Standardi, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT

- **Kodeks poklicne etike**
- **Standardi, smernice ter orodja in tehnike za strokovnjake revidiranja in dajanja zagotovil na področju IT**
- **Standardi za strokovnjake na področju kontrol IS**

ISACA®
Zaupanje v informacijske sisteme in korist od njih
Slovenia Chapter

V veljavi od 16. avgusta 2010

ISACA

Standards Disclaimer

ISACA has designed this guidance as of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA *Code of Professional Ethics* for IT audit and assurance professionals. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the security and control professional should apply his/her own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Izjava o neprevzemanju odgovornosti za standarde

ISACA je oblikovala ta navodila glede najnižje še sprejemljive ravni uspešnosti pri izpolnjevanju strokovnih nalog in odgovornosti, določenih v Kodeksu poklicne etike ISACA za strokovnjake za revidiranje in dajanje zagotovil za IT. ISACA ne trdi, da bo uporaba teh navodil zagotovila uspešen izid. Tega gradiva ne smete razumeti kot delo, ki vključuje vse ustrezne informacije, postopke in preizkuse, ali kot delo, ki izključuje vse druge informacije, postopke in preizkuse, ki so razumno usmerjeni k pridobivanju istih rezultatov. Pri ugotavljanju ustreznosti določene informacije, postopka ali preizkusa mora strokovnjak za varnost in kontrolo uporabljati lastno strokovno presojo posameznih okoliščin, ki jih predstavljajo določeni sistemi ali okolje informacijske tehnologije.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telefon: +1.847.253.1545
Faks: +1.847.253.1443
E-naslov: *standards@isaca.org*
Spletna stran: *www.isaca.org*

Vsebina

Kodeks poklicne etike

Združenje ISACA postavlja *Kodeks poklicne etike* kot vodilo za strokovno in osebno ravnanje članov združenja in/ali imetnikov licence ISACA.

Člani in imetniki licence ISACA:

1. podpirajo vpeljavo ustreznih standardov, postopkov in kontrol za informacijske sisteme in spodbujajo skladnost z njimi;

2. opravljajo svoje naloge skrbno, vestno in strokovno v skladu s strokovnimi standardi in najboljšimi praksami;

3. delujejo zakonito in pošteno v korist zainteresiranih, ob tem pa vzdržujejo visoke standarde obnašanja in osebnostnih lastnosti ter se izogibajo dejanjem, ki bi lahko škodovala ugledu stroke;

4. varujejo zasebnost in zaupnost informacij, pridobljenih med opravljanjem svojih nalog, razen če razkritje zahteva zakonodaja. Takih informacij ne smejo uporabljati za osebne koristi ali jih razkrivati neprimernim osebam;

5. ohranjajo strokovno usposobljenost na svojih področjih in prevzemajo samo tiste naloge, za katere lahko upravičeno pričakujejo, da jih bodo opravili strokovno neoporečno;

6. obveščajo ustrezne stranke o rezultatih opravljenega dela, pri čemer jim razkrijejo vsa pomembna in znana dejstva;

7. zaradi izboljšanja razumevanja varnosti in kontrol informacijskih sistemov podpirajo strokovno izobraževanje zainteresiranih.

V primeru neizpolnjevanja *Kodeksa poklicne etike* se lahko proti članu ISACA ali imetniku njene licence uvede preiskava o njegovem ravnanju in se na koncu lahko izreče tudi disciplinski ukrep.

Kako uporabljati to gradivo?

Razmerje standardov do smernic ter orodij in tehnik

Standardi revidiranja in dajanja zagotovil za IT so obvezne zahteve za poročila imetnikov licence o reviziji in njenih ugotovitvah. Smernice ter orodja in tehnike revidiranja in dajanja zagotovil za IT so podrobna navodila za izvajanje teh standardov. Smernice revidiranja in dajanja zagotovil za IT so navodila, po katerih se bo strokovnjak za revidiranje in dajanje zagotovil za IT običajno ravnal, pri čemer pa je treba razumeti, da lahko obstajajo tudi okoliščine, v katerih se revizor ne bo ravnal po teh navodilih. V takem primeru bo strokovnjak za revidiranje in dajanje zagotovil za IT moral utemeljiti način svojega dela. Primeri orodij in tehnik ponazarjajo korake, ki jih opravi strokovnjak za revidiranje in dajanje zagotovil za IT in so bolj informativni kot smernice revidiranja in dajanja zagotovil za IT. Primeri so sestavljeni tako, da sledijo standardom revidiranja in dajanja zagotovil za IT in smernicam revidiranja in dajanja zagotovil za IT ter obveščajo o tem, kako slediti standardom revidiranja in dajanja zagotovil za IT. V določeni meri predstavljajo tudi najboljše prakse za postopke, ki jih je treba izvajati.

Označevanje

Standardi so oštevilčeni po zaporedju njihovega izdajanja od S1 dalje.
Smernice so oštevilčene po zaporedju njihovega izdajanja od G1 dalje.
Orodja in tehnike so oštevilčeni po zaporedju njihovega izdajanja od P1 dalje.

Uporaba

Pričakuje se, da ob pripravi letnega revizijskega programa kakor tudi ob posameznih pregledih med letom strokovnjak za revidiranje in dajanje zagotovil za IT pregleda standarde, da zagotovi skladnost z njimi. Strokovnjak za revidiranje in dajanje zagotovil za IT se v svojem poročilu lahko sklicuje na standarde ISACA in navede, da je bil pregled opravljen v skladu z domačo zakonodajo, ustreznimi revizijskimi predpisi in standardi ISACA.

Elektronski prepisi

Vsi standardi ISACA ter smernice in postopki so na voljo tudi na spletni strani ISACA na naslovu *www.isaca.org/standards*.

Glosar

Celoten glosar izrazov lahko najdete na spletni strani ISACA na naslovu *www.isaca.org/glossary*.

Pregled standardov revidiranja in dajanja zagotovil za IT

Izdala jih je ISACA.

Posebnosti revidiranja in dajanja zagotovil za informacijsko tehnologijo (IT) in veščine, ki so potrebne za izvajanje takih revizij, zahtevajo standarde, ki veljajo posebej za revidiranje in dajanje zagotovil za IT. Eden od ciljev mednarodnega združenja ISACA® je razvoj globalno uporabnih standardov za uresničevanje njegove vizije. Razvoj in razširjanje standardov revidiranja in dajanja zagotovil za IT je temelj strokovnega prispevka združenja ISACA skupnosti, ki izvaja revidiranje in daje zagotovila. Navodila so sestavljena na več ravneh:

- **Standardi** določajo obvezne zahteve za revidiranje in dajanje zagotovil za IT. Obveščajo:
  - strokovnjake za revidiranje in dajanje zagotovil za IT o najnižji še sprejemljivi ravni izpolnjevanja strokovnih nalog in odgovornosti, določenih v Kodeksu poklicne etike ISACA,
  - poslovodstvo in druge zainteresirane stranke o pričakovanjih stroke glede dela strokovnih delavcev,
  - nosilce naziva preizkušeni revizor informacijskih sistemov™ (CISA®) o zahtevah. V primeru neizpolnjevanja teh standardov lahko upravni odbor ISACA ali ustrezen odbor ISACA uvede preiskavo o ravnanju imetnika licence CISA in na koncu izreče tudi disciplinski ukrep.
- **Smernice** dajejo navodila za uporabo standardov revidiranja in dajanja zagotovil za IT. Strokovnjak za revidiranje in dajanje zagotovil za IT naj jih upošteva pri odločanju o tem, kako doseči uveljavitev standardov, uporabiti strokovno presojo pri njihovi uporabi in biti pripravljen utemeljiti vsako odstopanje. Namen smernic revidiranja in dajanja zagotovil za IT je dati nadaljnje informacije o tem, kako ravnati v skladu s standardi revidiranja in dajanja zagotovil za IT.
- **Orodja in tehnike** ponujajo primere postopkov, ki jih lahko upošteva strokovnjak za revidiranje in dajanje zagotovil za IT. Gradivo o orodjih in tehnikah daje informacije o tem, kako je pri izvajanju revidiranja in dajanja zagotovil za IT mogoče izpolnjevati standarde, ne postavlja pa nobenih zahtev. Namen orodij in tehnik revidiranja in dajanja zagotovil za IT je dati nadaljnje informacije o tem, kako ravnati v skladu s standardi revidiranja in dajanja zagotovil za IT.

