Dokument:	**VODNIK: Načrtovanje revizijskega posla osnutek**
Namen dokumenta:	Podrobno opredeliti način načrtovanja, oblikovanja sodil, izvedbe postopkov in poročanja o izsledkih posla.
Povzetek točk:	
Avtor:	Maja Hmelak, Uroš Žust

Verzija	Datum	Oseba	Opis
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	20.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

1. Načrtovanje revizijskega posla

Usmeritve na področju načrtovanja revizijskega posla podajajo **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[1]. V nadaljevanju

[1] Do vključno 30.10.2013 so veljali Standardi, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT, od 1.11.2013 pa veljajo prenovljeni **Standardi za revidiranje informacijskih sistemov in dajanja zagotovil**. Le-ti so del novega **Okvira poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil ITAF** (ITAF™: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition). V obdobju priprave standardne revizijske mape ti še niso prevedeni v slovenščino. V tekstu nove standarde in smernice le povzemava, posebej pa poudarjava, da pričujoči prevodi niso uradni in veljavni prevodi, temveč sva jih pripravila avtorja. **Pred izvedbo vsakega revizijskega posla mora strokovnjak za revizijo IS in dajanje zagotovil preveriti besedila veljavnih in uradno objavljenih standardov in smernic za revidiranje informacijskih sistemov in dajanje zagotovil.**

podajamo nekatere pomembnejše standarde in smernice, ki se neposredno nanašajo na načrtovanje revizijskega posla[2] ter njihovo interpretacijo.

Standard 1201 Načrtovanje posla *zahteva:*

1201.1 Strokovnjak za revizijo IS in dajanje zagotovil[3] mora v načrtovanje vsakega posla revidiranja ali dajanja zagotovil vključiti:

- *Cilj, obseg, časovnico in pričakovane rezultate posla;*
- *Skladnost z zakoni in poklicnimi standardi revidiranja;*
- *Uporabo na tveganjih temelječega pristopa, kjer je to primerno;*
- *Zadeve, povezane s specifičnim poslom;*
- *Zahteve za dokumentiranje in poročanje.*

1201.2 Strokovnjak za revizijo IS in dajanje zagotovil mora razviti in dokumentirati projektni načrt posla revidiranja ali dajanja zagotovil, ki bo opisoval

- *Naravo posla, njegove cilje, časovnico in potrebe po človeških virih;*
- *čas in obseg potrebnih revizijskih postopkov za izvedbo posla.*

Razlaga ključnih vidikov standarda[4] določa med drugim, da mora Strokovnjak za revizijo IS in dajanje zagotovil spoznati dejavnost, ki se revidira. Obseg potrebnega znanja naj se določi na podlagi vrste organizacije, njenega okolja, tveganj in ciljev revizije. Strokovnjak za revizijo IS in dajanje zagotovilnaj poleg tega oceni tveganja, da lahko dá sprejemljivo zagotovilo, da bodo med revizijo ustrezno obravnavane vse pomembne zadeve. Šele nato je mogoče določit strategije revidiranja, ravni pomembnosti in potrebne vire.

[2] Poleg naštetih standardov in smernic se na revizorjevo načrtovanje posredno ali neposredno nanašajo tudi drugi dokumenti - tu so podani le glavni.

[3] Smernice za revidiranje informacijskih sistemov, ki so bile v pripravi novega Okvira poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil le na novo oštevilčene, ne pa tudi spremenjene, govorijo o strokovnjaku za revidiranje in dajanje zagotovil za IT, revizorju IT in revizorju IS. Novi, prenovljeni standardi, govorijo o Strokovnjaku za revizijo IS in dajanje zagotovil ter revizorju IS. V pričujočih dokumentih uporabljava oba izraza glede na to ali govoriva o standardu ali o smernici za revidiranje informacijskih sistemov in dajanje zagotovil skladno z novimi standardi.

[4] Novi Okvir poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil ITAF poleg standardov in smernic vključuje tudi njihove razlage ozirom ključne vidike.

2. Listina o poslu

Načrtovanje revizijskega posla bo v veliki meri razvidno iz Listine o poslu ali primerljivega načrtovalnega dokumenta. **Listina o poslu** je dokument, ki ga pripravi strokovnjak za revizijo IS in dajanje zagotovil[5], ki deluje kot zunanji strokovnjak (veščak) notranjerevizijske delovne skupine ali samostojni zunanji strokovnjak. Strokovnjak za revizijo IS in dajanje zagotovil, ki je član notranjerevizijske delovne skupine, bo elemente, vezane na izvedbo revizijske naloge opredelil v načrtovalnem dokumentu.

