Dokument:	**VODNIK elementi revizorjevega poročila osnutek**
Namen dokumenta:	Podrobno opredeliti način poročanja o izsledkih revizijskega posla
Povzetek točk:	
Avtor:	Maja Hmelak, Uroš Žust

Verzija	Datum	Oseba	Opis
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	23.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

Dokument je pripravljen kot pomoč pri izvedbi revizijskega posla. Pred izvedbo vsakega revizijskega posla ga je potrebno prilagoditi zahtevam in posebnostim dogovorjenega posla. Elementi dokumenta niso obvezni in ne predstavljajo obveznega ravnanja strokovnjakov za revizijo IS in dajanje zagotovil.

Pomembno

Smernice[1] za revidiranje informacijskih sistemov in dajanje zagotovil izpostavljajo zlasti tiste revizijske posle, ki so usmerjeni v učinkovitost delovanja kontrol, kar je posebej razvidno v smernicah, ki obravnavajo poročanje. Vse revizije informacijskih sistemov pa niso usmerjene v presojo učinkovitosti delovanja kontrol: strokovnjak za revizijo IS in dajanje zagotovil[2] lahko pregleda skladnost upravljanja informacijskih sistemov z izbranimi standardi, uspešnost in učinkovitost izvedbe določenega IT projekta ipd. V teh primerih naj smiselno prilagodi in uporablja Standarde za revidiranje informacijskih sistemov in dajanje zagotovil.

Primer poročila o učinkovitosti delovanja izmišljenega informacijskega sistema podrobno obravnavava v dokumentu **6003 PRIMER Porocilo**. Hkrati v tem dokumentu podajava tudi primere ubeseditev posameznih vidikov poročila.

1. Temeljni vidiki revizijskega poročanja

Poročilo je končni izdelek revizijskega posla. V njem morajo biti učinkovito in pregledno navedene ugotovitve, do katerih je strokovnjak za revizijo IS in dajanje zagotovil prišel na podlagi opravljenih postopkov. Oblika in obseg poročila sta odvisna od vsebine revizijske naloge. Pri pripravi poročila pa mora strokovnjak za revizijo IS in dajanje zagotovil upoštevati **Standarde za revidiranje informacijskih sistemov in dajanje zagotovil**[3], kjer so podane zahteve in priporočila za obliko in vsebino revizorjevega poročila. V nadaljevanju podajava nekatere pomembnejše Standarde za revidiranje informacijskih sistemov in dajanje zagotovil, ki se neposredno nanašajo na

[1] 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] 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.

[3] 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.**

revizorjevo poročanje[4]. Vpliv vrste revizijskega posla na poročanje je podrobneje predstavljen v dokumentu **0001 VODNIK Vrste poslov v reviziji IS, sodila in izrazanje mnenja.**

Standardi za revidiranje informacijskih sistemov in dajanje zagotovil usmeritev in zahtev za revizorjevo poročilo ne navajajo na enem samem mestu, temveč posamezne elemente opisujejo v vrsti različnih dokumentov. Smiselno je, da strokovnjak za revizijo IS in dajanje zagotovil posamezne elemente vključi v urejeno oz. logično strukturo.

Standard 1401 Poročanje *določa:*

1401.1 Po zaključku naloge morajo strokovnjaki za revizijo IS in dajanje zagotovil pripraviti poročilo o rezultatih dela, ki mora vključevati:

- *navedbo organizacije, predvidene prejemnike in morebitne omejitve glede razširjanja,*
- *obseg, cilje, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela,*
- *izsledke, ugotovitve in priporočila,*
- *vse morebitne pridržke, omejitve ali omejitve področja dela, ki jih ima revizor IS v zvezi z revizijo,*
- *podpis, datum in razpečevanje v skladu z določbami revizijske listine.*

1401.2 Za ugotovitve, ki jih strokovnjak za revizijo IS in dajanje zagotovil vključi v revizorjevo poročilo, morajo obstajati zadostni in primerni dokazi.

