Dokument:	**PRIMER Ocena tveganj in revizijski programa za SPLOŠNE RAČUNALNIŠKE KONTROLE osnutek**
Namen dokumenta:	Dokument povzema revizorjeve postopke za pridobitev informacij o delovanju splošnih računalniških kontrol, ki jih revizor določi na podlagi ocenjenih tveganj okolja revidirane organizacije.
Povzetek točk:	1. Strategija informacijskih sistemov 2 2. Nadzor nad obdelavo podatkov in procesiranjem 3 3. Fizična in logična varnost informacijskega sistema 6 4. Upravljanje sprememb informacijskega sistema 9
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

Sodila presoje oziroma revizijski program lahko oblikujemo sami (brez zanašanja na nek splošno sprejeti okvir dobrih praks, kot je na primer COBIT[1]), vendar moramo v listini o poslu, načrtu revizijske naloge in poročilu razkriti sodila, po katerih smo opravljali revizijo. V tem

[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

vzorčnem programu smo vidik ocenjevanja tveganj združili z vidikom splošnih dobrih praks za kontrolno okolje, ki smo jih uporabili kot odziv na zaznana tveganja in hkrati za sodilo revizorja. To je mogoče narediti le v nekaterih revizijah[2]

1. Strategija informacijskih sistemov

Tveganja[3]	**Vzorčne kontrole / kontrolni cilji**	**Opis področja**[4]	**Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja**	**Ugotovitve**
Informacijski sistem v prihodnosti ne bo zagotavljal ustreznih podatkov za finančno-računovodsko poročanje in/ali ne bo ustrezno podpiral ključnih poslovnih procesov organizacije.	Strategije, načrti ter proračuni za informacijsko tehnologijo so skladni s poslovnimi in strateškimi cilji organizacije		o Primerjava strateškega načrta razvoja organizacije ter načrta razvoja informacijskih tehnologij. o Pregled letnih taktičnih načrtov za razvoj informacijske tehnologije.	

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 na podlagi opredelitve t.i. *splošnih računalniških kontrol*. Primer je izbran ker gre za pogost tip pregleda. Dokument mora biti prilagojena zahtevam konkretne revizijske naloge.

[3] Ocena tveganj je lahko združena s pregledom vzorčnih kontrolnih ciljev, lahko pa jih navajamo in pregledamo v ločenih dokumentih.

[4] Ta del programa navadno izpolnimo istočasno s spoznavanjem informacijskega okolja organizacije. V tej fazi podatki, ki jih navaja revidirana enota pogosto še niso povsem zanesljivi, saj revizor še ni izvedel postopkov za njihovo potrditev.

Tveganja[3]	**Vzorčne kontrole / kontrolni cilji**	**Opis področja**[4]	**Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja**	**Ugotovitve**
Razvoj, nabava in uvajanje informacijskih tehnologij ne bo potekalo skladno s prihodnjim razvojem organizacije.	Projekti za razvoj, nabavo in uvedbo informacijskih tehnologij ustrezajo dejanskim potrebam organizacije.		o Primerjava ključnih prihodnjih projektov informacijskih tehnologij s strateškimi načrti organizacije.	
Podpora informacijskemu sistemu v prihodnosti ne bo ustrezna.	Organizacija ima interne ali zunanje zagotovljene strokovnjake, ki bodo v prihodnosti vzdrževali in podpirali informacijski sistem.		o Presoja razpoložljivosti strokovnjakov informacijskih tehnologij glede na tehnologijo, ki jo uporablja organizacija (kontrolni cilj je še posebej relevanten v primeru organizacij s starejšimi informacijskimi sistemi, ki niso razviti na pogosto uporabljanih in poznanih tehnologijah)	

2. Nadzor nad obdelavo podatkov in procesiranjem

Tveganja	**Vzorčne kontrole / kontrolni cilji**	**Opis področja**	**Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja**	**Ugotovitve**
Velike obdelave podatkov niso izvedene, niso	Sistem avtomatsko zazna		o Pregled (sistemskih)	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
izvedene v celoti ali so izvedene z napakami, kar povzroči napake v finančnih in računovodskih podatkih. Vsa programska oprema za paketno in sprotno procesiranje transakcij v produkcijskem okolju se izvaja pravočasno in z normalnim zaključkom procesiranja.	nedokončane obdelave podatkov oziroma obdelave podatkov, ki so se izvedle z napakami. Rezultati avtomatskih obdelav so pravilni, pravočasni in uspešno zaključeni.		dnevniških zapisov o poteku in izvajanju obdelav. o Pregled (sistemskih) dnevniških zapisov napak v obdelavah. o Pregled urnikov avtomatskih obdelav. o Pregled korakov v skripti za izvedbo obdelave.	
V avtomatskih obdelavah so (namerno) vgrajene napake, ki posledično povzročijo napake v finančnih in računovodskih podatkih.	Postopki razvoja velikih obdelav so formalizirani in spremljani. Vloge pri razvoju avtomatičnih obdelav so ustrezno ločene. Dostopi do skript za avtomatične obdelave so formalizirani in spremljani.		o Pregled postopkov razvoja / konfiguracije velikih obdelav. o Ponoven predračun ključnih obdelav. o Pregled transakcije od nastanka do knjižbe oz. prenosa v glavno knjigo. o Pregled ločevanja vlog pri razvoju avtomatičnih obdelav ter njihovem prenosu v produkcijsko	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
			delovanje. o Pregled načina omejevanja dostopa do skript za avtomatične obdelave ter dostopa do urnika avtomatičnih obdelav. o Pregled dostopa do funkcionalnosti za konfiguracijo avtomatičnih obdelav.	
Organizacija v primeru nesreče ali namernega incidenta izgubi podatke, o svojem poslovanju ter potrebne za prihodnje poslovanje.	Podatki so shranjeni v skladu z zakoni, predpisi in politiko Organizacije, da bi tako omogočili njihovo ponovno pridobitev, ko bi bilo potrebno. Izdelujejo se varnostne kopije, shranjujejo se na varni lokaciji in so primerno označene.		o o Pregled postopkov načrtovanja izdelave varnostnih kopij podatkov ter njihovo ohranjanje ter njihovega brisanja, ko kopije niso več potrebne. o Pregled urnika izdelave varnostnih kopij. o Pregled (sistemskih) dnevniških zapisov o izdelavi varnostnih kopij ter	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
	Odgovorni zaposleni periodično preverijo možnost obnove podatkov iz varnostnih kopij.		o napakah pri izdelavi varnostnih kopij. o Preiskovanje opredmetenih osnovnih sredstev -pregled načina hranjenja varnostnih kopij (priporočljivo na oddaljeni lokaciji). o Preiskovanje opredmetenih osnovnih sredstev - pregled medijev, na katerih so varnostne kopije podatkov ter njihovih oznak.	

