Dokument:	**VODNIK Vrste poslov v reviziji IS, sodila in izražanje mnenja osnutek**
Namen dokumenta:	Podrobno opredeliti vrste poslov v reviziji IS, predstaviti podane usmeritve za področje sodil revizije, ter predstaviti različne načine izražanja mnenja.
Povzetek točk:	
Seznam primerov:	Primer 1: Besedilo mnenja o skladnosti z zahtevami standarda ISO 27001 – pozitivno mnenje (revizija) Primer 2: Izbrana sodila za presojanje uspešnosti projekta prenove informacijskega sistema ABC Primer 3: Besedilo mnenja v primeru, da je bila revizija izvedena na podlagi dogovorjenih in prilagojenih sodil – pozitivno mnenje (revizija) Primer 4: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – pozitivno mnenje (pregled – nikalno zagotovilo). Primer 5: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – pozitivno mnenje (revizija) i Primer 6: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – pozitivno mnenje (revizija) ii Primer 7: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – odklonilno mnenje (revizija) ii

	Primer 8: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – negativno mnenje (pregled) Primer 9: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 - mnenje s pridržki (revizija) Primer 10: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – mnenje s pridržki (pregled) Primer 11: Besedilo mnenja v primeru, da je bila revizija izvedena na podlagi dogovorjenih in prilagojenih sodil – mnenje s pridržki (revizija)
Avtor:	Maja Hmelak, Uroš Žust

VERZIJA	DATUM	OSEBA	OPIS
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	22.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

1. Vrste revizijskih poslov

Standardi za revidiranje informacijskih sistemov in dajanje zagotovil[1], razlikujejo med različnimi vrstami revizijskih poslov. Od vrste revizijskega posla

[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.**

so odvisni način sklepanja listine o poslu, načrtovanje posla, izvedba posla in poročanje.

Smernica 2401 Poročanje (G20)[2] *razlikuje med več vrstami revizijskih poslov.*

1.2.2 ***Posel potrditvenega poročanja*** *je posel, pri katerem strokovnjak za revizijo IS in dajanje zagotovil*[3] *preiskuje uradne trditve poslovodstva v zvezi z določeno zadevo ali pa neposredno zadevo samo. Poročilo strokovnjaka za revizijo IS in dajanje zagotovil vsebuje mnenje o naslednjih zadevah:*

- ***Vsebina zadeve****: ta poročila se nanašajo bolj neposredno na zadevo samo kot na uradno trditev. V nekaterih situacijah poslovodstvo ne bo moglo izdati uradne trditve o zadevi. Tak primer so storitve IT, ki so oddane v izvajanje tretji stranki. Poslovodstvo običajno ne bo moglo dati uradne trditve o kontrolah, za katere je odgovorna tretja stranka. Zato bo moral strokovnjak za revizijo IS in dajanje zagotovil verjetneje poročati neposredno o zadevi sami in ne o uradni trditvi poslovodstva;*
- ***Uradna trditev poslovodstva o učinkovitosti kontrolnih postopkov*** *Ključno za to vrsto poslov je, da je, poslovodstvo pred njegovo izvedbo podalo neko uradno trditev o učinkovitosti kontrolnih postopkov IT, učinkovitosti podpore organizacijskim procesom, skladnosti informacijske varnosti z izbranim standardom ipd.*

V tujini obstajajo primeri, ko mora poslovodstvo organizacij kot del svojih letnih poročil podati na primer izjavo o učinkovitosti delovanja notranjih kontrol[4]. V ZDA je zelo pogosto tudi poročanje po SSAE 16[5], ki je zamenjal bolj znani in dolgo uporabljani standard SAS 70. V Sloveniji bi med tovrstne posle potencialno lahko uvrstili akreditacijo strojne in programske opreme, storitev

[2] 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

[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] Npr. Sarbanes-Oxley zahteve za poročanje v ZDA.

[5] Vrsta revizijskega posla po dokumentu Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, ki ga je izdala organizacija American Institute of Certified Public Accountants v ZDA. Namenjen je strokovnjakom za revizijo IS in dajanje zagotovil , ki ocenjujejo notranje-kontrolno okolje organizacij, ki nudijo zunanje izvajanje storitev (npr. storitev računalništva v oblaku). Pri poslu tipa I strokovnjak za revizijo IS in dajanje zagotovil izrazi mnenje o poštenosti ocene zasnove in učinkovitosti delovanja notranjih kontrol, ki jo pripravi revidirana organizacija.

zajema in hrambe v gradiva v elektronski obliki in spremljevalnih storitev, ki jih skladno z *Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)*[6] izvaja Arhiv Republike Slovenije ter pregled izjave v okviru samoocenitve in izjave predstojnika o oceni notranjega nadzora javnih financ[7] ipd.

