SLOVENSKI STANDARD

SIST ISO/IEC 27001

oktober 2010

Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

Information technology – Security techniques – Information security management systems – Requirements

Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27001:2010 (sl)

Nadaljevanje na straneh 2 do 35

NACIONALNI UVOD

Standard SIST ISO/IEC 27001 (sl), Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve, 2010, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27001 (en), Information technology – Security techniques – Information security management systems – Requirements, prva izdaja, 2005-10-15.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27001:2005 je pripravil pododbor združenega tehničnega odbora Mednarodne organizacije za standardizacijo in Mednarodne elektrotehniške komisije ISO/IEC JTC 1/SC 27 Varnostne tehnike v informacijski tehnologiji.

Slovenski standard SIST ISO/IEC 27001:2010 je prevod mednarodnega standarda ISO/IEC 27001:2005. Slovenski standard SIST ISO/IEC 27001:2010 je pripravil tehnični odbor SIST/TC ITC Informacijska tehnologija. V primeru spora glede besedila slovenskega prevoda je odločilen izvirni mednarodni standard v angleškem jeziku.

Odločitev za izdajo tega standarda je dne 23. aprila 2010 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27001:2005

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST ISO/IEC 27001:2010 to pomeni "slovenski standard".

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

– Definicije pojmov so povzete po naslednjih mednarodnih standardih:

  ISO/IEC 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

  ISO/IEC 17799, Informacijska tehnologija – Kodeks upravljanja varovanja informacij

  ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management

  ISO/IEC Guide 73, Risk management – Vocabulary

– V besedilu SIST ISO/IEC 27001 so v točkah 0.3, 1.1, 1.2, 2, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 6 in v dodatku navedeni mednarodni standardi ISO 9001, ISO/IEC 13335-1, ISO/IEC 13335-3, ISO/IEC 13335-4, ISO/IEC 17799, ISO/IEC TR 18044, ISO 19011, ISO 14001, ISO/IEC Guide 62 in ISO/IEC Guide 73. Pri tem je vedno mišljena njihova zadnja izdaja.

– Standard ISO/IEC 17799 je bil leta 2007 preštevilčen v ISO/IEC 27002.

VSEBINA **Stran**

Predgovor

ISO (Mednarodna organizacija za standardizacijo) in IEC (Mednarodna elektrotehniška komisija) tvorita specializiran sistem za svetovno standardizacijo. Nacionalni organi, ki so člani ISO ali IEC, sodelujejo pri pripravi mednarodnih standardov prek tehničnih odborov, ki jih za obravnavanje določenih strokovnih področij ustanovi ustrezna organizacija. Tehnični odbori ISO in IEC sodelujejo na področjih skupnega interesa. Pri delu sodelujejo tudi druge mednarodne, vladne in nevladne organizacije, povezane z ISO in IEC. Na področju informacijske tehnologije sta ISO in IEC vzpostavila združeni tehnični odbor ISO/IEC JTC 1.

Mednarodni standardi so pripravljeni v skladu s pravili, podanimi v 2. delu Direktiv ISO/IEC.

Glavna naloga tehničnih odborov je priprava mednarodnih standardov. Osnutki mednarodnih standardov, ki jih sprejmejo tehnični odbori, se pošljejo vsem članom v glasovanje. Za objavo mednarodnega standarda je treba pridobiti soglasje najmanj 75 odstotkov članov, ki se udeležijo glasovanja.

Opozoriti je treba na možnost, da je lahko nekaj elementov tega mednarodnega standarda predmet patentnih pravic. ISO in IEC ne prevzemata odgovornosti za prepoznavanje katerih koli ali vseh takih patentnih pravic.

ISO/IEC 27001 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

0 Uvod

0.1 Splošno

Ta mednarodni standard je bil pripravljen, da zagotovi model za vzpostavitev, izvajanje, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema upravljanja informacijske varnosti (SUIV). Odločitev za SUIV naj bi bila strateška odločitev za organizacijo. Na snovanje in izvedbo SUIV organizacije vplivajo njene potrebe in cilji, varnostne zahteve, vpeljani procesi ter velikost in struktura organizacije. Ti dejavniki in njihovi podporni sistemi se bodo po pričakovanjih s časom spreminjali. Pričakuje se, da se bo izvedba SUIV prilagajala potrebam organizacije, na primer enostavno stanje zahteva enostavno rešitev SUIV.

