Dokument:	**VODNIK Ocenjevanje tveganj v reviziji IS osnutek**
Namen dokumenta:	Predstaviti različna tveganja v organizacijah ter podati napotke za zmanjševanje revizijskega tveganja pri revizijskem poslu.
Povzetek točk:	**1. Standardi za revidiranje informacijskih sistemov in dajanje zagotovil (splošne usmeritve) 1** **2. Tveganja pri delovanju in tveganja pri kontroliranju v organizacijah 5** **3. Tveganje pri izvajanju revizijske naloge 8** *Tveganja in revizijski program 9*
Avtor:	Maja Hmelak, Uroš Žust

Verzija	Datum	Oseba	Opis
1.0	16.9.2013	MH, UŽ	Prva pripravljena verzija
1.1	20.10.2013	MH, UŽ	Uskladitev dokumentov na nivoju celotne mape
1.2	4.11.2013	MH, UŽ	Izboljšanje skladno s prvimi povratnimi komentarji

1. Standardi za revidiranje informacijskih sistemov in dajanje zagotovil (splošne usmeritve)

V tem poglavju naštevamo tiste **standarde za revidiranje IS in dajanje zagotovil**[1], ki podajajo splošne usmeritve na področju ocenjevanja tveganja. Dele standardov in smernic, ki jih lahko neposredno prevedemo v konkretne zahteve, navajamo tudi v nadaljevanju pod posameznimi poglavji.
Standard 1202 Ocena tveganja in načrtovanje *zahteva:*

[1] 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.**

1202.1 Funkcija revizije IS in dajanja zagotovil mora s primernim pristopom k oceni tveganj in podporno metodologijo razviti celovit revizijski načrt ter ugotoviti prioritete za učinkovito razporejanje revizijskih virov.

1202.2 Strokovnjak za revizijo IS in dajanje zagotovil bo pri načrtovanju posameznih poslov opredelil in ocenil tveganja področja, ki ga pregleduje.

1202.3 Strokovnjak za revizijo IS in dajanje zagotovil mora upoštevati tveganja, povezana s pregledovanim področjem, revizijsko tveganje in z njima povezano izpostavljenost organizacije.

Smernica 2201 Načrtovanje posla (G15) [2] *navaja:*

3.4.1 Strokovnjaki za revizijo IS in dajanje zagotovil naj za revizijo izdelajo revizijski načrt, da zmanjšajo revizijsko tveganje na sprejemljivo raven.

3.4.2 Izvede naj se ocenjevanje tveganj, da se pridobi sprejemljivo zagotovilo, da bodo pomembne teme med revizijo ustrezno pokrite. S tem ocenjevanjem naj se ugotovijo področja, na katerih so pomembne težave zelo verjetne.

3.4.3 Ocena tveganj in razvrstitev prepoznanih tveganj glede na pomembnost za področje, ki se pregleduje, in za okolje IT v podjetju naj bosta izvedeni v potrebnem obsegu.

Smernica 2202 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju (G13) *opredeljuje med drugim:*

2.1.1 Na voljo je veliko metodologij za ocenjevanje tveganja, med katerimi revizor IS lahko izbira. Njihov razpon zajema vse od preprostih razvrstitev na visoko, srednje in nizko tveganje na podlagi presoje revizorja IS pa vse do zapletenih in očitno znanstvenih izračunov, ki dajo številčno oceno tveganja. Revizorji IS naj upoštevajo raven zapletenosti in podrobne razčlenitve, ki je ustrezna za organizacijo, ki jo revidirajo.

2.1.5 Od nobene posamezne metodologije za ocenjevanje tveganja ni mogoče pričakovati, da bo ustrezna v vseh okoliščinah. Razmere, ki vplivajo na revizije, se sčasoma lahko spremenijo. Zato bi moral revizor IS občasno ponovno oceniti ustreznost izbranih metodologij za ocenjevanje tveganja.

