SLOVENSKI STANDARD

SIST ISO/IEC 27002

maj 2008

Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti / Opomba: Združuje ISO/IEC 17799 (2005-06) (preštevilčen v ISO/IEC 27002) in ISO/IEC 17799 Tehnični popravek 1 (2007-07)

Information technology – Security techniques – Code of practice for information security management / Note: Combines ISO/IEC 17799 (2005-06) (renumbered to ISO/IEC 27002) and ISO/IEC 17799 Technical Corrigendum 1 (2007-07)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27002:2008 (sl)

Nadaljevanje na straneh od 2 do 117

© 2013-05 Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

NACIONALNI UVOD

Standard SIST ISO/IEC 27002 (sl), Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti, 2008, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27002 (en), Information technology – Security techniques – Code of practice for information security management, prva izdaja, 2005-06-15.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27002:2005 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 27002:2008 je prevod mednarodnega standarda ISO/IEC 27002:2005. Slovenski standard SIST ISO/IEC 27002:2008 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 27. marca 2008 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27002:2005

OPOMBE

iTeh STANDARD PREVIEW
(standards.iteh.ai)

– Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST ISO/IEC 27002:2008 to pomeni "slovenski standard".

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8affe37/sist-iso-iec-27002-2008

– 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 TR 18044, Information technology – Security techniques – Information security incident management

  ISO/IEC Guide 2, Standardization and related activities – General vocabulary

  ISO/IEC Guide 73, Risk management – Vocabulary

– V besedilu SIST ISO/IEC 27002 so v točkah 2.1, 2.3, 2.6, 2.7, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 4.1, 5.1.1, 6.1.1, 6.1.8, 7.1.1, 10.6.1, 12.1.1, 12.3.1, 12.3.2, 12.4.3, 12.5.4, 13.1.1 in 15.1.3 navedeni mednarodni standardi ISO/IEC 13335-1, ISO/IEC 13335-3, ISO/IEC TR 18044, ISO 19011, ISO/IEC 18028, ISO/IEC 11770, ISO/IEC 9796, ISO/IEC 14888, ISO 10007, ISO/IEC 12207, ISO/IEC 15408, ISO 15489-1, ISO/IEC Guide 2, ISO/IEC Guide 73 in IEEE P1363. Pri tem je vedno mišljena njihova zadnja izdaja.

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

VSEBINA **Stran**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8affbc37/sist-iso-iec-27002-2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/1980af29-d798-4205-a199-b70bb8afbc37/sist-iso-iec-27002-2008

Predgovor k standardu ISO/IEC 27002:2005

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 27002 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

Prva izdaja tega standarda ISO/IEC 27002 združuje ISO/IEC 17799:2005 in ISO/IEC 17799:2005/Cor.1:2007. Njena tehnična vsebina je istovetna vsebini ISO/IEC 17799:2005. Popravek ISO/IEC 17799:2005/Cor.1:2007 spreminja referenčno številko standarda iz 17799 v 27002. ISO/IEC 17799:2005 in ISO/IEC 17799:2005/Cor.1: 2007 sta začasno zadržana do objave druge izdaje ISO/IEC 27002.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

Predgovor k standardu ISO/IEC 17799:2005

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 17799 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

Ta druga izdaja razveljavlja in nadomešča prvo izdajo (ISO/IEC 17799:2000), ki je bila tehnično spremenjena.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Skupina mednarodnih standardov o sistemu upravljanja informacijske varnosti (ISMS) se razvija v okviru ISO/IEC JTC 1/SC 27. Skupina vključuje mednarodne standarde o zahtevah za sistem upravljanja informacijske varnosti, obvladovanje tveganja, metrike in merjenja ter napotke za izvajanje. Ta družina bo sprejela sistem številčenja z nizom številk 27000 in zaporedno naprej.

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

Od leta 2007 se predlaga vključitev nove izdaje ISO/IEC 17799 v to novo shemo številčenja kot ISO/IEC 27002.

