SLOVENSKI STANDARD

SIST ISO/IEC 27003

marec 2011

Informacijska tehnologija – Varnostne tehnike – Smernice za izvedbo sistema upravljanja informacijske varnosti

Information technology – Security techniques – Information security management system implementation guidance

Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information

ICS 35.040

Referenčna oznaka
SIST ISO/IEC 27003:2011 (sl)

Nadaljevanje na straneh 2 do 65

NACIONALNI UVOD

Standard SIST ISO/IEC 27003 (sl), Informacijska tehnologija – Varnostne tehnike – Smernice za izvedbo sistema upravljanja informacijske varnosti, 2011, ima status slovenskega standarda in je istoveten mednarodnemu standardu ISO/IEC 27003 (en), Information technology – Security techniques – Information security management system implementation guidance, 2010-02-01.

NACIONALNI PREDGOVOR

Mednarodni standard ISO/IEC 27003:2010 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 27003:2011 je prevod mednarodnega standarda ISO/IEC 27003:2010. Slovenski standard SIST ISO/IEC 27003:2011 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 25. november 2010 sprejel SIST/TC ITC Informacijska tehnologija.

ZVEZA Z NACIONALNIMI STANDARDI

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 *(nadomeščen s SIST ISO/IEC 27001:2013)*

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO/IEC 27003:2010

OPOMBI

– Povsod, kjer se v besedilu standarda uporablja izraz “mednarodni standard”, v SIST ISO/IEC 27003:2011 to pomeni “slovenski standard”.

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

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.

Osnutki mednarodnih standardov so pripravljeni v skladu s pravili iz 2. dela 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 so lahko nekateri elementi tega dokumenta predmet patentnih pravic. ISO ne prevzema odgovornosti za identifikacijo nekaterih ali vseh takih patentnih pravic.

ISO/IEC 27003 je pripravil združeni tehnični odbor JTC ISO/IEC 1 *Informacijska tehnologija,* pododbor SC 27 *Varnostne tehnike IT.*

Uvod

Namen tega mednarodnega standarda je zagotoviti praktične napotke pri razvoju načrta izvedbe upravljavskega sistema za informacijsko varnost (SUIV) v organizaciji v skladu z ISO/IEC 27001:2005. Dejanska izvedba SUIV se v splošnem izvrši kot projekt.

Proces, opisan v tem mednarodnem standardu, je bil zasnovan, da zagotovi podporo izvajanju ISO/IEC 27001:2005 (ustrezni deli iz točk 4, 5 in vključujoč 7), in dokumentira:

a) pripravo začetka načrta izvedbe SUIV v organizaciji, opredelitev organizacijske projektne strukture in pridobivanje odobritve vodstva,

b) kritične aktivnosti za projekt SUIV in

c) primere za doseganje zahtev v ISO/IEC 27001:2005.

Z uporabo tega mednarodnega standarda bo organizacija sposobna razviti proces upravljanja informacijske varnosti in dajati zainteresiranim strankam zagotovila, da so tveganja informacijskih dobrin nenehno vzdrževana v okviru sprejemljivih meja informacijske varnosti, kot jih je opredelila organizacija.

Ta mednarodni standard ne obravnava operativnih aktivnosti in drugih aktivnosti SUIV, zajema pa koncepte, kako zasnovati aktivnosti, ki se bodo izvajale po začetku delovanja SUIV. Koncept se kaže v končnem projektnem načrtu izvedbe SUIV. Dejanska izvršitev specifičnih delov projekta SUIV organizacije je zunaj področja uporabe tega mednarodnega standarda.

Izvedba projekta SUIV naj se izvaja z uporabo standardnih metodologij projektnega vodenja (več informacij je navedenih v standardih ISO in ISO/IEC v zvezi s projektnim vodenjem).

Informacijska tehnologija – Varnostne tehnike – Smernice za izvedbo sistema upravljanja informacijske varnosti

1 Področje uporabe

Ta mednarodni standard se osredotoča na kritične vidike, ki so potrebni za uspešno zasnovo in izvedbo sistema upravljanja informacijske varnosti (SUIV) v skladu z ISO/IEC 27001:2005. Opisuje proces specifikacije in zasnove SUIV od začetka do izvajanja načrtov. Opisuje proces pridobivanja odobritve vodstva za izvedbo SUIV, definira projekt izvedbe SUIV (v tem standardu poimenovan projekt SUIV) in ponuja napotke, kako načrtovati projekt SUIV, kar se odraža v dokončanem načrtu izvedbe projekta SUIV.

