| | |
|---|---|
| Dokument: | **PRIMER Ocena tveganj po COBIT[1] osnutek** |
| Ime revidiranca: | |
| Ime revizije: | Revizija delovanja informacijskih sistemov po okviru COBIT 4.1[2] |
| Namen dokumenta: | Dokumentirati oceno tveganja, na podlagi opravljenih inicialnih postopkov spoznavanja organizacije[3]. |
| Povzetek točk: | **1. Tveganja pri delovanju in kontroliranju informacijskih sistemov - COBIT 2**<br><br>Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno NAČRTUJTE IN ORGANIZIRAJTE (PO) 3<br>Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno NABAVITE IN VPELJITE (AI) 7<br>Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno IZVAJAJTE IN PODPIRAJTE (DS) 11<br>Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno SPREMLJAJTE IN VREDNOTITE (ME) 16<br>**2. Tveganja pri odkrivanju oz. revizijskem poslu - COBIT 17** |
| Avtor: | Maja Hmelak, Uroš Žust |

| Verzija | Datum | Oseba | Opis |
|---|---|---|---|
| 1.0 | 16.9.2013 | MH, UŽ | Prva pripravljena verzija |

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

[2] 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.

[3] 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

| | | | |
|---|---|---|---|
| 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 |
| | | | |

Usmeritve na področju ocenjevanja tveganj podajajo **Standardi za revidiranje informacijskih sistemov in dajanje zagotovil**[4], ki jih podrobno predstavljava v dokumentih **105002_VODNIK_Ocenjevanje_Tveganj_V_Reviziji_IS_V1.1 ter 1001_VODNIK_Nacrtovanje_Revizijskega_Posla_V1.1**. V nadaljevanju predstavljamo konkretna tveganja pri delovanju in kontroliranju informacijskih sistemov ter tveganja pri odkrivanju na primeru revizije delovanja informacijskih sistemov po COBIT 4.1.

# 1. Tveganja pri delovanju in kontroliranju informacijskih sistemov - COBIT

Ocenjevanje tveganja pri delovanju in kontroliranju mora **vselej** temeljiti na dejanski situaciji revidirane organizacije in revidiranega področja. COBIT in sorodni okviri sicer predstavljajo »sezname« dobrih praks, a le te ne odgovarjajo nujno na tveganja konkretne organizacije.

Narava in obseg tveganj učinkovitosti delovanja ter kontrol posameznega informacijskega sistema sta odvisna od vrste različnih dejavnikov, med drugim od:

- Obdobja, ko so bile uvedene posamezne programske rešitve in tehnološka infrastruktura; v Sloveniji so se nekatere organizacije informatizirale zelo zgodaj – že v zgodnjih 80-tih letih. Številne rešitve, uvedene v prvem obdobju informatizacije še vedno delujejo, pri čemer so bile pogosto nadgrajene in dopolnjevane. Take rešitve marsikdaj ne ustrezajo sodobnim standardom delovanja, tako s stališča varnosti kot tudi z vidika avtomatiziranosti kontrol;
- Velikosti organizacije; manjše organizacije so izpostavljene zlasti tveganjem neprimernega ločevanja vlog, ker njihova organiziranost ne omogoča konsistentne ureditve tega področja. Večje organizacije so

[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.**

izpostavljene tveganjem nejasne sledi dela posameznih uporabnikov informacijskih sistemov;

- Zaveze poslovodstva k vzpostavitvi ustreznega kontrolnega okolja;
- Zrelosti okolja IT v revidirani organizaciji; pogosto imajo bolj zrela okolja tudi več kontrol, bolje uvedene kontrolne mehanizme ter manj tveganj pri delovanju;
- Sprememb, ki jim je bilo v zadnjem obdobju izpostavljeno okolje informacijskega sistema; bolj dinamična okolja so navadno povezana z večjimi tveganji.

