SLOVENSKI STANDARD

SIST ISO/IEC 27004

marec 2011

Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijske varnosti – Merjenje

Information technology – Security techniques – Information security management – Measurement

Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Mesurge

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27004:2011 (sl)

Nadaljevanje na straneh 2 do 65

NACIONALNI UVOD

Standard SIST ISO/IEC 27004 (sl), Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijske varnosti – Merjenje, 2011, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27004 (en), Information technology – Security techniques – Information security management – Measurement, 2009.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27004:2009 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 27004:2011 je prevod mednarodnega standarda ISO/IEC 27004:2009. Slovenski standard SIST ISO/IEC 27004:2011 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 25. novembra 2010 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

SIST ISO/IEC 27000:2011 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje

SIST ISO/IEC 27001:2010 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve *(nadomeščen s SIST ISO/IEC 27001:2013)*

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27004:2009

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27004:2011 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

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 iz 2. dela Direktiv ISO/IEC.

Glavna naloga združenega tehničnega odbora je priprava mednarodnih standardov. Osnutki mednarodnih standardov, ki jih sprejme združeni tehnični odbor, se pošljejo nacionalnim organom v glasovanje. Za objavo kot mednarodni standard je treba pridobiti soglasje najmanj 75 % glasov glasujočih nacionalnih organov.

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

ISO/IEC 27004 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 daje napotke za razvoj in uporabo meril in merjenja, da se oceni uspešnost izvajanega sistema upravljanja informacijske varnosti (SUIV) ter kontrol ali skupine kontrol, kot jih določa ISO/IEC 27001.

To naj vključuje politiko, obvladovanje tveganj informacijske varnosti, cilje kontrol, kontrole, procese in postopke ter podpira procese njihovih revizij, kar naj bi pomagalo ugotoviti, ali je katerega od procesov ali kontrol SUIV treba spremeniti ali izboljšati. Pri tem je treba upoštevati, da nobeno merjenje kontrol ne more jamčiti za popolno varnost.

Izvajanje tega pristopa predstavlja program merjenja informacijske varnosti. Program merjenja informacijske varnosti bo vodstvu pomagal pri prepoznavanju in vrednotenju neskladnih in neuspešnih postopkov in kontrol SUIV ter pri določanju prednostnih ukrepov za izboljšanje ali spreminjanje teh procesov in/ali kontrol. Prav tako lahko pomaga organizaciji pri dokazovanju skladnosti z ISO/IEC 27001 in poda dodatna dokazila za vodstveni pregled procesov obvladovanja tveganj informacijske varnosti.

Ta mednarodni standard predpostavlja, da je izhodišče za razvoj meril in merjenja dobro razumevanje tveganj informacijske varnosti, s katerimi se organizacija sooča, in da so bile aktivnosti ocenjevanja tveganj organizacije pravilno izvedene (tj. temeljijo na ISO/IEC 27005), kot zahteva ISO/IEC 27001. Program merjenja informacijske varnosti bo spodbudil organizacijo, da bo deležnikom dala zanesljive informacije v zvezi z njenimi informacijskimi varnostnimi tveganji in statusom izvajanega SUIV pri obvladovanju teh tveganj.

Uspešno izveden program merjenja informacijske varnosti bi izboljšal zaupanje deležnikov v rezultate merjenja in jim omogočil, da uporabljajo ta merila za nenehno izboljševanje informacijske varnosti in SUIV.

Zbrani rezultati merjenja bodo omogočili primerjavo napredka pri doseganju ciljev informacijske varnosti v nekem časovnem obdobju kot dela procesa nenehnega izboljševanja SUIV v organizaciji.

0.2 Vodstveni pregled

ISO/IEC 27001 zahteva od organizacije, da "izvaja redne preglede uspešnosti SUIV z upoštevanjem rezultatov merjenja uspešnosti" in da "meri uspešnost kontrol, da preveri, ali so izpolnjene varnostne zahteve". ISO/IEC 27001 tudi zahteva, da organizacija "določi, kako meriti uspešnost izbranih kontrol ali skupin kontrol, in opredeli, kako te meritve uporabiti za oceno uspešnosti kontrol, da proizvede primerljive in ponovljive rezultate".

Pristop, ki ga organizacija sprejme za izpolnitev zahtev po merjenju, določenih v ISO/IEC 27001, se bo razlikoval glede na število pomembnih dejavnikov, vključno z informacijskimi varnostnimi tveganji, s katerimi se organizacija sooča, njeno velikostjo, razpoložljivimi viri ter relevantnimi zakonskimi, pravnimi in pogodbenimi zahtevami. Skrbna izbira in utemeljitev metode, uporabljene za izpolnjevanje zahtev po merjenju, sta pomembni za zagotovitev, da aktivnostim SUIV niso namenjeni prekomerni viri v škodo drugim aktivnostim. Idealno bi bilo, da so tekoča merjenja vključena v redne dejavnosti organizacije z minimalnimi dodatnimi potrebami po virih.