Ta mednarodni standard naj bi uporabljale organizacije, ki uvajajo SUIV. Primeren je za vse vrste organizacij (na primer podjetja, vladne agencije, nepridobitne organizacije) vseh velikosti. Kompleksnost in tveganja vsake organizacije so edinstveni in njene specifične zahteve bodo vodile izvedbo SUIV. Manjše organizacije bodo ugotovile, da so aktivnosti, navedene v tem mednarodnem standardu, primerne zanje in da jih je mogoče poenostaviti. Velike in kompleksne organizacije bodo lahko ugotovile, da sta za učinkovito upravljanje aktivnosti iz tega mednarodnega standarda potrebna nivojska organiziranost ali nivojski sistem upravljanja. Vendar je v obeh primerih mogoče ustrezne aktivnosti načrtovati z uporabo tega mednarodnega standarda.

Ta mednarodni standard podaja priporočila in pojasnila; ne določa nobenih zahtev. Ta mednarodni standard je namenjen, da se uporablja skupaj z ISO/IEC 27001:2005 in ISO/IEC 27002:2005, ni pa namenjen spreminjanju in/ali zmanjševanju zahtev, danih v ISO/IEC 27001:2005, ali priporočil, danih v ISO/IEC 27002:2005. Trditve o skladnosti s tem mednarodnim standardom niso ustrezne.

2 Zveza s standardi

Naslednja dokumenta sta nujna za uporabo tega dokumenta. Pri datiranem sklicevanju velja samo navedena izdaja. Pri nedatiranem sklicevanju velja zadnja izdaja dokumenta, na katerega se nanaša sklic (vključno z morebitnimi dopolnitvami).

ISO/IEC 27000:2009 Informacijska tehnologija – Varnostne tehnike – Sistem upravljanja informacijske varnosti – Pregled in izrazoslovje

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

3 Izrazi in definicije

V tem dokumentu so uporabljeni izrazi in definicije, podani v nadaljevanju ter v ISO/IEC 27000:2009 in ISO/IEC 27001:2005.

3.1
projekt SUIV
strukturirane aktivnosti, ki jih opravlja organizacija za izvajanje SUIV

4 Struktura tega mednarodnega standarda

4.1 Splošna struktura poglavij

Izvedba SUIV je pomembna aktivnost in se v splošnem izvaja kot projekt organizacije. Ta dokument razlaga, kako izvesti SUIV z osredotočenjem na zasnovo, načrtovanje in opredelitev projekta. Proces načrtovanja končne izvedbe SUIV vsebuje pet faz in vsaka faza je predstavljena v svoji točki. Vse točke imajo podobno strukturo, kot je opisana spodaj. Pet faz je:

a) pridobitev odobritve vodstva za uvedbo projekta SUIV (točka 5),

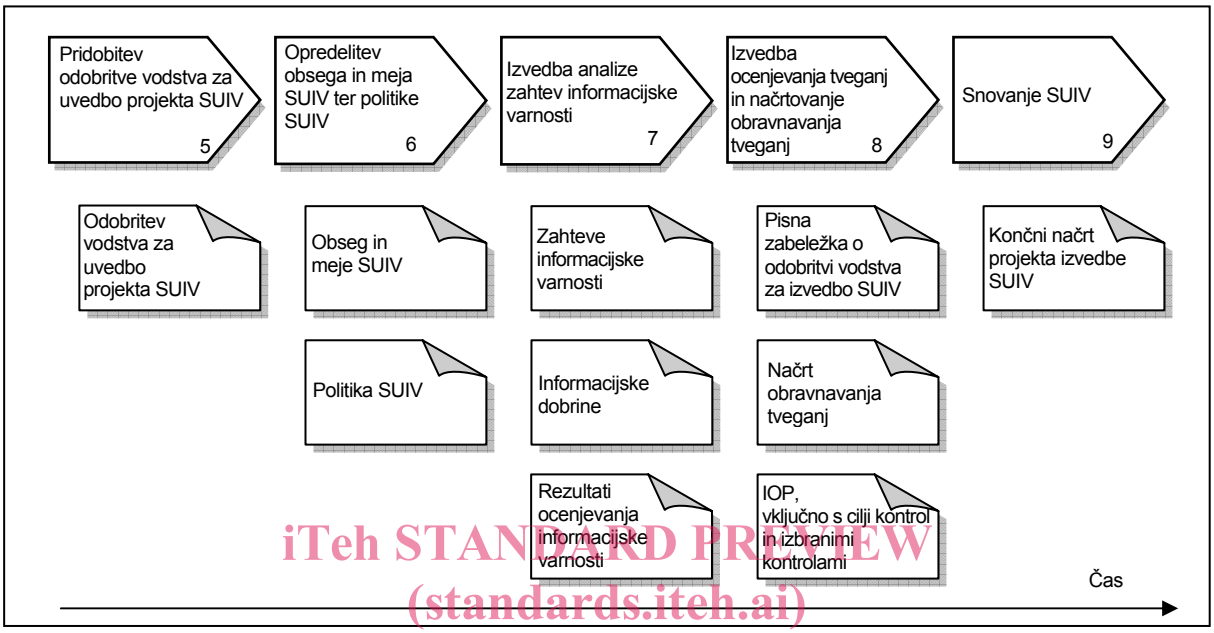
b) opredelitev obsega SUIV in politike SUIV (točka 6),