Vsaka COBIT domena in posledično vsak COBIT proces je povezan s svojim naborom tveganj učinkovitosti delovanja. V nadaljevanju predstavljava nekatere primere, ki so v povezavi s posameznim procesom COBIT v slovenskem okolju relativno pogosti[5].

## *Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno NAČRTUJTE IN ORGANIZIRAJTE (PO)*

| COBIT proces | Tveganja procesa |
|---|---|
| **PO1 Opredelite strateški načrt za IT** | Brez ustrezno opredeljenega strateškega načrta za IT organizacije tvegajo, da:<br>• v srednjem in dolgem roku ne bodo imele ustrezno podprtih poslovnih procesov, ker ne bodo upoštevale tehnoloških trendov in zahtev poslovanja,<br>• tehnološka infrastruktura v srednjem roku ne bo podpirala poslovnih programskih rešitev,<br>• bodo neustrezno načrtovale sredstva, namenjena IT,<br>• investicije v IT ne bodo izvedene na osnovi poslovnih potreb,<br>• ne bo mogoče na merljiv način spremljati rezultatov investicij v IT,<br>• bo ob večjih spremembah v poslovnem okolju organizacije potrebno zelo hitro in brez ustreznih načrtov razvijati nove programske rešitve ali širiti tehnološko infrastrukturo, kar |

[5] Seznam ni popoln – dejanska tveganja so vselej stvar razumevanja področja revizije.

| COBIT proces | Tveganja procesa |
|---|---|
| | je lahko povezano s stroški, zamudami napakami, …<br>• bo organizacija zaradi tehnoloških odločitev priklenjena na določenega dobavitelja ali tehnologijo[6],<br>• … |
| **PO2 Opredelite informacijsko arhitekturo** | Brez ustrezno opredeljene informacijske arhitekture organizacije tvegajo, da:<br>• ne bodo mogle učinkovito uporabljati svojih podatkov in drugih informacijskih virov,<br>• podatki in drugi informacijski vidi ne bodo celoviti,<br>• bodo zaostale pri tehnološkem razvoju,<br>• bo organizacija zaradi tehnoloških odločitev priklenjena na določenega dobavitelja ali tehnologijo<br>• … |
| **PO3 Določite tehnološko usmeritev** | Brez določene tehnološke usmeritve organizacije tvegajo, da:<br>• bodo vlagale v medsebojno različne gradnike informacijske arhitekture, kar bo potencialno pomenilo, da bodo imele večje stroške z licencami, vzdrževanjem, uporabo strokovnjakov, ki bodo potrebni za administracijo ipd.,<br>• posamezni gradniki IT med seboj ne bodo združljivi ali povezljivi,<br>• bodo zaostale pri tehnološkem razvoju,<br>• ne bodo pravočasno uvedle različnih zakonsko zahtevanih rešitev,<br>• ne bodo usklajene s področnimi tehničnimi standardi,<br>• bo organizacija zaradi tehnoloških odločitev |

[6] Angl. Vendor Lock-in.

| COBIT proces | Tveganja procesa |
|---|---|
| | priklenjena na določenega dobavitelja ali tehnologijo<br>• … |
| **PO4 Opredelite procese, organizacijo in razmerja IT** | Organizacije, ki nimajo opredeljenih procesov, organizacije in razmerij IT tvegajo, da:<br>• IT funkcija ne bo ustrezno umeščena v organizacijo,<br>• odgovornosti posameznih deležnikov v organizaciji v okviru IT procesov ne bodo jasne,<br>• zaveza poslovodstva za podporo delovanju in ustrezni kontroli IT ne bo jasno razvidna,<br>• korporativno upravljanje IT[7] ter celovit nadzor (na najvišjem nivoju) nad IT ne bosta opredeljena,<br>• bodo zaostale pri tehnološkem razvoju,<br>• odgovornost za zagotavljanje kakovosti IT ne bo jasno dodeljena,<br>• pomembni elementi ločevanja vlog (v različnih procesih ter na različnih nivojih) ne bodo uvedeni,<br>• … |
| **PO5 Upravljajte investicije v IT** | Brez ustreznega upravljanja investicij IT organizacije tvegajo, da:<br>• bodo za IT investicije porabile več, kot je potrebno,<br>• da IT investicije ne bodo prinesle pričakovanih koristi,<br>• da bo nadzor nad IT investicijami, zlasti nad z njimi povezanimi stroški neustrezen in necelovit,<br>• … |
| **PO6 Sporočajte** | Brez primernega procesa sporočanja ciljev in |