2.2.1 Revizorji IS bi morali pri pripravi celovitega revizijskega načrta in pri načrtovanju posebnih revizij uporabiti izbrane tehnike ocenjevanja tveganja.

[2] V tem dokumentu uporabljamo uradni prevod Mednarodnih smernic za strokovnjake revidiranja, kontrol in dajanja zagotovil na področju IT , ki ga objavlja Slovenski inštitut za revizijo na svoji spletni strani http://www.si-revizija.si/revizorji_is/dokumenti/smernice_revidiranja.pdf

Ocenjevanje tveganja v povezavi z drugimi revizijskimi tehnikami je treba upoštevati pri načrtovanih odločitvah, kot so:

- *vrsta, obseg in čas revizijskih postopkov,*
- *področja ali poslovne funkcije, ki jih je treba revidirati,*
- *količina časa in virov, ki jih je treba nameniti za revizijo.*

2.2.2 Revizor IS mora upoštevati vsako od naslednjih vrst tveganja, da določi njihovo celotno raven:

- *tveganje pri delovanju,*
- *tveganje pri kontroliranju,*
- *tveganje pri odkrivanj.*

2.3.1 ***Tveganje pri delovanju*** *je dovzetnost revizijskega področja za napako na način, ki utegne biti posamično ali v povezavi z drugimi napakami pomemben ob predpostavki, da ni bilo nobenih ustreznih notranjih kontrol. Tveganje pri delovanju, povezano z varnostjo operacijskega sistema, je običajno visoko, ker bi spremembe podatkov ali programov ali celo njihovo razkritje zaradi slabosti pri varnosti operacijskega sistema lahko povzročilo napačne poslovodne informacije ali slabšo konkurenčno prednost. Nasprotno pa je tveganje pri delovanju, povezano z varnostjo za nepovezan osebni računalnik, običajno majhno, če se z ustrezno analizo dokaže, da se ne uporablja za poslovno-kritične namene.*

2.3.2 ***Običajno je tveganje pri delovanju za večino revizijskih področij IS visoko****, ker morebitni učinki napak običajno segajo na več poslovnih sistemov in mnogo uporabnikov.*

2.3.3 Pri ocenjevanju tveganja pri delovanju mora revizor IS upoštevati tako vseobsegajoče kot tudi podrobne kontrole IS. To pa seveda ne velja, kadar se zadolžitev revizorja IS nanaša samo na vseobsegajoče kontrole IS.

2.3.4 Na ravni vseobsegajočih kontrol IS mora revizor IS glede na raven, ki je ustrezna za revizijsko področje, upoštevati:

- *neoporečnost vodstva IS ter izkušnje in znanje vodstva IS,*
- *spremembe v upravljanju IS,*
- *pritiske na vodstvo IS, ki jih lahko navede na skrivanje ali napačno navajanje informacij (na primer velike poslovno-kritične prekoračitve na projektih, hekerska dejavnost),*
- *naravo poslovanja in sistemov organizacije (na primer načrti za e-poslovanje, zapletenost sistemov, pomanjkanje celovitih sistemov),*

- *dejavnike, ki vplivajo na panogo organizacije kot celoto (na primer spremembe v tehnologiji, razpoložljivost osebja IS),*
- *stopnjo vpliva tretje stranke na nadzor sistemov, ki se revidirajo (na primer zaradi povezanosti dobavne verige, zunanjega izvajanja postopkov IS, skupnih poslovnih projektov in neposrednega dostopa strank),*
- *izsledke in čas prejšnjih revizij.*