c) izvedba analize organizacije (točka 7),

d) izvedba ocenjevanja tveganj in načrtovanje obravnave tveganj (točka 8),

e) snovanje SUIV (točka 9).

Slika 1 prikazuje pet faz načrtovanja projekta SUIV po standardih ISO/IEC ter glavne izhodne dokumente.



Slika 1: Faze projekta SUIV

Več informacij je navedenih v dodatkih. Ti dodatki so:

Dodatek A: Povzetek aktivnosti s sklici na ISO/IEC 27001:2005

Dodatek B: Vloge in odgovornosti v informacijski varnosti

Dodatek C: Informacije o načrtovanju notranjih presoj

Dodatek D: Struktura politik

Dodatek E: Informacije o načrtovanju spremljanja in merjenja

4.2 Splošna struktura točke

Vsaka točka vsebuje:

a) enega ali več ciljev, navedenih v okvirjenem besedilu na začetku vsake točke, ki navajajo, kaj naj se doseže,

in

b) eno ali več aktivnosti, potrebnih za doseganje cilja ali ciljev te faze.

Vsaka aktivnost je opisana v podtočki.

Opisi aktivnosti v vsaki podtočki so strukturirani na naslednji način:

Aktivnost
Aktivnost določa, kaj je potrebno, da se zadovolji ta aktivnost in dosežejo vsi ali nekaj ciljev te faze.

Vhod
Vhod opiše začetno točko, kot je obstoj dokumentiranih odločitev ali izhodov iz drugih aktivnosti, opisanih v tem mednarodnem standardu. Vhodi so lahko ali sklici na celovit izhod neke aktivnosti z navedbo ustrezne točke ali pa specifična informacija iz aktivnosti, dodana po sklicu na točko.

Napotki
Napotki dajejo podrobne informacije za omogočitev opravljanja te aktivnosti. Nekateri napotki morda niso ustrezni v vseh primerih in so lahko primernejši drugi načini doseganja rezultatov.

Izhod
Izhod opisuje rezultat(-e) ali izdelek(-ke) po končanju aktivnosti, na primer dokument. Izhodi so enaki ne glede na velikost organizacije ali obseg SUIV.

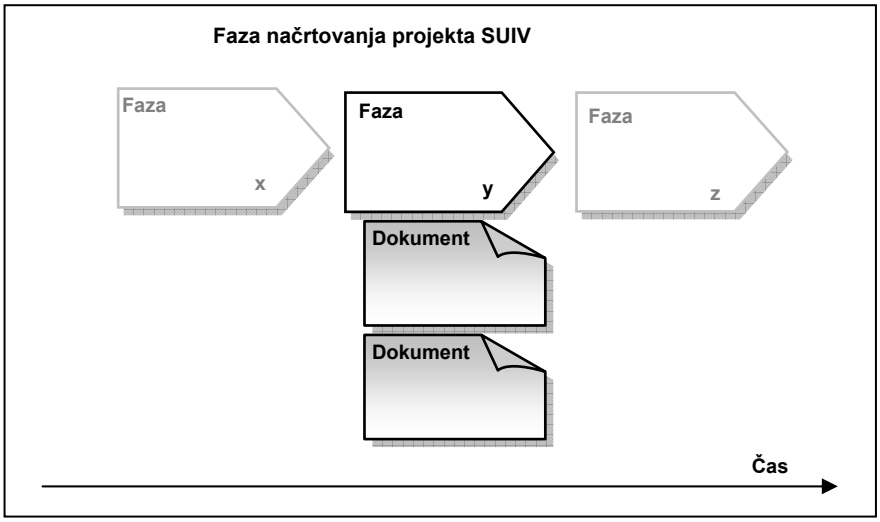
Druge informacije
Druge informacije dajejo morebitne dodatne informacije, ki lahko pomagajo pri opravljanju aktivnosti, na primer sklici na druge standarde.