- ***Poročila o preiskavah**, pri čemer strokovnjak za revizijo IS in dajanje zagotovil izda mnenje o določeni zadevi. Ti posli lahko vključujejo poročila o kontrolah, ki jih je uvedlo poslovodstvo, in o učinkovitosti njihovega delovanja.*

***Smernica 2401 Poročanje (G20)** je usmerjena v prvo vrsto od navedenih mnenj. Če so v opisu nalog in pristojnosti zahtevana mnenja druge vrste, je morda potrebno zahteve poročanja ustrezno prilagoditi.*

*1.2.7 **Posel neposrednega poročanja** je posel, pri katerem poslovodstvo ne da nobene pisne uradne trditve o učinkovitosti svojih kontrolnih postopkov in strokovnjak za revizijo IS in dajanje zagotovil da mnenje, na primer glede učinkovitosti kontrolnih postopkov, neposredno o zadevi sami.*

Oblika poročila in oblika mnenja bosta odvisni od posla, dogovorjenega z listino o poslu ali revizijsko listino ter od sodil, ki bodo uporabljena pri tem.

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

- *revizijo (neposredno ali potrditveno)*
- *pregled (neposreden ali potrditven)*
- *dogovorjene postopke.*

*3.2.1 **Revizija** zagotavlja visoko, vendar ne popolno (absolutno) raven zagotovila o učinkovitosti kontrolnih postopkov. To je običajno izraženo kot sprejemljivo zagotovilo ob priznavanju dejstva, da je popolno zagotovilo mogoče redko doseči zaradi dejavnikov, kot so potreba po presoji, uporaba preizkušanja, naravne omejitve delovanja notranje kontrole, in ker je veliko dokazov, ki jih ima na voljo strokovnjak za revizijo IS in dajanje zagotovil, po svoji naravi prej prepričljivih kot neizpodbitnih.*

*3.2.2 **Pregled** zagotavlja zmerno raven zagotovila o učinkovitosti kontrolnih postopkov. Raven dobljenega zagotovila je manjša, kot ga daje revizija, ker je obseg dela manj obsežen kot pri reviziji, vrsta, čas in obseg izvedenih postopkov pa ne dajejo zadostnih in ustreznih revizijskih dokazov, da bi strokovnjak za revizijo IS in dajanje zagotovil lahko izrazil pozitivno mnenje. Cilj pregleda je omogočiti strokovnjaku za revizijo IS in dajanje zagotovil, da*

[6] Uradni list RS, št. 30/2006.

[7] Navodilo o pripravi zaključnega računa državnega in občinskega proračuna ter metodologije za pripravo poročila o doseženih ciljih in rezultatih neposrednih in posrednih uporabnikov proračuna, Uradni list RS, št. 12/01,10/06, 8/07 in 102/10.

potrdi, ali je na podlagi postopkov njegovo pozornost pritegnilo kar koli, zaradi česar strokovnjak za revizijo IS in dajanje zagotovil meni, da na podlagi opredeljenih sodil kontrolni postopki niso bili uspešni (izraženo nikalno zagotovilo).

*3.2.3 Tako **revizije** kot **pregledi kontrolnih postopkov vključujejo**:*

- *načrtovanje posla,*
- *ovrednotenje učinkovitosti zasnove kontrolnih postopkov,*
- *preizkušanje učinkovitosti delovanja kontrolnih postopkov (med revizijo in pregledom so razlike v vrsti, času in obsegu preizkušanja),*
- *oblikovanje sklepa in poročanje o zasnovi in učinkovitosti delovanja kontrolnih postopkov na podlagi opredeljenih sodil:*
  - *sklep za revizijo je izražen kot pozitivno mnenje in daje visoko raven zagotovila,*
  - *sklep za pregled je izražen kot izjava negativnega zagotovila in daje le zmerno raven zagotovila.*

Poleg poslov kjer strokovnjak za revizijo IS in dajanje zagotovil poda mnenje, lahko opravi tudi posle t.i. dogovorjenih postopkov.

