Dokument:	**PRIMER Poročilo o učinkovitosti delovanja informacijskega sistema osnutek**
Revizija:	Revizija učinkovitosti delovanja informacijskega sistema po okviru COBIT 4.1[1]
Namen dokumenta:	Podrobno opredeliti način poročanja o izsledkih revizijske naloge na primerih[2]
Povzetek točk:	
Seznam primerov:	

[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.

	Primer 6: Opredelitev cilja pregleda iii Primer 7: Predstavitev konteksta ugotovitve. Primer 8: Kazalo s pregledom ugotovitev. Primer 9: Obdobje, na katerega se nanaša posel Primer 10: Odgovornost strokovnjaka za revidiranje za podajo mnenja: Primer 11: Izjava o viru uradne trditve poslovodstva o učinkovitost kontrolnih postopkov Primer 12: Sodila za izražanje mnenja A: Primer 13: Sodila za izražanje mnenja B: Primer 14: Odgovornost poslovodstva za področje revizijskega posla: Primer 15: Opredelitev namena, za katerega je bilo pripravljeno poročilo A Primer 16: Opredelitev namena, za katerega je bilo pripravljeno poročilo B Primer 17: Izvedba pregleda v skladu s standardi ISACA. Primer 18: Omejitve revizije zaradi narave revidiranja Primer 19: Opredelitev področja pregleda Primer 20: Omejitve revizije zaradi narave revidiranja Primer 21: Omejitev strokovnjaka za revizijo IS in dajanje zagotovil pri dostopu do informacij Primer 22: Razkritja o nasprotujočih si in zavajajočih informacijah, ki jih je revizorju posredovalo poslovodstvo Primer 23: Temeljna načela opisa IS v reviziji po okviru dobrih praks COBIT Primer 24: Ugotovitve o odmikih od dobrih praks COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe Primer 25: Tveganja, povezana z odmiki od dobrih praks COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe Primer 26: Priporočila, povezana z odmiki od dobrih praks

	COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe Primer 27: Odziv poslovodstva. Primer 28: Sodila za izražanje mnenja: Primer 29: Besedilo pozitivnega mnenja o delovanju informacijskega sistema i. Primer 30: Besedilo pozitivnega mnenja o delovanju informacijskega sistema ii. Primer 31: Besedilo odklonilnega mnenja Primer 32: Besedilo mnenja s pridržki
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

Pričujoči dokument predpostavlja, da smo za sodilo v revizijskem poslu uporabili okvir COBIT v 4.1. Kaj konkretno bomo opredelili kot sodilo revizijskega posla je odvisno od dogovora v listini o poslu ali v načrtovalnem dokumentu (glej **1001 VODNIK Načrtovanje revizijskega posla**), od sodil pa je odvisna struktura in vsebina revizorjevega poročila.

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[3] prišel na podlagi opravljenih postopkov. Oblika in obseg poročila sta odvisna od vsebine revizijske naloge. Pri pripravi poročila pa mora

[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.

strokovnjak za revizijo IS in dajanje zagotovil upoštevati dokument **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[4], kjer so podane zahteve in priporočila za obliko in vsebino revizorjevega poročila.

1. Elementi naslovnega dela poročila

Standardi za revidiranje informacijskih sistemov in dajanje zagotovil na različnih mestih navajajo zahteve za obvezne in priporočene elemente revizorjevega poročila. Za ustrezno strukturirano poročilo je smiselno nekatere pomembne informacije, ki jih zahtevajo, vključiti v naslovno stran, spremno pismo ali prvo/drugo stran poročila. Poleg tega nekatere informacije niso obvezne, jih pa standardno najdemo na dobro pripravljenih poročilih. Ti elementi so:

- naziv in naslov naročnika;
- naziv in naslov revidirane organizacije/poslovne enote;
- predmet (ime) revizije;
- naziv, naslov in logotip revizijske hiše/ strokovnjaka za revizijo IS in dajanje zagotovil;
- število strani revizorjevega poročila

Priporočljivo je, da so vse strani revizorjevega poročila enotno oštevilčene, saj se s tem prepreči morebitna namerna ali nenamerna odstranitev strani poročila.

- poimenski seznam prejemnikov poročila;
- (po dogovoru) omejitev pravico distribucije poročila tretjim osebam.

[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.**

Primer 1: Opredelitev distribucije poročila

> Poročilo je namenjeno za interno uporabo in ne za distribuiranje zunanjim nadzornim institucijam oziroma tretjim osebam. Prejemniki poročila so našteti v nadaljevanju.
>
> (*ime revizorja / revizijske hiše*) ne prevzema nikakršne odgovornosti v zvezi z nepooblaščenim posredovanjem omenjenega dokumenta tretjim osebam.

- (kadar je primerno) imena sodelujočih na strani naročnika, revidiranca in imena članov revizijske ekipe ter nazive njihovih delovnih mest;
- status poročila (osnutek in verzija osnutka, končno poročilo);

Dokler se poročilo nahaja v statusu osnutka je smiselno, da besedo OSNUTEK vključimo tudi v glavo/nogo revizorjevega poročila, da se posamezne strani kasneje ne zamešajo z dejanskim poročilom, ter da osebe na strani revidiranca, ki so odgovorne za pregled poročila, razumejo, da lahko v tej fazi še ugovarjajo na morebitne napačne navedbe.

- stopnjo tajnosti dokumenta v skladu z internimi predpisi organizacije.

