SLOVENSKI STANDARD

SIST ISO/IEC 27005

september 2011

Informacijska tehnologija – Varnostne tehnike – Obvladovanje informacijskih varnostnih tveganj

Information technology – Security techniques – Information security risk management

Technologies de l'information – Techniques de sécurité – Management du risque de la sécurité de l'information

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27005:2011 (sl)

Nadaljevanje na straneh 2 do 73

NACIONALNI UVOD

Standard SIST ISO/IEC 27005 (sl), Informacijska tehnologija – Varnostne tehnike – Obvladovanje informacijskih varnostnih tveganj, 2011, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27005 (en), Information technology – Security techniques – Information security risk, 2011-06.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27005:2011 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 27005:2011 je prevod mednarodnega standarda ISO/IEC 27005:2011. Slovenski standard SIST ISO/IEC 27005:2011 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 2. junija 2011 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

S privzemom tega evropskega standarda veljajo za omejeni namen referenčnih standardov vsi standardi, navedeni v izvirniku, razen tistih, ki so že sprejeti v nacionalno standardizacijo:

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

SIST ISO/IEC 27001:2005 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve *(zamenjan s SIST ISO/IEC 27001:2013)*

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27005:2011

OPOMBI

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27005:2011 to pomeni “slovenski standard”.

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 27005 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 27005:2008), ki je bila tehnično revidirana.

Uvod

Ta mednarodni standard zagotavlja smernice za obvladovanje informacijskih varnostnih tveganj v organizaciji, pri čemer še zlasti podpira zahteve za upravljanje informacijske varnosti (SUIV) glede na ISO/IEC 27001. Vendar pa ta mednarodni standard ne daje nobene posebne metode za obvladovanje informacijskih varnostnih tveganj. Organizacija sama mora opredeliti svoj pristop k obvladovanju tveganj, odvisno, na primer, od obsega SUIV, konteksta obvladovanja tveganja ali industrijske panoge. V okviru, ki je opisan v tem mednarodnem standardu za izvedbo zahtev SUIV, je mogoče uporabiti številne obstoječe metodologije.

Ta mednarodni standard je pomemben za vodje in zaposlene, ki delujejo na področju obvladovanja informacijskih varnostnih tveganj v organizaciji, in kadar je to primerno, tudi za zunanje stranke, ki podpirajo takšne dejavnosti.

Informacijska tehnologija – Varnostne tehnike – Obvladovanje informacijskih varnostnih tveganj

1 Področje uporabe

Ta mednarodni standard zagotavlja smernice za obvladovanje informacijskih varnostnih tveganj.

Ta mednarodni standard podpira splošne koncepte, določene v ISO/IEC 27001, in je namenjen kot pomoč pri zadovoljivem izvajanju informacijske varnosti, ki temelji na pristopu obvladovanja tveganj.

Poznavanje konceptov, modelov, procesov in terminologij, opisanih v ISO/IEC 27001 in ISO/IEC 27002, je pomembno za popolno razumevanje tega mednarodnega standarda.

Ta mednarodni standard se uporablja za vse vrste organizacij (npr. trgovska podjetja, vladne agencije, nepridobitne organizacije), ki nameravajo obvladovati tveganja, ki bi lahko ogrozila informacijsko varnost organizacije.

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 27000 Informacijska tehnologija – Varnostne tehnike – Sistemi za upravljanje informacijske varnosti – Pregled in izrazoslovje

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

3 Izrazi in definicije

V tem dokumentu so uporabljeni izrazi in definicije, podani v ISO/IEC 27000, ter naslednji:

OPOMBA: Razlike v definicijah, podanih v ISO/IEC 27005:2008 in v tem mednarodnem standardu, so prikazane v dodatku G.

3.1
posledica
izid **dogodka** (3.3), ki vpliva na cilje

[ISO Vodilo 73:2009]

OPOMBA 1: Dogodek lahko povzroči vrsto posledic.

OPOMBA 2: Posledica je lahko določena ali nedoločena in v kontekstu informacijske varnosti je po navadi negativna.

OPOMBA 3: Posledice se lahko izražajo kakovostno ali količinsko.

OPOMBA 4: Začetne posledice se lahko stopnjujejo z učinkom verižne reakcije.