*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 določenih strank,*
- *podatke za prepoznavanje vsebine zadeve (ali pisno uradno trditev, ki se nanjo nanaša) in naravo posla,*
- *identifikacijske podatke o pristojni stranki,*
- *izjavo, da je za vsebino zadeve zadolžena pristojna stranka,*
- *izjavo, da so izvedeni postopki tisti, za katere so se dogovorile stranke, navedene v poročilu,*

- *izjavo, da so za zadostnost postopkov izključno odgovorne določene 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.*

Namen pri poslih dogovorjenih postopkov je, da strokovnjak za revizijo IS in dajanje zagotovil izvede postopke revizijske narave, za katere se je dogovoril z organizacijo ali kako ustrezno tretjo osebo ter poroča o dejanskih ugotovitvah. Ker strokovnjak za revizijo IS in dajanje zagotovil pripravi poročilo o dejanskih ugotovitvah le na podlagi omejenih postopkov, ne izrazi nikakršnega zagotovila. Namesto tega uporabniki poročila sami presojajo postopke in ugotovitve, o katerih poroča ter sami oblikujejo sklepe na podlagi njegovega dela. V praksi se stranke včasih odločijo, da bodo v listini o poslu s strokovnjakom za revizijo IS in dajanje zagotovil dogovorile določen obseg dela, nato pa na podlagi opravljenega dela potegnile večje sklepe kot bi bilo to glede na opravljene postopke upravičeno. **V takšnih primerih lahko pride do zavajanja tretjih oseb.**

2. Sodila in izražanje mnenja

Največja dilema revizorjevih poročil o učinkovitosti delovanja IT, učinkovitosti kontrol IS in drugih poročil o revizijah IS je vprašanje **sodil**, ki jih strokovnjak za revizijo IS in dajanje zagotovil uporabi za oblikovanje mnenja.

Smernica 2401 Poročanje (G20) *podaja naslednje usmeritve za področje sodil revizije:*

1.2.6 so standardi in primerjalne analize, ki se uporabljajo za merjenje in predstavitev zadeve in na podlagi katerih strokovnjak za revizijo IS in dajanje zagotovil zadevo tudi ovrednoti. Sodila morajo biti:

- ***nepristranska*** *— objektivna in brez predsodkov,*
- ***merljiva*** *—zagotavljajo dosledno merjenje,*
- ***popolna*** *— vključujejo vse ustrezne dejavnike, potrebne za sklepno ugotovitev,*
- ***ustrezna*** *—nanašajo se na vsebino zadeve.*

Izražanje mnenja za posel poročanja o vsebini zadeve

Kadar strokovnjak za revizijo IS in dajanje zagotovil ne podaja mnenja o uradni trditvi poslovodstva gre za **posel poročanja o vsebini zadeve** in je potrebno najprej vzpostaviti sodila, ki bodo podlaga za izražanje mnenja. To so lahko različni **standardi** in v tem primeru je oblikovanje mnenja relativno enostavno (sodilo je besedilo oz. zahteva standarda).

Primer 1: Besedilo mnenja o skladnosti z zahtevami standarda ISO 27001 – pozitivno mnenje (revizija)

> Po našem mnenju so uvedeni kontrolni mehanizmi in postopki varovanja informacijskih sistemov, organizacije ABC na dan …(*datum*), v vseh pomembnih pogledih skladni z zahtevami standarda ISO 27001.

Vseh poslov pa ni mogoče zasnovati tako da izrazimo mnenje o skladnosti s standardi. Uporaba celotnega besedila nekega standarda večinoma ni primerna za majhna okolja, ki so tipična za slovenske organizacije, saj mora vsaka organizacija najti ustrezno ravnotežje med učinkovitostjo delovanja ter nadzorom oziroma uvedenimi kontrolami. Eden izmed načinov za izražanje mnenja v teh okoliščinah je oblikovanje takšnega okvira sodil, ki predstavljajo podlago za izrek mnenja.

Okvir sodil naj bi bil dogovorjen z naročnikom – naveden je na primer lahko v načrtovalnem dokumentu ali je celo priloga listini o poslu. Eden izmed načinov, kako lahko oblikujemo okvir sodil je, da postavimo splošne cilje posla ter na podlagi ciljev oblikujemo sodila, ki bodo podlaga za presojo, ali so bili cilji doseženi ali ne.

V primeru posla presojanja uspešnosti projekta prenove informacijskega sistema ABC za cilje posla lahko postavimo cilje, ki jih je revidiranec želel doseči s prenovo. Te s sodili razbijemo na posamezne sestavne dele, kot prikazuje naslednji primer.