2. Struktura revizorjevega poročila

Standardi za revidiranje informacijskih sistemov in dajanja zagotovil ne predpisujejo, kako oz. v kakšnem vrstnem redu mora biti izpolnjena posamezna zahteva za revizorjevo poročilo. Možen primer strukture poročila je:

Primer 2: Predlog strukture revizorjevega poročila

1. **Spremno pismo/naslovna stran** z osnovnimi informacijami, ki jih zahtevajo standardi za revidiranje informacijskih sistemov in dajanja zagotovil
2. **Povzetek za poslovodstvo**
3. **Informacije o opravljenem delu/uvod**
   - Predstavitev revidiranca/revidirancev
   - Sodelujoči zaposleni/sodelavci področja revizije
   - Obdobje, zajeto v revizijski posel
   - Obdobje poteka revizijskega posla
   - Predstavite področja revizije

- Podroben opis informacijskega sistema
- Revizijski cilji
- Sodila, ki so bila uporabljena kot podlaga za sklepno ugotovitev
- Obseg revizijske naloge in morebitne omejitve pri izvedbi
- Uporabljeni standardi
- Metode revizijskega dela in načini pridobivanja revizijskih dokazov
- V revizijskem poslu sodelujoči strokovnjaki za revizijo IS in dajanje zagotovil in strokovni sodelavci

4. Ugotovitve, tveganja in priporočila

- Odziv poslovodstva

5. Mnenje

3. 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. Priporočljivo je, da se vselej nahaja na začetku poročila. Standardi nimajo posebnih zahtev za povzetek revizorjevega poročila, dobra praksa pa je:

- da v nekaj stavkih kratko povzema opravljeno delo,

Primer 3: Uvodno besedilo povzetka

> Na podlagi listine o poslu z dne …. smo izvedli revizijo učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*) pri čemer smo kot sodilo učinkovitosti uporabili okvir dobrih praks upravljanja informacijskih sistemov COBIT.
>
> Revizijo smo izvedli med … in… (*obdobje poteka posla*), nanaša pa se na obdobje med … in… (*obdobje, zajeto v revizijo*).

- da povzema revizijske cilje

Primer 4: Opredelitev cilja pregleda i

Cilji pregleda je ugotoviti, ali je kontrolno okolje informacijskega sistema (*ime informacijskega sistema*) zasnovano skladno z načeli okvira COBIT 4.1[5] in o tem izreči mnenje.

Primer 5: Opredelitev cilja pregleda ii

Cilji pregleda je ugotoviti, ali avtomatizirane kontrole programske rešitve za podporo blagajniškemu poslovanju (*ime informacijskega sistema*) dajejo razumno zagotovilo, da so zabeleženi in pravilno obračunani vsi prodani izdelki.

Primer 6: Opredelitev cilja pregleda iii

Cilji pregleda je bil ugotoviti, ali informacijski sistem (*ime informacijskega sistema*) ter funkcije, ki podpirajo njegovo delovanje, delujejo učinkovito.

- da je napisan v laikom razumljivem jeziku, s čim manj strokovnimi termini in kraticami – kratice, ki se jim ni mogoče izogniti, naj bi bile pojasnjene v sprotnih opombah dokumenta,
- da je glavno sporočilo podano v kratkih a razumljivih stavkih,
- da so ugotovitve postavljene v ustrezen kontekst, zlasti, da so realno predstavljena tveganja, povezana s posameznimi ugotovitvami,

Primer 7: Predstavitev konteksta ugotovitve.

Upravljanje in varovanje podatkov ni povsem v skladu z določili ZVOP-1, pri čemer pa je potrebno poudariti, da Organizacija razen kadrovske evidence nima drugih zbirk osebnih podatkov.

[5] 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.

Organizacija v oddelku IT zaradi omejenega števila zaposlenih ne more zagotoviti ločevanja vlog v skladu s priporočili COBIT, vendar pa to pomanjkljivost kompenzira z drugimi kontrolnimi mehanizmi. Zaradi omejitev procesorske zmogljivosti glavnega računalnika velike operacije, med drugim tudi prenos podatkov o dnevni proizvodnji v glavno knjigo, včasih niso izvršene, ali pa se ne izvršijo do konca. Kontrolni postopki oddelka računovodstva zagotavljajo, da se tovrstne napake ažurno opazijo, manjkajoče transakcije pa se nato knjižijo ročno. Ročno knjiženje kljub temu predstavlja tveganje, da nastanejo razlike med podatki v skladišču končnih izdelkov ter vknjižbami v glavno knjigo.

- da je povzetek poročila kar se da objektiven.

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 strani revizijskih kolegov, strokovnjak za revizijo IS in dajanje zagotovil prosi tudi neodvisno osebo (npr. mlajšega člana revizijske ekipe), da prebere zgolj povzetek[6]. 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 prišli.

Kadar je bilo sodelovanje z zaposlenimi revidiranca korektno in učinkovito, je smiselno v povzetek poslovodstva vključiti tudi zahvalo za sodelovanje.

4. Kazalo

Kazalo revizorjevega poročila je dober pokazatelj ustreznosti strukture poročila ter njegove preglednosti. Včasih strukturo poročila določajo različne zakonske zahteve ali zahteve standardov. Nekateri strokovnjaki za revidiranje in dajanje zagotovil za IT oblikujejo naslove ključnih ugotovitev tako, da kazalo pravzaprav predstavlja povzetek ugotovitev.

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

Primer 8: Kazalo s pregledom ugotovitev.

