SLOVENSKI STANDARD

SIST ISO/IEC 27004

november 2018

Informacijska tehnologija – Varnostne tehnike – Vodenje informacijske varnosti – Spremljanje, merjenje, analiza in vrednotenje

Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

Sample Document

Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Surveillance, mesurage, analyse et évaluation

get full document from standards.iteh.ai

ICS 03.100.70; 35.030

Referenčna oznaka
SIST ISO/IEC 27004:2018 (sl)

Nadaljevanje na straneh 2 do 65

© 2026-03. Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

NACIONALNI UVOD

Standard SIST ISO/IEC 27004 (sl), Informacijska tehnologija – Varnostne tehnike – Vodenje informacijske varnosti – Spremljanje, merjenje, analiza in vrednotenje, 2018, ima status slovenskega standarda in je istoveten z mednarodnim standardom ISO/IEC 27004 (en, fr), Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation, 2016.

NACIONALNI PREDGOVOR

Besedilo standarda ISO/IEC 27004:2016 je pripravil združeni tehnični odbor Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehniške komisije (IEC) ISO/IEC JTC 1 Informacijska tehnologija. Slovenski standard SIST ISO/IEC 27004:2018 je prevod angleškega besedila mednarodnega standarda ISO/IEC 27004:2016. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvirni mednarodni standard v angleškem jeziku. Slovensko izdajo standarda je pripravil SIST/TC ITC Informacijska tehnologija.

Odločitev za privzem tega standarda je dne 1. novembra 2018 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27004:2016

Sample Document

PREDHODNA IZDAJA

get full document from standards.iteh.ai

– SIST ISO/IEC 27004:2011, Informacijska tehnologija – Varnostne tehnike – Upravljanje informacijske varnosti – Merjenje

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27004:2018 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

– Neustrezno označena imena primerov konstruktov merjenja v besedilu od B.31 na str. 57 do B.37 na str. 63 v primerjavi s preglednico imen konstruktov merjenja v B.1 Splošno k dodatku B.

– Napaka pri povezavi na točke ali številke ciljev kontrol v ISO/IEC 27001:2013 pri konstruktih merjenja B.11 (str. 36), B.13 (str. 39) in B.28 (str. 54).

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Vsebina **Stran**

Sample Document
Get full document from standards.iteh.ai

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Sample Document
get full document from standards.iteh.ai

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Predgovor k mednarodnemu standardu

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 ustanovila združeni tehnični odbor ISO/IEC JTC 1.

Postopki, uporabljeni pri pripravi tega dokumenta, in predvideni postopki za njegovo vzdrževanje so opisani v 1. delu Direktiv ISO/IEC. Posebna pozornost naj se nameni različnim kriterijem odobritve, potrebnim za različne vrste dokumentov. Ta dokument je bil zasnovan v skladu z uredniškimi pravili 2. dela Direktiv ISO/IEC (glej www.iso.org/directives).

Opozoriti je treba na možnost, da bi lahko bil kateri od elementov tega dokumenta predmet patentnih pravic. ISO in IEC nista odgovorna za identificiranje katerekoli ali vseh takih patentnih pravic. Podrobnosti o morebitnih patentnih pravicah, identificiranih med pripravo tega dokumenta, bodo navedene v uvodu in/ali na seznamu patentnih izjav, ki jih je prejela organizacija ISO (glej www.iso.org/patents).

Vsakršna trgovska imena, uporabljena v tem dokumentu, so informacije za uporabnike in ne pomenijo podpore blagovni znamki.

Za razlago pomena specifičnih pojmov in izrazov ISO, povezanih z ugotavljanjem skladnosti, ter informacij o tem, kako ISO spoštuje načela Svetovne trgovinske organizacije (WTO) v Tehničnih ovirah pri trgovanju (TBT), glej naslednji naslov URL: www.iso.org/iso/foreword.html.

Sample Document

Za ta dokument je pristojen tehnični odbor ISO/IEC JTC 1, *Informacijska tehnologija,* pododbor *SC 27, Varnostne tehnike IT*.

get full document from standards.iteh.ai

Ta druga izdaja standarda ISO/IEC 27004 razveljavlja in nadomešča prvo izdajo (ISO/IEC 27004:2009), ki je tehnično revidirana.

Ta izdaja v primerjavi s prejšnjo vključuje naslednje pomembne spremembe:

Popolno prestrukturiranje dokumenta, saj ima nov namen – podati smernice za točko 9.1 v ISO/IEC 27001:2013 –, ki pri prejšnji izdaji ni obstajala.

Koncepti in postopki so bili spremenjeni ter razširjeni. Teoretična osnova (ISO/IEC 15939) sicer ostaja enaka, številni primeri iz prejšnje izdaje pa so ohranjeni, čeprav posodobljeni.

