UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

REVIZIJA INFORMACIJSKIH SISTEMOV V PODJETJU

Ljubljana, september 2008 ROK HAJDUKOVIĆ

IZJAVA

Študent ROK HAJDUKOVIĆ izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. ALEŠA GROZNIKA, in dovolim njegovo objavo na fakultetnih spletnih straneh.

V Ljubljani, dne 11. 9. 2008 Podpis: _____

KAZALO

KAZALO SLIK IN TABEL

KAZALO PRILOG

UVOD

Revizija se z leti vedno bolj razvija v panogo z večimi specifičnimi področji, med katere sodi tudi revizija informacijskih sistemov (dalje revizija IS). Slednja postaja vedno pomembnejša z vidika poslovodstva in s tem tudi zahtevnejša za izvajalce. Informacijska tehnologija je tako napredovala v zadnjih letih, da je praktično nemogoče, da bi revizijo IS opravljal notranji revizor, kot je bila praksa pred leti. Zahtevana znanja o uporabi te tehnologije, kot tudi ugotavljanje tveganj povezanih z informacijskimi sistemi, so botrovala, da je postala revizija IS nepogrešljiv člen revizije večjih podjetij in finančnih institucij (Revizor informacijskih sistemov – priložnost za kariero!, 2007).

Informatika je v današnjem času eden najpomembnejših dejavnikov poslovanja podjetja. Vsako manjše ali večje podjetje ima v svoje poslovanje že integrirano nekakšno informacijsko tehnologijo oz. je uspeh podjetja pogojen z delujočim informacijskim sistemom. Informacijski sistemi se razlikujejo med podjetji tako po vrsti kot namenu, vendar glavna funkcija ostaja v oskrbovanju informacij uporabnikom za odločanje. Delovanje informacijskega sistema je tako eden ključnih dejavnikov za uspešno poslovanje podjetja in zato postaja potreba po reviziji informacijskih sistemov vedno pomembnejša.

Namen in cilj revizije informacijskih sistemov v podjetju je zagotovilo, da je delovanje informacijske tehnologije v skladu s pričakovanji. Z zbiranjem in oceno revizijskih dokazov je potrebno opredeliti, ali informacijski sistem zadovoljivo varuje sredstva, vzdržuje podatke in neoporečnost sistema, zagotavlja potrebne in zanesljive informacije, učinkovito dosega organizacijske cilje in ima vzpostavljene notranje kontrole, ki zagotavljajo, da bodo poslovni, operativni in kontrolni cilji doseženi in nezaželeni dogodki preprečeni (Botha, 2002).

Namen diplomske naloge je bolje spoznati smernice, standarde in glavne metodologije, ki se jih revizor IS poslužuje pri svojem delu. Za raziskovanje omenjenega področja sem se v diplomski nalogi odločil zaradi dejstva, ker v novejšem času informacijski sistemi v sodobnem podjetju predstavljajo samo jedro uspešnega poslovanja. Revizija IS je vedno bolj potrebna za zagotavljanje uspešnega in predvsem varnega informacijskega sistema, kar zmanjšuje različna tveganja, ki bi lahko negativno vplivala na nadaljnje poslovanje podjetja.

Cilj diplomske naloge je predstavitev mednarodnih smernic in standardov, ki določajo okvire revizije informacijskih sistemov. Mednarodne smernice ISACA ter standardi revizije IS predstavljajo glavne usmeritve za revizorja IS in so osnova za preverjanje dejanskega stanja informacijskega sistema. Kot dodaten cilj sem si zastavil preverbo, ali revizorji IS v Sloveniji dejansko opravljajo svoje delo na podlagi omenjenih smernic in standardov.

V diplomski nalogi bom tako na podlagi praktičnega primera in mednarodnih smernic ter standardov v zvezi z revizijo informacijskih sistemov poizkušal potrditi naslednjo tezo:

Revizija IS s svojim procesom dejansko omogoča ter prispeva k boljšem razvoju, učinkovitosti, ustreznosti in varnosti informacijskega sistema v podjetju.

V prvem poglavju bom podrobneje predstavil revizijo informacijskih sistemov ter opredelil zakonske podlage, standarde in smernice, ki jo definirajo. Poleg tega bom opredelil še glavno metodologijo, ki jo uporabljajo revizorji IS pri svojem delu.

V drugem poglavju bom podrobneje opredelil razloge, zakaj se podjetja odločajo za revizijo IS, zakaj je potrebna in kaj preprečuje.

Teoretična področja dela revizorja IS bom podrobneje opredelil v tretjem poglavju, medtem ko bom dejansko delo revizorja IS opisal v četrtem poglavju.

V petem poglavju bom še na kratko komentiral opravljen intervju z revizorjem IS in z zadnjim poglavjem sklenil ter povzel misli in ugotovitve celotnega diplomskega dela.

1 REVIZIJA INFORMACIJSKIH SISTEMOV

1.1 Opredelitev

»Revizija – pregled z namenom prepričati se, da je pregledovano urejeno v skladu z zakoni, pravili, standardi in *dobrimi navadami*.

Informacijski sistem – sistem zbiranja, urejanja, obdelovanja, hranjenja in prikazovanja podatkov ter njihovo preoblikovanje v informacije, največkrat s pomočjo računalniške tehnologije.« (Osnovni pojmi revizije informacijskih sistemov, 2007)

Tako lahko opredelimo revizijo IS kot pregled sistemov za zbiranje, urejanje, obdelovanje in prikazovanje podatkov, njihovo preoblikovanje v informacije, ter usklajenost le teh s standardi in zakoni ter dobrimi navadami s področja informacijskih tehnologij in informatike (Osnovni pojmi revizije informacijskih sistemov, 2007).

Za samo podjetje oz. organizacijo, ki se zanaša na informacijski sistem, lahko revizija IS izboljša nekatera področja uporabe in uvedbe informacijskega sistema. Ko se podjetje odloči za prenovo oz. uvajanje novega informacijskega sistema, je pri tem zelo dobrodošla revizija IS, ki usmerja prenovo v pravo smer in tudi poda nove rešitve za doseganje dolgoročnih ciljev organizacije. Revizorji IS preverijo ustreznost izrabe računalniške tehnologije ter izboljšajo učinkovitost informacijskega sistema pri upravljanju poslovnih procesov. Kot bolj pomembni prispevek revizije IS bi poudaril preprečevanje zlorabe informacijske tehnologije

in tudi preverjanje ali informacijski sistem uspešno varuje poslovne skrivnosti. Zadnji pomembnejši dejavnik potrebe po reviziji IS je tudi omogočanje neprekinjenega delovanja informacijskega sistema in s tem nepotrebne izgube zaradi prekinitev poslovanja (Pomen revizije informacijskih sistemov pri upravljanju poslovnih sistemov, 2007).

1.2 Zakoni in revizija informacijskih sistemov

Pri reviziji informacijskih sistemov mora preizkušeni revizor informacijskih sistemov pri svojem delu dosledno upoštevati naslednje zakone in predpise (Revizija IS, 2007):

- Standardi revidiranja informacijskih sistemov,
- Mednarodni splošni standardi za revidiranje informacijskih sistemov (ISACA, BS ISO/IEC 27002:2005, BS 7799-1:2000),
- Zakon o revidiranju,
- Kodeks poklicne etike revizorja informacijskih sistemov.

Zgoraj našteti zakoni in standardi so samo osnova, ki jo mora vsak revizor IS dobro poznati, poleg tega pa se mora zavedati, da je potrebno pri reviziji določenih informacijskih sistemov poznati še specifično zakonodajo.

Pri vsakem podjetju mora revizor IS upoštevati njegovo dejavnost in s tem povezana tveganja. Glede na dejavnost mora upoštevati tudi zakone in sklepe, ki ta področja določajo. Zakoni, kot je ZVOP-1, ki določa ravnanje z osebnimi podatki, veljajo za vsa podjetja, na drugi strani pa Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) velja samo za podjetja, ki jih uporabljajo. Sklepi pa natančneje določajo način dela, izračunavanja, vodenje revizijskih sledi, dokumentacije, ipd.

Glede na področje revidiranja mora tako revizor IS pred začetkom revizije preučiti zakone in uredbe, ki to področje urejajo. Sklep o kadrovskih, tehničnih in organizacijskih pogojih ter dokumentaciji npr. jasno določa kadrovske, tehnične in organizacijske pogoje, ki jih mora izpolnjevati družba za opravljanje storitev upravljanja investicijskih skladov. Tak sklep se npr. uporablja pri reviziji IS investicijskih skladov (KPMG Audit manual, 2007).

1.2.1 Standardi revidiranja informacijskih sistemov

Standarde revidiranja informacijskih sistemov sprejema in objavlja Slovenski inštitut za revizijo (Statut Slovenskega inštituta za revizijo, 2001).

Standarde revidiranja informacijskih sistemov pa oblikujejo naslednje tri ustanove:

- Slovenski inštitut za revizijo,
- ISACA (Information Systems Audit and Control Association),
- THEIIA (The Institute of Internal Auditor).

1.2.2 Mednarodni standardi za revidiranje informacijskih sistemov

Obstajata dve pomembni mednarodni instituciji, ki določata smernice in standarde potrebne pri reviziji IS – ISACA in ISO.

a.) ISACA smernice

Mednarodne smernice za revidiranje informacijskih sistemov, ki jih določa organizacija ISACA, so naslednje:

- **S1 - Listina o reviziji**

Poslovodstvo mora ustrezno dokumentirati in odobriti cilje, obveznosti, pooblastila in odgovornosti pri revidiranju informacijskih sistemov.

- **S2 – Neodvisnost**

Strokovna neodvisnost: revizor IS mora biti neodvisen v vseh zadevah revidiranja informacijskih sistemov, tako v ravnanju kot pri pristopu.
Organizacijska neodvisnost: revizija IS mora biti neodvisna od revidiranega področja, da je lahko delo revizorja IS objektivno opravljeno.

- **S3 - Strokovna etika in standardi**

Poklicna etika: revizor IS mora slediti pravilom poklicne etike, ki jih predpisuje ISACA.
Poklicna skrbnost: poklicna skrbnost revizorja IS zahteva, da pri vseh svojih aktivnostih upošteva vse vidike revizijskih standardov.

- **S4 – Strokovnost**

Revizor IS mora biti tehnično strokovno usposobljen za opravljanje svojega dela, mora pa tudi redno vzdrževati svojo usposobljenost s stalnim strokovnim izobraževanjem.

- **S5 – Načrtovanje**

Revizor IS mora načrtovati svoje revizijsko delo ob upoštevanju ciljev revizije in spoštovanju zakonodaje ter ustreznih strokovnih in revizijskih standardov. Poleg tega mora glede na oceno tveganja pripraviti in dokumentirati pristop k reviziji. Pripraviti mora načrt revizije v okviru ciljev, časa, obsega in sredstev, ki jih potrebuje za revizijo. Prav tako pa bi moral pripraviti še program postopkov, ki jih bo moral izvesti med postopkom.

- **S6 - Izvedba revizije**

Obstajati mora nadzor nad delom revizorjev IS. S tem se zagotovi ustreznost in pravilnost opravljenih revizijskih postopkov ob upoštevanju standardov revidiranja IS. Revizor IS mora pridobiti zadostne, zanesljive in ustrezne dokaze za dosego revizijskih ciljev, ki jih je potrebno podpreti s primernimi analitičnimi postopki in interpretacijo pridobljenih dokazov. Celotno delo mora tudi ustrezno dokumentirati.

- **S7 – Poročanje**

Revizor IS mora po zaključku revizije izdelati poročilo o ciljih, obsegu in opravljenih postopkih v reviziji ter navesti prejemnike poročila in organizacijsko enoto, ki je bila evidentirana. V poročilu mora navesti odkritja, zaključke, priporočila in kakršnekoli druge omejitve pri opredelitvah, ki jih zabeleži v povezavi z revizijo.

- **S8 - Po-revizijske aktivnosti**

Po izdanem poročilu ugotovitev in priporočil mora revizor oceniti na podlagi novo pridobljenih informacij, ali so bila priporočila v reviziji ustrezno upoštevana v predvidenem času.

- **S9 - Nepravilnosti in nezakonite dejavnosti**

Ta standard usmerja delo revizorja IS v primeru, da med postopkom odkrije nepravilnosti oziroma nezakonite dejavnosti. Poleg tega določa odgovornosti revizorja in postopke za razkritje ter ukrepanje v izbranih primerih.

- **S10 - IT nadzor**

Revizor IS mora preveriti in oceniti funkcionalnost in učinkovitost IS glede na vizijo, poslanstvo, vrednote, cilje in strategije organizacije. Prav tako se mora prepričati, ali je IS skladen z zakoni, okoljevarstvenimi, kakovostnimi in varstvenimi zahtevami.

- **S11 - Uporaba ocene tveganja pri načrtovanju revizije**

Revizor IS mora uporabiti ustrezne metode in tehnike za ocenitev tveganja pri načrtovanju celotne revizije IS in pri tem zagotoviti ustreznost virov za izvedbo revizije
(CISA Review manual 2006, 2006, str. 26-29).

b.) BS ISO/IEC 27002:2005

Poleg že navedenih standardov revidiranja informacijskih sistemov, revizorji uporabljajo še ISO (*International Standard Organization*) in BSi (*British Standard Institute*) standarde. Eden od bolj pomembnih standardov omenjenih organizacij se imenuje ISO/IEC 27002:2005. Vsebinski naslov tega standarda je »Informacijska tehnologija – Kodeks

varovanja informacij«. Že naslov nam pove, da standard opredeljuje najboljšo prakso za upravljanje z varnostjo informacij. Pri tem se osredotoča na več področij povezanih z doseganjem optimalne varnosti informacijskega sistema. Ta področja so (Informacijska tehnologija – Kodeks varovanja informacij, 2005):

- varnostna politika,
- organizacijska varnost,
- klasifikacija sredstev in kontrola,
- varnost osebja (varnost pri pridobivanju zaposlenih in opredelitvi dela, ...),
- fizična zaščita in zaščita okolja,
- upravljanje s komunikacijami in s produkcijo (skrbništvo, zaščita pred zlonamerno programsko opremo, ...),
- nadzor dostopa,
- razvijanje in vzdrževanje sistemov,
- upravljanje neprekinjenega poslovanja,
- združljivost.