5. Uvod

Uvod lahko predstavlja ločen del poročila ali pa so informacije uvoda vključene v različne druge dele poročila. Uvod naj bi povzemal ključne tehnične vidike revizijske naloge. Ker je predvideno, da se lahko povzetek uporablja tudi kot ločen dokument, naj uvod ponovi nekatere elemente povzetka, predvsem:

- povzetek opravljenega dela,
- obdobje, na katerega se nanaša revizija,
- obdobje poteka revizijskih postopkov,
- revizijske cilje,
- kratko predstavitev področja revizije, ki je bilo dogovorjeno z listino o poslu ali z načrtovalnim delovnim zapisom.

Poleg tega naj strokovnjak za revizijo IS in dajanje zagotovil v uvod vključi nekatere standardne tekste, ki jih priporočajo Standardi za revidiranje informacijskih sistemov in dajanje zagotovil med drugim:

- čas ali obdobje, na katerega se nanaša delo, ocenjevanje ali merjenje zadeve

Primer 9: Obdobje, na katerega se nanaša posel

V revizijo smo zajeli obdobje od 1.1.2012 do vključno 30.6.2012 (v nadaljevanju: revidirano obdobje).

- izjavo, da je strokovnjak za revizijo IS in dajanje zagotovil ta posel izvedel zato, da izrazi mnenje o zadevi, na katero se nanaša posel[7],

Primer 10: Odgovornost strokovnjaka za revidiranje za podajo mnenja:

Naša odgovornost je izraziti mnenje o učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*).

- pri potrditvenem poslu izjavo s podatki o viru uradne trditve poslovodstva o učinkovitost kontrolnih postopkov[8],

Primer 11: Izjava o viru uradne trditve poslovodstva o učinkovitost kontrolnih postopkov

Vzpostavitev in delovanje kontrolnega okolja sistema (*ime informacijskega sistema*) na dan …(*datum*) je pregledala in preizkusila notranjerevizijska služba organizacije v obdobju med (*datum začetka pregleda*) in (*datum konca pregleda*). Rezultati dela notranjerevizijske službe so pokazali, da sta vzpostavitev in delovanje kontrolnega okolja sistema (*ime informacijskega sistema*) v vseh pomembnih pogledih učinkovita. Poslovodstvo organizacije je (*datum*) s sklepom (*številka sklepa*) potrdilo rezultate njihovega dela.

- opis uporabljenih sodil ali razkritje vira teh sodil[9],

Primer 12: Sodila za izražanje mnenja A:

Mnenje o učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*) smo izrazili na podlagi dobrih praks, podanih v okviru COBIT 4.1.

Primer 13: Sodila za izražanje mnenja B:

Pregled je bil opravljen v skladu z zahtevami standarda ISO 27001.

[7] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

[8] Izrecno priporočilo dokumenta Smernica 2401 Poročanje (G20).

[9] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

Ta navedba gre lahko tudi v tisti del poročila, kjer je izraženo mnenje.

- Izjavo, da je za vzdrževanje ustroja učinkovitega ustroja notranjega nadzora, vključno s kontrolnimi postopki za to področje dejavnosti, odgovorno poslovodstvo[10],

Primer 14: Odgovornost poslovodstva za področje revizijskega posla:

Poslovodstvo je odgovorno za pošteno predstavitev informacij o področju pregleda, na podlagi katerih smo prišli do naših zaključkov.

- 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[11],

Primer 15: Opredelitev namena, za katerega je bilo pripravljeno poročilo A

Pričujoče revizorjevo poročilo je bilo pripravljeno z namenom seznanitve poslovodstva organizacije (*ime*) o učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*), ključnih odmikih delovanja od dobrih praks ter priložnostih za potencialne izboljšave. Družba (*ime revizijske hiše*)/(*strokovnjak za revizijo IS in dajanje zagotovil*) ne prevzema odgovornosti, če se poročilo uporabi v kakršen koli drug namen ali če ga uporabi kdo drug.

Primer 16: Opredelitev namena, za katerega je bilo pripravljeno poročilo B

Pričujoče poročilo je bilo pripravljeno kot povzetek ključnih ugotovitev, ki izhajajo iz naših revizijskih postopkov ter vsebuje naše mnenje o učinkovitosti kontrol informacijskega sistema (ime *informacijskega sistema*), skladno z listino o poslu (*referenca na listino o poslu*). Poročilo se sme uporabljati interno in ni namenjeno zunanjim nadzornim institucijam.

Izjava o neprevzemanju odgovornosti ni primerna v vseh okoliščinah (na primer kadar poročilo pripravljamo izrecno za zunanje institucije).

[10] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

[11] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

- izjavo, da je bila revizija izvedena v skladu s Standardi za revidiranje informacijskih sistemov in dajanje zagotovil ali drugimi veljavnimi strokovnimi standardi[12],

Primer 17: Izvedba pregleda v skladu s standardi ISACA.

> Pregled (*naziv področja oz. ime pregleda*) smo izvedli v skladu Standardi za revidiranje informacijskih sistemov in dajanje zagotovil, ki jih pripravlja ISACA.

- 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[13].

Primer 18: Omejitve revizije zaradi narave revidiranja

> Revizija učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*) ni zasnovana za odkrivanje vseh slabosti v kontrolnih postopkih, ker se je izvedla v obdobju med … in… (*obdobje poteka revizije*) in se ni izvajala neprekinjeno skozi celo obdobje, na katerega se nanaša. Na podlagi mnenja, izraženega za obdobje med … in… (*obdobje, zajeto v pregled*) prav tako ni mogoče sklepati na učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*) v prihodnjih obdobjih, saj lahko ključne notranje kontrole postanejo neustrezne zaradi spremenjenih okoliščin oz. se lahko poslabša raven skladnosti delovanja informacijskega sistema (*ime informacijskega sistema*) z usmeritvami ali postopki.

