverzacijskih transakcija.

Mnoge od navedenih kontrola mogu se rešiti primenom postupaka šifrovanja. Ugovori između partnera u elektronskoj trgovini treba da budu podržani na dokumentovan način i njima se obe strane obavezuju na uslove ugovora, uključujući detalje ovlašćivanja. Mogu biti neophodni i drugi ugovori sa davaocima informativnih i proširenih mrežnih usluga.

8. Zaštita elektronske pošte

Treba zacrtati jasnu politiku u pogledu elektronske pošte, uključujući:

- a) napade na elektronsku poštu, npr. viruse, prisluškivanja;
- b) zaštitu od sadržaja pridodatih elektronskoj pošti;
- c) uputstva kada ne treba koristiti elektronsku poštu;
- d) dužnosti zaposlenih kako se preduzeće ne bi kompromitovalo, npr. slanje elektronske pošte sa klevetama, primene dosađivanja, neovlašćeno kupovanje;
- e) korišćenje kriptografskih postupaka kako bi se zaštitili poverljivost i integritet elektronskih poruka;
- f) zadržavanje poruka koje bi, ako se sačuvaju, mogle biti otkrivene u slučaju sudskog spora;
- g) dodatna kontrolisanja radi istraživanja valjanosti poruka za koje se ne može proveriti verodostojnost.

9. Sistemi sa javnim pristupom

Softver, podaci i druge informacije za koje se zahteva visok nivo integriteta, koji se stavljaju na raspolaganje na javno dostupnim mrežama, treba zaštititi digitalnim potpisima. Sisteme za elektronsko objavljivanje, posebno one koji dozvoljavaju povratne odgovore i direktno unošenje informacija, treba pažljivo kontrolisati tako da se:

- a) informacije dobijaju u skladu sa svim propisima o zaštiti podataka;
- b) informacije, koje se unose i obrađuju u sistemu za objavljivanje, obrađuju u potpunosti, tačno i na vreme;
- c) osetljive informacije zaštite u toku postupka prikupljanja i prilikom skladištenja i čuvanja;
- d) pristupanje sistemu za objavljivanje ne omogući neželjeni pristup na mreže na koje je on priključen.

Treba uspostaviti procedure kojih osoblje treba da se pridržava prilikom korišćenja govornih, faksimil i video komunikacija.

Kontrolisanje pristupa

- Poslovni zahtevi za kontrolisanje pristupanja

Zahtevi poslovanja za kontrolisanje pristupa treba da budu definisani i dokumentovani. Pravila za kontrolisanje pristupa i prava svakog korisnika ili grupe treba da budu jasno iskazana u poslovniku o politici pristupanja. Korisnicima i davaocima usluga treba dati jasan stav o zahtevima poslovanja koji treba da se ispune putem kontrolisanja pristupa.

Ova politika treba da uzme u obzir sledeće:

- a) zahteve za sigurnost i zaštitu pojedinačnih poslovnih aplikacija;
- b) identifikovanje svih informacija koje su u vezi sa poslovnim primenama;
- c) politiku distribuiranja informacija i dozvola, npr. potreba za poznavanjem principa i nivoa zaštićenosti i klasifikovanja informacija;
- d) usklađenost između kontrolisanja pristupa i politike klasifikovanja informacija u različitim sistemima i mrežama;
- e) odgovarajuće zakonodavstvo i svaku ugovornu obavezu u pogledu zaštite pristupa podacima ili uslugama;
- f) profile pristupa standardnih korisnika za uobičajene kategorije posla;

- g) upravljanje pravima na pristup u distribuiranim i mrežnim okruženjima koje prepoznaju sve tipove priključaka koji su na raspolaganju.

1. Pravila za kontrolisanje pristupa

Prilikom specificiranja pravila za kontrolisanje pristupa, treba obratiti pažnju da se u obzir uzme sledeće:

- a) uvođenje razlike između pravila koja se moraju uvek sprovoditi i pravila koja su pitanje izbora ili su uslovljena;
- b) uspostavljanje pravila koja se zasnivaju na premisi "šta mora u opštem slučaju biti zabranjeno osim ako nije izričito dozvoljeno", umesto "Sve je u opštem slučaju dozvoljeno ukoliko nije izričito zabranjeno";
- c) promene oznaka na informacijama koje oprema za obradu informacija inicira automatski i one koje ekskluzivno inicira korisnik;
- d) promene odobrenja za korišćenje koje informacioni sistem inicira automatski i one koje inicira administrator;
- e) pravila za koja se pre proglašenja zahteva odobrenje upravnika (administratora) ili neko drugo odobrenje i ona za koja se to ne zahteva;

2. Upravljanje pristupanjem korisnika

Ove procedure treba da obuhvate sve faze životnog ciklusa korisnikovog pristupa, od polaznog registrovanja novih korisnika do završnog brisanja korisnika kojima više nije potreban pristup informacionim sistemima i uslugama.

- Registrovanje korisnika

Treba da postoji zvanična procedura za registrovanje i za brisanje korisnika iz registra odobrenja pristupa višekorisničkim informacionim sistemima i uslugama, koja obuhvata:

- a) korišćenje jedinstvenog identifikatora ID za koji se korisnici mogu vezati i učiniti odgovornim za svoje aktivnosti. Korišćenje grupnih identifikatora ID treba dozvoliti samo gde je to pogodno za obavljanje posla;
- b) proveravanje da korisnik ima odobrenje od vlasnika sistema za korišćenje tog informacionog sistema ili usluge. Mogu odgovarati i zasebna odobrenja rukovodstva u pogledu prava na pristupanje;
- c) proveravanje da odobreni nivo pristupa odgovara poslovnoj nameni i da je u skladu sa politikom sigurnosti i zaštite, npr. da ne narušava razdvajanje dužnosti;
- d) davanje korisnicima iskaza u pisanoj formi o njihovim pravima na pristup;
- e) zahtevanje od korisnika da potpišu iskaze u kojima se ukazuje na to da oni razumeju uslove pod kojima pristupaju;
- f) uveravanje da davaoci usluga neće davati pravo pristupa dok se ne dovrše postupci odobravanja;
- g) održavanje zvaničnih zapisa o svim osobama registrovanim za korišćenje usluga; h) neposrednim oduzimanjem prava na pristupanje korisnicima koji su promenili vrstu posla ili su napustili organizaciju;
- h) periodično proveravanje i uklanjanje višestrukih ID identifikatora korisnika i računa;
- i) osiguravanje da se višestruki identifikatori nekog korisnika ne izdaju drugim korisnicima.

U ugovorima sa osobljem ili zastupnicima u davanju usluga definisati članove u kojima se navode kazne za pokušaje neovlašćenog pristupanja sistemu.

- Preispitivanje prava korisnika na pristup

Da bi se održala efikasna kontrola pristupanja podacima i informacionim uslugama, rukovodstvo treba da u pravilnim razmacima sprovodi zvanični postupak preispitivanja prava korisnika na pristupanje.

- Upravljanje povlasticama

Dodelu i korišćenje povlastica (svaka funkcija ili uređaj u višekorisničkom informacionom sistemu koja korisniku omogućava prevladavanje ili zaobilazanje sistemskih ili aplikacijskih kontrola) treba izbeći.

- Obaveze korisnika

Za efikasnu sigurnost i zaštitu osnovna je saradnja ovlašćenih korisnika. Korisnici treba da budu svesni svoje odgovornosti za održavanje funkcionisanja kontrole pristupa, posebno u pogledu korišćenja lozinki i zaštite korisnikovih uređaja.

- Upravljanje korisničkim lozinkama

Lozinke (engl. *Password*) su uobičajeno sredstvo za validaciju korisnikovog identiteta radi pristupanja nekom informacionom sistemu ili usluzi. Dodelu lozinki treba kontrolisati kroz zvanični postupak upravljanja, kojim treba:

- a) zahtevati od korisnika da potpišu iskaz da će lične lozinke držati poverljivo a lozinke radne grupe samo među članovima te grupe;
- b) osigurati, gde se od korisnika zahteva da imaju svoje sopstvene lozinke, da im se na početku obezbede tajne privremene lozinke koje oni moraju odmah da izmene;
- c) tražiti da se privremena lozinka korisnicima daje na zaštićen način.

Lozinke nikada ne treba čuvati u računarskom sistemu u nezaštićenom obliku.

- Korišćenje lozinke

Prilikom izbora i korišćenja lozinki korisnici treba da se pridržavaju dobre prakse sigurnosti. Svim korisnicima treba savetovati da:

- a) lozinke drže u tajnosti i izbegavaju čuvanje lozinki zapisanih na papiru;
- b) zamenjuju lozinke kada god postoji bilo kakav signal o mogućem kompromitovanju sistema ili lozinke;
- c) odaberu dobru lozinku dužine od najmanje šest znakova koji se lako pamte i nisu zasnovani na bilo čemu što bi neko drugi mogao da pogodi ili dobije korišćenjem ličnih podataka osobe;
- d) koji u sebi ne sadrže uzastopne identične znakove ili grupe od isključivo brojeva ili slova;
- e) menjaju svoje lozinke u pravilnim razmacima i da izbegavaju ponovno korišćenje ili ponavljanje starih lozinki;
- f) zamene privremenu lozinku pri prvom prijavljivanju;
- g) da lozinke ne stavljaju u bilo koji automatizovani postupak prijavljivanja, npr. pod makro ili funkcionalni taster;
- h) da ne koriste zajedno istu pojedinačnu lozinku.

- Korisnički uređaji koji su bez nadzora

Uređaji postavljeni kod korisnika, npr. radne stanice ili serveri sa datotekama, mogu zahtevati posebnu zaštitu od neovlašćenog pristupanja kada se oni na duže vreme ostave bez nadzora.

- Kontrolisanje pristupa na mrežu

Treba kontrolisati pristup internim i eksternim mrežnim uslugama (servisima) da bi se osiguralo da korisnici koji imaju pristup na mrežu i mrežne usluge ne naruše sigurnost ovih mrežnih usluga obezbeđenjem:

- a) odgovarajućih međuspojeva između sopstvene mreže i mreža čiji su vlasnici druge organizacije, ili javnih mreža;
- b) odgovarajućeg mehanizma za proveru verodostojnosti korisnika ili uređaja;
- c) kontrolisanjem pristupa korisnika informacionim uslugama.

- Politika korišćenja mrežnih usluga (servisa)

Treba formulisati politiku u pogledu korišćenja mreže i mrežnih usluga. Ovim treba da se obuhvati sledeće:

- a) mreže i mrežne usluge kojima je pristup dozvoljen;
- b) procedure za utvrđivanje verodostojnosti prilikom utvrđivanja kome je dozvoljeno da pristupa kojoj mreži i kojim mrežnim uslugama;
- c) postupci i procedure upravljanja za zaštitu pristupa mrežnim priključcima i uslugama;

Ova politika treba da je u skladu sa politikom kontrolisanja poslovnog pristupanja;

- Zadana staza

Postoji potreba da se kontroliše staza od korisnikovog terminalskog uređaja do računarske usluge. Cilj neke zadate staze je da se spreči pristup neodobrenim podacima i uslugama na sistemu. Načini definisanja zadate staze:

- a) dodela određenih vodova ili telefonskih brojeva;
- b) automatsko uključivanje pristupa na sisteme sa navedenom aplikacijom ili na sigurnosne prolaze;
- c) ograničavanje opcija u meniju i podmeniju za pojedinačne korisnike;
- d) sprečavanje neograničenog pretraživanja na mreži;
- e) upućivanje spoljnih korisnika mreže na korišćenje navedenih sistema sa aplikacijama i/ili sigurnosnim prolazima;
- f) aktivno upravljanje dozvoljenim komunikacijama izvorišta prema odredištu preko sigurnosnih prolaza, npr. zaštitnim pregradnim zidovima;
- g) ograničavanje pristupanja mrežama postavljanjem odvojenih logičkih domena, npr. virtuelnih privatnih mreža, za grupe korisnika unutar organizacije.

- Provera verodostojnosti korisnika na spoljnim priključcima

Kod pristupa udaljenih korisnika mora se sprovesti utvrđivanje verodostojnosti. Provera verodostojnosti udaljenih korisnika može se ostvariti primenom, postupka na kriptografskoj osnovi, hardverskim žetonima, ili protokolom sa upitom/ odgovorom. Da bi se obezbedila zaštita izvorne strane na priključku, mogu se takođe koristiti dodeljeni privatni vodovi ili mrežni uređaji za proveru korisničke adrese.

- Provera verodostojnosti u čvorištima

Provera verodostojnosti u čvorištima može služiti kao alternativno sredstvo za proveru verodostojnosti grupa udaljenih korisnika pri čemu se oni priključuju na zaštićenu računarsku opremu sa zajedničkim korišćenjem.