COBIT® je okvir za upravljanje IT in sklop podpornih orodij, ki vodstvu omogočajo premostitev vrzeli med kontrolnimi zahtevami, tehničnimi vprašanji in poslovnimi tveganji. COBIT omogoča razvoj jasnih politik in dobre prakse za kontrolo IT v podjetjih. Poudarja skladnost s predpisi, pomaga podjetjem povečati vrednost, pridobljeno iz IT, omogoča usklajevanje in poenostavlja uvajanje zasnov okvira COBIT. COBIT je namenjen poslovnemu vodstvu in vodstvu IT ter strokovnjakom za revidiranje in dajanje zagotovil za IT; njegova uporaba torej omogoča razumevanje poslovnih ciljev in sporočanje dobrih praks in priporočil, ki se oblikujejo okrog vsem razumljivega in dobro sprejetega okvira. COBIT je na voljo za prenos na spletnem mestu ISACA (*www.isaca.org/cobit)*. Kot je opredeljeno v okviru COBIT, je v procesu upravljanja IT organiziran vsak od spodaj naštetih dejavnikov oziroma elementov:

- Kontrolni cilji — splošne trditve o najmanjši še dobri kontroli v povezavi s procesi IT.
- Smernice za poslovodstvo — navodila, kako oceniti in izboljšati izvajanje procesa IT z uporabo zrelostnih modelov, preglednic ZOPS (zadolžen, odgovoren, posvetovan oz. seznanjen), ciljev in metrik. Zagotavljajo poslovodstvu namenjen okvir za nenehno in dejavno samoocenjevanje kontrol, ki je posebej usmerjeno v:
  - merjenje zmogljivosti,
  - profiliranje kontrol IT,
  - ozaveščanje,
  - primerjanje.
- *Kontrolne prakse COBIT* — trditve o tveganju in vrednosti ter 'kako vpeljati' smernice za kontrolne cilje.
- *Vodič dajanja zagotovil v IT* — navodila za vsako področje kontroliranja o tem, kako pridobiti razumevanje, kako ovrednotiti vsako kontrolo, oceniti skladnost in utemeljiti tveganje, če kontrole ni.

Glosar izrazov je na voljo na spletnem mestu ISACA na naslovu *www.isaca.org/glossary*. Besedi revizija in pregled se v standardih, smernicah ter orodjih in tehnikah revidiranja in dajanja zagotovil za IT uporabljata izmenljivo.

Izjava o neprevzemanju odgovornosti: ISACA je oblikovala ta navodila glede na najnižje še sprejemljive ravni izpolnjevanja strokovnih nalog in odgovornosti, določenih v Kodeksu poklicne etike ISACA za strokovnjake za revidiranje in dajanje zagotovil za IT. ISACA ne zagotavlja, da bo uporaba teh navodil zagotovila uspešen izid. Tega gradiva ne smete razumeti kot delo, ki vključuje vse ustrezne postopke in preizkuse, ali kot delo, ki izključuje vse druge postopke in preizkuse, ki so razumno usmerjeni k pridobivanju istih rezultatov. Pri ugotavljanju ustreznosti določenega postopka ali preizkusa mora strokovnjak za kontrolo uporabiti lastno strokovno presojo posameznih kontrolnih okoliščin, ki jih predstavljajo določeni sistemi ali okolje IT.

Odbor ISACA za strokovne standarde si pri pripravi standardov, smernic ter orodij in tehnik revidiranja in dajanja zagotovil za IT prizadeva za posvetovanja v najširšem krogu. Pred izdajo vsakega dokumenta izda odbor za standarde osnutek v mednarodno javno obravnavo in zbira pripombe širše javnosti. Po potrebi odbor za strokovne standarde tudi poišče in povabi na posvetovanje strokovnjake, ki posebej dobro poznajo ali se zanimajo za obravnavano področje. Odbor za standarde ima stalen razvojni program in pozdravlja prispevke članov ISACA in druge zainteresirane stranke, da zazna nove izzive, ki zahtevajo nove standarde. Vse predloge lahko pošljete po e-pošti (*standards@isaca.org*), telefaksu (+1.847. 253.1443) ali jih po pošti naslovite na "ISACA International Headquarters, for the attention of the Val IT initiative manager" (naslov je na koncu gradiva).

Seznam standardov revidiranja in dajanja zagotovil za IT

	Datum uveljavitve
S1 Revizijska listina	1. januar 2005
S2 Neodvisnost	1. januar 2005
S3 Poklicna etika in standardi	1. januar 2005
S4 Strokovna usposobljenost	1. januar 2005
S5 Načrtovanje	1. januar 2005
S6 Izvajanje revizijskih del	1. januar 2005
S7 Poročanje	1. januar 2005
S8 Nadaljnja obravnava	1. januar 2005
S9 Nepravilnosti in nezakonita dejanja	1. september 2005
S10 Upravljanje IT	1. september 2005
S11 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju	1. november 2005
S12 Revizijska pomembnost	1. julij 2006
S13 Uporaba dela drugih strokovnjakov	1. julij 2006
S14 Revizijski dokazi	1. julij 2006
S15 Kontrole IT	1. februar 2008
S16 E-poslovanje	1. februar 2008

Seznam smernic revidiranja in dajanja zagotovil za IT

G1 Uporaba dela drugih strokovnjakov	1. junij 1998,	prenovljena 1. marca 2008
G2 Zahteva za revizijske dokaze	1. december 1998,	prenovljena 1. maja 2008
G3 Uporaba računalniško podprtih tehnik revidiranja (CAAT)	1. december 1998,	prenovljena 1. marca 2008
G4 Zunanje izvajanje dejavnosti IS	1. september 1999,	prenovljena 1. maja 2008
G5 Revizijska listina	1. september 1999,	prenovljena 1. februarja 2008
G6 Načela pomembnosti za revidiranje informacijskih sistemov	1. september 1999,	prenovljena 1. maja 2008
G7 Potrebna poklicna skrbnost	1. september 1999,	prenovljena 1. marca 2008
G8 Revizijska dokumentacija	1. september 1999,	prenovljena 1. marca 2008
G9 Revizorjeva obravnava in presoja nepravilnosti in nezakonitih dejanj	1. marec 2000,	prenovljena 1. septembra 2008
G10 Revizijsko vzorčenje	1. marec 2000,	prenovljena 1. avgusta 2008
G11 Učinek vseobsegajočih kontrol IS	1. marec 2000,	prenovljena 1. avgusta 2008
G12 Organizacijsko razmerje in neodvisnost	1. september 2000,	prenovljena 1. avgusta 2008
G13 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju	1. september 2000,	prenovljena 1. avgusta 2008
G14 Pregled aplikacijskih sistemov	1. november 2001,	prenovljena 1. oktobra 2008
G15 Revizijsko načrtovanje, prenovljena	1. maj 2010	
G16 Učinek tretjih strank na kontrole IT v podjetju	1. marec 2009	
G17 Učinek nerevizijske vloge na neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT	1. maj 2010	
G18 Upravljanje IT	1. julij 2002	
~~G19 Nepravilnosti in nezakonita dejanja 1. julij 2002~~	Umaknjena	1. septembra 2008
G20 Poročanje	1. januar 2003	
G21 Pregled sistemov celovitih programskih rešitev (ERP)	1. avgust 2003	
G22 Pregled e-poslovanja s strankami (B2C)	1. avgust 2003,	prenovljena 1. oktobra 2008
G23 Pregledi življenjskega cikla razvoja sistemov (SDLC)	1. avgust 2003	
G24 Spletno bančništvo	1. avgust 2003	
G25 Pregled navideznih zasebnih omrežij	1. julij 2004	
G26 Pregledi projektov prenove poslovnega procesa (BPR)	1. julij 2004	
G27 Mobilno računalništvo	1. september 2004	
G28 Računalniška forenzika	1. september 2004	
G29 Pregled po uvedbi	1. januar 2005	
G30 Strokovna usposobljenost	1. junij 2005	
G31 Zasebnost	1. junij 2005	
G32 Pregled načrta neprekinjenega poslovanja (BCP) z vidika IT	1. september 2005	
G33 Splošna obravnava in presoja o uporabi interneta	1. marec 2006	
G34 Zadolžitve, pristojnosti in odgovornost	1. marec 2006	
G35 Nadaljnja obravnava	1. marec 2006	
G36 Biometrične kontrole	1. februar 2007	
G37 Proces upravljanja konfiguracije	1. november 2007	
G38 Kontrole dostopa	1. februar 2008	
G39 Organizacija IT	1. maj 2008	
G40 Pregled praks upravljanja varnosti	1. oktober 2008	
G41 Donosnost naložb v varnost (ROSI)	1. maj 2010	
G42 Stalno dajanje zagotovil	1. maj 2010	

Seznam orodij in tehnik revidiranja in dajanja zagotovil za IT

P1 Ocenjevanje in vrednotenje tveganja IS	1. julij	2002
P2 Elektronski podpisi in upravljanje ključev	1. julij	2002
P3 Pregled sistema za zaznavanje vdorov	1. avgust	2003
P4 Virusi in druga zlonamerna koda	1. avgust	2003
P5 Samoocena tveganja pri kontroliranju	1. avgust	2003
P6 Požarni zidovi	1. avgust	2003
P7 Nepravilnosti in nezakonita dejanja	1. november	2003
P8 Varnostna ocena — penetracijsko testiranje in analiza ranljivosti	1. september	2004
P9 Ovrednotenje kontrol poslovodstva nad metodologijami šifriranja	1. januar	2005
P10 Kontrola sprememb poslovne aplikacije	1. oktober	2006
P11 Elektronski prenos sredstev (EFT)	1. maj	2007

Standardi revidiranja in dajanja zagotovil za IT

Izdala jih je ISACA. Prevodi teh standardov so dostopni na *www.isaca.org/standardstranslations*.

S1 Revizijska listina

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti in dati navodila v zvezi z revizijsko listino, ki se uporablja med revizijskim procesom.

