SLOVENSKI STANDARD

SIST ISO/IEC 27000

marec 2011

Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje

Information technology – Security techniques – Information security management systems - Overview and vocabulary

Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire

ICS 01.140.35, 35.040

Referenčna oznaka
SIST ISO/IEC 27000:2011 (sl)

Nadaljevanje na straneh od 2 do 25

NACIONALNI UVOD

Standard SIST ISO/IEC 27000 (sl), Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje, 2011, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27000 (en), Information technology – Security techniques – Information security management systems – Overview and vocabulary, prva izdaja, 2009-05-01.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27000:2009 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 27000:2011 je prevod mednarodnega standarda ISO/IEC 27000:2009. Slovensko izdajo standarda SIST ISO/IEC 27000:2011 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 18. novembra 2010 sprejel SIST/TC ITC Informacijska tehnologija.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27000:2009

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27000:2011 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

– Definicije pojmov so povzete po mednarodnih standardih ISO 9000, Sistemi vodenja kakovosti – Osnove in slovar, in ISO Guide 73, Risk management – Vocabulary.

– V besedilu SIST ISO/IEC 27000 so v točkah 0.2, 4.1, 4.2, 4.3, 4.4, 4.5 in v dodatku navedeni mednarodni standardi ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27011 in ISO 27799. Pri tem je vedno mišljena njihova zadnja izdaja.

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 27000 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

0 Uvod

0.1 Pregled

Mednarodni standardi za sisteme upravljanja zagotavljajo model za ravnanje pri vzpostavljanju in delovanju sistema upravljanja. Ta model vključuje značilnosti, za katere so strokovnjaki s tega področja dosegli soglasje, da je to mednarodno doseženo stanje tehnike. V okviru ISO/IEC JTC 1 SC 27 deluje strokovna komisija, namenjena razvoju mednarodnih standardov za sisteme upravljanja informacijske varnosti, sicer poznanih kot skupina standardov Sistem upravljanja informacijske varnosti – SUIV.

Z uporabo skupine standardov SUIV lahko organizacije razvijejo in ustvarijo okvir za upravljanje varnosti svojih informacij ter se pripravijo na neodvisno oceno svojega SUIV, ki ga uporabljajo za zaščito podatkov, kot so na primer finančni podatki, podatki o intelektualni lastnini in podrobnosti o zaposlenih ali informacije, ki jim jih zaupajo njihove stranke ali tretje osebe.

0.2 Skupina standardov SUIV

Namen skupine standardov SUIV[1] je pomagati organizacijam vseh vrst in velikosti pri izvedbi in delovanju SUIV. Skupino standardov SUIV sestavljajo naslednji mednarodni standardi pod skupnim naslovom Informacijska tehnologija – Varnostne tehnike:

- ISO/IEC 27000:2009, *Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje*
- ISO/IEC 27001:2005, *Sistemi upravljanja informacijske varnosti – Zahteve*
- *ISO/IEC 27002:2005, Pravila obnašanja pri upravljanju informacijske varnosti*
- *ISO/IEC 27003, Smernice za izvedbo sistema upravljanja informacijske varnosti*
- *ISO/IEC 27004, Upravljanje informacijske varnosti – Merjenje*
- *ISO/IEC 27005:2008, Obvladovanje tveganj informacijske varnosti*
- *ISO/IEC 27006:2007, Zahteve za organe, ki izvajajo presoje in certificiranje sistemov upravljanja informacijske varnosti*
- ISO/IEC 27007, *Smernice za presojo sistemov upravljanja informacijske varnosti*
- ISO/IEC 27011, *Smernice za upravljanje informacijske varnosti telekomunikacijskih organizacij, zasnovane na ISO/IEC 27002*

OPOMBA: Splošni naslov *"Informacijska tehnologija – Varnostne tehnike"* kaže, da je te standarde pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT*.