2.3.5 Na ravni podrobnih IS kontrol mora revizor IS glede na raven, ki je ustrezna za revizijsko področje, upoštevati:

- *izsledke in čas prejšnjih revizij na tem področju,*
- *zapletenost sistemov na tem področju,*
- *stopnjo potrebnih ročnih posegov,*
- *dovzetnost za izgubo ali nezakonito prisvojitev sredstev, ki jih sistem nadzoruje (na primer zaloge, plače),*
- *verjetnost konic dejavnosti ob določenem času v revizijskem obdobju,*
- *dejavnosti zunaj običajnih rednih vsakodnevnih obdelav IS (na primer uporaba pomožnih programov operacijskega sistema za spreminjanje podatkov),*
- *neoporečnost, izkušnje in sposobnosti poslovodstva in osebja, vključenega v uporabo kontrol IS.*

2.4.1 ***Tveganje pri kontroliranju*** *je tveganje, da sistem notranjih kontrol ne bo pravočasno preprečil ali odkril in popravil napake, ki bi se lahko zgodila na revizijskem področju in bi posamično ali v povezavi z drugimi napakami lahko bila pomembna. Tveganje pri kontroliranju, povezano z ročnimi pregledi računalniških dnevnikov, je na primer lahko visoko, ker so zaradi obsega vpisanih informacij dejavnosti, ki jih je treba preiskovati, pogosto lahko spregledane. Tveganje pri kontroliranju računalniško podprtih postopkov za preverjanje računalniško vodenih podatkov je običajno majhno, ker se ti postopki dosledno uporabljajo.*

2.4.2 Revizor IS naj oceni tveganje pri kontroliranju kot visoko, razen če so ustrezne notranje kontrole:

- *ugotovljene,*
- *ocenjene kot uspešne,*
- *preizkušene in dokazano ustrezno delujejo.*

*2.5.1 **Tveganje pri odkrivanju** je tveganje, da revizor IS s postopki preizkušanja podatkov ne bo odkril napake, ki bi bila posamično ali v povezavi z drugimi napakami lahko pomembna. Tveganje pri odkrivanju, povezano s prepoznavanjem kršitev varnosti v aplikacijskem sistemu, je na primer običajno visoko, ker med revizijo dnevniki za celotno obdobje revizije niso na voljo. Tveganje pri odkrivanju, povezano z ugotavljanjem pomanjkanja načrtov za obnovo po katastrofi, pa je običajno majhno, ker je obstoj takih načrtov lahko preveriti.*

2.5.2 Pri določanju ravni potrebnih postopkov za preizkušanja podatkov morajo revizorji IS upoštevati:

- *ocenjevanje tveganja pri delovanju in*
- *ugotovitve glede tveganja pri kontroliranju po preizkušanju skladnosti.*

2.5.3 Višje kot sta ocenjena tveganje pri delovanju in tveganje pri kontroliranju, več revizijskih dokazov morajo revizorji IS običajno pridobiti iz izvajanja revizijskih postopkov preizkušanja podatkov.

Podrobnejši prikaz uporabe usmeritev ***Smernice G13 Uporaba ocenjevanja tveganja pri revizijskem načrtovanju*** smo podrobneje podali v dokumentu **105004 PRIMER Ocena tveganja COBIT**.

2. Tveganja pri delovanju in tveganja pri kontroliranju v organizacijah

Tveganja v organizacijah uvrščamo med tveganja pri delovanju ter tveganja pri kontroliranju. Obvladovanje tveganj izhaja iz temeljne potrebe **po zaščiti virov organizacije**. Med vire organizacije štejemo njeno stvarno, pa tudi njeno neopredmeteno premoženje.

Grožnje lahko povzročijo nezaželena stanja, ki lahko povzročijo škodo. Povezane so z obstoječim **ranljivostmi** virov, sprožijo pa jih lahko naključja ter namerna ali nenamerna dejanja. Ključne grožnje je zato potrebno opredeliti, prav tako pa je potrebno opredeliti njihovo stopnjo in verjetnost.

Učinek je posledica nezaželenega dogodka in se lahko izrazi kot škoda življenju ali zdravju zaposlenih, uničenje določenega vira organizacije, finančna izguba, izguba tržnega deleža, izguba ugleda ali kakšna druga oblika škode.