0 Uvod

0.1 Kaj je informacijska varnost

Informacija je dobrina, ki je tako kot druge pomembne poslovne dobrine bistvenega pomena za poslovanje organizacije in jo je zato treba ustrezno zaščititi. To je še posebej pomembno v sedanjem, vse bolj povezanem poslovnem okolju. Kot rezultat tega povečanja medsebojne povezanosti so informacije zdaj vse bolj izpostavljene različnim grožnjam in ranljivostim (glej tudi Smernice OECD za varnost informacijskih sistemov in omrežij).

Informacija lahko obstaja v različnih oblikah. Lahko je natisnjena ali napisana na papirju, shranjena v elektronski obliki, prenesena po pošti ali z uporabo elektronskih sredstev, prikazana na filmu ali izgovorjena v pogovoru. Ne glede na obliko informacije ali sredstva, s katerim je v skupni rabi, mora vedno biti ustrezno zaščitena.

Informacijska varnost je zaščita informacij pred različnimi grožnjami, da bi zagotovili neprekinjeno poslovanje, zmanjšali poslovno tveganje ter čim bolj povečali donosnost naložb in poslovnih priložnosti.

Informacijska varnost se doseže z izvajanjem ustreznih nizov kontrol, vključno s politikami, procesi, postopki, organizacijskimi strukturami ter funkcijami programske in strojne opreme. Te kontrole je treba vzpostaviti, izvajati, spremljati, pregledovati in izboljševati, kadar je to potrebno, da se zagotovi, da so izpolnjeni posebni varnostni in poslovni cilji organizacije. To je treba storiti v povezavi z drugimi procesi upravljanja poslovanja.

0.2 Zakaj je informacijska varnost potrebna

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Informacije in podporni procesi, sistemi in omrežja so pomembne poslovne dobrine. Opredelitev, doseganje, vzdrževanje in izboljševanje informacijske varnosti so lahko bistvenega pomena za ohranjanje konkurenčne prednosti, denarnega toka, dobičkonosnosti, skladnosti z zakonodajo in poslovno podobo.

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

Organizacije ter njihovi informacijski sistemi in omrežja se soočajo z varnostnimi grožnjami iz širokega spektra virov, vključno z računalniško podprtimi prevarami, vohunstvom, sabotažami, vandalizmom, požari ali poplavami. Vzroki za poškodbe, kot so zlonamerne kode, računalniško vlamljanje in napadi za zavrnitev storitve, so postali pogostejši, ambicioznejši ter vse bolj prefinjeni.

Informacijska varnost je pomembna tako za javni kot za zasebni poslovni sektor ter za varovanje kritične infrastrukture. V obeh sektorjih bo informacijska varnost delovala kot dejavnik, ki omogoča na primer doseči e-upravo ali e-poslovanje, ter preprečuje ali zmanjšuje tveganja. Povezovanje javnih in zasebnih omrežij ter skupna raba informacijskih virov povečujeta težave pri doseganju nadzora dostopa. Trend porazdeljenega računalništva je tudi oslabil uspešnost osrednje, specializirane kontrole.

Mnogi informacijski sistemi niso bili zasnovani kot varni. Varovanje, ki ga je mogoče doseči s tehničnimi sredstvi, je omejeno ter naj bi bilo podprto z ustreznim upravljanjem in postopki. Prepoznavanje ustrezne kontrole naj se skrbno načrtuje in osredotoča na podrobnosti. Upravljanje Informacijske varnosti najmanj zahteva sodelovanje vseh zaposlenih v organizaciji. Prav tako lahko zahteva udeležbo delničarjev, dobaviteljev, tretjih oseb, odjemalcev ali drugih zunanjih strank. Potrebni so lahko tudi strokovni nasveti zunanjih organizacij.

0.3 Kako vzpostaviti varnostne zahteve

Bistveno je, da organizacija prepozna svoje varnostne zahteve. Obstajajo trije glavni viri varnostnih zahtev.

1. En vir je izpeljan iz ocenjevanja tveganj organizacije ob upoštevanju celovite poslovne organizacijske strategije in ciljev. Z oceno tveganja se prepoznajo grožnje dobrinam, ovrednotijo se ranljivost in verjetnost pojava ter ocenijo se potencialni vplivi.
2. Drug vir so pravne, zakonske in regulativne zahteve, ki jih morajo izpolniti organizacija, njeni poslovni partnerji, izvajalci in ponudniki storitev, ter njihovo družbeno-kulturno okolje.
3. Dodatni vir je še poseben niz načel, ciljev in poslovnih zahtev za obdelave informacij, ki jih je organizacija razvila v podporo svojega poslovanja.

