Dokument:	**PRIMER Listina o poslu osnutek**
Ime revidiranca:	
Ime revizije:	Revizija učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1[1]
Namen dokumenta:	Podrobno opredeliti temeljne elemente Listine o poslu[2].
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. Listina o poslu mora biti prilagojena zahtevam konkretne revizijske naloge.

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.

Seznam primerov:	
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

Listina o poslu je dokument, ki ga pripravi strokovnjak za revizijo IS in dajanje zagotovil[3], ki deluje kot zunanji strokovnjak (veščak) notranjerevizijske

[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

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. Usmeritve na področju priprave listine o poslu podajajo **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[4], podrobno jih predstavljamo v dokumentu **1001_VODNIK_Nacrtovanje_Revizijskega_Posla_V1.1**.

V nadaljevanju predlagava nekatera potencialna besedila listine o poslu. Gre le za primere besedil, ki so usklajeni z zahtevami standardov in priporočili smernic za revidiranje informacijskih sistemov in dajanje zagotovil.

Pomembno

Vsako pogodbo naj pred sklenitvijo pregleda strokovnjak s pravnega področja!!!

Vse primere, ki jih naštevava v nadaljevanju, sva pripravila ob predpostavki, da pripravljava listino o poslu revizije informacijskega sistema izbrane organizacije po okviru dobrih praks upravljanja informacijskih sistemov COBIT 4.1. Drugi tipi revizijskih poslov seveda zahtevajo drugačno opredelitev vsebinskih elementov posla.

V dejanski listini o poslu bi številne elemente, ki jih tu za večjo jasnost prikaza naštevava ločeno, združila in se s tem izognila morebitnemu podvajanju.

Namen listine o poslu

Opredelitev namena listine o poslu je priporočljivo opredeliti v začetku pogodbe.

Primer 1: Opredelitev namena pri reviziji delovanja informacijskih sistemov po okviru COBIT 4.1

> Namen te listine o poslu je določiti pogoje opravljanja storitev revizije delovanja informacijskih sistemov po okviru COBIT 4.1 v …(*ime revidirane organizacije*) s strani …(*ime strokovnjaka za revizijo IS in dajanje zagotovil ali družbe, ki je prevzela posel*), za …(*ime naročnika*).

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] 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.**

Če je primerno, lahko v listini o poslu opredelimo tudi okoliščine posla.

Primer 2: Opredelitev okoliščin posla

> Revizija delovanja informacijskih sistemov po okviru COBIT 4.1 je uvrščena v letni načrt notranjerevizijskih pregledov v …(*ime revidirane organizacije*). …(*ime strokovnjaka za revizijo IS in dajanje zagotovil ali družbe, ki je prevzela posel*) nastopa kot v vlogi zunanjega veščaka v skladu z revizijsko listino …(*naslov revizijske listine notranjerevizijske funkcije revidirane organizacije*)

Področje in predmet revizijskega posla

Področje in predmet revizije predstavljata opredelitev poslovnega področja, informacijskega sistema ali njegove komponente, ki bo predmet revizijskega posla. Načeloma naj bi bila predmet in področje revizijskega posla čim bolj natančno opredeljena, vendar to v primerih ko informacijski sistemi niso natančno dokumentirani, ni vselej mogoče.

Opredelitev področja/predmeta revizijskih postopkov naj bi obsegala vsaj:

- programske rešitve, ki bodo predmet revizijskih postopkov, 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[5].

Kadar zaradi nedokumentiranosti ni mogoče natančno opredeliti informacijskih rešitev, ki bodo vključene v revizijske postopke, je priporočljivo opredeliti poslovne procese, ki naj bi jih te rešitve pokrivale.

Primer 3: Opredelitev področja pri reviziji delovanja informacijskih sistemov po okviru COBIT 4.1

> V okviru revizije bomo pregledali delovanje informacijskega sistema organizacije …(*ime revidirane organizacije*) po okviru COBIT 4.1, kar zajema informacijske rešitve za podporo poslovnim procesom:
>
> - nabave,
> - skladiščenja,
> - prodaje,

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

- finančnega računovodstva in poročanja,
- upravljanja osnovnih sredstev

Pregledali bomo tudi tehnično infrastrukturo v obsegu, ki omogoča delovanje omenjenih poslovnih procesov.