Standard 1002 Organizacijska neodvisnost *nalaga, da naj listina o poslu obravnava tudi neodvisnost in odgovornost revizijske funkcije.*

Razlaga[6] ključnih vidikov ***Standarda 1201 Načrtovanje posla*** *vsebuje dodatna napotila, povezana z Listino o poslu:*

- *Za notranje posle naj strokovnjak za revizijo IS in dajanje zagotovil:*
  - *revidirancu pojasni revizijsko listino ter, kjer je potrebno uporabi tudi listino o poslu ali primerljiv dokument, s katerim podrobneje pojasni vlogo v specifičnih poslih,*
  - *revidirancu pojasni načrt dela tako, da je le ta z njim v celoti seznanjen in lahko, ko je potrebno omogoči dostop do dokumentov in drugih virov;*
- *Za zunanje posle naj strokovnjak za revizijo IS in dajanje zagotovil:*
  - *pripravi ločeno listino o poslu za vsak zunanji posle revizije ali dajanja zagotovil,*
  - *pripravi projektni načrt za zunanji posel revizije ali dajanja zagotovil, ki naj bi vseboval vsaj cilj in obseg posla.*

Smernica 2001 revizijska listina (G5)[7] *navaja:*

[5] Smernice za revidiranje informacijskih sistemov, ki so bile v pripravi novega Okvira poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil le na novo oštevilčene, ne pa tudi spremenjene, govorijo o strokovnjaku za revidiranje in dajanje zagotovil za IT, revizorju IT in revizorju IS. Novi, prenovljeni standardi, govorijo o Strokovnjaku za revizijo IS in dajanje zagotovil ter revizorju IS. V pričujočih dokumentih uporabljava oba izraza glede na to ali govoriva o standardu ali o smernici za revidiranje informacijskih sistemov in dajanje zagotovil skladno z novimi standardi. V tem dokumentu uporabljamo uradni prevod Mednarodnih smernic za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT , ki ga objavlja Slovenski inštitut za revizijo na svoji spletni strani http://www.si-revizija.si/revizorji_is/dokumenti/smernice_revidiranja.pdf.

[6] Novi Okvir poklicnih praks za revizijo informacijskih sistemov in dajanje zagotovil ITAF poleg standardov in smernic vključuje tudi njihove razlage ozirom ključne vidike.

[7] V tem dokumentu uporabljamo uradni prevod Mednarodnih smernic za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT , ki ga objavlja Slovenski inštitut za revizijo na svoji spletni strani http://www.si-revizija.si/revizorji_is/dokumenti/smernice_revidiranja.pdf

2.1.1 Revizor IS mora imeti jasno pooblastilo za izvajanje funkcije revidiranja IS. To pooblastilo je običajno dokumentirano v revizijski listini, ki mora biti uradno sprejeta.

3.1 Namen

3.1.1 Listine o poslu se pogosto uporabljajo za posamezne posle ali za določitev predmeta in obsega ter ciljev razmerja med zunanjo revizijo IS in organizacijo.

3.2 Vsebina

3.2.1 V listini o poslu morajo biti jasno obravnavani štirje vidiki: namen, zadolžitev, pristojnost in odgovornost. Vidiki, ki jih je treba upoštevati, so navedeni v naslednjih odstavkih.

3.2.2 Zadolžitev:

- *obseg,*
- *cilji,*
- *neodvisnost,*
- *ocena tveganja,*
- *posebne zahteve revidiranca,*
- *rezultati.*

3.2.3 Pristojnost:

- *pravica dostopa do informacij, zaposlenih, lokacij in sistemov, ki so pomembni za izvajanje naloge,*
- *obseg ali kakršne koli omejitve obsega dela,*
- *dokaz o dogovoru glede rokov in pogojev posla.*

3.2.4 Odgovornost:

- *predvideni prejemniki poročil,*
- *pravice revidiranca,*
- *pregledi kakovosti,*
- *dogovorjeni datumi dokončanja,dogovorjeni proračuni/honorarji, če so na voljo.*

Zahtevane elemente Listine o poslu predstavljamo v dokumentu **102001 PRIMER Listina o poslu**.

