SLOVENSKI STANDARD

SIST ISO/IEC 27006

november 2012

Informacijska tehnologija – Varnostne tehnike – Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information – Techniques de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

ICS 03.120.20; 35.040

Referenčna oznaka
SIST ISO/IEC 27006:2012 (sl)

Nadaljevanje na straneh 2 do 40

© 2015-07. Slovenski inštitut za standardizacijo. Razmnoževanje ali kopiranje celote ali delov tega standarda ni dovoljeno.

NACIONALNI PREDGOVOR

Standard SIST ISO/IEC 27006 (sl), Informacijska tehnologija – Varnostne tehnike – Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti, 2012, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27006 (en), Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems, 2011-12.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27006:2011 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 27006:2012 je prevod mednarodnega standarda ISO/IEC 27006:2011. V primeru spora glede besedila slovenskega prevoda je odločilen izvirni mednarodni standard v angleškem jeziku. Slovenski standard SIST ISO/IEC 27006:2012 je pripravil tehnični odbor SIST/TC ITC Informacijska tehnologija.

Odločitev za izdajo tega standarda je dne 26. septembra 2012 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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a5bcd456-d48c-40e-ba8c-a6c69e53286f/sist-iso-iec-27006-2012

SIST ISO/IEC 17021:2011	Ugotavljanje skladnosti – Zahteve za organe, ki presojajo in certificirajo sisteme vodenja (ISO/IEC 17021:2011)
SIST ISO/IEC 27001:2005	Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve *(zamenjan s SIST ISO/IEC 27001:2013)*
SIST ISO 19011	Smernice za presojanje sistemov vodenja (ISO 19011:2011)

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27006:2011

OPOMBI

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27006:2012 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

VSEBINA **Stran**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

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 27006 je pripravil združeni tehnični odbor ISO/IEC JTC 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

Uvod

Standard ISO/IEC 17021 določa kriterije za organe, ki presojajo in certificirajo sisteme vodenja organizacij. Če so ti organi akreditirani v skladu z ISO/IEC 17021 ter nameravajo presojati in certificirati sisteme upravljanja informacijske varnosti (SUIV) v skladu z ISO/IEC 27001:2005, potrebujejo nekatere dodatne zahteve in navodila k ISO/IEC 17021. Ti so na voljo v tem mednarodnem standardu.

Besedilo v tem mednarodnem standardu sledi strukturi ISO/IEC 17021 in zato so dodatne zahteve, specifične za SUIV, in navodila o uporabi ISO/IEC 17021 za certificiranje SUIV označeni s črkama "IV".

V celotnem mednarodnem standardu je modalni glagol "morati" uporabljen za označevanje tistih določil, ki odražajo zahteve ISO/IEC 17021 in ISO/IEC 27001 ter so obvezne. Izraz "naj" se uporablja za izražanje priporočil.

Eden od ciljev tega mednarodnega standarda je omogočiti akreditacijskim organom, da uspešneje uskladijo svojo uporabo standardov s tistimi, katerim so zavezani pri ocenjevanju certifikacijskih organov.

OPOMBA: V tem mednarodnem standardu se izraza "sistem upravljanja" in "sistem" uporabljata izmenično. Definicijo sistema upravljanja (vodenja) je mogoče najti v ISO 9000:2005. Sistem upravljanja, kot se uporablja v tem mednarodnem standardu, se ne sme zamenjati z drugimi vrstami sistemov, kot so sistemi IT.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

Informacijska tehnologija – Varnostne tehnike – Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti

1 Področje uporabe

Ta mednarodni standard določa zahteve in daje navodila organom, ki presojajo in certificirajo sistem upravljanja informacijske varnosti (SUIV), kot dodatek k zahtevam, ki jih vsebujeta ISO/IEC 17021 in ISO/IEC 27001. Namenjen je predvsem v podporo akreditiranju certifikacijskih organov, ki nudijo certificiranje SUIV.

Izpolnjevanje zahtev iz tega mednarodnega standarda mora vsak organ, ki nudi certificiranje SUIV, dokazati z vidika kompetentnosti in zanesljivosti, navodila iz tega mednarodnega standarda pa vsakemu organ, ki nudi certificiranje SUIV, zagotavljajo dodatno razlago teh zahtev.