Če v trenutku priprave listine o poslu še nimamo podatkov o točnem obsegu informacijskega sistema, ki bo predmet pregleda, lahko vanjo dodamo tudi člen, v katerem izpostavimo, da bo točen obseg pregleda določen v Načrtovalnem delovnem zapisu (ali drugem koraku revizijskega posla)

Pri revizijah učinkovitosti delovanja informacijskega sistema bo področje revizije najpogosteje opredeljeno kot informacijski sistem, ki je predmet posla.

Podrobna opredelitev področja revizije/pregleda je izjemno pomembna zato, da vse vpletene strani natančno razumejo, kaj je zajeto v postopke revizije/pregleda. Pogosto je smiselno še posebej poudariti, kaj bo zajeto v posel, npr. celotno komunikacijsko omrežje organizacije, programske rešitve, ki jih uporablja organizacija (pa niso naštete) ipd. Če tovrstna opredelitev ni smiselna v listini o poslu, jo je potencialno smiselno vključiti v Načrtovalni delovni zapis.

S podrobno opredelitvijo področja/predmeta revizije se lahko izognemo nenadzorovanemu širjenju revizijskih postopkov.

Sodila revizijskega posla

V listini o poslu moramo natančno opredeliti, kaj bomo uporabljali kot sodilo pri izvedbi posla. Kot sodila v poslu lahko uporabljamo splošno sprejete standarde, vodila in okvire dobrih praks ali pa sodila postavimo sami v sodelovanju z naročnikom posla.

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)[6], ki jih izdaja IIA,
- Kontrolni okvir za informacijske tehnologije COBIT, ki ga izdaja ISACA,
- ….

[6] Global Technology Audit Guide

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.

Primer 4: Opredelitev sodila pri reviziji delovanja informacijskih sistemov po okviru COBIT 4.1

> Za presojo učinkovitosti delovanja informacijskih sistemov v …(*ime revidirane organizacije*) bomo uporabili okvir dobrih praks COBIT 4.1, ki ga izdaja Inštitut za upravljanje IT (angl. IT Governance Institut).

Obseg revizijskega posla

Obseg revizijskega posla opredelimo oziroma omejimo s ponazoritvijo področja/predmeta revizije. Poleg predmeta revizije pa je potrebno opredeliti tudi obdobje, na katero se bo nanašala revizija.

Primer 5: Opredelitev področja/predmeta in časovne komponente posla

> Revizija bo obsegala učinkovitost delovanja informacijskega sistema ABC v obdobju …(*datum*), kar obsega naslednje programske rešitve …(*seznam programskih rešitev*).

Cilji revizijskega posla

Revizijski cilji so odvisni od revizijskega posla in morajo biti dogovorjeni z listino o poslu. Posebej pomembno je natančno opredeliti ali gre za revizijo oz. pregled, katerih cilj je izreči mnenje ali gre za dogovorjene postopke, ki se ne bodo zaključili z izrekom mnenja. V primeru revizije delovanja informacijskih sistemov po okviru COBIT 4.1 je cilj izreči mnenje.

Primer 6: Opredelitev cilja revizije

> Cilj revizijskega posla je ugotoviti, ali informacijski sistem (*ime informacijskega sistema, ki je predmet revizije*) ter funkcije, ki podpirajo njegovo delovanje, delujejo učinkovito in o tem izreči mnenje.

V praksi se strokovnjak za revizijo IS in dajanje zagotovil pogosto dogovarja za revizijski posel znotraj revizijske delovne skupine 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 delovno skupino 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.

Neodvisnost

Neodvisnost izvajalca in naročnika je mogoče opredeliti na različne načine.

Primer 7: Opredelitev neodvisnosti.

> Obe stranki te listine sta neodvisna izvajalca. Nobena stranka se ne bo, ne zdaj in ne v prihodnosti, obravnavala kot zastopnik, distributer ali predstavnik druge stranke. Nobena stranka se ne bo predstavljala, neposredno ali implicitno, kot zastopnik druge stranke ali na kakšen drug način ustvarila ali prevzela odgovornosti v korist ali v imenu druge stranke.