3. Načrt dela

Smernica 2201 Načrtovanje posla (G15) [8] *navaja:*

3.1.1 Strokovnjaki za revizijo IS in dajanje zagotovil naj posel načrtujejo tako, da bo uspešno izveden, za revizijo pa naj določijo celovito revizijsko strategijo. Ustrezno načrtovanje pomaga zagotoviti, da bo pomembnim področjem revizije namenjena ustrezna pozornost, da bodo morebitne težave pravočasno prepoznane in rešene ter da bo revizijski posel primerno organiziran in voden, tako da bo izveden uspešno in učinkovito.

3.1.2 Jasna opredelitev projekta je kritičen dejavnik uspeha, ki zagotovi uspešnost in učinkovitost projekta. Projekt revizije naj v opisu nalog in pristojnosti vsebuje zadeve, kot so:

- *področja, ki naj se revidirajo,*
- *vrsto načrtovanega dela,*
- *visokonivojske cilje in obseg dela,*
- *teme, kot na primer proračun, dodelitev virov, razpored datumov, vrsta poročila, predvideni uporabniki/prejemniki,*
- *druge splošne vidike dela, kadar je to primerno*

3.1.4 Običajno je načrt treba izdelati za vsako revizijsko nalogo. V načrtu morajo biti dokumentirani cilji revizije.

3.1.5 Vsak revizijski projekt se mora sklicevati na splošni revizijski načrt ali pa vsebovati posebna pooblastila, cilje in druge pomembne vidike dela, ki ga je treba opraviti.

Za usklajevanje med deležniki je poleg listine o poslu pogosto smiselno pripraviti interni načrt dela ali načrtovalni delovni zapis. Načrtovalni delovni zapis podrobneje ureja posamezne vidike revizijske naloge, zlasti skupno razumevanje vseh deležnikov glede ciljev naloge, njenega obsega, njenih omejitev, vrstah postopkov, uporabljenih standardih, času izvede in potrebnih virih za izvedbo revizije. Ti elementi so načeloma že urejeni v pogodbi ali listini o poslu. Dodatno je te elemente smiselno podrobneje opredeliti v neodvisnem dokumentu, ki ga je mogoče kasneje spreminjati, če se med samim potekom revizijske naloge izkaže, da bi lahko prišlo do sprememb njenih ključnih vidikov (na primer razširitev obsega, nastop novih omejitev, sprememba časovnega plana naloge,…..).

[8] V tem dokumentu uporabljamo uradni prevod Mednarodnih smernic za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT , ki ga objavlja Slovenski inštitut za revizijo na svoji spletni strani http://www.si-revizija.si/revizorji_is/dokumenti/smernice_revidiranja.pdf

Dokument ne predstavlja načrta revizijskega posla, temveč le usklajevanje med deležniki.

Dokument je v veliko primerih smiselno dati v vednost vsem relevantnim deležnikom, česar pri listini o poslu nikoli ne naredimo (saj pogosto vsebuje podatke zaupne narave na primer ceno ali zaupne vidike izvedbe posla).

Primer načrtovalnega delovnega zapisa predstavljamo v dokumentu **10301 PRIMER Uvodni dokument.**

4. Spoznavanje področja revizijskega posla

Področje revizijskega posla (dejavnost, ki se revidira) je okvirno opredeljeno v listini o poslu ali načrtovalnem dokumentu (glej tudi dokument **102001 PRIMER Listina o poslu**). Ker pa strokovnjak za revizijo IS in dajanje zagotovil področja revizije praviloma vnaprej podrobno ne pozna, se mora najprej podrobno spoznati z okoljem, ki predstavlja področje in predmet posla oz. revidirano dejavnost.

Spoznavanje področja revizijskega posla v Listini o poslu

Za namene pričujočega dokumenta, bomo *predmet revizijskega posla* opredelili kot *informacijski sistem*, *področje revizijskega posla* pa lahko na primer opredelimo kot *delovanje informacijskega sistema*. Kadar sta področje in predmet revizijskega posla nejasno opredeljena, lahko pride do nenadzorovanega širjenja obsega posla. Če je na primer predmet posla opredeljen le kot »informacijski sistem«, bi vanj teoretično lahko sodile vse rešitve, ki informacijsko podpirajo poslovne procese organizacije, vključno z na primer starimi (papirnimi) kartotečnimi sistemi, rešitvami na beleženje delovnega časa vratarjev in uporabniškimi tabelami, kjer zaposleni vodijo porabo in nabavo službene kave. Seveda številne manjše informacijske rešitve pogosto ne predstavljajo pomembnega tveganja za organizacijo, zato je ključno, da naročnik revizijskega posla kar se da natančno opredeli predmet in področje posla in s tem prepreči nenadzorovano širjenje njegovega obsega.