Kot podlago za izpolnitev zahtev po merjenju, določenih v ISO/IEC 27001, daje ta mednarodni standard organizaciji ustrezna priporočila za naslednje aktivnosti:

a) razvoj meril (npr. osnovnih meril, izpeljanih meril in kazalcev),

b) uvajanje in izvajanje programa merjenja informacijske varnosti,

c) zbiranje in analiziranje podatkov,

d) pridobivanje rezultatov merjenja,

e) sporočanje rezultatov razvitih merjenj deležnikom,

f) uporaba rezultatov merjenja kot prispevek k odločitvam v zvezi s SUIV,

g) uporaba rezultatov merjenja za prepoznavanje potreb po izboljšanju uporabljenega SUIV, vključno z njegovim obsegom, politikami, cilji, kontrolami, procesi in postopki, ter

h) spodbujanje nenehnega izboljševanja programa merjenja informacijske varnosti.

Eden od dejavnikov, ki vplivajo na sposobnost organizacije pri doseganju merjenja, je njena velikost. Na splošno velikost in kompleksnost poslovanja v kombinaciji s pomenom informacijske varnosti vplivata na obseg zahtevanega merjenja, in sicer tako glede števila meril, ki jih je treba izbrati, kot glede pogostosti zbiranja in analiziranja podatkov. Za MSP (majhna in srednje velika podjetja) bo zadostoval program merjenja informacijske varnosti z manj obsežnimi informacijami, medtem ko bodo večja podjetja hkrati uvedla in uporabila več programov merjenja informacijske varnosti.

V majhnih organizacijah lahko zadostuje enojni program merjenja informacijske varnosti, medtem ko lahko v velikih podjetjih obstaja potreba po večkratnem programu merjenja informacijske varnosti.

Napotki, ki jih zagotavlja ta mednarodni standard, bodo imeli za posledico izdelavo dokumentacije, ki bo prispevala k dokazovanju, da se uspešnost kontrol meri in ocenjuje.

Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijske varnosti – Merjenje

1 Področje uporabe

Ta mednarodni standard daje napotke za razvoj in uporabo meril in meritev, namenjenih oceni uspešnosti izvajanega sistema upravljanja informacijske varnosti (SUIV) in kontrol ali skupin kontrol, določenih v ISO/IEC 27001.

Ta mednarodni standard se uporablja za vse vrste in velikosti organizacij.

OPOMBA: Ta dokument uporablja glagolske oblike za izražanje določb (npr. "morati, je treba", "se ne sme", "naj bi", "naj ne bi", "lahko", "ni treba", " je mogoče" in "ni mogoče"), ki so določene v Direktivah ISO/IEC, 2. del, 2004, Dodatek H. Glej tudi ISO/IEC 27000:2009, Dodatek A.

2 Zveze s standardi

Naslednja dokumenta sta nujna za uporabo tega dokumenta. Pri datiranem sklicevanju velja samo navedena izdaja. Pri nedatiranem sklicevanju velja zadnja izdaja dokumenta, na katerega se nanaša sklic (vključno z morebitnimi dopolnitvami).

ISO/IEC 27000:2009 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje

ISO/IEC 27001:2005 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve

3 Izrazi in definicije

V tem dokumentu se uporabljajo izrazi in definicije iz ISO/IEC 27000 ter naslednje:

3.1 analitični model
algoritem ali izračun, ki združuje eno ali več osnovnih in/ali izpeljanih meril, povezanih z odločitvenimi kriteriji

[ISO/IEC 15939:2007]

3.2 lastnost
lastnost ali značilnost predmeta, ki jo je na podlagi človeške ali avtomatske ocene mogoče količinsko ali kakovostno razlikovati

[ISO/IEC 15939:2007]

3.3 osnovno merilo
merilo, opredeljeno z lastnostjo in metodo za določitev njene količine

[ISO/IEC 15939:2007]

OPOMBA: Osnovno merilo je funkcionalno neodvisno od drugih meril.