3.2
kontrola
ukrep, ki spreminja **tveganje** (3.9)

[ISO Vodilo 73:2009]

OPOMBA 1: Kontrole za informacijsko varnost vključujejo vsak proces, politiko, postopek, smernico, prakso ali organizacijsko strukturo, ki so lahko upravne, tehnične, upravljavske ali pravne narave, ki spreminja informacijsko varnostno tveganje.

OPOMBA 2: Kontrole ne uveljavljajo vedno predvidenega ali nameravanega učinka spremembe.

OPOMBA 3: Kontrola se uporablja tudi kot sopomenka za zaščito ali protiukrep.

3.3
dogodek
pojav ali sprememba posameznega niza okoliščin

[ISO Vodilo 73:2009]

OPOMBA 1: Dogodek je lahko en ali več pojavov in ima lahko več vzrokov.

OPOMBA 2: Dogodek je lahko sestavljen tudi iz nečesa, kar se ne dogaja.

OPOMBA 3: Dogodek je lahko včasih poimenovan "incident" ali "nesreča".

3.4
zunanji kontekst
zunanje okolje, v katerem organizacija poskuša doseči svoje cilje

[ISO Vodilo 73:2009]

OPOMBA: Zunanji kontekst lahko vključuje:

- kulturno, socialno, politično, zakonodajno, regulativno, finančno, tehnološko, ekonomsko, naravno in konkurenčno okolje, bodisi mednarodno, nacionalno, regionalno ali lokalno,
- ključne dejavnike in trende, ki vplivajo na cilje organizacije, in
- odnose z zunanjimi deležniki ter njihova dojemanja in vrednote.

3.5
notranji kontekst
notranje okolje, v katerem organizacija poskuša doseči svoje cilje

[ISO Vodilo 73:2009]

OPOMBA: Notranji kontekst lahko vključuje:

- upravljanje, organizacijsko strukturo, vloge in odgovornosti,
- politike in cilje ter strategije, vzpostavljene za njihovo doseganje,
- zmogljivosti, razumljene v pomenu virov in znanja (npr. kapital, čas, ljudje, procesi, sistemi in tehnologije),
- informacijske sisteme, informacijske tokove in procese odločanja (tako formalne kot neformalne),
- odnose z notranjimi deležniki ter njihova dojemanja in vrednote,
- kulturo organizacije,
- standarde, smernice in modele, ki jih je sprejela organizacija, ter
- obliko in obseg pogodbenih razmerij.

3.6
raven tveganja
velikost **tveganja** (3.9), izražena v kombinaciji **posledic** (3.1) in njihove **verjetnosti** (3.7)

[ISO Vodilo 73:2009]

3.7
verjetnost
možnost, da se nekaj dogaja

[ISO Vodilo 73:2009]

OPOMBA 1: V terminologiji obvladovanja tveganja se beseda "verjetnost" uporablja za sklicevanje na možnost, da se nekaj dogaja, bodisi določeno, merjeno ali opredeljeno objektivno ali subjektivno, kakovostno ali količinsko, in opisano z uporabo splošnih izrazov ali matematično (kot je verjetnost ali pogostost v določenem časovnem obdobju).

OPOMBA 2: Angleški izraz "likelihood" v nekaterih jezikih nima neposrednega enakovrednega izraza, ampak se pogosto uporablja ekvivalent izraza "probability". Vendar pa se v angleškem jeziku "probability" pogosto razlaga restriktivno

kot matematični izraz. Zato se v terminologiji obvladovanja tveganja "likelihood" uporablja z namenom, da naj bi to imelo enako široko razlago, kot jo ima izraz "probability" v številnih drugih jezikih razen v angleščini.

3.8
preostalo tveganje
tveganje (3.9), ki ostane po **obravnavanju tveganja** (3.17)

[ISO Vodilo 73:2009]

OPOMBA 1: Preostalo tveganje lahko vsebuje neprepoznano tveganje.

OPOMBA 2: Preostalo tveganje je lahko znano tudi kot "zadržano tveganje".

3.9
tveganje
učinek negotovosti na cilje

[ISO Vodilo 73:2009]

OPOMBA 1: Učinek je odstopanje od pričakovanega – pozitivno in/ali negativno.