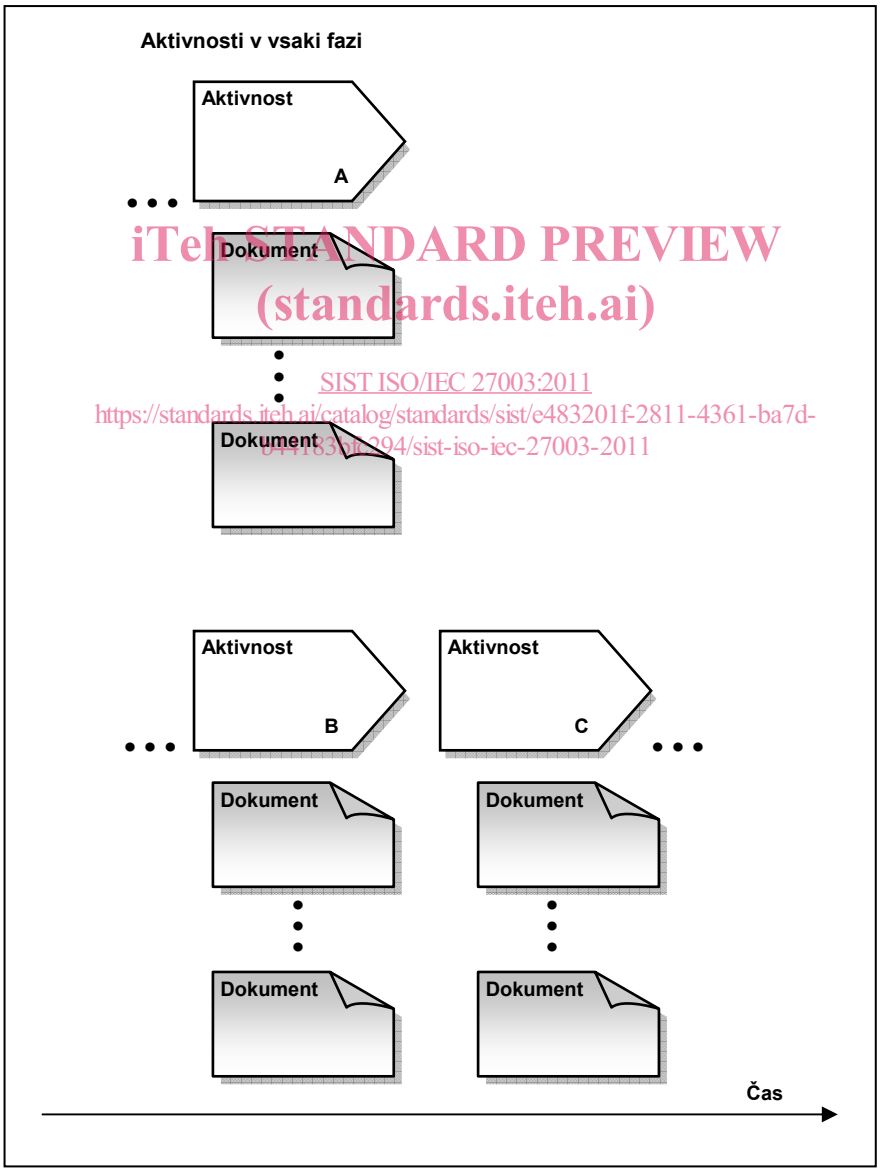
OPOMBA: Faze in aktivnosti, opisane v tem dokumentu, vključujejo predlagano zaporedje opravljanja aktivnosti, ki temeljijo na odvisnostih, ugotovljenih na podlagi opisov vhodov in izhodov vsake aktivnosti. Vendar lahko organizacija v odvisnosti od mnogih različnih dejavnikov (na primer uspešnosti sistema upravljanja, ki je trenutno v uporabi, razumevanja glede pomembnosti informacijske varnosti, razlogov za izvedbo SUIV) izbere katero koli aktivnost v katerem koli vrstnem redu, kot je to potrebno za vzpostavitev in izvedbo SUIV.