2. Elementi revizorjevega poročila

V nadaljevanju podrobneje razčlenjujeva priporočila ***Smernice 2401 Poročanje (G20)*** za elemente, vključene v revizorjevo poročilo ter podajava primere teksta, ki ga lahko strokovnjak za revizijo IS in dajanje zagotovil uporabi, da izpolni priporočila.

Obvezni elementi revizorjevega poročila – Smernica 2401 Poročanje (G20)

Prvi pregled nad priporočenimi elementi revizorjevega poročila daje točka 4.3.2 ***Smernice 2401 Poročanje (G20)***.

Smernica 2401 Poročanje (G20) *priporoča:*

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

4.3.2 Poročilo strokovnjaka za revizijo IS in dajanje zagotovil o učinkovitosti kontrolnih postopkov naj vključuje:

- *naslov,*
- *naslovnika,*
- *opis obsega revizije, ime podjetja ali dela podjetja, na katerega se zadeva nanaša, kar vključuje:*
  - *podatke za prepoznavanje ali opis področja dejavnosti[5],*
  - *sodila, ki so bila uporabljena kot podlaga za sklepno ugotovitev strokovnjaka za revidiranje in dajanje zagotovil[6],*
  - *čas ali obdobje, na katerega se nanaša delo, ocenjevanje ali merjenje zadeve,*
  - *Izjavo, da je za vzdrževanje učinkovitega ustroja notranjega nadzora, vključno s kontrolnimi postopki za to področje dejavnosti, odgovorno poslovodstvo,*
- *pri potrditvenem poslu tudi izjavo s podatki o viru uradne trditve poslovodstva o učinkovitost kontrolnih postopkov,*
- *izjavo, da je strokovnjak za revizijo IS in dajanje zagotovil ta posel izvedel zato, da izrazi mnenje o učinkovitosti kontrolnih postopkov[7],*
- *opredelitev namena, za katerega je bilo pripravljeno poročilo strokovnjaka za revizijo IS in dajanje zagotovil, in podatki o tistih, ki so do njega upravičeni, ter izjava o neprevzemanju odgovornosti, če se poročilo uporabi v kakršen koli drug namen ali če ga uporabi kdo drug,*
- *opis uporabljenih sodil ali razkritje vira teh sodil,*
- *izjavo, da je bila revizija izvedena v skladu s standardi za revidiranje IS ali drugimi veljavnimi strokovnimi standardi[8],*
- *nadaljnje pojasnjevalne podrobnosti o spremenljivkah, ki vplivajo na dano zagotovilo, in druge informacije, kot je ustrezno,*

---

[5] Navedeni so lahko v predstavitvi revidiranca/revidirancev, ki jo opisujemo v poglavju »***Predstavitev revidiranca/revidirancev«*** na strani 9.

[6] Vidik sodil podrobno obravnavamo v dokumentu **0001 VODNIK Vrste poslov v reviziji IS, sodila in izrazanje mnenja**.

[7] Kadar gre za posel,kjer je predvideno izražanje mnenja.

[8] Čeprav v tekstu navedene smernice to še ni spremenjeno, gre za dokument Standardi za revidiranje informacijskih sistemov in dajanje zagotovil.