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Uvod

Namen tega dokumenta je pomagati organizacijam ovrednotiti delovanje informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti za namene izpolnitve zahtev točke 9.1 v ISO/IEC 27001:2013: spremljanje, merjenje, analiziranje in vrednotenje.

Rezultati spremljanja in merjenja sistema vodenja informacijske varnosti (ISMS) lahko podpirajo odločitve v zvezi z upravljanjem, vodenjem, uspešnostjo delovanja in nenehnim izboljševanjem sistema ISMS.

Kot pri drugih dokumentih ISO/IEC 27000 naj se tudi ta dokument upošteva, razlaga in prilagodi posebnim razmeram v posamezni organizaciji. Koncepti in pristopi so namenjeni široki uporabi, vendar so posamezna merila, ki jih zahteva posamezna organizacija, odvisna od kontekstualnih dejavnikov (kot so velikost, sektor, zrelost, tveganja informacijske varnosti, obveznosti glede skladnosti in način vodenja), ki se v praksi zelo razlikujejo.

Ta dokument je priporočljiv za organizacije, ki uvajajo sistem vodenja informacijske varnosti, ki izpolnjuje zahteve standarda ISO/IEC 27001. Vendar pa ne določa nobenih novih zahtev za sisteme vodenja informacijske varnosti, ki so skladne s standardom ISO/IEC 27001, in organizacijam ne nalaga nobenih obveznosti glede upoštevanja predstavljenih smernic.

Sample Document

get full document from standards.iteh.ai

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Informacijska tehnologija – Varnostne tehnike – Vodenje informacijske varnosti – Spremljanje, merjenje, analiza in vrednotenje

1 Področje uporabe

Ta dokument podaja smernice za pomoč organizacijam pri vrednotenju delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti za namene izpolnitve zahtev točke 9.1 v ISO/IEC 27001:2013. Določa:

a) spremljanje in merjenje delovanja informacijske varnosti,

b) spremljanje in merjenje uspešnosti sistema vodenja informacijske varnosti (ISMS), vključno z njegovimi procesi in kontrolami,

c) analizo ter vrednotenje rezultatov spremljanja in merjenja.

Ta dokument se uporablja za vse vrste in velikosti organizacij.

2 Zveze s standardi

Naslednji dokumenti so navedeni v besedilu na način, da njihov del ali celotna vsebina predstavlja zahteve tega dokumenta. Pri datiranih sklicevanjih se uporablja le navedena izdaja. Pri nedatiranih sklicevanjih se uporablja zadnja izdaja navedenega dokumenta (vključno z dopolnili).

Ta dokument ne vsebuje zvez s standardi.

Sample Document

3 Izrazi in definicije

V tem dokumentu so uporabljeni izrazi in definicije, podani v standardu ISO/IEC 27000.

get full document from standards.iteh.ai

ISO in IEC hranita terminološke podatkovne zbirke za uporabo pri standardizaciji na naslednjih naslovih:

– IEC Electropedia: na voljo na http://www.electropedia.org/

– Platforma za spletno brskanje ISO: na voljo na http://www. iso.org/obp

4 Struktura in pregled

Ta dokument ima naslednjo strukturo:

a) Utemeljitev (točka 5),

b) Lastnosti (točka 6),

c) Vrste meril (točka 7),

d) Procesi (točka 8).