Mednarodni standard, ki ni naslovljen z istim splošnim naslovom, a je prav tako del skupine standardov SUIV, je:

- ISO 27799:2008, *Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002*

0.3 Namen tega mednarodnega standarda

Ta mednarodni standard daje pregled sistemov upravljanja informacijske varnosti, ki so predmet skupine standardov SUIV, in določa s tem povezane izraze.

OPOMBA: Dodatek A pojasnjuje uporabo izrazov za izražanje zahtev in/ali navodil v skupini standardov SUIV.

Skupina standardov SUIV vključuje standarde, ki:

a) določajo zahteve za SUIV in za tiste, ki certificirajo takšne sisteme,

[1] Standardi, navedeni v tej podtočki brez letnice objave, so še v razvoju.

b) zagotavljajo neposredno podporo, podrobna navodila in/ali razlage za celotne procese in zahteve postopka »načrtuj-izvedi-preveri-ukrepaj« (PDCA),

c) se nanašajo na smernice za SUIV, specifične za posamezne sektorje,

d) se nanašajo na ugotavljanje skladnosti za SUIV.

Izrazi in definicije, navedeni v tem mednarodnem standardu:

- obsegajo izraze in definicije, pogosto uporabljene v skupini standardov SUIV,
- ne bodo zajeli vseh izrazov in definicij, ki se uporabljajo v skupini standardov SUIV, in
- ne omejujejo skupine standardov SUIV pri opredeljevanju pogojev za lastno uporabo.

Standardi, ki obravnavajo le izvedbo kontrol, namesto da bi obravnavali vse kontrole, so izključeni iz skupine standardov SUIV.

Da bi ta mednarodni standard odražal spreminjajoči se status skupine standardov SUIV, je pričakovati, da se bo posodabljal nenehno in pogosteje, kot to ponavadi velja za druge standarde ISO/IEC.

Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje

1 Področje uporabe

Ta mednarodni standard navaja:

a) pregled skupine standardov SUIV,

b) uvod v sisteme upravljanja informacijske varnosti (SUIV),

c) kratek opis procesa načrtuj-izvedi-preveri-ukrepaj (PDCA) ter

d) izraze in definicije za uporabo v skupini standardov SUIV.

Ta mednarodni standard je uporaben za vse vrste organizacij (npr. gospodarske družbe, državne organe, nepridobitne organizacije).

2 Izrazi in definicije

V tem dokumenta so uporabljeni naslednji izrazi in definicije.

OPOMBA: Izraz v definiciji ali opombi, ki je opredeljen drugje v tej točki, je zapisan s krepko pisavo in mu sledi njegovo številčenje v oklepaju. Tak krepko označen izraz v definiciji se lahko nadomesti z njegovo celotno definicijo.

Na primer:

napad (2.4) je opredeljen kot "poskus uničiti, izpostaviti, spremeniti, onemogočiti, ukrasti ali pridobiti nepooblaščen dostop do **dobrine** ali nepooblaščena uporaba te **dobrine** (2.3)".

dobrina je opredeljena kot "kar koli, kar ima vrednost za organizacijo".

Če se izraz **"dobrina"** nadomesti s svojo definicijo:

napad potem postane "poskus uničiti, izpostaviti, spremeniti, onemogočiti, ukrasti ali pridobiti nepooblaščen dostop do česar koli, kar ima vrednost za organizacijo, ali nepooblaščena uporaba česar koli, kar ima vrednost za organizacijo ".

2.1
nadzor dostopa
pomeni zagotovitev, da je dostop do **dobrin** (2.3) pooblaščen in omejen na podlagi poslovnih in varnostnih zahtev

2.2
odgovornost
odgovornost subjekta za njegova dejanja in odločitve

2.3
dobrina
kar koli, kar ima vrednost za organizacijo

OPOMBA: Obstaja več vrst dobrin, vključno z:

a) **informacijo** (2.18),

b) programsko opremo, kot je računalniški program,

c) fizičnimi sredstvi, kot je računalnik,

d) storitvami,

e) osebjem in njegovimi kvalifikacijami, veščinami in izkušnjami ter

f) neopredmetenimi dobrinami, kot sta ugled in javna podoba.