0.4 Ocenjevanje varnostnih tveganj

Varnostne zahteve se prepoznajo z metodičnim ocenjevanjem varnostnih tveganj. Izdatke za kontrole je treba uravnotežiti glede na poslovno škodo, ki navadno izhaja iz napak pri varovanju.

Rezultati ocenjevanja tveganja bodo pomagali voditi in določiti ustrezne ukrepe vodstva in prednostne naloge za obvladovanje informacijskih varnostnih tveganj ter za izvajanje kontrol, izbranih za varovanje pred temi tveganji.

Ocenjevanje tveganja naj se redno ponavlja in obravnava vse spremembe, ki lahko vplivajo na rezultate ocenjevanja tveganja.

iTeh STANDARD PREVIEW

Več informacij o ocenjevanju varnostnih tveganj je mogoče najti v točki 4.1 Ocenjevanje varnostnih tveganj.

(standards.iteh.ai)

0.5 Izbiranje kontrol

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8affbc37/sist-iso-iec-27002-2008

Ko so varnostne zahteve in tveganja prepoznani in so sprejete odločitve za obravnavanje tveganj, naj se izberejo in izvajajo ustrezne kontrole, da se tveganja zmanjšajo na sprejemljivo raven. Kontrole je mogoče izbrati iz tega standarda ali drugih nizov ukrepov, lahko pa se zasnujejo tudi nove kontrole za zadovoljitev posebnih potreb. Izbor varnostnih ukrepov je odvisen od organizacijskih odločitev, ki temeljijo na kriterijih za sprejem tveganja, možnostih obravnavanja tveganja ter na splošnem pristopu k upravljanju tveganja, ki ga uporablja organizacija, ter naj ustreza vsem ustreznim nacionalnim in mednarodnim zakonodajam in predpisom.

Nekatere kontrole v tem standardu je mogoče obravnavati kot vodilna načela za upravljanje informacijske varnosti in ustrezajo večini organizacij. Podrobneje so pojasnjene v nadaljevanju pod naslovom "Izhodišče informacijske varnosti".

Več informacij o izbiranju kontrol in drugih možnostih obravnavanja tveganja je mogoče najti v točki 4.2 Obravnavanje varnostnih tveganj.

0.6 Izhodišče informacijske varnosti

Število kontrol je mogoče obravnavati kot dobro izhodišče za izvajanje informacijske varnosti. Kontrole temeljijo na bistvenih zakonodajnih zahtevah ali pa so del splošne prakse za informacijsko varnost.

Kontrole, ki naj bi bile bistvene za organizacijo z zakonodajnega vidika, vključujejo glede na ustrezno zakonodajo:

a) varovanje podatkov in zasebnost osebnih podatkov (glej 15.1.4),

b) zaščito organizacijskih zapisov (glej 15.1.3),

c) pravice intelektualne lastnine (glej 15.1.2).

Kontrole, sprejete kot splošna praksa za informacijsko varnost, vključujejo:

a) dokument o informacijski varnostni politiki (glej 5.1.1),

b) dodelitev odgovornosti za informacijsko varnost (glej 6.1.3),

c) ozaveščenost o informacijski varnosti, izobraževanje in usposabljanje (glej 8.2.2),

d) pravilno obdelavo v aplikacijah (glej 12.2),

e) tehnično upravljanje ranljivosti (glej 12.6),

f) upravljanje neprekinjenega poslovanja (glej 14),

g) upravljanje incidentov informacijske varnosti in izboljšave (glej 13.2).

Te kontrole ustrezajo večini organizacij in večini okolij.

Naj velja opozorilo, da čeprav so vsi ukrepi v tem standardu pomembni in naj se upoštevajo, naj se določi primernost vsake kontrole v luči specifičnih tveganj, s katerimi se organizacija sooča. Zato je gornji pristop lahko dobro izhodišče, ampak ne nadomešča izbire kontrol na podlagi ocenjevanja tveganja.