[12] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

[13] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

Poleg tega so preizkusi kontrolnih postopkov izvedeni po metodi vzorčenja ter tako dajejo razumno, ne pa tudi popolno zagotovilo, da so se odkrile vse pomembno napačne navedbe, do katerih bi lahko prišlo zaradi prevare ali napake.

- nadaljnje pojasnjevalne podrobnosti o spremenljivkah, ki vplivajo na dano zagotovilo, in druge informacije, kot je ustrezno[14].

6. Področje revizijskega posla

Področje revizijskega posla je mogoče predstaviti ali že v uvodu ali kot ločeno poglavje revizorjevega poročila. Pri revizijah učinkovitosti delovanja informacijskega sistema bo področje revizijskega posla najpogosteje opredeljeno kot informacijski sistem, ki je predmet posla. Načeloma naj bi bilo področje posla čim bolj natančno opredeljeno že v listini o poslu ali načrtovalnem dokumentu, vendar to v primerih ko informacijski sistemi niso natančno dokumentirani, ni vselej mogoče. **Zato je ključno, da je področje revizije v poročilu kar se da natančno opredeljeno** ter da se tako zagotovi, da vsi deležniki v procesu natančno razumejo, kaj je bilo vključeno v revizijo in kaj iz nje izpuščeno.

Primer 19: Opredelitev področja pregleda

Pregled je obsegal učinkovitost delovanja informacijskega sistema (*ime informacijskega sistema*), kar obsega naslednje programske rešitve:

1. Programsko rešitev za upravljanje osnovne organizacijske dejavnosti (npr. programsko rešitev za podporo bančnim procesom upravljanja s komitenti, bančnemu okencu in opravljanju bančnih poslov komitentov in poročanje nadzornim inštitucijam),
2. Programsko rešitev za vodenje računovodstva, kontroling in upravljanje kadrovskih virov (npr. SAP modula FI/CO in HR),
3. Programsko rešitev za podporo procesom elektronskega bančništva.

Poleg naštetih programskih rešitev je pregled učinkovitosti delovanja informacijskega sistema organizacije vključeval ključno tehnološko

[14] Neposredno povzeto po dokumentu Smernica 2401 Poročanje (G20).

infrastrukturo, na kateri delujejo naštete programske rešitve med drugim rešitev za upravljanje podatkovnih zbirk Oracle 10g, podatkovni strežnik, na katerem je nameščena QNAP TS-x59 Pro z operacijskim sistemom Microsoft Windows Server 2008 R2, aplikativni strežniki HP DL380G7 in dva strežnika HP ML350 z operacijskim sistemom Microsoft Windows Server 2008 R2 ter tisti elementi komunikacijskega omrežja organizacije, katerih delovanje je neposredno povezano z zagotavljanjem delovanja naštetih programskih rešitev.

Podrobna opredelitev področja revizijskega posla je izjemno pomembna zato, da vse v vpletene strani natančno razumejo, kaj je zajeto v postopke. Pogosto je smiselno še posebej poudariti, kaj v posel ni bilo zajeto, npr. celotno komunikacijsko omrežje organizacije, programske rešitev, ki jih uporablja organizacija, pa niso naštete ipd.

7. Omejitve obsega revizijskih postopkov

Kadar je strokovnjak za revizijo in dajanje zagotovil pri svojem delu naletel na kakršnekoli pomembne omejitve svojih opravljenih postopkov, mora te razkriti v revizijskem poročilu. Do omejitev lahko pride iz različnih razlogov – do nekaterih zaradi same narave revidiranja.

Primer 20: Omejitve revizije zaradi narave revidiranja

Revizija (*naziv področja oz. ime revizije*) ni zasnovana za odkrivanje vseh slabosti v kontrolnih postopkih, ker se je izvedla v obdobju med … in… (*obdobje poteka revizije*) in se ni izvajala neprekinjeno skozi celo obdobje, na katerega se nanaša. Na podlagi mnenja, izraženega za obdobje med … in… (*obdobje, zajeto v pregled*) prav tako ni mogoče sklepati na (*naziv področja oz. ime revizije*) v prihodnjih obdobjih, saj lahko ključne notranje kontrole postanejo neustrezne zaradi spremenjenih okoliščin oz. se lahko poslabša raven skladnosti (*naziv področja oz. ime revizije*) z usmeritvami ali postopki.

Poleg tega so preizkusi kontrolnih postopkov izvedeni po metodi vzorčenja ter tako dajejo razumno, ne pa tudi popolno zagotovilo, da so se

odkrile vse pomembno napačne navedbe, do katerih bi lahko prišlo zaradi prevare ali napake.

To omejitev je smiselno vključiti v velik del poročil o revizijskih poslih.

Do omejitev pa lahko pride tudi zaradi ravnanj revidiranca, na primer zaradi omejitev,ki jih postavlja revizorju pri njegovem delu.

Primer 21: Omejitev strokovnjaka za revizijo IS in dajanje zagotovil pri dostopu do informacij

Organizacija nam pri izvedbi pregleda ni predstavila in razkrila informacij (*navesti je treba opis zahtevanih informacij ter okoliščine – datum, kraj način ipd. v katerih je revizor zaprosil za informacije*), čeprav bi jih v skladu z zahtevo o popolnosti predstavitev in razkritij o delovanju morala predstaviti in razkriti.