Opredelitev področja in predmeta revizijskega posla naj bi obsegala vsaj:

- Programske rešitve, ki bodo predmet revizijskega posla, če te še niso znane pa vsaj področja delovanja, ki jih te programske rešitve podpirajo;
- Tehnološko in organizacijsko infrastrukturo, ki omogoča delovanje programskih rešitev, ki so predmet revizijskih postopkov[9].

[9] Tehnološka in organizacijska infrastruktura sta povezani s t.i. vseobsegajočimi IT kontrolami oz. sta pomembni za celostno razumevanje IT kontrolnega okolja.

Kljub temu, da naj bi bilo področje revizijskega posla čim bolj natančno opredeljeno, to v primerih ko informacijski sistemi niso natančno dokumentirani, ni vselej mogoče. Kadar zaradi nedokumentiranosti vnaprej ni mogoče natančno opredeliti informacijskih rešitev, ki bodo vključene v revizijski posel, je večinoma mogoče opredeliti vsaj poslovne procese, ki naj bi jih te rešitve pokrivale. Na ta način lahko uredimo opredelitev področja posla v listini o poslu, nato pa skozi nadaljnje revizijske postopke podrobno spoznamo področje kot celoto.

Spoznavanje področja revizijskega posla v fazi načrtovanja

V fazi načrtovanja podrobnih revizijskih postopkov mora revizor čim bolj natančno spoznati informacijsko okolje organizacije.

Smernica 2201 Načrtovanje posla (G15) *navaja:*

3.2.1 Razumevanje revidirančevega poslovanja in tveganj, s katerimi se sooča, je odločilen korak pri pripravi učinkovitega revizijskega načrta, osredotočenega na področja, ki so najobčutljivejša za prevare ali netočna ravnanja.

3.2.2 Pred začetkom revizijskega projekta naj bo delo strokovnjakov za revizijo IS in dajanje zagotovil načrtovano na način, ki je najprimernejši za dosego revizijskih ciljev. V okviru načrtovalnega postopka naj spoznajo ***podjetje in njegove procese****. Poleg tega, da bodo strokovnjaki za revizijo IS in dajanje zagotovil spoznali delovanje podjetja in njegove zahteve za IT, jim bo to pomagalo pri določanju pomembnosti virov IT, ki jih pregledujejo, saj so ti povezani s cilji podjetja. Strokovnjaki za revizijo IS in dajanje zagotovil naj določijo obseg revizijskega dela ter izvedejo predhodno oceno notranjih kontrol nad funkcijo, ki jo pregledujejo.*

3.2.3 Obseg poznavanja podjetja in njegovih procesov, ki se zahteva od strokovnjakov za revizijo IS in dajanje zagotovil, bo določen glede na vrsto podjetja in raven podrobnosti izvajanja revizijskega dela. Kadar strokovnjaki za revizijo IS in dajanje zagotovil obravnavajo neobičajne ali zapletene postopke, se od njih lahko zahteva tudi specializirano znanje. Obsežnejše poznavanje podjetja in njegovih procesov bo običajno prej zahtevano, kadar revizijski cilj zajema velik razpon funkcij IT, kot če se cilji nanašajo le na omejene funkcije. Za pregled s ciljem ovrednotenja nadzora nad plačnim sistemom podjetja bi bilo na primer običajno potrebno temeljitejše poznavanje podjetja kot za pregled s ciljem preizkusa kontrol v posebnem sistemu programskih knjižnic.

3.2.4 Strokovnjaki za revizijo IS in dajanje zagotovil naj spoznajo tipe osebja, dogodkov, transakcij in ravnanj, ki lahko bistveno vplivajo na določeno podjetje, funkcijo, proces ali podatke, ki so predmet revizijskega projekta. Poznavanje podjetja naj vključuje tudi poslovna, finančna in vgrajena tveganja, s katerimi se podjetje sooča, kakor tudi razmere na trgu podjetja in informacije o tem, v kolikšnem obsegu se podjetje pri doseganju svojih ciljev

zanaša na zunanje storitve. Strokovnjaki za revizijo IS in dajanje zagotovil naj te informacije uporabijo pri prepoznavanju morebitnih težav, oblikovanju ciljev in področja dela, pri izvajanju dela in proučevanju ukrepov poslovodstva, na katera bi morali biti pozorni.