3.4 podatki
zbirka vrednosti, dodeljenih osnovnim merilom, izpeljanim merilom in/ali kazalcem

[ISO/IEC 15939:2007]

3.5 odločitveni kriteriji
pragovi, cilji ali vzorci, uporabljeni za določanje potrebe po nadaljnjem ukrepu ali preiskavi ali za opis stopnje zaupanja v dani rezultat

[ISO/IEC 15939:2007]

3.6 izpeljano merilo
merilo, ki je opredeljeno kot funkcija vrednosti dveh ali več osnovnih meril

[ISO/IEC 15939:2007]

3.7 kazalec
merilo, ki zagotovi oceno ali vrednotenje določenih lastnosti, izpeljanih iz analitičnega modela, glede na opredeljene informacijske potrebe

3.8 informacijska potreba
vpogled, ki je potreben za upravljanje ciljev, nalog, tveganj in problemov

[ISO/IEC 15939:2007]

3.9 merilo
spremenljivka, katere vrednost je določena kot rezultat merjenja

[ISO/IEC 15939:2007]

OPOMBA: Izraz "merilo" se uporablja kot skupno poimenovanje osnovnih meril, izpeljanih meril in kazalcev.

PRIMER: Primerjava izmerjene stopnje napake z načrtovano stopnjo napake skupaj z oceno ali razliko nakazuje na problem.

3.10 merjenje
proces pridobivanja informacij o uspešnosti SUIV in kontrol z uporabo metode merjenja, merilne funkcije merjenja, analitičnega modela in odločitvenega kriterija

3.11 funkcija merjenja
algoritem ali izračun, izpeljan z združitvijo dveh ali več osnovnih meril

[ISO/IEC 15939:2007]

3.12 metoda merjenja
logično zaporedje generično opisanih postopkov, uporabljenih pri določanju velikosti lastnosti z upoštevanjem določene lestvice

[ISO/IEC 15939:2007]

OPOMBA: Vrsta metode merjenja je odvisna od narave postopkov, uporabljenih za določanje velikosti lastnosti. Razlikovati je mogoče dve vrsti metod:

– subjektivne metode: določanje velikosti, ki vključuje človeško presojo;

– objektivne metode: določanje velikosti, ki temelji na numeričnih pravilih.

3.13 rezultati merjenja
eden ali več kazalcev in z njimi povezane razlage, ki se nanašajo na neko informacijsko potrebo

3.14 predmet
stvar, opredeljena z merjenjem njenih lastnosti

3.15 lestvica
urejen niz vrednosti, zvezni in diskretni, ali niz kategorij, na katere so vezane lastnosti

[ISO/IEC 15939:2007]

OPOMBA: Vrsta lestvice je odvisna od narave razmerja med vrednostmi na lestvici. Splošno so opredeljene štiri vrste lestvic:

– nominalna: vrednosti merjenja so kategorične;

– vrstilna: vrednosti merjenja so razvrstitvene;

– intervalna: vrednosti merjenja so enakih razdalj, ki ustrezajo enakim velikostim lastnosti;

– razmernostna: vrednosti merjenja so enakih razdalj, ki ustrezajo enakim velikostim lastnosti, kjer vrednost nič ne ustreza nobeni lastnosti.

To so le primeri vrste lestvic.

3.16 merska enota
specifična velikost, določena in sprejeta s konvencijo, s katero se druge velikosti iste vrste primerjajo z namenom, da se izrazijo njihove velikosti glede na to količino

[ISO/IEC 15939:2007]

3.17 potrjevanje
potrdilo z zagotavljanjem stvarnih dokazov, da so izpolnjene zahteve za posebej predvideno uporabo ali aplikacijo

3.18 preverjanje (preveritev)
potrdilo z zagotavljanjem stvarnih dokazov, da so določene zahteve izpolnjene

[ISO 9000:2005]

OPOMBA: To se lahko imenuje tudi preskušanje skladnosti.

4 Struktura tega mednarodnega standarda

Ta mednarodni standard pojasnjuje merila in aktivnosti merjenja, potrebne za oceno uspešnosti zahtev SUIV za upravljanje ustreznih in sorazmernih varnostnih kontrol, kot je zahtevano v ISO/IEC 27001:2005, 4.2.

Ta mednarodni standard je strukturiran na naslednji način:

- pregled programa merjenja informacijske varnosti in modela merjenja informacijske varnosti (točka 5),
- odgovornosti vodstva za merjenja informacijske varnosti (točka 6) ter
- konstrukti merjenja in procesi (tj. načrtovanje in razvoj, izvajanje in delovanje ter izboljševanje merjenj: sporočanje rezultatov merjenja), ki se izvajajo v okviru programa merjenja informacijske varnosti (točke 7–10).

Poleg tega dodatek A navaja vzorčno predlogo konstrukta merjenja, katerega sestavine so elementi modela merjenja informacijske varnosti (glej točko 7). Dodatek B določa vzorce konstrukta merjenja za posebne kontrole ali procese SUIV z uporabo vzorca iz dodatka A.

Namen teh primerov je pomagati organizaciji pri načinu, kako izvajati merjenje informacijske varnosti ter kako merjenja in njihove rezultate dokumentirati.