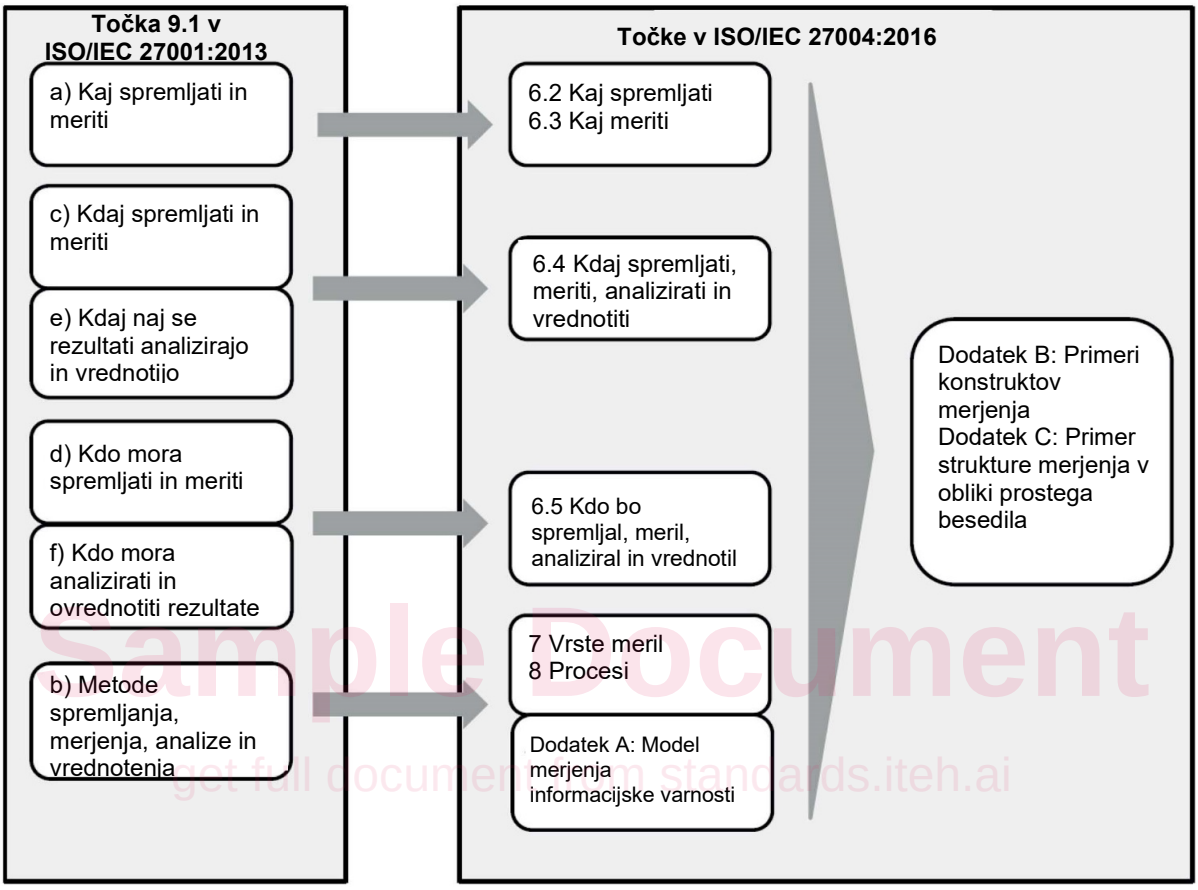
Razporeditev teh točk je namenjena lažjemu razumevanju in ustreza zahtevam 9.1 standarda ISO/IEC 27001:2013, kot je prikazano na sliki 1.

Organizacija začne z informacijami, potrebnimi za izpolnitev te zahteve, imenovanimi potrebe po informacijah, nato pa določi merila, ki jih bo uporabila za izpolnitev teh potreb po informacijah. S spremljanjem in merjenjem se pridobivajo podatki, ki se nato analizirajo. Rezultati analize se ovrednotijo z vidika izpolnjevanja potreb po informacijah organizacije.

Poleg tega je v dodatku A opisan model merjenja informacijske varnosti, vključno z razmerjem med komponentami modela merjenja in zahtevami točke 9.1 v ISO/IEC 27001:2013.

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

V dodatku B je na voljo širok nabor primerov. Ti primeri so namenjeni zagotavljanju praktičnih smernic, kako lahko organizacije spremljajo, merijo, analizirajo ter ovrednotijo izbrane procese sistema vodenja informacijske varnosti in območja delovanja informacijske varnosti. V teh primerih je uporabljena predlagana predloga iz preglednice 1. V dodatku C je naveden dodaten primer z uporabo alternativne besedilne oblike zapisa v prosti obliki.



Sample Document
get full document from standards.iteh.ai

Slika 1: Preslikava na zahteve točke 9.1 v ISO/IEC 27001:2013

5 Utemeljitev

5.1 Potreba po merjenju

Splošni cilj sistema vodenja informacijske varnosti je ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij v njegovem obsegu. Obstajajo aktivnosti sistema vodenja informacijske varnosti, ki se navezujejo na načrtovanje, kako to storiti, in na izvajanje teh načrtov. A te aktivnosti same po sebi ne morejo zagotoviti, da realizacija teh načrtov izpolnjuje cilje informacijske varnosti. Zato je v sistemu vodenja informacijske varnosti, kot ga opredeljuje standard ISO/IEC 27001, več zahtev za ovrednotenje, ali načrti in aktivnosti zagotavljajo izpolnjevanje ciljev informacijske varnosti.

5.2 Izpolnjevanje zahtev standarda ISO/IEC 27001

Točka 9.1 v ISO/IEC 27001:2013 zahteva, da organizacija ovrednoti delovanje informacijske varnosti in uspešnost sistema vodenja informacijske varnosti. Vrste meril, ki lahko izpolnijo te zahteve, so navedene v točki 7.

Točka 9.1 v ISO/IEC 27001:2013 zahteva tudi, da organizacija določi:

a) katere potrebe morajo biti spremljane in merjene, vključno s procesi in kontrolami informacijske

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

varnosti,

b) metode za spremljanje, merjenje, analizo in vrednotenje, če je potrebno, da se zagotovijo veljavni rezultati,

c) kdaj se morata izvajati spremljanje in merjenje,

d) kdo mora spremljati in meriti,

e) kdaj se morajo analizirati in vrednotiti rezultati spremljanja in merjenja; ter

f) kdo mora analizirati in ovrednotiti te rezultate.