1.2.3 Zakon o revidiranju

Zakon o revidiranju (2008) opredeljuje revizijo vseh vrst, med njimi prav tako revizijo informacijskih sistemov. Temeljne določbe zakona med drugimi določajo pojem revizije, način revidiranja, nadzor nad revizijo, osebe in družbe zmožne opravljanja storitev revidiranja ter strokovna področja, povezana z revidiranjem. Poleg temeljnih določb zakon določi tudi inštitut za revizijo, katerega temeljne naloge so:

- sprejemanje standardov za posamezne vrste revizij;
- določanje strokovnih znanj in izkušenj, potrebnih za opravljanje nalog;
- organiziranje strokovnih izobraževanj, izvajanje preizkusov strokovnih znanj in izdajanje potrdil o strokovnih znanjih za opravljanje nalog določenih s prejšnjo točko;
- odločanje o izdaji in odvzemu dovoljenj za opravljanje: storitev revidiranja, nalog pooblaščenega revizorja in revizorja ter nalog pooblaščenega ocenjevalca;
- določanje strokovnih znanj in izkušenj, potrebnih za pridobitev strokovnega naziva: preizkušeni notranji revizor, preizkušeni računovodja, preizkušeni poslovni finančnik, preizkušeni revizor informacijskih sistemov;
- organiziranje strokovnih izobraževanj, izvajanje preizkusov strokovnih znanj in izdajanje potrdil o strokovnih znanjih za pridobitev strokovnih nazivov iz prejšnje točke;
- opravlja druge strokovne naloge in storitve, povezane z razvojem revizijske stroke in drugih strokovnih področij, povezanih z revidiranjem;
- vodenje registrov: revizijskih družb in samostojnih revizorjev, pooblaščenih revizorjev in revizorjev, pooblaščenih ocenjevalcev ter oseb, ki so pridobile strokovne nazive, ki jih podeljuje inštitut;
- določa smernice za oblikovanje cen revizijskih storitev;
- opravlja druge naloge, določene z zakonom oziroma statutom inštituta.

Organi inštituta so svet inštituta, direktor inštituta, revizijski svet, strokovni svet (ZREv-2, 2008).

Ostali členi zakona podrobneje opredeljujejo (ZREv-2, 2008):

- način in potek revidiranja,
- pooblaščenega revizorja in revizorja ter nadzor nad njimi,
- revizijsko družbo in samostojnega revizorja,
- pooblaščenega ocenjevalca,
- postopke odločanja inštituta v posamičnih zadevah,
- vrste registrov in njihovega upravljavca,
- kazenske določbe,
- ter prehodne in končne določbe.

1.2.4 Kodeks poklicne etike revizorja informacijskih sistemov

»Kodeks poklicne etike revizorja IS (odslej kodeks) je zapis pravil obnašanja, po katerih se revizor IS ravna pri opravljanju svojih strokovnih nalog« (Kodeks poklicne etike revizorja IS, 2000, str. 1).

Kodeks sprejme strokovni svet Inštituta in zavezuje revizorje IS, ki jim je Inštitut podelil naziv.

Namen kodeksa
Namen kodeksa poklicne etike revizorja IS je v določitvi pravil etičnega in poklicnega obnašanja revizorja IS in da mu le ta pravila služijo kot vodilo pri opravljanju svojega dela. V primeru, da se revizor IS ne bi obnašal v skladu z načeli kodeksa, se mu izreče disciplinski ukrep.

Temeljna načela poklicne etike revizorja informacijskih sistemov
Načela poklicne etike predpisujejo delo revizorja IS z vidika vzdrževanja visokih standardov strokovnosti kontroliranja ter etičnosti in dostojanstva na tem področju. Te standarde določa ISACA, ki tudi spodbuja njihovo upoštevanje. Poleg navedenega mora revizor nenehno spremljati teoretične in praktične dosežke v stroki in se temu primerno izobraževati ter svoje znanje prenašati na mlajše kolege. Zadnje načelo poklicne etike revizorja IS navaja, da je sodelovanje med revizorji zaželeno in se ga tudi spodbuja. Tako se ne zavrača pomoči kolegom v stroki z nasvetom ali mnenjem.

Načela obnašanja revizorja informacijskih sistemov
Načela obnašanja revizorja informacijskih sistemov določajo stališča, ki jih mora revizor IS vestno upoštevati. Vsebinsko se opredeljujejo glede revizorjeve odgovornosti, zaupnosti, neoporečnosti, nepristranskosti in neodvisnosti ter dolžne poklicne skrbnosti oz. strokovnosti.

Revizor IS nikoli zavestno ne sodeluje pri kakršnihkoli nezakonitih in neetičnih dejavnosti in deluje v korist strank, zaposlenih, delničarjev in drugih.

Kratek povzetek posameznih načel:

1 Revizor IS učinkovito opravlja zadane naloge strokovno in pošteno ter pri tem dosledno spoštuje etična načela in pravila iz kodeksa.
2 Revizor IS mora biti odgovoren, tako strokovno kot etično, pri svojem delu, ter se zavedati, da lahko prevzame samo tiste naloge, katere je sposoben strokovno neoporečno opraviti.
3 Revizor IS ohranja visoko stopnjo strokovnosti na vseh področjih informacijskih sistemov.
4 Revizor IS upošteva slovenske predpise delujoče v slovenskem prostoru in mednarodne v mednarodnem prostoru.
5 Revizor IS podpira izobraževanje vseh sodelujočih v reviziji, da bi se vsi zavedali nujnosti revizije in kontrole informacijskih sistemov.
6 Revizor IS sprejema obveznosti v skladu z javnim interesom ter upravičuje zaupanje javnosti in izkazuje predanost poklicu.
7 Revizor IS ne sme razkriti zaupnih informacij pridobljenih pri svojem delu ter jih ne sme uporabljati v svojo korist (spoštuje načelo zaupnosti).
8 Revizor IS mora opravljati svoje delo kar se da neoporečno in v nobenem primeru ne podredi svoje presoje v korist naročnika, saj bi s tem preprečil nepristransko oceno vrednosti. Prav tako ne sme sprejeti večje vrednosti od stranke, dobavitelja, sodelavca ali drugega poslovnega partnerja, ker bi to škodovalo ugledu stroke, njegovem ugledu in ugledu Inštituta.
9 Revizor IS mora biti strokovno neodvisen in mora se zavedati, da sta bistveni neoporečnost in nepristranskost pri opravljanju tega poklica. Revizor IS mora torej biti pošten pri svojem razmišljanju ter se izogibati navzkrižnih interesov s sodelujočimi v reviziji.
10 Revizor IS spoštuje strokovna pravila (strokovna načela, standarde in poklicno-etična načela) ter se dopolnjuje v svoji strokovnosti, povečuje kakovost storitev in je poklicno skrben. Revizor IS je osebno odgovoren za zagotovitev organizacijskih rešitev, ki zagotavljajo neodvisnost revidiranja informacijskih sistemov v okolju, v katerem deluje. V skladu z poklicno skrbnostjo mora ustrezno načrtovati, uresničevati in nadzirati te dejavnosti. V zaključku mora vestno pripraviti mnenja, ki so poštena slika revizije, ter so dovolj jasna za prejemnike (Kodeks poklicne etike revizorja IS, 2000, str. 2).

1.3 Metodologija

Edina mednarodno priznana metodologija revidiranja informacijskih sistemov se imenuje COBIT. Nastala je pod okriljem mednarodnega združenja za kontrolo in revizijo

informacijskih sistemov – ISACA in bila prvič izdana leta 1996. Sama metodologija opredeljuje cilje in postopke revidiranja informacijskih sistemov.

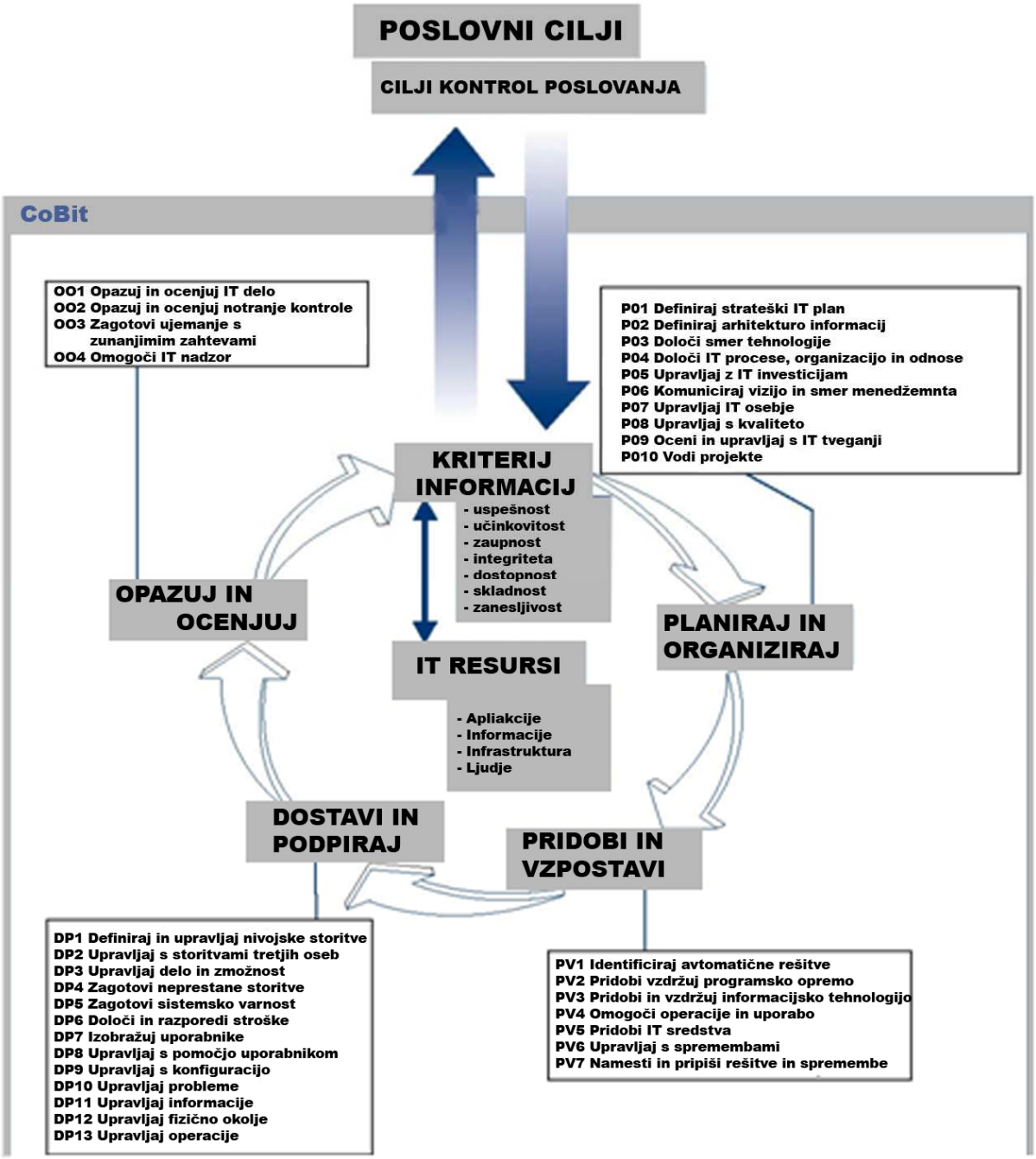
Po metodologiji COBIT morajo informacije izpolnjevati določene kriterije kot so:

- učinkovitost,
- zmogljivost,
- zaupnost,
- popolnost,
- razpoložljivost,
- skladnost,
- zanesljivost.

Cilji revizije informacijskih sistemov so po metodologiji COBIT sestavljeni iz štirih domen in štiriintridesetih procesov. Za vsak proces so določene metode pregleda ter kaj je treba proučiti, kaj proces omogoča in kako mora biti izvajana kontrola procesa. Domene ciljev revizije IS predstavljajo štiri različne vidike pregleda informacijskih sistemov.

Kot prvo domeno bi omenil samo načrtovanje in organiziranje informacijskih sistemov, strateško planiranje, definiranje informacijske arhitekture, tehnoloških usmeritev ter upravljanje investicij. Druga domena predstavlja pridobivanje, izbor, izvedbo in uvajanje informacijskih sistemov ter vzdrževanje informacijskih sistemov po uvedbi. Kot tretjo domeno lahko opredelimo področja upravljanja in zagotavljanje delovanja IS, pomoč, servise, varnost, zagotavljanje neprekinjenosti poslovanja ter izobraževanje in usposabljanje uporabnikov. Zadnja, četrta domena ciljev revizija IS pa predstavlja opazovanje in nadzor procesov. Na sliki 1 so shematsko prikazane zgoraj omenjene domene in procesi. Predstavljeno je tudi ogrodje metodologije COBIT (Osnovni pojmi revizije informacijskih sistemov, 2007).