[7] Angl. IT governance.

| COBIT proces | Tveganja procesa |
|---|---|
| **cilje in usmeritev vodstva** | usmeritev poslovodstva organizacije tvegajo, da:<br>• zaposleni ne bodo imeli jasne predstave o ustreznem in neustreznem ravnanju v povezavi z viri IT, kar lahko vodi v različne škandale, prevare ipd.<br>• se politike in postopki, ki jih zahteva poslovodstvo ne bodo dosledno uvedli in upoštevali v vsakodnevnem ravnanju,<br>• zaposleni ne bodo poznali primernih postopkov ukrepanja v primerih, ko opazijo kršitve varnosti,<br>• … |
| **PO7 Upravljajte človeške vire v sektorju IT** | Brez definiranega procesa upravljanja IT virov v sektorju IT organizacije tvegajo, da:<br>• ne bodo imele ustreznih kadrov, ko jih bodo potrebovale,<br>• bodo preveč odvisne od majhnega števila ključnih zaposlenih ali celo zunanjih sodelavcev,<br>• bodo zaposlile kandidate, ki iz različnih razlogov ne bi smeli imeti dostopa do zaupnih podatkov organizacij,<br>• … |
| **PO8 Upravljajte kakovost** | Brez definiranega procesa upravljanja kakovosti organizacije tvegajo, da:<br>• standardi kakovosti ne bodo dosledno upoštevani v organizacijskih procesih,<br>• procesi stalnega izboljševanja ne bodo ustrezno delovali,<br>• bodo na področju IT doživljale večja nihanja v kakovosti storitve,<br>• da bosta kakovost IT storitev ter s tem njena cena bistveno višji, kot ju organizacija potrebuje,<br>• … |

| COBIT proces | Tveganja procesa |
|---|---|
| **PO9 Ocenjujte in obvladujte tveganja IT** | Brez procesa ocenjevanja in obvladovanja tveganj IT organizacije tvegajo, da:<br>• ne bodo zaznale pomembnih tveganj in uvedle ukrepov za njihovo zmanjševanje,<br>• da ob uresničitvi groženj učinkovitemu delovanju IT ne bodo imele pripravljenega primernega odziva,<br>• ne bodo skladne z deli področne zakonodaje (npr. v bančništvu, zavarovalništvu, …),<br>• …. |
| **PO10 Upravljajte projekte** | Brez procesov upravljanja IT projektov organizacije tvegajo, da IT projekti oz. projekti z IT komponento ne bodo primerno potekali z vidika:<br>• rokov izvedbe,<br>• projektnih stroškov,<br>• projektnih rezultatov,<br>• opredelitve obsega in sprememb obsega,<br>• … |

## *Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno NABAVITE IN VPELJITE (AI)*

| COBIT proces | Tveganja procesa |
|---|---|
| **AI1 Določite avtomatizirane rešitve** | Brez procesa določitve avtomatiziranih rešitev organizacije tvegajo, da:<br>• ne bodo imele programskih rešitev, ki jih potrebujejo za podporo svojim organizacijskim procesom ali da jih ne bodo imele takrat, ko jih potrebujejo,<br>• bodo sprejele odločitve za tehnološke rešitve, ki v praksi ne bodo izvedljive,<br>• pred odločitvijo za določeno tehnološko rešitev ne bodo ustrezno presodile drugih, |