Tveganje lahko opredelimo kot funkcijo verjetnosti, da bo določena grožnja izkoristila določeno ranljivost ter tako nezaželeno vplivala na delovanje organizacije (povzročila škodo) ter učinka, ki ga bo ta dogodek imel na vire

organizacije. K grožnjam, ranljivostim in potencialnim učinkom strukturirano pristopamo v okviru faze **analize tveganj**.

Celovito obvladovanje tveganj poleg zgoraj opisanih elementov vsebuje tudi **ukrepe za zmanjševanje izpostavljenosti tveganjem**. To vključuje vzpostavitev ustreznega notranje-kontrolnega okolja oz. vse mehanizme - **kontrolne aktivnosti**, s katerimi se:

- ščiti zaposlene in vire organizacije pred nezaželenimi dogodki,
- zmanjšujejo ranljivosti,
- omejuje učinek nezaželenih dogodkov,
- odkrivajo nezaželeni dogodki,
- pospeši okrevanje oz. ponovna vzpostavitev delovanja po nezaželenem dogodku.

Kontrolne aktivnosti imajo eno ali več naslednjih vlog:

- preprečevanje,
- odvračanje,
- odkrivanje,
- omejevanje učinka,
- okrevanje,
- nadzor in
- osveščanje.

Preostala (inherentna) tveganja so tveganja, ki bodo vselej prisotna tudi po uvedbi aktivnosti za zmanjševanje tveganj.

Za namene razumevanja kontrol programskih rešitev je tveganja smiselno opazovati z vidika različnih vsebinskih skupin. Tveganja so vsebinsko tako različna, da moramo k njim pristopati na zelo specifične načine. S tem preprečimo, da bi pri ocenjevanju tveganj in načrtovanju notranje-kontrolnega okolja na primer tveganje administrativne napake pri izpolnjevanju obrazcev obravnavali enako pomembno kot tveganje izgube ugleda zaradi nelegalnega oziroma protizakonitega delovanja organizacije.

Slika 1: Predlog vsebinske delitve tveganj

Organizacijska tveganja so skupina tveganj, katerih potencialna realizacija lahko predstavlja resno grožnjo ugledu, delovanju ali celo obstoju organizacije. Za spremljanje ter obvladovanje teh tveganj je praviloma zadolženo neposredno poslovodstvo organizacije. Notranje-kontrolne aktivnosti za omejevanje organizacijskih tveganj so redko tehnološke narave oz. avtomatizirane, z izjemo kontrol, povezanih z varovanjem podatkov ter na splošno z varovanjem pred zunanjimi vdori v informacijske sisteme organizacije.

Tveganja poslovnih procesov opredeljujemo kot tveganja, katerih uresničitev bi sicer predstavljala finančno ali drugačno škodo, vendar pa posledice ne bi ogrozile delovanja organizacije kot celote. Za spremljanje ter obvladovanje teh tveganj so zadolženi lastniki poslovnih procesov, na poslovodstvu pa je odgovornost za vzpostavitev ustreznega notranje-kontrolnega okvira ter za zagotavljanje podpore lastnikom poslovnih procesov pri obvladovanju tveganj. Tu igrajo avtomatizirane kontrole organizacijskih procesov - **kontrole programskih rešitev**[3] ključno vlogo, saj po eni strani zagotavljajo ustrezno vršenje poslovnih procesov, po drugi strani pa tudi višjo učinkovitost v primerjavi z ročnimi kontrolami.