- Razdvajanje u mrežama

Jedna metoda za kontrolisanje sigurnosti u velikim mrežama je da se one podele u odvojene mrežne logičke domene, npr. na domene interne mreže organizacije i na domene spoljne mreže, pri čemu se svaki domen štiti u definisanom prečniku. Takav prečnik se

može uvesti postavljanjem sigurnosnog priključka između dva domena. Ovakav priključak treba da se konfiguriše tako da filtrira saobraćaj između tih domena i da zaustavlja neovlašćeno pristupanje u skladu sa politikom organizacije za kontrolisanje pristupa. Primer ovakvog tipa priključka se obično navodi kao zaštitni pregradni zid.

- Kontrolisanje priključaka na mrežu

Prema politici pristupanja i zahtevima za poslovne aplikacije treba ograničiti mogućnost korisnika za neovlašćeno priključivanje na mrežu, i uvesti kontrole preko mrežnih priključaka koji filtriraju saobraćaj pomoću prethodno definisanih tabela ili pravila.

- Kontrolisanje preusmeravanja u mreži

Kod mreža koje se koriste zajedno sa korisnicima koji nisu iz organizacije (trećim stranama), upravljanje preusmeravanjem treba da se zasniva na mehanizmima za pouzdanu proveru adrese izvorišta i odredišta. Prevođenje adrese na mreži je takođe vrlo koristan mehanizam za razdvajanje mreža i sprečavanje puteva za prostiranje sa mreže jedne organizacije u mrežu neke druge organizacije.

Oni se mogu ugraditi u softver ili u hardver. Primenioci treba da poznaju snagu svakog mehanizma koji je postavljen.

- Kontrola pristupanja operativnom sistemu

Za ograničavanje pristupa računarskim resursima treba da se koriste sigurnosna sredstva na nivou rada sistema. Ova sredstva treba da imaju sledeće sposobnosti:

- a) identifikovanje i verifikovanje identiteta, a ako je neophodno i terminalskog uređaja ili lokacije ovlašćenog korisnika;
- b) zapisivanje uspešnih i neuspešnih pristupanja sistemu;
- c) pružanje odgovarajućih mehanizama za proveru verodostojnosti; ako se koristi sistem za upravljanje lozinkama, on treba da osigura kvalitetne lozinke;
- d) tamo gde to odgovara, ograničavanje dužine trajanja priključivanja korisnika.

- Korišćenje sistemskih pomoćnih programa

Najveći broj ugrađenih računara sadrži jedan ili više pomoćnih programa kojim se mogu prevladati postojeće kontrole u sistemu ili aplikaciji. Bitno je da njihovo korišćenje bude ograničeno i strogo kontrolisano. Treba predvideti sledeće kontrole:

- a) kod sistemskih pomoćnih programa, korišćenje procedura za utvrđivanje verodostojnosti;
- b) izdvajanje sistemskih pomoćnih programa iz aplikacijskog softvera;

Da bi se podržali zahtevi za ograničenje pristupa, treba predvideti primenu sledećih kontrola:

- a) obezbeđenje menija (opcija) za kontrolu pristupa funkcijama aplikativnog sistema;
- b) ograničavanje korisnicima poznavanja informacija ili funkcija aplikativnog sistema kojima oni nisu ovlašćeni da pristupaju, unošenjem odgovarajućih izmena u korisničku dokumentaciju;
- c) kontrolisanje prava korisnika kod pristupanja, npr. na čitanje, upisivanje, brisanje ili izvršavanje;
- d) osiguravanje da podaci na izlazu iz aplikativnih sistema u kojima se radi sa osetljivim podacima sadrže samo informacije koje se odnose na primenu tih izlaznih podataka i da se oni šalju samo prema odobrenim terminalskim uređajima i lokacijama, uključujući periodično preispitivanje takvih izlaznih podataka kako bi se osiguralo da se nepotrebne informacije uklanjaju.

- Izdvajanje osetljivih sistema

Osetljivi sistemi mogu zahtevati posebno (izdvojeno) računarsko okruženje. Ova osetljivost može ukazivati na to da takav aplikativni sistem zahteva izvršenje na nekom određenom računaru, da koristi zajedničke resurse samo sa poverljivim aplikativnim sistemima, ili da ne treba da ima ograničenja. Primenljiva su sledeća rešenja:

- a) Osetljivost nekog aplikativnog sistema vlasnik takve aplikacije treba da eksplicitno utvrdi i dokumentuje;
- b) Kada neku osetljivu aplikaciju treba izvršavati u zajedničkom okruženju, treba identifikovati aplikativne sisteme sa kojima se resursi zajednički koristiti a o tome treba da se postigne sporazum sa vlasnikom te osetljive aplikacije.

- Nadgledanje pristupa i korišćenja sistema

Sisteme treba nadgledati kako bi se otkrila odstupanja od politike kontrole pristupa i zapisali uočljivi događaji kako bi se obezbedili dokazi za slučajeve incidenata u pogledu sigurnosti.

1. Nadgledanje pristupa i zapisivanje događanja

Treba sačiniti zapisnike provere sa zapisanim izuzetnim događanjima i drugim događajima u vezi sigurnosti a treba ih čuvati u određenom periodu kako bi se pomoglo u budućem istraživanju i nadgledanju kontrole pristupa. Zapisnici provere treba da uključuje:

- a) korisničke identifikatore (ID);
- b) datume i vremena prijavljivanja i odjavljivanja;
- c) identitet terminalskog uređaja ili njegova lokacija ukoliko je moguće;
- d) zapisi o uspešnim i odbijenim pokušajima pristupanja sistemu;
- e) zapise o uspešnim i odbijenim pokušajima pristupanja podacima i drugim resursima.

Prilikom dodeljivanja obaveza za preispitivanje zapisa, treba praviti razliku između osoba koje to preduzimaju i onih čije se aktivnosti nadgledaju. Posebnu pažnju treba pokloniti sigurnosti opreme za zapisivanje jer ako se sa njom nestručno radi ona može dati neispravan utisak o sigurnosti.

- Sinhronizacija satova

Da bi se osigurala tačnost zapisa za provere važno je ispravno postavljanje računarskih taktova, što može biti potrebno prilikom istrage ili kao dokaz pri pravnim sporovima ili kažnjavanju. Neprecizni zapisi provere mogu smetati u takvim istragama i mogu naškoditi verodostojnosti takvih dokaza.

2. Nadgledanje korišćenja sistema

Treba uspostaviti procedure za nadgledanje korišćenja opreme za obradu informacija. Potrebni nivo nadgledanja kod pojedinačne opreme treba odrediti preko ocenjivanja rizika. Oblasti koje treba uzeti u obzir uključuju:

- a) ovlašćeno pristupanje, uključujući detalje kao što su:
 - 1) identifikator korisnika (ID);
 - 2) datum i vreme ključnih događanja;
 - 3) tipove događanja;
 - 4) datoteke kojima se pristupalo;
 - 5) korišćeni program / pomoćni programi;
- b) sve povlašćene operacije, kao što su:
 - 1) korišćenje nadzorničkog računara;
 - 2) puštanje u rad i zaustavljanje sistema;
 - 3) priključivanje /odspajanje ulazno /izlaznog uređaja;

c) pokušaje neovlašćenog pristupanja, kao što su:

- 1) neuspeli pokušaji;
- 2) kršenja politike pristupa i javljanje na ulazu u mrežu i na zaštitnim pregradama;
- 3) upozorenja iz sistema za otkrivanje upada u imovinu;

d) sistemska upozorenja ili otkazi kao što su:

- 1) upozorenja ili poruke na konzoli;
- 2) izuzeci prilikom prijavljivanja na sistem;
- 3) alarmi iz upravljanja mrežom.

3. Faktori rizika

Treba redovno pregledati rezultate aktivnosti nadgledanja. Učestalost pregledanja treba da zavisi od prisutnih rizika. Faktori rizika koje treba uzeti u obzir uključuju:

- a) kritičnost aplikativnih procesa;
- b) vrednost, osetljivost ili kritičnost prisutnih informacija;
- c) prethodna iskustva o infiltracijama i zloupotrebama sistema;
- d) obim povezanosti sistema (posebno sa javnim mrežama).

- Rad na nestacionarnim računarima (prenosivi uređaji) i rad sa udaljenosti

Potrebna zaštita treba da bude istog obima kao i rizici do kojih dovodi ovakav način rada.

1. Rad sa prenosivim računarima

Kada se koristi prenosiva (nestacionarna) računarska oprema, npr. rokovnici, računari koji se drže na dlanu, računari koji se drže na krilu i mobilni telefoni, treba usvojiti zvaničnu politiku kojom se uzimaju u obzir rizici rada sa prenosivom računarskom opremom, i preduzeti posebne mere kako bi se osiguralo da se poslovne informacije neće kompromitovati. Takva politika treba da uključi pravila za fizičku zaštitu, kontrolu pristupa, kriptografske postupke, rezervne kopije i zaštitu od virusa. Treba sprovesti obuku osoblja koje koristi nestacionarnu računarsku opremu, kojom treba povećati njihovo znanje o dodatnim rizicima do kojih dolazi usled ovakvog načina rada i o kontrolama koje treba ugraditi.

2. Rad sa udaljenosti

Kod rada sa udaljenosti primenjuju se komunikacione tehnologije kako bi se osoblju omogućilo da radi na udaljenoj lokaciji izvan sopstvene organizacije. Na udaljenoj lokaciji treba da je postavljena odgovarajuća zaštita, npr. protiv krađe uređaja i informacija, neovlašćenog razotkrivanja informacija, neovlašćenog daljinskog pristupa unutrašnjim sistemima organizacije ili zloupotrebe opreme. Organizacije treba da odobre rad sa udaljenosti tek ako su zadovoljne ugrađenim odgovarajućim sredstvima zaštite i kontrolama i ako su one u skladu sa politikom sigurnosti u organizaciji. Organizacije treba da kod rada sa daljine razmotre izradu politike, procedura i kriterijuma za kontrolisanje aktivnosti. Treba razmotriti sledeće:

- a) postojeću fizičku sigurnost mesta za rad sa udaljenosti, uzimajući u obzir fizičku sigurnost zgrade i lokalnog okruženja;
- b) predloženo okruženje za rad sa udaljenosti;
- c) zahteve za zaštitu komunikacija, uzimajući u obzir potrebe za daljinsko pristupanje sistemima unutar organizacije, osetljivost informacija kojima se pristupa ili koje se predaju preko komunikacionih veza i osetljivost internih sistema;
- d) pretnja neovlašćenog pristupanja informacionim resursima od strane drugih ljudi koji koriste isti smeštaj, npr. kod rodbine i prijatelja.

Kontrole i sredstva koja treba predvideti su:

- a) obezbeđenje pogodnih uređaja i opreme za smeštaj kod rada sa udaljenosti;
- b) definisanje dozvoljene vrste posla, radnih časova, klasifikovanje informacija koje mogu biti sadržane i interni sistemi i usluge za koje je dozvoljeno da im udaljeni radnik može pristupati;
- c) obezbeđenje pogodnih komunikacionih uređaja, uključujući metode za zaštitu kod daljinskog pristupanja;
- d) fizička sigurnost;
- e) pravila i smernice o dostupnosti uređaja i informacija rođacima i posetiocima;
- f) obezbeđenje hardverske i softverske podrške i održavanja;
- g) procedure izrade rezervnih kopija i kontinuiteta poslovanja;
- h) provera i nadgledanje sigurnosti;
- i) ukidanje odobrenja, prava na pristupanje i vraćanje uređaja po prestanku aktivnosti sa udaljenosti.

- Sigurnost i zaštita u organizaciji

1. Infrastruktura zaštite informacija

Uz rukovodni forum treba osnovati savetodavni tim specijalista za zaštitu informacija da bi bio na raspolaganju unutar organizacije, i razviti spoljne veze sa specijalistima iz oblasti zaštite kako bi bili u toku sa kretanjima u struci, nadgledali kriterijume i metode za ocenjivanje kao i da bi se obezbedile tačke za vezu i saradnju po pitanju incidenata ugrožavanja sigurnosti. Kod sigurnosti informacija treba savetovati multidisciplinarni pristup, što npr. uključuje saradnju i zajednički rad rukovodilaca, korisnika, projekatnata aplikacija, kontrolora i osoblja obezbeđenja, kao i specijalista iz oblasti zaštite, osiguranja i upravljanja rizicima.

2. Koordinacija zaštite informacija

U velikoj organizaciji, kod uvođenja i primene kontrola za zaštitu informacija može biti neophodan forum sa unakrsnim funkcijama sastavljen od predstavnika rukovodstva iz odgovarajućih delova organizacije. Ovakav forum tipično:

- a) usaglašava specifične uloge i obaveze radi zaštite informacija u celoj organizaciji;
- b) usaglašava specifične metodologije i postupke u zaštiti informacija, npr. procenjivanje rizika, sistem klasifikovanja sigurnosti i zaštićenosti;
- c) usaglašava i daje podršku inicijativama za zaštitu informacija širom organizacije, npr. program upoznavanja sa zaštitom;
- d) obezbeđuje i osigurava da zaštita bude deo postupka planiranja informacija;
- e) ocenjuje adekvatnost i koordiniše ugradnju i primenu specifičnih kontrola za zaštitu informacija kod novih sistema ili usluga;
- f) preispituje incidente narušavanja sigurnosti;
- g) unapređuje vidljivost poslovne podrške zaštiti informacija po celoj organizaciji.