Ta mednarodni standard lahko notranje in zunanje stranke uporabijo za oceno skladnosti.

0.2 Procesni pristop

Ta mednarodni standard privzema procesni pristop k vzpostavitvi, izvajanju, delovanju, spremljanju, pregledovanju, vzdrževanju in izboljševanju SUIV organizacije.

Organizacija mora prepoznati in upravljati številne aktivnosti, da bi delovala uspešno. Vsaka aktivnost, ki uporablja vire in se upravlja, da bi omogočila preoblikovanje vhodov v izhode, se lahko šteje, da je proces. Pogosto izhod iz enega procesa predstavlja neposredni vhod v drug proces.

Uporaba sistema procesov v organizaciji skupaj s prepoznavanjem in medsebojnim delovanjem teh procesov ter njihovim upravljanjem se lahko imenuje "procesni pristop".

Procesni pristop pri upravljanju informacijske varnosti, ki je predstavljen v tem mednarodnem standardu, spodbuja svoje uporabnike, da se poudari pomen:

a) razumevanja zahtev informacijske varnosti organizacije ter potreb po vzpostavitvi politike in ciljev informacijske varnosti,

b) izvajanja in delovanja kontrol za obvladovanje informacijskih varnostnih tveganj organizacije znotraj celotnih poslovnih tveganj organizacije,

c) spremljanja in pregledovanja delovanja in uspešnosti SUIV ter

d) nenehnega izboljševanja na podlagi objektivnih meritev.

Ta mednarodni standard privzema model "načrtuj-izvedi-preveri-ukrepaj" (PDCA), ki se uporablja za strukturiranje vseh procesov SUIV. Slika 1 prikazuje, kako SUIV na vhodu sprejema zahteve informacijske varnosti in pričakovanja zainteresiranih strank ter s pomočjo potrebnih ukrepov in procesov proizvede izhode informacijske varnosti, ki izpolnjujejo te zahteve in pričakovanja. Slika 1 ponazarja tudi povezave v procesih, ki so predstavljeni v točkah 4, 5, 6, 7 in 8.

Privzem modela PDCA bo prav tako odražal načela, določena v Smernicah OECD (2001)[1], ki urejajo varnost informacijskih sistemov in omrežij. Ta mednarodni standard zagotavlja trden model za izvajanje načel iz teh smernic, ki urejajo ocenjevanje tveganja, zasnovo in izvedbo varnosti ter upravljanje in ponovno ocenjevanje varnosti.

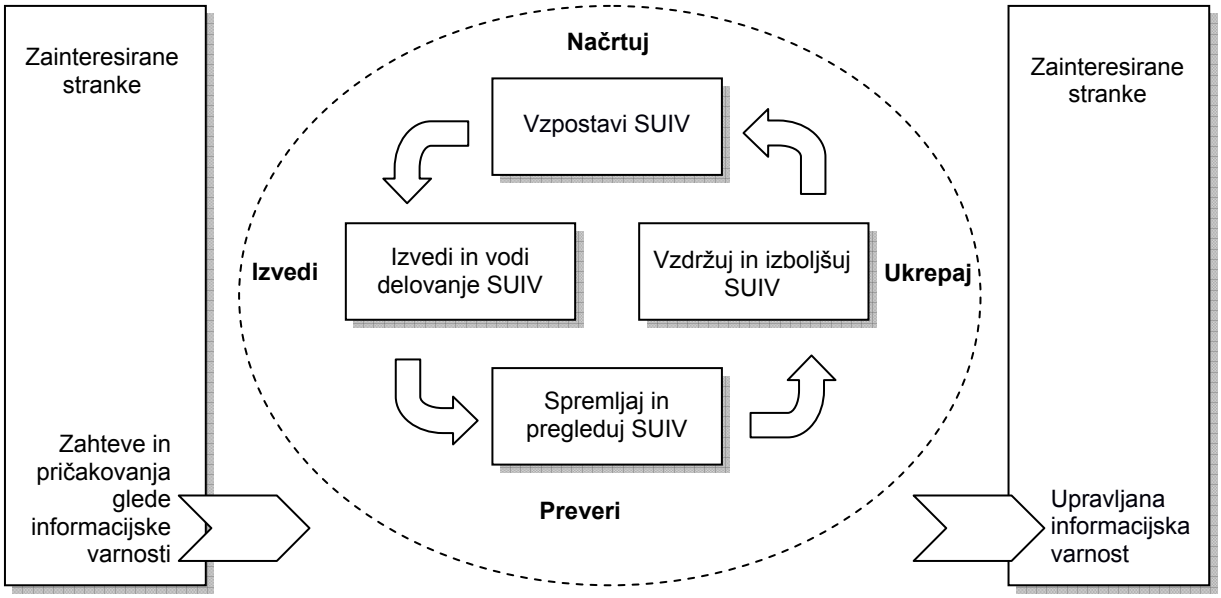
PRIMER 1:

Zahteva je lahko, da kršitve informacijske varnosti ne bodo povzročile resne finančne škode organizaciji in/ali jo osramotile.

PRIMER 2:

Pričakuje se lahko, da če se zgodi resen incident – morda vdor na spletno stran organizacije, namenjeno e-poslovanju, naj bi bili na voljo ljudje, ki so zadostno usposobljeni v postopkih za čim uspešnejše zmanjšanje tega vpliva.

[1] OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, julij 2002. www.oecd.org.



Slika 1: Model PDCA, uporabljen pri procesih SUIV

Načrtuj (vzpostavi SUIV)	Vzpostavi politiko SUIV, cilje, procese in postopke, ki so potrebni za obvladovanje tveganja in izboljševanje informacijske varnosti, tako, da se dosežejo rezultati v skladu s splošnimi politikami in cilji organizacije.
Izvedi (izvedi in vodi delovanje SUIV)	Izvedi in vodi delovanje politik, kontrol, procesov in postopkov SUIV.
Preveri (spremljaj in pregleduj SUIV)	Oceni, in kjer je mogoče, meri delovanje procesa glede na politiko SUIV, cilje in praktične izkušnje ter poročaj o rezultatih vodstvu, da jih pregleda.
Ukrepaj (vzdržuj in izboljšuj SUIV)	Na podlagi rezultatov notranjih presoj SUIV, vodstvenih pregledov in drugih pomembnih informacij izvedi popravne in preprečevalne ukrepe, da bi se dosegalo nenehno izboljševanje SUIV.

0.3 Združljivost z drugimi sistemi upravljanja

Ta mednarodni standard je usklajen z ISO 9001:2000 in ISO 14001:2004, da bi se podprli dosledna in združena izvedba in delovanje po ustreznih standardih za upravljanje. En primerno zasnovan sistem upravljanja lahko tako zadovolji zahteve vseh teh standardov. Preglednica C.1 ponazarja odnose med točkami tega mednarodnega standarda, ISO 9001:2000 in ISO 14001:2004.

Ta mednarodni standard je zasnovan, da omogoči organizaciji uskladitev ali združevanje njenega SUIV z zahtevami ustreznih sistemov upravljanja.

Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

POMEMBNO – To delo nima namena vključevati vseh potrebnih določb pogodbe. Uporabniki so odgovorni za njegovo pravilno uporabo. Skladnost z mednarodnim standardom sama po sebi ne odvezuje od zakonskih obveznosti.

1 Področje uporabe

1.1 Splošno

Ta mednarodni standard je namenjen vsem vrstam organizacij (na primer komercialnim podjetjem, državnim organom, nepridobitnim organizacijam). Ta mednarodni standard določa zahteve za vzpostavitev, izvajanje, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje dokumentiranega SUIV znotraj celotnih poslovnih tveganj organizacije. Določa zahteve za izvedbo varnostnih kontrol, ki so prilagojene potrebam posameznih organizacij ali njihovih delov.

SUIV je zasnovan, da zagotavlja izbiro primernih in sorazmernih varnostnih kontrol, ki ščitijo informacije in vzbujajo zaupanje zainteresiranim strankam.