Tveganja informacijskih tehnologij lahko sodijo tako med organizacijska, kot tudi med poslovna tveganja. Razlog, da jih z vsebinskega vidika smiselno obravnavati ločeno je v tem, da je praviloma nemogoče povezati uresničitev nekega tveganja informacijskih tehnologij s konkretnim organizacijskim procesom, na katerem bo nastala poslovna škoda. Izpad glavnega strežnika centralne programske na primer lahko povzroči materialno škodo samo na nekaterih organizacijskih procesih, medtem ko pri izpadu drugih procesov ne pride do poslovne škode. V drugih okoliščinah lahko isti incident povzroči poleg materialne škode vsem organizacijskim procesom tudi izgubo ugleda organizacije. Nekatera tveganja informacijskih tehnologij predstavljajo zgolj grožnjo ugledu organizacije, druga tveganja ogrožajo informacijske vire in organizacijske procese. Tveganja informacijskih tehnologij zmanjšujemo z

[3] V slovenskem jeziku zanje uporabljamo tudi izraze *aplikativne kontrole, aplikacijske kontrole* in *kontrole uporabnostnih rešitev*.

uvedbo kontrolnih aktivnosti - **splošnih kontrol informacijskih tehnologij**[4], ki pa ponovno niso povezane s konkretnimi organizacijskimi procesi temveč se nanašajo na celotno tehnološko infrastrukturo organizacije.

Vsi trije nivoji obvladovanja tveganj so med seboj povezani - uresničitev grožnje, zaznane v skupini tveganj poslovnih procesov ali tveganj informacijskih tehnologij lahko vpliva na poslovanje celotne organizacije. Delitev, ki jo uporabljamo, je pripravljena z vidika primarne odgovornosti za spremljanje tveganj in predlaganje ukrepov za izboljšavo kontrolnih aktivnosti in drugih ukrepov za zmanjševanje tveganj. Navadno srednji nivo poslovodstva za svoja področja podrobno pozna potencialna tveganja in je hkrati v okviru svojih strokovnih področij najbolje usposobljeno predlagati ukrepe za zmanjševanje izpostavljenosti. Poslovodstvo je odgovorno za vzpostavitev okolja, kjer strokovnjaki lahko izvajajo aktivnosti za spremljanje in zmanjševanje tveganj ter za zagotavljanje podpore tem aktivnostim. Poslovodstvo nosi končno odgovornost za obvladovanje tveganj v organizaciji, vključno s tveganji na nivoju poslovnih procesov, za identifikacijo in spremljavo katerih, so odgovorni lastniki poslovnih procesov.

Poslovodstvo je odgovorno tudi za identifikacijo in neposredno spremljanje organizacijskih tveganj, torej vseh tveganj, katerih realizacija bi lahko resno škodovala organizaciji ali celo ogrozila njen obstoj.

3. Tveganje pri izvajanju revizijske naloge

Tveganja pri delovanju in kontroliranju so pokrita v okviru ocene tveganj revidiranega področja, tveganje pri odkrivanju pa z opredelitvijo revizijske naloge in izvedenimi postopki. Tveganja pri odkrivanju izvirajo iz možnosti, da bi strokovnjak za revizijo IS in dajanje zagotovil pri pregledu spregledal nedelujoče kontrole ali druge pomanjkljivosti. Tveganja pri odkrivanju ni nikoli mogoče v celoti odstraniti, je pa potrebno revizijske postopke načrtovati tako, da se pokrijejo glavne skupine izpostavljenosti.

Tveganja pri odkrivanju lahko nastanejo zaradi neustreznega načrtovanja, nepopolnega razkritja podatkov s strani revidirancev ali iz drugih razlogov. Zmanjšanje tveganj pri odkrivanju je med drugim mogoče z:

- ustreznim načrtovanem,
- kakovostnim pregledom revizijskega načrta in drugih delovnih dokumentov s strani drugega usposobljenega strokovnjaka za revizijo

[4] V slovenskem jeziku zanje uporabljamo tudi izraz *splošne računalniške kontrole*.

IS in dajanje zagotovil ali nadrejenega z ustreznimi strokovnimi kompetencami,

- prilagodljivostjo pri načrtovanju postopkov - možnostjo spremembe postopkov med izvajanjem pregleda kot odziv na nova zaznana tveganja.