Standard

03 Namen, zadolžitve, pristojnosti in odgovornost funkcije revidiranja informacijskih sistemov ali poslov revidiranja informacijskih sistemov morajo biti ustrezno dokumentirane v revizijski listini ali listini o poslu.

04 Revizijska listina ali listina o poslu mora biti dogovorjena in odobrena na ustrezni ravni v organizaciji(ah).

Komentar

05 Za funkcijo notranje revizije informacijskih sistemov naj bo revizijska listina pripravljena za redne dejavnosti. Revizijsko listino je treba pregledati vsaj enkrat letno ali pogosteje, če se zadolžitve razlikujejo ali spreminjajo. Listino o poslu lahko uporabi notranji revizor IS, da dodatno pojasni ali potrdi vključevanje v določene revizijske ali nerevizijske naloge. Za zunanjo revizijo IS je treba listino o poslu običajno pripraviti za vsak revizijski ali nerevizijski posel posebej.

06 Revizijska listina ali listina o poslu naj bo sestavljena dovolj podrobno, da so iz nje razvidni namen, zadolžitve in omejitve revizijske funkcije ali revizijskega posla.

07 Revizijsko listino ali listino o poslu je treba redno pregledovati, da se zagotovi, da so namen in naloge dokumentirani.

08 Nadaljnje informacije o pripravi revizijske listine ali listine o poslu lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G5 *Revizijska listina,*
- *Okvir* CobiT, kontrolni cilj M4 (CobiT3).

Datum uveljavitve

09 Ta standard ISACA velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005 ali pozneje.

S2 Neodvisnost

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti standarde in navodila o neodvisnosti med revizijskim procesom.

Standard

03 Strokovna neodvisnost

Revizor IS mora biti zaznan kot neodvisen in delovati neodvisno od revidiranca v vseh zadevah, povezanih z revizijo.

04 Organizacijska neodvisnost

Funkcija revidiranja IS mora biti neodvisna od področja ali dejavnosti, ki se pregleduje, tako da je mogoče nepristransko dokončanje revizijske naloge.

Komentar

05 Revizijska listina ali listina o poslu naj obravnava tudi neodvisnost in odgovornost revizijske funkcije.

06 Revizor IS naj vedno deluje neodvisno in daje videz neodvisnosti.

07 Če je neodvisnost dejansko oslabljena ali je videti oslabljena, je treba podrobnosti oslabitve razkriti ustreznim strankam.

08 Revizor IS naj bo organizacijsko neodvisen od področja, ki se revidira.

09 Neodvisnost naj redno ocenjujejo revizor IS ter poslovodstvo in revizijska komisija, kadar obstaja.

10 Če tega ne prepovedujejo drugi strokovni standardi ali regulativni organi, se za revizorja IS ne zahteva, da je neodvisen ali da ga drugi tako zaznavajo, kadar se v pobudo IS vključuje z opravljanjem nerevizijske vloge.

11 Nadaljnje informacije o strokovni ali organizacijski neodvisnosti lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G17 *Učinek nerevizijske vloge na neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT*,
- smernica za revidiranje informacijskih sistemov G12 *Organizacijsko razmerje in neodvisnost*,
- *Okvir* CobiT, kontrolni cilj M4 (CobiT 3).

Datum uveljavitve

12 Ta standard ISACA velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S3 Poklicna etika in standardi

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti standard in dati revizorju IS navodilo, naj upošteva Kodeks poklicne etike ISACA in skrbi za poklicno skrbnost pri opravljanju revizijskih nalog.

Standard

05 Revizor IS mora pri opravljanju revizijskih nalog dosledno upoštevati Kodeks poklicne etike ISACA.

06 Revizor IS mora pri opravljanju revizijskih nalog zagotavljati potrebno poklicno skrbnost, vključno z upoštevanjem ustreznih strokovnih revizijskih standardov.

Komentar

07 Kodeks poklicne etike, ki ga je izdala ISACA, bo občasno spremenjen in dopolnjen, tako da bo sledil novim usmeritvam in zahtevam revizijske stroke. Člani ISACA in revizorji IS naj bodo seznanjeni z najnovejšo izdajo Kodeksa poklicne etike in se pri opravljanju svojih nalog kot revizorji IS po njem ravnajo.

08 Standardi revidiranja IS, ki jih je izdala ISACA, se redno pregledujejo in dopolnjujejo zaradi stalnih izboljšav, tako da sledijo novim izzivom v revizijski stroki. Člani ISACA in revizorji IS naj poznajo zadnje veljavne standarde revidiranja IS in pri opravljanju revizijskih nalog skrbijo za potrebno poklicno skrbnost.

09 Če član ISACA ali imetnik licence CISA ne ravna s skladu s Kodeksom poklicne etike ISACA in/ali standardi revidiranja IS, se proti njemu lahko uvede preiskava in na koncu tudi izrečejo disciplinski ukrepi.

10 Člani ISACA in revizorji IS naj se dogovarjajo s člani svoje skupine in zagotovijo, da se cela skupina ravna po Kodeksu poklicne etike in pri opravljanju revizijskih nalog upošteva ustrezne standarde revidiranja IS.

11 Revizorji IS naj ustrezno rešujejo vse zadeve, ki se med opravljanjem revizijske naloge pojavijo v zvezi z uporabo poklicne etike ali standardov revidiranja IS. Če je spoštovanje poklicne etike ali standardov revidiranja IS oslabljeno ali se zdi oslabljeno, naj revizor IS preuči možnost, da od posla odstopi.

12 Revizor IS naj pri svojem ravnanju ohrani najvišjo stopnjo neoporečnosti in ravnanja in za pridobitev ali izvedbo revizijskih nalog ne uporablja nobenih metod, ki bi bile lahko videti nezakonite, neetične ali nestrokovne.

11 Nadaljnje informacije o poklicni etiki in standardih lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G19 *Nepravilnosti in nezakonita dejanja*,
- smernica za revidiranje informacijskih sistemov G7 *Potrebna poklicna skrbnost*,
- smernica za revidiranje informacijskih sistemov G12 *Organizacijsko razmerje in neodvisnost*,
- *Okvir* CobiT, kontrolni cilj M4 (COBIT 3).

Datum uveljavitve

12 Ta standard za revidiranje IS velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S4 Strokovna usposobljenost

Uvod

01 Standardi ISACA za revidiranje IS vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti in dati navodilo, da se od revizorja IS zahteva, da doseže in vzdržuje strokovno usposobljenost.

Standard

03 Revizor IS mora biti strokovno usposobljen in imeti veščine in znanje za izvajanje revizijske naloge.

04 Revizor IS mora vzdrževati svojo strokovno usposobljenost z ustreznim stalnim strokovnim izobraževanjem in usposabljanjem.

Komentar

05 Preden revizor IS začne delo, naj predloži sprejemljiva zagotovila, da ima zadostne strokovne sposobnosti (veščine, znanje in izkušnje, pomembne za načrtovano nalogo). Če jih nima, naj revizor IS nalogo odkloni ali od nje odstopi.

06 Če ima revizor IS licenco CISA ali druge z revizijo povezane strokovne nazive, naj izpolnjuje njihove zahteve po stalnem strokovnem izobraževanju ali razvoju. Člani ISACA, ki nimajo licence CISA ali drugega z revizijo povezanega strokovnega naziva in so vključeni v revidiranje informacijskega sistema, naj imajo zadostno formalno izobrazbo in raven strokovne usposobljenosti ter delovnih izkušenj.

07 Kadar revizor IS vodi skupino za opravljanje pregleda, naj priskrbi sprejemljiva zagotovila, da imajo vsi člani ustrezno stopnjo strokovne usposobljenosti za delo, ki ga opravljajo.

08 Nadaljnje informacije o strokovni usposobljenosti lahko najdete v naslednjih navodilih:

- gradiva za pridobitev naziva CISA in učno gradivo CISA,
- podaljšanje licence CISA in zahteve po izobraževanju,
- *Okvir* CobiT, kontrolni cilji M2, M3 in M4 (CobiT3).

Datum uveljavitve

09 Ta standard za revidiranje IS velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S5 Načrtovanje

Uvod

01 Standardi ISACA za revidiranje IS vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti standarde in dati navodila za načrtovanje revizije.

Standard

03 Revizor IS mora načrtovati obseg revizije informacijskih sistemov tako, da upošteva cilje revizije in zagotovi skladnost z ustreznimi zakoni in strokovnimi revizijskimi standardi.

04 Revizor IS mora oblikovati in dokumentirati revizijski pristop, ki temelji na tveganjih.

05 Revizor IS mora izdelati in dokumentirati revizijski načrt, v katerem so našteti revizijski postopki s podrobnim opisom njihove vrste in ciljev, čas in obseg revizije, cilji revizije in potrebni viri.

06 Revizor IS mora pripraviti revizijski program in/ali načrt in podrobno navesti vrsto, čas in obseg revizijskih postopkov, potrebnih za dokončanje revizije.

Komentar

07 Za funkcijo notranje revizije naj se načrt pripravi/posodobi najmanj enkrat letno za redne dejavnosti. Tak načrt je okvir za revizijske aktivnosti in je namenjen izpolnjevanju zadolžitev, določenih z revizijsko listino. Vsak nov/posodobljen načrt mora odobriti revizijska komisija, če obstaja.