| COBIT proces | Tveganja procesa |
|---|---|
| | potencialno primernejših možnosti,<br>• … |
| **AI2 Nabavite in vzdržujte aplikacijske programe** | Brez primernih procesov nabave in vzdrževanja programskih rešitev organizacije tvegajo:<br>• uvedbo neprimerno načrtovanih in zasnovanih programskih rešitev,<br>• uvedbo programskih rešitev, ki ne ustrezajo sodobnim ali interno-organizacijskim kriterijem varnosti,<br>• uvedbo predragih programskih rešitev ali uvedbo programskih rešitev s predragim vzdrževanjem,<br>• neustrezno konfiguracijo uvedenih programskih rešitev (npr. na nivoju uporabniških vlog ali varnosti),<br>• uvedbo programskih rešitev, ki jih kasneje ni mogoče ustrezno nadgrajevati,<br>• uvedbo programskih rešitev, ki ne ustrezajo sodobnim ali interno-organizacijskim kriterijem kakovosti,<br>• … |
| **AI3 Nabavite in vzdržujte tehnološko infrastrukturo** | Brez primernih procesov nabave in vzdrževanja tehnološke infrastrukture organizacije tvegajo, da:<br>• bo tehnološka infrastruktura predstavljala ozko grlo pri delovanju programskih rešitev organizacije,<br>• bo tehnološka infrastruktura neprimerno velika glede na zahteve po obdelavah,<br>• tehnološka infrastruktura ne bo redno in ustrezno vzdrževana,<br>• bo organizacija zaradi tehnoloških odločitev priklenjena na določenega dobavitelja ali tehnologijo |

| COBIT proces | Tveganja procesa |
|---|---|
| | • … |
| **AI4 Omogočite delovanje in uporabo** | Brez procesov, ki omogočijo delovanje in uporabo programskih rešitev organizacije tvegajo, da:<br>• na uporabnike in na administratorje programskih in infrastrukturnih rešitev ne bodo prenesle znanja, ki bi ga ti potrebovali za podporo svojemu delu.<br>• bo organizacija zaradi neustreznega prenosa znanja priklenjena na določenega dobavitelja ali tehnologijo<br>• … |
| **AI5 Zagotovite vire IT** | Brez procesov za zagotovitev IT virov organizacije tvegajo, da:<br>• plačane tehnološke rešitve ne bodo enake dobavljenim,<br>• bo pri izbiri dobaviteljev IT rešitev prihajalo do nepravilnosti ali nezakonitosti, zlasti v okoljih, ki imajo posebne zakonske zahteve glede nabavnih postopkov,<br>• pogodbe z IT dobavitelji ne bodo ustrezno pripravljene oz. ne bodo pripravljene tako, da optimalno ščitijo interese organizacije,<br>• se ne bo primerno spremljalo uresničevanje pogodb z IT dobavitelji,<br>• … |
| **AI6 Upravljajte spremembe** | Brez procesov upravljanja sprememb organizacije tvegajo, da:<br>• se zahtevajo neodobrene spremembe,<br>• se preobremeni razvojna ekipa in drugo tehnično osebje,<br>• se zahtevajo parcialne spremembe brez celovite slike o tem, kaj določen proces dejansko potrebuje,<br>• se zahtevajo nasprotujoče si spremembe |