Primer 22: Razkritja o nasprotujočih si in zavajajočih informacijah, ki jih je revizorju posredovalo poslovodstvo

Informacije v poročilu notranje revizije o delovanju avtomatiziranih notranjih kontrol na področju (*ime področja*) se po naši oceni pomembno razlikujejo od poročila o delovanju istih kontrol, ki ga je pripravilo poslovodstvo oddelka IT podpore.

8. Podroben opis informacijskega sistema

Strokovnjak za revizijo IS in dajanje zagotovil se lahko odloči za podrobnejši opis informacijskega sistema.

Primer 23: Temeljna načela opisa IS v reviziji po okviru dobrih praks COBIT

Pri reviziji po okviru dobrih praks COBIT je smiselno, da poleg klasičnega opisa informacijskega sistema, ki vključuje podroben opis ključnih programskih rešitev ter tehnične infrastrukture, na kateri temelji, pripravi tudi opise obstoječega stanja procesov upravljanja IT na vseh 4 COBIT domenah:

* Procesi načrtovanja in organiziranja informacijskega sistema (*ime informacijskega sistema*),

* Procesi nabave in vpeljave informacijskega sistema (*ime informacijskega sistema*),

* Procesi izvajanja in podpore delovanju informacijskega sistema (*ime informacijskega sistema*),

* Procesi spremljanja in vrednotenja delovanja informacijskega sistema (*ime informacijskega sistema*).

Ugotovitve o pomembnih pomanjkljivostih, kontrolnih slabostih ali priložnostih za izboljšanje so praviloma vezane na posamezna področja delovanja informacijskega sistema. Strokovnjak za revizijo IS in dajanje zagotovil jih lahko predstavi tako, da jih razdeli v 4 poglavja skladu s COBIT domenami, v začetku posameznega poglavja predstavi obstoječe stanje procesov upravljanja IT ter pod tem našteje svoja opažanja.

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.

9. Ugotovitve o odmikih od dobrih praks COBIT

Okvir COBIT, ki smo ga uporabili kot sodilo v našem primeru, podaja dobre prakse upravljanja informacijskih sistemov ter sodila, na podlagi katerih je mogoče oceniti zrelost posameznega procesa z vidika učinkovitosti delovanja in kontrol (glej tudi dokument **105001 VODNIK Razumevanje okvira COBIT**).

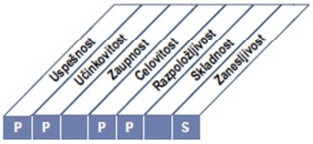
Poročilo naj, če je tako dogovorjeno, poleg mnenja, vključuje tudi navedbe odmikov od dobrih praks COBIT, z njimi povezana tveganja ter priporočila za izboljšanje.

Pregled 1: Dobre prakse COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe[15]

OPIS PROCESA

AI6 Upravljajte spremembe

Vse spremembe infrastrukture in aplikacij v produkcijskem okolju, vključno z nujnimi vzdrževanji in popravki, je treba formalno upravljati na nadzorovan način. Spremembe (vključno s spremembami postopkov, procesov, sistemov in parametrov storitev) so pred vpeljavo ustrezno evidentirane, ocenjene in odobrene, po vpeljavi pa se dobljeni rezultati primerjajo z načrtovanimi rezultati. S tem se zagotovi zmanjšanje tveganja negativnega vpliva na stabilnost ali celovitost produkcijskega okolja.



Nadzor nad procesom IT

Upravljajte spremembe,

ki izpolnjuje poslovno zahtevo za IT glede

odzivanja na poslovne zahteve v skladu s poslovno strategijo, pri čemer se zmanjšujejo napake in ponovni popravki rešitev in storitev

z usmerjanjem na

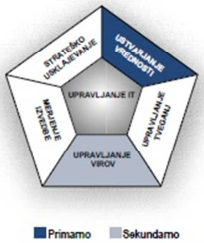
nadzor ocene vpliva, odobritve in vpeljave vseh sprememb v infrastrukturi IT, aplikacijah in tehničnih rešitvah, minimiziranje napak zaradi nepopolnih specifikacij zahtevkov in zaustavitev vpeljave nepooblaščenih sprememb,

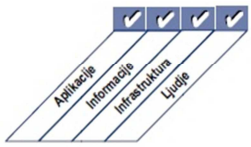
kar se doseže

- z opredelitvijo in objavo postopkov za spremembe, vključno z nujnimi spremembami,
- z ocenjevanjem, določanjem prednosti in odobravanjem sprememb,
- s spremljanjem stanja in poročanjem o spremembah

ter se meri

- s številom motenj ali napak v podatkih zaradi netočnih specifikacij ali nepopolne ocene vpliva,
- s ponovnimi popravki aplikacij ali infrastrukture zaradi neustreznih specifikacij spremembe,
- z odstotkom sprememb, realiziranih po formalnem procesu upravljanja s spremembami.





[15] Vir: Okvir COBIT 4.1.

Pregled 2: Dobre prakse COBIT na področju AI - Nabavite in vpeljite -kontrolni cilji AI6 Upravljajte spremembe[16]

KONTROLNI CILJI

AI6 Upravljajte spremembe

AI6.1 Standardi in postopki sprememb
Vzpostavite formalne postopke za standardizirano upravljanje sprememb za obravnavo vseh zahtev za spremembe (vključno z vzdrževanjem in popravki) aplikacij, postopkov, procesov, sistemskih in storitvenih parametrov in temeljnih platform.

