Dokument:	**PRIMER Uvodni dokument oz. načrtovalni delovni zapis osnutek**
Ime revidiranca:	
Ime revizije:	Revizija učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1[1]
Namen dokumenta:	Podrobno opredeliti posamezne vidike ter skupno razumevanje vseh deležnikov revizijske naloge[2].
V vednost:	
Povzetek točk:	

[1] 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.

[2] Delovni zapis je pripravljen ob predpostavki, da organizacija naroča revizijo učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1. Primer je izbran ker gre za pogost tip pregleda. Dokument mora biti prilagojena zahtevam konkretne revizijske naloge.

	14.Priloge 7 **15.Mnenje 7**
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. Standardi za revidiranje informacijskih sistemov in dajanje zagotovil (splošne usmeritve)

Usmeritve na področju načrtovanja revizijskega posla podajajo **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[3]. V tem poglavju naštevamo tiste standarde, ki podajajo splošne usmeritve. Dele standardov in smernic, ki jih lahko neposredno prevedemo v konkretne zahteve, navajamo tudi v nadaljevanju pod posameznimi poglavji.

Smernica 2201 Načrtovanje posla (G15)[4] *navaja:*

3.1.1 Strokovnjaki za revizijo IS in dajanje zagotovil [5]*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] 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.**

[4] 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.

[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.

3.1.2 Jasna opredelitev projekta je kritičen dejavnik, da se lahko 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,*
- *cilje na visoki ravni in obseg dela,*
- *posamezne teme, npr. predračun, dodeljevanje virov, predvideni datumi, vrsta poročila, nameravani 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.

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 (npr. razširitev obsega, nastop novih omejitev, sprememba časovnega plana naloge,…..).

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

Dokument je smiselno dati v vednost vsem relevantnim deležnikom.

Podrobne elemente standardov in smernic za revidiranje informacijskih sistemov in dajanje zagotovil, ki se nanašajo na načrtovanje, navajamo v dokumentu **1001 VODNIK Načrtovanje revizijskega posla.**

2. Cilj revizijske naloge

V praksi revizije informacijskih sistemov pogosto dogovarjamo znotraj revizijske ekipe ali z naročnikom, ki nima specialističnega znanja o informacijskih sistemih. V takih primerih mora strokovnjak za revizijo IS in dajanje zagotovil skupaj z naročnikom ali z revizijsko ekipo zelo podrobno in konkretno opredeliti revizijske cilje posamezne revizijske naloge. Konkretna opredelitev ciljev naloge in s tem ciljev revizijskega projekta je ključna za njegovo učinkovito in uspešno izvedbo. Cilje revizijske naloge je smiselno opredeliti tudi v pogodbi ali listini o poslu.

3. Področje revizijske naloge

Področje revizijskega pregleda je opredelitev poslovnega področja, informacijskega sistema ali njegove komponente, ki predstavlja predmet revizijskega pregleda. Področje pregleda izhaja iz vprašanj, na katera želi odgovoriti naročnik ali vodja revizijskega pregleda.

4. Obseg revizijske naloge

Določitev obsega pregleda natančno določi meje področja, ki predstavlja predmet pregleda. Brez ustrezno opredeljenega obsega revizijske naloge lahko pride do nekontrolirane rasti obsega revizijske naloge. V praksi je koristno konkretno našteti vse programske rešitve, področja, dokumente, tehnološko infrastrukturo, oddelke oz. druge elemente, s katerimi je opredeljen obseg naloge.

5. Omejitve revizijske naloge

V nekaterih primerih je poleg obsega naloge smiselno našteti tudi vse omejitve, povezane s posamezno nalogo ter opredeliti, kako se bodo omejitve v končnem poročilu razkrile. Zlasti je v tem kontekstu nujno razkriti kakršnekoli omejitve pri dostopu do informacij ter omejitve glede obsega revizijske naloge, npr. izključena področja.

6. Standardi in relevantna zakonodaja

Tako načrtovalni delovni zapis kot tudi kasnejše poročilo naj naštevata standarde, v skladu s katerimi je bila opravljena revizija ter vse zakone in podzakonske akte, ki so posebej relevantni za revidirano področje ali za revizijsko nalogo.

Primeri standardov, v skladu s katerimi so bili opravljeni revizijski postopki, so:

- Standardi za revidiranje informacijskih sistemov in dajanje zagotovil, ki jih pripravlja ISACA[6],
- Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju, ki jih pripravlja IIA[7].

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

- Standard informacijske varnosti ISO 27001, ki ga izdaja Mednarodna organizacija za standardizacijo,

[6] Združenje za revizijo in nadzor informacijskih sistemov, nekdaj znana pod angleškim imenom Information Systems Audit and Control Association, vendar se zdaj uporablja le še akronim.

[7] Mednarodni inštitut notranjih revizorjev, ang. The Institute of Internal Auditors.

- Globalna vodila za revizijo tehnologij (GTAG)[8], ki jih izdaja IIA;
- Kontrolni okvir za informacijske tehnologije COBIT[9], ki ga izdaja ITGI™ oziroma ISACA,
- ….

V vseh komunikacijah z deležniki, ki nimajo strokovnega znanja o področju IS ali reviziji IS je smiselno s sprotnimi opombami pojasniti vse kratice in strokovne izraze.