OPOMBA 1: Sklici na "poslovanje" v tem mednarodnem standardu naj se razumejo širše, da pomenijo tiste dejavnosti, ki so temeljne za namene obstoja organizacije.

OPOMBA 2: ISO/IEC 17799 zagotavlja smernice za izvedbo, ki se lahko uporabijo pri snovanju kontrol.

1.2 Uporaba

Zahteve, postavljene v tem mednarodnem standardu, so generične in so namenjene uporabi v vseh organizacijah ne glede na vrsto, velikost in naravo. Izključevanje katere koli zahteve, določene v točkah 4, 5, 6, 7 in 8, ni sprejemljivo, kadar organizacija zagotavlja skladnost s tem mednarodnim standardom.

Vsakršno izključitev kontrol, za katere se je ugotovilo, da so potrebne za zadovoljevanje kriterijev za sprejem tveganja, je treba utemeljiti in zagotoviti je treba dokaze, da so odgovorne osebe sprejele s tem povezana tveganja. Kadar so katere koli kontrole izključene, trditve o skladnosti s tem mednarodnim standardom niso sprejemljive, razen če takšne izključitve ne vplivajo na sposobnost organizacije in/ali odgovornost, da zagotavlja informacijsko varnost, ki dosega varnostne zahteve, določene z ocenjevanjem tveganja, in ustrezne zahteve zakonodaje in predpisov.

OPOMBA: Če organizacija že ima delujoč sistem upravljanja poslovnih procesov (na primer v povezavi z ISO 9001 ali ISO 14001), je v večini primerov boljše, da se zahteve tega mednarodnega standarda izpolnijo znotraj tega obstoječega sistema upravljanja.

2 Zveza s standardi

Za uporabo tega standarda so nujno potrebni naslednji navedeni dokumenti. Pri datiranih sklicevanjih se uporablja zgolj navedena izdaja. Pri nedatiranih sklicevanjih se uporablja zadnja izdaja navedenega dokumenta (vključno z dopolnili).

ISO/IEC 17799:2005 Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti

3 Izrazi in definicije

V tem dokumentu so uporabljeni naslednji izrazi in definicije.

3.1
dobrina
kar koli, kar ima vrednost za organizacijo

[ISO/IEC 13335-1:2004]

3.2
razpoložljivost
lastnost, da je nekaj na zahtevo pooblaščenega subjekta dostopno in uporabno

[ISO/IEC 13335-1:2004]

3.3
zaupnost
lastnost, da informacija ni na voljo ali razkrita nepooblaščenim posameznikom, subjektom ali procesom

[ISO/IEC 13335-1:2004]

3.4
informacijska varnost
ohranjanje zaupnosti, celovitosti in razpoložljivosti informacije, dodatno so lahko vključene tudi druge lastnosti, kot so verodostojnost, odgovornost, nezanikanje in zanesljivost

[ISO/IEC 17799:2005]

3.5
informacijski varnostni dogodek

prepoznano dogajanje v sistemu, storitvi ali omrežju, ki kaže na morebitno kršitev informacijske varnosti, politike ali odpovedi kontrol ali na do tedaj še neznano okoliščino, ki je lahko pomembna za varnost

[ISO/IEC TR 18044:2004]

3.6
informacijski varnostni incident
eden ali več neželenih ali nepričakovanih informacijskih varnostnih dogodkov, ki predstavljajo veliko verjetnost ogrožanja poslovnih dejavnosti in informacijske varnosti

[ISO/IEC TR 18044:2004]

3.7
sistem upravljanja informacijske varnosti
SUIV
del celotnega sistema upravljanja, ki temelji na pristopu poslovnega tveganja in ki je namenjen vzpostavitvi, izvedbi, delovanju, spremljanju, pregledovanju, vzdrževanju in izboljševanju informacijske varnosti

OPOMBA: Sistem upravljanja vključuje organizacijsko strukturo, politike, aktivnosti načrtovanja, odgovornosti, prakse, postopke, procese in vire.