3. Preraspodela obaveza i odgovornosti u zaštiti informacija

Politika zaštite informacija treba da pruži opšte smernice u pogledu preraspodele uloga u zaštiti i obaveza u organizaciji. Treba jasno definisati lokalne obaveze i odgovornosti za pojedinačnu fizičku i informacionu imovinu i postupke zaštite, kao što je planiranje kontinuiteta poslovanja. Za razvoj i primenu zaštite i podršku pri utvrđivanju kontrola u mnogim organizacijama imenuje se rukovodilac za sigurnost i zaštitu informacija kako bi on preuzeo ukupne obaveze i odgovornosti u tom pogledu. Za svako informaciono dobro imenuje se vlasnik čije dalje zaduženje ostaje svakodnevna zaštita. Vlasnici informacionih dobara mogu svoja zaduženja u pogledu zaštite preneti na pojedine rukovodioce ili na

davaoce usluga. Ipak takav vlasnik ostaje u krajnjem slučaju odgovoran za sigurnost te imovine i treba da je u stanju da utvrdi da se svako preneto zaduženje ispravno sprovodi. Osnovno je da se jasno definiše oblast za koju je svaki od rukovodilaca zadužen; posebno treba sprovoditi sledeće:

- a) Treba utvrditi i jasno definisati razna dobra i postupke zaštite za svaki pojedinačni sistem.
- b) Za svako pojedino dobro ili postupak zaštite treba napraviti sporazum oko zaduženja rukovodioca a detalji oko njegove odgovornosti treba da budu dokumentovani.
- c) Nivoi ovlašćenja treba da budu jasno definisani i dokumentovani.

4. Postupak ovlašćivanja za rad sa opremom za obradu informacija

Treba uspostaviti postupak ovlašćivanja rukovodstva za novu opremu za obradu informacija.

Treba predvideti sledeće kontrole.

- a) Nova oprema treba da dobije odobrenje rukovodstva za odgovarajućeg korisnika, odobravanjem njene namene i korišćenja. Odobrenje treba dobiti i od rukovodioca zaduženog za održanje sigurnosti informacionog sistema u lokalnom okruženju kako bi se osiguralo da budu ispunjeni svi zahtevi i politika zaštite.
- b) Kada je potrebno, treba proveriti hardver i softver kako bi se osiguralo da su oni kompatibilni sa ostalim komponentama u sistemu.
- c) Za korišćenje lične opreme za obradu informacija u obradi poslovnih informacija treba da se dobije odobrenje.
- d) Korišćenje lične opreme za obradu informacija na radnom mestu može dovesti do ranjivosti i zato se ono mora proceniti i odobriti.

Ove kontrole posebno su važne u mrežnom okruženju.

5. Specijalistički saveti o zaštiti informacija

Specijalističke savete o zaštiti treba da pruža iskusan savetnik za zaštitu informacija, zaposlen u samoj organizaciji ili da se odredi posebna osoba koja će u samoj organizaciji koordinisati znanja i iskustva kako bi se osigurala ujednačenost i obezbedila pomoć u odlučivanju o zaštiti. Ove osobe treba takođe da imaju kontakt sa pogodnim spoljnim savetnicima kako bi se pružili specijalistički saveti koji su van sopstvenih iskustava. Kvalitet njihove procene pretnji po sigurnost i saveti u pogledu kontrola će odrediti efikasnost zaštite informacija u organizaciji. Radi maksimalne efikasnosti i uticaja njima treba dozvoliti direktan pristup rukovođenju u celoj organizaciji. Savetnike za zaštitu informacija ili ekvivalentne tačke za kontakt treba konsultovati u najranijoj mogućoj fazi koja sledi posle sumnje da se dogodio incident u vezi sigurnosti ili upad kako bi se obezbedio izvor ekspertskih smernica ili resursi za istragu. Iako se najveći broj internih istraga normalno sprovodi pod kontrolom rukovodstva, savetnik za sigurnost se može pozvati radi davanja saveta, vođenja ili upravljanja istragom.

6. Saradnja među organizacijama

Treba održavati odgovarajuće kontakte sa ovlašćenima za sprovođenje zakona, regulativnim telima, davaocima informativnih usluga i telekomunikacionim operatorima kako bi se osiguralo da se odgovarajuća akcija može brzo sprovesti i kako bi se dobio savet, u slučaju nekog incidenta u vezi sigurnosti. Na sličan način, treba uzeti u obzir i učešće u forumima i grupama iz delatnosti zaštite. Razmena informacija o sigurnosti treba da se ograniči kako bi se osiguralo da poverljive informacije o organizaciji ne dopru do neovlašćenih osoba.

7. Nezavisno preispitivanje sigurnosti informacija

Dokument o politici zaštite informacija uspostavlja politiku i zaduženja u pogledu zaštite informacija. Njeno primenjivanje treba preispitivati nezavisno kako bi se obezbedila potvrda da praksa u organizaciji odgovarajuće odražava tu politiku, kao i da se ona ostvaruje i da je i efikasna. Takvo preispitivanje može se sprovoditi funkcijom interne provere, angažovanjem nezavisnog rukovodioca ili organizacije treće strane koja je specijalizovana za takva preispitivanja, čiji kandidati imaju odgovarajuća znanja i iskustvo.

- Zaštita kod pristupanja treće strane

Kada je takvoj trećoj strani potreban poslovni pristup, treba sprovesti procenu rizika kako bi se odredile posledice po sigurnost i zahtevi za kontrolisanje. O definisanju kontrole treba se sporazumeti sa trećom stranom preko ugovora. Pristupanje treće strane može obuhvatiti i druge učesnike. Ugovori koji sadrže pristup treće strane treba da uključe odobrenje za druge moguće učesnike i uslove za njihovo pristupanje.

- Identifikovanje rizika kod pristupanja treće strane

1. Tipovi pristupanja

Tip pristupanja koji se daje trećoj strani ima poseban značaj. Na primer, rizici od pristupanja preko spoja sa mrežom drugačiji su od rizika koji su rezultat fizičkog pristupa. Tipovi pristupa koje treba uzeti u obzir su:

- a) fizički pristup, npr. u kancelarije, prostorije sa računarima, ormanima sa fasciklama;
- b) logički pristup, npr. bazama podataka u organizaciji, informacionim sistemima.

2. Razlozi za pristupanje

Trećim stranama može biti odobreno pristupanje iz više razloga. Na primer, postoje treće strane koje pružaju usluge nekoj organizaciji a nisu smeštene u samoj organizaciji ali im se može dati odobrenje za fizički i logički pristup kao što su:

- a) osoblje za hardversku i softversku podršku, kojem je potreban pristup do nivoa sistema ili nižih nivoa funkcija aplikacije;
- b) trgovinski partneri ili partneri u zajedničkom ulaganju;

Tamo gde postoji poslovna potreba za priključivanje na mestu treće strane treba sprovesti procenu kako bi se utvrdila potreba za specifičnim kontrolisanjem. U obzir treba uzeti tip pristupanja koji se zahteva, vrednost informacija, kontrole koje primenjuje ta treća strana i posledice ovakvog pristupanja po informacije u organizaciji.

3. Ugovorne strane na licu mesta

Treće strane koje su smeštene na licu mesta na određeno vreme koje je utvrđeno njihovim ugovorom mogu takođe dovesti do slabljenja zaštite. Primeri takvih trećih strana na licu mesta uključuju:

- a) osoblje koje održava i daje podršku za hardver i softver;
- b) službe za održavanje čistoće, ishrane, bezbednosti i druge pomoćne službe izvan organizacije;
- c) učenici i druga povremena kratkotrajna postavljenja;
- d) konsultanti.

4. Zahtevi za sigurnost i zaštitu u ugovorima sa trećim stranama

Sporazumi koji uključuju pristupanje trećih strana u prostore za obradu informacija treba da se zasnivaju na zvaničnim ugovorima koji sadrže, ili se pozivaju na, sve zahteve za zaštitu kako bi se osigurala usaglašenost sa politikom zaštite i kriterijumima organizacije. Takav ugovor treba da osigura da ne dođe do nesporazuma između organizacije i treće strane. Organizacije treba da zadovolje sopstvene interese u pogledu odštete od svojih isporučilaca. Za uključivanje u ugovor treba imati u vidu sledeće uslove:

- a) opštu politiku u pogledu sigurnosti
- b) zaštite informacija i zaštitu dobara, uključujući:
 - 1) procedure za zaštitu imovine organizacije, uključujući informacije i softver;
 - 2) procedure za utvrđivanje da li je došlo do ugrožavanja dobara, npr. do gubitka ili menjanja podataka;
 - 3) kontrolisanja kako bi se osigurao povraćaj ili uništenje informacija ili dobara po isteku ili u određenom vremenskom trenutku ugovora;
 - 4) celovitost i raspoloživost;
 - 5) ograničenja u pogledu kopiranja i obelodanjivanja informacija;
- c) opis svake usluge koja će biti na raspolaganju;
- d) željeni nivo i neprihvatljiv nivo usluge;
- e) odredbe o prelasku osoblja kada je to potrebno;
- f) odgovarajuće obaveze ugovornih strana;
- g) odgovornosti u pogledu zakonskih obaveza, npr. zakona u pogledu zaštite podataka, posebno uzimajući u obzir različite nacionalne zakonske sisteme kada ugovor uključuje saradnju sa organizacijama iz drugih zemalja;
- h) prava intelektualne svojine i zaštitu prava na kopiranje kao i zaštitu od bilo kakvog zakulisnog posla;
- i) sporazume o kontrolisanju pristupa, uključujući:
 - 1) dozvoljene metode pristupanja, kao i kontrolisanje i primenu jedinstvenih identifikatora kao što su korisnički ID identifikatori i lozinke;
 - 2) postupak ovlašćivanja korisnika za pristupanje i njegova prava;
 - 3) zahtev za čuvanje spiska pojedinaca ovlašćenih za korišćenje usluga koje se daju na raspolaganje i kakva su njihova prava i povlastice u odnosu na takvo korišćenje;
- j) definisanje kriterijuma rada koji se mogu verifikovati, njihovo nadgledanje i izveštavanje;
- k) pravo na nadgledanje i prekidanje korisnikove aktivnosti;
- l) pravo na kontrolisanje ispunjavanja ugovornih obaveza ili na sprovođenje takve kontrole preko treće strane;
- m) uspostavljanje pokretanja postupka za razrešavanje problema; takođe treba uzeti u obzir i nepredviđene okolnosti kada je to potrebno;
- n) obaveze i odgovornosti u pogledu postavljanja i održavanja hardvera i softvera;
- o) jasnu strukturu izveštaja i dogovorenu formu izveštavanja;
- p) jasan i utvrđen postupak upravljanja promenama;
- q) sve potrebne mehanizme i kontrole za fizičku zaštitu kako bi se osiguralo da se takve kontrole sprovode;
- r) obuku korisnika i administratora (upravnika) u pogledu metoda, procedura i zaštite;
- s) kontrole za osiguranje zaštite od zloćudnih softvera;
- t) dogovore o izveštavanju, beleženju i istraživanju incidenata u vezi sigurnosti i upada;
- u) povezanost treće strane sa podugovaračima.

- Korišćenje spoljnih resursa

Kada je obaveza obrade informacija poverena nekoj drugoj organizaciji, ugovori između strana i sporazumi o korišćenju spoljnih resursa treba da sadrže rizike, procedure za kontrolisanje i zaštitu informacionih sistema, mreža i/ili radnih stanica.

1. Zahtevi za sigurnost u ugovorima o korišćenju spoljnih resursa

U ugovor koji se sklapa između strana treba uneti zahteve za sigurnost organizacije koja spoljnim resursima daje upravljanje i kontrolu nad svim ili samo nekim svojim

informacionim sistemima, mrežama i/ili radnim stanicama. Na primer, ugovor treba da sadrži:

- a) kako treba ispuniti zakonske uslove, npr. zakon o zaštiti podataka;
- b) kakve sporazume treba uspostaviti kako bi se osiguralo da sve strane koje sudeluju u korišćenju spoljnih resursa, uključujući podugovarače, budu upoznate sa svojim obavezama i odgovornostima u pogledu sigurnosti;
- c) kako treba održavati i ispitivati celovitost i poverljivost poslovnih informacionih dobara organizacije;
- d) koje fizičke i logičke kontrole koristiti da bi se ovlašćenim korisnicima ograničio i sprečio pristup osetljivim poslovnim informacijama;
- e) kako treba održati dostupnost usluga u slučaju neke nesreće;
- f) kakve nivoe fizičke zaštite treba obezbediti za opremu u spoljnim resursima;
- g) prava na kontrolu i proveru.