4.3 Diagrami

Projekt je pogosto prikazan v grafični obliki ali z diagramom, tako da je prikazan pregled aktivnosti in izhodov.

Slika 2 prikazuje legendo diagramov, ki so prikazani v podtočki pregleda vsake faze. Diagrami nudijo splošen pregled aktivnosti, vključenih v vsaki fazi.





Slika 2: Legenda diagrama pretoka

Zgornji kvadratek prikazuje faze načrtovanja projekta SUIV. Faza, pojasnjena v posamezni točki, je nato poudarjena z njenimi glavnimi izhodnimi dokumenti.

Spodnji diagram (aktivnosti te faze) vključuje glavne aktivnosti, ki so vključene v poudarjeno fazo zgornjega kvadratka, in glavne izhodne dokumente vsake aktivnosti.

Potek časa v spodnjem kvadratku temelji na poteku časa v zgornjem kvadratku.

Aktivnost A in aktivnost B sta lahko izvršeni hkrati. Aktivnost C naj se začne po koncu aktivnosti A in B.

5 Pridobitev odobritve vodstva za uvedbo projekta SUIV

5.1 Pregled pridobivanja odobritve vodstva za uvedbo projekta SUIV

Ko se odloča o izvedbi SUIV, naj se upoštevajo številni dejavniki. Za upoštevanje teh dejavnikov naj vodstvo razume poslovni razlog izvedbe projekta SUIV in naj ga odobri. Tako je cilj te faze:

Cilj:

Pridobiti odobritev vodstva za začetek projekta SUIV z opredelitvijo poslovnega razloga in načrta projekta.

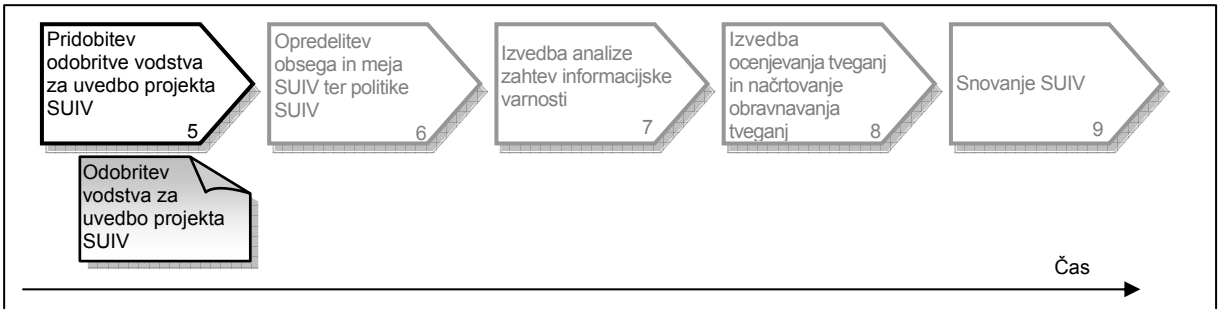
Da organizacija pridobi odobritev vodstva, naj pripravi poslovni razlog, ki vključuje prednostne naloge in cilje za izvedbo SUIV kot dodatek k strukturi organiziranosti SUIV. Pripravi naj tudi začetni načrt projekta SUIV.