5 Pregled merjenja informacijske varnosti

5.1 Cilji merjenja informacijske varnosti

Cilji merjenja informacijske varnosti v okviru SUIV vključujejo:

a) vrednotenje uspešnosti izvajanih kontrol ali skupin kontrol (glej "4.2.2.d)" na sliki 1);

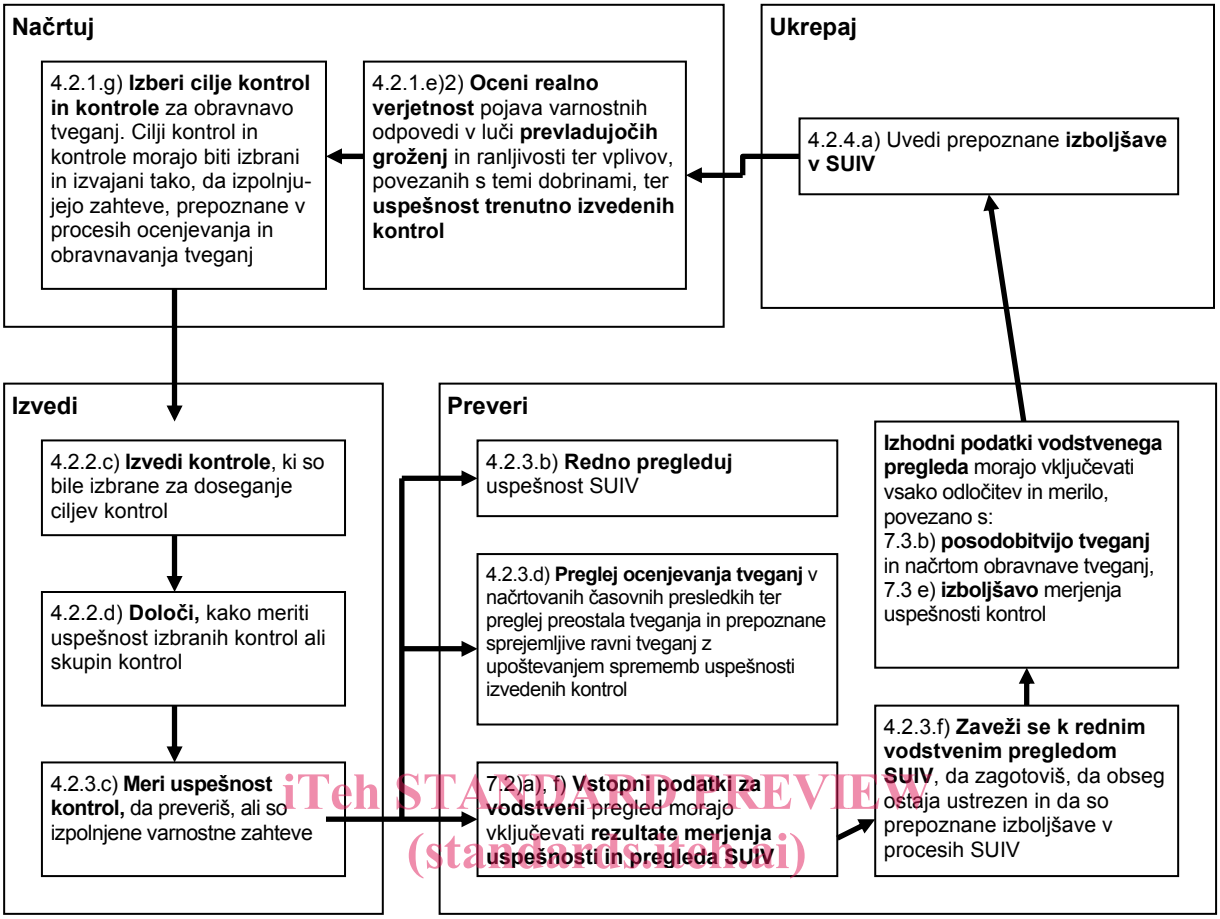
b) vrednotenje uspešnosti izvajanega SUIV (glej "4.2.3.b)" na sliki 1);

c) preverjanje obsega, do katerega so bile izpolnjene prepoznane varnostne zahteve (glej "4.2.3.c)" na sliki 1);

d) pospeševanje izboljšanja uspešnosti informacijske varnosti glede na celotna poslovna tveganja organizacije;

e) zagotavljanje vstopnih podatkov za vodstveni pregled, namenjen pospeševanju sprejemanja odločitev v zvezi s SUIV in utemeljitvi potrebnih izboljšav pri izvedbi SUIV.

Slika 1 prikazuje ciklično vhodno-izhodno razmerje meritev v razmerju do cikla Načrtuj–Izvedi–Preveri–Ukrepaj (PDCA), opredeljenega v standardu ISO/IEC 27001. Številke v vsaki sliki predstavljajo ustrezne podtočke ISO/IEC 27001:2005.