0.7 Ključni dejavniki uspeha

Izkušnje so pokazale, da so naslednji dejavniki pogosto ključnega pomena za uspešno izvajanje informacijske varnosti v organizaciji:

a) informacijska varnostna politika, cilji in aktivnosti, ki odražajo poslovne cilje,

b) pristop in okvir za izvajanje, vzdrževanje, spremljanje in izboljševanje informacijske varnosti, ki je v skladu z organizacijsko kulturo,

c) vidna podpora in zavezanost na vseh ravneh vodstva,

d) dobro razumevanje zahtev informacijske varnosti, ocenjevanja in obvladovanja tveganja,

e) uspešno trženje informacijske varnosti vsem vodjem, zaposlenim in drugim strankam za doseganje ozaveščenosti,

f) razdeljevanje napotkov o politiki in standardih informacijske varnosti vsem vodjem, zaposlenim in drugim strankam,

g) zagotavljanje financiranja dejavnosti upravljanja informacijske varnosti,

h) zagotavljanje ustreznega ozaveščanja, usposabljanja in izobraževanja,

i) vzpostavitev uspešnega procesa upravljanja informacijskih varnostnih incidentov,

j) izvajanje sistema merjenja[1], ki se uporablja za vrednotenje delovanja upravljanja informacijske varnosti in daje povratne predloge za izboljšanje,

k) upravljanje informacijske varnosti in povratne informacije predlogov za izboljšave.

0.8 Razvijanje lastnih smernic

Ta pravila obnašanja je mogoče upoštevati kot izhodišče za razvoj posebnih smernic organizacije. Vse kontrole in smernice iz teh pravil obnašanja morda niso primerne. Poleg tega so lahko potrebne dodatne kontrole in smernice, ki niso vključene v ta standard. Ko bodo razviti dokumenti z dodatnimi kontrolami ali smernicami, je morda koristno vključiti sklice na točke v tem standardu, kjer je to primerno, kar bo olajšalo preverjanje skladnosti presojevalcem in poslovnim partnerjem.

[1] Upoštevajte, da merjenja informacijske varnosti niso vključena v področje uporabe tega standarda.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70b08a1bc37/sist-iso-iec-27002-2008

Informacijska tehnologija – Varnostne tehnike – Pravila obnašanja pri upravljanju informacijske varnosti

1 Področje uporabe

Ta mednarodni standard določa smernice in splošna načela za začetek, izvajanje, vzdrževanje in izboljševanje upravljanja informacijske varnosti v organizaciji. Cilji, opisani v tem mednarodnem standardu, so zagotoviti glavne smernice splošno uveljavljenih ciljev upravljanja informacijske varnosti.

Cilji kontrol in kontrole tega mednarodnega standarda naj bi se izvedli za izpolnitev zahtev, ki so bile prepoznane z ocenjevanjem tveganja. Ta mednarodni standard lahko služi kot praktična smernica za razvoj organizacijskih varnostnih standardov in praks uspešnega upravljanja varnosti ter kot pomoč pri gradnji zaupanja v medorganizacijskih aktivnostih.

2 Izrazi in definicije

V tem dokumentu so uporabljeni naslednji izrazi in definicije.

2.1
dobrina
kar koli, kar ima vrednost za organizacijo

[ISO/IEC 13335-1:2004]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.2
kontrola
načini obvladovanja tveganja, vključno s politikami, postopki, smernicami, praksami ali organizacijskimi strukturami, ki so po naravi lahko upravni, tehnični, upravljalni ali pravni

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f880af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

OPOMBA: Kontrola se uporablja tudi kot sopomenka za ukrep ali protiukrep.