- *kadar je to primerno, naj ločeno poročilo vključuje priporočila za popravljalne ukrepe in odziv poslovodstva,*
- *odstavek, v katerem je navedeno, da je lahko prišlo do kakšnih napačnih navedb zaradi napak ali goljufije, ki so zaradi omejitev pri delovanju katere koli notranje kontrole ostale neodkrite. Poleg tega naj bo v tem odstavku tudi navedeno, da je projiciranje ocene notranje kontrole za finančno poročanje v naslednja obdobja povezano s tveganjem, da ta notranja kontrola lahko postane neustrezna zaradi spremenjenih okoliščin ali da se lahko poslabša raven njene skladnosti s usmeritvami ali postopki. Revizija ni zasnovana za odkrivanje vseh slabosti v kontrolnih postopkih, ker se ne izvaja neprekinjeno skozi celo obdobje in ker so preizkusi kontrolnih postopkov izvedeni po metodi vzorčenja. Če je strokovnjak za revizijo IS in dajanje zagotovil izrazil mnenje s pridržki, naj bo vključen tudi odstavek z opisom pridržkov.*
- *izraženo mnenje o tem, ali sta bila načrt in delovanje kontrolnih postopkov v vseh pomembnih pogledih za zadevno področje dejavnosti učinkovita*[9]*,*
- *podpis strokovnjaka za revizijo IS in dajanje zagotovil,*
- *naslov strokovnjaka za revizijo IS in dajanje zagotovil,*
- *datum poročila strokovnjaka za revizijo IS in dajanje zagotovil. V večini primerov je datiranje poročila urejeno z veljavnimi strokovnimi standardi. V vseh drugih primerih pa naj bo datum poročila enak datumu dokončanja dela na terenu.*

Poleg elementov naštetih v točki 4.3.2 ***Smernice 2401 (G20) Poročanje*** je v poročilo o reviziji priporočeno dodati še druge (neobvezne) elemente, ki jih naštevamo v nadaljevanju in od katerih nekateri so del Standardov za revidiranje informacijskih sistemov in dajanja zagotovil, nekateri pa del splošno sprejetih dobrih praks.

Obvestilo o tajnosti ali zaupnosti poročila

V primerih dela v javnem sektorju je področje varovanja zaupnosti urejeno z zakonskimi in podzakonskimi akti[10] v podjetjih pa najpogosteje z internimi predpisi. Glede na predpise naj bo celotna revizijska dokumentacija, zlasti pa revizorjevo poročilo, na naslovnici in v glavi ali nogi teksta označena s stopnjo tajnosti ter morebitnimi drugimi opozorili s področja varovanja podatkov.

[9] V primeru da je bilo področje pregleda učinkovitost delovanja notranjih kontrol.

[10] V Sloveniji sta na tem področju najpomembnejša akta Zakon o tajnih podatkih (ZTP-UPB2, Uradni list RS št. 50/06, 60/11) in Uredba o pisarniškem poslovanju in o dolžnostih upravnih organov do dokumentarnega gradiva (Uradni list RS št. 72/94, 82/94, 91/01), ki določata ravnanje glede tajnosti podatkov v javnem sektorju.

Povzetek za poslovodstvo

Povzetek za poslovodstvo je navadno tisti del revizorjevega poročila, ki je namenjen najširšemu krogu bralcev – osebam, ki niso nujno tehnični strokovnjaki ali strokovnjaki za posamezno področje revidiranja in ki ne bodo nujno prejele ali brale celotnega poročila. V praksi je povzetek pogosto najbolj vpliven del poročila.

Smernice za revidiranje informacijskih sistemov in dajanje zagotovil nimajo posebnih zahtev za povzetek revizorjevega poročila, dobra praksa pa je:

- da v nekaj stavkih kratko povzema opravljeno delo,
- da je napisan v laikom razumljivem jeziku, s čim manj strokovnimi termini in kraticami,
- da je glavno sporočilo podano v kratkih, razumljivih stavkih,
- da povzema revizijske cilje,
- da so ugotovitve postavljene v ustrezen kontekst, ter da so realno predstavljena tveganja, povezana s posameznimi ugotovitvami,
- da je povzetek poročila kar se da objektiven in ob vseh ugotovitvah predstavi tudi ustrezni kontekst; tako se izognemo morebitnemu napačnemu razumevanju.

Organizacije bodo odločitve o ukrepih za zmanjševanje tveganj pogosto sprejemale na podlagi povzetka revizorjevega poročila (kljub temu, da je strokovnjak za revizijo IS in dajanje zagotovil v nadaljevanju poročila podrobno opisal vse ugotovitve, njihove posledice in podal svoja priporočila za izboljšanje kontrolnega okolja). Včasih je zato dobra praksa, da poleg rednega postopka drugega branja za zagotavljanje kakovosti s strani revizijskih kolegov, strokovnjak za revizijo IS in dajanje zagotovil prosi tudi neodvisno osebo (npr. mlajšega člana revizijske ekipe), da prebere zgolj povzetek[11]. To strokovnjaku za revizijo IS in dajanje zagotovil omogoči presoditi učinke, ki jih bo imel povzetek na bralce poročila, ki s samim področjem revizije niso imeli direktne povezave ter zaključke, do katerih bodo na podlagi povzetka ti prišli.