Ugovor koji se sklapa između dveju strana treba da omogući da se zahtevi i postupci za sigurnost i zaštitu prošire u planu za upravljanje sigurnošću.

Iako ugovori o korišćenju spoljnih resursa mogu postaviti neka složena pitanja u vezi sigurnosti, kontrole koje su uključene u ova pravila za primenu u praksi mogu poslužiti kao polazna tačka u sporazumevanju o strukturi i sadržaju plana za upravljanje sigurnošću.

- Klasifikovanje i kontrolisanje imovine

1. Odgovornost za imovinu

Popisivanje imovine pomaže da se osigura održavanje odgovarajuće zaštite. Za sva glavna dobra treba definisati vlasnike i treba odrediti obaveze i odgovornosti za održavanje odgovarajućih kontrola. Obaveza uvođenja kontrola može se preneti na drugoga. Popisivanje treba da ostane kod naimenovanog vlasnika imovine.

2. Popisivanje imovine

Postupak sprovođenja popisa imovine i dobara predstavlja važan vid upravljanja rizicima. Organizaciji je potrebno da je u stanju da utvrdi svoju imovinu i relativnu vrednost i važnost tih dobara. Zasnovano na ovim informacijama organizacija može da obezbedi da nivoi zaštite budu u skladu sa vrednošću i značajem tih dobara. U svakom informacionom sistemu treba sprovesti i održavati popisivanje svih važnih pripadajućih dobara. Svako od dobara treba jasno identifikovati a dogovor o njegovom vlasniku i klasi sigurnosti treba dokumentovati zajedno sa njegovim trenutnim mestom (važno kod pokušaja da se ono obnovi pri gubitku ili oštećenju). Primeri dobara koja pripadaju informacionim sistemima su:

- a) informaciona dobra: baze i datoteke sa podacima, sistemska dokumentacija, uputstvo za korisnika, materijal za obuku, procedure za rad ili podršku, planovi kontinuiteta, planovi za povlačenje, sačuvane informacije;
- b) softverska dobra: aplikativni softver, sistemski softver, razvojni alati i pomoćni programi;
- c) fizička dobra: računarska oprema (procesori, monitori, prenosivi računari, modemi), komunikaciona oprema (usmeravači - ruteri, PABX, faksimil aparati, telefonske sekretarice), magnetni medijumi (trake i diskovi), ostali tehnički uređaji (izvori napajanja, klimatizeri), nameštaj, prostorije;
- d) usluge: računarske i komunikacione usluge, opšte usluge, npr. grejanje, osvetljenje, električno napajanje, klimatizacija.

3. Klasifikovanje informacija

Informacije imaju promenljivi stepen osetljivosti i kritičnosti. Neki elementi mogu zahtevati dodatni stepen zaštite ili poseban postupak. Sistem za klasifikovanje informacija treba primenjivati kako bi se definisao odgovarajući skup nivoa zaštite i iskazala potreba za posebnim merama u postupanju.

4. Smernice za klasifikovanje i postupanje sa informacijama

Klasifikovanje informacija i pripadajuće zaštitne kontrole treba da uzme u obzir poslovne potrebe za zajedničko korišćenje ili uskraćivanje informacija i poslovne posledice takvih potreba, npr. neovlašćeno pristupanje ili oštećenje informacija. Informacije treba da budu označene u pogledu njihove vrednosti i kritičnosti po organizaciju, npr. u pogledu celovitosti i dostupnosti. Informacije posle određenog vremenskog perioda prestaju da budu osetljive ili kritične, na primer kada se one javno objave. Smernice za klasifikovanje treba da unapred uzmu u obzir i računaju sa činjenicom da klasifikovanje svakog datog elementa informacija nije jednom zauvek, kao i da se može promeniti u skladu sa nekom predodređenom politikom. Za označavanje i postupanje sa informacijama definiše se odgovarajući skup procedura, u skladu sa klasifikacionom šemom koju je organizacija usvojila. Ove procedure treba da obuhvate informacionu imovinu u fizičkoj i elektronskoj formi. Složene šeme mogu postati glomazne i neekonomične za primenu ili da se pokažu kao neprimenjive. Zaduženje za definisanje klasifikacije nekog elementa informacija, npr. dokumenta, zapisa sa podacima, datoteke sa podacima ili diskete kao i za periodično preispitivanje te klasifikacije, treba da ostane kod tvorca ili nimenovanog vlasnika tih informacija.

Kod svakog klasifikovanja, treba definisati procedure za postupanje kako bi se obuhvatili sledeći tipovi aktivnosti u obradi informacija:

- a) kopiranje;
- b) skladištenje;
- c) prenošenje poštom, faksimilom i elektronskom poštom;
- d) prenošenje govorom, uključujući mobilne telefone, govornu poštu, telefonske sekretarice;
- e) uništenje.

Izlazi iz sistema koji sadrže informacije koje su klasifikovane kao osetljive ili kritične treba da nose odgovarajuću klasifikacionu oznaku (na izlazu). Stavke koje treba uzeti u obzir obuhvataju štampane izveštaje, prikaze na ekranima, medijume sa zapisima (trake, diskove, CD, kasete), poruke u elektronskom obliku, i prenošenje datoteka.

Fizičke oznake su u opštem slučaju najpogodniji oblik označavanja. Međutim neka informaciona dobra, kao što su dokumenti u elektronskom obliku, ne mogu se fizički označavati i potrebno je koristiti elektronska sredstva za označavanje.

- Razvoj i održavanje sistema

1. Sistemski zahtevi za sigurnost i zaštitu

Pre projektovanja informacionog sistema treba utvrditi zahteve za sigurnost i zaštitu i o tome treba ostvariti sporazum. Ovim su obuhvaćene infrastruktura, poslovne aplikacije i aplikacije koje razvija korisnik. Svi zahtevi u pogledu sigurnosti, uključujući potrebu za vraćanje u prethodno stanje, treba da se utvrde u fazi projektnih zahteva i treba da se obrazlože, usaglase i dokumentuju kao deo u okviru ukupnog poslovnog projekta informacionog sistema.

2. Analiza i specificiranje zahteva za sigurnost i zaštitu

Prilikom utvrđivanja poslovnih zahteva za nove sisteme ili za poboljšavanje postojećih sistema, treba utvrditi zahteve za kontrolisanje. Zahtevi za sigurnost i kontrolisanje treba da odražavaju poslovnu vrednost informacione imovine i potencijalnu poslovnu štetu, koja može nastati usled otkaza ili odsustva zaštite.

Ovakva specificiranja treba da predvide automatizovane kontrole koje treba ugraditi u sistem, kao i potrebu za podršku ručnog kontrolisanja. Slična razmatranja treba primeniti prilikom ocenjivanja softverskih paketa za poslovne aplikacije. Ako se utvrdi potrebnim, rukovodstvo može poželeti da koristi nezavisno ocenjene i sertifikovane proizvode.

Kontrole koje se uvode u fazi projektovanja znatno su jeftinije za ugradnju i održavanje od onih koje se uključuju tokom ili posle ugradnje.

3. Sigurnost i zaštita u aplikativnim sistemima

U aplikativnim sistemima, uključujući aplikacije koje piše korisnik, treba da su projektovane odgovarajuće kontrole i tragovi za proveru ili zapisi o aktivnostima. One treba da uključuju validaciju ulaznih podataka, unutrašnju obradu i izlazne podatke. Kod sistema u kojima se obrađuju, ili koji imaju uticaja na osetljivu, vrednu ili kritičnu imovinu organizacije, možda će biti potrebne dodatne kontrole. Takve kontrole treba odrediti na osnovu zahteva za sigurnost i zaštitu i ocene rizika.

4. Validacija ulaznih podataka

Na ulazu u aplikativni sistem treba sprovesti validaciju podataka kako bi se osiguralo da oni budu ispravni i odgovarajući. Provere treba primenjivati na ulaze u poslovne transakcije, na prisutne podatke (nazive i adrese, kreditna ograničenja, referentne brojeve učesnika) i na tabele sa parametrima (prodajne cene, odnose valuta, procenat takse). Treba predvideti sledeće kontrole:

- a) proveru dupliranih unošenja ili drugih ulaza kako bi se otkrile sledeće greške:
 - 1) veličine koje su izvan dozvoljenog opsega;
 - 2) nevažeći znakovi u polju podataka;
 - 3) nedostajući ili nekompletni podaci;
 - 4) premašenje gornje ili donje granice za veličinu podataka;
 - 5) neovlašćeni ili neujednačeni upravljački podaci;
- b) periodično preispitivanje sadržaja ključnih polja ili datoteka sa podacima kako bi se potvrdila njihova validnost i celovitost;
- c) pretraživanje ulaznih papirnih dokumenata zbog mogućeg neovlašćenog menjanja ulaznih podataka (sve izmene na ulaznim dokumentima moraju imati odobrenje);
- d) procedure za odgovor na greške pri validaciji;
- e) procedure za proveru verodostojnosti ulaznih podataka;
- f) definisanje obaveza i odgovornosti sveg osoblja koje učestvuje u postupku unošenja podataka.

- Kontrolisanje unutrašnje obrade

1. Rizična područja

Podaci koji su ispravno uneti mogu se oštetiti greškom u njihovoj obradi ili namerno. Da bi se takva oštećenja otkrila, u sistem treba da budu ugrađene provere validnosti. Aplikacije svojom konstrukcijom treba da osiguraju da su ugrađena ograničenja kako bi se na minimum smanjio rizik od grešaka u obradi koje bi dovele do gubitka celovitosti. Posebne oblasti koje treba uzeti u obzir su:

- a) položaj u programima i korišćenje funkcija brisanja ili dodavanja radi uvođenja izmena na podacima;
- b) procedure za sprečavanje da se programi izvršavaju u pogrešnom redosledu ili da rade i posle otkaza u prethodnoj obradi;
- c) korišćenje programa za ispravke i oporavak posle otkaza kako bi se osigurala ispravna obrada podataka.

2. Provere i kontrole

Potrebne kontrole zavise od prirode aplikacije i uticaja bilo kakvog oštećenja podataka na poslovanje. Primeri provera koje se mogu ugraditi uključuju sledeće:

- a) kontrole pojedinačnog ili ukupnog rada, radi uspostavljanja ravnoteže u datotekama podataka posle ažuriranja transakcije;
- b) kontrole uravnoteženosti, za proveru ravnoteže prilikom otvaranja u odnosu na ravnotežu prilikom prethodnog zatvaranja, naime:
 - 1) kontrole izvršno - prema - izvršnom;
 - 2) ukupni broj ažuriranih datoteka;
 - 3) kontrole program - prema - programu;
- c) validacija sistemski generisanih podataka;
- d) provera celovitosti podataka ili softvera, koji se preuzimaju ili koji se dostavljaju između centralnog i udaljenog računara;
- e) primena zbirova haš funkcije na zapise i datoteke;
- f) provere kako bi se osiguralo da se aplikativni programi izvršavaju u ispravnom trenutku;
- g) provere da bi se osiguralo da se programi izvršavaju po ispravnom redosledu i da se okončavaju u slučaju otkaza, kao i da se dalja obrada zaustavi dok se problem ne razreši.

3. Utvrđivanje i provera verodostojnosti poruke

Utvrđivanje verodostojnosti je postupak koji se koristi da bi se otkrile neovlašćene izmene ili oštećenja sadržaja elektronske poruke koja se prenosi. On se može ugraditi u hardver ili u softver kojim se podržava neki uređaj za fizičko utvrđivanje verodostojnosti ili neki softverski algoritam.

Na osnovu procene rizika po sigurnost, treba predvideti utvrđivanje verodostojnosti poruka u aplikacijama kod kojih postoji zahtev za zaštitu celovitosti sadržaja poruke, npr. elektronsko prenošenje sredstava, specifikacije, ugovori, ponude i predlozi od velikog značaja itd. ili kod drugih sličnih elektronskih razmena podataka. Utvrđivanje verodostojnosti poruka nije projektovano da bi se sadržaj neke poruke zaštitio od neovlašćenog razotkrivanja. Za ugradnju verodostojnosti u poruke kao odgovarajuće sredstvo mogu se primenjivati kriptografski postupci.

4. Validacija izlaznih podataka

Na podacima na izlazu iz aplikacijskog sistema treba izvršiti validaciju kako bi se osiguralo da je obrada uskladištenih informacija ispravna i da odgovara okolnostima. Tipično, sistemi se grade na polaznoj pretpostavci da će, kada se preduzme odgovarajuća validacija, verifikovanje i ispitivanje uvek dati ispravan rezultat. Ovo nije uvek slučaj. Validacija na izlazu može da uključuje:

- a) provere uverljivosti kako bi se ispitalo da li podaci na izlazu imaju smisla;
- b) usklađivanje broja kontrola kako bi se osigurala obrada svih podataka;
- c) pružanje čitaocu ili narednom sistemu za obradu, dovoljnih informacija da bi se odredila tačnost, kompletnost, preciznost i klasifikovanje informacija;
- d) procedure odziva na rezultate ispitivanja na izlazu;

- e) definisanje obaveza i odgovornosti za sve osoblje koje učestvuje u obradi podataka na izlazu.