Preslikava teh zahtev je na voljo na sliki 1.

Točka 9.1 v ISO/IEC 27001:2013 nazadnje zahteva, da organizacija hrani ustrezne dokumentirane informacije kot dokaz o rezultatih spremljanja in merjenja (glej 8.9).

Točka 9.1 v ISO/IEC 27001:2013 navaja tudi, da naj izbrane metode zagotovijo primerljive in ponovljive rezultate, da se lahko ti štejejo za veljavne (glej 6.4).

5.3 Veljavnost rezultatov

Točka 9.1 b) v ISO/IEC 27001:2013 zahteva, da organizacije izberejo metode za spremljanje, merjenje, analizo in vrednotenje, ki zagotavljajo veljavne rezultate. V točki je navedeno, da naj bodo rezultati primerljivi in ponovljivi, da bodo veljavni. V ta namen naj organizacije zberejo, analizirajo in sporočijo merila ter pri tem upoštevajo naslednje točke:

a) za pridobivanje primerljivih rezultatov glede meril, ki temeljijo na spremljanju v različnih časovnih obdobjih, je treba zagotoviti, da se obseg in kontekst sistema vodenja informacijske varnosti ne spremenita,

b) spremembe metod ali tehnik, ki se uporabljajo za merjenje in spremljanje, na splošno ne zagotavljajo primerljivih rezultatov. Za ohranitev primerljivosti se lahko zahtevajo posebni testi, kot je vzporedna uporaba prvotnih in spremenjenih metod,

c) če so subjektivni elementi del metod ali tehnik, ki se uporabljajo za merjenje in spremljanje, bodo za pridobitev ponovljivih rezultatov morda potrebni posebni koraki. Rezultati vprašalnika naj bodo na primer ovrednoteni na podlagi opredeljenih kriterijev; in

d) v nekaterih primerih je mogoče ponovljivost zagotoviti le v specifičnih okoliščinah. Včasih rezultatov na primer ni mogoče ponoviti, vendar so veljavni, če so združeni.

5.4 Koristi

Izpolnjevanje procesov in kontrol sistema vodenja informacijske varnosti ter zagotavljanje delovanja informacijske varnosti lahko zagotovi številne organizacijske in finančne koristi. Glavne koristi so lahko:

a) **Povečana odgovornost:** spremljanje, merjenje, analiza in vrednotenje lahko povečajo odgovornost za informacijsko varnost, saj so v pomoč pri prepoznavanju specifičnih procesov ali kontrol informacijske varnosti, ki se izvajajo nepravilno, se ne izvajajo ali so neučinkoviti.

b) **Izboljšanje delovanja informacijske varnosti in procesov sistema vodenja informacijske varnosti:** spremljanje, merjenje, analiza in vrednotenje lahko organizacijam omogočijo, da količinsko opredelijo izboljšave pri varovanju informacij v obsegu svojega sistema vodenja informacijske varnosti in izkažejo merljiv napredek pri doseganju ciljev organizacije na področju informacijske varnosti.

c) **Dokaz o izpolnjevanju zahtev:** spremljanje, merjenje, analiza in vrednotenje lahko zagotovijo dokumentirane dokaze, ki so v pomoč pri izkazovanju izpolnjevanja zahtev standarda ISO/IEC 27001 (in drugih standardov) ter veljavnih zakonov, pravil in predpisov.

Sample Document
www.iteh.ai | iTeh Standards

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

d) **Podpora pri odločanju:** spremljanje, merjenje, analiza in vrednotenje lahko podpirajo odločanje na podlagi informacij o tveganjih, saj v proces obvladovanja tveganja prispevajo merljive informacije. Organizacije lahko tako merijo uspešnost oziroma neuspešnost preteklih in trenutnih naložb v informacijsko varnost ter pridobijo merljive podatke, ki lahko podpirajo dodeljevanje virov za prihodnje naložbe.

6 Lastnosti

6.1 Splošno

Spremljanje in merjenje sta prvi korak v procesu vrednotenja delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti.

Ob potencialno velikem številu atributov subjektov, povezanih z informacijsko varnostjo, ki jih je mogoče meriti, ni povsem jasno, katere naj se meri. To je pomembno vprašanje, saj merjenje prevelikega števila lastnosti ali napačnih lastnosti ni praktično oziroma je drago in kontraproduktivno. Poleg očitnih stroškov merjenja, analiziranja in sporočanja številnih atributov obstaja jasna možnost, da se v veliki količini informacij zameglijo ključna vprašanja ali pa se ta v celoti spregledajo, če niso določena ustrezna merila.