Slika 1: Merjenje vhodnih in izhodnih podatkov v ciklusu PDCA SUIV upravljanja informacijske varnosti

Organizacija naj vzpostavi cilje merjenja, ki temeljijo na številnih dejavnikih, vključno z:

a) vlogo informacijske varnosti pri podpori celotne poslovne dejavnosti organizacije in tveganjih, s katerimi se sooča,

b) veljavnimi zakonodajnimi, regulatornimi in pogodbenimi zahtevami,

c) organizacijsko strukturo,

d) stroški in koristmi merjenja izvedenih ukrepov informacijske varnosti,

e) kriteriji sprejemljivosti tveganj za organizacijo in

f) potrebo po primerjanju več SUIV znotraj iste organizacije.

5.2 Program merjenja informacijske varnosti

Organizacija naj vzpostavi in upravlja program merjenja informacijske varnosti, da doseže zastavljene cilje merjenja in sprejme model PDCA v okviru celotnih dejavnosti merjenja organizacije. Organizacija naj tudi razvije in izvaja konstrukte merjenja za doseganje ponovljivih, objektivnih in koristnih rezultatov merjenja, ki temeljijo na modelu merjenja informacijske varnosti (glej 5.4).

Program merjenja informacijske varnosti in razviti konstrukt merjenja naj zagotovi, da organizacija uspešno doseže objektivne in ponovljive meritve ter deležnikom zagotovi rezultate merjenja za prepoznavanje potreb po izboljšanju izvajanja SUIV, vključno z njegovim obsegom, politikami, cilji, kontrolami, procesi in postopki.

Program merjenja informacijske varnosti naj vsebuje naslednje postopke:

a) razvoj meril in merjenja (glej točko 7),

b) postopek merjenja (glej točko 8),

c) analizo podatkov in poročanje o rezultatih merjenja (glej točko 9) ter

d) vrednotenje in izboljševanje programa merjenja informacijske varnosti (glej točko 10).

Organizacijska in izvedbena struktura programa merjenja informacijske varnosti naj se določita ob upoštevanju obsega in zahtevnosti SUIV, katerega del sta. V vseh primerih naj se vloge in odgovornosti za program merjenja informacijske varnosti izrecno dodelijo kompetentnemu strokovnemu osebju (glej 7.5.8).

Merila, izbrana in izvedena s programom merjenja informacijske varnosti, naj bodo neposredno povezana s postopkom SUIV, z drugimi merili in tudi s poslovnimi procesi organizacije. Merjenje je mogoče vključiti v običajne operativne dejavnosti ali ga izvajati v točnih časovnih razmikih, ki jih določi vodstvo SUIV.

5.3 Dejavniki uspeha

V nadaljevanju so podani nekateri dejavniki, ki prispevajo k uspehu programa merjenja informacijske varnosti pri spodbujanju nenehnega izboljševanja SUIV:

a) zavezanost vodstva, podprta z ustreznimi viri,

b) obstoj procesov in postopkov SUIV,

c) ponovljivi procesi, sposobni zajemanja in poročanja o pomembnih podatkih za zagotovitev ustreznih trendov v določenem časovnem obdobju,

d) merljivi ukrepi na podlagi ciljev SUIV,

e) preprosto dosegljivi podatki, ki jih je mogoče uporabiti za merjenje,

f) vrednotenje uspešnosti programa merjenja informacijske varnosti in izvajanje prepoznanih izboljšav,

g) dosledno periodično zbiranje in analiziranje podatkov merjenja ter poročanje o njih na smiseln način,

h) uporaba rezultatov merjenja pri deležnikih za prepoznavanje potreb po izboljšanju izvajanja SUIV, vključno z njegovim obsegom, politikami, cilji, kontrolami, procesi in postopki,

i) sprejem povratnih informacij o rezultatih merjenja od ustreznih deležnikov in

j) vrednotenje uporabnosti rezultatov merjenja in izvajanja prepoznanih izboljšav.

Ko je program merjenja informacijske varnosti uspešno izveden, je z njim mogoče:

1) prikazati skladnost organizacije z veljavnimi zakonskimi ali regulatornimi zahtevami in pogodbenimi obveznostmi;

2) podpreti prepoznavanje prej nezaznanih ali neznanih vprašanj informacijske varnosti;

3) pomagati pri izpolnjevanju potreb upravljavskega poročanja, ko se podajajo merila za pretekle in sedanje aktivnosti, ter

4) ga uporabiti kot vir vstopnih podatkov za proces obvladovanja tveganja informacijske varnosti, notranje presoje SUIV in vodstvene preglede.