Primer 2: Izbrana sodila za presojanje uspešnosti projekta prenove informacijskega sistema ABC

Cilj projekta prenove informacijskega sistema ABC	**Sodila za presojanje uspešnosti doseganja ciljev projekta ABC**
Prenovljeni informacijski sistem ABC omogoča funkcionalnosti …(*seznam funkcionalnosti in dopolnitev, ki so bili izvorno vzrok za začetek prenove - seznam ciljev, ki jih je hotel doseči revidiranec s*	*Organizacija je pripravila funkcionalne specifikacije zahtevanih sprememb, ki so izražale njene dejanske potrebe po spremembah in dodatnem razvoju.*
	Uvedene spremembe in funkcionalnosti so skladne s funkcionalnimi specifikacijami, vzpostavitvenim dokumentom projekta in

Cilj projekta prenove informacijskega sistema ABC	**Sodila za presojanje uspešnosti doseganja ciljev projekta ABC**
prenovo).	*seznamom vseh zahtevkov za spremembe in dopolnitve, ki so nastali v postopku izvajanja projekta.*
	…
Projekt prenove informacijskega sistema ABC je bil zastavljen in voden učinkovito.	*Projektno vodenje projekta ABC je bilo zastavljeno v skladu z dobrimi praksami projektnega vodenja.*
	Projekt prenove informacijskega sistema ABC je imel jasno opredeljene vloge in odgovornosti udeležencev v projektu (projektni sponzor, vodja projekta, člani projektne ekipe za posamezne naloge,…)
	Projekt prenove informacijskega sistema ABC je potekal skladno z zastavljenimi roki za posamezne mejnike v projektu ter je bil dokončan v roku, ki ga je predvidel vzpostavitveni dokument projekta.
	…

V primeru, da se revizijsko mnenje oblikuje na podlagi posebej za revizijsko nalogo postavljenih sodil, je to potrebno jasno navesti:

Primer 3: Besedilo mnenja v primeru, da je bila revizija izvedena na podlagi dogovorjenih in prilagojenih sodil – pozitivno mnenje (revizija)

> Naše mnenje smo oblikovali na podlagi sodil, naštetih v …(*referenca na sodila*). Po našem mnenju je bil projekt prenove informacijskega sistema ABC uspešno izveden.

Smernica 2401 Poročanje (G20) izpostavlja ključno razliko med pregledom in revizijo v tem, ali je mnenje zasnovano kot pozitivno ali kot negativno (nikalno) zagotovilo. **Pozitivno zagotovilo** predstavlja visoko stopnjo zagotovila oz. izraža visoko raven zagotovila. **Negativno (nikalno) zagotovilo** predstavlja manjšo stopnjo zagotovila oz. izraža zmerno raven zagotovila.

Primer 4: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – pozitivno mnenje (pregled – nikalno zagotovilo).

> Pri pregledu uvedenih kontrolnih mehanizmov in postopkov varovanja informacijskih sistemov, organizacije ABC nismo opazili ničesar, na podlagi česar bi lahko sklepali, da le ti niso v vseh pomembnih pogledih skladni z zahtevami standarda ISO 27001.

Izražanje mnenja za posel poročanja o uradni trditvi poslovodstva o učinkovitosti kontrolnih postopkov

Kadar izražamo **mnenje o uradni trditvi poslovodstva o učinkovitosti kontrolnih postopkov** je izražanje mnenja relativno nezahtevno – mnenje, ki ga izrazimo je ali je zadeva skladna, delno skladna ali neskladna z uradno trditvijo poslovodstva (sodilo je uradna trditev poslovodstva):

Primer 5: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – pozitivno mnenje (revizija) i

> Po našem mnenju uradne trditve poslovodstva, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito, v vseh pomembnih pogledih pošteno predstavljajo stanje kontrolnega okolja informacijskega sistema ABC na dan …(*datum*).

Primer 6: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – pozitivno mnenje (revizija) ii

> Po našem mnenju so uradne trditve poslovodstva, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito, v vseh pomembnih pogledih resnične in odražajo pošten prikaz kontrolnega okolja sistema ABC na dan …(*datum*).

Našteti primeri predstavljajo možne, ne pa tudi edine oblike mnenja. Strokovnjak za revizijo IS in dajanje zagotovil lahko uporablja fraze kot so:

- »v vseh pomembnih pogledih skladen«,
- »v nobenem pomembnem pogledu ne odstopa od«,
- »je usklajen z«

Način kako bo strokovnjak za revizijo IS in dajanje zagotovil izrazil mnenje, je odvisen od dogovora v listini o poslu.