| COBIT proces | Tveganja procesa |
|---|---|
| | tehničnih rešitev,<br>• se zahtevajo spremembe, ki bodo imele nepredviden vpliv na delovanje programske rešitve,<br>• se razvijejo popravki programskih rešitev, ki ne ustrezajo kakovostnim standardom organizacije,<br>• se izgubi sledljivost o izvoru zahtevkov za spremembe,<br>• spremembe tehničnih rešitev zahtevajo zaposleni, ki za to nimajo pooblastil,<br>• pride do razvoja in uvedbe tehničnih rešitev z nedovoljenimi rutinami,<br>• nujne spremembe preidejo v razvoj in produkcijsko okolje mimo predpisanih postopkov,<br>• …. |
| **AI7 Namestite in potrdite rešitve in spremembe** | Brez procesov nameščanja in potrjevanja sprememb organizacije tvegajo, da:<br>• se uvedejo neodobrene spremembe v produkcijsko okolje,<br>• se uvedejo spremembe, ki bodo imele nepredviden vpliv na delovanje tehničnih rešitev,<br>• se uvedejo popravki tehničnih rešitev, ki niso ustrezno preizkušeni v testnem okolju ali pa niso preizkušeni v tehničnem okolju, ki bi ustrezalo produkciji,<br>• se uvedejo popravki tehničnih rešitev, ki ne ustrezajo kakovostnim standardom organizacije,<br>• uvedbo sprememb tehničnih rešitev odobrijo zaposleni, ki za to nimajo pooblastil,<br>• pride do uvedbe programskih rešitev z nedovoljenimi rutinami, |

| COBIT proces | Tveganja procesa |
|---|---|
| | • nujne spremembe preidejo v razvoj in produkcijsko okolje mimo predpisanih postopkov,<br>• …. |

## *Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno IZVAJAJTE IN PODPIRAJTE (DS)*

| COBIT proces | Tveganja procesa |
|---|---|
| **DS1 Opredelite in upravljajte ravni storitve** | Brez procesov za opredelitev in upravljanje ravni storitev organizacije tvegajo, da:<br>• ne bo jasno, kak nivo IT storitev lahko uporabniki pričakujejo ter ali je kakovost storitev dejansko primerna glede na njeno ceno,<br>• nivo IT storitev ne bo primeren,<br>• bo organizacija sicer opredelila pričakovani nivo IT storitev, ne bo pa uvedla procesa, s katerim bi lahko sistematično spremljala, ali se tak nivo dejansko dosega,<br>• … |
| **DS2 Upravljajte storitve tretje stranke** | Brez procesov upravljanja storitev tretje stranke organizacije tvegajo, da:<br>• tretja stranka ne bo zagotavljala ustreznega nivoja storitev,<br>• bo pri tretji stranki prišlo do kršitev dobrih poslovnih praks ali celo zakonodaje, zaradi katerih bo organizacija sama odgovarjala za kršitev, saj je prav organizacija odgovorna za svoje kontrolno okolje (npr. za kontrole nad varovanjem osebnih podatkov) in te odgovornosti ne more prenesti na tretje stranke,<br>• bo nivo zagotavljanja storitev neustrezen ali da bo pogosto nihal, |

| | |
|---|---|
| | • organizacija ne bo mogla presoditi, ali je nivo zagotavljanja storitev tretje stranke ustrezen,<br>• bo organizacija plačevala za storitve, ki jih ni naročila ali ki niso bile izvedene,<br>• bo organizacija kritično navezana na enega dobavitelja, katerega bo težko zamenjala ter da bo zaradi tega preplačevala njegove storitve,<br>• bo pri sodelovanju z dobaviteljem prišlo do podkupovanja odgovornih zaposlenih,<br>• … |
| **DS3 Upravljajte delovanje in zmogljivost** | Brez procesov upravljanja delovanja in zmogljivosti organizacije tvegajo, da:<br>• bo tehnološka infrastruktura predstavljala ozko grlo pri delovanju programskih rešitev organizacije,<br>• bo tehnološka infrastruktura neprimerno velika glede na zahteve po obdelavah,<br>• tehnološka infrastruktura ne bo redno in ustrezno vzdrževana,<br>• zaradi pomanjkanja možnosti meritev ne bo mogoče ugotoviti, kje nastajajo težave pri zagotavljanju delovanja,<br>• … |
| **DS4 Zagotovite neprekinjenost storitev** | Brez procesov za zagotavljanje neprekinjenosti storitev organizacije tvegajo, da:<br>• ob nesreči ali prekinitvi poslovanja le tega ne bo mogoče ponovno v vzpostaviti ali da tega ne bo mogoče narediti v ustreznem času,<br>• se bodo izgubili podatki o poslovanju,<br>• bo ponovna vzpostavitev tehnoloških rešitev po prekinitvi delovanja sicer uspešna, ne bo pa mogoče v ustreznem času vzpostaviti organizacijskega dela poslovanja,<br>• bo v zagotavljanje neprekinjenosti delovanja vloženih neprimerno veliko sredstev, glede |