Slika 1: Ogrodje metodologije COBIT



Vir: Cobit 4.1, str. 26; Lastna priredba

1.4 Družbe zavezane za revizijo informacijskih sistemov

Družbe, ki so zavezane k reviziji informacijskih sistemov, morajo imeti izpolnjenega vsaj enega izmed spodaj navedenih kriterijev (KPMG Audit manual, 2007):

- družba kotira na borzi;
- družba je finančna institucija (borznoposredniške hiše, družbe za upravljanje, zavarovalnice, banke);

- v primeru, da revizija računovodskih izkazov za družbo obsega več kot tisoč delovnih ur, je družba tudi zavezana k reviziji informacijskih sistemov;
- informacijska tehnologija je kritična za poslovanje podjetja.

Od teh so zakonsko določene družbe zavezane k reviziji IS banke, borznoposredniške družbe, družbe za upravljanje, zavarovalnice in igralnice (ZREv-2, 2008).

2 POTREBA PO KONTROLI IN REVIZIJI INFORMACIJSKIH SISTEMOV

V uvodu diplomskega dela sem izpostavil dejstvo, da postaja revizija IS vedno bolj potreben del samega poslovanja, brez katere bi večja in informacijsko podprta podjetja težko dosegala optimalne poslovne rezultate. Poleg zakonsko zavezanih podjetij k reviziji IS se vse več družb odloča za pregled njihovega informacijskega sistema s strani preizkušenih revizorjev IS, ker se zavedajo pomena kvalitetnega informacijskega sistema ter optimizacije poslovnih rezultatov. V tem poglavju bom predstavil glavne prednosti in razloge za opravljanje revizije IS ter poskusil opravičiti strošek revizorjev IS z vidika poslovodstva podjetja.

Obstaja sedem pomembnih razlogov zaradi katerih se upoštevata kontrola in revizija IS za nepogrešljiva člena v sestavi pričakovanega kvalitetnega in učinkovitega informacijskega sistema (Panian, 2001, str. 5):

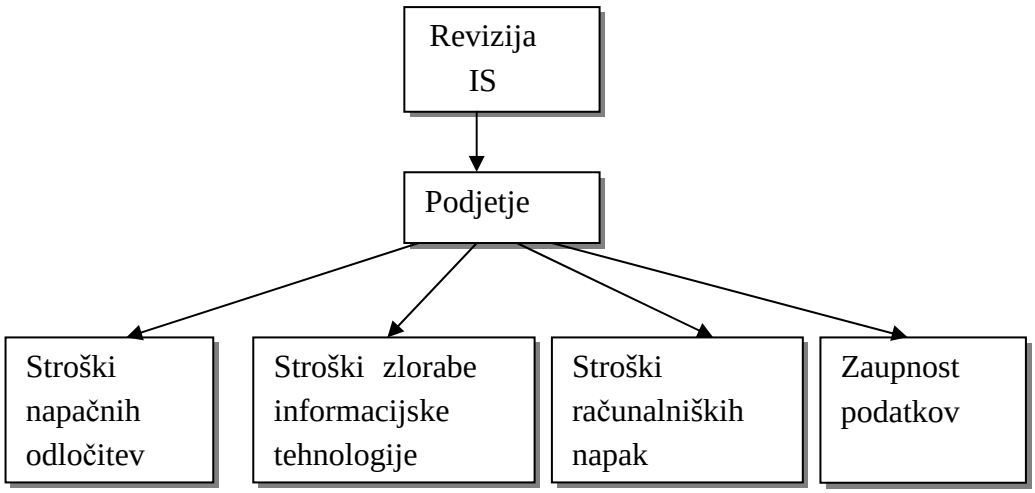
- stroški izgube podatkov,
- stroški napačnih odločitev na podlagi nepravilnih podatkov,
- stroški zlorabe informacijske tehnologije,
- vrednost tehnologije, programov in zaposlenih,
- stroški napak zaradi informacijske tehnologije,
- zaupnost podatkov,
- kontrolirani razvoj uporabe informacijske tehnologije

Revizijo IS lahko opredelimo kot sredstvo za doseganje ciljev, kot so (Panian, 2001, str. 15):

- izboljšanje varnosti informacijskega sistema podjetja,
- višanje stopnje integritete podatkov,
- izboljšanje uporabnosti informacijskega sistema,
- izboljšanje učinkovitosti informacijskega sistema

Zgoraj navedeni cilji so predstavljeni tudi v obliki shematskega prikaza, vendar z vidika vpliva revizije IS na podjetje (glej sliko 2).

Slika 2: Vpliv funkcije revizije IS na podjetje



Vir: Panian, 2001, str. 15

Iz sheme (Slika 2) lahko razberemo, kako revizija IS vpliva na podjetje in predvsem katera področja pomaga obvladovati in preprečevati večje izgube prihodkov ter višje stroške zaradi napak v informacijskem sistemu.

2.1 Stroški napačnih odločitev

Informacijsko podprto podjetje se zanaša na svoj informacijski sistem pri odločanju o vseh zadevah, med katerimi so tako menedžerske kot tudi operativne odločitve. Slednje se morajo še toliko bolj opreti na pravilnost podatkov, na podlagi katerih se zaposleni v operativi odločajo, kajti najmanjša napaka lahko bistveno vpliva na pravilnost poslovanja. Npr., banka računa podjetju obresti za dani kredit in se le te na podlagi napak v informacijskem sistemu (napačni algoritem za obračun mesečnih obresti) obračunavajo za 0,1% višje, kot je dogovorjeno s pogodbo. Medtem, ko napaka v smislu trenutne vrednosti ni nujno velika, lahko podjetje, ki ima kredit pri banki, zavrne prihodnje medsebojno poslovanje, kajti zaupanje v to banko je izpuhtelo. Tako lahko razmeroma majhna napaka v informacijskem sistemu povzroči velike, že načrtovane izgube prihodkov.

Na drugi strani pa imamo menedžerske odločitve, ki se v večini primerov zanašajo na analize in statistike vzete iz velike količine podatkov, tako da majhna napaka ne bo toliko vplivala na končno odločitev menedžerja, saj se v analizi ogromne količine podatkov le ta ne bo videla. Kljub temu pa v primeru napak v informacijskem sistemu, menedžer ne more biti 100% prepričan v svojo odločitev, kar lahko povzroči mnogo problemov podjetju. Prav tako lahko napake v informacijskem sistemu vplivajo na odločitve drugih interesnih skupin, kot so npr. delničarji podjetja. Slednji se lahko na podlagi napačnih finančnih izkazov odločajo drugače oz. nepravilno o svojem bodočem investiranju v podjetje (Panian, 2001, str. 7).

2.2 Stroški zlorabe informacijske tehnologije

Zloraba informacijske tehnologije je po naravi eden bistvenih razlogov revizije informacijskih sistemov, ki v veliki meri preprečuje takšne zlorabe. Definicija zlorabe informacijske tehnologije po Icove, Serger in VonStorch je sledeča:

»Zloraba informacijske tehnologije je lahko vsak dogodek, pri katerem zlorabljen subjekt utrpi ali lahko utrpi izgubo oz. škodo in pri tem zlorabnež namerno dosega oz. bi lahko dosegel korist« (Panian, 2001, str. 9).

V praksi pa lahko opredelimo kot najverjetnejše in najpomembnejše naslednje oblike zlorab informacijske tehnologije:

- zloraba drugače legalnih pooblastil uporabnika informacijske tehnologije,
- napadi tako imenovanih »hekerjev«,
- računalniški virusi,
- nedovoljeni fizični pristopi k informacijski tehnologiji in podatkom,
- delno ali popolno uničenje uporabnosti informacijske tehnologije,
- kraja informacijske tehnologije,
- nedovoljena sprememba v informacijski tehnologiji,
- ogrožanje zaupnosti uporabnikov informacijskega sistema,
- preprečevanje normalnega funkcioniranja informacijske tehnologije,
- nedovoljena uporaba informacijske tehnologije,
- nedovoljena uporaba računalniških programov in neupoštevanje avtorskih pravic,
- fizični napadi na uporabnike informacijskega sistema.

Zgoraj navedeni razlogi so postali bolj izraziti šele v zadnjih letih, ko je tudi sama informacijska tehnologija masovno prešla v dobo brezžične komunikacije na medmrežju. Večina informacijskih sistemov v teh primerih postala veliko bolj ranljiva za zlorabe, tako zunanje kot notranje. Zato je potrebno, da podjetje opravlja kontrole nad svojo informacijsko tehnologijo ter redno naroča tudi revizijo svojega informacijskega sistema. S tem se še dodatno prepriča o varnosti podatkov s strani zunanjega ocenjevalca (Panian, 2001, str. 9).

2.2.1 Primeri zlorabe informacijske tehnologije

V Sloveniji je znan eden bolj odmevnih primerov zlorabe informacijske tehnologije primer Roberta Škulja, ki je ustvaril program (trojanski konj[1]), s katerim bi lahko, ob neznanju uporabnika NLB Klika, posameznik (ti. heker) vdrl v sistem NLB Klik. Po zahtevku Škulja, da mu NLB izplača 500.000 EUR za zaščitni program, ki bi ustavil tega »trojanskega konja«, ki ga je sam ustvaril, se je NLB odločila, da poda zahtevek ovadbe policiji, ki pa je tudi kazensko ovadila Škulja. Na sodišču so ga spoznali za nedolžnega in tudi priznali, da je

[1] Trojanski konj je računalniški program, ki se zdi navidez uporaben, v resnici pa povzroča škodo (Predstavitev virusov, črvov in trojanskih konjev, 2008).

sistem NLB Klik na ta način ranljiv. Kljub vsemu je Škulj deloval proti banki in dejansko ustvaril zlonamerni program, s katerim bi lahko zlorabil informacijski sistem banke (Potočnik, 2003).

V svetu je eden bolj odmevnih primerov zlorabe informacijske tehnologije primer finančnega podjetja UBS PaineWebber iz leta 2002, pri katerem je nezadovoljni sistemski administrator Roger Duronio sprožil tako imenovano »logično bombo[2]«, s katero je poškodoval celotno računalniško omrežje podjetja in naredil za 3 milijone dolarjev škode in tudi za namen svoje koristi v primeru padca delnice podjetja. Duronio je pred napadom kupil za 21.000 $ opcij, ki bi narasle v primeru padca cene delnice podjetja (Hulme, 2002). V letu 2006 je bil Duronio obtožen na 97 mesecev zapora za planiranje in izvedbo napada na informacijski sistem z logično bombo, s katero je onesposobil 2000 strežnikov in onemogočil trgovanje več kot 17.000 borznih posrednikov znotraj podjetja. Škodo napada je podjetje čutilo še 4 leta kasneje (Gaudin, 2006).

Dejansko obstaja veliko zlorab informacijske tehnologije, za katere sploh ne vemo. S pomočjo revizije informacijske tehnologije bi lahko podjetja take zlorabe zelo omejile in zmanjšale, vendar si odprave takih zlorab v celoti, v današnjem svetu, ob naraščajočem številu zlonamernih dejanj in vedno novih iznajdljivosti »hekerjev«, težko predstavljamo.

2.3 Stroški računalniških napak

Informacijsko podprto podjetje si prav tako ne more privoščiti napak zaradi napačno implementiranega informacijskega sistema. Informacijski sistem mora delovati čim bolj brezhibno, s čim manjšim številom možnih napak v procesu poslovanja. Bolj kot informacijski sistem odstopa od svoje namenjene funkcije, večje so lahko posledice napačnih podatkov, ki jih potrebujejo uporabniki oz. zaposleni pri svojem delu. Revizija IS preverja postavljene kontrole in dodaja morebitne nove kontrole informacijskega sistema, ter tako zmanjšuje tveganje napak v informacijski tehnologiji in s tem tudi zmanjšanje stroškov posledic teh napak (Panian, 2001, str. 10).

2.4 Zaupnost podatkov

Zaupnost podatkov in informacij je vedno bolj pomembno področje dobrega in konkurenčno zavedajočega sodobnega podjetja. Podjetje mora zaupati svojim zaposlenim ter svojemu informacijskemu sistemu, da varujejo zaupne podatke, ki bi lahko pomagali konkurenčnemu podjetju prevzeti del trga. Prav tako mora biti informacijski sistem zastavljen tako, da ima vsak zaposleni v podjetju določene pravice do dostopa podatkov, ki so omejene na njegovo področje dela. Tako se izniči oz. omeji možnost zlorabe podatkov. Vse to mora biti

[2] Logična bomba - zlonamerni program, ki se sproži ob izpolnitvi določenih pogojev, kot so npr. pretečen čas, število ponovitev, količina podatkov (islovar, 2008).

opredeljeno z varnostno politiko podjetja. Revizor IS v svojih postopkih preverja pravice uporabnikov informacijskega sistema ter oceni ali so le te pravilno oz, optimalno določene glede na delovno mesto posameznih zaposlenih (Varnostna politika, 2008; Panian, 2001, str. 11).