Odklonilno mnenje, mnenje s pridržki in zavrnitev mnenja

Strokovnjak za revizijo IS in dajanje zagotovil izrazi odklonilno mnenje, kadar, potem ko je pridobil zadostne in ustrezne revizijske dokaze, ugotovi npr.:

- da uradne trditve poslovodstva ne predstavljajo resnične in poštene slike področja posla;
- da je slabost v delovanju kontrol pomembna v kontekstu področja posla,
- da določena slabost v delovanju kontrol ali druga ugotovitev predstavlja pomembno neskladnost z zakonodajo ali tveganje prevare,
- …

Primer 7: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito – odklonilno mnenje (revizija) ii

> Po našem mnenju uradne trditve poslovodstva, da je v okviru informacijskega sistema ABC vzpostavljeno ustrezno kontrolno okolje ter da vzpostavljene kontrole delujejo učinkovito, ne predstavljajo resničnega in poštenega prikaza kontrolnega okolja sistema ABC na dan …(*datum*).

Primer 8: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – negativno mnenje (pregled)

> Pri pregledu uvedenih kontrolnih mehanizmov in postopkov varovanja informacijskih sistemov, organizacije ABC smo prišli do ugotovitev, na podlagi katerih sklepamo, da le ti niso v vseh pomembnih pogledih skladni z zahtevami standarda ISO 27001.

Strokovnjak za revizijo IS in dajanje zagotovil izrazi mnenje s pridržki, kadar, potem ko je pridobil zadostne in ustrezne revizijske dokaze, da obstajajo na področju posla pomembne slabosti, ne pa tudi bistvene pomanjkljivosti.

Primer 9: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 - mnenje s pridržki (revizija)

Z izjemo v nadaljevanju naštetih pridržkov, so po našem mnenju na dan …(*datum*) uvedeni kontrolni mehanizmi in postopki varovanja informacijskih sistemov organizacije ABC v vseh pomembnih pogledih skladni z zahtevami standarda ISO 27001.

Primer 10: Besedilo mnenja v primeru, da poslovodstvo postavlja uradno trditev, da je varnost informacijskih sistemov organizacije skladna z zahtevami standarda ISO 27001 – mnenje s pridržki (pregled)

Z izjemo ugotovitev, naštetih v poglavju …(*sklic na poglavje*), pri pregledu uvedenih kontrolnih mehanizmov in postopkov varovanja informacijskih sistemov, organizacije ABC nismo opazili ničesar, na podlagi česar bi lahko sklepali, da le ti na dan …(*datum*) niso bili v vseh pomembnih pogledih skladni z zahtevami standarda ISO 27001.

Primer 11: Besedilo mnenja v primeru, da je bila revizija izvedena na podlagi dogovorjenih in prilagojenih sodil – mnenje s pridržki (revizija)

Naše mnenje smo oblikovali na podlagi sodil, naštetih v …(*referenca na* sodila). Po našem mnenju je bil projekt prenove informacijskega sistema ABC z izjemo ugotovitev, ki jih navajamo v poglavju …(*sklic na poglavje*), učinkovito voden in uspešno izveden.

Smernica 2401 Poročanje (G20) *navaja, da naj bo, če je strokovnjak za revizijo IS in dajanje zagotovil izrazil mnenje s pridržki, v poročilo vključen tudi odstavek z opisom pridržkov.*

Čeprav to večinoma ni posebej opredeljeno v revizijski listini, je smiselno, da strokovnjak za revizijo IS in dajanje zagotovil vse ugotovitve povzame v posebnem delu poročila o reviziji/pregledu. Pri tem naj poleg tega, da navede bistvene slabosti, opozori tudi na pomembne pomanjkljivosti, ki sicer ne predstavljajo pomembnega tveganja za organizacijo, kljub temu pa lahko vplivajo na učinkovitost njenega delovanja, učinkovitost delovanja njenih kontrol ipd.

Strokovnjak za revizijo IS in dajanje zagotovil **zavrne**, da bi izrazil mnenje, kadar ne more pridobiti zadostnih in ustreznih revizijskih dokazov, na katerih bi utemeljil svoje mnenje.

Področje poročanja je podrobno opisano v dokumentu **6001 VODNIK Elementi revizorjevega porocila.**