7. Ocena tveganj

Oceno tveganj je mogoče podrobno izvesti v fazi spoznavanja informacijskega okolja področja, ki je predmet pregleda. V fazi izdelave načrtovalnega delovnega zapisa, ki je namenjen predvsem uskladitvi razumevanja strokovnjaka za revizijo IS in dajanje zagotovil in naročnika revizijske naloge oz. vodje revizijske ekipe, je večinoma mogoče izvesti vsaj preliminarno oceno tveganj področja ter jo opisati v nekaj stavkih. Vir informacij o tveganjih, povezanih s posameznim področjem je lahko letna ocena tveganj, ki je osnova letnega načrta rednih revizijskih nalog in razlog za določitev konkretne revizijske naloge. V primerih izrednih pregledov je preliminarna ocena tveganj povezana z vzrokom za uvrstitev izrednega revizijskega pregleda v letni načrt dela.

8. Rok izvedbe revizijske naloge

Opredeliti je potrebno termine začetka in konca izvedbe revizijske naloge, ključne mejnike v izvajanju naloge, po potrebi faze izvedbe naloge ter roke za pripravo osnutka poročila in končnega poročila. V primeru zamikanja rokov, je potrebno o tem pravočasno opozoriti naročnika naloge ter spremeniti načrt izvede naloge.

9. Naloge deležnikov

V primerih, ko medsebojno sodelovanje strokovnjakov za revizijo IS in dajanje zagotovil, naročnikov in revidirancev še ni utečeno, je smiselno opredeliti naloge vsake izmed skupin

[8] Global Technology Audit Guide

[9] Kljub temu, da je že na voljo verzija 5 okvira COBIT, se v tem delu zanašamo na v slovenščino prevedeni 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 (verzijo 5 pripravlja ISACA). Okvir opisuje dobre prakse celotne domene IT in procesnega okvirja 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 v pomoč 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 potrebno 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.

ter potencialno tudi naloge drugih deležnikov. Zlasti je smiselno opredeliti kontaktne osebe na obeh straneh, zahtevano odzivnost,način komunikacije in metode eskalacije problemov.

10. Uporaba dela drugih strokovnjakov

Kadar so v revizijsko nalogo vključeni zunanji strokovnjaki, to spremeni način dela tako z vidika revidirane enote, kot tudi z vidika revizijske ekipe. Smiselno je opredeliti vsaj s katerimi zunanjimi strokovnjaki sme revidirana enota komunicirati (praviloma poimensko, saj se tako ščiti pred socialnim inženiringom), v kaki obliki (praviloma pisno), kako odzivna mora biti revidirana enota, kdo je kontaktna oseba za zunanje strokovnjake, metode eskalacije ipd.

11. Načini pridobivanja revizijskih dokazov

V načrtovalnem delovnem zapisu je smiselno čim bolj podrobno opredeliti metode dela, ki jih bo strokovnjak za revizijo IS in dajanje zagotovil uporabljal za pridobivanje revizijskih dokazov ter s tem posredno opredeliti dokumente, ki jih bo potreboval pri svojem delu. Prav tako je smiselno opredeliti v kateri obliki naj se dokazi nahajajo, kako naj bodo označeni, na kak način se bodo arhivirali in kdo je za to odgovoren.

12. Komunikacija z revidirano enoto in z naročnikom

Opredeliti je treba vse oblike komunikacije z revidirano enoto ter tudi z naročnikom. To lahko vključuje dogovore o:

- komunikacijskih kanalih,
- ključni kontaktni osebi na revidiranem področju ter po potrebi pri naročniku,
- osebah, ki so vključene v vsako komunikacijo,
- dokumentih, ki jih mora pripraviti revidirana enota ter načinih njihovega posredovanja,
- rokih za posredovanje informacij,
- poročanju naročniku o izvedbi naloge.

13. Poročanje

V pogodbi oz. listini o poslu ter v načrtovalnem delovnem zapisu je potrebno opredeliti, obliko poročanja, s katero se bo zaključila revizijska naloga.

V primerih ko izvajalec revizijske naloge ni reden član revizijske ekipe oz. ni vnaprej seznanjen s predpisanimi načini poročanja, je v načrtovalni delovni zapis smiselno vključiti dogovor o:

- formatu in standardnih elementih končnega poročila,
- osebah, odgovornih za prejem in pregled osnutka poročila,
- prejemnikih končnega poročila.

14. Priloge

V fazi usklajevanja je smiselno z naročnikom ali revidirancem uskladiti tudi osnovne dokumente, ki naj bi jih ta pripravil za hiter potek revizijskega dela. Primeri dokumentov, ki so koristni za pripravo načrta revizijske naloge so:

- **103002 PREDLOGA Seznam dokumentacije**
- **103003 PREDLOGA Seznam aplikacij**

15. Mnenje

Praviloma bo področje priprave mnenja vsebovano v Listini o poslu. Kadar za interno rabo delamo le načrtovalni delovni zapis, pa vidik izražanja mnenja opredelimo v tem dokumentu. Vsa revizorjeva poročila ne bodo nujno vsebovala mnenja - v številnih primerih je dovolj, če se naročnik in strokovnjak za revizijo IS in dajanje zagotovil dogovorita da naj poročilo podrobneje osvetli posamezne vidike revidiranega področja, navede morebitna odstopanja od dobrih praks in z njimi povezana tveganja ter poda priporočila. Če je mnenje del poročila, je v načrtovalnem delovnem zapisu potrebno opredeliti:

- obliko, v kateri bo izrečeno mnenje,
- kriterije oz. sodila za izrek posamezne vrste mnenja.

Mnenje mora biti jasno povezano z revizijskim ciljem.