| | |
|---|---|
| | na potencialna iz prekinitve izhajajoča tveganja,<br>• bodo načrti neprekinjenega poslovanja in okrevanja po katastrofi, ki praviloma vsebujejo zelo podrobne podatke o delovanju tehnološke infrastrukture ter delovanju organizacije kot celote, pristali v napačnih rokah,<br>• … |
| **DS5 Zagotovite varnost sistemov** | Brez procesov za zagotavljanje varnosti sistemov organizacije tvegajo, da:<br>• bodo do IT virov dostopali uporabniki brez ustreznih pooblastil,<br>• bo prišlo do kršitve načel ločevanja vlog na nivoju programskih rešitev in drugih tehničnih rešitev,<br>• bo prišlo do razkritja zaupnih podatkov in drugih varnostnih incidentov,<br>• bo prišlo do ogrožanja stabilnosti tehničnih rešitev,<br>• bo prišlo do izgube sledljivosti nad delovanjem uporabnikov v programskih rešitvah,<br>• bo prišlo do ponarejenih transakcij, goljufij in tatvin,<br>• bo prišlo do izgube ugleda organizacije ali druge nematerialne škode,<br>• … |
| **DS6 Ugotovite in porazdelite stroške** | Brez procesov za ugotavljanje in prerazporejanje stroškov organizacija tvega, da:<br>• ne bo imela ustreznega pregleda nad stroški IT<br>• ne bo imela ustreznega pregleda nad koristmi IT ter nad rabo IT virov na različnih mestih v organizaciji.<br>• … |
| **DS7 Izobrazite in usposobite** | Brez procesov usposabljanja in izobraževanja uporabnikov organizacije tvegajo, da: |

| | |
|---|---|
| **uporabnike** | • uporabniki ne bodo ustrezno ali celovito uporabljali IT virov v organizaciji,<br>• uporabniki ne bodo spoštovali načel varnosti in zaupnosti podatkov,<br>• zaposleni ne bodo imeli jasne predstave o ustreznem in neustreznem ravnanju v povezavi z viri IT, kar lahko vodi v različne škandale, prevare ipd.<br>• … |
| **DS8 Upravljajte službo za pomoč uporabnikom in obvladujte incidente** | Brez procesov upravljanja službe za pomoč uporabnikom in obvladovanja incidentov organizacije tvegajo, da:<br>• uporabniki ne bodo ustrezno ali celovito uporabljali IT virov v organizaciji,<br>• težave uporabnikov pri delu ne bodo zaznane in ustrezno rešene,<br>• ne bo mogoče zaznati širših trendov in potencialnih težav uporabnikov, ker se ne spremlja statistika njihovih poizvedb,<br>• zaznani incidenti ne bodo ustrezno obravnavani in razrešeni<br>• … |
| **DS9 Upravljajte konfiguracijo** | Brez procesov upravljanja konfiguracij organizacije tvegajo, da:<br>• bodo izvedene nepreizkušene in neodobrene spremembe konfiguracij, ki bodo ogrožale varnost ali stabilnost tehničnih rešitev,<br>• ne bo mogoče slediti izvoru sprememb določenih konfiguracij,<br>• … |
| **DS10 Upravljajte probleme** | Brez procesov upravljanja problemov organizacije tvegajo, da:<br>• ne bo mogoče zaznati širših trendov in potencialnih težav uporabnikov, ker se ne spremlja statistika njihovih poizvedb,<br>• problemi ne bodo pravočasno rešeni, |