Poleg tveganja, povezanega z revidiranim področjem, je potrebno v načrtovanju upoštevati tudi tveganja, povezana z revizijskim poslom.

Tveganja in revizijski program

Pri načrtovanju in izvajanju revizije naj si strokovnjak za revizijo IS in dajanje zagotovil prizadeva, da zmanjša revizijsko tveganje na sprejemljivo nizko raven in izpolni revizijske cilje. To doseže z ustreznim ocenjevanjem kontrol IS in z njimi povezanih kontrol.

Standardi za revidiranje informacijskih sistemov in dajanje zagotovil so do neke mere usmerjeni v revizije kontrol. To pa niso edini tipi revizijskih poslov, ki se izvajajo skladno s temi standardi. Pri drugih poslih (na primer reviziji učinkovitosti delovanja informacijskega sistema) je potrebno zahteve standardov in usmeritve smernic primerno prilagoditi.

Pomembnost in stopnja revizijskega tveganja, ki sta za strokovnjaka za revizijo IS in dajanje zagotovil še sprejemljivi, sta v obratnem sorazmerju; večja kot je stopnja pomembnosti, manjša je sprejemljivost revizijskega tveganja in obratno. To strokovnjak za revizijo IS in dajanje zagotovil omogoča, da določi vrsto, čas in obseg revizijskih postopkov.

Za vsako opredeljeno tveganje je potrebno opredeliti revizijska dejanja, s katerimi bo strokovnjak za revizijo IS in dajanje zagotovil presojal pomen tega tveganja.

Če je cilj revizijskega posla*: Podati mnenje o varnosti IS organizacije XY*, bo strokovnjak za revizijo IS in dajanje zagotovil na podlagi postopkov spoznavanja IS opredelil osnovna tveganja, ki jim je izpostavljena varnost IS. Tovrstna tveganja bi bila lahko:

- neustrezno razkritje osebnih podatkov,
- neoperativnost zaradi vdora zunanjih napadalcev,
- neoperativnost zaradi okužbe z zlonamerno programsko kodo…..

Za tveganje neustrezno razkritje osebnih podatkov, je odziv strokovnjaka za revizijo IS in dajanje zagotovil lahko načrtovanje postopkov za presojo:

- splošnih postopkov za upravljanje zaupnih podatkov,

- postopkov za zagotavljane in ohranjanje revizijske sledi vpogledov v zaupne podatke,
- postopkov za upravljanje uporabniških dostopov, zlasti postopkov za dodeljevanje in odvzemanje dostopov do osebnih podatkov ter postopkov za opredeljevanje uporabniških vlog z dostopi do osebnih podatkov,
- postopkov za izobraževanje uporabnikov o ravnanju z osebnimi podatki,
- postopkov za upravljanje administrativnih in drugih močnih dostopov,
- tehničnih rešitev za prenos osebnih podatkov po komunikacijskih omrežjih,
- tehničnih rešitev za omejevanje možnosti masovnega shranjevanja osebnih podatkov izven glavne programske rešitve (na pomnilniške enote kot so trdi diski uporabnikov, prenosne pomnilniške enote,….)
- postopkov za zagotavljanje skladnosti z zakonodajnimi zahtevami.

Revizijski program primarno izhaja iz opredelitve tveganj, viri za postopke pa so lahko različna vodila IIA in ISACA, strokovno delo drugih revizorjev, pretekli revizijski programi ipd.

Tabela 1: Vzorčni primer na oceni tveganj temelječega revizijskega programa

Tveganja	Vzorčne kontrole / kontrolni cilji	Opis področja iz faze spoznavanja informacijskega okolja organizacije (teoretičen primer)[5]	Postopki strokovnjaka za revizijo IS in dajanje zagotovil za pridobitev zagotovila o ustreznosti kontrolnega okolja

[5] 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 strokovnjak za revizijo IS in dajanje zagotovil še ni izvedel postopkov za njihovo potrditev.