2.5 Posledice nepravilne presoje revizorja IS

Ena izmed posledic prehitre odločitve revizorja IS, da nekatere določene kontrole v informacijskem sistemu delujejo brez napak, je lahko v slabši izvedbi revizije računovodskih izkazov. V primeru, da dobijo revizorji računovodskih izkazov pozitivno mnenje revizorja IS o delovanju kontrole, ki vpliva na finančne izkaze podjetje, revizorji računovodskih izkazov ne opravijo kontrole nad večjim vzorcem podatkov, kot bi v primeru negativnega mnenja revizorja IS. Tako lahko tudi revizor RI izda pozitivno mnenje o računovodskih izkazih na podlagi nezadostne kontrole pravilnosti podatkov na premajhnem vzorcu. (KPMG Audit Manual, 2007)

3 POSTOPKI REVIZORJA INFORMACIJSKIH SISTEMOV

Večina večjih organizacij oz. podjetij v Sloveniji se zanaša na zmogljive informacijske sisteme, ki zbirajo, shranjujejo in obdelujejo podatke za namen boljšega odločanja posameznih uporabnikov sistema. Zato je glavna naloga revizorja IS pridobiti zadostna zagotovila o obstoju notranjih kontrol, njihovi učinkovitosti in stalnosti (Mugerle, 1995, str. 70).

Revizor informacijskih sistemov pri svojem delu upošteva več različnih smernic, standardov ter postopkov. Pri tem so mednarodno priznani in upoštevani postopki določeni od organizacije ISACA. Postopki, ki jih določa ISACA, niso obvezni za revizorja informacijskih sistemov, so pa zagotovilo, da revizor pri svojem delu upošteva zakone in standarde, ki opredeljujejo revizijo IS. Postopki so naslednji (CISA Review Manual 2006, 2006, str. 37):

- ugotavljanje tveganja informacijskih sistemov,
- digitalni podpisi,
- odkrivanje vdorov,
- virusi in druge zlonamerne kode,
- oceni tveganje kontrol,
- požarni zidovi,
- nepravilnosti in nezakonska dejanja,
- ocena varnosti – testiranje vdorov in analiza slabosti,
- ocena kontrola managementa nad metodologijo zaščite podatkov

Poleg upoštevanja zgoraj naštetih postopkov pa revizor informacijskih sistemov svoje delo razdeli v več področij (KPMG Audit Manual, 2007):

- Faza planiranja revizije IS:

    - določanje področja revizije IS,
    - odkrivanje prevar,
    - revizijsko tveganje in materialnost,
    - tehnike ocene tveganja,
    - revizijski cilji.
- Operativna faza revizije IS:
    - test kontrol in test podatkov,
    - dokazi,
    - pogovori z osebjem ter vpogled v njihovo delo,
    - vzorčenje,
    - računalniško podprte revizijske tehnike.
- Zaključna faza revizije IS:
    - ocena revizijskih slabosti in moči,
    - predstavitev revizijskih rezultatov,
    - dejanja managementa pri upoštevanju priporočil revizorja,
    - revizijska dokumentacija.

3.1 Faza planiranja revizije IS

V fazi planiranja revizije IS revizor IS opravi določene postopke, s katerimi si zagotovi, da bo revizija IS potekala v skladu z pričakovanji, tekoče in brez nepotrebnih komplikacij.

3.1.1 Določanje področja revizije IS

Revizor IS, glede na namen revizije IS, pred začetkom dela določi področja revizije IS, ki jih bo dejansko pregledal. Pri reviziji IS, ki služi kot dodatno zagotovilo delovanja notranjih kontrol informacijskega sistema za revizorje računovodskih izkazov, revizor IS opravi pregled splošnih kontrol in vseh splošnih področjih. Če bi pri katerem splošnem področju ugotovil oz. posumil v slabše delovanje kontrol, bi pri tem področju poglobil pregled ter tako ugotovil pravilno stanje kontrol in zmanjša tveganja, ki jih prvotne kontrole niso odkrile. V primeru naročene revizije IS s strani stranke, se ponavadi določi posebno področje revizije IS oz. celoten obseg revizije IS ter pregleda samo določen del informacijskega sistema, za katerega stranka (podjetje) verjame, da bi ga lahko z revizijo IS precej izboljšali. Poleg tega lahko revizor IS tudi z zbiranjem dejstev (prebiranje dokumentacije, internih aktov podjetja, nastavitve sistemov, opravljena testiranja) o poslovnem procesu, standardov podjetja in obsegu notranjih kontrol, določi področja revizije IS (Carlin & Gallegos, 2007).

Primer najbolj splošnih in pomembnejših področij revizije IS so (Revizija IS, 2007):

- varnost uporabniških programov (*Application Security Audit*),
- načrtovanje neprekinjenega poslovanja (*Business Continuity Plan (BCP) Audit),*
- upravljanje podatkov (*Data Management Audit),*
- organizacija informacijske tehnologije (*IT Organization Audit*),

- upravljanje strategije informacijske tehnologije (*IT Strategy Management Audit*),
- sistem načrtovanja virov podjetja (*Enterprise Resource Planning (ERP) Systems Audit*),
- upravljanje omrežja (*Network Management Audit*),
- varnost upravljanja in izvajanja postopkov (*Security Administration Audit*),
- licenčna ustreznost programje (*Software Licensure Compliance Audit*)

3.1.2 Odkrivanje prevar

Leta 1996 je Robert Klitgaard v raziskavi prevar in korupcije v državah po svetu predstavil formulo (1), ki na enostaven način pojasnjuje dinamiko gibanja obsega prevar in korupcije:

$$\boxed{PK = M + D - O} \quad (1)$$

(PK) Prevare in korupcija = M (stopnja monopolne (centralizirane) moči javnih uradnikov) + D (stopnja diskrecijskega uveljavljanja te moči) – O (odgovornost oz. polaganje računov) (Klitgaard, 1998).

Formula (1) nam nakazuje, da je obseg prevar in korupcije odvisen od obsega monopolne moči in možnosti njene diskrecijske uporabe javnih uradnikov, zmanjšana za stopnjo prevzemanja odgovornosti za odkrite prevare.

V reguliranih družbah je monopolna moč lahko zelo visoka, vendar je pa toliko manjša diskrecijska uporaba te moči. Diskrecijska uporaba je bolj prisotna v tranzicijskih državah in državah v razvoju, kjer so postopki upravljanja slabo opredeljeni in regulirani, in kjer je tudi sama stopnja prevzemanja odgovornost na nizki stopnji. Ta stopnja je nizka zaradi šibkih standardov etičnega ravnanja javnih uradnikov, pomanjkljivega sistema notranjega kontroliranja, pomanjkljive urejenosti javnega upravljanja in neučinkovitosti delovanja nadzornih institucij. Revizorji pomagajo vzpostaviti boljše kontrole nad poslovanjem, s tem se poveča možnost odkritja prevar, ter vzpostavijo standardi za bolj transparentno poslovanje in predvsem bolj pošteno in tako tudi bolj rastoče in uspešno poslovanje (Klitgaard, 1998).

Uprava podjetja je odgovorna za vzpostavitev, uveljavitev in vzdrževanje kontrol v informacijskem sistemu (dalje notranje kontrole), da zavaruje svoje poslovanje in pretok informacij. Revizor IS mora biti skozi celotno revizijo pozoren na možnosti prevar znotraj podjetja, kjer bi lahko določeni zaposleni izkoristili slabosti notranjih kontrol in tako zaradi osebnih koristi škodovali podjetju. Revizor IS je dolžan opazovati možne prevare in zlorabe vzpostavljenih notranjih kontrol na vsakem koraku svojega dela. Management se poleg neprestanega vzpostavljanja in vzdrževanja notranjih kontrol zanaša na revizorja IS za zagotovitev, da njihov informacijski sistem deluje v skladu z dobro prakso in da so vzpostavljene kontrole zadovoljive in zmožne odpravljati in opaziti morebitne zlorabe. Prav

tako se management zanaša na revizorja IS, da jim ob morebitnih nezadovoljivih kontrolah le to revizor sporoči in predlaga možne rešitve. V primeru, da revizor IS pri svojem delu odkrije kakšne primere prevare oz indikatorje zlorabe, mora po skrbnem premisleku, da obstaja potreba po bolj podrobni raziskavi, to poročati nadrejenim oblastem. V primeru odkritja večje prevare oz. ugotovitve velikega tveganja za možnost prevare pa mora le to revizor poročati revizijskem odboru (CISA Review Manual 2006, 2006, str. 39).

3.1.3 Revizijsko tveganje in materialnost

Podjetja in organizacije se medsebojno razlikujejo v svoji dejavnosti, naravi dela, načinom poslovanja in še mnogo drugih faktorjih, na kar mora biti revizor IS pozoren pri ocenjevanju revizijskega tveganja. Pri zdravstvenih organizacijah, letalskih družbah in drugih podjetij, kjer ima lahko vsaka napaka v sistemu tragične posledice, mora revizor upoštevati, da morajo biti notranje kontrole 100 % učinkovite z razliko v npr. proizvodnih podjetjih, kjer so lahko notranje kontrole nastavljene tako, da preprečijo samo večje napake oz. take, ki bi bistveno vplivale na finančne izkaze in učinkovitost poslovanja. Tako revizor tudi določi materialnost glede na organizacijo, kjer opravlja revizijo IS. Materialnost je skupek največjih možnih napak v informacijskem sistemu, ki ne vpliva bistveno na računovodske izkaze organizacije oz. ne vpliva bistveno na učinkovito poslovanje podjetja.

Revizijsko tveganje pa bi lahko definirali tudi kot tveganje, da finančni izkazi oz. informacije vsebujejo materialno napako, katere revizor IS tokom revizije ne bi odkril (CISA Review Manual 2006, 2006, str. 39).

Revizija tveganja je kombinacija treh kategoriziranih tveganj:

- tveganje pri delovanju (*Inherent risk* – IR),
- tveganje pri kontroliranju (*Control risk* – CR).
- tveganje pri odkrivanju (*Detection risk* – DR).

Tveganje pri delovanju. Je tveganje, da obstaja pomembna nepravilnost ali napačna navedba tako sama kot v kombinaciji z drugimi nepravilnostmi. To tveganje je povezano s samo naravo dejavnosti podjetja in se določi brez upoštevanja vzpostavljenih notranjih kontrol podjetja.

Tveganje pri kontroliranju. Je tveganje, da notranje kontrole v revidiranem podjetju ne bodo odkrile oz. preprečile pomembnih nepravilnosti in napak, ki lahko nastanejo.

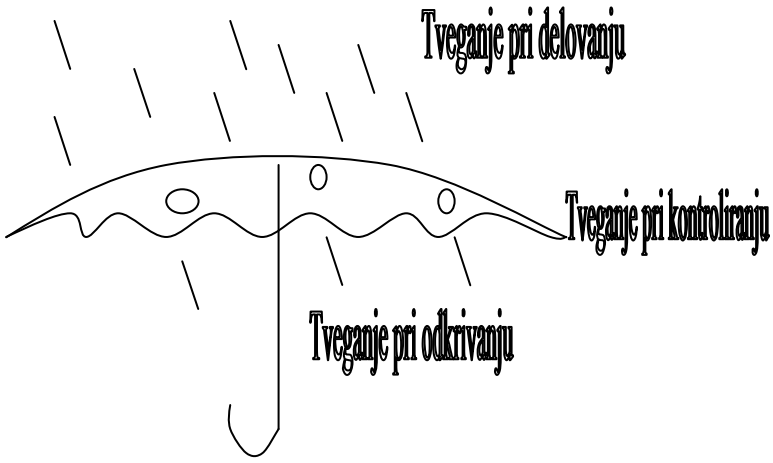
Tveganje pri odkrivanju. Je tveganje, ki ni odvisno oz. določeno s strani podjetja, ampak je to tveganje predvsem tveganje revizorja. To tveganje lahko opredelimo kot tveganje revizorja, da pri svojem delu ni opravil zadosti učinkovitih postopkov, da bi odkril pomembno napako, kljub temu da le ta obstaja v podjetju (Glosar, 2007).

Revizijsko tveganje = IR x CR x DR	(2)

Enačba (2) predstavlja povezanost opisanih tveganj, ki se pojavljajo v podjetju in revizorju pomaga pri določitvi revizijskega tveganja (Goldwasser, 2005).

Enačbo pa lahko predstavimo tudi na bolj grafični način (glej sliko 4). Dež predstavlja tveganje pri delovanju in bolj kot dežuje, večje je tveganje. Dežnik predstavlja kontrole in bolj kot je dežnik zapolnjen (brez lukenj), bolj bo zaustavil bistvene napake z naslova tveganja pri delovanju, oz. več lukenj, ki jih ima, večje tveganje pri kontroliranju bo imel. Ves dež, ki gre skozi dežnik pa predstavlja tveganje pri odkrivanju. Več kot je dežja ušlo skozi dežnik, več dela bo imel revizor, da le te odkrije in tako je tudi tveganje pri odkrivanju večje. Tako lahko vidimo povezanost vseh treh različnih tveganj med seboj. Če je tveganje pri delovanje visoko, morajo biti kontrole veliko bolje vzpostavljene, da preprečujejo bistvene napake. Slabše kot so te kontrole vzpostavljene, bolj mora biti revizor pozoren, da najde vse napake, ki so »ušle skozi dežnik« (KPMG Audit Manual, 2007).

Slika 3: Revizijsko tveganje



Vir: KPMG Audit Manual, 2007

3.1.4 Tehnike ocene tveganja

Pri oceni tveganja v podjetju se mora revizor odločiti, katera področja so bolj tvegana in katera manj, da temu primerno planira svojo revizijo. Pri svojem delu tako obišče veliko različnih podjetjih, kjer ima vsaka družba svoje specifične lastnosti, katere mora IS upoštevati pri reviziji.

Za izračun oz. oceno tveganja ima revizor IS na voljo več različnih tehnik. Tako lahko uporabi enostavne postopke, vezane na njegovo presojo, kot tudi kompleksne in že praktično znanstvene postopke, ki dejansko podajo numerično tveganje.