Ocena tveganja

Kadar se izvaja revizijski posel, kjer so sodila določena z znanimi okviri ali dobrimi praksami, kot je COBIT 4.1, pomembna tveganja praviloma izhajajo iz odmikov izvajanjih aktivnosti od aktivnosti, priporočenimi v izbranem sodilu. Kljub temu pa je potrebno okvir prilagoditi konkretnim okoliščinam, iz katerih izhaja revizijska naloga. Osnova za razumevanje tveganj posameznega revizijskega okolja je spoznavanje njegovih značilnosti v okviru postopkov načrtovanja revizijske naloge in priprave revizijskega programa.

Primer 8: Ocena tveganja

> Obseg in narava revizijskih postopkov, ki jih bo …(*ime strokovnjaka za revizijo IS in dajanje zagotovil ali družbe, ki je prevzela posel*) opravil da doseže navedene revizijske cilje bosta temeljila na oceni tveganja, ki bo opravljena preden se bosta pripravila končni načrt revizijskega dela ter revizijski program.

Rezultati revizijskega posla

Rezultat revizijskega dela je poročilo o revizijskem poslu, ki je lahko omejeno le na mnenje in potencialne pridržke (kadar strokovnjak za revizijo IS in dajanje zagotovil izrazi mnenje s pridržki). Že v listini o poslu pa se lahko strokovnjak za revizijo IS in dajanje zagotovil in naročnik dogovorita, da bodo vse bistvene ugotovitve, do katerih je prišel pri izvedbi posla, povzete v posebnem delu poročila. Pri tem naj strokovnjak za revizijo informacijskega

sistema in dajanje zagotovil 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.

Dobra praksa je vse ugotovitve pred izdajo potrditi z revidirancem, kadar je to le mogoče. Tudi to je včasih smiselno formalno navesti že v listini o poslu, saj se s tem vnaprej opredeli tudi odgovornost revidiranca za kakovost revizijskih ugotovitev.

Primer 9: Opredelitev rezultatov revizijskega dela.

> Po izvedbi revizijskih postopkov bomo pripravili poročilo, v katerem bomo izrazili naše mnenje o tem, ali je upravljanje informacijskega sistema (*ime informacijskega sistema, ki je predmet revizije*) zasnovano skladno z načeli okvira COBIT 4.1., skupaj z morebitnimi ugotovitvami, opisom iz obstoječega stanja izhajajočih tveganj ter našimi priporočili. Vsebino poročila bomo pred izdajo uradnega poročila potrdili z udeleženci revizijskega pregleda.

Pristojnost

V listini o poslu je potrebno opredeliti tudi pristojnosti strokovnjaka za revizijo informacijskih sistemov in dajanje zagotovil. Te se lahko nanašajo na dostop do listin in osebja, programskih rešitev, tehnološke infrastrukture in podobno.

Primer 10: Pravica dostopa do informacij.

> …(*ime revidiranca*) bo …(*ime strokovnjaka za revizijo IS in dajanje zagotovil ali družbe, ki je prevzela posel*) omogočil dostop do vseh informacij, ki bodo potrebne za zagotovitev revizijskih dokazov, ki so podlaga za doseganje revizijskih ciljev, med drugim do bistvenih informacij, dokumentov, informacijskih sistemov, zaposlenih in lokacij.

Omejitve pri izvedbi revizijskega posla

V nekaterih primerih bo naročnik omejil informacije, do katerih bo lahko dostopal strokovnjak za revizijo informacijskih sistemov in dajanje zagotovil, ali pa bo omejitve določil predmet revizije. Primeri omejitev so:

- strokovnjak za revizijo IS in dajanje zagotovil in naročnik se dogovorita, da določene nastavitve ali določeni dokumenti ne bodo vključeni v postopke npr. zaradi posebnih zahtev po varovanju njihove zaupnosti;
- informacijski sistem, ki predstavlja predmet pregleda, v času pregleda še ne deluje v produkcijskem okolju, zato se bodo postopki pregleda izvedli le v testnem okolju.