Korake za spoznavanje področja revizijskega posla podrobno opisujemo v razdelku (mapi) **1040 Spoznavanje okolja organizacije**.

5. Ocena tveganja

Področje ocenjevanja tveganj je izjemno široko in kompleksno, zato ga predstavljamo v ločenem dokumentu **105002 VODNIK Ocenjevanje tveganj v reviziji IS**.

6. Sodila in revizijski program

Sodila za izvedbo revizijskega posla so odvisna od vrste revizijskega posla (glej dokument **0001 VODNIK Vrste poslov v reviziji IS, sodila in izražanje mnenja**). V nadaljevanju povzemamo tiste vidike področja sodil, ki so relevantna za oblikovanje revizijskega programa:

- Kadar izražamo mnenje o uradni trditvi poslovodstva (**Posel potrditvenega poročanja)** je mnenje, ki ga izrazimo ali je zadeva skladna, delno skladna ali neskladna z uradno trditvijo poslovodstva (sodilo je uradna trditev poslovodstva). Revizijski program je v tem primeru oblikovan skladno z uradno trditvijo poslovodstva.
- Kadar strokovnjak za revizijo IS in dajanje zagotovil ne podaja mnenja o uradni trditvi poslovodstva (**posel neposrednega poročanja)** je potrebno najprej vzpostaviti sodila, ki bodo podlaga za izražanje mnenja. To so lahko:
    - različni **standardi, zakonske zahteve** in **okviri dobrih praks** - zahteve standardov se prenesejo v revizijski program,
    - okvir sodil, posebej dogovorjen z naročnikom revizijskega posla – tu naročnik in strokovnjak za revizijo IS in dajanje zagotovil skupaj oblikujeta sodila, ki bodo podlaga za podajo mnenja.
- Poleg poslov, kjer strokovnjak za revizijo IS in dajanje zagotovil poda mnenje lahko opravi tudi posle t.i. **dogovorjenih postopkov**. V tem primeru se postopki za pridobivanje dokazov oblikujejo po tistem, kar je bilo z dogovorom sprejeto med naročnikom in strokovnjakom za revizijo IS in dajanje zagotovil.

Primeri standardov, vodil in okvirov, na katerih bi lahko temeljili revizijski programi so lahko:

- Standard informacijske varnosti ISO 27001, ki ga izdaja Mednarodna organizacija za standardizacijo,
- Globalna vodila za revizijo tehnologij (GTAG)[10], ki jih izdaja IIA;
- Kontrolni okvir za informacijske tehnologije COBIT[11], ki ga izdaja ISACA,
- ….

Sodila presoje oziroma revizijski program lahko oblikujemo tudi sami (glej **105003 PRIMER Ocena tveganj in revizijski program Splošne računalniške kontrole**), vendar moramo v listini o poslu načrtu revizijske naloge in poročilu razkriti sodila, po katerih smo opravljali revizijo.

7. Pomembnost

Standard 1204 Pomembnost *predpisuje:*

1204.1 Strokovnjak za revizijo IS in dajanje zagotovil mora pri načrtovanju posla upoštevati potencialne šibkosti ali odsotnost kontrol ter preučiti, če bi te šibkosti in odsotnosti kontrol lahko predstavljale bistveno pomanjkljivost ali pomembno slabost.

1204.2 Strokovnjak za revizijo IS in dajanje zagotovil bo pri opredelitvi narave, časa in obsega revizijskih procedur upošteval revizijsko pomembnost in njeno razmerje z revizijskim tveganjem.

1204.3 Strokovnjak za revizijo IS in dajanje zagotovil mora upoštevati tudi skupni učinek manjših pomanjkljivosti ali slabosti kontrole in pomanjkanje