Za določitev, kaj spremljati in meriti, naj organizacija najprej razmisli, kaj želi doseči pri vrednotenju delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti. Tako lahko določi svoje potrebe po informacijah.

Organizacije naj se nato odločijo, katera merila so potrebna za podporo posamezne diskretne potrebe po informacijah in kateri podatki so potrebni za izpeljavo zahtevanih meril. Zato naj merjenje vedno ustreza potrebam po informacijah organizacije.

Sample Document

6.2 Kaj spremljati

Spremljanje določa stanje sistema, procesa ali aktivnosti za izpolnjevanje specifične potrebe po informacijah.

get full document from standards.iteh.ai

Sistemi, procesi in aktivnosti, ki jih je mogoče spremljati, med drugim vključujejo, vendar niso omejeni na:

a) izvajanje procesov sistema vodenja informacijske varnosti,

b) vodenje incidentov,

c) upravljanje ranljivosti,

d) upravljanje konfiguracije,

e) ozaveščenost in usposabljanje o varnosti,

f) nadzor dostopa, požarni zid in drugo beleženje dogodkov

g) presojo,

h) proces ocenjevanja tveganj,

i) proces obravnavanja tveganj,

j) obvladovanje tveganja tretjih strani,

k) vodenje neprekinjenega poslovanja,

l) upravljanje fizične in okoljske varnosti; ter

m) spremljanje sistema.

Te aktivnosti spremljanja zagotavljajo podatke (dnevnike dogodkov, razgovore z uporabniki, statistiko

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

usposabljanja, informacije o incidentih itd.), ki se lahko uporabijo za podporo drugim merilom. V procesu določanja atributov, ki jih je treba meriti, se lahko zahteva dodatno spremljanje, da se zagotovijo podporne informacije.

S spremljanjem lahko organizacija ugotovi, ali se je tveganje uresničilo, in tako določi ukrepe, ki jih lahko sprejme za obravnavanje takega tveganja. Upošteva naj se tudi, da so lahko nekatere vrste kontrol informacijske varnosti izrecno namenjene spremljanju. Pri uporabi rezultatov takih kontrol za podporo merjenju naj organizacije zagotovijo, da proces merjenja upošteva, ali so bili uporabljeni podatki pridobljeni pred ali po izvedenem ukrepu obravnavanja.

6.3 Kaj meriti

Merjenje je aktivnost, ki se izvaja za določitev vrednosti, stanja ali trenda delovanja ali uspešnosti, da se lažje opredelijo morebitne potrebe po izboljšavah. Merjenje se lahko uporablja za vse procese, aktivnosti, kontrole in skupine kontrol sistema vodenja informacijske varnosti.

Kot primer se lahko navede točka 7.2 c) v ISO/IEC 27001:2013, ki od organizacije zahteva, da po potrebi sprejme ukrepe za pridobitev potrebne usposobljenosti. Organizacija lahko ugotovi, ali so bili vsi posamezniki, ki so potrebovali usposabljanje, tega deležni in ali je bilo usposabljanje izvedeno, kot je bilo načrtovano. To je mogoče izmeriti s številom ali odstotkom usposobljenih oseb. Organizacija lahko tudi ugotovi, ali so posamezniki, ki so se usposabljali, dejansko pridobili in ohranili potrebne usposobljenosti (kar je mogoče izmeriti z vprašalnikom po usposabljanju).

V zvezi s procesi sistema vodenja informacijske varnosti naj organizacije upoštevajo, da standard ISO/IEC 27001 vsebuje več točk, ki izrecno zahtevajo, da se določi uspešnost nekaterih aktivnosti. Točka 10.1 d) v ISO/IEC 27001:2013 na primer zahteva, da organizacije *"pregledajo uspešnost vseh izvedenih korektivnih ukrepov".* Za izvedbo takega pregleda naj se najprej določi uspešnost korektivnih ukrepov v smislu neke opredeljene oblike merila. V ta namen naj organizacija najprej opredeli ustrezno potrebo po informacijah in merilo ali merila za njeno izpolnitev. Postopek za to je pojasnjen v točki 8.

Sample document
get full document from standards.iteh.ai

Procesi in aktivnosti sistema vodenja informacijske varnosti, ki so primerni za merjenje, vključujejo:

a) načrtovanje,

b) voditeljstvo,

c) obvladovanje tveganj,

d) vodenje politike,

e) upravljanje virov,

f) sporočanje,

g) vodstveni pregled,

h) dokumentiranje; in

i) presojo.