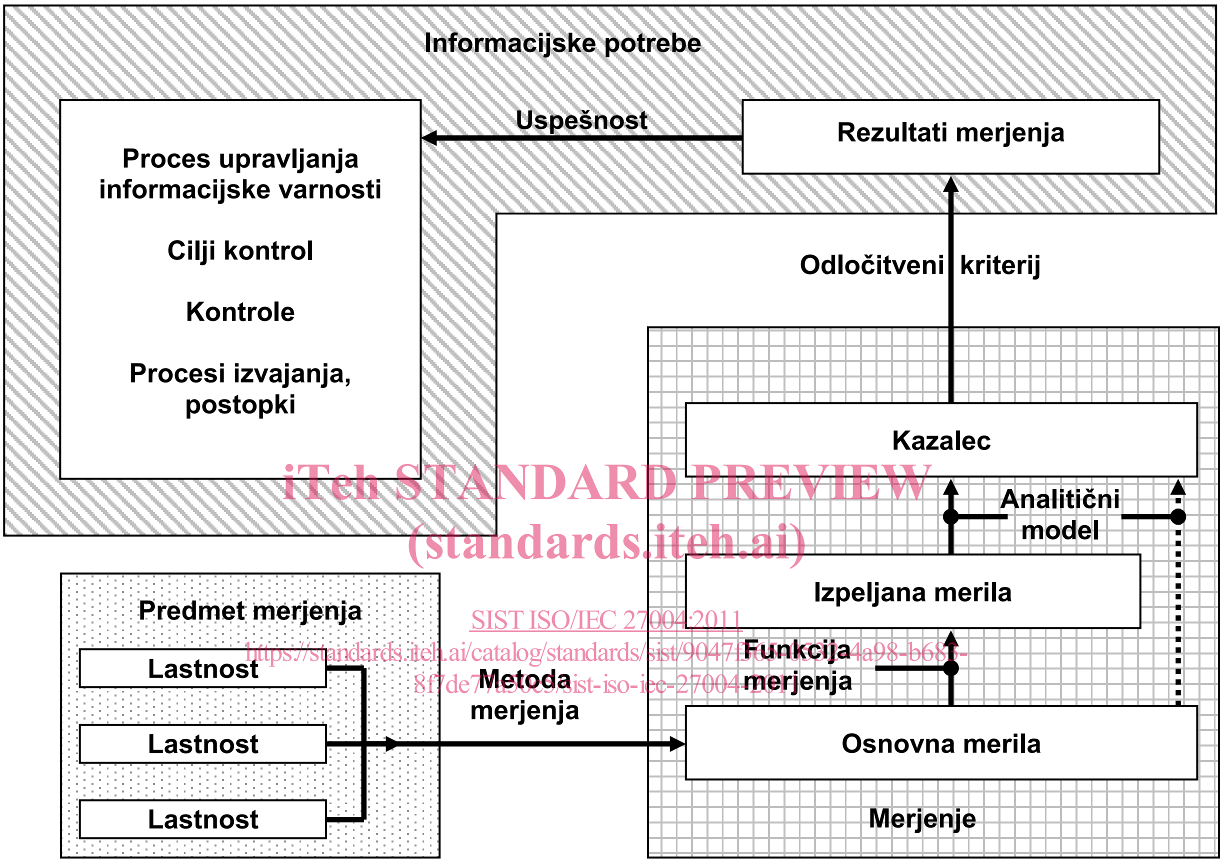
5.4 Model merjenja informacijske varnosti

OPOMBA: Koncepti modela merjenja informacijske varnosti in konstruktov merjenja, sprejetih v tem mednarodnem standardu, temeljijo na tistih, ki so navedeni v ISO/IEC 15939. Izraz "podatki o izdelku", ki se uporablja v ISO/IEC 15939, je sinonim za "rezultati merjenja" v tem mednarodnem standardu, in izraz "proces merjenja", uporabljen v ISO/IEC 15939, je sinonim za “program merjenja” v tem mednarodnem standardu.

5.4.1 Pregled

Model merjenja informacijske varnosti je struktura, ki povezuje informacijske potrebe z ustreznimi predmeti merjenja in njihovimi lastnostmi. Predmeti merjenja lahko vključujejo načrtovane ali izvedene procese, postopke, projekte ali vire.

Model merjenja informacijske varnosti opisuje, kako so ustrezne lastnosti kvantificirane in pretvorjene v kazalce, ki so podlaga za sprejemanje odločitev. Slika 2 prikazuje model merjenja informacijske varnosti.



Slika 2: Model merjenja informacijske varnosti

OPOMBA: Točka 7 zagotavlja podrobne informacije o posameznih elementih modela merjenja informacijske varnosti.

Naslednje podtočke uvajajo posamezne elemente modela. Navajajo tudi primere, kako so ti posamezni elementi uporabljeni.