Eden takih sistemov je tako imenovan »scoring system«, ki daje prednost revidiranja posameznih področjih glede na oceno dejavnikov tveganja. Pri tem upošteva spremenljivke kot so tehnična zahtevnost, nivo nameščenih kontrolnih postopkov in vpliv na finančno izgubo. Tem spremenljivkam lahko revizor tudi določi težo in tako da prednost njemu bolj pomembnim spremenljivkam. Temu primerno planira revizijo IS in da prednost predhodno ocenjeno bolj tveganim področij.

Na drugi strani pa lahko revizor oceni revizijsko tveganje na podlagi neodvisne osebne presoje, na katero vpliva predhodno znanje o poslovanju podjetja, direktivah managementa, ciljih podjetja in faktorjih okolja.

Revizor se lahko odloči tudi za kombinacijo obeh metod, ki sta v praksi ponavadi tudi najbolj pogosta načina ocene revizijskega tveganja v podjetju. Revizor lahko skozi čas pri ponovnih revizijah tudi spreminja svoje tehnike ocene tveganja, pri sami oceni pa mora upoštevati nivo kompleksnosti in podrobnosti primernih za revidirano podjetje (CISA Review Manual 2006, 2006, str. 41).

3.1.5 Revizijski cilji

Revizor mora pri svojem delu razlikovati med revizijskimi cilji in cilji notranjih kontrol. Cilj kontrole določa, kako bi morala dana kontrola delovati, medtem ko se revizijski cilj nanaša na specifične cilje revizije. Torej revizija IS lahko vsebuje več revizijskih ciljev.

Revizijski cilji se pogosto osredotočajo na potrditev obstoja notranjih kontrol, ki učinkovito zmanjšujejo tveganje poslovanja. Ti cilji vključujejo:

- potrditev skladnosti z zakonom in pravnimi omejitvami;
- potrditev v zaupnost, integriteto, zanesljivost in dostopnost do podatkov.

Pomemben dejavnik pri planiranju revizije IS je določanje specifičnih ciljev revizije IS iz običajnega, generalnega cilja revizije. Na primeru lahko pojasnimo tako:
V reviziji računovodskih izkazov bi lahko bil cilj notranje kontrole zagotovitev, da so transakcije pravilno prenesene v bruto bilanco. Na drugi strani pa v reviziji informacijskih sistemov razširimo ta cilj tudi tako, da zagotovimo, da so med tem postopkom nastavljene dodatne kontrole, ki najdejo napake v transakcijah, ki so ključne za pravilen prenos podatkov v bruto bilanco.

Pravilno določanje revizijskih ciljev je ključen dejavnik pri planiranju revizije informacijskih sistemov.

Pri prvotnem pregledu informacijskih sistemov (oz. tako imenovan »od zgoraj« pregled) revizor IS identificira ključne kontrole. V naslednjem koraku se revizor IS odloči katere

kontrole bo preveril in testiral. Pri tem mora določiti tako generalne kontrole kot kontrole vezane na posamezno aplikacijo in to naredi na podlagi splošnega razumevanja in dokumentacije poslovnega procesa in aplikacij, ki poslovni proces sestavljajo. Potem lahko revizor IS določi kontrolne točke (CISA Review Manual 2006, 2006, str. 42).

3.2 Operativna faza revizije IS

Po opravljenih postopkih, potrebnih pri planiranju revizije IS, lahko revizor začne z operativnim delom, ki bo zaradi predhodno opravljenega dela precej olajšan in tudi bolj učinkovit.

3.2.1 Test kontrol in test podatkov

Revizor IS bo po prvi določitvi kontrolnih točk lahko opravil teste teh kontrol in določil, če le te delujejo kot bi morale. Rezultati teh kontrol bodo pomagali revizorju IS določiti nove teste kontrol in teste integritete podatkov.

Test kontrol pokaže, ali so kontrole v organizaciji izvajane po navodilih in v skladu s politiko managementa. Generalni cilj vsakega testa kontrol je v tem, da se revizor prepriča, da kontrola deluje z zadostno učinkovitostjo tako kot bi morala oz. tako kot je revizor pričakoval po prvotni oceni kontrole.

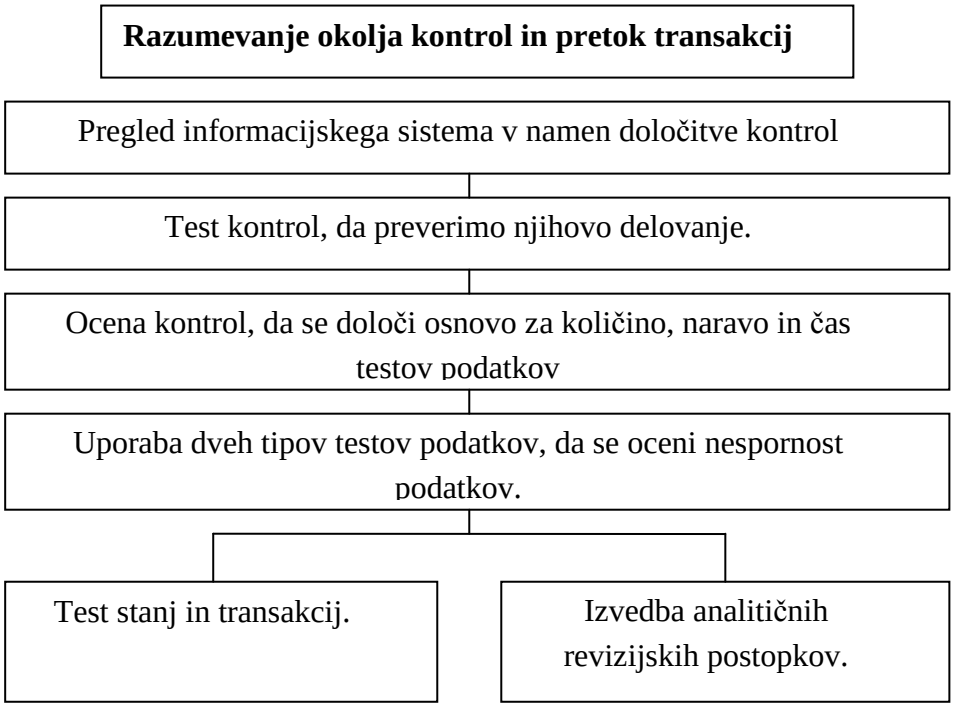
Pomembno pa je, da revizor IS razume specifične cilje testa kontrol in kontrolo, ki je testirana. Testi kontrol so lahko uporabljeni za testiranje obstoja in učinkovitosti določenega procesa, kar lahko vključuje sled dokumentov in/ali avtomatske dokaze, na primer z zagotovilom, da se lahko zgodijo samo avtorizirane spremembe pri produkcijskih programih.

Test podatkov nam zagotovi, da lahko zaupamo v nespornost in integriteto podatkov v finančnih izkazih in transakcij, ki ustvarjajo ta stanja. Revizorji IS uporabljajo teste podatkov za testiranje denarnih napak, ki direktno vplivajo na finančne izkaze. Revizor IS bi lahko naredil test podatkov za zaloge, da bi preveril pravilnost baze podatkov za zaloge na vzorcu podatkov. Slednji test bi revizorju IS bil v pomoč pri oceni točnosti celotne zaloge.

Obstaja tudi direktna korelacija med količino testov kontrol in testov podatkov. Če rezultati testov kontrol potrdijo zadovoljivo raven kakovosti, lahko revizor IS minimizira količino testov podatkov. Seveda se mora v primeru najdenih slabosti v kontrolah revizor z obsežnejšim testiranjem podatkov prepričati, da stanja kontov odražajo dejansko stanje.

Slika 4 prikazuje korelacijo med testi kontrol in testi podatkov (CISA Review Manual 2006, 2006, str. 43).

Slika 4: Razumevanje okolja kontrol in pretok transakcij



Vir: CISA Review Manual 2006, 2006, str. 4; Lastna priredba

Revizor IS je svoje delo opravil učinkovito, če uspe preprečiti nastanek napak oz. le te pravočasno odkrije. Pri tem preveri obstoj vseh notranjih kontrol z vidika tveganj in zaščite pred poslovnimi nevarnostmi ter izvede presojo tveganja in predlaga izboljšave (Brečko, 2001, str. 1-3).

3.2.2 Revizijski dokazi

Dokaz v reviziji informacijskih sistemov je vsaka informacija, ki jo pridobi revizor IS kot zagotovilo, da družba oz. revidirani podatki delujejo s skladu z revizijskimi kriteriji oz.cilji. Že v planiranju revizije IS mora revizor IS določiti, katere revizijske dokaze bo potreboval, da doseže cilje revizije. Revizijski dokazi so lahko:

- opazovanja revizorja,
- zapiski z razgovorov,
- razni dopisi,
- notranja dokumentacija,
- rezultati revizijskih testov.

Vsak dokaz lahko ocenimo na podlagi spodnjih kriterijev:

- **neodvisnost osebe, ki je izdala dokaz** (dokaz tretje osebe je več vreden kot dokaz, pridobljen znotraj revidirane družbe);

- **izobrazba osebe, ki revizorju IS podaja informacije/dokaze** (tako od družbe kot revizorja IS; če revizor IS ne razume pridobljenih informacij, ne more pravilno oceniti zadovoljivost revizijskega dokaza);
- **objektivnost dokaza** (manj kot je prisotna ocena in razumevanje dokaza, bolj objektiven je revizijski dokaz);
- **čas pridobitve dokaza** (revizor IS mora paziti na časovno dobo, ko je določena informacija (dokaz) na razpolago za primerno analizo).

Revizor IS mora v reviziji IS zbrati zadostno število zadovoljivih dokazov, da pravilno opravi in zaključi revizijo IS. Ta postopek je ključen za uspešno opravljeno revizijo IS.
Revizor IS pa ima pri svojem delu določene tehnike pridobivanja revizijskih dokazov, in sicer:

- **pregled organizacijske strukture informacijskih sistemov** (organizacijska struktura IS, ki zadovoljivo deli naloge je ključna kontrola v okolju informacijskih sistemov);
- **pregled politike in postopkov informacijskega sistema** (revizor mora oceniti primernost politike informacijskega sistema in tudi razumevanje zaposlenih te politike in postopkov;
- **pregled standardov informacijskih sistemov;**
- **pregled dokumentacije informacijskih sistemov** (revizor IS mora potrditi obstoj minimalnega nivoja dokumentacije IS in preveriti točnost le te);
- **razgovori z odgovornim osebjem** (zelo pomemben del revizije IS pri katerem se mora revizor IS zavedati, da gre pri razgovorih le za zbiranje dokazov, in ne za obtožujoče razgovore, kjer bi revizor že dajal mnenja na delovanje informacijskih sistemov);
- **opazovanje procesov in delo zaposlenih** (revizor IS mora pri tem biti čimbolj neopazen in diskretno opazovati delo zaposlenih in dokumentirati opaženo v zadostni količini, za primer predstavitve kot revizijski dokaz, na kasnejši datum).

Revizor IS mora tudi prepoznati, kdaj tradicionalna dokumentacija ni na voljo, zaradi avtomatične obdelave podatkov (neobstoj papirne dokumentacije) in pri tem upoštevati standarde organizacije. Vsa dokumentacija (tako papirna kot elektronska) mora biti skladna z določenimi standardi organizacije (CISA Review Manual 2006, 2006, str. 44).

3.2.3 Pogovori z osebjem ter vpogled v njihovo delo

Opazovanje zaposlenih pri delu pomaga revizorju IS oceniti:

- **dejanske funkcije** (ali oseba, ki je določena za neko delo, to delo dejansko tudi opravlja),
- **dejanske procese in postopke** (pri tem mora revizor opraviti »walk-through«, s katerim pridobi dokaze o morebitnih odstopanj od standardiziranih postopkov),

- **zavednost varnosti** (revizor se pri vpraša ali zaposleni prakticirajo varnostne postopke pri svojem delu in se zavedajo pomembnosti le teh),
- **odnose poročanja** (obstoj zadovoljive segregacije dela in odgovornosti).

Razgovori z osebjem, ki se ukvarja s procesiranjem informacij in managementom, bi moralo zadostovati revizorju IS za zaključek, da ima osebje zadostno znanje za opravljanje svojega dela. To je pomembno dejstvo za zagotovitev učinkovitih in zadostnih delovnih operacij (CISA Review Manual 2006, 2006, str. 45).

3.2.4 Vzorčenje

Revizor IS se mora pri preveritvi velikega števila populacije zanesti na vzorčenje zaradi prevelike časovne in stroškovne obremenitve v primeru pregleda celotne populacije. Populacija predstavlja celotno število stvari, ki morajo biti pregledane. Pri izbiri vzorca, ki gre v revizijski pregled in na kateremu se opravijo predpisani revizijski postopki, mora biti revizor IS zelo pozoren, da le ta predstavlja tak del populacije, kateri bo lahko po uspešnim pregledom zagotovil čim bolje, da je tudi celotna populacija brez bistvenih nepravilnosti (G10 Audit Sampling, 2008).

Za izbiranje vzorca pa ima revizor IS na voljo dva pristopa:

- **statistični pristop** (revizor IS objektivno izbere vzorec populacije na matematični način – npr. v vzorec vzame vsak trideseti del populacije),
- **nestatistični pristop** (revizor IS uporablja svojo presojo pri izbiri vzorca in se odloči o velikosti vzorca, metodi izbire in katere dele populacije bo vzel v pregled).