08 Za zunanjo revizijo IS se načrt običajno pripravi za vsak revizijski ali nerevizijski posel posebej. Načrt naj dokumentira cilje revizije.

09 Revizor IS mora spoznati dejavnost, ki se revidira. Obseg potrebnega znanja naj se določi na podlagi vrste organizacije, njenega okolja, tveganj in ciljev revizije.

10 Revizor IS naj oceni tveganja, da lahko dá sprejemljivo zagotovilo, da bodo med revizijo ustrezno obravnavane vse pomembne zadeve. Šele nato je mogoče določiti strategije revidiranja, ravni pomembnosti in potrebne vire.

11 Revizijski program in/ali načrt lahko zahteva prilagoditve med potekom revizije, tako da se lahko obravnavajo zadeve, ki se pojavijo med revizijo (nova tveganja, napačne predpostavke ali ugotovitve iz že opravljenih postopkov).

12 Nadaljnje informacije o pripravi revizijske listine ali listine o poslu lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G6 *Načela pomembnosti za revidiranje informacijskih sistemov*,
- smernica za revidiranje informacijskih sistemov G15 *Revizijsko načrtovanje, prenovljena*,
- smernica za revidiranje informacijskih sistemov G13 *Uporaba ocenjevanja tveganja pri revizijskem načrtovanju*,
- smernica za revidiranje informacijskih sistemov G16 *Učinek tretjih strank na kontrole IT v podjetju*,
- *Okvir* CobiT, kontrolni cilji.

Datum uveljavitve

13 Ta standard za revidiranje IS velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S6 Izvajanje revizijskih del

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti standarde in dati navodila v zvezi z izvajanjem revizijskega dela.

Standard

03 Nadzor — osebje, ki izvaja revizijo IS, mora biti nadzorovano, da bi bilo dano sprejemljivo zagotovilo, da bodo revizijski cilji doseženi in da so izpolnjeni ustrezni strokovni revizijski standardi.

04 Dokazi — med potekom revizije mora revizor IS pridobiti zadostne, zanesljive in ustrezne dokaze, da se dosežejo revizijski cilji. Revizijski izsledki in ugotovitve morajo biti podprti z ustrezno analizo in razlago teh dokazov.

05 Dokumentacija — revizijski postopek mora biti dokumentiran z opisi opravljenega revizijskega dela in revizijskimi dokazi, ki podpirajo izsledke in ugotovitve revizorja IS.

Komentar

06 Vloge in zadolžitve skupine za revizijo IS naj bi bile določene na začetku revizije; vsaj z opredelitvijo vlog odločanja, izvajanja in pregleda.

07 Delo, opravljeno med izvajanjem posla, naj bi bilo organizirano in dokumentirano po vnaprej določenih dokumentiranih postopkih. Dokumentacija naj vsebuje zadeve, kot so cilji in področje dela, revizijski program, opravljeni revizijski koraki, zbrani dokazi, izsledki, ugotovitve in priporočila.

08 Revizijska dokumentacija naj bi bila zadostna, da neodvisni stranki omogoči ponovno izvedbo vseh med revizijo izvedenih del, s katerimi pride do enakih ugotovitev.

09 Revizijska dokumentacija naj bi vsebovala podrobne podatke o tem, kdo je opravil posamezno revizijsko opravilo in kakšna je bila njegova vloga. Na splošno velja, da naj bi vsako opravilo, odločitev, korak ali izid revizije, ki je delo posameznega ali več članov skupine, pregledal še drug član skupine, imenovan v skladu s pomembnostjo obravnavane teme.

10 Revizor IS naj bi načrtoval uporabo najboljših dosegljivih revizijskih dokazov skladno s pomembnostjo cilja revizije ter časa in truda, potrebnega za pridobitev revizijskih dokazov.

11 Revizijski dokazi naj bi bili zadostni, zanesljivi ter ustrezni in uporabni za oblikovanje mnenja ali v podporo izsledkov in ugotovitev revizorja IS. Če po presoji revizorja IS pridobljeni revizijski dokazi ne izpolnjujejo teh meril, naj bi revizor IS pridobil dodatne revizijske dokaze.

12 Nadaljnje informacije o izvajanju revizijskih del lahko najdete v naslednjih navodilih:

- *Okvir* COBIT, kontrolni cilji.

Datum uveljavitve

13 Ta standard za revidiranje IS velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S7 Poročanje

Uvod

01 Standardi ISACA za revidiranje IS vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti in dati navodila o poročanju, tako da revizor IS lahko izpolni to obveznost.

Standard

03 Revizor IS mora po končani reviziji pripraviti poročilo v primerni obliki. Iz poročila morajo biti razvidni organizacija, predvideni prejemniki in morebitne omejitve glede razširjanja.

04 Revizijsko poročilo mora navajati področje, cilje, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela.

05 Poročilo mora vsebovati izsledke, ugotovitve in priporočila ter vse morebitne pridržke, omejitve ali omejitve področja dela, ki jih ima revizor IS v zvezi z revizijo.

06 Revizor IS mora imeti zadostne in ustrezne revizijske dokaze, da z njimi podpre rezultate, o katerih poroča.

07 Ob izdaji mora biti poročilo revizorja IS podpisano, opremljeno z datumom in predloženo v skladu z določili revizijske listine ali listine o poslu.

Komentar

08 Oblika in vsebina poročila sta običajno različni glede na vrsto storitve ali posla. Revizor IS lahko izvaja:

- revizijo (neposredno ali za potrditev),
- pregled (neposredno ali za potrditev),
- dogovorjene postopke.

09 Kadar se od revizorja IS zahteva mnenje o kontrolnem okolju prevzetega posla in obstajajo revizijski dokazi o pomembni ali bistveni slabosti, naj revizor IS ne bi ugotovil, da so notranje kontrole učinkovite. Revizor IS naj bi v poročilu opisal tako pomembno ali bistveno slabost in njen učinek na doseganje ciljev kontrolnih meril.

10 Preden revizor IS poročilo dokonča in ga izda, naj se o vsebini osnutka poročila pogovori s poslovodstvom obravnavanega področja in pripombe poslovodstva vključi v končno poročilo, kjer je to le primerno.

11 Kadar revizor IS v kontrolnem okolju odkrije pomembne pomanjkljivosti, naj bi o teh pomanjkljivostih obvestil revizijsko komisijo ali pristojni organ in v poročilu razkril, da jih je o pomembnih pomanjkljivostih obvestil.

12 Kadar revizor IS izdaja ločena poročila, naj se končno poročilo sklicuje na vsa ločena poročila.

13 Revizor IS naj preuči in oceni, ali naj poslovodstvo obvesti o pomanjkljivostih notranje kontrole, ki so manjše od pomembnih pomanjkljivosti. Tudi v takih primerih naj revizor IS revizijski komisiji ali pristojnemu organu sporoči, da je o takih pomanjkljivostih notranje kontrole obvestil poslovodstvo.

14 Revizor IS naj zahteva in ovrednoti ustrezne informacije o izsledkih, ugotovitvah in priporočilih predhodnega poročila, da ugotovi, ali so bili pravočasno uvedeni ustrezni ukrepi.

15 Nadaljnje informacije o poročanju lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G20 *Poročanje,*
- *Okvir* CobiT, kontrolni cilji M4.7 in M4.8 (CobiT3).

Datum uveljavitve

16 Ta standard za revidiranje IS velja za vse revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S8 Nadaljnja obravnava

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti standarde in dati navodila v zvezi z nadaljnjo obravnavo med procesom revidiranja IS.

Standard

03 Po poročanju o izsledkih in priporočilih mora revizor IS zahtevati in ovrednotiti ustrezne informacije, da ugotovi, ali je poslovodstvo pravočasno ustrezno ukrepalo.

Komentar

04 Če je poslovodstvo z revizorjem IS razpravljalo o svojih predlaganih ukrepih za izvajanje priporočil iz poročila ali mu jih je sporočilo, naj bodo ti ukrepi kot odziv poslovodstva zapisani v končnem poročilu.

05 Pri vrstah, času in obsegu nadaljnje obravnave naj se upoštevajo pomembnost poročanih ugotovitev in njihov vpliv, če popravni ukrepi ne bodo izvedeni. Čas nadaljnje obravnave po reviziji IS glede na prvotno poročanje naj bo predmet strokovne presoje, odvisen od več premislekov, kot so vrsta ali velikost s tem povezanih tveganj in stroškov za organizacijo.

06 Funkcija notranje revizije IS naj vzpostavi proces nadaljnje obravnave, s katerim spremlja in zagotavlja, da so bili ukrepi poslovodstva učinkovito vpeljani ali da je višje poslovodstvo sprejelo tveganje neukrepanja. Odgovornost za tako nadaljnjo obravnavo se lahko opredeli v revizijski listini te funkcije.

07 Odvisno od obsega in pogojev prevzetega posla se zunanji revizorji IS lahko zanesejo na funkcijo notranje revizije IS, da bo nadalje obravnavala njihova dogovorjena priporočila.