Informacijske potrebe ali namen merjenj, uporabljenih v primerih, ki jih vsebujejo preglednice 1 do 4 naslednjih podtočk, so namenjeni oceni ozaveščenosti ustreznega osebja organizacije o stanju skladnosti z varnostno politiko organizacije (cilj kontrole A.8.2 ter kontrol A.8.2.1 in A.8.2.2 standarda ISO/IEC 27001:2005).

5.4.2 Osnovno merilo in metoda merjenja

Osnovno merilo je najenostavnejše merilo, ki ga je mogoče pridobiti. Osnovno merilo je rezultat uporabe metode merjenja na izbranih lastnostih predmeta merjenja. Predmet merjenja ima lahko veliko lastnosti, vendar lahko le nekatere nudijo uporabne vrednosti, povezljive z osnovnim merilom. Dana lastnost se lahko uporablja za več različnih osnovnih meril.

Metoda merjenja je logično zaporedje postopkov, uporabljenih pri kvantifikaciji lastnosti v zvezi z določenim merilom. Postopek lahko vključuje aktivnosti, kot so štetje dogodkov ali opazovanje skozi čas.

Metoda merjenja lahko omogoča dodelitev lastnosti predmetu merjenja. Primeri predmeta merjenja vključujejo, vendar niso omejeni na:

- delovanje kontrol, izvedenih v SUIV;
- status informacijskih dobrin, zaščitenih s kontrolami;
- delovanje procesov, ki se izvajajo v SUIV;
- ravnanje osebja, ki je odgovorno za izvajanje SUIV;
- aktivnosti organizacijske enote, odgovorne za informacijsko varnost; in
- obseg zadovoljstva zainteresiranih strani.

Metoda merjenja lahko uporabi za merjenje predmete merjenja in lastnosti iz različnih virov, kot so:

- rezultati analize tveganj in ocene tveganj;
- vprašalniki in osebni intervjuji;
- notranja in/ali zunanja poročila o presoji;
- zapisi dogodkov, kot so dnevniki, statistična poročila in revizijske sledi;
- poročila o incidentih, še posebej tistih, ki povzročijo nastanek vpliva na dogodke;
- rezultati testov, na primer testiranja penetracije, socialnega inženiringa, skladnosti orodij in orodij za presojo varnosti; ali
- zapisi iz postopkov in programov v zvezi z informacijsko varnostjo organizacije, na primer rezultati usposabljanja o ozaveščanju o informacijski varnosti.

Spodnje preglednice 1 do 4 predstavljajo uporabo modela informacijske varnosti za naslednji kontroli:

- "kontrola 2" se nanaša na kontrolo A.8.2.1 Odgovornosti vodstva iz ISO/IEC 27001:2005 ("Vodstvo mora zahtevati od zaposlenih, pogodbenikov in uporabnikov tretje stranke varnostno ravnanje v skladu z vzpostavljenimi politikami in postopki organizacije"), ki se izvaja na naslednji način: "Vse osebje, ki je pomembno za SUIV, mora podpisati uporabniško izjavo, preden se mu odobri dostop do določenega informacijskega sistema."