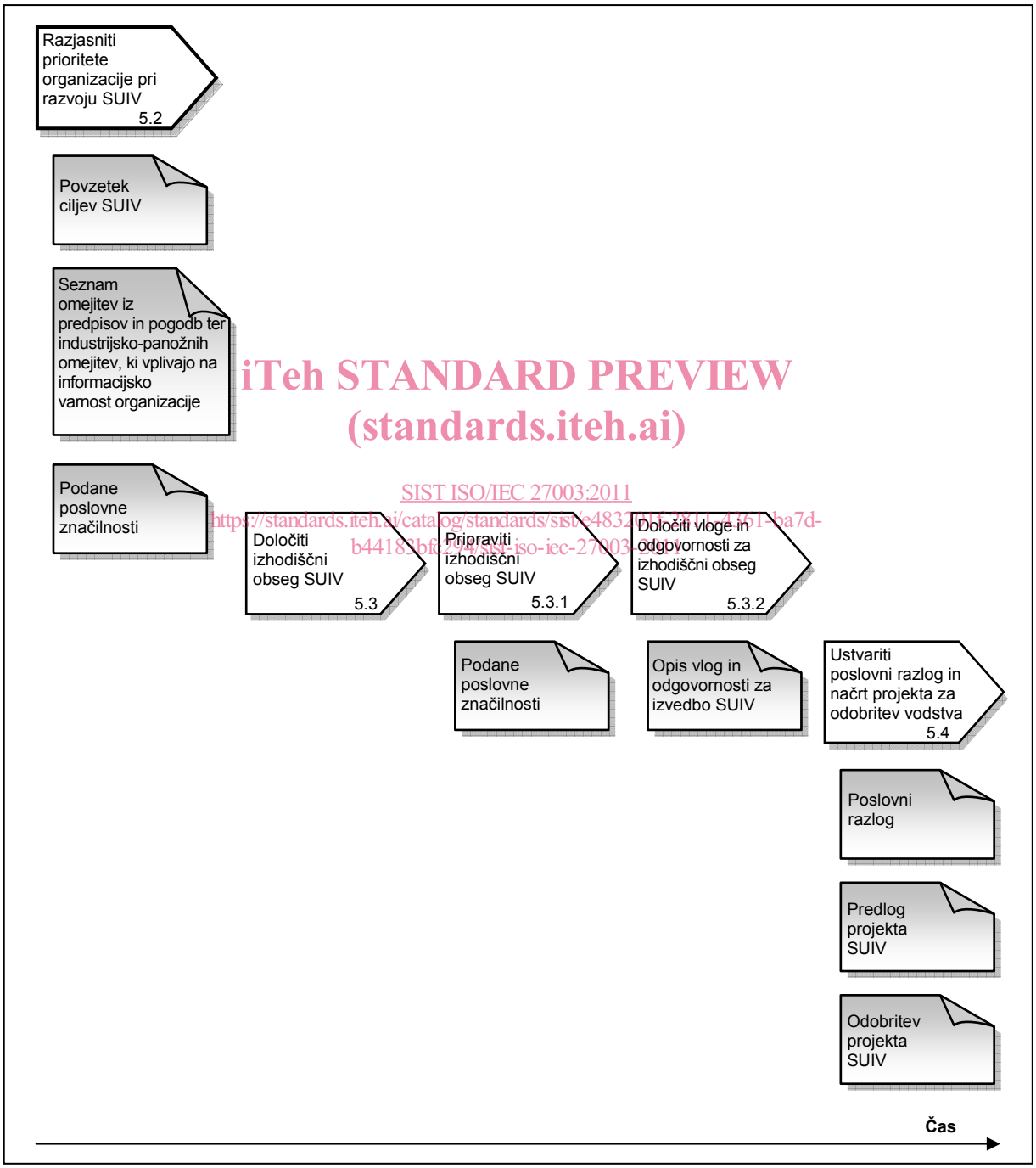
Delo, opravljeno v tej fazi, bo omogočilo organizaciji razumeti pomembnost SUIV ter razjasnilo vloge in odgovornosti informacijske varnosti v organizaciji, potrebne za projekt SUIV.

Pričakovani izhod iz te faze bosta predhodna odobritev vodstva ter njegova zavezanost k izvedbi SUIV in opravljanju aktivnosti, opisanih v tem mednarodnem standardu. Izdelki te točke vključujejo poslovni razlog in osnutek načrta projekta SUIV z glavnimi mejniki.

Slika 3 prikazuje proces pridobivanja odobritve vodstva za uvedbo projekta SUIV.

OPOMBA: Izhod točke 5 (dokumentirana zavezanost vodstva k načrtovanju in izvedbi SUIV) in eden od izhodov točke 7 (povzemanje dokumentov s statusom informacijske varnosti) nista zahtevi ISO/IEC 27001:2005. Vendar sta ta dva izhoda priporočena vhoda za druge aktivnosti, opisane v tem dokumentu.