OPOMBA 2: Cilji imajo lahko različne vidike (kot so finančni, v zvezi z zdravjem in varnostjo pri delu, informacijsko varnostjo in okoljskimi cilji) in se lahko uporabljajo na različnih ravneh (kot so strateška raven, raven celotne organizacije ter raven projektov, izdelkov in procesov).

OPOMBA 3: Tveganje je pogosto označeno glede na morebitne **dogodke** (3.3) in **posledice** (3.1) ali kombinacijo le-teh.

OPOMBA 4: Informacijsko varnostno tveganje je pogosto izraženo v pomenu kombinacije posledic informacijskega varnostnega dogodka in povezane **verjetnosti** (3.7) pojava.

OPOMBA 5: Negotovost je stanje, tudi delno, pomanjkanja informacij, ki se nanašajo na razumevanje ali vedenje o dogodku, njegovih posledicah ali verjetnosti.

OPOMBA 6: Informacijsko varnostno tveganje je povezano z možnostjo, da bodo grožnje izkoristile ranljivosti informacijskih dobrin ali skupine informacijskih dobrin in s tem povzročile škodo organizaciji.

3.10
analiza tveganja
proces razumevanja narave tveganja in določitve **ravni tveganja** (3.6)

[ISO Vodilo 73:2009]

OPOMBA 1: Analiza tveganja je podlaga za vrednotenje tveganja in odločitve o obravnavanju tveganja.

OPOMBA 2: Analiza tveganja vključuje oceno tveganja.

3.11
ocenjevanje tveganja
celoten proces **prepoznavanja tveganja** (3.15), **analize tveganja** (3.10) in **vrednotenja tveganja** (3.14)

[ISO Vodilo 73:2009]

3.12
obveščanje o tveganju in posvetovanje
stalni in ponovljivi procesi, ki jih organizacija vodi, da zagotavlja, deli ali pridobiva informacije in da vodi dialog z **deležniki** (3.18) v zvezi z obvladovanjem **tveganja** (3.9)

[ISO Vodilo 73:2009]

OPOMBA 1: Informacije se lahko nanašajo na obstoj, naravo, obliko, verjetnost, pomen, vrednotenje, sprejemljivost in obravnavanje tveganja.

OPOMBA 2: Posvetovanje je dvosmerni proces obveščanja med organizacijo in njenimi deležniki o določenem vprašanju pred odločitvijo ali določitvijo usmeritve o tem vprašanju. Posvetovanje je:

– proces, ki vpliva na odločitev s pomočjo vplivanja in ne z uporabo moči, ter
– vhod za sprejemanje odločitev in ne skupno odločanje.

3.13
kriterij tveganja
področje delovanja, na podlagi katerega se vrednoti pomen **tveganja** (3.9)

[ISO Vodilo 73:2009]

OPOMBA 1: Kriteriji tveganja temeljijo na organizacijskih ciljih ter na zunanjem in notranjem kontekstu.

OPOMBA 2: Kriterije tveganja je mogoče izpeljati iz standardov, zakonov, politik in drugih zahtev.

3.14
vrednotenje tveganja
proces primerjanja rezultatov **analize tveganja** (3.10) s **kriteriji tveganja** (3.13), da se ugotovi, ali sta tveganje in/ali njegova velikost sprejemljiva ali znosna

[ISO Vodilo 73:2009]

OPOMBA: Vrednotenje tveganja pomaga pri odločitvi o obravnavanju tveganja.

3.15
prepoznavanje tveganja
proces iskanja, spoznavanja in opisovanja tveganj

[ISO Vodilo 73:2009]

OPOMBA 1: Prepoznavanje tveganja vključuje prepoznavanje virov tveganja, dogodkov tveganja, njihovih vzrokov in možnih posledic.

OPOMBA 2: Prepoznavanje tveganja lahko vključuje zgodovinske podatke, teoretične analize, mnenja poznavalcev in strokovnjakov ter potrebe deležnikov.

3.16
obvladovanje tveganja
usklajene aktivnosti za usmerjanje in nadzorovanje organizacije v zvezi s tveganjem

[ISO Vodilo 73:2009]

OPOMBA: Ta mednarodni standard uporablja izraz "proces" za opis obvladovanja tveganja v celoti. Elementi v procesu obvladovanja tveganja se imenujejo "aktivnosti".