08 Kadar poslovodstvo sporoči informacije o sprejetih ukrepih za izvajanje priporočil in revizor IS dvomi o teh informacijah, naj izvede ustrezne preizkuševalne ali druge postopke, da ugotovi dejanski položaj ali stanje pred končanjem nadaljnje obravnave.

09 Poročilo o stanju nadaljnje obravnave spremljanja napredovanja, vključno z neizvedenimi dogovorjenimi priporočili, se lahko predloži revizijski komisiji, kadar obstaja, sicer pa poslovodstvu organizacije na ustrezni ravni.

10 Kot del nadaljnje obravnave spremljanja napredovanja naj revizor IS oceni, ali so ugotovitve, če niso bile izpeljane, še vedno pomembne.

Datum uveljavitve

11 Ta standard za revidiranje IS velja za revizije informacijskih sistemov, ki se začnejo 1. januarja 2005.

S9 Nepravilnosti in nezakonita dejanja

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda ISACA je določiti in dati navodila o nepravilnostih in nezakonitih dejanjih, ki jih mora revizor IS proučiti med revizijskim procesom.

Standard

03 Pri načrtovanju in izvajanju revizije mora revizor IS proučiti tveganje nepravilnosti in nezakonitih dejanj, da zmanjša revizijsko tveganje na nizko raven.

04 Revizor IS mora med revizijo vztrajati na stališču poklicne nezaupljivosti in upoštevati možnost, da bi ne glede na njegovo oceno tveganja nepravilnosti in nezakonitih dejanj lahko prišlo do pomembno napačnih navedb zaradi nepravilnosti in nezakonitih dejanj.

05 Revizor IS mora spoznati organizacijo in njeno okolje, vključno z notranjimi kontrolami.

06 Revizor IS mora pridobiti zadostne in ustrezne revizijske dokaze, da ugotovi, ali poslovodstvo ali drugi v organizaciji vedo za ali sumijo na kakršne koli dejanske ali domnevne nepravilnosti in nezakonita dejanja.

07 Pri izvajanju revizijskih postopkov za boljše poznavanje organizacije in njenega okolja mora revizor IS proučiti neobičajne ali nepričakovane odnose, ki lahko nakazujejo tveganje pomembno napačnih navedb zaradi nepravilnosti in nezakonitih dejanj.

08 Revizor IS mora zasnovati in izvesti postopke za preverjanje primernosti notranje kontrole in tveganja, da se poslovodstvo izogne kontrolam.

09 Kadar revizor IS odkrije napačno navedbo, mora oceniti, ali taka napačna navedba lahko nakazuje nepravilnost ali nezakonito dejanje. Če tak znak obstaja, mora revizor IS proučiti vplive na druge vidike revizije in zlasti na predstavitve poslovodstva.

10 Revizor IS mora pridobiti od poslovodstva pisne predstavitve vsaj enkrat letno ali pogosteje, odvisno od revizijskega posla. Poslovodstvo mora:

- **potrditi svojo odgovornost za zasnovo in izvajanje notranjih kontrol, da se preprečijo in odkrivajo nepravilnosti ali nezakonita dejanja;**
- **razkriti revizorju IS rezultate ocenjevanja tveganja obstoja pomembno napačne navedbe, ki je posledica nepravilnosti ali nezakonitega dejanja;**
- **razkriti revizorju IS svoje védenje o nepravilnostih ali nezakonitih dejanjih, ki vplivajo na organizacijo in so z njimi povezani:**
  - **poslovodstvo,**
  - **zaposleni, ki imajo pomembno vlogo pri notranjem kontroliranju;**
- **razkriti revizorju IS svoje védenje o kakršnih koli obtožbah nepravilnosti ali nezakonitih dejanj ali sumu na nepravilnosti ali nezakonita dejanja, ki vplivajo na organizacijo, kot so ga o njih obvestili zaposleni, nekdanji zaposleni, regulatorji in drugi.**

11 Če je revizor IS ugotovil pomembno nepravilnost ali nezakonito dejanje ali pridobil informacije, da utegne obstajati pomembna nepravilnost ali nezakonito dejanje, mora revizor IS o teh zadevah pravočasno obvestiti ustrezno raven poslovodstva.

12 Če je revizor IS ugotovil pomembno nepravilnost ali nezakonito dejanje, v katero so vpleteni poslovodstvo ali zaposleni, ki imajo pomembno vlogo pri notranjem kontroliranju, mora revizor IS o teh zadevah pravočasno obvestiti pristojne za upravljanje.

13 Revizor IS mora obvestiti ustrezno raven poslovodstva in pristojne za upravljanje o pomembnih slabostih v zasnovi in izvajanju notranje kontrole, da se preprečijo in odkrijejo nepravilnosti in nezakonita dejanja, ki jih je revizor IS opazil med revizijo.

14 Če revizor IS zaradi pomembno napačne navedbe ali nezakonitega dejanja naleti na izjemne okoliščine, ki vplivajo na njegovo zmožnost, da nadaljuje izvajanje revizije, mora revizor IS proučiti svoje pravne in strokovne zadolžitve v takih okoliščinah, vključno z obveznostjo, da revizor IS o tem poroča tistim, ki so sklenili revizijski posel, ali v nekaterih primerih pristojnim za upravljanje ali regulativnim organom, ali da prouči možnost umika iz posla.

15 Revizor IS mora dokumentirati vso komunikacijo, načrtovanje, izide, ocene in ugotovitve v zvezi s pomembnimi nepravilnostmi in nezakonitimi dejanji, o katerih je poročal poslovodstvu, pristojnim za upravljanje, regulatorjem in drugim.

Komentar

16 Revizor IS naj opredelitev, kaj je nepravilnost in nezakonito dejanje, poišče v smernici za revidiranje informacijskih sistemov G19 *Nepravilnosti in nezakonita dejanja*.

17 Revizor IS naj pridobi sprejemljiva zagotovila, da ni nobenih pomembno napačnih navedb zaradi nepravilnosti in nezakonitih dejanj. Revizor IS ne more pridobiti popolnega zagotovila zaradi dejavnikov, kot so uporaba presoje, obseg preizkušanja in omejitev delovanja notranje kontrole. Revizijski dokazi, ki so na voljo revizorju IS med revizijo, morajo biti po svoji naravi prej prepričljivi kot neizpodbitni.

18 Tveganje neodkritja pomembno napačne navedbe, ki je posledica nezakonitega dejanja, je večje od tveganja neodkritja pomembno napačne navedbe zaradi nepravilnosti ali napake, ker nezakonita dejanja lahko vključujejo obsežne in zapletene sisteme, zasnovane zato, da revizorju IS prikrijejo ali utajijo dogodke ali namerno napačne predstavitve.

S9 Nepravilnosti in nezakonita dejanja, nadaljevanje

19 Pretekle izkušnje revizorja IS in njegovo poznavanje organizacije naj revizorju IS med revizijo pomagajo. Od revizorja IS ni mogoče pričakovati, da pri poizvedovanjih in pri izvajanju revizijskih postopkov ne bi upošteval svojih preteklih izkušenj, vendar pa se od njega pričakuje, da bo ohranjal primerno raven poklicne nezaupljivosti. Revizor IS se ne sme zadovoljiti z manj kot prepričljivimi revizijskimi dokazi, ki temeljijo na prepričanju, da so poslovodstvo in pristojni za upravljanje pošteni in neoporečni. Revizor IS in delovna skupina za posel naj razpravljajo o dovzetnosti organizacije za nepravilnosti in nezakonita dejanja v okviru načrtovanja revizijskega postopka in ves čas trajanja revizije.

20 Pri presoji, ali obstaja tveganje pomembnih nepravilnosti in nezakonitih dejanj, naj revizor IS prouči možnost uporabe:

- svojega preteklega poznavanja organizacije in izkušenj z njo (vključno s svojimi izkušnjami o poštenosti in neoporečnosti poslovodstva in pristojnih za upravljanje),
- informacij, pridobljenih iz poizvedovanj pri poslovodstvu,
- predstavitev poslovodstva in potrditev notranjih kontrol,
- drugih zanesljivih informacij, pridobljenih med potekom revizije,
- presoje poslovodstva o tveganju nepravilnosti in nezakonitih dejanj in njegovih postopkov za prepoznavanje tveganj in odzivanja nanje.

21 Nadaljnje informacije o nepravilnostih in nezakonitih dejanjih lahko najdete v naslednjih navodilih:

- smernica za revidiranje informacijskih sistemov G5 *Revizijska listina*,
- *Okvir* CobiT, kontrolni cilj DS3, DS5, DS9, DS11 in PO6,
- Sarbanes-Oxleyjev zakon iz leta 2002,
- ameriški zakon o koruptivnih dejanjih v tujini (*Foreign Corrupt Practices Act*) iz leta 1977.

Datum uveljavitve

22 Ta standard ISACA velja za vse revizije informacijskih sistemov, ki se začnejo 1. septembra 2005 ali pozneje.

S10 Upravljanje IT

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda ISACA je določiti in dati navodila o upravljanju področij IT, ki ga mora revizor IS upoštevati med revizijskim postopkom.

Standard

03 Revizor IS mora pregledati in oceniti, ali je funkcija IS skladna s poslanstvom, vizijo, vrednotami, cilji in strategijami organizacije.