3.8
celovitost
lastnost varovanja točnosti in celovitosti dobrin

[ISO/IEC 13335-1:2004]

3.9
preostalo tveganje
tveganje, ki ostane po obravnavanju tveganja

[ISO/IEC Guide 73:2002]

3.10
sprejetje tveganja
odločitev, da se tveganje sprejme

[ISO/IEC Guide 73:2002]

3.11
analiza tveganja
sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja

[ISO/IEC Guide 73:2002]

3.12
ocenjevanje tveganja
celovit proces analize tveganja in vrednotenja tveganja

[ISO/IEC Guide 73:2002]

3.13
vrednotenje tveganja
proces, s katerim se ocenjeno tveganje primerja s kriterijem tveganja, da se določi pomembnost tveganja

[ISO/IEC Guide 73:2002]

3.14
obvladovanje tveganja
usklajene aktivnosti organizacije za usmerjanje in nadzor tveganja

[ISO/IEC Guide 73:2002]

3.15
obravnavanje tveganja
proces izbire in izvedbe ukrepov za spremembo tveganja

[ISO/IEC Guide 73:2002]

OPOMBA: V tem mednarodnem standardu se izraz "kontrola" uporablja kot sinonim za "ukrep".

3.16
izjava o uporabnosti
dokumentirana izjava, ki opisuje cilje kontrole in kontrole, ki so pomembni in uporabni za SUIV organizacije

OPOMBA: Cilji kontrole in kontrole temeljijo na rezultatih in ugotovitvah procesov ocenjevanja tveganja in obravnavanja tveganja, zahtevah zakonodaje in predpisov, pogodbenih obveznostih in poslovnih zahtevah za informacijsko varnost organizacije.

4 Sistem upravljanja informacijske varnosti

4.1 Splošne zahteve

Organizacija mora vzpostaviti, izvesti, voditi delovanje, spremljati, pregledovati, vzdrževati in izboljševati dokumentirani SUIV znotraj celotnih poslovnih dejavnosti organizacije in tveganj, s katerimi se sooča. V tem mednarodnem standardu je uporabljen proces, ki temelji na modelu PDCA in je prikazan na sliki 1.

4.2 Vzpostavljanje in upravljanje SUIV

4.2.1 Vzpostavi SUIV

Organizacija mora storiti naslednje:

a) določiti obseg in meje SUIV glede na značilnosti poslovanja, organizacije, svoje lokacije, dobrine in tehnologijo, vključno s podrobnostmi in utemeljitvami za vse izključitve iz obsega (glej 1.2);

b) določiti politiko SUIV glede na značilnosti poslovanja, organizacije, svoje lokacije, dobrine in tehnologije, tako da:

   1) vključi okvir za postavljanje ciljev ter vzpostavi celoten občutek za usmeritev in načela za ukrepanje v zvezi z informacijsko varnostjo,

   2) upošteva zahteve poslovanja, zakonodaje in predpisov ter pogodbene varnostne dolžnosti,

   3) uskladi z okoliščinami strateškega obvladovanja tveganja organizacije, v katerih bosta vzpostavitev in vzdrževanje SUIV potekali,

   4) vzpostavi kriterije za vrednotenje tveganja (glej 4.2.1.c)) in

   5) jo odobri vodstvo;

   OPOMBA: V tem mednarodnem standardu je politika SUIV mišljena kot razširitev informacijske varnostne politike. Ti politiki se lahko zapišeta v enem dokumentu.

c) določiti pristop k ocenjevanju tveganja organizacije:

   1) prepoznati metodologijo ocenjevanja tveganja, ki je primerna za SUIV in za prepoznane zahteve varnosti poslovnih informacij, zakonodaje in predpisov,

   2) razviti kriterije za sprejem tveganja in prepoznati sprejemljive ravni tveganja (glej 5.1.f));

   Izbrana metodologija ocenjevanja tveganja mora zagotoviti, da ocenjevanja tveganja proizvedejo primerljive in ponovljive rezultate.