OPOMBA: Ta mednarodni standard se lahko uporablja kot dokument kriterijev za akreditacijo, medsebojno ocenjevanje ali druge procese presoje.

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 17021:2006 Ugotavljanje skladnosti – Zahteve za organe, ki presojajo in certificirajo sisteme vodenja

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

ISO/IEC 19011 Smernice za presojanje sistemov vodenja

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-16c69e532866/sist-iso-iec-27006-2012

3 Izrazi in definicije

V tem dokumentu se uporabljajo izrazi in definicije, podani v ISO/IEC 17021, ISO/IEC 27001 in v nadaljevanju.

3.1
certifikat
certifikat, ki ga izda certifikacijski organ v skladu s pogoji svoje akreditacije in ima znak akreditacije ali izjavo

3.2
certifikacijski organ
tretja stranka, ki ocenjuje in certificira SUIV organizacije stranke glede na objavljene standarde SUIV in vso dodatno dokumentacijo, ki se potrebuje v sistemu

3.3
certifikacijski dokument
dokument, ki dokazuje, da je SUIV organizacije stranke v skladu z določenimi standardi SUIV in vso dodatno dokumentacijo, ki se potrebuje v sistemu

3.4
znak
zakonito registrirana blagovna znamka ali drugačen zaščiten simbol, ki je izdan v skladu s pravili akreditacijskega ali certifikacijskega organa in kaže, da so ti organi dokazali ustrezno zaupanje v delovanje sistemov in da ustrezni proizvodi oziroma posamezniki ustrezajo zahtevam določenega standarda

3.5
organizacija
družba, korporacija, podjetje, organ ali institucija ali kombinacija vseh teh, ki je bodisi združena ali ne, javna ali zasebna, ima lastne naloge in upravo ter je sposobna zagotoviti izvajanje informacijske varnosti

4 Načela

Veljajo načela iz ISO/IEC 17021:2011, točka 4.

5 Splošne zahteve

5.1 Pravne in pogodbene zadeve

Veljajo zahteve iz ISO/IEC 17021:2011, točka 5.1.

5.2 Obvladovanje nepristranskosti

Veljajo zahteve iz ISO/IEC 17021:2011, točka 5.2. Poleg tega veljajo naslednje zahteve in navodila, specifični za SUIV.

5.2.1 IV 5.2 Nasprotje interesov

Certifikacijski organi lahko opravljajo naslednje naloge, ne da bi bile obravnavane kot svetovanje ali da bi vsebovale morebitno nasprotje interesov:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) certificiranje, vključno z informativnimi srečanji, srečanji načrtovanj, pregledi dokumentov, presojanjem (ki ni notranje presojanje SUIV ali notranje ocenjevanje varnosti) in spremljanjem neskladnosti,

b) urejanje in sodelovanje kot predavatelj v programih usposabljanja, pri čemer se morajo certifikacijski organi, kadar se ti programi nanašajo na upravljanje informacijske varnosti in z njimi povezanih sistemov upravljanja ali presojanja, omejiti le na zagotavljanje splošnih informacij in nasvetov, ki so brezplačno na voljo v javnem interesu, kar pomeni, da ne smejo dajati specifičnih nasvetov posameznim podjetjem, ki so v nasprotju z zahtevami iz c) spodaj,

SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a350ca4a3c-d48c-4f0e-baac-aoca0ye53/sist-iso-iec-27006-2012

c) omogočanje dostopa do informacij ali objavljanje informacij na zahtevo, v katerih certifikacijski organ razlaga zahteve standardov o certifikacijski presoji (glej 9.1.1.1),

d) aktivnosti pred presojo, namenjene zgolj ugotavljanju pripravljenosti na certifikacijsko presojo, vendar pa takšne aktivnosti ne smejo voditi v dajanje priporočil ali nasvetov, ki bi bili lahko v nasprotju s to točko, certifikacijski organ pa mora biti sposoben potrditi, da te aktivnosti niso v nasprotju s temi zahtevami ter da se ne uporabljajo za utemeljitev skrajšanja trajanja morebitne certifikacijske presoje,

e) izvajanje presoj v vlogi druge in tretje stranke, v skladu s standardi ali predpisi, razen tistih, ki so del obsega akreditacije,

f) dodajanje vrednosti med certifikacijskimi presojami in rednimi obiski, na primer, s prepoznavanjem možnosti za izboljšave, ko te postanejo očitne med presojanjem, brez priporočil posebnih rešitev.