AI6.2 Ocena vpliva, razvrščanje po pomembnosti in odobravanje
Ocenite vse zahteve za spremembe na strukturiran način, da določite vpliv na produkcijski sistem in na njegovo funkcionalnost. Zagotovite, da so spremembe kategorizirane, prednostno razvrščene in odobrene.

AI6.3 Nujne spremembe
Vzpostavite proces za opredelitev, sprožitev, testiranje, dokumentiranje, ocenjevanje in odobravanje nujnih sprememb, ki se ne izvajajo po vzpostavljenem procesu sprememb.

AI6.4 Spremljanje statusa sprememb in poročanje
Vzpostavite sistem za spremljanje in poročanje, ki bo zagotavljal dokumentiranje zavrnjenih sprememb, sporočanje stanja odobrenih sprememb, sprememb v teku in poročanje o zaključenih spremembah. Zagotovite, da se odobrene spremembe vpeljujejo po načrtu.

AI6.5 Zaključek spremembe in dokumentacija
Kadarkoli se vpeljejo spremembe sistema, ustrezno posodobite pripadajočo sistemsko in uporabniško dokumentacijo in postopke.

Primer 24: Ugotovitve o odmikih od dobrih praks COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe

Ugotovitve

Organizacija v praksi sicer uporablja nekatere dobre pristope k uvajanju sprememb, nima pa formalno potrjenih ter za vse zaposlene zavezujočih postopkov uvajanja sprememb. Področje upravljanja sprememb zato v nekaterih pogledih odstopa od dobrih praks[17]:

1. <u>Uporabniške zahteve so slabo dokumentirane.</u>

Uporabniške zahteve za nove programske rešitve ali njihove spremembe niso jasno in pregledno pripravljene. Uporabniki svoje zahteve sicer pripravijo v pisni obliki, njim samim pa je prepuščeno, katere podatke bodo vanje vključili. Organizacija nima navodil za pripravo uporabniških zahtev ali standardnih vzorcev zanje. Prav tako ni strukturiranega postopka za spreminjanje uporabniških zahtev po tem, ko se je razvoj že začel

[16] Vir: Okvir COBIT 4.1.

[17] Generična oblika stavka, ki nakazuje, da organizacija informacijskega sistema ne upravlja skladno z revizijskimi sodili oz. načeli (v tem primeru COBIT)

ter za odobritev sprememb, ki jih po začetku razvojnega procesa še zahtevajo uporabniki.

2. Ocenjevanje vpliva spremembe ni strukturirano in se ne izvaja redno.

Organizacija ne uporablja postopka, s katerim bi ocenila vpliv nameravane spremembe na informacijski sistem (*ime informacijskega sistema*), zlasti potencialne vplive na skupne šifrante in druge matične podatke.

3. Testiranje pred prenosom v produkcijsko okolje je pomanjkljivo.

Informacijski sistem (*ime informacijskega sistema*) ima poleg produkcijskega tudi ločeno testno okolje. Testiranje novo razvitih rešitev ter sprememb v testnem okolju izvajajo predvsem odgovorni informatiki, testiranje, ki ga opravijo končni uporabniki, se redko izvaja. Napake v programiranju ali interpretaciji vsebinskih zahtev se zato pogosto odkrijejo, ko je sprememba že v produkcijskem delovanju. Organizacija tudi ne uporablja koncepta "lastnika" programske rešitve – osebe, ki bi bila odgovorna za potrditev vsebinske ustreznosti posamezne zahteve ter odobritev njenega prenosa v produkcijsko okolje.

4. Večje število razvijalcev ima neposreden dostop v produkcijsko okolje informacijskega sistema (*ime informacijskega sistema*).

Organizacija ima omejeno število usposobljenih informatikov. Zaradi kadrovske stiske ne more zagotavljati ustreznega ločevanja vlog med produkcijskim, testnim in razvojnim okoljem.

5. Organizacija nima opredeljenega postopka uvedbe izrednih (nujnih) sprememb.

Izredne spremembe se pogosto uvedejo v produkcijsko delovanje brez testiranja ter celo brez kakršnekoli evidence, da so bile sploh kdaj razvite in uvedene.

6. Uporabniki nimajo možnosti spremljati statusa svojih zahtevkov.

Uporabniki, ki naročijo različne nadgradnje in popravke pogosto ne vedo, ali so razvojniki sploh začeli delati na zahtevkih ali ne.

7. Sistemska dokumentacija je pomanjkljiva.

Odgovorni informatiki o nekaterih elementih informacijskega sistema (*ime informacijskega sistema*), na primer orodju za upravljanje zbirk podatkov Oracle, vodijo ustrezno dokumentacijo. Dokumentacija drugih delov sistema, na primer vsebinski opisi modulov in funkcionalnosti, je slabše pripravljena ali je celo ni. Zaradi omejenosti kadrovskih virov, kompleksnosti sistema in pomanjkljivosti v strateškem načrtovanju je slabo dokumentiran tudi Informacijski sistem (*ime informacijskega sistema*) kot celota, njegovi skupni elementi ter soodvisnosti med programskimi rešitvami.