2.3
smernica
opis, ki pojasnjuje, kaj naj se stori in kako, da se dosežejo cilji, določeni v politikah

[ISO/IEC 13335-1:2004]

2.4
naprave za obdelavo informacij
kakršen koli sistem, storitev ali infrastruktura za obdelavo informacij ali fizične lokacije, kjer se le-ta nahaja

2.5
informacijska varnost
ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij, dodatno so lahko vključene tudi druge lastnosti, kot so verodostojnost, odgovornost, nezanikanje in zanesljivost

2.6
informacijski varnostni dogodek
Informacijski varnostni dogodek je prepoznano dogajanje v sistemu, storitvi ali omrežju, ki kaže na morebitno kršitev informacijske varnosti, politike ali odpoved zaščitnih ukrepov ali na do tedaj še neznano okoliščino, ki je lahko pomembna za varnost

[ISO/IEC TR 18044:2004]

2.7
informacijski varnostni incident
informacijski varnostni incident je določen z enim ali več neželenimi ali nepričakovanimi informacijskimi varnostnimi dogodki, ki predstavljajo veliko verjetnost ogrožanja poslovanja in informacijske varnosti

[ISO/IEC TR 18044:2004]

2.8
politika
celovit namen in usmeritev, kot ju formalno izrazi vodstvo

2.9
tveganje
kombinacija verjetnosti dogodka in njegove posledice

[ISO/IEC Vodilo 73:2002]

2.10
analiza tveganja
sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja

[ISO/IEC Vodilo 73:2002]

2.11
ocenjevanje tveganja
celovit proces analize tveganja in vrednotenja tveganja

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC Vodilo 73:2002]

SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

2.12
vrednotenje tveganja
proces primerjave ocenjenega tveganja s kriteriji tveganja, da se določi pomembnost tveganja

[ISO/IEC Vodilo 73:2002]

2.13
obvladovanje tveganja
usklajene aktivnosti organizacije za usmerjanje in nadzor tveganja

OPOMBA: Obvladovanje tveganja na splošno vključuje ocenjevanje tveganja, obravnavanje tveganja, sprejetje tveganja in obveščanje o tveganju.

[ISO/IEC Vodilo 73:2002]

2.14
obravnavanje tveganja
postopek izbire in izvedbe ukrepov za spremembo tveganja

[ISO/IEC Vodilo 73:2002]

2.15
tretja stranka
oseba ali organ, ki je glede na zadevno vprašanje priznan kot neodvisen od vpletenih strani

[ISO/IEC Vodilo 2:1996]

2.16
grožnja
možen vzrok neželenega incidenta, ki lahko povzroči škodo sistemu ali organizaciji

[ISO/IEC 13335-1:2004]

2.17
ranljivost
slabost dobrine ali skupine dobrin, ki jo lahko izkoristi ena ali več groženj

[ISO/IEC 13335-1:2004]

3 Struktura tega standarda

Ta standard vsebuje 11 točk o varnostnih kontrolah, ki skupaj tvorijo 39 glavnih varnostnih kategorij, in uvodno poglavje, ki predstavlja ocenjevanje in obravnavanje tveganja.

3.1 Točke

Vsaka točka vsebuje več glavnih varnostnih kategorij. Enajst točk (opremljenih s številom glavnih varnostnih kategorij, vključenih v posamezni točki) je:

a) Varnostna politika (1),
b) Organiziranje informacijske varnosti (2),
c) Upravljanje dobrin (2),
d) Varnost človeških virov (3),
e) Fizična in okoljska varnost (2),
f) Upravljanje komunikacij in delovanja (10),
g) Nadzor dostopa (7),
h) Pridobivanje, razvoj in vzdrževanje informacijskih sistemov (6),
i) Upravljanje informacijskih varnostnih incidentov (2),
j) Upravljanje neprekinjenega poslovanja (1),
k) Skladnost (3).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27002:2008
https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008

OPOMBA: Vrstni red točk v tem standardu ne nakazuje njihove pomembnosti. Vse točke so lahko pomembne, odvisno od okoliščin, zato naj vsaka organizacija, ki uporablja ta standard, določi, kako pomembne so in njihovo uporabo v posameznih poslovnih procesih. Prav tako tudi noben seznam v tem standardu ni zapisan v prednostnem vrstnem redu, razen, če je tako navedeno.

3.2 Glavne varnostne kategorije

Vsaka glavna varnostna kategorija vsebuje:

a) cilj kontrole, ki navaja, kaj je treba doseči, ter
b) eno ali več kontrol, ki jih je mogoče uporabiti za doseganje cilja kontrole.

Opisi kontrole so strukturirani na naslednji način:

Kontrola
Določa specifične kontrolne izjave za izpolnitev cilja kontrole.