Certifikacijski organ mora biti neodvisen od organa ali organov (vključno z vsemi posamezniki), ki izvajajo notranjo presojo SUIV organizacije stranke, ki je predmet certificiranja.

5.3 Obveznosti in financiranje

Veljajo zahteve iz ISO/IEC 17021:2011, točka 5.3.

6 Strukturne zahteve

6.1 Organizacijska struktura in najvišje vodstvo

Veljajo zahteve iz ISO/IEC 17021:2011, točka 6.1.

6.2 Odbor za varovanje nepristranskosti

Veljajo zahteve iz ISO/IEC 17021:2011, točka 6.2.

7 Zahteve glede virov

7.1 Kompetentnost vodstva in osebja

Veljajo zahteve iz ISO/IEC 17021:2011, točka 7.1. Poleg tega pa veljajo naslednje zahteve in navodila, specifični za SUIV.

7.1.1 IV 7.1.1 Splošno

Bistveni elementi kompetentnosti, potrebni za izvajanje certificiranja SUIV, so izbiranje, zagotavljanje in vodenje tistih posameznikov, katerih veščine in kolektivna kompetentnost so primerne za presojane aktivnosti in za povezana vprašanja informacijske varnosti.

7.1.1.1 Analiza kompetentnosti in pregled pogodb

Certifikacijski organ mora zagotoviti, da ima znanje o tehnološkem in pravnem razvoju, pomembnem za SUIV organizacije stranke, katerega ocenjuje.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Certifikacijski organ mora imeti uspešen sistem za analiziranje kompetentnosti pri upravljanju informacijske varnosti, ki jih mora imeti na voljo, glede na vsa strokovna področja, na katerih deluje.

SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a9c49e53250f/sist-iso-iec-27006-2012

Za vsako stranko mora biti certifikacijski organ sposoben dokazati, da je pred pregledom pogodbe izvedel analizo kompetentnosti (ocenjevanje veščin kot odgovor na ovrednotene potrebe) za zahteve vsakega pomembnega sektorja. Certifikacijski organ mora nato na podlagi rezultatov te analize pregledati pogodbo z organizacijo stranke. Še posebej mora biti certifikacijski organ sposoben dokazati, da je kompetenten za dokončanje naslednjih aktivnosti:

a) da razume področja dejavnosti organizacije stranke in s tem povezana poslovna tveganja,

b) da opredeli kompetence, potrebne certifikacijskemu organu za certificiranje v zvezi s prepoznanimi aktivnostmi in informacijsko varnostjo glede na grožnje dobrinam, ranljivosti in vplive na organizacijo stranke,

c) da potrdi razpoložljivost potrebnih kompetenc.

7.1.1.2 Viri

Vodstvo certifikacijskega organa mora imeti potrebne procese in vire, da je sposobno ugotoviti, ali so posamezni presojevalci kompetentni za naloge, ki jih morajo opravljati v obsegu certifikacije, v katerem delujejo. Kompetentnost presojevalcev se lahko ugotavlja s preverjanjem osnovnih veščin in posebnim usposabljanjem ali kratkimi napotki (glej tudi dodatek B). Certifikacijski organ mora biti sposoben učinkovito komunicirati z vsemi tistimi strankami, ki jim zagotavlja storitve.

7.1.2 IV Določanje kriterijev kompetentnosti

V dodatku B so navedene dodatne informacije o znanju in veščinah, ki podpirajo kriterije kompetentnosti iz ISO/IEC 17021.

7.2 Osebje, vključeno v aktivnosti certificiranja

Veljajo zahteve iz ISO/IEC 17021:2011, točka 7.2. Poleg tega veljajo naslednje zahteve in navodila, specifični za SUIV.

7.2.1 IV 7.2 Kompetentnost osebja certifikacijskega organa

Certifikacijski organi morajo imeti osebje, kompetentno, da:

a) izbere in preveri kompetentnost presojevalcev SUIV za presojevalske skupine, primerne za presojo,

b) da napotke presojevalcem SUIV in uredi vsako potrebno usposabljanje,

c) odloča o podelitvi, vzdrževanju, preklicu, začasnem odvzemu, razširitvi ali krčenju obsega certifikacije,

d) vzpostavi in vodi proces pritožb in prizivov.