Primer 25: Tveganja, povezana z odmiki od dobrih praks COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe

Tveganja

Organizacija je zaradi neustreznih postopkov uvajanja sprememb v revidiranem obdobju doživela dva primera daljšega nedelovanja sistema (*ime informacijskega sistema*) - obakrat ob postopkih uvajanja nujnih sprememb. Druge posledice neprimerno strukturiranih postopkov uvajanja sprememb v programske rešitve so lahko:

- nadgradnja programske rešitve ali odprava napake ne dosega želenih učinkov, ali pa ima neugoden vpliv na kakšno drugo funkcionalnost programske rešitve,
- pričakovanja uporabnikov se razlikujejo od dejansko pripravljene nove rešitve ali izvedene spremembe,
- sprememba ni izvedena v predvidenem roku,
- že razvite rešitve je treba večkrat dopolnjevati in spreminjati,
- sprememba programske rešitve povzroči napake v podatkih,

- sprememba programske rešitve povzroči napake v produkcijskem delovanju programske rešitve oziroma poslabša njeno stabilnost,
- razvojniki v programsko kodo programskih rešitev sistema (*ime informacijskega sistema*) vstavijo neodobrene ali celo škodljive rutine.

Primer 26: Priporočila, povezana z odmiki od dobrih praks COBIT na področju AI - Nabavite in vpeljite - proces AI6 Upravljajte spremembe

Priporočila

Organizaciji priporočamo, naj pripravi formalno politiko uvajanja novih programskih rešitev ter upravljanja sprememb, ki bo prilagojena sistemu in uporabnikom. Pri pripravi politik in postopkov koordiniranja in uvajanja sprememb priporočamo, naj upošteva zlasti naslednja načela:

- Vsaka sprememba programske rešitve mora biti sledljiva. To pomeni, da mora za vsako spremembo obstajati ustrezna sled vsaj o tem, kdo jo je zahteval, pripravil in potrdil. Uporabniki naj bi imeli, če je le mogoče, nadzor nad statusom sprememb, ki so jih predlagali, ter informacije o tem, kdaj bo posamezna sprememba najverjetneje pripravljena za testiranje. Zlasti zunanji izvajalci morajo spremembe in dopolnitve sistemske in programske opreme ustrezno dokumentirati.
- Spremembe naj bi bile pred prenosom v produkcijsko okolje testirane v testnem okolju. Del testov naj bi izvedli končni uporabniki, ti pa naj bi tudi potrdili, da je sprememba pripravljena za prenos v produkcijsko delovanje. Izvajali naj bi se osnovno testiranje, uporabniško testiranje scenarijev, integracijsko testiranje, testiranje tehnične infrastrukture in druga smiselna testiranja.
- Smiselno je, da se spremembe programskih rešitev obravnavajo glede na tveganje, ki ga prinašajo delovanju sistema, ter glede na njihov potencialni vpliv. Za lažje praktično upravljanje sprememb naj organizacija pripravi različne

operativne postopke uvedbe sprememb glede na velikost oziroma pomen spremembe.

- Poleg postopkov rednih sprememb je smiselno pripraviti tudi postopke za izredne (nujne) spremembe. Te ne smejo ostati nezabeležene (zavedemo jih lahko po njihovi uvedbi).

Pregled 3: Dobre prakse COBIT na področju AI - Nabavite in vpeljite - zrelostni model AI6 Upravljajte spremembe

ZRELOSTNI MODELI

AI6 Upravljajte spremembe

Upravljanje procesa *Upravljajte spremembe*, ki izpolnjuje poslovno zahtevo za IT glede *odzivanja na poslovne zahteve v skladu s poslovno strategijo, pri čemer se zmanjšujejo napake in ponovni popravki v rešitvah in storitvah*, je

0 Neobstoječe, kadar
Organizacija nima opredeljenega procesa za upravljanje sprememb; te je mogoče vpeljati praktično brez vsakega nadzora. Organizacija se ne zaveda, da so lahko spremembe moteče za IT in poslovne dejavnosti, prav tako se ne zaveda koristi dobrega upravljanja sprememb.

1 Začetno/ Ad Hoc, kadar
Organizacija zaznava, da je treba spremembe upravljati in nadzorovati. Prakse se razlikujejo, prav tako je verjetno, da bo prišlo do neodobrenih sprememb. Ima slabo ali neobstoječo dokumentacijo o spremembah, dokumentacija o konfiguracijah pa je nepopolna in nezanesljiva. Napake se bodo verjetno pojavile skupaj z motnjami produkcijskega okolja zaradi slabega upravljanja sprememb.

2 Ponovljivo, vendar intuitivno, kadar
Organizacija ima neformalen proces upravljanja sprememb in večina le-teh upošteva ta pristop, vendar je nestrukturiran, na začetni ravni in nagnjen k napakam. Dokumentacija o konfiguracijah je nedosledna, pred spremembo pa se načrtuje in ocenjuje vplive le v omejenem obsegu.

3 Opredeljeno, kadar
Organizacija ima opredeljen formalni proces upravljanja sprememb, ki vključuje kategorizacijo, prednostno razvrščanje, postopke v primeru sile, odobritev sprememb in upravljanje izdaj. V organizaciji obstajajo zametki skladnosti. Postopki in procesi se pogosto zaobidejo. Lahko pride do napak, prav tako se občasno pojavljajo neodobrene spremembe. Analiza vpliva sprememb IT na poslovne dejavnosti postaja formalizirana, da se podpre načrtovano uvajanje novih aplikacij in tehnologij.