3.17
obravnavanje tveganja
proces za spremembo tveganja

[ISO Vodilo 73:2009]

OPOMBA 1: Obravnavanje tveganja lahko vključuje:
– preprečevanje tveganja z odločitvijo, da se ne začne ali ne nadaljuje z aktivnostjo, ki povzroča tveganje,
– privzemanje ali povečanje tveganja, da bi se lahko zasledovale priložnosti,
– odstranitev vira tveganja,
– spreminjanje verjetnosti,
– spreminjanje posledic,
– delitev tveganja z drugo stranko ali strankami (vključno s pogodbami in financiranjem tveganj) in
– ohranjanje tveganja na podlagi utemeljene izbire.

OPOMBA 2: Obravnavanja tveganja, ki se ukvarjajo z negativnimi posledicami, se včasih označujejo kot "ublažitev tveganja", "odpravljanje tveganja", "preprečevanje tveganja" in "zmanjšanje tveganja".

OPOMBA 3: Obravnavanje tveganja lahko ustvari nova tveganja ali spreminja obstoječa tveganja.

3.18
deležnik
oseba ali organizacija, ki lahko prizadene, je lahko prizadeta ali meni, da je prizadeta, z določeno odločitvijo ali dejavnostjo

[ISO Vodilo 73:2009]

OPOMBA: Oseba, ki sprejema odločitve, je lahko deležnik.

4 Struktura tega mednarodnega standarda

Ta mednarodni standard vsebuje opis procesov obvladovanja informacijskih varnostnih tveganj in njihovih aktivnosti.

Informacije o ozadju so podane v točki 5.

Splošni pregled postopkov obvladovanja informacijskih varnostnih tveganj je podan v točki 6.

Vse aktivnosti obvladovanja informacijskih varnostnih tveganj, predstavljene v točki 6, so opisane v naslednjih točkah:

- vzpostavljanje konteksta v točki 7,
- ocenjevanje tveganj v točki 8,
- obravnavanje tveganj v točki 9,
- sprejetje tveganj v točki 10,
- obveščanje o tveganjih v točki 11,
- spremljanje in pregled tveganj v točki 12.

Dodatne informacije o aktivnostih obvladovanja informacijskih varnostnih tveganj so predstavljene v dodatkih. Vzpostavljanje konteksta je podprto z dodatkom A (Opredelitev obsega in mej procesov obvladovanja informacijskih varnostnih tveganj). Prepoznavanje in vrednotenje dobrin ter ocenjevanje vplivov so obravnavana v dodatku B. Dodatek C navaja primere tipičnih groženj, v dodatku D pa so obravnavane ranljivosti in metode za ocenjevanje ranljivosti. Primeri pristopov k ocenjevanju informacijskih varnostnih tveganj so predstavljeni v dodatku E.

Omejitve za spremembo tveganj so predstavljene v dodatku F.

Razlike v definicijah med ISO/IEC 27005:2008 in ISO/IEC 27005:2011 so prikazane v dodatku G.

Vse aktivnosti obvladovanja tveganj, kot so prikazane v točkah od 7 do 12, so strukturirane na naslednji način:

Vhodni podatki: Prepoznana je vsaka zahtevana informacija za izvajanje dejavnosti.

Ukrep: Opisana je aktivnost.

Napotki za izvajanje: Dani so napotki za izvajanje ukrepa. Nekateri od teh napotkov morda niso ustrezni v vseh primerih in so lahko primernejši tudi drugi načini izvajanja ukrepa.

Izhodni podatki: Prepoznana je vsaka informacija, pridobljena po izvedeni aktivnosti.

5 Ozadje

Da se prepoznajo organizacijske potrebe glede zahtev informacijske varnosti in da se ustvari učinkovit sistem upravljanja informacijske varnosti (SUIV), je potreben sistematičen pristop k obvladovanju informacijskih varnostnih tveganj. Ta pristop naj bo primeren za okolje organizacije in zlasti naj bo usklajen s celotnim obvladovanjem tveganj podjetja. Prizadevanja za varnost naj obravnavajo tveganja učinkovito in pravočasno, kjerkoli in kadarkoli je potrebno. Obvladovanje informacijskih varnostnih tveganj naj bo sestavni del vseh aktivnosti upravljanja informacijske varnosti in naj se uporablja tako za uvajanje kot za tekoče delovanje SUIV.