   OPOMBA: Obstajajo različne metodologije ocenjevanja tveganja. Primeri metodologij ocenjevanja tveganja so obravnavani v ISO/IEC TR 13335-3, Informacijska tehnologija – Smernice za upravljanje informacijske varnosti – Tehnike upravljanja informacijske varnosti.

d) prepoznati tveganja:

   1) prepoznati dobrine, ki so zajete v SUIV, in njihove lastnike[2],

   2) prepoznati grožnje, ki ogrožajo te dobrine,

   3) prepoznati ranljivosti, ki bi jih grožnje lahko izkoristile,

   4) prepoznati vplive, ki bi jih izgube zaupnosti, celovitosti in razpoložljivosti lahko imele na te dobrine;

e) analizirati in ovrednotiti tveganja:

   1) oceniti poslovne vplive na organizacijo, ki bi lahko bili posledica varnostnih odpovedi, z upoštevanjem posledic izgube zaupnosti, celovitosti ali razpoložljivosti dobrin,

[2] Izraz "lastnik" označuje posameznika ali subjekt, ki ga vodstvo določi za odgovornega za nadzor proizvodnje, razvoja, vzdrževanja, uporabe in varovanja dobrin. Izraz "lastnik" ne pomeni osebe, ki bi dejansko imela kakršne koli lastninske pravice nad dobrino.

2) oceniti realno verjetnost pojava varnostnih odpovedi v luči prevladujočih groženj in ranljivosti ter vplivov, povezanih s temi dobrinami, ter trenutno izvedenih kontrol,

3) oceniti ravni tveganja,

4) določiti, ali so tveganja sprejemljiva, ali zahtevati obravnavo z uporabo kriterijev za sprejem tveganj, vzpostavljenih v 4.2.1.c)2);

f) prepoznati in vrednotiti možnosti obravnave tveganj:

Možni ukrepi so:

1) uporaba primernih kontrol,

2) zavestno in objektivno sprejemanje tveganj pod pogojem, da jasno zadovoljujejo politike organizacije in kriterije za sprejem tveganj (glej 4.2.1.c)2),

3) izogibanje tveganjem in

4) prenos povezanih poslovnih tveganj na druge stranke, na primer zavarovalnice, dobavitelje;

g) izbrati cilje kontrol in kontrole za obravnavo tveganj;

Cilje kontrol in kontrole je treba izbrati in izvesti tako, da izpolnjujejo zahteve, prepoznane v procesih ocenjevanja in obravnavanja tveganja. Izbira mora upoštevati kriterije za sprejem tveganj (glej 4.2.1.c)2)) ter tudi zahteve zakonodaje, predpisov in pogodb.

Cilje kontrol in kontrole iz dodatka A je treba izbrati kot del tega procesa kot ustrezne za zadovoljevanje prepoznanih zahtev.

Cilji kontrol in kontrole, navedeni v dodatku A, niso izčrpni in izbrati je mogoče dodatne cilje kontrol in kontrole.

OPOMBA: Dodatek A vsebuje obsežen seznam ciljev kontrol in kontrol, za katere se je ugotovilo, da so pogosto pomembni v organizacijah. Uporabniki tega mednarodnega standarda naj dodatek A upoštevajo kot začetno točko za izbiro kontrol, da zagotovijo, da nobena pomembna možnost kontrole ni spregledana.

h) pridobiti odobritev vodstva glede predlaganih preostalih tveganj;

i) pridobiti pooblastilo vodstva za izvedbo in vodenje delovanja SUIV;

j) pripraviti izjavo o uporabnosti:

Izjavo o uporabnosti je treba pripraviti tako, da vključuje:

1) cilje kontrol in kontrole, izbrane v 4.2.1.g), in razloge za njihovo izbiro,

2) cilje kontrol in kontrole, ki se trenutno izvajajo (glej 4.2.1.e)2)), in

3) izključitev katerih koli ciljev kontrol in kontrol iz dodatka A in utemeljitev za njihovo izključitev.

OPOMBA: Izjava o uporabnosti je povzetek odločitev glede obravnavanja tveganja. Utemeljevanje izključitev zagotavlja navzkrižno preverjanje, da nobene kontrole ne bi bile nehote izpuščene.