4 Vodeno in merljivo, kadar
Proces upravljanja sprememb je dobro razvit in se dosledno upošteva za vse spremembe. Vodstvo trdno verjame, da je izjem le malo. Proces je uspešen in učinkovit, vendar zagotavljanje doseganja kakovosti temelji pretežno na ročnih postopkih in kontrolah. Vse spremembe se natančno načrtujejo, opravi se ocena vpliva, da se zmanjša verjetnost težav po uvedbi. Organizacija izvaja postopek odobritve. Dokumentacija o upravljanju sprememb je ažurirana in pravilna, spremembam se formalno sledi. Dokumentacija o konfiguraciji je navadno pravilna. Načrtovanje in vpeljava upravljanja sprememb IT postajata vedno bolj združena s spremembami v poslovnih procesih, da se zagotovi obravnava vprašanj usposabljanja, organizacijskih sprememb in neprekinjenega poslovanja. Pojavlja se vedno večje usklajevanje med upravljanjem sprememb IT in ponovnim oblikovanjem poslovnega procesa. Organizacija ima dosleden proces za spremljanje kakovosti in izvedbe procesa upravljanja sprememb.

5 Optimizirano, kadar
Organizacija redno pregleduje proces upravljanja sprememb in ga posodablja, da ostaja v skladu z dobrimi praksami. Postopek pregleda odraža rezultate spremljanja. Informacije o konfiguraciji so v računalniški obliki in zagotavljajo nadzor verzij. Sledenje spremembam je sofisticirano in vključuje orodja za odkritje neodobrene in nelicenčne programske opreme. Upravljanje sprememb IT je združeno z upravljanjem poslovnih sprememb za zagotovitev, da IT omogoča večjo produktivnost in da ustvarja nove poslovne priložnosti za organizacijo.

Tabela 1: Ocena zrelosti procesov COBIT na področju AI - Nabavite in vpeljite - zrelostni model AI6 Upravljajte spremembe

Proces področja AI	Ocenjena stopnja zrelosti procesa	0	1	2	3	4	5
AI1 Določite avtomatizirane rešitve	4						
AI2 Nabavite in vzdržujte aplikacijske programe	3						
AI3 Nabavite in vzdržujte tehnološko infrastrukturo	3						
AI4 Omogočite delovanje in uporabo	2						
AI5 Zagotovite vire IT	4						
AI6 Upravljajte spremembe	2						
AI7 Namestite in potrdite rešitve in spremembe	1						

Če je le mogoče, naj bo ob ugotovitvah naveden tudi odziv poslovodstva, zlasti pojasnila ugotovitev, opis prihodnjih korakov in podobno.

Primer 27: Odziv poslovodstva.

Odziv poslovodstva

Na podlagi ugotovitev revizije smo se odločili, da formaliziramo naše postopke uvajanja sprememb. Že v marcu nameravamo izvesti usmerjeno oceno tveganj navedenega področja, kar bo podlaga da opredelimo, kakšne (in kako obsežne) postopke dejansko potrebujemo. Osnutek novih postopkov upravljanja sprememb bi moral biti po načrtih pripravljen do maja.

10. 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**. V primeru revizije učinkovitosti delovanja informacijskega sistema ABC po okviru COBIT 4.1 gre za izražanje mnenja za posel revizije (torej se bo mnenje izražalo v

pozitivni obliki), sodila, ki so podlaga za izražanje mnenja pa so podana v okviru dobrih praks COBIT 4.1.

Sodila za izražanje mnenja lahko podamo v uvodu, kot posebno poglavje poročila in/ali v samem mnenju (za razliko od številnih drugih navedb, ni narobe, če so izražena oz. opisana na dveh mestih).

Primer 28: Sodila za izražanje mnenja:

> Mnenje o učinkovitosti delovanja informacijskega sistema (*ime informacijskega sistema*) smo izrazili na podlagi dobrih praks, podanih v okviru COBIT 4.1.

Mnenje je lahko pozitivno, mnenje s pridržki ali odklonilno mnenje. Načini izražanja mnenja so prav tako različni oz. se med sabo deloma razlikujejo.

Primer 29: Besedilo pozitivnega mnenja o delovanju informacijskega sistema i.

> Po našem mnenju sta informacijski sistem (*ime informacijskega sistema*) ter njegovo vzpostavljeno kontrolno okolje v obdobju …(*datum*) v vseh pomembnih pogledih učinkovito delovala.

Primer 30: Besedilo pozitivnega mnenja o delovanju informacijskega sistema ii.

> Na podlagi opravljenih postopkov menimo, da sta informacijski sistem (*ime informacijskega sistema*) ter njegovo vzpostavljeno kontrolno okolje v obdobju …(datum) v vseh pomembnih pogledih učinkovito delovala.

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 revizijskega posla;
- da je slabost v delovanju kontrol pomembna v kontekstu področja revizijskega posla,
- da določena slabost v delovanju kontrol ali druga ugotovitev predstavlja pomembno neskladnost z zakonodajo ali tveganje prevare,
- …

Primer 31: Besedilo odklonilnega mnenja

Pri reviziji delovanja informacijskega sistema (*ime informacijskega sistema*) ter vanj vgrajenih in v zvezi z njim vzpostavljenih kontrol smo prišli do ugotovitev, na podlagi katerih sklepamo, da v obdobju …(*datum*) ne delovanje samega informacijskega sistema (*ime informacijskega sistema*) ne delovanje vanj vgrajenih in v zvezi z njim vzpostavljenih kontrol ni učinkovito.

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 revizijskega posla pomembne slabosti, ne pa tudi bistvene pomanjkljivosti.

Primer 32: Besedilo mnenja s pridržki

Z izjemo v nadaljevanju naštetih pridržkov, so po našem mnenju v obdobju …(*datum*) informacijski sistem (*ime informacijskega sistema*) ter vanj vgrajeni kontrolni mehanizmi v vseh pomembnih delovali učinkovito.