5. Kriptografske kontrole

Kriptografske sisteme i postupke treba primenjivati radi zaštite informacija za koje se smatra da su u opasnosti i kojima druge kontrole ne pružaju dovoljnu zaštitu.

- Politika korišćenja kriptografskih kontrola

Organizacija treba da razvije politiku korišćenja kriptografskih kontrola radi zaštite sopstvenih informacija. Takva politika je neophodna kako bi se ostvarila maksimalna korist i da bi se na minimum smanjili rizici od primene kriptografskih postupaka, kao i da bi se izbeglo neodgovarajuće ili neispravno korišćenje. Ocenjivanje rizika treba sprovedi kako bi se odredio nivo zaštite koji informacijama treba pružiti. Ovo ocenjivanje se zatim može koristiti da bi se utvrdilo da li kriptografska kontrola odgovara, koji tip kontrola treba primeniti i za koje svrhe i poslovne operacije.

Prilikom razvoja politike treba uzeti u obzir sledeće:

- a) stav rukovodstva prema korišćenju kriptografskih kontrola unutar cele organizacije, uključujući opšte principe prema kojima bi poslovne informacije trebalo da se štite;
- b) upravljanje pristupom ključevima, uključujući metode za postupanje sa obnavljanjem šifrovanih informacija u slučaju gubljenja, kompromitovanja ili oštećenja ključeva;
- c) uloge odgovornosti, npr. ko je za šta odgovoran;
- d) primenu te politike;
- e) upravljanje ključevima;
- f) kako treba određivati odgovarajući nivo kriptografske zaštite;
- g) standarde koje treba preuzeti radi efikasne primene u celoj organizaciji (koje rešenje se koristi u kojim poslovnim operacijama).

- Šifrovanje

Šifrovanje predstavlja kriptografski postupak koji se može koristiti za zaštitu poverljivosti informacija. Njega treba uzeti u obzir kod zaštite osetljivih ili kritičnih informacija. Potreban nivo zaštite treba utvrditi na osnovu ocene rizika, uzimajući u obzir tip i kvalitet šifarskog algoritma koji se koristi i dužinu šifarskih ključeva koje treba primeniti. Prilikom uvođenja politike šifrovanja u neku organizaciju, treba razmotriti nacionalnu regulativu i ograničenja koja mogu važiti u pogledu korišćenja kriptografskih postupaka u raznim delovima sveta i probleme protoka šifrovanih informacija preko granica. Pored toga treba voditi računa o kontrolama koje se primenjuju na uvoz i izvoz kriptografskih tehnologija.

Da bi se odabrao odgovarajući nivo zaštite treba zatražiti savet stručnjaka, kako bi se odabrali pogodni proizvodi koji će pružiti potrebnu zaštitu i uvođenje zaštićenog sistema upravljanja ključevima. Pored toga možda će biti potreban pravni savet u pogledu zakona i regulative koja je primenljiva na nameravano korišćenje šifrovanja u organizaciji.

- Digitalni potpisi

Digitalni potpisi pružaju sredstvo za zaštitu verodostojnosti i celovitosti dokumenata u elektronskom obliku. Na primer oni se mogu primenjivati u elektronskoj trgovini gde postoji potreba da se verifikuje ko je potpisao neki dokument u elektronskom obliku i da se proveriti da li je u sadržini potpisanog dokumenta dolazilo do izmena.

Digitalni potpisi se mogu primenjivati na svaki oblik dokumenta koji se obrađuje elektronski, npr. oni se mogu koristiti za potpisivanje elektronskih plaćanja, prenošenja sredstava, ugovora i sporazuma. Digitalni potpisi mogu se ugrađivati korišćenjem kriptografskih postupaka koji se zasnivaju na jedinstvenoj vezi para ključeva gde se jedan od ključeva koristi za izradu potpisa (tajni ključ) a drugi za proveru potpisa (javni ključ). Pažnju treba

obratiti na poverljivost tajnog ključa. Ovaj ključ treba čuvati u tajnosti jer svako ko ima pristup ovom ključu može da potpisuje dokumente, npr. isplate, ugovore, čime se falsifikuje potpis imaoca tog ključa. Pored toga važna je zaštita celovitosti javnog ključa. Ova zaštita se ostvaruje primenom sertifikata za javni ključ.

Treba razmotriti tip i kvalitet algoritma za potpisivanje koji se koristi kao i dužinu ključeva koji će se primenjivati. Kriptografski ključevi koji se koriste za digitalno potpisivanje treba da se razlikuju od onih koji se koriste za šifrovanje.

Kada se primenjuju digitalni potpisi, treba razmotriti svu odgovarajuću pravnu regulativu kojom se opisuju uslovi pod kojima neki digitalni potpis predstavlja zakonsku obavezu. Tamo gde su pravni okviri neadekvatni, za podršku primene digitalnog potpisa možda će biti neophodni obavezujući ugovori ili neki drugi sporazumi. O zakonima i regulativi koji mogu biti primenljivi kada neka organizacija namerava da koristi digitalne potpise treba potražiti pravni savet.

- Servisi neporicanja

Servisi neporicanja treba da se koriste gde je neophodno razrešiti sporove oko odvijanja ili neodvijanja nekog događaja ili aktivnosti, npr. spor oko korišćenja digitalnog potpisa u nekom elektronskom ugovoru ili plaćanju. Ovi servisi mogu pomoći pri uspostavljanju evidencije radi dokazivanja da li su se neki određeni događaj ili aktivnost odigrali, npr. poricanje slanja nekog digitalno potpisanog naloga poslatog elektronskom poštom. Ovi servisi se zasnivaju na korišćenju postupaka šifrovanja i digitalnog potpisivanja.

- Upravljanje ključevima

1. Zaštita šifarskih ključeva

Za efikasnu primenu postupaka šifrovanja od bitnog je značaja upravljanje šifarskim ključevima. Svako kompromitovanje ili gubljenje šifarskih ključeva može dovesti do narušavanja poverljivosti, verodostojnosti i/ili celovitosti informacija. U organizaciji treba uspostaviti sistem upravljanja za podršku korišćenja dva tipa postupaka šifrovanja:

a) postupci sa tajnim ključem, kada dve ili više strana zajednički koriste isti ključ a taj ključ se primenjuje i za šifrovanje i za dešifrovanje informacija. Ovakav ključ treba držati u tajnosti jer je svako ko ima pristup tom ključu u stanju da dešifruje sve informacije šifrovane pomoću tog ključa, ili da unese neke nedozvoljene informacije.

b) postupci sa javnim ključem, kada svaki korisnik poseduje par ključeva, jedan javni ključ (koji se može razotkriti bilo kome) i jedan privatni ključ (koji se mora držati u tajnosti). Postupci sa javnim ključem mogu se koristiti za šifrovanje i za izradu digitalnih potpisa.

Svi ključevi treba da su zaštićeni od modifikovanja i uništenja, a tajni i privatni ključevi treba da su zaštićeni od neovlašćenog razotkrivanja. Za ovu svrhu se takođe mogu primenjivati postupci šifrovanja. Fizička zaštita treba da se primenjuje za zaštitu uređaja za generisanje, čuvanje i arhiviranje ključeva.

2. Normativi, procedure i metode

Sistem za upravljanje ključevima treba da se zasniva na dogovorenom skupu kriterijuma, procedura i metoda zaštite kod:

- a) generisanja ključeva za razne kriptografske sisteme i različite aplikacije;
- b) generisanja i dobijanja sertifikata javnih ključeva;
- c) distribuiranja ključeva namenskim korisnicima, uključujući i način kako ključ treba aktivirati nakon prijema;
- d) skladištenja ključeva, uključujući i način kako ovlašćeni korisnici dobijaju pristup ključevima;

- e) menjanja ili ažuriranja ključeva uključujući pravila o tome kada ključeve treba zameniti i način kako to treba učiniti;
- f) postupanja sa kompromitovanim ključevima;
- g) opozivanja ključeva uključujući način kako ključeve treba povući ili deaktivirati, npr. kada su ključevi kompromitovani ili kada korisnik napušta organizaciju (u kom slučaju ključeve treba i arhivirati);
- h) obnavljanja ključeva koji su bili izgubljeni ili oštećeni kao dela upravljanja kontinuitetom poslovanja, mpr. za obnavljanje šifrovanih informacija;
- i) arhiviranja ključeva, npr. za arhivirane informacije ili za rezervne kopije;
- j) uništavanja ključeva;
- k) zapisivanja i proveru aktivnosti u vezi upravljanja ključevima.

Da bi se umanjili izgledi za kompromitovanje, ključevi treba da imaju definisane datume aktiviranja i deaktiviranja tako da se mogu primenjivati samo u ograničenom vremenskom periodu. Ovaj vremenski period treba da zavisi od okolnosti u kojima se kriptografska kontrola primenjuje, kao i od sagledanih opasnosti.

Može postojati potreba za uvođenjem procedura u pogledu pravnih zahteva za pristup šifarskim ključevima, npr. kada je u nekom slučaju na sudu kao dokaz potrebno da informacije budu dostupne u dešifrovanom obliku.

Pored problema sigurnosnog upravljanja tajnim i privatnim ključevima, treba predvideti i zaštitu javnih ključeva. Postoji pretnja da neko potpis falsifikuje zamenjivanjem korisnikovog javnog ključa sopstvenim. Ovaj problem se rešava primenom sertifikata javnog ključa. Sertifikate treba izrađivati na način pomoću kojeg se javni ključ jedinstveno vezuje za informacije koje se odnose na vlasnika para javni / tajni ključ. Zbog toga je važno da postupak upravljanja kojim se generišu ovakvi sertifikati bude poverljiv. Ovaj postupak normalno sprovodi ovlašeni za izdavanje sertifikata koji treba da bude neka priznata organizacija sa uspostavljenim odgovarajućim kontrolama i procedurama kako bi se pružio potreban stepen poverenja.

Sadržaj sporazuma ili ugovora sa spoljnim isporučiocima kriptografskih usluga o nivou tih usluga, npr. sa ovlašćenim za izdavanje sertifikata, treba da obuhvati probleme odgovornosti, pouzdanosti usluge i vremena odziva kod pružanja usluge.

- Sigurnost i zaštita sistemskih datoteka

Održavanje celovitosti sistema treba da je obaveza funkcionalne ili razvojne grupe kod korisnika kojem aplikativni sistem ili softver pripada.

1. Kontrola izvršnog softvera

Kontrolu treba obezbediti kod ugradnje softvera u operativni sistem. Da bi se rizik oštećenja operativnog sistema sveo na minimum, treba predvideti sledeće kontrole:

- a) Ažuriranje biblioteka operativnih programa treba da obavlja samo osoba naimenovana za održavanje biblioteke koja ima odgovarajuće odobrenje rukovodstva.
- b) Ako je moguće, operativni sistem treba da sadrži samo izvršni kod.
- c) Izvršni kod ne treba ugrađivati u operativni sistem dok se ne dobije dokaz uspešnosti ispitivanja i prihvatanje korisnika i dok se ne ažuriraju biblioteke izvornih programa.
- d) Treba održavati zapise provera za sva ažuriranja biblioteka operativnih programa.
- e) Kao meru predostrožnosti za neočekivane situacije treba sačuvati prethodne verzije softvera.

Softver za operativni sistem koji je kupljen od nekog isporučioca treba održavati na nivou koji podržava taj isporučilac. Svaka odluka da se on unapredi novim izdanjem treba da razmotri sigurnost tog izdanja, tj. uvođenje novih funkcija sigurnosti ili broj i ozbiljnost

problema sigurnosti kojima podleže ta verzija. Za uklanjanje ili smanjivanje slabosti u zaštiti treba primeniti popravke softvera ako to pomaže.

Fizički ili logički pristup isporučiocima treba davati samo kada je neophodno radi podrške i uz odobrenje rukovodstva. Aktivnosti isporučioaca treba nadgledati.

2. Zaštita sistemskih podataka o ispitivanju

Podatke o ispitivanju treba zaštititi i držati pod kontrolom. Kod prijemnog ispitivanja najčešće su potrebne znatne količine ispitnih podataka koji su što je moguće bliži stvarnim radnim podacima. Treba izbegavati da radne baze podataka sadrže lične podatke.

Ako se takve informacije koriste, njih treba pre korišćenja depersonalizovati. Kada se za ispitivanje koriste operativni podaci, treba primenjivati sledeće kontrole:

- a) Kod ispitivanja na operativnim aplikativnim sistemima, treba takođe primeniti procedure za kontrolu pristupa.
- b) Svako kopiranje operativnih informacija u aplikativni sistem koji se ispituje treba posebno odobriti.
- c) Operativne informacije treba odmah po završetku ispitivanja izbrisati iz aplikativnog sistema koji se ispituje.
- d) Kopiranje i korišćenje operativnih informacija treba zapisivati kako bi se obezbedio trag za proveru.