3. Fizična in logična varnost informacijskega sistema

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
Uporabniki nenamerno kršijo načela	Organizacija je uvedla in		o Pregled dokumentacije povezane z varnostno politiko	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
informacijske varnosti ter se izpostavljajo možnostim prevar in kraje identitete.	formalno objavila varnostno politiko, ki vsebuje in določa osnovna načela informacijske varnosti.		Organizacije.	
Nepooblaščeni uporabniki lahko dostopajo do programskih rešitev in podatkov ter jih nepooblaščeno spremenijo (možnost prevare)	Dostop do programskih rešitev, podatkov in drugih virov informacij je omejen na tiste uporabnike, ki jih potrebujejo za svoje delo. Samo zelo omejeno število zaposlenih lahko opravlja spremembe varnostnih parametrov v celotnem sistemu.		o Pregled omejevanja dostopa (gesel ali drugih mehanizmov omejevanja dostopa) na nivoju operacijskih sistemov, baz podatkov in programskih rešitev. o Pregled postopkov načrtovanja standardnih uporabniških vlog. o Pregled postopkov dodajanja in odvzemanja uporabniških pravic. o Pregled uporabnikov, definiranih na nivoju operacijskih sistemov, baz podatkov ter njihovih uporabniških pravic.	o
Uporabniki z visokim nivojem	Uporabniška imena z visokim		O Pregled (sistemskega) dnevnika	

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
uporabniških pravic (super-uporabniki, administratorji) namerno ogrozijo varnost podatkov in varnost sistema.	nivojem uporabniških pravic so ustrezno nadzorovana.		in razpoložljivosti sledi v dnevniku. o Pregled dostopnih pravic do sistemskega dnevnika.	
Nepooblaščene osebe pridobijo uporabniško ime z visokim nivojem uporabniških pravic (super-uporabnik, administrator) ter ga zlorabijo za nenadzorovana dejanja v programski rešitvi (možnost prevare)	Dostop do programskih rešitev, podatkov in drugih virov informacij je omejen na tiste uporabnike, ki jih potrebujejo za svoje delo.		o Pregled pred-nastavljenih gesel standardnih uporabniških imen operacijskih sistemov, baz podatkov, programskih rešitev… o Pregled postopkov za ravnanje z močnimi uporabniškimi imeni ter njihovimi gesli.	o
Nepooblaščene osebe lahko prestrežejo in spremenijo podatke, ki potujejo po (javnih ali notranjih) komunikacijskih omrežjih (možnost kraje identitete in prevare).	Občutljivi podatki so med prenosom šifrirani.		o Pregled kodiranja podatkov pri prenosu po javnih in internih komunikacijskih omrežjih.	
Nepooblaščene osebe lahko vdrejo v informacijski sistem organizacije ter spreminjajo podatke (možnost kraje	Informacijski sistemi so pred zunanjimi omrežju zaščiteni z ustreznimi tehnologijami		o Pregled tehnologij za zaščito pred zunanjim prometom ter njihovih nastavitev. o Pregled programske opreme za	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
identitete in prevare)	(požarni zid, DMZ,…). Informacijski sistemi so zaščiteni pred zlonamerno programsko opremo (virusi, črvi ipd).		zaščito pred zlonamerno programsko kodo na strežnikih in delovnih postajah.	

4. Upravljanje sprememb informacijskega sistema

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
Nova programska rešitev ali nadgradnja programske rešitve ne deluje oz. deluje neustrezno.	Nove programske rešitve oz. nadgradnje programskih rešitev delujejo ustrezno.		o Pregled internih postopkov za izbiro in vodenje IT projektov. o Pregled najpomembnejših sprememb oz. nadgradenj programskih rešitev. o Pregled standardnih postopkov sprememb in nadgradenj programskih	o

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja	Revizorjevi postopki za pridobitev zagotovila o ustreznosti kontrolnega okolja	Ugotovitve
			rešitev. o Potrditev ločenosti razvojnega, testnega in produkcijskega okolja.	
Pri prehodu na novo programsko rešitev ali novo verzijo baze podatkov pride do izgube podatkov oz. ti niso ustrezno preneseni v novo programsko rešitev.	Prehod na novo programsko rešitev oz. novo bazo podatkov je ustrezno načrtovan, migracija podatkov pa celovita.		o Pregled dokumentacije o migraciji baze podatkov. o Uskladitev zaključnega stanja postavk pred migracijo in otvoritvenega stanja po migraciji	o