Prejemniki poročila

Smernica 2401 (G20) Poročanje *priporoča:*

5.2.1 Revizor IS naj po končanem revizijskem delu predloži poročilo v primerni obliki predvidenim prejemnikom in uporabnikom storitev.

[11] Kjer je to glede na zahteve po zaupnosti vsebine poročila mogoče.

5.2.3 V poročilu naj bodo natančno določene omejitve glede razdeljevanja poročila, za katere sta se po dogovoru odločila revizor IS ali poslovodstvo. Revizor IS naj prouči tudi možnost o vključitvi izjave o neprevzemanju odgovornosti do tretjih strank.

Prejemnike poročila in omejitve glede distribucije je smiselno navesti na prvi strani ali prvih straneh revizorjevega poročila, saj so to prve strani, ki jih bo morebitna nepooblaščena oseba, ki bi pridobila kopijo poročila, videla. Na ta način je mogoče v nekaterih primerih kasneje dokazovati njeno odgovornost za nepooblaščen dostop do podatkov.

Predstavitev revidiranca/revidirancev

Predstavitev revidirancev je potrebna takrat, ko strokovnjak za revizijo IS in dajanje zagotovil poroča tretji osebi in ne revidirancu. Nekateri strokovnjaki za revizijo IS in dajanje zagotovil predstavitev revidiranca vključujejo tudi kadar poročajo neposredno revidirancu, navadno zato, da se ustvari skupno razumevanje okoliščin, v katerih je bil opravljen revizijski posel ter tudi kot del dobre poslovne komunikacije.

Kadar strokovnjak za revizijo IS in dajanje zagotovil informacijskih sistemov deluje kot veščak v poslih notranjega revidiranja, bo v skladu s splošnimi zahtevami poročanja notranje revizije revidirane organizacije predstavil revidirano poslovno enoto ali revidirani oddelek. V predstavitev lahko vključi različne organigrame in druge oblike oddelčnih predstavitev.

V poslu sodelujoči strokovnjaki za revizijo IS in dajanje zagotovil in zaposleni na revidiranem področju

Čeprav Standardi za revidiranje informacijskih sistemov in dajanje zagotovil zahtevajo navedbe v poslu sodelujočih strokovnjakov za revizijo IS in dajanje zagotovil, strokovnih sodelavcev in zaposlenih revidirane poslovne enote ali organizacije, jih je pogosto smiselno v poročilu posebej navesti. Ta informacija prejemniku poročila pomaga identificirati ključne zaposlene, ki jih je potrebno vključiti v popravljalne ukrepe ter razkriti vire informacij, ki so bile podlaga za revizorjeve sklepe in mnenja.

Uporaba dela zunanjih strokovnjakov

Smernica 2206 Uporaba dela drugih strokovnjakov (G1) *napotuje:*

4.2.5 Če je revizor IS za oblikovanje svojega mnenja uporabil poročilo drugega strokovnjaka, naj bodo sestavni del poročila revizorja IS tudi njegova mnenja/pripombe o sprejemljivosti in pomembnosti strokovnjakovega poročila.

Strokovnjak za revizijo IS in dajanje zagotovil naj v tem primeru v poročilo vključi najmanj:

- ime in priimek strokovnjaka, strokovni naziv ali drugo utemeljitev njegove strokovnosti, ime organizacije, kjer je zaposlen in okoliščine, ki so vodile do zanašanja na njegovo delo,
- kjer je to primerno naziv poročila, ki je predmet zanašanja na delo zunanjega strokovnjaka, skupaj z navedbo revidiranega področja, revizijskih ciljev, obravnavanega obdobja, vrsto, časom ter trajanjem opravljenega revizijskega dela.