04 Revizor IS mora pregledati, ali ima funkcija IS jasno določeno zmogljivost, kot jo pričakuje poslovanje (uspešnost in učinkovitost), in oceniti njeno doseganje.

05 Revizor IS mora pregledati in oceniti uspešnost procesov upravljanja virov in zmogljivosti IS.

06 Revizor IS mora pregledati in oceniti skladnost z zakonskimi in okoljskimi zahtevami ter zahtevami glede kakovosti informacij, verodostojnosti in varovanja.

07 Pri ocenjevanju funkcije IS mora revizor IS uporabiti pristop, ki temelji na tveganju.

08 Revizor IS mora pregledati in oceniti kontrolno okolje organizacije.

09 Revizor IS mora pregledati in oceniti tveganja, ki lahko škodljivo vplivajo na okolje IS.

Dodatna navodila

10 Revizor IS naj se sklicuje na smernico za revidiranje informacijskih sistemov G18 *Upravljanje IT*.

11 Revizor IS naj pregleda in oceni tveganja delovnega okolja IS, ki podpira poslovne procese. Dejavnost revidiranja IS naj organizaciji pomaga pri prepoznavanju in ocenjevanju pomembne izpostavljenosti tveganju in prispeva k boljšim sistemom za obvladovanje in kontrolo tveganj.

12 Upravljanje IT je mogoče pregledovati samostojno ali pa ga upoštevati pri vsakem pregledu funkcije informacijskih sistemov.

13 Za nadaljnje informacije o upravljanju IT naj se revizor IS sklicuje na naslednja navodila:

- smernice za revidiranje IS:
  - G5 *Revizijska listina*,
  - *G6 Načela pomembnosti za revidiranje informacijskih sistemov*,
  - G12 *Organizacijsko razmerje in neodvisnost*,
  - G13 *Uporaba ocenjevanja tveganja pri revizijskem načrtovanju*,
  - G15 *Revizijsko načrtovanje, prenovljena*,
  - G16 *Učinek tretjih strank na kontrole IT v podjetju*,
  - G17 *Učinek nerevizijske vloge na neodvisnost strokovnjaka za revidiranje in dajanje zagotovil za IT*,
- *Smernice* CobiT *za poslovodstvo (*CobiT *Management Guidelines),*
- *Okvir* CobiT, *kontrolni cilji*; ta standard se povezuje z vsemi kontrolnimi cilji in vsemi domenami CobiT,
- *Kratke informacije za upravni odbor o upravljanju IT (Board Briefing on IT Governance), druga izdaja,* IT Governance Institute,
- *Kontrolni cilji IT za Sarbanes-Oxleyjev zakon (IT Control Objectives for Sarbanes-Oxley)*, IT Governance Institute,
- uporabiti je mogoče tudi Sarbanes-Oxleyjev zakon iz leta 2002 in druge posebne predpise**.**

Datum uveljavitve

14 Ta standard ISACA velja za vse revizije informacijskih sistemov od 1. septembra 2005.

S11 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju

Uvod

01 Standardi ISACA za revidiranje IS vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda je določiti standarde in dati navodila v zvezi z uporabo ocenjevanja tveganja pri revizijskem načrtovanju.

Standard

03 Revizor IS mora pri pripravi celovitega načrta revidiranja IS in pri določanju prednostnih nalog za učinkovito razporeditev virov za revidiranje IS uporabiti ustrezno tehniko ocenjevanja tveganja oziroma ustrezen pristop k temu ocenjevanju.

04 Pri načrtovanju posameznih pregledov mora revizor IS prepoznati in oceniti tveganja, ki so povezana s področjem pregleda.

Komentar

05 Ocenjevanje tveganja je tehnika, ki se uporablja za proučevanje za revizijo primernih enot v celotnem obsegu revidiranja IS in izbiro tistih področij za pregled, ki se jih vključi v letni načrt revidiranja IS, ker so najbolj izpostavljena tveganju.

06 Za revizijo primerna enota je opredeljena kot ločen del vsake organizacije in njenih sistemov.

07 Določitev celotnega obsega revidiranja IS naj temelji na poznavanju strateškega načrta IT poslovanja organizacije in na razpravah z odgovornim poslovodstvom.

08 Za lažjo pripravo načrta revidiranja IS naj bodo posamezna ocenjevanja tveganja izvedena in dokumentirana najmanj enkrat letno. Strateški načrti, cilji in okvir obvladovanja tveganj organizacije naj bodo obravnavani kot del vsakega posameznega ocenjevanja tveganj.

09 Uporaba ocenjevanja tveganja in izbira revizijskih projektov omogočata revizorju IS, da količinsko opredeli in utemelji količino virov za revizijo IS, potrebnih za dokončanje načrta revidiranja IS ali določenega pregleda. Prav tako lahko revizor IS po prednostnem vrstnem redu razporedi predvidene preglede na podlagi zaznanega tveganja in s tem prispeva k dokumentiranju okvirjev obvladovanja tveganj.

10 Revizor IS naj izvede predhodno oceno tveganj za posamezno področje pregleda. Cilji revizijskega posla za vsak posamezen pregled naj bodo odraz izidov takega ocenjevanja tveganj.

11 Po končanem pregledu naj revizor IS zagotovi, da se ustrezno posodobi okvir obvladovanja tveganja organizacije ali register tveganj, če ga je organizacija že pripravila, tako da se v njem odražajo izsledki in priporočila revizijskega pregleda in nadaljnjih aktivnosti.

12 Revizor IS naj upošteva tudi smernico za revidiranje informacijskih sistemov G13 *Uporaba ocenjevanja tveganja pri revizijskem načrtovanju* in revizijski postopek za informacijske sisteme P1 *Ocenjevanje in vrednotenje tveganja IS*.

Datum uveljavitve

13 Ta standard velja za revizije IS, ki se začnejo 1. novembra 2005 ali pozneje.

S12 Revizijska pomembnost

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti in dati navodila o načelu revizijske pomembnosti in njeni povezanosti z revizijskim tveganjem.

Standard

03 Revizor IS mora upoštevati revizijsko pomembnost in njeno povezanost z revizijskim tveganjem, ko se odloča o vrsti, času in obsegu revizijskih postopkov.

04 Pri načrtovanju revizije mora revizor IS upoštevati morebitne slabosti ali pomanjkanje kontrol in pretehtati, ali bi take slabosti ali pomanjkanje kontrol lahko povzročile tudi bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu.

05 Revizor IS mora upoštevati tudi skupni učinek manjših pomanjkljivosti ali slabosti kontrole in pomanjkanje kontrol, ki se lahko preoblikujejo v bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu.

06 V svojem poročilu mora revizor IS razkriti neučinkovite kontrole ali pomanjkanje kontrol ter pomembnost neučinkovitosti kontrol in možnost, da te slabosti povzročijo bistveno pomanjkljivost ali pomembno slabost.

Dodatna navodila

07 Revizijsko tveganje je tveganje, da bo revizor IS na podlagi revizijskih izsledkov prišel do nepravilnih sklepov. Revizor IS naj se zaveda tudi treh sestavin revizijskega tveganja, in sicer tveganja pri delovanju, tveganja pri kontroliranju in tveganja pri odkrivanju. Podrobnejšo razpravo o tveganjih si oglejte v *G13 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju*.

08 Pri načrtovanju in izvajanju revizije naj si revizor IS prizadeva za zmanjšanje revizijskega tveganja na sprejemljivo nizko raven in izpolnitev revizijskih ciljev. To doseže z ustreznim ocenjevanjem kontrol IS in z njimi povezanih kontrol.

09 Slabost pri kontroli velja za pomembno, če zaradi pomanjkanja kontrole ni mogoče dati sprejemljivih zagotovil, da bo kontrolni cilj dosežen.

10 Slabost, ki je opredeljena kot pomembna, pomeni, da:

- kontrole niso vzpostavljene in/ali se ne uporabljajo in/ali niso ustrezne,
- opravičuje eskalacijo.

11 Pomembna slabost je bistvena pomanjkljivost ali splet bistvenih pomanjkljivosti, zaradi katerih dokaj verjetno lahko pride do nezaželenih dogodkov, ki jih ni mogoče preprečiti ali odkriti.

12 Pomembnost in stopnja revizijskega tveganja, ki sta za revizorja IS še sprejemljivi, sta v obratnem sorazmerju; večja kot je stopnja pomembnosti, manjša je sprejemljivost revizijskega tveganja in obratno. To revizorju IS omogoča, da določi vrsto, čas in obseg revizijskih postopkov. Če se na primer pri načrtovanju za neki poseben revizijski postopek revizor IS odloči, da je pomembnost nižja, s tem povečuje revizijsko tveganje. Revizor IS bo potem želel to nadomestiti bodisi z obsežnejšim preverjanjem kontrol (da zmanjša oceno tveganja pri kontroliranju) ali z več postopki preizkušanja podatkov (da zmanjša oceno tveganja pri odkrivanju).

13 Pri ugotavljanju, ali je neka pomanjkljivost pri kontroli ali splet pomanjkljivosti pri kontroli lahko bistvena pomanjkljivost ali pomembna slabost, naj revizor IS ovrednoti učinek kompenzacijskih kontrol in oceni, ali so take kompenzacijske kontrole učinkovite.