Kar zadeva delovanje informacijske varnosti, so najbolj očitni kandidati kontrole informacijske varnosti organizacije ali skupine takih kontrol (ali celo celoten načrt obravnavanja tveganj). Te kontrole so določene znotraj procesa obravnavanja tveganja in so v standardu ISO/IEC 27001 navedene kot potrebne kontrole. To so lahko kontrole iz standarda ISO/IEC 27001:2013 (dodatek A), področne kontrole (npr. opredeljene v standardih, kot je ISO/IEC 27010), kontrole, določene v drugih standardih, in kontrole, ki jih je zasnovala organizacija. Ker je namen kontrole spreminjanje tveganja, je mogoče meriti različne atribute, kot so:

j) stopnja, do katere kontrola zmanjšuje verjetnost nastanka dogodka,

k) stopnja, do katere kontrola zmanjšuje posledice dogodka,

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

l) pogostost dogodkov, ki jo kontrola lahko obvladuje pred odpovedjo; in

m) v kolikšnem času po nastopu dogodka kontrola zazna, da je dogodek nastopil.

6.4 Kdaj spremljati, meriti, analizirati in vrednotiti

Organizacije naj opredelijo posebne časovne okvire za spremljanje, merjenje, analizo in vrednotenje na podlagi posameznih potreb po informacijah, zahtevanih meril in življenjskega cikla podatkov, ki podpirajo posamezna merila. Zbiranje podatkov, ki podpirajo merila, se lahko izvaja pogosteje kot analiza in sporočanje teh meril posameznim zainteresiranim stranem. Podatke o varnostnih incidentih je na primer mogoče zbirati neprekinjeno, poročanje o teh podatkih zunanjim zainteresiranim stranem pa naj temelji na posebnih zahtevah, kot so resnost (po možnosti zahteva po takojšnjem obvestilu kot v primeru kršitve, o kateri je treba poročati) ali zbirne vrednosti (kot v primeru poskusov vdorov, ki so bili odkriti in blokirani).

Organizacije naj upoštevajo, da je treba za izpolnitev nekaterih potreb po informacijah pred začetkom analize in vrednotenja zbrati ustrezno količino podatkov, da se zagotovi smiselna podlaga za ocenjevanje in primerjavo (npr. pri izvajanju statistične analize). Poleg tega je treba postopke spremljanja, merjenja, analize in vrednotenja testirati ter prilagoditi, preden so pridobljena merila uporabna za organizacijo. Organizacije naj zato določijo omejitev trajanja morebitnega natančnega prilagajanja (da lahko nadaljujejo s končnim ciljem, merjenjem sistema vodenja informacijske varnosti) in kako dolgo naj se izvajata spremljanje in zbiranje, preden se lahko začneta analiza in vrednotenje.

Organizacije lahko ob posodobitvi svojih aktivnosti merjenja prilagodijo svoje časovne okvire merjenja tako, da upoštevajo posebne spremembe v okolju, navedene v 8.2. Če na primer organizacija prehaja z ročnega vira podatkov na avtomatizirani vir, bo morda potrebna sprememba pogostosti zbiranja. Poleg tega je potrebno izhodišče za primerjavo dveh naborov meril, uporabljenih v različnih časovnih obdobjih in morebiti z različnimi metodami, vendar za namene izpolnjevanja iste potrebe po informacijah.

Sample Document

Organizacija lahko svoje dejavnosti spremljanja, merjenja, analize in vrednotenja strukturira v program merjenja, vendar pa je pomembno vedeti, da ISO/IEC 27001 od organizacij ne zahteva, da imajo vzpostavljen tak program.

Preview of full document from standards.iteh.ai

6.5 Kdo bo spremljal, meril, analiziral in vrednotil

Organizacije (ob upoštevanju zahtev točk 9.1 in 5.3 v ISO/IEC 27001:2013) naj določijo, kdo spremlja, meri, analizira in vrednoti v smislu posameznikov ali vlog. Spremljanje, merjenje, analizo in vrednotenje je mogoče izvajati z ročnimi ali avtomatiziranimi sredstvi. Ne glede na to, ali se merjenje izvaja ročno ali samodejno, lahko organizacije opredelijo naslednje vloge in odgovornosti, povezane z merjenjem:

a) naročnik merjenja: vodstvo ali druge zainteresirane strani, ki zahtevajo informacije o uspešnosti sistema vodenja informacijske varnosti, kontrol ali skupine kontrol,

b) načrtovalec merjenja: oseba ali organizacijska enota, ki opredeli merilne konstrukcije, ki povezujejo merljive atribute z določeno potrebo po informacijah,

c) recenzent merjenja: oseba ali organizacijska enota, ki potrdi, da so oblikovani konstrukti merjenja primerni za vrednotenje delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti, kontrol ali skupine kontrol,

d) lastnik informacij: oseba ali organizacijska enota, ki je lastnik informacij, ki zagotavljajo vhodne podatke za merila. Ta oseba je odgovorna za zagotavljanje podatkov in je pogosto (vendar ne vedno) odgovorna tudi za izvajanje aktivnosti merjenja,

e) zbiralec informacij: oseba ali organizacijska enota, odgovorna za zbiranje, evidentiranje in shranjevanje podatkov,

f) informacijski analitik: oseba ali organizacijska enota, odgovorna za analizo podatkov; in

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

g) sporočevalec informacij: oseba ali organizacijska enota, odgovorna za posredovanje rezultatov analize.