Pri obeh pristopih pa se revizor IS odloči še med dvema primarnima metodama vzorčenja, ki jih uporabljajo revizorji IS:

- vzorčenje na podlagi **lastnosti populacije**,
- vzorčenje na podlagi **spremenljivk.**

Vzorčenje na podlagi lastnosti populacije je pomembno takrat, kadar revizor IS išče potrdila o skladnosti in ustreznosti populacije (test kontrol), medtem ko je pri vzorčenju na podlagi spremenljivk aplicirano takrat, kadar revizor IS testira podatke (zanimajo ga deviacije posameznih spremenljivk od pričakovanega, znotraj izbranega vzorca) (CISA Review Manual 2006, 2006, str. 46)..

Ključni postopki pri izbiri vzorca, na katerih se bodo opravili revizijski postopki, so (CISA Review Manual 2006, 2006, str. 46):

- določitev ciljev testiranja,
- določitev testirane populacije,
- določitev metode vzorčenja
- določitev velikosti vzorca,

- izbrati vzorec,
- oceniti vzorec z revizijskega vidika.

3.2.5 Računalniško podprte revizijske tehnike

V današnjih časih prihaja do vedno večjega povpraševanja po elektronskem (brez papirnem) poslovanju. S tem tudi podjetja vedno bolj prehajajo na bolj avtomatizirane informacijske sisteme, kjer lahko izločimo veliko nepotrebne papirne dokumentacije. Temu pa se mora prilagoditi tudi revizija podjetja, še posebej revizija IS. Tako revizorji IS pri svojem delu vedno bolj uporabljajo računalniško podprte revizijske tehnike (CAAT – Computer-assisted audit techniques). Te tehnike pa morajo biti razvite tako, da so čim bolje kompatibilne z revidiranim informacijskim sistemom, oz. morajo biti primerne za uporabo podatkov iz revidiranega informacijskega sistema.

Računalniško podprte revizijske tehnike nam ponujajo naslednje prednosti:

- zmanjšano revizijsko tveganje,
- večja neodvisnost od revidiranega podjetja,
- širše in bolj konsistentno revizijsko pokritje,
- hitrejši dostop do podatkov,
- izboljšanje identificiranja izjem,
- večja fleksibilnost delovanja,
- večje možnosti določanja slabosti internih kontrol,
- boljše vzorčenje,
- manj stroškov glede na čas revizije.

Seveda pa ni vsaka računalniško podprta revizijska tehnika tako učinkovita. Revizor se mora vprašati, koliko časa bo potreboval za pridobitev elektronskih podatkov ter prirejanja le teh v obliko, na kateri bo lahko izvajal revizijske postopke in le to primerjati z že obstoječo tehniko, ki ni računalniško podprta. Prav tako pa se mora revizor IS tudi navaditi na novo, bolj elektronsko revidiranje, kot tudi upoštevati stroške povezane z implementacijo računalniško podprtih revizijskih tehnik in seveda upoštevati mora tudi čas razvoja (CISA Review Manual 2006, 2006, str. 48).

Sporne točke, ki jih mora revizor preveriti pred samo implementacijo računalniško podprtih revizijskih tehnik, so (G3 – Use of computer-assisted audit techniques – CAATs, 2008):

- enostavnost uporabe, tako za zdajšnje revizorje, kot tudi za bodoče;
- potrebe po izobraževanju in izkušnjah revizorja IS;
- zapletenost vzdrževanja;
- fleksibilnost uporabe;
- primernost CAAT v uporabi z informacijskim sistemom revidiranega podjetja;
- inštalacijske potrebe;
- učinkovitost procesiranja (čas delovanja za izvedbo nekega procesa);

- čas in trud, potreben za prenos izvirnih podatkov v računalniško podprte revizijske tehnike za analizo v primerjavi z ročnimi postopki;
- revizijsko tveganje;
- integriteta informacijskega sistema in okolja informacijske tehnologije.

V praksi se zgoraj omenjene tehnike uporabljajo vedno bolj tudi v reviziji računovodskih izkazov in sčasoma bodo postale večinski del celotne revizije podjetja, predvsem zaradi svoje učinkovitosti in preprostosti uporabe ter pridobivanja večjega zagotovila o dejanskem stanju podjetja. Največji problem je še vedno v prenosu podatkov iz revidiranega sistema v tako obliko podatkov (predvsem čas in trud pri tem potreben), katere lahko revizor analizira. V tej smeri tudi poteka največji del razvoja računalniško podprtih revizijskih tehnik.

3.3 Zaključna faza revizije IS

Ko revizor IS zaključi svoje operativno delo, se na samem sedežu stranke lahko v tej fazi osredotoči na pridobljene revizijske dokaze ter oceni informacijski sistem in poda bolj podrobne ugotovitve IT osebju revidiranega podjetja oz. upravi podjetja, v primeru bolj zahtevnih popravkov.

3.3.1 Ocena revizijskih slabosti in moči

Potem ko revizor IS zbere vse revizijske dokaze, se mora prepričati, da je bilo le teh zbranih dovolj in da so bili opravljeni postopki zadostni za izdajo pozitivnega revizijskega mnenja. Pri tem mora upoštevati vse slabosti in moči revizije in se predvsem na podlagi izkušenj odločiti, kakšno mnenje bo izdal.

Pri delu revizor IS opazi vzpostavljene kontrole, ki so lahko šibke ali močne. Pri oceni celotnega sistema kontrol pa mora upoštevati vse vzpostavljene kontrole. Tako lahko ugotovimo, da v nekaterih primerih močnejša kontrola lahko izniči slabosti šibke kontrole. Na primer, če revizor IS najde slabosti v poročilu o napakah pri transakcijah, lahko na drugi strani najde kompenzacijo za to v natančnem ročnem procesu balansiranja. Tako se mora revizor zavedati, da ob ugotoviti šibke kontrole, mora obstajati še dodatna kompenzacijska kontrola, ki močno zniža tveganje napak.

Glede vseh teh ugotovitev se revizor na podlagi svoje presoje odloča ali so ugotovljene kontrole v zadostnem številu (ali je potrebno več revizijskih postopkov) učinkovite in preprečujejo, da bi se v sistemu naredile bistveno večje napake.

Pri vseh ugotovitvah slabosti kontrol pa mora revizor paziti, komu bo sporočil ugotovljene slabosti. Kako velika je napaka v smislu materialnosti, je vprašanje na katerega revizor IS odgovori preden komunicira napako določenem nivoju managementa. Bolj ko slabost v kontroli omogoča večje napake, bolj pomembna je napaka za višji nivo managementa. Prav tako o nekaterih napakah najvišji nivo managementa ne potrebuje informacij , zato jih nima

smisla posredovati na ta nivo, ampak se jih uredi na nižjem, bolj operativnem nivoju managementa, kjer lahko napako takoj odpravijo (CISA Review Manual 2006, 2006, str. 49).

3.3.2 Predstavitev revizijskih rezultatov

Na koncu vsake revizije revizor opravi razgovor z managementom, kjer opredeli revizijska odkritja in predstavi morebitne možne izboljšave v sistemu. Pri tem mora paziti:

- da so vsa dejstva v revizijskem poročilu točna,
- da so vse predlagane rešitve in izboljšave realistične in stroškovno učinkovite oz. se v nasprotnem primeru, s pogajanjem, določi alternativne, manj stroškovno obremenjujoče rešitve,
- da se določijo datumi implementacij dogovorjenih rešitev.

Revizor IS mora večkrat predstaviti rezultate revizije različnim nivojem managementa, tako da zna svoje ugotovitve na čim boljši način prenesti naročnikom. S tem bodo rezultati revizije dobro sprejeti.

Pred poročanjem rezultatov revizije IS višjemu managementu se mora revizor IS prej posvetovati z managementom revidirane entitete. Cilj take diskusije je v tem, da se doseže sporazum o odkritjih revizije in da se določi postopke popravljanja napak. Pri nesporazumih mora revizor IS še posebej razložiti pomembnost ugotovljenih napak in tveganja, ki lahko nastajajo zaradi slabo postavljene kontrole. Včasih pa bo management revidirane entitete prosil za pomoč pri implementaciji priporočenih napak, vendar mora revizor v tem primeru dobro premisliti, če lahko daje nepristranske nasvete. V takem primeru bi bilo svetovanje bolj delo zunanjega svetovalca, ki bi opravil storitev svetovanja za revidirano entiteto in revizor IS ne bi tvegal svoje neodvisnosti v reviziji.

Pri sestavljanju revizijskega poročila mora biti revizor IS zelo pozoren na dejstva, katere ugotovitve bo omenil v svojem poročilu. Načeloma mora revizor IS sestaviti balansirano poročilo, kjer bo opisal tako negativne točke, potrebne popravkov, kot tudi podati pozitivne konstruktivne komentarje o možnih izboljšavah procesov ter kontrol in izboljšanja obstoječih kontrol. Revizijsko poročilo mora biti čim bolj objektivno, tako da so revizijske ugotovitve tudi sprejete bolj konstruktivno in v dobri nameri upoštevanja le teh (CISA Review Manual 2006, 2006, str. 51).

3.3.3 Dejanja managementa pri upoštevanju priporočil revizorja

Pri reviziji IS je zelo pomembno revizorjevo zavedanje, da je treba po revizijskem poročilu in predlaganih popravkih v predhodno določenem roku tudi preveriti, ali je management revidirane družbe dejansko upošteval priporočila. Pri zunanji reviziji IS je to manj nujno in v praksi tudi redkeje opravljeno, pa vendar, če se z revidirano stranko določi, da se potrebne spremembe v sistemu tudi preverijo, mora revizor IS to tudi upoštevati. Čas preverjanja potrebne implementacije sprememb je odvisen od kritičnosti posameznih kontrol in je stvar

presoje revizorja IS. Rezultate kontrole mora revizor IS posredovati primernem nivoju managementa. Pri zunanji reviziji IS se ponavadi od revizorja pričakuje, da predvsem preveri trenutno stanje v implementaciji sprememb v podjetju, medtem ko morajo notranji revizorji IS opraviti določene revizijske postopke, da se dodatno prepričajo, ali so spremembe dejansko tudi implementirane (CISA Review Manual 2006, 2006, str. 52).

3.3.4 Revizijska dokumentacija

Pri reviziji IS in tudi pri ostalih revizijah je zelo pomembno, da po reviziji ostaja pregledna revizijska dokumentacija, v kateri se jasno razbere potek revizije in so vidni pridobljeni revizijski dokazi, na podlagi katerih so izdelane revizijske ugotovitve. Zaradi morebitnih problemov v prihodnosti mora imeti revizor vedno pripravljeno revizijsko dokumentacijo, na podlagi katere dokazuje, da je opravil vse potrebne postopke in da bi bilo dejansko nemogoče ugotoviti morebitne prevare podjetja, ki se ugotovijo v prihodnosti. Take kasnejše ugotovitve, ki gredo v javnost, kažejo veliko nezaupnico v revizijsko družbo in v primeru, da na podlagi revizijske dokumentacije revizor ne dokaže primernosti in zadostnosti svojih postopkov, lahko revizor pričakuje tožbo delničarjev in tudi propad revizijske družbe ni izključen.

Revizijska dokumentacija načeloma vsebuje:

- revizijski plan,
- opis okolja informacijskega sistema,
- revizijske programe,
- zapiske sestankov,
- revizijske dokaze,
- ugotovitve,
- zaključke in priporočila,
- poročila na podlagi revizijskega dela,
- morebitne komentarje revizorjevih nadrejenih.

Revizijska dokumentacija bi morala biti hranjena na varnem in biti na voljo toliko časa, kolikor je zakonsko potrebno (6 let po ZRev-2 v Sloveniji) ter profesionalno in organizacijsko zadovoljivo. Revizor IS mora biti tako previden, da ugotovitve, ki jih poda na zaključku revizije, lahko potrdi z zbranimi revizijskimi dokazi (CISA Review Manual 2006, 2006, str. 53).

4 REVIZIJA INFORMACIJSKIH SISTEMOV V PODJETJU

Za boljšo predstavo dela revizorja informacijskih sistemov bom v tem poglavju predstavil praktične postopke revizorja informacijskih sistemov v podjetju. Zaradi zaupnosti podatkov imena revidiranega podjetja ne morem razkriti. Podjetje je proizvodna družba in tako za učinkovito delovanje potrebuje kvalitetni informacijski sistem. Družba uporablja

informacijski sistem SAP, vendar je sistem zamenjal prejšnjega približno pol leta pred revizijo IS, tako da je bil revizor IS tudi posebno pozoren na morebitne porodne napake v informacijskem sistemu. Revizijo je opravila revizijska družba KPMG v mesecu marcu leta 2007. Vse nadaljnje podatke, za proučitev revizije IS na dejanskem primeru podjetja, sem pridobil pri omenjeni revizijski družbi in preko pogovora z revizorjem IS, ki je vodil revizijo IS proučevanega podjetja.

Zakaj se je proučevano podjetje odločilo za revizijo informacijskih sistemov? Družba se za revizijo informacijskih sistemov ni odločila kot za samostojno revizijo, ampak je bila le ta opravljena v okviru revizije računovodskih izkazov za potrebe boljše zanesljivosti v prejete podatke iz informacijskega sistema, katere so potrebovali revizorji računovodskih izkazov za uspešno opravljanje svojih postopkov.

Revizor IS je zaradi namena revizije IS, pojasnjenega zgoraj, opravil revizijo splošnih kontrol, ki vključuje preveritev vseh področij informacijskega sistema, v primeru večjih tveganj pri določenem področju, pa bi se revizor IS bolj poglobil in opravil podrobnejši pregled tveganega področja.