14 Revizor IS lahko včasih različno oceni pomembnost in revizijsko tveganje, kar je odvisno od okoliščin v spreminjajočem se okolju.

15 Revizor IS naj se sklicuje na smernico za revidiranje informacijskih sistemov *G6 Načela pomembnosti za revidiranje informacijskih sistemov.*

16 Za nadaljnje informacije o revizijski pomembnosti si oglejte naslednja navodila:

- Smernice za revidiranje IS:
  - *G2 Zahteva za revizijske dokaze,*
  - *G5 Revizijska listina,*
  - *G8 Revizijska dokumentacija,*
  - *G9 Revizorjeva obravnava in presoja nepravilnosti in nezakonitih dejanj,*
  - *G13 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju,*
- COBIT 4.0, IT Governance Institute, 2005,
- *Kontrolni cilji IT za Sarbanes-Oxleyjev zakon (IT Control Objectives for Sarbanes-Oxley)*, IT Governance Institute, 2004.

Datum uveljavitve

17 Ta standard ISACA velja za vse revizije IS, ki se začnejo 1. julija 2006 ali pozneje.

S13 Uporaba dela drugih strokovnjakov

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda za revidiranje IS je določiti in dati navodila revizorju IS, ki pri reviziji uporablja delo drugih strokovnjakov.

Standardi

03 Revizor IS mora, kjer je to primerno, proučiti možnost uporabe dela drugih strokovnjakov za revizijo.

04 Revizor IS mora oceniti in sprejeti kot zadovoljive strokovno usposobljenost, sposobnosti, ustrezne izkušnje, vire, neodvisnost in postopke kontrole kakovosti drugih strokovnjakov, preden jih vključi v posel.

05 Revizor IS mora oceniti, pregledati in ovrednotiti delo drugih strokovnjakov kot del revizije in se odločiti, v kolikšnem obsegu bo uporabil in se zanašal na delo strokovnjaka.

06 Revizor IS mora ugotoviti in se odločiti, ali je delo drugih strokovnjakov ustrezno in popolno, da bo revizor IS lahko sprejel odločitve za zastavljene revizijske cilje. Take odločitve morajo biti jasno dokumentirane.

07 Revizor IS mora uporabiti dodatne preizkusne postopke, da pridobi zadostne in ustrezne revizijske dokaze v okoliščinah, v katerih uporaba dela drugih strokovnjakov ne zagotavlja zadostnih in ustreznih revizijskih dokazov.

08 Revizor IS mora dati ustrezno revizijsko mnenje in vanj vključiti omejitve glede področja dela, kjer zahtevanih dokazov ni pridobil z dodatnimi preizkusnimi postopki.

Dodatna navodila

09 Revizor IS naj prouči možnosti uporabe dela drugih strokovnjakov pri reviziji, kadar naleti na ovire, ki bi lahko oslabile revizijsko delo, ki ga je treba opraviti, ali kadar lahko s tem izboljša kakovost revizije. Primeri tega so: raven potrebnega znanja zaradi strokovnosti nalog, ki jih je treba izvesti, pomanjkanje virov za izvedbo revizije in časovne omejitve.

10 Strokovnjak bi bil lahko revizor IS iz zunanje revizijske družbe, svetovalec poslovodstvu, strokovnjak za IT ali strokovnjak na revizijskem področju, ki ga je imenovalo najvišje poslovodstvo ali skupina za revizijo IS.

11 Strokovnjak lahko prihaja iz organizacije ali od zunaj. Če je strokovnjak vključen v delo v drugem delu organizacije, se je na poročilo strokovnjaka mogoče zanesti. V nekaterih primerih se s tem lahko zmanjša tudi obseg področij IS, ki jih je pri reviziji treba pregledati, čeprav revizor IS nima dostopa do dokazne dokumentacije in delovnega gradiva. Revizor IS naj bo previden pri dajanju mnenja o takih primerih.

12 Revizor IS naj ima dostop do vsega delovnega gradiva, dokazne dokumentacije in poročil drugih strokovnjakov, kadar tak dostop ne povzroča pravnih vprašanj. Če se v zvezi z dostopom strokovnjaka do evidenc pojavijo pravna vprašanja in takega dostopa ni na voljo, mora revizor IS ustrezno določiti obseg uporabe dela takega strokovnjaka in ugotoviti, koliko se na njegovo delo lahko zanese.

13 Stališča, bistvenost in pripombe revizorja IS glede sprejemljivosti strokovnjakovega poročila in njegove pomembnosti naj bodo sestavni del revizorjevega poročila.

14 Revizor IS naj se sklicuje na standard revidiranja informacijskih sistemov S6 *Izvajanje revizijskih del*, ki pravi, da mora revizor IS pridobiti zadostne, zanesljive, ustrezne in uporabne dokaze, da se dosežejo revizijski cilji.

15 Če revizor IS nima potrebnih veščin ali drugih sposobnosti za opravljanje revizije, mora poiskati ustrezno pomoč drugih strokovnjakov; vsekakor naj ima revizor IS dobro znanje o opravljenem delu, vendar se od njega ne pričakuje znanje na enaki ravni, kot ga ima strokovnjak.

16 Revizor IS naj se sklicuje na smernico za revidiranje informacijskih sistemov *G1 Uporaba dela drugih strokovnjakov*.

17 Nadaljnje informacije o uporabi dela drugih revizorjev in strokovnjakov najdete v naslednjih navodilih:

- smernice za revidiranje IS:
  - *G5 Revizijska listina,*
  - *G8 Revizijska dokumentacija,*
  - *G2 Zahteva za revizijske dokaze,*
  - *G10 Revizijsko vzorčenje,*
  - *G13 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju,*
- COBIT 4.0, IT Governance Institute, 2005,
- *Kontrolni cilji IT za Sarbanes-Oxleyjev zakon (IT Control Objectives for Sarbanes-Oxley)*, IT Governance Institute, 2004.

Datum uveljavitve

18 Ta standard ISACA velja za vse revizije IS, ki se začnejo 1. julija 2006.

S14 Revizijski dokazi

Uvod

01 Standardi ISACA vsebujejo s krepkim tiskom označena osnovna načela in bistvene postopke, ki so obvezni, skupaj z navodili, ki se nanje nanašajo.

02 Namen tega standarda je določiti standarde in dati navodila o tem, kaj predstavlja revizijske dokaze ter kakšno kakovost in količino revizijskih dokazov mora revizor IS pridobiti.

Standard

03 Revizor IS mora pridobiti zadostne in ustrezne revizijske dokaze, da lahko sprejme razumne sklepe, s katerimi utemelji izide revizije.

04 Revizor IS mora ovrednotiti zadostnost revizijskih dokazov, pridobljenih med revizijo.

Komentar

Ustrezni dokazi

05 Revizijski dokazi:

- vključujejo postopke, kot jih opravi revizor,
- vključujejo izide postopkov, ki jih je opravil revizor IS,
- vključujejo izvorne dokumente (v elektronski ali papirni obliki), zapise in potrdilne informacije, uporabljene v podporo reviziji,
- vključujejo izsledke in izide revizijskega dela,
- izkazujejo, da je bilo delo opravljeno in je skladno z ustreznimi zakoni, predpisi in usmeritvami.

06 Kadar se revizijski dokazi pridobijo pri preizkusu kontrol, naj revizor IS prouči popolnost teh revizijskih dokazov, da z njimi podpre ocenjeno raven tveganja pri kontroliranju.

07 Revizijski dokazi naj bodo ustrezno prepoznani, medsebojno povezani in katalogizirani.

08 Pri ocenjevanju zanesljivosti revizijskih dokazov je treba upoštevati njihove lastnosti, kot so izvor, vrsta (npr. pisni, ustni, vizualni, elektronski) in pristnost (npr. elektronski in lastnoročni podpisi, žigi).

Zanesljivi dokazi

09 Na splošno je zanesljivost revizijskih dokazov večja, kadar:

- so v pisni obliki in ne samo kot ustni izrazi mnenja,
- so pridobljeni iz neodvisnih virov,
- jih je pridobil revizor IS sam in jih ni predložila revidirana enota,
- jih je potrdila neodvisna stranka,
- so v hrambi pri neodvisni stranki.

10 Revizor IS naj prouči, kako s čim manjšimi stroški najuspešneje zbrati potrebne dokaze, da izpolni cilje in tveganja revizije. Vsekakor pa težavnost ali stroški pridobivanja dokazov niso ustrezna podlaga za opustitev potrebnih postopkov.

11 Postopki, ki se uporabljajo za zbiranje revizijskih dokazov, se razlikujejo in so odvisni od predmeta revidiranja (tj. od njegove vrste, časa revizije, strokovne presoje). Revizor IS naj izbere najprimernejši postopek glede na cilj revizije.

12 Revizor IS lahko pridobi revizijske dokaze na načine, kot so:

- preiskovanje,
- opazovanje,
- poizvedovanje in potrjevanje,
- ponovno izvajanje,
- ponovni izračun,
- računanje,
- analitični postopki,
- druge splošno sprejete metode.

13 Revizor IS naj prouči vir in naravo vsake pridobljene informacije, da ovrednoti njeno zanesljivost in postavi zahteve za nadaljnje preverjanje.