Organizacije lahko nekatere ali celo vse te vloge združijo.

Posamezniki, ki med procesi opravljajo različne vloge in odgovornosti, bodo morda potrebovali različna znanja in spretnosti ter s tem povezano ozaveščenost in usposabljanje.

7 Vrste meril

7.1 Splošno

Za namene teh smernic je mogoče delovanje načrtovanih aktivnosti in uspešnost rezultatov izmeriti z uporabo naslednjih dveh vrst meril:

a) merila učinkovitosti delovanja: merila, ki odražajo načrtovane rezultate v smislu značilnosti načrtovane aktivnosti, kot so število zaposlenih, doseganje mejnikov ali stopnja izvajanja kontrol informacijske varnosti,

b) merila uspešnosti: merila, ki odražajo učinek, ki ga ima uresničevanje načrtovanih aktivnosti na cilje informacijske varnosti organizacije.

Ta merila so lahko specifična za posamezno organizacijo, saj ima vsaka organizacija svoje posebne cilje, politike in zahteve glede informacijske varnosti.

Izraza "merila učinkovitosti delovanja" in "merila uspešnosti" naj se ne zamenjata z zahtevo točke 9.1 v ISO/IEC 27001:2013 za vrednotenje delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti.

Sample Document

7.2 Merila učinkovitosti delovanja

Merila učinkovitosti delovanja je mogoče uporabiti za prikaz napredka pri izvajanju procesov sistema vodenja informacijske varnosti, povezanih postopkov in posebnih varnostnih kontrol. Medtem ko se uspešnost navezuje na obseg, v katerem so bile izvedene načrtovane aktivnosti in doseženi načrtovani rezultati, naj se merila učinkovitosti delovanja navezujejo na obseg, v katerem so bili izvedeni procesi in kontrole informacijske varnosti. Ta merila so v pomoč pri ugotavljanju, ali so bili procesi sistema vodenja informacijske varnosti in kontrole informacijske varnosti izvedeni, kot je določeno.

Merila učinkovitosti delovanja uporabljajo podatke, ki jih je mogoče pridobiti iz zapisnikov, evidenc prisotnosti, projektnih načrtov, samodejnih orodij za optično branje ter drugih pogosto uporabljenih sredstev za dokumentiranje, beleženje in spremljanje dejavnosti sistema vodenja informacijske varnosti.

Zbiranje, analiza in sporočanje meril naj bodo avtomatizirani, če je to mogoče, da se zmanjšajo potrebni stroški in delo ter možnost človeških napak.

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Primer 1

Pri merjenju stopnje izvajanja specifičnih kontrol informacijske varnosti, kot je odstotek prenosnih računalnikov s šifriranjem trdega diska, bodo rezultati tega merila sprva verjetno nižji od 100 %. Ko rezultat doseže 100 % in tam ostane, je mogoče sklepati, da so informacijski sistemi v celoti izvedli varnostne kontrole, ki jih obravnava to merilo, aktivnosti merjenja pa je mogoče osredotočiti na druge kontrole, ki jih je treba izboljšati.

Primer 2

Pri novem sistemu vodenja informacijske varnosti naj si organizacija najprej prizadeva, da se najvišje vodstvo udeleži pregleda in drugih sestankov, ki jih je mogoče sklicati. Načrtovani (ali predvideni) rezultat v tem primeru je popolna udeležba na vseh sestankih, razen v primeru bolezni in dovoljenih predhodnih obveznosti. Merilo preprosto izraža razmerje med številom udeležencev in številom tistih, ki bi se morali udeležiti, z morebitnim dejavnikom sprememb, da je bila odsotnost upravičena. Sprva bi rezultati teh meril lahko kazali na primanjkljaj, vendar bi morali sčasoma doseči načrtovane cilje in ostati blizu njih. Na tej točki naj organizacija svoja prizadevanja za merjenje osredotoči na merila uspešnosti (glej 7.3).

Ko večina meril učinkovitosti delovanja doseže 100 % in tam ostane, naj organizacija svoja prizadevanja za merjenje osredotoči na merila uspešnosti. Organizacije naj nikoli ne opustijo meril učinkovitosti delovanja v celoti, saj so lahko koristna pri opozarjanju na določene varnostne kontrole, ki jih je treba izboljšati. Sčasoma naj se poudarek in viri, ki se uporabljajo za merjenje, s teh meril preusmerijo na merila uspešnosti (glej 7.3).