4.2.2 Izvedi in vodi delovanje SUIV

Organizacija mora storiti naslednje:

a) oblikovati načrt obravnavanja tveganja, ki prepozna ustrezni ukrep vodstva, vire, odgovornosti in prednostne naloge za obvladovanje informacijskih varnostnih tveganj (glej 5);

b) izvesti načrt obravnavanja tveganja, da doseže prepoznane cilje kontrol, kar vključuje upoštevanje zagotavljanja finančnih sredstev ter dodelitev vlog in odgovornosti;

c) izvesti kontrole, izbrane v 4.2.1.g), da doseže cilje kontrol;

d) določiti, kako meriti uspešnost izbranih kontrol ali skupin kontrol, in opredeliti, kako te meritve uporabiti za oceno uspešnosti kontrol, da proizvede primerljive in ponovljive rezultate (glej 4.2.3.c));

OPOMBA: Merjenje uspešnosti kontrol omogoča vodstvu in osebju določiti, kako dobro kontrole dosegajo načrtovane cilje kontrol.

e) izvesti programe usposabljanja in ozaveščanja (glej 5.2.2);

f) upravljati delovanje SUIV;

g) upravljati vire za SUIV (glej 5.2);

h) Izvesti postopke in druge kontrole, ki so sposobni omogočati hitro odkrivanje varnostnih dogodkov in odzivanje na varnostne incidente (glej 4.2.3.a)).

4.2.3 Spremljaj in pregleduj SUIV

Organizacija mora storiti naslednje:

a) izpeljati postopke spremljanja in pregledovanja ter druge kontrole za:

   1) hitro odkrivanje napak v rezultatih obdelav,

   2) hitro prepoznavanje poskusov in uspešnih varnostnih kršitev in incidentov;

   3) omogočanje vodstvu, da ugotovi, ali se varnostne aktivnosti, ki jih je dodelilo ljudem ali se izvajajo z informacijsko tehnologijo, opravljajo v skladu s pričakovanji;

   4) pomoč zaznavanju varnostnih dogodkov in tako preprečevanju varnostnih incidentov z uporabo indikatorjev ter

   5) ugotavljanje, ali so bili uspešni ukrepi, izvedeni za reševanje varnostne kršitve;

b) izvajati redne preglede uspešnosti SUIV (vključno z uresničevanjem politike in ciljev SUIV ter pregledovanjem varnostnih kontrol) z upoštevanjem rezultatov varnostnih presoj, incidentov, rezultatov merjenja uspešnosti, predlogov in povratnih informacij vseh zainteresiranih strank;

c) meriti uspešnost kontrol, da preveri, ali so izpolnjene varnostne zahteve.

d) pregledovati ocenjevanja tveganja v načrtovanih časovnih presledkih ter pregledovati preostala tveganja in prepoznane sprejemljive ravni tveganj z upoštevanjem sprememb v:

   1) organizaciji,

   2) tehnologiji,

   3) poslovnih ciljih in procesih,

   4) prepoznanih grožnjah,

   5) uspešnosti izvedenih kontrol ter

   6) zunanjih dogodkih, kot so spremembe v zakonodajnem in regulativnem okolju, spremenjene pogodbene obveze in spremembe v družbenem ozračju;

e) voditi notranje presoje SUIV v načrtovanih časovnih presledkih (glej 6);

   OPOMBA: Notranje presoje, včasih imenovane presoje prve stranke, vodi za notranje potrebe organizacija sama ali se vodijo v njenem imenu.

f) redno izvajati vodstvene preglede SUIV, da zagotovi, da obseg ostaja ustrezen in da so prepoznane izboljšave v procesih SUIV (glej 7.1);

g) posodabljati varnostne načrte, da upoštevajo ugotovitve aktivnosti spremljanja in pregledovanja;

h) zapisati ukrepe in dogodke, ki bi lahko vplivali na uspešnost ali delovanje SUIV (glej 4.3.3).

4.2.4 Vzdržuj in izboljšuj SUIV

Organizacija mora redno opravljati naslednje:

a) uvesti prepoznane izboljšave v SUIV;

b) sprejeti primerne popravne in preprečevalne ukrepe v skladu z 8.2 in 8.3. Uporabiti spoznanja, pridobljena na podlagi varnostnih izkušenj drugih organizacij in svojih lastnih;