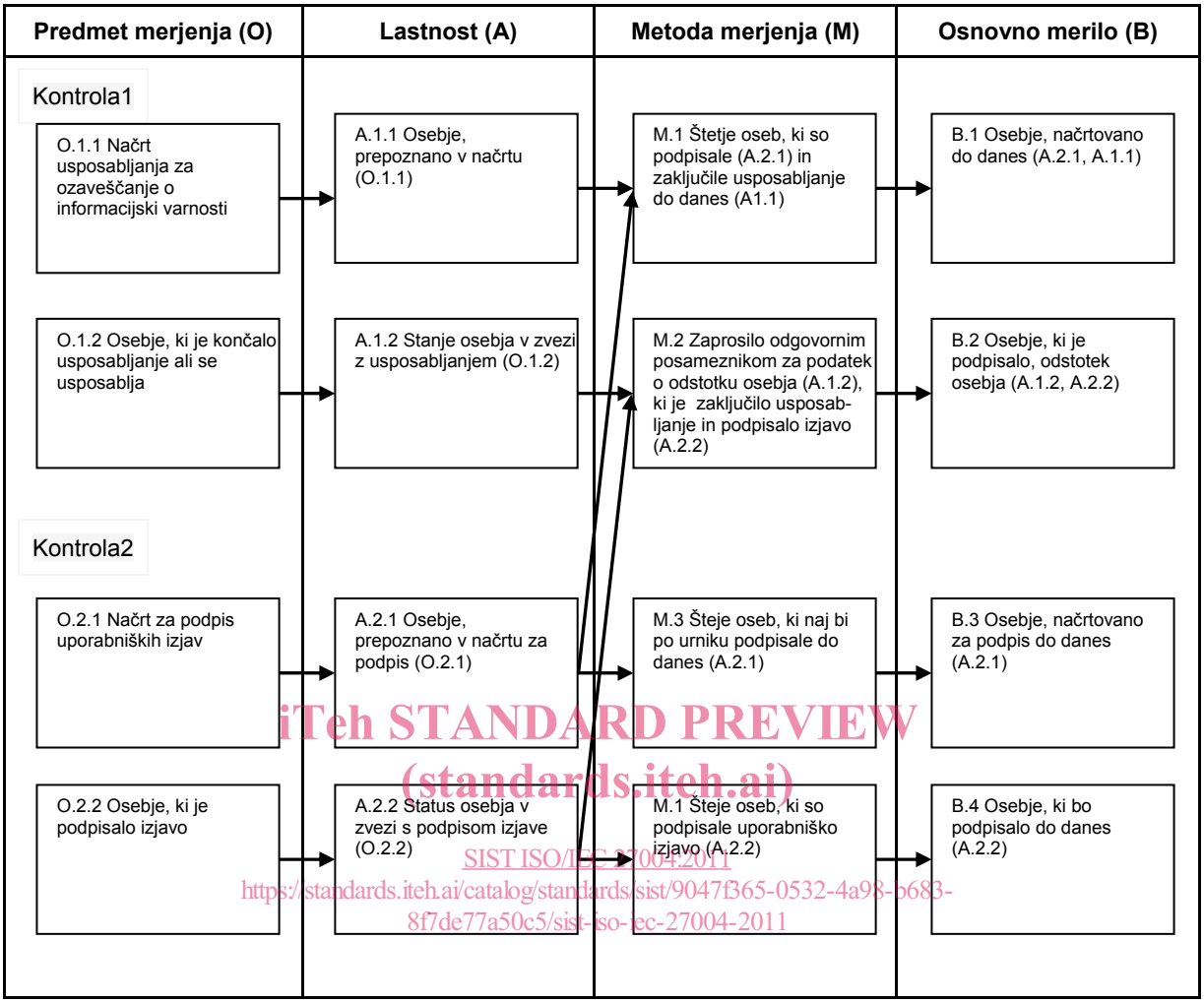
- "kontrola 1" se nanaša na kontrolo A.8.2.2 Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti" iz ISO/IEC 27001:2005 ("Vsi zaposleni v organizaciji, in kadar je to ustrezno, pogodbeniki in uporabniki tretje stranke morajo biti ustrezno ozaveščeni in seznanjeni z rednimi posodobitvami organizacijskih politik in postopkov, ki so pomembni za njihovo delovno mesto"), ki se izvaja na naslednji način: "Vse osebje, pomembno za SUIV, mora opraviti informativno usposabljanje o informacijski varnosti, preden se jim dodeli dostop do določenega informacijskega sistema".

Ustrezni konstrukti merjenje so vsebovani v B.1.

OPOMBA: Preglednice 1 do 4 so sestavljene iz različnih stolpcev (preglednica 1 iz štirih stolpcev, preglednice 2 do 4 iz treh stolpcev), katerim so dodeljene črkovne oznake. Vsakemu polju v posameznem stolpcu je dodeljena številčna oznaka. Kombinacije oznak s črko in številko se uporabljajo v poljih, ki sledijo prejšnjim poljem. Puščice označujejo pretok podatkov med posameznimi elementi modela merjenja informacijske varnosti v nekem konkretnem primeru.

Preglednica 1 vsebuje primer odnosov med predmetom merjenja, lastnostjo, metodo merjenja in osnovnim merilom za merjenje predmetov, določenih za izvajanje zgoraj opisanih kontrol.

Preglednica 1: Primer osnovnega merila in metode merjenja



5.4.3 Izpeljano merilo in funkcija merjenja

Izpeljano merilo je agregat dveh ali več osnovnih meril. Dano osnovno merilo lahko služi kot vhodni podatek za več izpeljanih meril.

Funkcija merjenja je izračun, uporabljen za kombiniranje osnovnih meril za oblikovanje izpeljanega merila.

Lestvica in enota izpeljanega merila sta odvisni od lestvic in enot osnovnih meril, iz katerih sta sestavljeni, ter tudi, kako so te kombinirane s pomočjo funkcije merjenja.

Funkcija merjenja lahko vključuje različne tehnike, kot so povpreček osnovnih meril, uporaba uteži pri osnovnih merilih ali dodelitev kvalitativne vrednosti osnovnim merilom. Funkcija merjenja lahko kombinira osnovna merila z uporabo različnih obsegov, kot so odstotki in rezultati kakovostnega ocenjevanja.

Primer razmerja drugih elementov uporabe modela merjenja informacijske varnosti, to je osnovnega merila, merilne funkcije in izpeljanega merila, je predstavljen v preglednici 2.