Primer 11: Omejitve pri dostopu do področja revizije v primeru pregleda v testnem ali pred-produkcijskem okolju.

> Informacijski sistem ABC bo v obdobju poteka revizijskega pregleda deloval v testnem okolju. Mnenje o tem, ali je upravljanje informacijskega sistema ABC zasnovano skladno z načeli okvira COBIT 4.1. se bo nanašalo na testno in ne na produkcijsko okolje sistema. Naše ugotovitve se bodo nanašale na testno okolje informacijskega sistema ter na nastavitve in postopke v obdobju testiranja. Pregled nastavitev informacijskega sistema ter njegovega delovanja v produkcijskem okolju, bi lahko dal drugačne rezultate.

Roki in pogoji revizijskega posla

V tem delu je v listini o poslu potrebno opredeliti roke izvajanja posla, zlasti roke, ko bo revizijska delovna skupina delala pri revidirancu. Smiselno je tudi vnaprej opredeliti datum izdaje osnutka revizorjevega poročila (ključno je, da se opredeli datum izdaje osnutka – v primeru, da strokovnjak za revizijo IS in dajanje zagotovil pošlje osnutek v potrditev revidirancu, ne more vplivati na čas, ki ga bo ta potreboval za pregled).

Primer 12: Opredelitev obdobja izvedbe revizijskega pregleda.

> Storitve, opredeljene v okviru ….(*točka ali paragraf, kjer je opredeljen posel*), se bodo izvajale v obdobju od … do …(*datum*).

Člani revizijske delovne skupine

V nekaterih primerih je smiselno v listini o poslu poimensko našteti člane revizijske delovne skupine, ki bo opravila postopke. Revizijska družba s tem prepreči morebitne lažne predstavnike družbe ter poveča varnost podatkov revidiranca. To je zlasti pomembno zaradi mlajših članov revizijske delovne skupine, ki navadno ne sodelujejo v dogovarjanju o poslu ter jih revidiranec/naročnik ne pozna.

Če revizijska družba pričakuje, da bo potrebno člane delovne skupine pred nastopom dela menjati (npr. zaradi velikih delovnih zahtev in težav z urnikom) je smiselno to točko izpustiti. Člane revizijske delovne skupine se vedno lahko določi v načrtovalnem delovnem dokumentu.

Predvideni prejemniki poročil

Dobra praksa je tudi poimensko našteti prejemnike poročila ter (po dogovoru že v listini o poslu) omejiti pravico distribucije poročila (in osnutkov poročila ter drugih komunikacij) tretjim osebam.

Pravice revidiranca

V dogovoru z naročnikom je smiselno na tem mestu opredeliti kakršnekoli posebne zahteve naročnika glede revidiranca. Do takih določb lahko pride, kadar naročnik in revidiranec nista ista organizacija ali kadar revidirana organizacijska enota izrecno zahteva opredelitev svojih pravic v postopku.

Pregledi kakovosti

Tudi če listina o poslu ne navaja podrobno članov revizijske delovne skupine, je smiselno izpostaviti ime in naziv osebe, ki bo odgovorna za zagotavljanje kvalitete opravljenega dela.

Datum izdaje osnutka poročila o revizijskem poslu

Smiselno je vnaprej opredeliti datum izdaje osnutka poročila o revizijskem poslu.

Primer 13: Opredelitev datuma izdaje osnutka revizorjevega poročila.

Osnutek revizorjevega poročila bo izdan najkasneje do …(*datum*)

Cena storitve

V Sloveniji je cena izvedbe storitev večinoma vnaprej natančno dogovorjena. Poleg cene storitve je včasih smiselno opredeliti tudi urne postavke osebja, ki bodo veljale, če bi se v dogovoru z naročnikom obseg dela razširil. Včasih se je mogoče na ta način izogniti sklepanju dodatne pogodbe, kar je lahko praktično, kadar do povečanja obsega posla pride nepričakovano (npr. odkritje pomembnega tveganja, prevare,…)

Smiselno je opredeliti tudi dinamiko plačevanja in morebitne zamudne obresti.