2.4
napad
poskus uničiti, izpostaviti, spremeniti, onemogočiti, ukrasti ali pridobiti nepooblaščen dostop do dobrine ali nepooblaščena uporaba te **dobrine** (2.3)

2.5
overjanje
priskrba zagotovila, da je zatrjevana lastnost subjekta prava

2.6
verodostojnost
lastnost, da je subjekt to, kar trdi, da je

2.7
razpoložljivost
lastnost, da je nekaj na zahtevo pooblaščenega subjekta dostopno in uporabno

2.8
neprekinjeno poslovanje
procesi (2.31) in/ali **postopki** (2.30) za zagotavljanje neprekinjenih poslovnih dejavnosti

2.9
zaupnost
lastnost, da informacija ni na voljo ali razkrita nepooblaščenim posameznikom, subjektom ali **procesom** (2.31)

2.10
kontrola
načini obvladovanja **tveganja** (2.34), vključno s **politikami** (2.28), **postopki** (2.30), **smernicami** (2.16), praksami ali organizacijskimi strukturami, ki so po naravi lahko upravni, tehnični, upravljalni ali pravni

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

2.11
cilj kontrole
izjava, ki opisuje, kaj bo doseženo kot rezultat izvajanja **kontrol** (2.10)

2.12
korektivni ukrep[1)]
ukrep za odpravo vzroka ugotovljene neskladnosti ali druge neželene situacije

[ISO 9000:2005]

2.13
uspešnost
obseg, v katerem so planirane aktivnosti realizirane in planirani rezultati doseženi

[ISO 9000:2005]

2.14
učinkovitost
razmerje med doseženimi rezultati in sredstvi, ki so bili zanje porabljeni

1) Opomba SI: V skupini standardov SUIV se uporablja tudi izraz popravni ukrep.

2.15
dogodek
nastop določenega niza okoliščin

[ISO/IEC Guide 73:2002]

2.16
smernica
priporočilo, kaj se pričakuje, da je treba storiti za dosego cilja

2.17
vpliv
sprememba, neugodna za raven doseženih poslovnih ciljev

2.18
informacija
znanje ali podatek, ki ima vrednost za organizacijo

2.19
informacijska varnost
ohranjanje **zaupnosti** (2.9), **celovitosti** (2.25) in **razpoložljivosti** (2.7) informacije

OPOMBA: Poleg tega so lahko vključene tudi druge lastnosti, kot so **verodostojnost** (2.6), **odgovornost** (2.2), **nezanikanje** (2.27) in **zanesljivost** (2.33).

2.20
informacijski varnostni dogodek
prepoznano dogajanje v sistemu, storitvi ali omrežju, ki kaže na morebitno kršitev **informacijske varnosti** (2.19), **politike** (2.28) ali odpovedi **kontrol** (2.10) ali na do tedaj še neznano okoliščino, ki je lahko pomembna za varnost

2.21
informacijski varnostni incident
eden ali več neželenih ali nepričakovanih **informacijskih varnostnih dogodkov** (2.20), ki predstavljajo veliko verjetnost ogrožanja poslovnih dejavnosti in **informacijske varnosti** (2.19)

2.22
upravljanje informacijskih varnostnih incidentov
procesi (2.31) za odkrivanje, poročanje in ocenjevanje **informacijskih varnostnih incidentov** (2.21) ter za odzivanje nanje, ukvarjanje z njimi in učenje iz njih

2.23
sistem upravljanja informacijske varnosti
SUIV
del celotnega **sistema upravljanja** (2.26), ki temelji na pristopu poslovnega tveganja in je namenjen vzpostavitvi, izvedbi, delovanju, spremljanju, pregledovanju, vzdrževanju in izboljševanju **informacijske varnosti** (2.19)