Slika 3: Pregled pridobivanja odobritve vodstva za začetek projekta SUIV

5.2 Razjasniti prioritete organizacije pri razvoju SUIV

Aktivnost
Na podlagi določitve prioritet in zahtev informacijske varnosti organizacije naj se vključijo cilji izvedbe SUIV.

Vhod

a) Strateški cilji organizacije,

b) pregled obstoječih sistemov upravljanja,

c) seznam zakonodajnih, regulatornih in pogodbenih zahtev informacijske varnosti, ki veljajo za organizacijo.

Napotki
Za začetek projekta SUIV je v splošnem potrebna odobritev vodstva. Zato je prva aktivnost, ki naj se opravi, zbiranje ustreznih informacij, ki prikazujejo pomen SUIV za organizacijo. Organizacija naj razjasni, zakaj potrebuje SUIV, določi cilje izvedbe SUIV in zasnuje projekt SUIV.

Cilje izvedbe SUIV je mogoče določiti z odgovori na naslednja vprašanja:

a) upravljanje tveganj – kako bo SUIV izboljšal upravljanje informacijskih varnostnih tveganj,

b) učinkovitost – kako je mogoče s SUIV izboljšati upravljanje informacijske varnosti,

c) poslovne prednosti – kako je s SUIV mogoče ustvariti konkurenčno prednost za organizacijo.

Da organizacija odgovori na gornja vprašanja, upošteva pri prioritetah in varnostnih zahtevah naslednje možne dejavnike:

a) kritična poslovna in organizacijska področja:

   1. Katera poslovna in organizacijska področja so kritična?
   2. Katera organizacijska področja ustvarjajo posel in na kaj so osredotočena?
   3. Kateri odnosi in sporazumi s tretjimi strankami obstajajo?
   4. Ali obstajajo storitve v zunanjem izvajanju?

b) občutljive in dragocene informacije:

   1. Katere informacije so kritične za organizacijo?
   2. Kakšne bi bile verjetne posledice, če bi se določene informacije razkrile nepooblaščenim osebam (na primer izguba konkurenčne prednosti, škoda za blagovne znamke in ugled, pravni postopki itd.)?

c) zakoni, ki določajo ukrepe na področju informacijske varnosti:

   1. Kateri zakoni, ki se nanašajo na obravnavo tveganj ali informacijsko varnost, veljajo za organizacijo?
   2. Ali je organizacija del javne globalne organizacije, za katero veljajo zahteve za zunanje finančno poročanje?

d) pogodbeni ali organizacijski sporazumi v zvezi z informacijsko varnostjo:

   1. Kakšne so zahteve za hrambo podatkov (vključujoč roke hrambe)?
   2. Ali obstajajo pogodbene zahteve, ki se nanašajo na zasebnost ali kakovost (na primer sporazumi o ravni storitev – SLA)?

e) industrijsko-panožne zahteve, ki določajo posebne kontrole in ukrepe za informacijsko varnost:

   1. Katere specifične panožne zahteve veljajo za organizacijo?

f) okolje groženj:
   1. Kakšna zaščita je potrebna in proti katerim grožnjam?
   2. Katere različne kategorije informacij zahtevajo zaščito?
   3. Katere različne informacijske aktivnosti morajo biti zaščitene?

g) konkurenčne gonilne sile:
   1. Katere so na trgu minimalne zahteve informacijske varnosti?
   2. Katere dodatne kontrole informacijske varnosti naj bi omogočale konkurenčno prednost za organizacijo?

h) zahteve za neprekinjeno poslovanje:
   1. Kateri poslovni procesi so kritični?
   2. Kako dolgo lahko organizacija prenaša prekinitve posameznih kritičnih poslovnih procesov?

Na podlagi odgovorov na gornje informacije je mogoče določiti izhodiščni obseg SUIV. Ta je potreben tudi za postavitev poslovnega razloga in celovitega načrta projekta SUIV za pridobitev odobritve vodstva. Podroben obseg SUIV bo določen med izvajanjem projekta SUIV.

Zahteve, navedene v ISO/IEC 27001:2005, točka 4.2.1.a), postavljajo obseg glede na značilnosti poslovanja, organizacije, njene lokacije, dobrin in tehnologije. Iz tega izhajajoče informacije podpirajo to določitev.