| | |
|---|---|
| | • … |
| **DS11 Upravljajte podatke** | Brez procesov upravljanja podatkov organizacije tvegajo, da:<br>• podatkov ne bodo varovale in hranile skladno z zakonodajnimi zahtevami,<br>• podatkov ne bodo hranile z dovolj veliko frekvenco glede na zahteve poslovnih procesov,<br>• ne bodo hranile pravih podatkov,<br>• mediji, na katerih se bodo hranili podatki, ne bodo dejansko omogočali njihovega ponovnega priklica,<br>• bo incident uničil tako podatke na medijih tehničnih rešitev, kot tudi vse rezervne kopije (če so npr. te hranjene na isti lokaciji),<br>• bo prišlo do kraje podatkov iz varnostnih kopij podatkov (ker so te pogosto slabše varovane in lažje prenosljive kot originali),<br>• podatki, ki jih organizacija ne potrebuje več ali kjer nima več zakonske osnove za njihovo hrambo, ne bodo pravočasno in primerno uničeni,<br>• … |
| **DS12 Upravljajte fizično okolje** | Brez procesov upravljanja fizičnega okolja organizacije tvegajo, da:<br>• bo prišlo do varnostnih incidentov, kraje podatkov (na prenosnih medijih) ali do uničenja informacijskih virov organizacije,<br>• bo prišlo do izgube informacijskih virov zaradi okoljskih dejavnikov,<br>• … |
| **DS13 Upravljajte delovanje** | Brez procesov upravljanja delovanja organizacije tvegajo, da:<br>• bo zaradi pomanjkljivih navodil prišlo do težav pri delovanju,<br>• težave pri delovanju (npr. nihanje |

| | |
|---|---|
| | zmogljivosti) ne bodo pravočasno opažene in da se ne bo pravočasno ukrepalo,<br>• bo prišlo do istočasnega prevzema velikega števila obdelav in s tem do zastojev pri delovanju,<br>• strojna oprema ne bo ustrezno preventivno vzdrževana,<br>• strojna oprema v primeru okvare ne bo v primernem času nadomeščena,<br>• …. |

## *Tveganja učinkovitosti delovanja in kontroliranja, povezana z domeno SPREMLJAJTE IN VREDNOTITE (ME)*

| COBIT proces | Tveganja procesa |
|---|---|
| **ME1 Spremljajte in vrednotite delovanje IT** | Brez primernih procesov spremljanja in vrednotenja delovanja IT organizacije tvegajo, da:<br>• ne bodo mogle oceniti delovanja IT funkcije,<br>• ne bodo mogle izvesti morebitnih popravnih ukrepov za pomanjkljivosti pri delovanju IT,<br>• … |
| **ME2 Spremljajte in vrednotite notranje kontrole** | Brez primernih procesov spremljanja in vrednotenja notranjih kontrol organizacije tvegajo, da:<br>• ne bodo pravočasno zaznale slabosti v zasnovi ali delovanju notranjih kontrol, kar lahko vodi v različne škandale, prevare ipd.<br>• ne bodo zaznale priložnosti za izboljšanje učinkovitosti notranjekontrolnega okolja,<br>• ne bodo imele ustreznega nadzora nad tistimi notranjimi kontrolami, za katere so sicer odgovorne same (npr. zaupnost podatkov strank), vendar pa se deloma izvajajo pri tretjih strankah,<br>• … |