V skladu z 9.1 v ISO/IEC 27001:2013 je prav tako pomembno, da se meri tudi uspešnost sistema vodenja (obravnavano v nadaljevanju). Za delovanje ustreznega sistema vodenja informacijske varnosti naj organizacije v načrtovanih časovnih intervalih merijo delovanje in uspešnost.

Sample Document

7.3 Merila uspešnosti

Merila uspešnosti naj bodo uporabljena za opis uspešnosti in vpliva, ki ga ima uresničevanje načrta obravnavanja tveganj sistema vodenja informacijske varnosti ter procesov in kontrol sistema vodenja informacijske varnosti na cilje informacijske varnosti organizacije. S temi merili naj se ugotovi, ali procesi sistema vodenja informacijske varnosti in kontrole informacijske varnosti delujejo, kot je bilo predvideno, in dosegajo želene rezultate. Glede na te cilje je mogoče merila uspešnosti uporabiti za količinsko opredelitev, npr.:

a) prihrankov, ki jih zagotovi sistem vodenja informacijske varnosti, ali stroškov, nastalih zaradi obravnavanja informacijskih varnostnih incidentov,

b) stopnje zaupanja strank, ki jo je pridobil ali ohranil sistem vodenja informacijske varnosti; in

c) doseganja drugih ciljev informacijske varnosti.

Merila uspešnosti je mogoče oblikovati z združevanjem podatkov, pridobljenih iz avtomatiziranih orodij za spremljanje in vrednotenje, in ročno pridobljenih podatkov o aktivnostih sistema vodenja informacijske varnosti. To lahko zahteva sledenje različnim merilom v organizaciji na način, ki ga je mogoče neposredno povezati z aktivnostmi sistema vodenja informacijske varnosti in informacijskimi varnostnimi dogodki. Za doseganje tega naj ima organizacija vzpostavljene zmogljivosti za:

d) ovrednotenje stopnje uvedbe procesov, kontrol ali skupin kontrol sistema vodenja informacijske varnosti na podlagi meril učinkovitosti delovanja,

e) zbiranje podatkov avtomatiziranih orodij za spremljanje in vrednotenje,

f) ročno zbiranje podatkov iz aktivnosti sistema vodenja informacijske varnosti,

g) normaliziranje in analiziranje podatkov iz več avtomatiziranih in ročnih virov; ter

h) razlago in sporočanje teh podatkov odločevalcem.

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018

Ta merila uspešnosti združujejo informacije o uresničevanju načrta obravnavanja tveganj z različnimi informacijami o virih in lahko prispevajo k procesu obvladovanja tveganja. Prav tako lahko zagotovijo najbolj neposreden vpogled v vrednost informacijske varnosti za organizacijo in so lahko tisti, ki bi morali biti najbolj zanimivi za najvišje vodstvo.

Primer 3

Izkoriščanje znanih ranljivosti je poznano kot vzrok za velik del informacijskih varnostnih incidentov. Večje kot je število znanih ranljivosti in dlje kot se ne odpravijo (npr. popravijo), večja je verjetnost, da jih bodo izkoristile povezane grožnje, in večja je izpostavljenost s tem povezanemu tveganju. Merilo uspešnosti je lahko organizaciji v pomoč pri ugotavljanju njene izpostavljenosti tveganjem zaradi takšnih ranljivosti.

Primer 4

Tečaj usposabljanja ima lahko za vsak modul določene cilje usposabljanja. Na podlagi merila uspešnosti lahko organizacija ugotovi, v kolikšni meri je posamezen udeleženec usposabljanja razumel posamezno lekcijo in je sposoben uporabiti svoje novo znanje in spretnosti. Ta merila običajno zahtevajo več podatkovnih točk, kot so: rezultati testov po usposabljanju, pregled podatkov o incidentih, povezanih s temami usposabljanja, ali analiza klicev oddelka za pomoč uporabnikom, povezanih s temami usposabljanja.

8 Procesi

8.1 Splošno

Spremljanje, merjenje, analiza in vrednotenje (glej sliko 2) so sestavljeni iz naslednjih procesov:

a) prepoznavanje potreb po informacijah,

b) ustvarjanje in vzdrževanje meril,

c) vzpostavitev postopkov,

d) spremljanje in merjenje,

e) analiza rezultatov; in

f) vrednotenje delovanja informacijske varnosti in uspešnosti sistema vodenja informacijske varnosti.

Poleg tega obstaja proces upravljanja sistema vodenja informacijske varnosti, ki zajema pregled in izboljševanje zgornjih postopkov (glej 8.8).

Sample Document
Get full document from standards.iteh.ai

SIST ISO/IEC 27004:2018 • https://standards.iteh.ai/catalog/standards/sist/d4ff9c0a-29c2-4f7c-814b-8c12c9af1abf/sist-iso-iec-27004-2018