7.2.1.1 Usposabljanje presojevalskih skupin

Certifikacijski organ mora imeti kriterije za usposabljanje presojevalskih skupin tako, da zagotovijo:

a) znanje o standardih za SUIV in o drugih ustreznih normativnih dokumentih,

b) razumevanje informacijske varnosti,

c) razumevanje ocenjevanja tveganja in obvladovanja tveganja z vidika poslovanja,

d) tehnično znanje o presojani aktivnosti,

e) splošno znanje o regulativnih zahtevah, pomembnih za SUIV,

f) znanje o sistemih vodenja,

g) razumevanje načel presojanja, ki temeljijo na ISO 19011,

h) znanje o uspešnosti pregleda SUIV in merjenju uspešnosti nadzora.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

Te zahteve za usposabljanje veljajo za vse člane presojevalske skupine, razen d), ki se lahko razdeli med člani presojevalske skupine.

7.2.1.1.1 Pri izbiri presojevalske skupine, ki bo imenovana za posebno certifikacijsko presojo, mora certifikacijski organ zagotoviti, da so veščine, ki jih prinese vsak imenovani, ustrezne. Skupina mora:

a) imeti ustrezno tehnično znanje o posebnih aktivnostih v obsegu SUIV, za katerega se zahteva certificiranje, in kjer je to primerno, z njimi povezanih postopkih in njihovih morebitnih informacijskih varnostnih tveganjih (tehnični strokovnjaki, ki niso presojevalci, lahko opravljajo to funkcijo),

b) imeti zadostno stopnjo razumevanja organizacije stranke, da izvede zanesljivo certifikacijsko presojo njenega SUIV pri upravljanju vidikov informacijske varnosti pri njenih aktivnostih, proizvodih in storitvah,

c) imeti ustrezno razumevanje regulativnih zahtev glede SUIV organizacije stranke.

7.2.1.1.2 Kadar je potrebno, se presojevalska skupina lahko dopolni s tehničnimi strokovnjaki, ki lahko dokažejo posebne kompetence na področju tehnike, primerne za presojo. Pri tem naj se opomni, da tehničnih strokovnjakov ni mogoče uporabiti namesto presojevalcev SUIV, lahko pa svetujejo presojevalcem o zadevah tehnične ustreznosti v okviru presojanega sistema upravljanja. Certifikacijski organ mora imeti postopek za:

a) izbiro presojevalcev in tehničnih strokovnjakov na podlagi njihove kompetentnosti, usposobljenosti, kvalifikacij in izkušenj,

b) začetno ocenjevanje ravnanja presojevalcev in tehničnih strokovnjakov med certifikacijskimi

presojami in nato spremljanje dela presojevalcev in tehničnih strokovnjakov.

7.2.1.2 Vodenje procesa sprejemanja odločitev

Vodstvena funkcija mora biti tehnično kompetentna in sposobna voditi proces sprejemanja odločitev v zvezi s podelitvijo, vzdrževanjem, razširitvijo in krčenjem obsega, začasnim odvzemom in preklicem certifikacije SUIV na podlagi zahtev ISO/IEC 27001.

7.2.1.3 Zahtevane stopnje izobrazbe, delovne izkušnje, usposobljenost in izkušnje za presojevalce, ki izvajajo presoje SUIV

7.2.1.3.1 Vsak presojevalec v presojevalski skupini za SUIV mora izpolnjevati naslednje kriterije. Presojevalec mora:

a) imeti srednješolsko izobrazbo,

b) imeti najmanj štiri leta praktičnih izkušenj s polnim delovnim časom na delovnem mestu s področja informacijske tehnologije, od katerih je bil vsaj dve leti v vlogi ali funkciji, povezani z informacijsko varnostjo,

c) uspešno zaključiti pet dni usposabljanja s področja, ki zajema presoje SUIV, in ga mora vodstvo presoje šteti za ustreznega,

d) pridobiti izkušnje v celotnem procesu ocenjevanja informacijske varnosti, preden prevzame odgovornost za izvajanje kot presojevalec. Te izkušnje naj pridobi s sodelovanjem v najmanj štirih certifikacijskih presojah v skupnem trajanju najmanj 20 dni, vključno s pregledom dokumentacije in analizami tveganja, izvajanjem ocenjevanja in poročanjem o presoji,

e) imeti izkušnje, ki so razumno posodobljene,

f) biti sposoben postaviti zapletene postopke v širše perspektive in razumeti vlogo posameznih enot v večjih organizacijah stranke,

g) ohranjati na tekočem svoje znanje in veščine na področju informacijske varnosti in presojanja z nenehnim strokovnim razvojem.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

Tehnični strokovnjaki morajo izpolnjevati kriterije a), b), e) in f).