3. Kontrola pristupa bibliotekama izvornih programa

Da bi se smanjila mogućnost oštećenja računarskih programa, strogu kontrolu treba održavati nad pristupom bibliotekama sa izvornim programima kako sledi.

- a) Gde je moguće, biblioteke sa izvornim programima ne treba držati u operativnim sistemima.
- b) Za svaku aplikaciju treba naimenovati programskog bibliotekara.
- c) Osoblje za podršku IT uređaja ne treba da ima neograničeni pristup bibliotekama izvornih programa.
- d) Programe koji su u fazi razvoja ili održavanja ne treba držati u bibliotekama izvornih operativnih programa.
- e) Ažuriranje biblioteka izvornih programa i izdavanje izvornih programa programerima treba da sprovodi samo naimenovani bibliotekar po odobrenju rukovodioca za podršku IT uređaja za određenu aplikaciju.
- f) Izlistane programe treba čuvati u zaštićenom okruženju.
- g) Treba održavati zapise provere za sva pristupanja bibliotekama izvornih programa.
- h) Starije verzije izvornih programa treba arhivirati, sa jasnom i preciznom oznakom datuma i vremena kada su one bile u upotrebi, zajedno sa svim softverima za podršku, kontrolu poslova, definicijama podataka i procedurama.
- i) Održavanje i kopiranje biblioteka izvornih programa treba da se vrši po strogim procedurama za kontrolisanje izmena.

- Sigurnost i zaštita u postupcima razvoja i podrške

Rukovodioci zaduženi za aplikativne sisteme treba takođe da budu odgovorni za sigurnost i zaštitu u okruženju projekta ili podrške. Oni treba da osiguraju da se sve predložene izmene na sistemu preispitaju kako bi se proverilo da one ne narušavaju sigurnost ni sistema ni radnog okruženja.

1. Postupci za kontrolisanje izmena

Da bi se oštećenja na informacionom sistemu svela na minimum, treba da postoji stroga kontrola nad uvođenjem izmena. Treba sprovoditi zvanične procedure za kontrolu izmena. One treba da osiguraju da se ne naruše procedure za sigurnost i kontrolisanje, da se

programerima za podršku daje pristup samo onim delovima sistema koji su njima neophodni za rad, kao i da se za svaku izmenu obezbedi zvanična saglasnost i odobrenje.

Menjanje aplikativnog softvera može uticati na radno okruženje. Kad god je izvodljivo, treba objediniti procedure za kontrolisanje izmena na operativnom i na aplikativnom sistemu. Ovaj postupak treba da obuhvati:

- a) čuvanje zapisa o dogovorenim nivoima ovlašćenja;
- b) osiguranje da se izmene unose na zahtev ovlašćenih korisnika;
- c) preispitivanje kontrola i procedura za zaštitu celovitosti kako bi se osiguralo da se one unošenjem izmena neće narušiti;
- d) identifikovanje svih računarskih softvera, informacija, entiteta u bazama podataka i hardvera za koji je potrebna dopuna;
- e) dobijanje zvaničnog odobrenja za detaljne ponude pre otpočinjanja radova;
- f) osiguranje pre bilo kakvog uvođenja da ovlašćeni korisnik prihvata izmene;
- g) osiguranje da se uvođenje sprovodi uz minimalno ometanje poslova;
- h) osiguranje da se po završetku svake izmene komplet systemske dokumentacije ažurira, a da se starija dokumentacija arhivira ili da se odbaci;
- i) održavanje kontrole nad verzijama svih softverskih ažuriranja;
- j) održavanje traga provere svih zahteva za izmenama;
- k) osiguranje da se u radnu dokumentaciju i procedure za korisnike po potrebi unesu izmene kako bi bile odgovarajuće;
- l) osiguranje da se ugradnja izmena događa u pravom trenutku i da to ne ometa odgovarajuće poslovne operacije.

Mnoge organizacije održavaju okruženje u kojem korisnici isprobavaju novi softver i koje je odvojeno od okruženja razvoja i proizvodnje. Ovim se pruža sredstvo za preuzimanje kontrole nad novim softverom i omogućava dopunska zaštita operativnih informacija koje se primenjuju za svrhu ispitivanja.

1. Tehničko preispitivanje izmena na operativnom sistemu

Povremeno su neophodne izmene na operativnom sistemu, npr. radi postavljanja novog izdanja softvera ili popravki. Kada se dogode izmene, aplikativne sisteme treba preispitati i isprobati kako bi se osiguralo da nema nepovoljnih uticaja na funkcionisanje ili na sigurnost. Ovaj postupak treba da obuhvati:

- a) preispitivanje aplikativnih kontrola i procedura za održanje celovitosti kako bi se uverilo da uvođenjem izmena na operativnom sistemu one nisu narušene;
- b) osiguranje da će godišnji plan podrške i sredstva biti dovoljni za preispitivanja i isprobavanje sistema koja proizlaze iz izmena na operativnom sistemu;
- c) osiguranje da se obaveštavanje o izmenama na operativnom sistemu obezbedi pravovremeno kako bi se omogućilo da se pre ugradnje obave odgovarajuća isprobavanja;
- d) osiguranje da se u planove za kontinuitet poslovanja unesu odgovarajuće izmene.

2. Ograničenja za izmene na softverskim paketima

Izmene na softverskim paketima treba izbegavati. Softverske pakete nabavljene od prodavca treba koristiti bez modifikacija, koliko god je to moguće. Gde se smatra da je modifikovanje nekog softverskog paketa od suštinskog značaja, treba razmotriti sledeće:

- a) rizik da se naruše ugrađene kontrole i postupci za održanje celovitosti;
- b) da li za to treba dobiti saglasnost prodavca;
- c) mogućnost da se potrebne izmene dobiju od prodavca kao standardna poboljšanja;
- d) posledice ukoliko, zbog unetih izmena, organizacija preuzme na sebe odgovornost za održavanje softvera u budućnosti.

Ako se smatra da su izmene neophodne izvorni softver treba sačuvati a izmene treba uneti na jasno identifikovanoj kopiji. Sve izmene treba u potpunosti isprobati i dokumentovati, tako da se one mogu ponovo primeniti na buduća poboljšanja softvera.

3. Tajna vrata i Trojanski konj

Tajna vrata mogu odati informacije pomoću nekog indirektnog i prikrivenog sredstva. Ona se mogu aktivirati menjanjem nekog parametra koji je dostupan preko zaštićenih i nezaštićenih elemenata u nekom računarskom sistemu, ili umetanjem informacija u neki tok podataka. Trojanski konj se projektuje tako da utiče na sistem na način za koji nije dobijeno odobrenje i koji primalac ili korisnik tog programa ne uočava odmah niti ga je zahtevao. Tajni kanal i Trojanski konj se retko javljaju slučajno. Kada su tajni kanal ili Trojanski konj predmet zabrinutosti, treba predvideti sledeće:

- a) kupovanje programa samo od pouzdanog izvora;
- b) kupovanje programa u izvornom kodu tako da se taj kod može verifikovati;
- c) korišćenje ocenjenih proizvoda;
- d) pregledanje svih izvornih kodova pre njihove primene u radu;
- e) kontrolisanje pristupa i modifikovanja na prvobitno ugrađenom kodu;
- f) korišćenje osoblja dokazanog poverenja za rad na ključnim sistemima.

- Razvoj softvera u spoljnim resursima

Kada se softver razvija u spoljnim resursima, treba voditi računa o sledećem:

- a) dogovorima o licencnim pravima, vlasništvu nad kodovima i pravima na intelektualnu svojinu;
- b) sertifikovanje kvaliteta i tačnosti rada koji se obavlja;
- c) ugovorima o garancijama u slučaju otkaza treće strane;
- d) pravima pristupa radi provere kvaliteta i tačnosti urađenog posla;
- e) ugovornim zahtevima za kvalitet koda;
- f) ispitivanjima pre ugradnje radi otkrivanja Trojanskog konja.

- Upravljanje kontinuitetom poslovanja

Postupak upravljanja kontinuitetom poslovanja treba uvesti kako bi se smanjile smetnje usled nesreća i otkaza zaštite (što može biti rezultat npr. prirodnih nepogoda, nesrećnih slučajeva, otkaza uređaja i namernih radnji) na prihvatljiv nivo kombinovanjem kontrola za prevenciju i za oporavak.

Treba izvršiti analizu posledica nesreća, otkaza zaštite i gubitka usluga. Treba da postoje razvijeni i ugrađeni planovi za neočekivane situacije kako bi se osiguralo da se poslovne operacije mogu obnoviti unutar zahtevanog vremenskog perioda. Takve planove treba održavati i isprobavati kako bi postali integralni deo svih drugih postupaka upravljanja. Upravljanje kontinuitetom poslovanja treba da obuhvati kontrole za identifikovanje i smanjivanje rizika, za ograničavanje posledica incidenata sa oštećenjima i da osigura da se važne operacije pravovremeno ponovo započnu.

1. Postupak upravljanja kontinuitetom poslovanja

Kroz celu organizaciju treba da postoji postupak za razvoj i održanje kontinuiteta poslovanja kojim se može upravljati. Njime treba da se objedine sledeći ključni elementi upravljanja kontinuitetom poslovanja:

- a) razumevanje rizika sa kojima se organizacija suočava u pogledu izgleda za njihov nastanak i njihovih posledica, uključujući identifikovanje i utvrđivanje prioriteta kritičnih poslovnih operacija;

- b) razumevanje posledica koje prekidi mogu imati po poslovanje (važno je da se pronađu rešenja kojima će se razrešavati manji incidenti, kao i ozbiljni incidenti koji mogu predstavljati životnu pretnju organizaciji), kao i uspostavljanje poslovnih ciljeva u pogledu opreme informacionih tehnologija.
- c) uzimanje u obzir kupovine pogodnog osiguranja koje može predstavljati deo postupka za kontinuitet poslovanja;
- d) formulisanje i dokumentovanje strategije za kontinuitet u skladu sa dogovorenim poslovnim ciljevima i prioritetima;
- e) formulisanje i dokumentovanje planova za kontinuitet poslovanja u skladu sa dogovorenom strategijom;
- f) periodično isprobavanje i ažuriranje ugrađenih planova i postupaka;
- g) uverenje da je upravljanje kontinuitetom poslovanja ugrađeno u strukturu i postupke unutar organizacije. Obaveze za koordinisanje postupka upravljanja kontinuitetom poslovanja treba da se dodele na odgovarajućem nivou unutar organizacije, npr. na forumu za sigurnost i zaštitu.

2. Kontinuitet poslovanja i analiza uticaja

Kontinuitet poslovanja treba započeti identifikovanjem događanja koja mogu dovesti do prekidanja poslovnih operacija, npr. otkaz uređaja, poplava i požar. Ovome treba da sledi ocenjivanje rizika kako bi se odredile posledice tih prekida (u pogledu stepena štete i trajanja oporavka). Obe ove aktivnosti treba sprovoditi uz puno učešće vlasnika poslovnih resursa i procesa. Ovo ocenjivanje uzima u obzir sve poslovne operacije i nije ograničeno na određenu opremu za obradu informacija.

3. Pisanje i ugradnja planova kontinuiteta

Da bi se održavale ili ponovo uspostavile poslovne operacije u zahtevanom vremenskom roku posle prekida ili otkaza u kritičnim poslovnim obradama, za tu svrhu treba imati razvijene planove. Postupak planiranja kontinuiteta poslovanja treba da predvidi sledeće:

- a) identifikovanje i dogovaranje o svim obavezama i procedurama u vanrednim situacijama;
- b) ugradnju procedura za vanredne situacije kako bi se omogućio oporavak i ponovno uspostavljanje rada unutar zahtevanog vremenskog perioda. Posebnu pažnju treba pokloniti ocenjivanjima zavisnosti od spoljnog poslovanja i od postojećih ugovora;
- c) dokumentaciju o dogovorenim procedurama i postupcima;
- d) odgovarajuće obrazovanje osoblja o dogovorenim procedurama za vanredne situacije i postupcima uključujući krizno rukovođenje;
- e) isprobavanje i ažuriranje planova.

Postupak planiranja treba da je usmeren na željene poslovne ciljeve, npr. obnavljanje specifičnih usluga korisnicima u prihvatljivom vremenskom roku. Treba predvideti usluge i resurse koji će to omogućiti, uključujući osoblje, neinformacione resurse potrebne za obradu, kao i sporazume o povratku opreme za obradu informacija u prethodno stanje.