[10] Global Technology Audit Guide

[11] Kljub temu, da je že izdana različica 5 okvira COBIT, se v standardni revizijski mapi zanašamo na v slovenščino prevedeno različico COBIT 4.1. Okvir COBIT 4.1 (Kontrolni cilji za informacijsko in sorodno tehnologijo) pripravlja Inštitut za upravljanje IT (angl. IT Governance Institut ITGI™), ki pripravlja standarde v zvezi z usmerjanjem in nadzorom informacijske tehnologije v podjetjih (različico 5 pripravlja ISACA). Okvir opisuje dobre prakse celotne domene IT in procesnega okvira ter predstavlja aktivnosti na področju IT na obvladljiv in logičen način. COBIT-ove dobre prakse so usmerjene bolj na kontrolo in manj na izvajanje. Namenjene so pomoči pri optimiziranju investicij s komponento IT, pri zagotavljanju storitev IT ter pri presojanju v primerih, ko gredo stvari narobe. Kot okvir dobrih praks izvajanja domene IT jih lahko uporabljamo tudi kot vodilo priporočenega stanja procesov in kontrol na tem področju, pri čemer pa je treba upoštevati uporabnost posameznih dobrih praks v dejanskih organizacijah. Slovenski prevod COBIT 4.1 je na voljo na spletni strani http://www.isaca.si/. Gradivo je avtorsko zaščiteno ter je v pričujoče materiale vključeno izključno v izobraževalne namene.

kontrol, ki se lahko preoblikujejo v bistveno pomanjkljivost ali pomembno slabost v informacijskem sistemu.

1204.4 V svojem poročilu mora strokovnjak za revizijo IS in dajanje zagotovil razkriti:

- *manjkajoče ali neučinkovite kontrole,*
- *pomembnost kontrolne pomanjkljivosti,*
- *verjetnost, da bodo te šibkosti povzročile v bistveno pomanjkljivost ali pomembno slabost.*

***Smernica 2204 Revizijska pomembnost (G6)** podaja naslednje usmeritve glede pomembnosti v reviziji informacijskih sistemov:*

3.1.1 Ocena, kaj je pomembno, je stvar strokovne presoje in vključuje upoštevanje učinka in/ali morebitnega učinka na zmožnost organizacije, da uresniči svoje poslovne cilje pri napakah, opustitvah, nepravilnostih in nezakonitih dejanjih, do katerih bi lahko prišlo zaradi slabosti nadzora na posameznem področju.

3.1.2 Pri ocenjevanju pomembnosti naj revizor IS upošteva:

- *skupno raven napake, ki je še sprejemljiva za poslovodstvo, revizorja IS, ustrezne regulativne agencije in druge zainteresirane,*
- *možnost, da skupni učinek majhnih napak ali slabosti postane pomemben.*

3.1.3 Da doseže revizijske cilje, mora revizor IS prepoznati ustrezne kontrolne cilje in na podlagi ravni sprejemljivega tveganja določiti, kaj je treba pregledati. Za posamezen kontrolni cilj je pomembna posamezna kontrola ali skupina kontrol, brez katere kontrolni postopki ne dajo utemeljenega zagotovila, da bo kontrolni cilj dosežen.

3.1.10 V nadaljevanju so primeri sodil, ki jih je treba upoštevati pri ocenjevanju pomembnosti:

- *kritičnost poslovnih procesov, podprtih s sistemom ali postopki,*
- *kritičnost informacijskih podatkovnih baz, podprtih s sistemom ali postopki,*
- *število in vrsta razvitih aplikacij,*
- *število uporabnikov informacijskih sistemov,*
- *število vodij in direktorjev, ki delajo z informacijskimi sistemi, razvrščenih po pooblastilih,*
- *kritičnost omrežnih komunikacij, podprtih s sistemom ali postopki,*

- *stroški sistema ali postopkov (strojna oprema, programska oprema, osebje, storitve tretjih strank, režijski stroški ali kombinacija teh),*
- *morebitni stroški napak (mogoče v smislu izgubljene prodaje, reklamacij v garancijskem roku, nepovračljivih razvojnih stroškov, stroški potrebnih objav opozoril, stroški popravkov, stroški za zdravje in varstvo, nepotrebno visoki stroški proizvodnje, veliko izgub itd.),*
- *stroški izgube kritičnih in pomembnih informacij v smislu denarja in časa za njihovo ponovno pridobitev,*
- *učinkovitost protiukrepov,*
- *število dostopov/transakcij/poizvedb, obdelanih v obdobju,*
- *vrsta, čas in obseg priprave poročil in vzdrževanja datotek,*
- *vrsta in količina obdelanih materialov (na primer kadar se premiki zalog evidentirajo brez vrednosti),*
- *zahteve sporazuma o ravni storitev in stroški morebitnih pogodbenih kazni,*
- *kazni za nespoštovanje zakonskih, drugih predpisanih in pogodbenih zahtev,*
- *kazni za nespoštovanje zahtev javnega zdravja in varstva.*

3.1.11 Poleg tega, da škodujejo ugledu podjetja, lahko napake v kontroli povzročijo denarne izgube, slabšo konkurenčnost ter izgubo zaupanja ali dobrega imena. Revizor IS mora ovrednotiti tveganja v primerjavi z možnimi protiukrepi.