| | |
|---|---|
| **ME3 Zagotovite skladnost z zunanjimi zahtevami** | Brez primernih procesov za zagotavljanje skladnosti z zunanjimi zahtevami IT organizacije tvegajo, da:<br>• ne bodo skladne z zakonodajnimi zahtevami, zahtevami strokovnih standardov ali drugimi predpisanimi okviri kar lahko vodi v različne škandale, finančne in drugačne kazni ipd..<br>• … |
| **ME4 Zagotovite upravljanje IT** | Brez primernih procesov za upravljanje IT organizacije tvegajo, da:<br>• IT funkcija kot celota organizaciji ne bo zagotavljala ustrezne dodane vrednosti,<br>• strategija IT funkcije ne bo usklajena s strategijo organizacije,<br>• bo organizacija kot celota pretirano odvisna od majhne skupine zaposlenih,<br>• bo organizacija sprejela odločitve o tehnoloških rešitvah, ki bodo imele dolgoročen vpliv na delovanje organizacije, hkrati pa jih ne bo obravnavala z vidika organizacije kot celote, temveč le kot IT odločitve,<br>• bo organizacija zaradi tehnoloških odločitev priklenjena na določenega dobavitelja ali tehnologijo,<br>• organizacija kot celota ne bo ustrezno upoštevala vpliva tveganj IT,<br>• organizacija ne bo imela ustreznega nadzora nad stroški IT,<br>• … |

# 2. Tveganja pri odkrivanju oz. revizijskem poslu - COBIT

Standardi in smernice ISACA natančno ne opredeljujejo načinov, kako lahko pride do tega, da revizor IS s postopki preizkušanja podatkov ne bo odkril napake, ki bi bila posamično ali v povezavi z drugimi napakami lahko pomembna. Zelo dobro opredelitev revizorjeve napake oz. tveganja pri

odkrivanju podajajo Mednarodni standardi revidiranja in mednarodna stališča o revidiranju, ki jih izdaja Mednarodna zveza računovodskih strokovnjakov, v slovenskem jeziku pa objavlja Slovenski inštitut za revizijo[8]. ***Standard MSR 530 - Revizijsko vzorčenje*** in drugi izbirni postopki revizijskega preizkušanja na naslednji način definira tveganja povezana z revizorjevim delom:

Tveganje pri vzorčenju – tveganje, da bi se revizorjev sklep na podlagi vzorca lahko razlikoval od sklepa, ki bi ga oblikoval, če bi bila celotna populacija obravnavana po istem revizijskem postopku. Tveganje pri vzorčenju lahko pripelje do dveh vrst napačnih sklepov:

i. pri preizkušanju kontrol do sklepa, da so kontrole uspešnejše, kot so v resnici, ali pri preizkušanju podrobnosti do sklepa, da ni pomembno napačne navedbe, čeprav ta v resnici obstaja (revizor se ukvarja predvsem s to vrsto napačnih sklepov, ker vpliva na uspešnost revizije in povečuje verjetnost za neustrezno revizijsko mnenje);
ii. pri preizkušanju kontrol do sklepa, da so kontrole manj uspešne, kot so v resnici, ali pri preizkušanju podrobnosti do sklepa, da obstaja pomembno napačna navedba, čeprav je v resnici ni (ta vrsta napačnih sklepov vpliva na učinkovitost revizije, ker se običajno šele z dodatnim delom lahko ugotovi, da so bili prvotni sklepi nepravilni).

Tveganje zunaj vzorčenja – tveganje, da bo revizor prišel do zmotne ugotovitve zaradi česarkoli, kar ni povezano s tveganjem pri vzorčenju, torej zaradi napake, ki je drugačen ali večji vzorec ne bi odpravil

[8] Razen ko revizor IS sodeluje kot veščak pri reviziji računovodskih izkazov**, ni zavezan k spoštovanju Mednarodnih standardov revidiranja in mednarodnih stališč o revidiranju**. Na tem mestu jih navajamo **zgolj zato**, ker primerno podajajo definicije napak pri revidiranju računovodskih izkazov, ki pa so primerljive z napakami revizorja IS pri odkrivanju.