Obvladovanje informacijskih varnostnih tveganj naj bo nenehen proces. Proces naj vzpostavi zunanji in notranji kontekst, ocenjuje naj tveganja in naj jih obravnava z uporabo načrta za obravnavanje tveganja za izvedbo priporočil in odločitev. Analize obvladovanja tveganj s stališča, kaj se lahko zgodi in katere so lahko možne posledice, so potrebne pred odločitvijo, kaj naj se stori in kdaj, da se zmanjšajo tveganja na sprejemljivo raven.

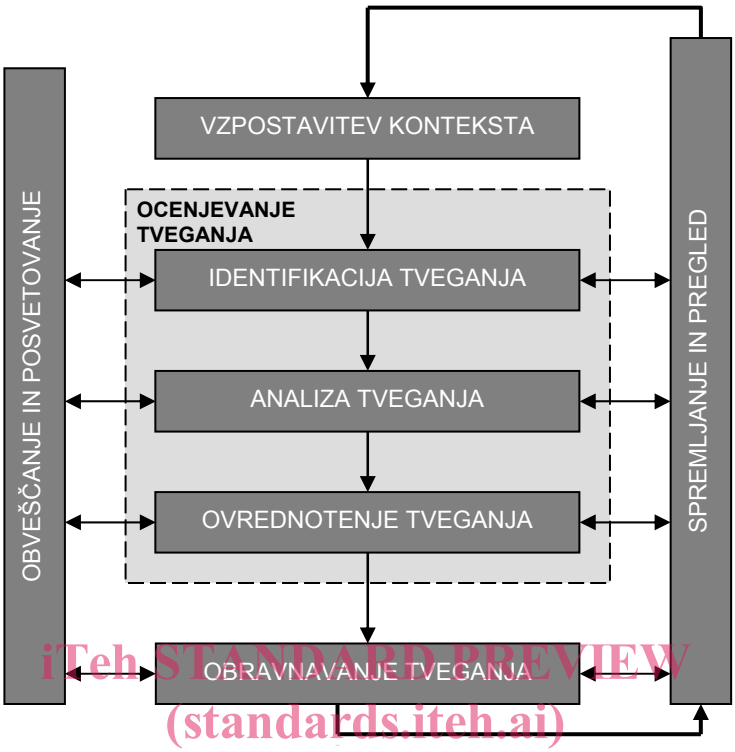
Obvladovanje informacijskih varnostnih tveganj naj prispeva k naslednjemu:

- Tveganja so prepoznana.
- Tveganja so ocenjena glede na njihove posledice na poslovanje in verjetnost njihovega pojava.
- Verjetnost in posledice teh tveganj so posredovane in razumljene.
- Prednostni vrstni red obravnavanja tveganj je vzpostavljen.
- Prednostni vrstni red ukrepov za zmanjšanje tveganj je izdelan.
- Deležniki sodelujejo pri odločanju o obvladovanju tveganj in so sproti obveščeni o stanju obvladovanja tveganj.
- Spremlja se uspešnost obravnavanja tveganj.
- Tveganja in proces obvladovanja tveganj se redno spremljajo in pregledujejo.
- Informacije se zajemajo za izboljšanje pristopa k obvladovanju tveganj.
- Vodstvo in osebje se izobražujeta o tveganjih in sprejetih ukrepih za njihovo ublažitev.

Proces obvladovanja informacijskih varnostnih tveganj se lahko uporablja za organizacijo kot celoto, za kateri koli ločeni del organizacije (npr. oddelek, fizično lokacijo, storitev), za kateri koli informacijski sistem ali za obstoječe, načrtovane ali posebne vidike kontrol (npr. načrtovanje neprekinjenega poslovanja).