Pomembnost ocenjujemo na podlagi ugotovitev v okviru spoznavanja informacijskega okolja organizacije, kar vključuje tudi spoznavanje kontrolnih mehanizmov in kontrolnega okolja.

***Smernica 2201 Načrtovanje posla (G15)** navaja:*

3.3.1 V postopku načrtovanja naj strokovnjaki za revizijo IS in dajanje zagotovil praviloma določijo ravni pomembnosti načrtovanja, tako da bo revizijsko delo zadoščalo za uresničitev revizijskih ciljev in da bodo revizijski viri učinkovito uporabljeni. Na primer, pri pregledu obstoječega sistema bo strokovnjak za revizijo IS in dajanje zagotovil med načrtovanjem revizijskega programa za delo, ki ga je treba opraviti, ocenil pomembnost različnih sestavnih delov sistema. Pri določanju pomembnosti naj se upoštevajo tako kakovostni kot tudi količinski vidiki.

Pomembnost je pri reviziji IS pogosto težko opredeliti, ker potencialnih učinkov pomanjkljivosti pogosto ni mogoče natančno izraziti v denarnih enotah, ena pomanjkljivost pa pogosto vpliva na dva ali več procesov. Poleg tega je pomembnost odvisna od izbranih sodil revizijskega posla in od načina, kako posamezno sodilo vpliva na revizijsko mnenje, tolmačenje pomembnosti pa je zato pogosto tudi stvar strokovnega tolmačenja posameznega strokovnjaka za revizijo IS in dajanje zagotovil. Zato je v tem tipu revizijskih poslov pomembno, če je le mogoče, podrobno pojasniti vse ugotovitve o pomanjkljivostih revidiranega področja, skupaj s pojasnili tveganj, ki iz navedenih pomanjkljivosti izhajajo.

8. Pridobivanje revizijskih dokazov

Standard 1205 Dokazi *predpisuje:*

1205.1 Strokovnjak za revizijo IS in dajanje zagotovil bo pridobil zadostne in primerne dokaze, na podlagi katerih bo lahko prišel do razumnih zaključkov kot osnovo za rezultate posla.

1205.2 Strokovnjak za revizijo IS in dajanje zagotovil po presodil, ali so pridobljeni dokazi zadostni, da podpirajo zaključke posla in da je bil dosežen cilj posla.

Razlaga ključnih vidikov standarda določa, da mora revizor IS pridobiti zadostne in ustrezne revizijske dokaze, da lahko sprejme razumne sklepe, s katerimi utemelji izide revizije. 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.*

Smernica 2205 Revizijski dokazi (G2) *med drugim priporoča:*

2.1.2 Pri načrtovanju revizijskega dela naj revizor IS upošteva vrsto revizijskih dokazov, ki jih je treba zbrati, njihovo uporabo za uresničitev revizijskih ciljev in njihove različne stopnje zanesljivosti. Med načeli, ki jih je treba upoštevati, sta neodvisnost in strokovna usposobljenost predlagatelja revizijskih dokazov.

Potrditveni revizijski dokazi neodvisne tretje stranke so lahko zanesljivejši od revizijskih dokazov pregledovane organizacije. Fizični revizijski dokazi so na splošno zanesljivejši od navedb posameznika.

2.1.4 Različne vrste revizijskih dokazov, za katere naj možnost uporabe prouči revizor IS, so med drugim:

- *opazovani postopki in obstoj fizičnih predmetov,*
- *dokumentarni revizijski dokazi,*
- *navedbe,*
- *analiza.*

2.1.5 Opazovani postopki in obstoj fizičnih predmetov lahko vključujejo opazovanja dejavnosti, premoženja in funkcij IS, kot so:

- *zaloga nosilcev podatkov v dislociranem skladišču,*
- *delujoči varnostni sistem v računalniškem prostoru.*

2.1.6 Dokumentarni revizijski dokazi, zapisani na papirju ali drugih nosilcih, lahko vključujejo:

- *izide izvlečkov podatkov,*
- *zapise transakcij,*
- *izpise izvorne kode,*
- *račune,*
- *dnevnike dejavnosti in kontrol,*
- *dokumentacijo o razvoju sistema.*