2.24
informacijsko varnostno tveganje
možnost, da bo **grožnja** (2.45) izkoristila **ranljivost** (2.46) **dobrine** (2.3) ali skupine dobrin in s tem škodila organizaciji

2.25
celovitost
lastnost varovanja točnosti in celovitosti **dobrin** (2.3)

2.26
sistem upravljanja
ogrodje **politik** (2.28), **postopkov** (2.30), **smernic** (2.16) in z njimi povezanih virov za doseganje ciljev organizacije

2.27
nezanikanje
sposobnost dokazati, da je določeni subjekt izvedel zahtevani **dogodek** (2.15) ali dejanje, zaradi razrešitve spora glede izvedbe ali neizvedbe **dogodka** (2.15) oziroma dejanja ter vključenosti subjekta v **dogodek** (2.15).

2.28
politika
celota namena in usmeritev, kot jih je uradno izrazilo vodstvo

2.29
preventivni ukrep[1)]
ukrep za odpravo vzroka potencialne neskladnosti ali druge potencialne neželene situacije

[ISO 9000:2005]

2.30
postopek
specificiran način za izvedbo aktivnosti ali **procesa** (2.31)

[ISO 9000:2005]

2.31
proces
skupek med seboj povezanih ali medsebojno vplivajočih aktivnosti, ki pretvarja vhode v izhode

[ISO 9000:2005]

2.32
zapis
dokument, ki navaja dosežene rezultate ali podaja dokaz o izvedenih aktivnostih

[ISO 9000:2005]

2.33
zanesljivost
čvrsto predvideno ravnanje in učinki

2.34
tveganje
kombinacija verjetnosti **dogodka** (2.15) in njegove posledice

[ISO/IEC Guide 73:2002]

2.35
sprejetje tveganja
odločitev, da se **tveganje** (2.34) sprejme

[ISO/IEC Guide 73:2002]

[1)] Opomba SI: V skupini standardov SUIV se uporablja tudi izraz preprečevalni ukrep.

2.36
analiza tveganja
sistematična uporaba informacij za prepoznavanje virov in ocenjevanje **tveganja** (2.34)

[ISO/IEC Guide 73:2002]

OPOMBA: Analiza tveganja je podlaga za **vrednotenje tveganja** (2.41), **obravnavo tveganja** (2.43) in **sprejetje tveganja** (2.35).

2.37
ocenjevanje tveganja
celovit proces (2.31) **analize tveganja** (2.36) in **vrednotenja tveganja** (2.41)

[ISO/IEC Guide 73:2002]

2.38
obveščanje o tveganju
izmenjava ali razpošiljanje informacije o **tveganju** (2.34) med odločevalci in drugimi deležniki

[ISO/IEC Guide 73:2002]

2.39
kriterij tveganja
formalni pogoji, po katerih se ocenjuje pomembnost **tveganja** (2.34)

[ISO/IEC Guide 73:2002]

2.40
ocena tveganja
povezovanje vrednosti z verjetnostjo in posledicami **tveganja** (2.34)

[ISO/IEC Guide 73:2002]

2.41
vrednotenje tveganja
proces (2.31), s katerim se ocenjeno **tveganje** (2.34) primerja s **kriterijem tveganja** (2.39), da se določi pomembnost **tveganja** (2.34)

[ISO/IEC Guide 73:2002]

2.42
obvladovanje tveganja
usklajene aktivnosti organizacije za usmerjanje in nadzor **tveganja** (2.34)

[ISO/IEC Guide 73:2002]

OPOMBA: Obvladovanje tveganja na splošno vključuje **ocenjevanje tveganja** (2.37), **obravnavanje tveganja** (2.43), **sprejetje tveganja** (2.35), **obveščanje o tveganju** (2.38), spremljanje tveganja in proučitev tveganja.

2.43
obravnavanje tveganja
proces (2.31) izbire in izvedbe ukrepov za spremembo **tveganja** (2.34)

[ISO/IEC Guide 73:2002]