6 Pregled procesa obvladovanja informacijskih varnostnih tveganj

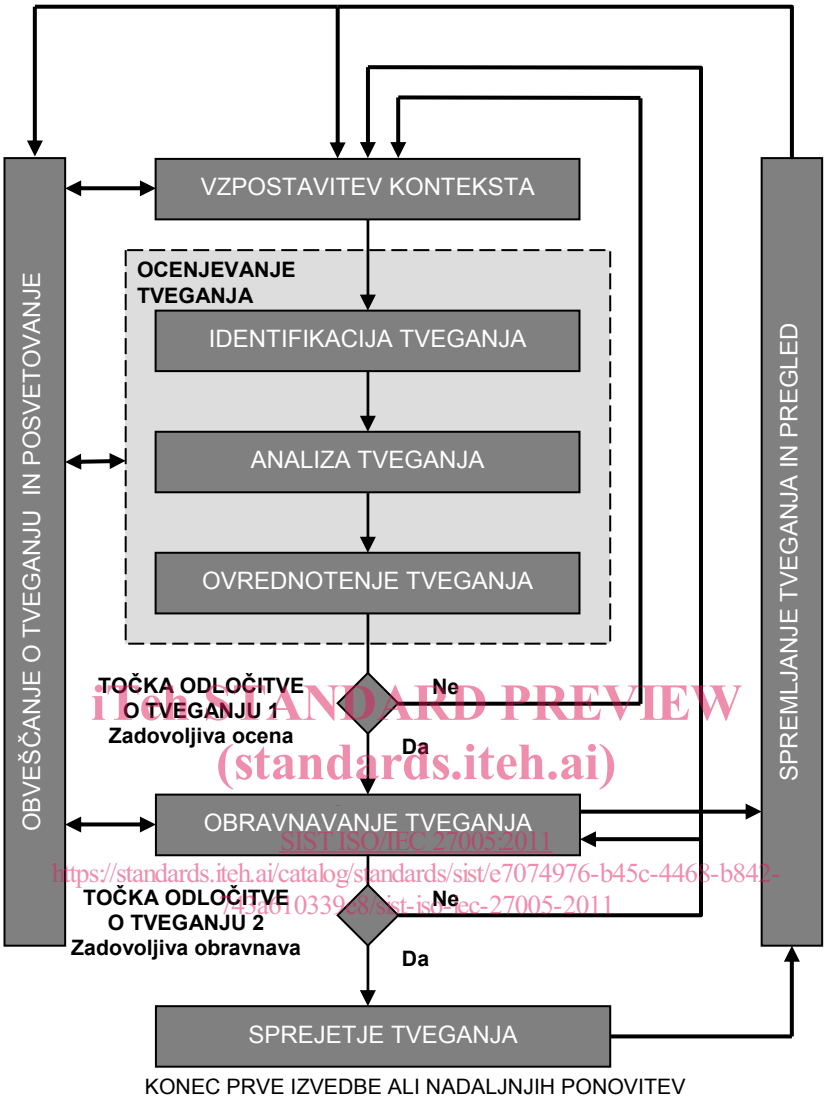
Pogled z vrha na proces obvladovanja tveganj je specificiran v ISO 31000 in je prikazan na sliki 1.



Slika 1: Proces obvladovanja tveganj

Slika 2 prikazuje, kako se ta mednarodni standard uporablja pri procesu obvladovanja tveganj.

Proces obvladovanja informacijskih varnostnih tveganj je sestavljen iz vzpostavljanja konteksta (točka 7), ocenjevanja tveganja (točka 8), obravnavanja tveganja (točka 9), sprejetja tveganja (točka 10), obveščanja o tveganju in posvetovanja (točka 11) ter spremljanja in pregleda tveganja (točka 12).



Slika 2: Prikaz procesa obvladovanja informacijskih varnostnih tveganj

Kot prikazuje slika 2, se proces obvladovanja informacijskih varnostnih tveganj lahko ponavlja pri ocenjevanju tveganj in/ali pri aktivnostih obravnavanja tveganj. Ponavljajoči pristop k izvedbi ocenjevanja tveganj lahko poveča globino in podrobnosti ocenjevanja pri vsaki ponovitvi. Zagotavlja dobro ravnotežje med skrajšanjem časa in vloženimi napori pri prepoznavanju kontrol, medtem ko še vedno zagotavlja, da so velika tveganja ustrezno ocenjena.

Najprej se vzpostavi kontekst. Nato se izvede ocenjevanje tveganj. Če to zagotavlja dovolj informacij za uspešno določanje ukrepov, potrebnih za spremembo tveganj na sprejemljivo raven, potem je naloga končana in temu sledi obravnavanje tveganj. Če informacije ne zadostujejo, bo izpeljana druga ponovitev ocenjevanja tveganj z revidiranim kontekstom (npr. kriteriji za vrednotenje tveganja, kriteriji za sprejetje tveganja ali kriteriji vpliva), po možnosti na omejenih delih celotnega obsega (glej sliko 2, točka odločitve o tveganju 1).