7.2.1.3.2 Dodatno k zahtevam iz 7.2.1.3.1 morajo vodje presojevalske skupine izpolnjevati naslednje zahteve, ki jih morajo pokazati pri vodeni in nadzorovani presoji:

a) imeti znanje in veščine za vodenje procesa certifikacijske presoje,

b) so bili presojevalci v vsaj treh celotnih presojah SUIV,

c) so pokazali sposobnost uspešnega komuniciranja, tako ustnega kot pisnega.

7.3 Uporaba posameznih zunanjih presojevalcev in zunanjih tehničnih strokovnjakov

Veljajo zahteve iz ISO/IEC 17021:2011, točka 7.3. Poleg tega veljajo naslednje zahteve in navodila, specifični za SUIV.

7.3.1 IV 7.3 Uporaba zunanjih presojevalcev ali zunanjih tehničnih strokovnjakov kot del presojevalske skupine

Kadar so del presojevalske skupine tudi posamezni zunanji presojevalci ali zunanji tehnični strokovnjaki, mora certifikacijski organ zagotoviti, da so usposobljeni in v skladu z veljavnimi določili te publikacije ter da niso, bodisi neposredno ali prek svojega delodajalca, vključeni v snovanje, izvajanje ali vzdrževanje SUIV ali podobnega(-ih) sistema(-v) za upravljanje tako, da bi bila lahko ogrožena nepristranskost.

7.3.1.1 Uporaba tehničnih strokovnjakov

Tehnični strokovnjaki s posebnim znanjem v zvezi s procesom ter vprašanji informacijske varnosti in

zakonodaje, ki vplivajo na organizacijo stranke, ki pa ne izpolnjujejo vseh kriterijev iz 7.2, so lahko del presojevalske skupine. Tehnični strokovnjaki morajo delovati pod nadzorom presojevalca.

7.4 Zapisi o osebju

Veljajo zahteve iz ISO/IEC 17021:2011, točka 7.4.

7.5 Oddajanje del zunanjim izvajalcem

Veljajo zahteve iz ISO/IEC 17021:2011, točka 7.5.

8 Zahteve glede informacij

8.1 Javno dostopne informacije

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8,1. Poleg tega veljajo naslednje zahteve in navodila, specifični za SUIV.

8.1.1 IV 8.1 Postopki za podelitev, vzdrževanje, razširitev ali krčenje obsega, začasni odvzem ali preklic certifikacije

Certifikacijski organ mora zahtevati od organizacije stranke, da ima dokumentiran in izveden SUIV, ki je skladen z ISO/IEC 27001 in drugimi dokumenti, zahtevanimi za certifikacijo.

Certifikacijski organ mora imeti dokumentirane postopke za:

a) začetno certifikacijsko presojo SUIV organizacije stranke v skladu z določili ISO/IEC 17021 in drugimi ustreznimi dokumenti,

b) redne in obnovitvene certifikacijske presoje SUIV organizacije stranke v skladu z ISO/IEC 17021 v rednih časovnih presledkih za nadaljnjo skladnost z ustreznimi zahtevami ter za preverjanje in poročanje, da organizacija stranke izvaja popravne ukrepe pravočasno za popravilo vseh neskladnosti.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

8.2 Certifikacijski dokumenti

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8.2. Poleg tega veljajo naslednje zahteve in navodila, specifični za SUIV.

8.2.1 IV 8.2 Certifikacijski dokumenti SUIV

Certifikacijski organ mora vsaki svoji stranki, katere SUIV je certificiran, zagotoviti certifikacijske dokumente, kot so pismo ali certifikat, ki ga je podpisala uradna oseba, imenovana za podpisovanje. Za stranko organizacije in vsak njen informacijski sistem, ki ga certifikacija zajema, morajo ti dokumenti določiti obseg, za katerega je certifikacija dodeljena, in navesti standard ISO/IEC 27001 o sistemih upravljanja informacijske varnosti, po katerem je bil SUIV certificiran. Poleg tega se mora certifikacija sklicevati na posebno različico izjave o uporabnosti.