Predstavite področja revizijskega posla

Področje revizijskega posla naj bi bilo dogovorjeno z listino o poslu ali z načrtovalnim delovnim zapisom. Področje revizijskega posla je opredelitev poslovnega področja, informacijskega sistema ali njegove komponente, ki predstavlja predmet revizijskega posla. Področje izhaja iz vprašanj, na katera želi odgovoriti naročnik ali vodja revizijskega posla.

Smernica 2401 Poročanje (G20) *napotuje:*

1.2.1 Zadeva ali področje dejavnosti so posebne informacije, obdelane v poročilu in povezanih postopkih strokovnjaka za revizijo IS in dajanje zagotovil. Vključuje lahko zadeve, kot so zasnova ali delovanje notranjih kontrol v skladu s prakso ali standardi ali določenimi zakoni in predpisi o varovanju zasebnosti

Podroben opis informacijskega sistema

Strokovnjak za revizijo IS in dajanje zagotovil se lahko odloči za podrobnejši opis informacijskega sistema (kadar želi s tem npr. podati dodatne informacije za poslovodstvo). Osnova za podroben opis informacijskega sistema je lahko dokument **104001 PRIMER Spoznavanje IS organizacije - Maloprodajna veriga.** Podroben opis informacijskega sistema lahko vključuje med drugim:

- Osnovne informacije o informacijskem sistemu (obdobje pridobitve/razvoja, število aktivnih uporabnikov,…);
- Seznam programskih rešitev, ki so bile zajete v revizijski posel, skupaj s kratkim opisom njihovega delovanja ter opisom načina njihove pridobitve (zunanji razvijalci, lasten razvoj, kupljena programska rešitev ipd);
- Seznam relevantnih zbirk podatkov ter orodij za njihovo upravljanje;
- Ključne elemente strežniške infrastrukture;
- Ključne elemente telekomunikacijske infrastrukture.

Podroben opis informacijskega sistema naj bo opisan v preprostem in berljivem jeziku.

Ker lahko vsako revizorjevo poročilo v določenih okoliščinah postane javen dokument, naj se strokovnjak za revizijo IS in dajanje zagotovil izogiba navedbam potencialno občutljivih podatkov npr. skic omrežja z IP številkami ipd.

Revizijski cilji

Standard S6 Izvajanje revizijskih del *zahteva da mora revizor IS med potekom revizije 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. Revizor IS naj bi načrtoval uporabo najboljših dosegljivih revizijskih dokazov skladno s pomembnostjo cilja revizije ter časa in truda, potrebnega za pridobitev revizijskih dokazov.*

Standard S7 Poročanje *navaja, da mora revizorjevo poročilo navajati področje,* ***cilje****, obravnavano obdobje in vrsto, čas in trajanje opravljenega revizijskega dela. 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.*

Standard S12 Revizijska pomembnost *zahteva, da naj si pri načrtovanju in izvajanju revizije revizor IS prizadeva, da zmanjša revizijsko tveganje na sprejemljivo nizko raven in izpolni revizijske cilje. To doseže z ustreznim ocenjevanjem kontrol IS in z njimi povezanih kontrol.*

Standard S14 Revizijski dokazi *navaja, da naj revizor IS 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.*

Revizijski cilji so opredeljeni odvisno od revizijske naloge, vedno pa morajo biti nedvoumno in podrobno izraženi.