Zadostni dokazi

14 Dokazi so lahko upoštevani kot zadostni, če podpirajo vsa pomembna vprašanja cilja in področja revizije.

15 Revizijski dokazi naj bodo nepristranski in zadostni, da strokovno usposobljeni neodvisni stranki omogočijo ponoviti preizkuse in pridobiti enake izide. Dokazi morajo biti sorazmerni s pomembnostjo teme in vpletenimi tveganji.

16 Zadostnost je merilo količine revizijskih dokazov, ustreznost pa je merilo kakovosti revizijskih dokazov, oboje pa je med seboj povezano. Glede na to naj revizor IS, kadar za izvajanje revizijskih postopkov uporabi informacije, ki jih je pridobil od organizacije, posveti posebno pozornost točnosti in popolnosti informacij.

17 Kadar je revizor IS prepričan, da ni mogoče pridobiti zadostnih revizijskih dokazov, naj revizor IS to razkrije na način, ki je skladen z načinom obveščanja o izidih revizije.

S14 Revizijski dokazi, nadaljevanje

Zaščita in hramba

18 Revizijski dokazi naj bodo zaščiteni pred nepooblaščenim dostopom in spreminjanjem.

19 Revizijski dokazi naj bodo po končanem revizijskem delu shranjeni toliko časa, kot je potrebno v skladu z vsemi ustreznimi zakoni, predpisi in politikami.

Reference

20 Nadaljnje informacije o revizijskih dokazih najdete v naslednjih navodilih:

- standard revidiranja informacijskih sistemov *S6 Izvajanje revizijskih del,*
- smernica za revidiranje informacijskih sistemov *G2 Zahteva za revizijske dokaze,*
- smernica za revidiranje informacijskih sistemov *G8 Revizijska dokumentacija,*
- CobiT, kontrolni cilji *ME2 Spremljajte in vrednotite notranje kontrole* in *ME3 Zagotovite skladnost s predpisi.*

Datum uveljavitve

21 Ta standard velja za revizije informacijskih sistemov, ki se začnejo 1. julija 2006.

S15 Kontrole IT

Uvod

01 Standardi ISACA vsebujejo osnovna obvezna načela in bistvene postopke, označene s krepkim tiskom (črne črke), skupaj z navodili, ki se nanašajo nanje.
02 Namen tega standarda ISACA je določiti standarde in dati navodila za kontrole IT.

Standard

03 Revizor IS mora ovrednotiti in spremljati kontrole IT, ki so sestavni del notranjega kontrolnega okolja organizacije.
04 Revizor IS mora pomagati poslovodstvu z nasveti glede zasnove, uvajanja, delovanja in izboljšanja kontrol IT.

Komentar

05 Poslovodstvo je odgovorno za notranje kontrolno okolje organizacije, kar vključuje tudi kontrolo IT. Notranje kontrolno okolje zagotavlja disciplino, okvir in strukturo za dosego glavnega cilja sistema notranje kontrole.
06 CobiT opredeljuje kontrolo kot 'politike, postopke, prakse in organizacijske strukture, oblikovane za zagotavljanje razumnega jamstva, da bodo poslovni cilji doseženi ter neželeni dogodki preprečeni ali odkriti in popravljeni'. CobiT opredeljuje tudi kontrolni cilj kot 'opis želenega rezultata ali namena, ki naj bi bil dosežen z uvedbo kontrolnih postopkov v posamezen proces'.
07 Kontrole IT sestavljajo splošne kontrole IT, ki vključujejo vseobsegajoče kontrole IT, podrobne kontrole IT in aplikativne kontrole ter se nanašajo na kontrole nabave, uvajanja, dobave in podpore sistemov in storitev IT.
08 Splošne kontrole IT so kontrole, ki zmanjšujejo tveganje za celotno delovanje sistemov in infrastrukture IT v organizaciji in za širok spekter avtomatiziranih rešitev (aplikacij).
09 Aplikativne kontrole so množica kontrol, vgrajenih v aplikacije.
10 Vseobsegajoče kontrole IT so splošne kontrole IT, ki so zasnovane za upravljanje in spremljanje okolja IT in zato vplivajo na vse dejavnosti, povezane z IT. So podmnožica splošnih kontrol, in sicer so to tiste splošne kontrole IT, ki so osredotočene na upravljanje in spremljanje IT.
11 Podrobne kontrole IT sestavljajo aplikativne kontrole in tiste splošne kontrole IT, ki niso vključene v vseobsegajoče kontrole IT.
12 Pri pripravi celovitega načrta revidiranja IS in pri določanju prednostnih nalog za učinkovito razporejanje virov za revizijo IS naj revizor IS uporabi ustrezno tehniko ali način za ocenjevanje tveganja, da lahko dá zagotovila v zvezi s stanjem kontrolnih procesov IT. Kontrolni procesi so politike, postopki in aktivnosti, ki so del kontrolnega okolja, zasnovanega tako, da z obvladovanjem tveganja zagotavljajo, da tveganja ostajajo v sprejemljivih mejah.
13 Revizor IS naj prouči uporabo tehnik analiziranja podatkov, vključno z uporabo pristopa stalnega dajanja zagotovil, ki revizorjem IS omogoča, da nenehno spremljajo zanesljivost sistema in da pri pregledovanju kontrol IT z uporabo računalnika zbirajo selektivne revizijske dokaze.
14 Kadar organizacije uporabljajo tretje stranke, lahko te postanejo ključni element v kontroli organizacije in njenem doseganju kontrolnih ciljev. Revizor IS mora ovrednotiti vlogo, ki jo ima tretja stranka v zvezi z okoljem IT, z njim povezanimi kontrolami in kontrolnimi cilji za IT.
15 Nadaljnje informacije o kontrolah IT najdete v naslednjih navodilih ISACA in inštituta za IT Governance Institute® (ITGI™):

- smernica G3 *Uporaba računalniško podprtih tehnik revidiranja (CAAT),š'*
- smernica G11 *Učinek vseobsegajočih kontrol IS,*
- smernica G13 *Uporaba ocenjevanja tveganja pri revizijskem načrtovanju,*
- smernica G15 *Revizijsko načrtovanje, prenovljena*,
- smernica G16 *Učinek tretjih strank na kontrole IT v podjetju*,
- smernica G20 *Poročanje*,
- smernica G36 *Biometrične kontrole*,
- smernica G38 *Kontrole dostopa*,
- *Okvir* CobiT in kontrolni cilji.

Datum uveljavitve
16 Ta standard ISACA velja za revizije IS, ki se začnejo 1. februarja 2008.

S16 E-poslovanje

Uvod

01 Standardi ISACA vsebujejo osnovna obvezna načela in bistvene postopke, označene s krepkim tiskom (črne črke), skupaj z navodili, ki se nanašajo nanje.
02 Namen tega standard ISACA je določiti standarde in dati navodila v zvezi s pregledom okolij e-poslovanja.

Standard

03 Revizor IS mora pri pregledu okolij e-poslovanja oceniti tveganje in ovrednotiti kontrole, ki se nanašajo na ta okolja, da zagotovi ustrezen nadzor transakcij pri e-poslovanju.

Komentar

04 E-poslovanje je opredeljeno kot vrsta procesov, v katerih organizacije elektronsko poslujejo s svojimi strankami, dobavitelji in drugimi zunanjimi poslovnimi partnerji, pri tem pa uporabljajo internet kot tehnologijo, ki jim to omogoča. Zato vključuje modele e-poslovanja med podjetji (B2B) in s strankami (B2C).
05 Revizor IS naj pri pripravi celovitega revizijskega načrta za IS uporabi ustrezno tehniko ali pristop za ocenjevanje tveganja; načrt naj zajema okolja e-poslovanja.
06 Revizor IS naj pri pregledovanju dejavnosti e-poslovanja prouči uporabo tehnik analiziranja podatkov, vključno z uporabo pristopa stalnega dajanja zagotovil, ki revizorjem IS omogoča, da stalno spremljajo zanesljivost sistema in da pri pregledovanju kontrol IT s pomočjo računalnika zbirajo selektivne revizijske dokaze.
07 Raven zahtevanih veščin in znanja za razumevanje vplivov kontrol in upravljanja tveganja e-poslovanja se spreminja glede na zapletenost aktivnosti e-poslovanja organizacije.
08 Revizor IS naj pozna vrsto in razume kritičnost poslovnega procesa, ki ga podpira aplikacija e-poslovanja, preden začne revizijo, tako da je izide mogoče ovrednotiti v pravilnem kontekstu.
09 Nadaljnje informacije v zvezi z e-poslovanjem lahko najdete v naslednjih navodilih:

- smernica G21 *Pregled sistemov celovitih programskih rešitev (ERP)*,
- smernica G22 *Pregled e-poslovanja s strankami (B2C),*
- smernica G24 *Spletno bančništvo*,
- smernica G25 *Pregled navideznih zasebnih omrežij* (VPN),
- smernica G33 *Splošna obravnava in presoja o uporabi interneta*,
- postopek P6 *Požarni zidovi*,
- okvir CobiT in kontrolni cilji.

Datum uveljavitve

10 Ta standard ISACA velja za revizije IS, ki se začnejo 1. februarja 2008.