8.3 Register certificiranih strank

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8.3.

8.4 Sklicevanje na certifikacijo in uporaba znakov

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8.4. Poleg tega veljajo še naslednje zahteve in navodila, specifični za SUIV.

8.4.1 IV 8.4 Nadzor nad certifikacijskimi znaki

Certifikacijski organ mora izvajati ustrezen nadzor nad lastništvom, uporabo in prikazom svojih certifikacijskih znakov za SUIV. Če certifikacijski organ podeli pravico do uporabe znaka za prikaz certifikacije SUIV, mora zagotoviti, da organizacija stranke uporablja poseben znak le na način, kot jo je pisno pooblastil certifikacijski organ. Certifikacijski organ ne sme dati pravice organizaciji stranki za uporabo tega znaka na izdelku ali na način, ki bi se lahko razlagal, kot da označuje skladnost proizvoda.

8.5 Zaupnost

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8.5. Poleg tega veljajo še naslednje zahteve in navodila, specifični za SUIV.

8.5.1 IV 8.5 Dostop do zapisov organizacije

Pred certifikacijsko presojo mora certifikacijski organ zaprositi organizacijo stranke za poročilo, ali kateri od zapisov o SUIV ni na voljo za pregled presojevalski skupini, ker vsebuje zaupne ali občutljive informacije. Certifikacijski organ mora ugotoviti, ali je mogoče SUIV ustrezno presoditi brez teh zapisov. Če certifikacijski organ ugotovi, da SUIV ni mogoče ustrezno presoditi brez pregleda prepoznanih zaupnih ali občutljivih zapisov, mora o tem obvestiti organizacijo stranke, da certifikacijske presoje ni mogoče opraviti, dokler se ne odobri ustrezen način dostopa.

8.6 Izmenjava informacij med certifikacijskim organom in njegovimi strankami

Veljajo zahteve iz ISO/IEC 17021:2011, točka 8.6.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

9 Zahteve glede procesov

9.1 Splošne zahteve

SIST ISO/IEC 27006:2012
https://standards.iteh.ai/catalog/standards/sist/a3bca456-d48c-4f0e-ba8e-a6c69e53286f/sist-iso-iec-27006-2012

Veljajo zahteve iz ISO/IEC 17021:2011, točka 9.1. Poleg tega veljajo še naslednje zahteve in navodila, specifični za SUIV.

9.1.1 IV 9.1.1 Splošne zahteve za presojo SUIV

9.1.1.1 Kriteriji certifikacijske presoje

Kriteriji, po katerih se presojajo SUIV strank, morajo biti enaki opisanim v standardu za ISO/IEC 27001 o SUIV in v drugih dokumentih, ki se zahtevajo za certificiranje in se nanašajo na izvajano funkcijo. Če je v zvezi z uporabo teh dokumentov za poseben program certificiranja potrebno pojasnilo, potem mora tako pojasnilo podati ustrezen in nepristranski odbor ali osebe s potrebnim tehničnim znanjem, katerih imena je objavil certifikacijski organ.

9.1.1.2 Politike in postopki

Dokumentacija certifikacijskega organa mora vključevati politiko in postopke za izvajanje procesa certificiranja, vključno s preverjanji njihove uporabe in uporabe dokumentov pri certificiranju SUIV ter postopkov za presojanje in certificiranje SUIV organizacije stranke.

9.1.1.3 Presojevalska skupina

Presojevalska skupina mora biti formalno imenovana in opremljena z ustreznimi delovnimi dokumenti. O načrtu in datumu pregleda se je treba dogovoriti z organizacijo stranke. Naročilo, dano presojevalski skupini, mora biti jasno opredeljeno in biti znano organizaciji stranke ter mora od presojevalske skupine zahtevati, da preuči strukturo, politike in postopke organizacije stranke ter potrdi, da ti izpolnjujejo vse zahteve, pomembne za obseg certifikacije, in da se postopki izvajajo in so taki, da dajejo zaupanje v SUIV organizacije stranke.