2.1.7 Revizijski dokazi so lahko tudi navedbe revidirancev, kot so:

- *pisne usmeritve in postopki,*
- *diagrami poteka sistema,*
- *pisne ali ustne izjave.*

2.1.8.1 Tudi izide analiz informacij s primerjavami, simulacijami, izračuni in sklepanji je mogoče uporabiti kot revizijske dokaze. Tako na primer:

- *primerjavo delovanja IS z drugimi organizacijami ali preteklimi obdobji,*
- *primerjavo pogostosti napak med aplikacijami, transakcijami in uporabniki.*

Dejanski postopki za izvedbo revizijskega posla so na primer:

- Pregled dokumentacije o informacijskem sistemu, ki je predmet pregleda ter o organiziranosti področja pregleda;
- Pregled testnih in produkcijskih nastavitev informacijskega sistema, ki je predmet pregleda;
- Pregled primerov delovanja informacijskega sistema ter primerov delovanja podpore informacijskem sistemu, ki je predmet pregleda;
- Pregled zasnove in delovanja avtomatiziranih in ročnih kontrol informacijskega sistema, ki je predmet pregleda ali delovanja področja, ki je predmet pregleda;
- Pregled po načelu skritega nakupovanja;
- …

Poleg samih revizijskih dokazov je za kakovost opravljenih postopkov zelo pomembno kako te dokaze uredimo in shranimo za morebitno kasnejšo referenco. Strokovnjak za revizijo IS in dajanje zagotovil naj o vsakem pridobljenem dokazu hrani najmanj podatke o:

- datumu pridobitve,
- načinu pridobitve,
- osebi znotraj revidirane enote, ki je sodelovala pri pridobitvi revizijskega dokaza,
- mestu, kjer je revizijski dokaz shranjen.

V primeru, da pričakujemo, da bodo pridobljeni revizijski dokazi kasneje potrebni v sodnem postopku je smiselno izvesti dodatne postopke za povečanje možnosti, da bo sodišče pridobljeni dokaz priznalo kot verodostojen. Strokovnjak za revizijo IS in dajanje zagotovil naj se, če je potrebno, o načinu pridobivanja dokazov posvetuje s pravnikom.

Za vsako revizijsko ugotovitev je poleg tega smiselno, da strokovnjak za revizijo IS in dajanje zagotovil vodi podrobno evidenco o tem, na katerih konkretnih revizijskih dokazih je osnovana.

9. Uporaba dela drugih strokovnjakov

Standard 1206 Uporaba dela drugih strokovnjakov *zahteva:*

1206.1 Strokovnjak za revizijo IS in dajanje zagotovil mora, kjer je to primerno, proučiti možnost uporabe dela drugih strokovnjakov za revizijo.

1206.2 Strokovnjak za revizijo IS in dajanje zagotovil mora oceniti in sprejeti kot zadovoljive strokovno usposobljenost, sposobnosti, ustrezne izkušnje, vire, neodvisnost in postopke kontrole kakovosti drugih strokovnjakov, preden jih vključi v posel.

1206.3 Strokovnjak za revizijo IS in dajanje zagotovil 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.

1206.4 Strokovnjak za revizijo IS in dajanje zagotovil 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.

1206.5 Strokovnjak za revizijo IS in dajanje zagotovil se mora odločiti, ali se bo zanašal na delo drugih strokovnjakov ter ali ga bo neposredno vključil v poročilo ali se bo nanj skliceval ločeno.

1206.6 Strokovnjak za revizijo IS in dajanje zagotovil 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.

1206.7 Strokovnjak za revizijo IS in dajanje zagotovil mora dati ustrezno revizijsko mnenje in vanj vključiti omejitve glede področja dela, kjer zahtevanih dokazov ni pridobil z dodatnimi preizkusnimi postopki.

V primeru vključitve drugih strokovnjakov v revizijske postopke je v načrtovalnem delovnem zapisu in/ali listini o poslu primerno določiti obseg in naravo njihove vključenosti, navesti strokovnjake ki bodo vključeni ter pooblastila za izvedbo postopkov, ki jih zunanji strokovnjaki imajo. Prav tako je smiselno opredeliti dokumentacijo, pripravljeno s strani zunanjih strokovnjakov, do katere bo imel dostop strokovnjak za revizijo IS in dajanje zagotovil ter način vodenja in predaje delovnih zapisov izvedbe naloge.