Omejitve obsega revizijskih postopkov

Nepravilnosti in nezakonita dejanja

Smernica 2207 Nepravilnosti in nezakonita dejanja (G9) *napotuje, da naj, kadar sta predmet in obseg revizije omejena, strokovnjak za revizijo IS in dajanje zagotovil IS vključi pojasnilo o naravi in učinku te omejitve v revizorjevo poročilo. Do take omejitve lahko pride, če:*

- *revizor IS ni mogel opraviti nadaljnjega dela, ki je po njegovem mnenju potrebno za izpolnitev prvotnih revizijskih ciljev in v podporo revizijskim ugotovitvam, npr. zaradi nezanesljivih revizijskih dokazov,*

pomanjkanja virov ali omejitev, ki jih je revizijskim dejavnostim postavilo poslovodstvo;

- *poslovodstvo ni izvedlo preiskav, ki jih je priporočil revizor IS.*

Pri obsegu revizijskega posla mora strokovnjak za revizijo IS in dajanje zagotovil navesti vse omejitve, na katere je naletel pri izvajanju. Primeri omejitev so:

- Revidirana organizacija ni imela ali pa strokovnjaku za revizijo IS in dajanje zagotovil ni dala vpogleda v pomembno dokumentacijo;
- Revidirana organizacija je strokovnjaku za revizijo IS in dajanje zagotovil predala zavajajočo ali neustrezno dokumentacijo, ali pa je bila ta izročena prepozno;
- Strokovnjak za revizijo IS in dajanje zagotovil in naročnik sta se dogovorila, da določene nastavitve ali določeni dokumenti ne bodo vključeni v postopke npr. zaradi posebnih zahtev po varovanju njihove zaupnosti;
- Informacijski sistem, ki je bil predmet pregleda, še ni deloval v produkcijskem okolju, zato so se postopki izvedli le v testnem okolju.

Zunanje izvajanje dejavnosti IS

Včasih je del funkcionalnosti informacijskega sistema v zunanjem izvajanju, strokovnjak za revizijo IS in dajanje zagotovil pa nima dostopa do njega.

Smernica 2006 Strokovna usposobljenost (G30) *glede zunanjega izvajanja priporoča:*

2.7.1 Kadar je del revizijskega posla oddan v izvajanje ali je pridobljena zunanja strokovna pomoč, je treba dati sprejemljivo zagotovilo, da je zunanji strokovnjak ali agencija, ki ji je delo oddano v izvajanje, ustrezno usposobljena. Ta smernica se uporablja tudi za izbiro zunanjega strokovnjaka.

2.7.2 Kadar je pritegnjena stalna strokovna pomoč, je treba usposobljenost zunanjih strokovnjakov redno meriti in spremljati oziroma pregledovati[12].

[12] Kot smo že omenili, se s 30.10.2013 prenehajo veljati *Standardi, smernice ter orodja in tehnike za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT*, z njimi pa tudi *Smernica G4 Zunanje izvajanje dejavnosti IS.* Ta je priporočala, da če se izkaže, da izvajalec storitev ni pripravljen sodelovati z revizorjem IS, mora revizor IS o tem poročati poslovodstvu uporabnika storitev. To se lahko nanaša tudi na operacije, ki jih je izvajalec storitev oddal v podizvajanje dodatnim tretjim strankam brez določbe o pravici do revizije v pogodbi. V revizijskem poročilu naj bo jasno opredeljena omejitev obsega revizije, če revizor ni imel pravice revizijskega dostopa, pojasnjen pa mora biti tudi učinek te omejitve na revizijo.

Omejitve zaradi obsega revizijskega posla

Do omejitve obsega revizijskega posla lahko pride tudi takrat, kadar se področje revizije nanaša na programske rešitve, izključena pa je tehnološka infrastruktura, na kateri programske rešitve delujejo ter postopki podpore delovanja informacijske funkcije, ki so ključni za t.i. vseobsegajoče kontrole IT – kontrole, ki niso usmerjene v konkretno programsko rešitev, temveč so zasnovane tako, da so relevantne za vse programske rešitve v organizaciji. Primeri vseobsegajočih kontrol so:

- Postopki uvajanja sprememb v delovanje ali konfiguracijo programskih rešitev;
- Splošni postopki za zagotavljanje informacijske varnosti;
- Postopki za arhiviranje podatkov;
- …

Strokovnjak za revizijo IS in dajanje zagotovil mora v poročilu navesti vse tovrstne omejitve revizijskega posla.