4. Okviri planiranja kontinuiteta poslovanja

Treba održavati jedinstveni okvir planova za kontinuitet poslovanja kako bi se osiguralo da svi planovi budu usklađeni, kao i da bi se identifikovali prioriteti kod ispravljanja i održavanja. U svakom planu za kontinuitet poslovanja treba da su jasno navedeni uslovi za njegovo aktiviranje, kao i pojedinci čija je obaveza izvršenje svake od komponenata plana. Kada se utvrde novi zahtevi, uspostavljene postupke treba prema potrebi dopuniti postupcima u vanrednim situacijama, npr. planovima za evakuaciju ili za vraćanje u prethodno stanje.

Okviri planiranja kontinuiteta poslovanja treba da uzmu u obzir i predvide sledeće:

- a) uslove za aktiviranje ovih planova kojima se opisuje postupak kojeg se treba pridržavati (kako oceniti situaciju, koga sve treba uključiti itd.) pre nego što se neki plan aktivira;
- b) procedure za hitne situacije kojima se opisuju aktivnosti koje treba preduzeti posle nastanka nekog incidenta kojim se ugrožavaju poslovne operacije i/ili ljudski životi. Ovim treba da se obuhvate planovi za upravljanje kontaktima sa javnošću i za efikasnu vezu sa odgovarajućim javnim službama, npr. policijom, vatrogasnom službom i lokalnom upravom.
- c) procedure za povratak u prethodno stanje kojima se opisuju aktivnosti koje treba preduzeti radi premeštanja najvažnijih poslovnih aktivnosti ili za podršku uslugama, na alternativne privremene lokacije, kao i da poslovne postupke vrate u funkciju unutar zahtevanog vremenskog perioda;
- d) procedure za nastavljjanje kojima se opisuju aktivnosti koje treba preduzeti da bi se vratilo na normalne poslovne aktivnosti;
- e) termin plan održavanja kojim se definiše kako i kada će se plan proveravati, kao i postupak za održavanje tog plana;
- f) aktivnosti obuke i upoznavanja koje se projektuju kako bi se ostvarilo razumevanje postupaka za kontinuitet poslovanja i kako bi se osiguralo da postupci i dalje budu na snazi;
- g) pojedinačne obaveze i odgovornosti, kojima se opisuje ko je obavezan za izvršavanje kojih komponenata plana. Po potrebi treba uvesti alternative.

Svaki plan treba da ima specifičnog vlasnika. Procedure za hitne situacije, planovi za ručni povratak na ranije stanje i planovi za nastavljjanje treba da su obaveza vlasnika odgovarajućih poslovnih resursa ili pripadajućih postupaka. Pripreme za povratak u prethodno stanje za alternativne usluge, kao što je oprema za obradu informacija i komunikacije, najčešće treba da bude obaveza davaoca usluga.

5. Ispitivanje, održavanje i ponovno ocenjivanje planova za kontinuitet poslovanja

- Ispitivanje planova

Planovi za kontinuitet poslovanja mogu da ne zadovolje prilikom ispitivanja, često zbog netačnih pretpostavki, previda, ili promena uređaja i osoblja. Zbog toga ih treba redovno isprobavati kako bi se osiguralo da oni budu ažurni i efikasni. Takva ispitivanja treba takođe da osiguraju da svi članovi tima za obnavljanje i drugo odgovarajuće osoblje budu upoznati sa tim planovima.

Termin plan ispitivanja planova za kontinuitet poslovanja treba da ukaže na to kako i kada treba ispitivati svaki od elemenata plana. Preporučuje se da se pojedine komponente plana ispituju češće. Treba primenjivati razne postupke kako bi se pružila sigurnost da će planovi funkcionisati u stvarnom životu. To treba da uključuje:

- a) isprobavanje na radnom mestu različitih tokova događanja (detaljno pretresanje pripremljenosti za obnavljanje poslovanja korišćenjem modela prekida);
- b) simuliranja (posebno za obuku ljudi u njihovim rukovodećim ulogama posle incidenata i kriza);
- c) ispitivanje tehničkog oporavka (osiguranje da se informacioni sistem može efikasno oporaviti);
- d) ispitivanje oporavka na nekom alternativnom mestu (sprovođenje poslovnih postupaka paralelno sa postupcima za oporavak sa mesta udaljenog od glavne lokacije);

- e) ispitivanja isporučilaca opreme i usluga (osiguranjem da usluge i proizvodi koji se pružaju spolja ispunjavaju ugovorne obaveze);
- f) kompletne probe (ispitivanja da se organizacija, osoblje, uređaji, oprema i postupci mogu suprotstaviti prekidima).

Ove postupke može primenjivati svaka organizacija i oni treba da odraze prirodu nekog specifičnog plana za oporavak.

- Održavanje i ponovno ocenjivanje planova

Planove za kontinuitet poslovanja treba održavati kroz redovno preispitivanje i ažuriranje kako bi se osigurala njihova efikasnost. U program organizacije za upravljanje izmenama treba da su uključene procedure kako bi se osiguralo da su problemi kontinuiteta poslovanja odgovarajuće obuhvaćeni. Za svaki plan kontinuiteta poslovanja treba dodeliti obavezu za njegovo redovno preispitivanje; identifikovanje izmena u poslovnim sporazumima koje još nisu dobile odraz u planovima za kontinuitet poslovanja treba da prati odgovarajuće ažuriranje plana. Ovaj zvanični postupak upravljanja izmenama treba da osigura da se ažurirani planovi distribuiraju i sprovode preko redovnih preispitivanja kompletnog plana.

Primeri situacija u kojima može biti neophodno ažuriranje uključuju nabavku novih uređaja, ili poboljšanje operativnih sistema kao i promene:

- a) osoblja;
- b) adresa ili telefonskih brojeva;
- c) poslovne strategije;
- d) lokacije, opreme i resursa;
- e) zakona;
- f) ugovarača, isporučilaca i ključnih korisnika;
- g) postupaka, novih / ili povučenih;
- h) rizika (radnih ili finansijskih).

- Usaglašenost sa zakonskim odredbama

Da bi se izbegla kršenja bilo kojeg od krivičnih ili građanskih zakona, ustavnih regulativnih ili ugovornih obaveza kao i bilo kojeg zahteva za sigurnost, projektovanje, rad, korišćenje i upravljanje informacionim sistemima treba usaglasiti sa zakonskim odredbama. Savete o specifičnim zakonskim zahtevima treba potražiti od pravnih savetnika u organizaciji, ili odgovarajuće kvalifikovanih pravnih lica. Zakonski zahtevi variraju od zemlje do zemlje i od informacija stvorenih u jednoj zemlji koje se šalju u drugu zemlju (tj. tok podataka preko granica).

1. Identifikovanje primenljivih zakona

Za svaki informacioni sistem treba eksplicitno definisati i dokumentovati sve odgovarajuće ustavne, regulativne i ugovorne zahteve. Na sličan način treba definisati i dokumentovati specifične kontrole i pojedinačne obaveze radi ispunjenja tih zahteva.

2. Prava na intelektualnu svojinu (IPR)

Treba uvesti odgovarajuće procedure kako bi se osigurala usklađenost sa zakonskim ograničenjima u pogledu korišćenja materijala koji može biti predmet prava na intelektualnu svojinu, kao što su pravo na kopiranje, projektantska prava, oznake proizvođača. Narušavanje prava na kopiranje može dovesti do zakonske akcije koja može obuhvatiti i krivično gonjenje.

3. Pravo na kopiranje softvera

Zakonodavni, regulativni i ugovorni zahtevi mogu postaviti ograničenja u pogledu kopiranja materijala u vlasništvu. Softverski proizvodi u vlasništvu najčešće se isporučuju prema ugovoru o licenci kojim se korišćenje takvih proizvoda ograničava na posebne mašine a može ograničavati kopiranje samo na stvaranje rezervnih kopija. Treba predvideti sledeće kontrole:

- a) politiku usaglašenosti izdavanja softvera sa pravom na kopiranje kojom se definiše punopravno korišćenje softvera i informacionih proizvoda;
- b) izdavanje kriterijuma za procedure za nabavku softverskih proizvoda;
- c) održavanje obaveštenosti o politici nabavke i prava na kopiranje softvera, kao i davanje poruka o nameri za preduzimanje kaznenih mera protiv osoba koje ih krši;
- d) održavanje odgovarajućih registara imovine;
- e) održavanje dokaza i evidencije o vlasništvu licenci, izvornih diskova, priručnika sa uputstvima itd;
- f) uvođenje kontrola kako bi se osiguralo da nije prekoračen najveći dozvoljeni broj korisnika;
- g) sprovođenje provera da su ugrađeni samo odobreni softveri i proizvodi sa licencom;
- h) obezbeđenje politike održavanja odgovarajućih uslova licence;
- i) obezbeđenje politike davanja ili prenošenja softvera drugima;
- j) korišćenje odgovarajućih sredstava za proveru;
- k) usklađivanje sa uslovima za softver i informacije koji se dobijaju sa javnih mreža

- Samozaštita zapisa u organizaciji

Važne zapise u nekoj organizaciji treba zaštititi od gubljenja, uništenja i falsifikovanja. Za neke zapise može biti potrebno da se posebno štite kako bi se ispunili statutarni ili regulativni zahtevi, kao i da bi se podržale najvažnije poslovne aktivnosti. Primeri ovoga su zapisi koji mogu biti potrebni kao dokaz da organizacija posluje unutar statutarnih ili regulativnih pravila, ili da se osigura odgovarajuća odbrana protiv mogućih pravnih ili kriminalnih aktivnosti, ili da bi se potvrdilo finansijsko stanje organizacije u odnosu na deoničare, partnere ili kontrole. Vremenski period i sadržaj podataka za informacije koje se čuvaju mogu biti postavljene nacionalnim zakonom ili regulativom.

Zapise treba razvrstati u kategorije tipova zapisa, npr. obračunske zapise, zapise u bazama podataka, zapisnike o transakcijama, zapise o proverama i operativnim procedurama, svaki sa detaljima o periodu čuvanja i tipu medijuma na kojima se oni čuvaju, npr. papiru, mikrofilmu, magnetskom, optičkom medijumu. Svaki pridruženi kriptografski ključ koji pripada šifrovanom arhivskom materijalu ili digitalnom potpisu, treba da se čuva zaštićeno i da se prema potrebi daje na raspolaganje ovlašćenim osobama.

Treba uzeti u obzir mogućnosti propadanja medijuma koji se koriste za čuvanje zapisa. Treba uvesti procedure za čuvanje i postupanje koje su u skladu sa preporukama proizvođača.

Gde se za čuvanje odaberu elektronski medijumi, treba uključiti procedure za osiguranje sposobnosti pristupanja podacima (čitljivost medijuma i formata) u celom periodu čuvanja, kako bi se zaštitilo od njihovog gubljenja usled budućih promena tehnologija.

Sistem za skladištenje podataka treba odabrati tako da se potrebni podaci mogu pretraživati na način koji je zakonski i sudski prihvatljiv, npr. da se svi potrebni zapisi mogu izvući u prihvatljivom vremenskom roku i u prihvatljivom formatu.

Sistemi za skladištenje i rad sa podacima treba da osiguraju jasnu identifikaciju zapisa i njihov statutarni ili regulativni period čuvanja. Sistem mora dozvoljavati odgovarajuće uništavanje zapisa po isteku tog perioda ako organizaciji više nisu potrebni.

Da bi se ispunile ove obaveze, unutar organizacije treba preduzeti sledeće korake:

- a) Treba izdati uputstvo o čuvanju, skladištenju, postupanju i odbacivanju zapisa i informacija.
- b) Treba izraditi nacrt termin plana za čuvanje kojim se identifikuju najvažniji tipovi zapisa i vremenski period u kojem ih treba sačuvati.
- c) Treba održavati inventarski popis izvora ključnih informacija.
- d) Treba uvesti odgovarajuće kontrole radi zaštite najvažnijih zapisa i informacija od gubljenja, uništenja i falsifikovanja.

- Zaštita podataka i tajnost informacija o ličnostima

Neke zemlje uvele su zakonske mere kojim su postavljene kontrole pri obradi i prenošenju ličnih podataka (opštih informacija o živim pojedincima koje je na osnovu tih informacija moguće identifikovati). Takve kontrole mogu postaviti obaveze pred one koji prikupljaju, obrađuju i distribuiraju informacije o ličnostima, i mogu ograničiti mogućnost prenošenja tih podataka u druge zemlje.

Usklađenost sa zakonskom regulativom o zaštiti podataka zahteva odgovarajuću strukturu rukovođenja i kontrole. Često se ovo najbolje postiže imenovanjem službenika za zaštitu podataka koji treba da pruža smernice rukovodiocima, korisnicima i davaocima usluga o njihovim ličnim odgovornostima i specifičnim procedurama koje treba da poštuju. Vlasnik podataka treba da bude obavezan da službenika za zaštitu podataka obavesti o bilo kakvom predlogu da se informacije o ličnostima drže u nekoj strukturisanoj datoteci, kao i da se osigura obaveštenost o principima zaštite podataka koji su definisani u odgovarajućem zakonodavstvu.