Revizorjevo delo je bilo sestavljeno iz štirih večjih faz revizije:

- pogovor z vodjo informacijskega oddelka,
- pregled revizijskih dokazov,
- zaključni pogovor z vodjo informacijskega oddelka o ugotovitvah revizorja,
- priporočila revizorja.

4.1 Informacijski sistem SAP

Informacijski sistem SAP se uvršča na sam vrh ERP (Enterprise Resource Planning) sistemov, ki temeljijo na oblikovanju celotnega sistema v okviru poslovnih procesov (od naročila kupca do denarja na računu, od nabavne potrebe do plačila dobavilteju, …) in ne več v okviru poslovnih funkcij (prodaja, nabava,…), kot so oblikovani starejši informacijski sistemi, katerih problem je podvajanje podatkov in s tem tudi večje možnosti napak v podatkih.

Revizija SAP sistemov, ki se v Sloveniji pojavlja vse pogosteje, postaja ena od pomembnejših specializacij revizorjev informacijskih sistemov. Zaradi omenjene specifike in kompleksnosti sistema SAP mora revizor informacijskih sistemov poleg vsega znanja in izkušenj s področja revizij standardnih ERP sistemov poznati tudi SAP specifike in celotno strukturo ter komponente sistema, da bi lahko uspešno opravil revizijo IS.

SAP sistem je po funkcionalnosti združen v več modulov, od katerih vsak pokriva zaključen nabor funkcionalnosti za posamezno področje. Enotna podatkovna baza pa združuje vse module in tako tvori center celotnega sistema ter zagotavlja centralno kontrolo in obdelavo

vseh podatkov. SAP moduli so oblikovani v naslednja funkcionalna področja (Moškon, 2006):

- FI – računovodstvo in finance,
- CO – kontroling,
- SD – prodaja in distribucija,
- MM – nabava in skladišča,
- PP – proizvodnja,
- PM – vzdrževanje,
- PS – upravljanje projektov,
- BC – osnovne komponente in nastavitve sistema.

Ena izmed posebnosti SAP sistemov je tudi dodatni modul oz. program, ki je namenjen izključno podpori reviziji informacijskih sistemov, imenovan AIS (*Audit information system*). SAP AIS predstavlja vse naslednje točke (Hahn, 1999):

- zbirka SAP poročil (iskanja bazirana na drevo poročanja),
- orodje za revizijo SAP sistema,
- izkoristi vso SAP-ovo funkcionalnost,
- je načrtovan za namen racionalizacije revizijskega procesa,
- organizira vse aktivnosti pomembne za revizijo, pod enim dežnikom,
- cilja na izboljšanje revizije IS.

SAP AIS ni vključen v vseh SAP sistemih (odvisno od naročnika). Vseeno pa navedeni modul nima samo dobrih značilnosti kot so (Hahn, 1999):

- centralizirana revizija,
- neprekinjena revizija,
- uskupinjevanje dela notranjih in zunanjih revizorjev,
- bolj učinkovita izraba časa,
- eno drevo poročanja,
- poenostavi iskanje podatkov,
- ima potencial imeti vsa SAP poročila samo v AIS,
- prilagojen vzgled,

ampak tudi nekaj slabosti (Hahn, 1999):

- potreben pregled po vsaki SAP nadgradnji,
- vsa poročila se morajo nastaviti,
- revizor IS mora imeti znanje SAP sistema, da lahko interpretira dobljene rezultate,
- prekomerna revizija,
- pomanjkljiva revizija,
- dostop do SAP-a,
- možnost revizije samo na finančnem (FI) modulu,
- avtomatično je predvidena zanesljivost SAP sistema,

- trenutno AIS še ni dozorel.

4.2 Delo revizorja informacijskih sistemov proučevanega podjetja

V začetni fazi revizije IS se je v proučevanem primeru revizor pogovoril z vodjo informacijskega oddelka. Pri tem se je držal vnaprej določenega vprašalnika, sestavljenega po interni metodologiji revizijske družbe ter določenega na podlagi metodologije COBIT. Revizor je bil osredotočen na pet glavnih področij pregleda informacijske tehnologije:

- dostop do programov in podatkov,
- spremembe v informacijskem sistemu,
- razvoj programske opreme,
- delovanje informacijske tehnologije,
- operacije končnih uporabnikov.

Po pogovoru z vodjo informacijskega oddelka je revizor zahteval dokumentacijo, ki so potrdile izjave vodje ter opravil revizijske postopke. S tem se je prepričal glede varnosti ter učinkovitosti informacijskega sistema. Ob enem se je prepričal, da je vodja informacijskega oddelka res odgovarjal po svoji vednosti ter preveril informacijski sistem tudi s svojimi postopki. Revizor je do končnih ugotovitev prišel s prebiranjem in pregledom internih aktov podjetja, interne dokumentacije, pregledom nastavitev informacijskega sistema (povezave sistemov, mreže, programske rešitve, različna poročila, testiranja, …) ter zatem opravil razgovore z zaposlenimi in vmes še opravil vzorčenje ter pregled na samem informacijskem sistemu. V naslednjih poglavjih bom opisal, do katerih ugotovitev je revizor IS prišel pri našem primeru z že omenjenimi postopki.

4.2.1 Dostop do programov in podatkov

Dostop do programov in podatkov je eden ključnih področij uspešnega delovanja informacijskega sistema in zato ga mora revizor tudi dobro preveriti. V proučevanem primeru podjetja in revizije IS se je revizor znotraj tega področja odločil preveriti naslednje tri pomembnejše lastnosti sistema:

- uveljavljanje varnostne politike,
- logični in fizični dostop do uporabe informacijske tehnologije,
- segregacijo funkcij po delovnih mestih.

a.) Uveljavljanje varnostne politike

Revizor IS je v tem področju preverjal, če je varnost informacij upravljana tako, da se varnostne politike in smernice stalno izboljšujejo ter da se uporabniki zavedajo pomembnosti varnosti podatkov in s tem integriteto finančnih poročevalskih paketov.

Pri tem je revizor preveril, ali ima družba organizacijsko shemo, kjer je razvidno, kje je pozicionirana funkcija za varnost informacij in sistemov (neodvisno znotraj IT oddelka oz. neposredno pod upravo). Poleg tega je revizor IS preveril izobrazbo (ustreznost licenc – CISM, ocenjevalec BS 7799) in tehnično znanje zaposlenih v IT oddelku. Revizor IS je tudi pridobil interne akte za področje varovanja informacij in sistemov ter preveril ali je v teh aktih zajeto IT okolje, ki je pomembno za področje računovodskega poročanja. Pri že naštetih postopkih revizor ni ugotovil bistvenih nepravilnosti, pri zadnjem pa je ugotovil napako. In sicer, revizor je preveril še odobritev varnostne politike s strani primernega nivoja vodstva (uprava, forum za varnost,...), preveril je seznanjenost zaposlenih s to varnostno politiko ter načine seznanjanja. Opravil je intervjuje z zaposlenimi in zaključil ta del z ugotovitvijo, da varnostna politika ni bila potrjena s strani uprave, kar bi lahko resno ogrozilo varnost informacijskega sistema. Prav tako je ugotovil, da družba ni organizirala formalnega izobraževanja o varnosti informacij, vendar so zaposleni osveščeni o vzdrževanju varnosti informacijskega sistema po elektronski pošti s strani administratorjev informacijskega sistema.

b.) Logični in fizični dostop do uporabe informacijske tehnologije

Informacijska tehnologija mora biti primerno zaščitena ter dostop uporabnikov primerno kontroliran. Revizor IS je v podjetju preveril tudi, kako je logični in fizični dostop do uporabe informacijske tehnologije omejen. Do ugotovitev je revizor IS prišel s pogovori z zaposlenimi, pregledom internih aktov ter pravilnikov v podjetju, ki se nanašajo na nastavitve gesel v informacijskem sistemu in še vzorčno preveril pregledano dokumentacijo s vstopom v informacijski sistem. Pri tem je pregledal načine, kako se uporabniki informacijskega sistema identificirajo in overijo ter kakšna so določena pooblastila posameznih uporabnikov. To vključuje določitve:

- da so v sistem vključeni postopki, ki preverjajo ali se uporabniški računi redno dodajajo, spreminjajo in izbrisujejo ter s tem zmanjšujejo tveganje nepooblaščenega dostopa do pomembnih informacij znotraj informacijskega sistema;
- da obstaja učinkoviti kontrolni proces, ki sistematično preverja primernost dostopnih pravic uporabnikov ter s tem zmanjšuje tveganje nepooblaščenega dostopa do pomembnih informacij znotraj informacijskega sistema.

Znotraj področja se je revizor IS osredotočil na več posameznih del, da bi temeljito ocenil delovanje zgoraj omenjenih postopkov. Ti deli so naslednji:

- postopek overitve,
- opravljanje z gesli,
- omejitev dostopnih pravic,
- opravljanje z logičnimi dostopi,
- opravljanje s spremembami pri uporabnikih,
- neposredni dostop do podatkov,
- dodeljevanje gesel z najvišjimi prioritetami,

- fizična zaščita informacijske tehnologije,
- kršitve varnosti,
- periodično preverjanje dostopnih pravic uporabnikov,
- varnostne nastavitve.

Pri **postopku overitve** je revizor ugotovil, da uporabljajo uporabniki gesla v okviru domene in programskih rešitev. Poleg tega je ugotovil, da ima vsak uporabnik informacijskega sistema SAP svoje lastno geslo in uporabniško ime, da so ta tudi primerna ter da se ne uporabljajo skupinskega gesla. Za dodatno varnost pomembnejših podatkov je poskrbljeno tako, da imata direktorica in direktor komerciale tudi nameščene certifikate za dostop do podatkov.

Pri **opravljanju z gesli** je revizor spoznal, da lahko zahteve za spremembo pravic dajejo samo vodje posameznih služb. Nastavitve gesel pa so napisane v varnostni politiki, ki pa kot smo ugotovili v prejšnjem poglavju, še ni bila v celoti sprejeta. Prav tako nastavitve gesel v domeni in sistemu SAP niso primerne (niso v skladu z dobro prakso).

Ko je revizor preverjal sistem **omejitve dostopnih pravic** uporabnikov, je ugotovil, da so v podjetju napisali dokument, ki določa delitve dolžnosti glede na funkcijo uporabnika (listina projekta ABC)). Te pravice so bile uvedene skupaj z uvajanjem celotnega sistema SAP. Vloge in pravice posameznih uporabnikov pa je določil nosilec skupine. Poleg tega imajo uporabniki primerno ločene dostopne pravice glede na izvajanje svojih nalog. Za določanje teh pravic se uporablja obrazec »Zahteva za avtorizacijo« (glej prilogo), dostop do pomembnejših podatkov pa odobri direktorica. Sistemski administratorji na vsake 3 mesece preverjajo, kdo ima dostop do katerih direktorijev.

Opravljanje z logičnimi dostopi ter kakršnekoli **spremembe pri uporabnikih** so določene na enak način, kot sem ga opisal v prejšnjem odstavku. Gre za uporabo obrazca »Zahteva za avtorizacijo« ter primerno ločene dostopne pravice posameznih uporabnikov glede na izvajanje svojih nalog in samo potrditev direktorice pri dostopu do pomembnejših podatkov.

Neposredni dostop do podatkov (npr. z uporabo SQL stavkov) ni mogoč v sistemu.

Dodeljevanje gesel z najvišjimi prioritetami je določen z naslednjim postopkom. Nameščena so administratorska gesla. Sam dostop do najvišjih gesel imata izključno sistemski administrator in administrator za SAP. Gesla se hranijo v Excel-ovem dokumentu, ki je zaščiten z geslom, tega pa poznata le omenjena glavna administratorja.

Fizična zaščita je opredeljena na naslednji način. Naprave so nameščene v posebej za to določenem prostoru – sistemskem prostoru, ki je zaščiten s PIN kodo pri vstopu. Sam prostor ima nameščen javljalnik vode ter avtomatski sistem za gašenje, dvojna tla, dve klimi, pri katerih je rezervna dovolj močna, da prevzame primarno vlogo hlajenja.

Za beleženje **kršitev varnosti** se zapisujejo dnevniki dostopov, za karje izdelan pravilnik o dostopu zunanjih SAP svetovalcev. Dnevnike občasno pregledujejo administratorji. Vodijo se tudi zapisi VPN dostopov ter izdelujejo mesečni izpisi iz požarne pregrade Checkpoint.

Periodično preverjanje dostopnih pravic je vsake tri mesece, ko preverijo kdo ima dostop do katerih direktorijev in če so le ti dostopi v skladu z delovnimi potrebami po podatkih pri posameznem uporabniku. Predvsem pazijo, da nimajo dostopa do kritičnih finančnih transakcij uporabniki, ki le tega ne potrebujejo za uspešno delo znotraj podjetja.

Varnostne nastavitve na posameznih sistemov nadzoruje vodja informatike v podjetju.

c.) Segregacija funkcij po delovnih mestih

Revizor je tudi preveril, ali so določene skupine uporabnikov ter sam postopek za omejevanje dostopnih pravic. Skupine so določene v podjetju glede na delovno mesto, nosilci skupin (vodje enot) pa določijo pravice uporabnikov. Določeni so tudi ključni uporabniki za posamezna področja, ki tudi skrbijo za določitev pravic podrejenih na njihovih področjih. Razvijalci imajo še vedno dostop do produkcijskega okolja, vendar pa ga imajo le v prostorih družbe v času, ko so prisotni ključni uporabniki. Zahteva je bila direktoričina.