Uspešnost obravnavanja tveganj je odvisna od rezultatov ocenjevanja tveganj.

Upoštevati je treba, da obravnavanje tveganj vključuje cikličen proces:

- ocenjevanja obravnavanja tveganj,
- odločanja, ali so ravni preostalega tveganja sprejemljive,
- ustvarjanja nove obravnave tveganj, če ravni tveganj niso sprejemljive, in
- ocenjevanja uspešnosti te obravnave.

Mogoče je, da obravnavanje tveganj ne bo peljalo takoj do sprejemljive ravni preostalega tveganja. V tem primeru, če je potrebno, je lahko zahtevana druga ponovitev ocenjevanja tveganj s spremenjenimi parametri konteksta (npr. kriteriji za ocenjevanje tveganja, kriteriji za sprejetje tveganja ali kriteriji vpliva), kateri sledi nadaljnja obravnava tveganj (glej sliko 2, točka odločitve o tveganju 2).

Aktivnost sprejetja tveganj mora zagotoviti, da vodje organizacije izrecno sprejmejo preostala tveganja. To je še posebej pomembno, kadar je izvajanje kontrol opuščeno oziroma preloženo, na primer zaradi stroškov.

Med celotnim procesom obvladovanja informacijskih varnostnih tveganj je pomembno, da se tveganja in njihova obravnavanja posredujejo – sporočajo ustreznim vodjem in zaposlenemu osebju na operativni ravni. Že pred obravnavanjem tveganj so informacije o prepoznanih tveganjih lahko zelo dragocene za upravljanje incidentov in lahko prispevajo k zmanjšanju potencialne škode. Zavedanje vodij in zaposlenega osebja o tveganjih, naravi kontrol za zmanjševanje tveganj in o področjih v zvezi z organizacijo pomaga h kar najuspešnejšemu reševanju incidentov in nepričakovanih dogodkov. Podrobni rezultati vsake aktivnosti procesa obvladovanja informacijskih varnostnih tveganj in obeh točk odločitve o tveganjih naj se dokumentirajo.

ISO/IEC 27001 določa, da morajo kontrole, ki se izvajajo v okviru področja, meja in konteksta SUIV, temeljiti na tveganju. Uporaba procesa obvladovanja informacijskih varnostnih tveganj lahko zadovolji to zahtevo. Pristopov, s katerimi je v posamezni organizaciji mogoče uspešno izvajati proces, je veliko. Organizacija naj ne glede na pristop uporabi za vsako posamezno uporabo procesa tistega, ki najbolj ustreza njenim okoliščinam.

V SUIV so vzpostavljanje konteksta, ocenjevanje tveganj, izoblikovanje načrta obravnavanja tveganj in sprejetje tveganj skupaj del faze "načrtuj". V fazi "izvedi" določenega SUIV so ukrepi in kontrole, zahtevani za zmanjšanje tveganj na sprejemljivo raven, izvedeni v skladu z načrtom obravnavanja tveganj. V fazi "preveri" določenega SUIV bodo vodje določili potrebo po revizijah ocenjevanja in obravnavanja tveganja v luči incidentov in sprememb okoliščin. V fazi "ukrepaj" so izvedeni vsi zahtevani ukrepi, vključno z izvedbo dodatnih ponovitev procesa obvladovanja informacijskih varnostnih tveganj.

Naslednja preglednica povzema aktivnosti obvladovanja informacijskih varnostnih tveganj, pomembnih za štiri faze procesa SUIV:

Preglednica 1: Uskladitev SUIV in procesa obvladovanja informacijskih varnostnih tveganj

Procesi SUIV	**Proces obvladovanja informacijskih varnostnih tveganj**
Načrtuj	Vzpostavljanje konteksta Ocenjevanje tveganj Razvoj načrta obravnavanja tveganj Sprejetje tveganj
Izvedi	Izvedba načrta obravnavanja tveganj
Preveri	Nenehno spremljanje in pregledovanje tveganj
Ukrepaj	Vzdrževanje in izboljševanje procesa obvladovanja informacijskih varnostnih tveganj