Pri postavljanju začetnih odločitev o obsegu naj se razmisli o temah, med katerimi so:

a) Katere naloge vodstvo organizacije postavlja vodstvu informacijske varnosti in katere so zunanje obveznosti organizacije?

b) Ali je odgovornost za predlagane sisteme v obsegu naložena več kot eni vodstveni ekipi (na primer ljudem v različnih hčerinskih družbah ali oddelkih)?

c) Kako se bodo dokumenti v zvezi s SUIV razširjali po organizaciji (na primer na papirju ali z intranetom organizacije)?

d) Ali lahko sedanji sistemi upravljanja podpirajo potrebe organizacije? Ali so v celoti operativni, dobro vzdrževani in delujejo, kot je bilo zamišljeno?

Primeri ciljev vodstva, ki so lahko uporabljeni kot vhod za določitev izhodiščnega obsega SUIV, vključujejo:

a) spodbujanje neprekinjenega poslovanja in okrevanja po katastrofi,
b) izboljševanje odpornosti proti incidentom,
c) obravnavanje zakonskih/pogodbenih zahtev/obveznosti,
d) omogočanje certificiranja po standardih ISO/IEC,
e) omogočanje razvoja in položaja organizacije,
f) zmanjševanje cene varnostnih kontrol,
g) zaščito dobrin s strateško vrednostjo,
h) ustanovitev zdravega in uspešnega okolja notranjih kontrol,
i) zagotavljanje zainteresiranim strankam, da so informacijske dobrine ustrezno zaščitene.

Izhod
Izdelki te aktivnosti so:

a) dokument, ki povzema cilje, prioritete informacijske varnosti in organizacijske zahteve za SUIV,

b) seznam zakonodajnih, pogodbenih in industrijsko-panožnih zahtev v zvezi z informacijsko varnostjo organizacije,

c) podane značilnosti poslovanja, organizacije, njene lokacije, dobrin in tehnologije.

Druge informacije
ISO/IEC 9001:2008, ISO/IEC 14001:2004, ISO/IEC 20000-1:2005.

5.3 Določiti izhodiščni obseg SUIV

5.3.1 Pripraviti izhodiščni obseg SUIV

Aktivnost
Cilji izvedbe SUIV naj vključujejo določitev izhodiščnega obsega SUIV, ki je potreben za projekt SUIV.

Vhod
Izhod iz aktivnosti 5.2 Razjasniti prioritete organizacije pri razvoju SUIV

Napotki
Da bi projekt izvedbe SUIV potekal, naj se določi struktura organizacije SUIV. Sedaj naj se določi izhodiščni obseg SUIV, da se vodstvu zagotovijo napotki za izvedbene odločitve in da se podprejo aktivnosti, ki sledijo.

Izhodiščni obseg SUIV je potreben za ustvarjanje poslovnega razloga in predloga načrta projekta za odobritev vodstva.

Izhod tega koraka bo dokument, ki določa izhodiščni obseg SUIV in vključuje:

a) povzetek nalog, ki jih vodstvo organizacije podaja vodstvu informacijske varnosti, zunanjih obveznosti organizacije,

b) opis, kako področje(-a) v obsegu sodeluje(-jo) z drugimi sistemi upravljanja,

c) seznam poslovnih ciljev vodstva informacijske varnosti (kot določa točka 5.2),

d) seznam kritičnih poslovnih procesov, sistemov, informacijskih dobrin, organizacijskih struktur in geografskih lokacij, na katere se bo SUIV nanašal,

e) odnos med obstoječimi upravljavskimi sistemi, predpisi, določili skladnosti in cilji organizacije,

f) značilnosti poslovanja, organizacije, njene lokacije, dobrin in tehnologije.

Prepoznajo naj se skupni elementi in operativne razlike med procesi vseh obstoječih upravljavskih sistemov in predlaganega SUIV.

Izhod
Izdelek je dokument, ki opisuje izhodiščni obseg SUIV.

Druge informacije
Ni drugih specifičnih informacij.

OPOMBA: Posebna pozornost naj bo posvečena izpolnitvi specifičnih certifikacijskih zahtev za dokumentacijo ISO/IEC 27001:2005 v zvezi z obsegom SUIV, ko morajo biti te izpolnjene ne glede na delujoče upravljavske sisteme v organizaciji.

5.3.2 Določiti vloge in odgovornosti za izhodiščni obseg SUIV

Aktivnost
Določijo naj se splošne vloge in odgovornosti za izhodiščni obseg SUIV.