Ugotovitve o kontrolnih slabostih, pomembnih pomanjkljivostih in priložnostih za izboljšanje

Včasih je bolj kot revizorjevo mnenje revidirancu dragoceno poročilo z ugotovitvami o bistvenih pomanjkljivostih, pomembnih slabostih ter drugih priložnostih za izboljšanje. Nekatere dobre prakse pri pisanju ugotovitev v poročilu so:

- Če je poročilo namenjeno laičnim bralcem, naj bodo ugotovitve splošne in napisane v širše razumljivem jeziku. Če je poročilo namenjeno omejenemu krogu strokovnih bralcev in se ne bo razširjalo izven tega kroga, naj bodo ugotovitve čim bolj konkretne.
- Ton ugotovitev naj bo nevtralen. Nujno se je izogibati navedbam, ki bi lahko izpadle neobjektivno ali obtožujoče.
- Ker se bo pogled strokovnjaka za revizijo IS in dajanje zagotovil pogosto razlikoval od pogleda revidiranca, je smiselno ob vsaki ugotovitvi navesti potencialna tveganja, povezana z ugotovitvijo. Kjer je le mogoče, naj bi se navedle tudi že uresničene grožnje, povezane z ugotovitvijo (če je do njih že prišlo ter če jih je mogoče dokazati). Vsako ugotovitev je potrebno postaviti v ustrezen kontekst.
- Če je le mogoče, naj bi strokovnjak za revizijo IS in dajanje zagotovil (v dogovoru z naročnikom) pripravil priporočila za izboljšanje kontrolnega okolja, odpravo pomanjkljivosti ali nadgradnjo obstoječih sistemov in postopkov.

- Pred dokončanjem poročila je treba opažanja in priporočila pregledati in potrditi skupaj z organizacijo.

Standard 1402 Nadaljnja obravnava (S8) *predpisuje:*

1402.1 Po poročanju o izsledkih in priporočilih mora revizor IS zahtevati in ovrednotiti ustrezne informacije, da ugotovi, ali je poslovodstvo pravočasno ustrezno ukrepalo.

Če je le mogoče, naj bo odziv poslovodstva naveden tudi že v samem poročilu (ob posameznih ugotovitvah). Ker strokovnjak za revizijo IS in dajanje zagotovil informacijskih sistemov pogosto revidira določeno poslovno enoto organizacije, je odziv poslovodstva včasih dejansko odziv te poslovne enote z namenom podaje pojasnila posamezne ugotovitve poslovodstvu organizacije.

Standardi za revidiranje informacijskih sistemov in dajanje zagotovil ne opredeljujejo kaj točno mora biti podano v odzivu poslovodstva, zato je omenjena odločitev prepuščena strokovnjaku za revizijo IS in dajanje zagotovil. Priporočeno je, da se v odziv poslovodstva vključi vsaj[13]:

- Komentar na vsako podano ugotovitev
- Seznam načrtovanih aktivnosti za vsako podano ugotovitev
- Predvidene datume izvedbe načrtovanih aktivnosti

Posebnosti poročanja glede na vrsto revizijskega posla

3.1.1 ***Smernica 2401 Poročanje (G20)*** *ločuje med tremi vrstami storitev:*

- *revizijo (neposredno ali potrditveno)*
- *pregled (neposreden ali potrditven)*
- *dogovorjenimi postopki.*

Mnenje

Oblika izražanja mnenja je odvisna od vrste dogovorjenega posla. Vpliv vrste revizijskega posla na poročanje je podrobneje predstavljen v dokumentu **0001 VODNIK Vrste poslov v reviziji IS, sodila in izrazanje mnenja**.

[13] Našteti so predlogi posameznih elementov odziva poslovodstva. V praksi naj strokovnjak za revizijo IS in dajanje zagotovil prilagodi vključene elemente po svoji presoji.

3. Elementi poročila glede na tip revizijskega posla

Obvezni elementi poročila se nekoliko razlikujejo po posameznem tipu revizijskega posla, kar predstavljamo v nadaljevanju.