- Sprečavanje zloupotrebe opreme za obradu informacija

Oprema za obradu informacija u nekoj organizaciji se obezbeđuje za poslovne namene. Svako korišćenje ove opreme za neposlovne ili neodobrene namene, bez odobrenja rukovodstva, treba smatrati neodobrenim. Ako se takva aktivnost utvrdi nadgledanjem ili pomoću drugih sredstava, na to treba skrenuti pažnju pojedinačom rukovodiocu zaduženom za odgovarajuću kaznenu akciju. Zakonitost takvog nadgledanja korišćenja razlikuje se od zemlje do zemlje i može biti potrebno da zaposleni budu obavešteni o takvom nadgledanju kako bi se dobio njihov pristanak. Pre uvođenja procedura za nadgledanje o tome treba potražiti pravni savet. Mnoge zemlje su uvele ili su u postupku uvođenja zakonskih mera da bi se uvela zaštita od zloupotrebe računara. Korišćenje računara na neodobren način može biti krivični prestup. Zbog toga je jako važno da svi korisnici budu precizno upoznati sa dozvoljenim područjem njihovog pristupanja. Prilikom prijavljivanja, na ekranu računara treba da bude prisutna poruka upozorenja kojom se ukazuje da je sistem u koji se ulazi privatno vlasništvo i da neovlašćeni pristup nije dozvoljen. Da bi se postupak prijavljivanja nastavio, korisnik treba da tu poruku potvrdi i da na nju reaguje na odgovarajući način.

- Regulativa za kriptografska kontrolisanja

Neke zemlje su uvele sporazume, zakone, regulativu ili druge instrumente za kontrolu pristupa ili za primenu kriptografskih kontrola. Takve kontrole mogu da obuhvate:

- a) uvoz i/ili izvoz računarskog hardvera i softvera za obavljanje kriptografskih funkcija;
- b) uvoz i/ili izvoz računarskog hardvera i softvera koji je projektovan da mu se dodaju kriptografske funkcije;
- c) obavezne ili diskrecione metode pristupanja zemalja informacijama koje su šifrovane hardverski ili softverski kako bi se obezbedila poverljivost sadržaja.

Da bi se osigurala usklađenost sa nacionalnim zakonom treba potražiti pravni savet. Pravni savet treba potražiti i pre nego što se započne sa prebacivanjem šifrovanih informacija ili kriptografskih kontrola u neku drugu zemlju.

- Prikupljanje dokaza

1. Pravila za dokaze

Za podršku akciji protiv neke osobe ili organizacije potrebno je da se imaju odgovarajući dokazi. Kad god ova aktivnost predstavlja internu kaznenu meru neophodni dokazi se opisuju kroz unutrašnje procedure. Kada takva aktivnost uključuje zakon, građanski ili krivični, podneti dokazi treba da su u skladu sa pravilima dokazivanja koje utvrđuje odgovarajući zakon ili sa pravilima specifičnog suda u kojem se slučaj ispituje. U opštem slučaju, ova pravila obuhvataju:

- a) prihvatljivost dokaza: da li se dokazi mogu koristiti na sudu ili ne;
- b) težinu dokaza: kvalitet i kompletnost dokaza;
- c) odgovarajući dokazi da su kontrole funkcionisale ispravno i ujednačeno (tj. dokaz o kontroli postupaka) u celom periodu u kojem je sistem dokaze koje treba obnoviti skladištio i obrađivao.

2. Prihvatljivost dokaza

Da bi se ostvarila prihvatljivost dokaza, organizacije treba da osiguraju da su njihovi informacioni sistemi u skladu sa svim kriterijumima ili pravilima rada za izradu prihvatljivih dokaza.

3. Kvalitet i kompletnost dokaza

Da bi se ostvarili kvalitet i kompletnost dokaza, potreban je jak trag praćenja za dokazivanje. U opštem slučaju, takav jak trag praćenja može se uspostaviti u sledećim uslovima.

- a) Za papirne dokumente: original se čuva na sigurnom i zapisuje se ko ga je našao, gde je nađen, kada je nađen i ko je bio svedok nalaženja. Svaka istraga treba da osigura da se sa originalima ne manipuliše.
- b) Za informacije na računarskim medijumima: kopije na pokretnim medijumima, informacije na čvrstim diskovima ili u memoriji treba preuzeti kako bi se obezbedila dostupnost. Treba praviti zapisnike o svim aktivnostima tokom postupka kopiranja i za to treba imati svedoke. Jednu kopiju medijuma i zapisnik treba držati na sigurnom.

Kada se neki incident prvi put otkrije, ne mora biti očigledno da će on možda dovesti do suda. Zbog toga postoji opasnost da se potrebni dokazi unište slučajno pre nego se shvati ozbiljnost tog incidenta. Savetuje se da se u bilo kojoj planiranoj pravnoj akciji već na početku uključi pravnik ili policija i da se potraži savet o potrebnim dokazima.

- Preispitivanje politike sigurnosti i zaštite i tehničke usaglašenosti

Da bi se osigurala usaglašenost sistema sa politikom sigurnosti u organizaciji i sa standardima, sigurnost i zaštitu informacionih sistema treba redovno preispitivati.

Takva preispitivanja treba obavljati u odnosu na odgovarajuću politiku sigurnosti i tehničke platforme a treba proveravati usaglašenost informacionih sistema sa standardima za primenu sigurnosti i zaštite.

1. Usklađenost sa politikom zaštite

Rukovodioci treba da osiguraju da se sve procedure za sigurnost i zaštitu u području njihove odgovornosti ispravno sprovode. Pored toga, za sva područja unutar organizacije treba predvideti redovna preispitivanja kako bi se osigurala usklađenost sa politikom sigurnosti i sa standardima. Time treba da se obuhvate:

- a) informacioni sistemi;
- b) davaoci sistema;
- c) vlasnici informacija i informacionih dobara;
- d) korisnici;
- e) rukovodstvo.

Vlasnici informacionih sistema treba da podrže redovna preispitivanja usklađenosti svojih sistema sa odgovarajućom politikom sigurnosti, standardima i svim drugim zahtevima za sigurnost.

2. Provera tehničke usaglašenosti

Redovno treba proveravati usaglašenost informacionih sistema sa standardima za primenu sigurnosti i zaštite. Provera tehničke usaglašenosti uključuje ispitivanje operativnih sistema kako bi se osiguralo da su ispravno primenjene hardverske i softverske kontrole. Ovaj tip provere usaglašenosti zahteva tehničku pomoć specijaliste. Nju treba da obavlja ručno (uz pomoć softverskih alata, ako je potrebno) iskusan sistemski inženjer, ili softverski paket za automatizovanu proveru koji generiše tehnički izveštaj za tehničkog specijalistu kako bi ga on naknadno tumačio.

Provera usaglašenosti takođe obuhvata, na primer, ispitivanje upada, što mogu sprovoditi nezavisni stručnjaci koji su posebno pozvani za ovu svrhu. Ovo može biti korisno za otkrivanje ranjivosti sistema i za proveru koliko su efikasne kontrole za sprečavanje neovlašćenog pristupanja usled ovih ranjivosti. Potrebne su mere opreza jer bi u slučaju uspešnog probnog upada moglo doći do narušavanja sigurnosti sistema i nenamernog iskorišćenja drugih ranjivosti.

Svaku proveru tehničke usaglašenosti treba da sprovede, ili da vrše nadzor, samo kompetentne, ovlašćene osobe.

3. Provera sistema

Prilikom provera sistema treba da postoje kontrole za samozaštitu operativnih sistema kao i alata za proveru. Zaštita je potrebna radi samozaštite celovitosti i sprečavanje zloupotreba alata za proveru.

4. Kontrolisanja za proveru sistema

Zahtevi za proveru i aktivnosti koje obuhvataju provere na operativnim sistemima treba pažljivo planirati i dogovoriti kako bi se na minimum sveo rizik od ometanja poslovnih obrada. Treba paziti na sledeće.

- a) Zahteve za proveru treba dogovoriti sa odgovarajućim rukovodstvom.
- b) Predmet i područje provera treba dogovoriti i kontrolisati.
- c) Provere softvera i podataka treba ograničiti i treba odobriti samo pristup sa čitanjem.
- d) Pristup koji nije ograničen samo na čitanje treba dozvoliti samo izdvojenim kopijama sistemskih datoteka, koje po završenoj proveri treba izbrisati.
- e) IT resurse za obavljanje provera treba eksplicitno identifikovati i staviti na raspolaganje.
- f) Zahteve za posebne ili dopunske obrade treba identifikovati i dogovoriti.
- g) Sva pristupanja treba nadgledati i zapisivati kako bi se napravio trag za proveru.
- h) Sve procedure, zahteve i odgovornosti treba dokumentovati.

5. Zaštita alata za proveru sistema

Pristupanje alatima za proveru sistema, tj. softverima ili datotekama sa podacima treba zaštititi kako bi se sprečila svaka moguća zloupotreba ili kompromitovanje. Takve alate treba izdvojiti iz razvojnih ili operativnih sistema i ne treba ih držati u bibliotekama na

trakama ili u korisničkim područjima, osim ako im se ne dodeli odgovarajući nivo dopunske zaštite.

7. Zaključak

Informacione tehnologije igraju značajnu ulogu u razvoju i održavanju konkurentnosti savremenih organizacija. Svaki ERP paket može se posmatrati kao integralni deo informacione tehnologije i konvencionalnih sistema, kao što su transportni, proizvodni, vojni sistem, zdravstvo i finansije. Postoji proliferacija standarda, procedura, metoda, alata i okruženja za razvoj i upravljanje softverom. Ova proliferacija je stvorila poteškoće u upravljanju softverom i softverskom inženjeringu, posebno u integrisanim proizvodima i uslugama. Potrebno je softversku disciplinu izmestiti van proliferacije ka zajedničkom okviru koji bi poslužio praktičarima, koji se bave softverom, da "govore istim jezikom" u stvaranju i upravljanju softverom u njegovim okruženjima. Standardi daju takve okvire. Procesi koji su navedeni u standardima čine jedan sveobuhvatan skup. Svaka organizacija, zavisno od svojih ciljeva, može izabrati odgovarajući podskup kojim će ostvariti ciljeve. Svaki standard je, prema tome, projektovan da bude prilagođavan za pojedine organizacije, projekte ili primene. On je, takođe, projektovan da se koristi u slučajevima kada je softver samostalan entitet, ili umetnuti ili sastavni deo čitavog sistema.

8. Literatura

- [1] Kenning, M., *Security management standard - ISO 17799/BS 7799*, BT Technology Journal, Vol 19, No 3, July 2001, (pp 132-136).
- [2] Humphreys, T., Plate, A., *An International Common Language for Information Security*, ISMS Journal, Issue 6, Jan 2006, (pp. 2-3).
- [3] Vermeulen, C., Van Solms, R., *The information security management toolbox - taking the pain out of security management*, Information Management & Computer Security, Vol 10, No 3, 2002, (pp 119-125).
- [4] Broderick, S., *ISMS, security standards and security regulations*, Information Security Technical Report IT, 2006, (pp 26-31).
- [5] Solms, R., *Information security management: why standards are important*, Information Management & Computer Security, Vol 7, No 1, 1999 (pp 50-57)
- [6] Fawaz, M., *Information security management systems*, ppt, QMI seminar, Malezija, 2004.
- [7] ISO/IEC 27001:2005, *Information technology - security techniques - information security management systems - Requirements*.
- [8] ISO/IEC 17799:2005, *Information technology - security techniques - code of practice for information security management*.
- [9] Veselin Gredić *Pregled evolucije standarda, modela i uputstava iz oblasti softverskog i sistem inženjeringa i njihovih međusobnih odnosa*, VOC, ppt
- [10] Uroš Katić, *ebXML: Globalni standard za poslovanje na Internetu*, Ekonomski fakultet Ljubljana, diplomski rad, 2002
- [11] mr Darinka Ivaneža, *Standardizacija – vrednovanje*, ppt
- [12] <http://standardi.yubc.net>
- [13] <http://www.iso-17799.com>
- [14] <http://www.itgovernance.co.uk/page.bs7799>
- [15] <http://www.ISO27001security.com/html/iso27000.html>
- [16] <http://csrc.nist.gov/publications/fips>

- [17] <http://csrc.nist.gov/publications/nistpubs>
- [18] <http://commoncriteriaportal.org>
- [19] http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_standard.pdf
- [20] <http://www.cissp.com>
- [21] <http://www.giac.org>
- [22] http://www.cisco.com/web/learning/le3/le2/le37/le54/learning_certification_type.htm
- [23] <http://www.jus.org.yu>
- [24] Dr Boško Rodić i mr Goran Đorđević - "Da li ste sigurni da ste bezbedni"
- [25] Dr Milan Milosavljević i mr Gojko Grubor - „Osnovi bezbednosti i zaštite informacionih sistema“