Posebnosti posla neposrednega poročanja

Smernica 2401 Poročanje (G20) *priporoča:*

4.3.3 Pri poslu neposrednega poročanja poroča strokovnjak za revizijo IS in dajanje zagotovil neposredno o zadevi sami in ne o uradni trditvi o njej. Poročilo naj se sklicuje samo na zadevo posla in naj ne vsebuje nobenega sklicevanja na uradno trditev poslovodstva o zadevi.

Posebnosti posla pregleda

Smernica 2401 Poročanje (G20) *priporoča:*

3. 4 Kadar strokovnjak za revizijo IS in dajanje zagotovil prevzame posel pregleda, naj bo v poročilu navedeno, da se sklep nanaša samo na zasnovo in učinkovitost delovanja in da je bilo delo strokovnjaka za revizijo IS in dajanje zagotovil v zvezi z učinkovitostjo delovanja omejeno predvsem na poizvedbe, preiskovanje, opazovanje in le minimalno preizkušanje delovanja notranjih kontrol. Poročilo vključuje izjavo, da revizija ni bila izvedena, da dajejo izvedeni postopki manjše zagotovilo kot revizija in da revizijsko mnenje ni izraženo. V izraženem zagotovilu v nikalni obliki je navedeno, da strokovnjak za revizijo IS in dajanje zagotovil ni opazil ničesar, zaradi česar bi menil, da so bili kontrolni postopki podjetja za zadevno področje dejavnosti v katerem koli pomembnem pogledu na podlagi opredeljenih sodil neučinkoviti.

Posebnosti posla dogovorjenih postopkov

Smernica 2401 Poročanje (G20) *priporoča:*

*3.3.1 Izvajanje **dogovorjenih postopkov** se ne konča z izražanjem kakršnega koli zagotovila strokovnjaka za revizijo IS in dajanje zagotovil . Strokovnjak za revizijo IS in dajanje zagotovil je zadolžen za izvedbo določenih postopkov, da zagotovi zahtevane informacije tistim strankam, ki so se dogovorile za postopke, ki jih je treba izvesti. Strokovnjak za revizijo IS in dajanje zagotovil izda poročilo o dejanskih izsledkih tistim strankam, ki so se dogovorile za postopke. Iz tega poročila izoblikujejo prejemniki svoje lastne ugotovitve, ker strokovnjak za revizijo IS in dajanje zagotovil ni sam določil vrste, časa in obsega postopkov, da bi lahko izrazil kakršno koli zagotovilo. Poročilo je omejeno na tiste stranke (npr. regulativni organ), ki so se dogovorile za postopke, ki jih je treba izvesti, saj drugi ne poznajo razlogov za te postopke in*

bi njihove izide lahko napačno razlagali. Poročilo o dogovorjenih postopkih naj bo v obliki postopkov in izsledkov. Poročilo naj vsebuje te elemente:

- *naslov, ki vključuje besedo neodvisen,*
- *identifikacijske podatke o določenih strankah,*
- *podatke za prepoznavanje zadeve (ali pisno uradno trditev, ki se nanjo nanaša) in naravo posla,*
- *identifikacijske podatke o pristojni stranki,*
- *izjavo, da je za zadevo zadolžena pristojna stranka,*
- *izjavo, da so izvedeni postopki tisti, za katere so se dogovorile določene stranke, navedene v poročilu,*
- *izjavo, da so za zadostnost postopkov izključno odgovorne stranke same in izjavo o omejitvi odgovornosti za zadostnost postopkov,*
- *seznam izvedenih postopkov (ali sklic nanje) in izsledkov, ki se nanje nanašajo,*
- *izjavo, da strokovnjak za revizijo IS in dajanje zagotovil ni bil najet za preiskavo zadeve in je tudi ni opravil,*
- *izjavo, da bi strokovnjak za revizijo IS in dajanje zagotovil , če bi izvedel dodatne postopke, lahko opazil še druge zadeve in bi o njih poročal,*
- *izjavo o omejitvi uporabe poročila, ker je namenjeno samo za uporabo določenih strank.*