Prav tako se preverja na vsake tri mesece dostopnost posameznikov do izbranih direktorijev. Izvajanje dodatne kontrole direktorici zagotavlja ažurne podatke o vsaki spremembi dostopnih pravic uporabnikov sistema in preglednost nad dostopnimi pravicami.

4.2.2 Spremembe v informacijskem sistemu

Naslednje večje področje, ki je pomembno pri uspešnem opravljanju revizije informacijskih sistemov in prav tako za samo delovanje informacijskega sistema v skladu z interesi podjetja, je nadzor sprememb v informacijskem sistemu. Znotraj tega področja se je revizor IS v našem primeru osredotočil na tri pomembnejša območja kontrol:

- obstoj ustrezne avtorizacije, dokumentacije in testiranja sprememb;
- konfiguracijske spremembe v sistemu in aplikacijah;
- omejevanje migracije sprememb v produkcijsko okolje za sisteme in aplikacije (povezane s procesi finančnega poročanja).

a.) Obstoj ustrezne avtorizacije, dokumentacije in testiranja sprememb

Generalni cilj, ki si ga je postavil revizor IS, je predstavljala poizvedba ali obstajajo kontrole nad finančnim poročanjem, ki so bile odobrene s strani primernega nivoja management-a, ustrezno dokumentirane s strani managementa in testirane, preverjene ter odobrene pred samo implementacijo v sistem.

Revizor IS se je v podjetju osredotočil na glavno spremembo v sistemu in sicer zamenjavo starega informacijskega sistema na nov informacijski sistem SAP. Pripravili so projektni list, na katerem je zapisan celoten postopek spreminjanja programskih rešitev, znotraj projekta pa izdelan dokument »Zahteva za spremembo projekta« ter »Projektna listina«. Podjetje se je z uvajalcem sistema SAP dogovorilo o načinu posredovanja zahtev za spremembe pri uvajanju sistema SAP.

Sam postopek sprememb se začne na podlagi zahtevkov (izpolni se obrazec »Zahteva za spremembo projekta«, lahko tudi elektronsko), katere vgrajujejo v sistem razvijalci. Imajo redne sestanke projektnega sveta, kjer se predstavijo zahteve in potem še možne rešitve v primeru odobritve sprememb.

Družba pa nima izdelanega formalnega postopka za upravljanje s spremembami programskih rešitev (razen v okviru projekta SAP). Družbi je bilo predlagano, da to v kratkem času uredijo.

Zahtevi za spremembe v elektronski obliki se shranjujejo v okviru delovanja elektronske pošte. Vse zahtevke so podpisali vodja projekta, direktor projekta, včasih pa tudi direktorica.

Pri postopkih testiranja je v podjetju določeno, da so pri večjih spremembah formalno predpisani načrti testiranj in samo testiranje. Pri manjših spremembah pa se izvedejo testiranja glede na zahtevano funkcionalnost. Za preveritev, da se tovrstno testiranje dejansko izvaja, je revizor zahteval, da uporabniki potrdijo pravilnost delovanja na zahtevku za večje spremembe, pri manjših spremembah pa morali ključni uporabniki na delavnici potrditi pravilnost delovanja.

Revizor je tudi preverjal ločenost testnega okolja s produkcijskim in ugotovil, da sta v sistemu SAP okolja nameščena na dveh fizično ločenih strežnikih, delitev okolij v SAP-u pa je primerna in se deli na razvojno, testno in produkcijsko okolje.

Vsa testna dokumentacija se hrani, nujne spremembe pa nadzoruje vodja informatike.

b.) Konfiguracijske spremembe v sistemu in aplikacijah

Večje spremembe v sistemu in aplikacijah mora odobriti direktorica, medtem ko pri manjših spremembah odloča vodja IT.

c.) Omejevanje migracije sprememb v produkcijsko okolje za sisteme in aplikacije (povezane s procesi finančnega poročanja)

Pri vnašanju sistemskih sprememb v produkcijsko okolje je določen postopek, kjer prenos v produkcijo opravi glavni sistemski administrator na podlagi odobritve ključnega uporabnika. V času revizije so to še počeli razvijalci, vendar jih je nadziral glavni sistemski administrator.

4.2.3 Razvoj programske opreme

Razvoj programske opreme je področje, ki je zelo pomembno za napredek podjetja v določeno smer. Zato mora biti vsaka programska oprema tudi primerno razvita oz. pridobljena in testirana na način, da ima management postavljene kontrole, ki zagotavljajo:

- da je vsaka nova programska oprema odobrena s strani primerno visokega nivoja, tako IT managementa kot poslovodstva;
- da je prisotna zadovoljiva metodologija, ki se tudi upošteva pri razvoju in pridobivanju programske opreme uporabljene med procesi finančnega poročanja;
- da je prisotno zadostno testiranje za tako programsko opremo uporabljeno med procesi finančnega poročanja in da je le to odobreno tako s strani uporabnikov na primernem nivoju IT oddelka ter s strani poslovodstva;
- da podatki, ki so bili preneseni v novo aplikacijo ali sistem in uporabljeni pri finančnem poročanju, obdržijo svojo integriteto.

Revizor IS je v reviziji preveril, ali so postavljene zgoraj omenjene kontrole.

a.) Avtorizacija, razvoj in testiranje novih sistemov in aplikacij

Pred pomembnejšim projektom razvoja sistemov in infrastrukture mora le te odobriti direktorica družbe. Podjetje pa nima sprejete metodologije za razvoj programskih rešitev, ker nima lastnega razvoja programske opreme.

Formalni postopek o spremembi sistema v nov sistem SAP, ki se vodi še kot projekt, obstaja in je dokumentiran znotraj projektnega lista (tudi v pogodbi z zunanjim izvajalcem). Poleg tega uporabniki preverjajo in odobrijo pravilnost popravkov (vendar ne vedno pisno – lahko tudi ustno od ključnih uporabnikov pri manjših popravkih, ko skupaj z razvijalci preverijo pravilnost delovanja programov). Celoten proces pri večjih spremembah pa nadzoruje vodja informatike.

V okviru projekta SAP pa se je izvajala tudi sama konverzija podatkov, zato še niso bili izdelani posebni postopki za konverzijo iz prejšnjega sistema.

4.2.4 Operativnost informacijske tehnologije

Samo delovanje in operacije računalnikov so seveda tudi ključno področje, ki ga mora revizor IS preveriti v svojih postopkih revizije IS. V našem podjetju se je revizor odločil pokriti in preveriti tri bistvene dele operacij informacijske tehnologije:

- uvedbo varnostnih kopij in postopkov za ponovno vzpostavitev,
- postopke pri obvladovanju problemov,
- točnost, celoto in pravočasnost sistemskih del.

a.) Uvedba varnostnih kopij in postopkov za ponovno vzpostavitev

Družba izvaja varnostno arhiviranje podatkov. Kopije podatkov izdelujejo dnevno (na 2 uri – inkrementalne kopije), tedensko, mesečno ter letno s TSM. Kopije hranijo v ognjevarnem sefu v pritličju uprave (300 m stran od glavne stavbe), kar je na drugi lokaciji, vendar še vedno na območju družbe, tako da je revizor podal priporočilo o zamenjavi lokacije varnostnih kopij na bolj oddaljeno.

Družba ima izdelana navodila za primere nedelovanja sistemov, ki obsegajo tudi navodila pri prenehanju delovanja baznega strežnika (Strežnik1). Izdelan imajo tudi dokument TSM, t.j. okrevalni načrt za ponovno vzpostavitev podatkov iz trakov.

Testiranje rezervnih podatkov, ki jih hranijo na ločeni lokaciji, je bilo uspešno opravljeno, vendar ni bilo formalno dokumentirano.

b.) Postopki pri obvladovanju problemov

V družbi uporabniki nadzirajo obdelave. Delovanje in obremenjenosti sistemov pa spremlja sistemski administrator. Poleg tega v družbi uporabljajo protivirusno zaščito, ki jo redno posodabljajo. Glede vprašanja avtomatskega monitoringa podatkov, je revizor spoznal, da uporabniki nadzirajo obdelave sistemov, sistemski administrator pa redno nadzira delovanje in obremenjenosti sistemov, kar je zadovoljiv nivo kontrole nad obvladovanjem problemov. V primeru incidentov in napak v sistemu, le te sporočajo uporabniki v informacijski oddelek po telefonu ali elektronski pošti.

c.) Točnost, celota in pravočasnost sistemskih del

Revizor IS je ugotovil, da v podjetju nadzor nad obdelavami v sistemu izvajajo uporabniki. Dodaten nadzor nad sistemi in obdelavo podatkov izvaja sistemski administrator, zaposleni pa sporočajo motnje in zastoje na sistemih administratorju. V primeru, da administrator ne more rešiti problema, ga posreduje zunanjim izvajalcem.

4.2.5 Operacije končnih uporabnikov

Pri tem področju se je revizor odločil, da ne bo opravil podrobnejšega pregleda, ker podjetje ne uporablja programa Excel, kot njihovo glavno rešitev oz. orodje pri podpori poslovanja.

4.3 Ugotovitve revizorja IS

Po opravljenih revizijskih postopkih, predstavljenih v tem poglavju, je revizor podal svoje ugotovitve vodji informacijskega oddelka, ter razložil kje so možnosti izboljšanja in kje so nujne potrebe po spremembi postopkov. Ugotovitve revizorja IS, ki nakazujejo nepravilnosti v informacijskem sistemu in vzdrževanju le tega, so prikazane v tabeli 1.

Tabela 1: Ugotovitve revizorja IS

#	**Ugotovitve revizorja IS**	**Postopki ravnanja s problemi**
1.	Družba ima izdelane nekatere akte s področja varovanja informacij in sistemov, ki jih tudi uporabljajo, vendar osnutek varnostne politike še ni bil sprejet s strani uprave družbe. Družba za zaposlene ni izvedla formalnega izobraževanja o varnosti informacij, administratorji sistemov pa samo neformalno izobražujejo uporabnike, jih obveščajo z obvestili, ki jim jih pošiljajo po elektronski pošti.	Družba je bila seznanjena z ugotovitvami, pripravljen imajo tudi osnutek varnostne politike, ki čaka na potrditev uprave.
2.	Nastavitve gesel v domeni in sistemu SAP niso primerne ter niso v skladu z dobro prakso, varnostna politika pa še ni sprejeta.	Vodja IT je bil seznanjen z ugotovitvami in se nadeja, da bo varnostna politika sprejeta v kratkem času, ter da bodo nastavitve urejene primerno.
3.	Družba nima izdelanega formalnega postopka za upravljanje s spremembami programskih rešitev (razen znotraj projektnega lista). Družba se je z uvajalcem sistema SAP dogovorila za način posredovanja zahtev za spremembe pri uvajanju sistema SAP.	Družba je bila seznanjena z ugotovitvijo. Spremembe v SAP se vodijo po dogovorjenem (z revizorjem) načinu izvajanja.
4.	Družba hrani kopijo podatkov na drugi lokaciji (vendar je ta lokacija od glavne stavbe oddaljena le 300 metrov)	Družba je bila seznanjena z ugotovitvijo ter razmišljajo o drugi nadomestni lokaciji.
5.	Družba hrani rezervno kopijo podatkov v drugi stavbi (stavba uprave) na območju družbe.	Družba je bila seznanjena z ugotovitvijo. Razmišljajo o drugi nadomestni lokaciji.

Vir: Interni podatki revizijske družbe KPMG, 2007

Glede ne zgornje ugotovitve revizorja IS je revidirana družba upoštevala vsa priporočila in bo tudi poskušala vse pomanjkljivosti odpraviti v najkrajšem času. To bo revizor IS preveril z naslednjo revizijo IS oz. nekaj mesecev po opravljeni prvotni reviziji IS.

Revizor IS je dejansko pripomogel k uspešnosti razvoja in varnosti informacijskega sistema in potrjujem zastavljeno tezo, da je revizija IS potrebna za izboljšanje kvalitete in

učinkovitosti informacijskega sistema ter tudi same varnosti podatkov, katero informacijski sistem zagotavlja. Ugotavljam tudi, da je revizor IS opravljal svoje delo v skladu z mednarodnimi smernicami ISACA in se dejansko prepričal o zadovoljivem delovanju vseh bistvenih elementov informacijskega sistema. Revizija IS je potrdila, da informacijski sistem v proučevanem podjetju deluje v skladu s pričakovanji in služi namenom, kot so zbiranje, urejanje, obdelovanje, hranjenje podatkov ter njihovo preoblikovanje v informacije. Kljub temu pa je vseeno ostalo nekaj področij, predvsem pri hranjenju in varnosti podatkov, ki jih mora podjetje popraviti.

Na podlagi raziskovanja standardov, zakonov in glavne metodologije, uporabljenih pri reviziji IS, ter na podlagi proučevanega praktičnega primera revizije IS v Sloveniji, bi revizijo IS priporočal tudi podjetjem, ki k njej niso zakonsko obvezani, vendar pa so vedno bolj odvisni od svojega informacijskega sistema. Slednji lahko v praksi pomeni glavno razliko med uspešnim podjetjem in podjetjem, ki zaradi svoje kompleksnosti poslovanja enostavno ne more konkurirati brez učinkovitega informacijskega sistema. (Interni podatki revizijske družbe KPMG, 2007)

5 RAZGOVOR Z REVIZORJEM INFORMACIJSKIH SISTEMOV

Za boljše razumevanje revizije IS v Sloveniji sem uspel preživeti kratek čas s preizkušenim revizorjem IS, ki opravlja svoje delo pri revizijski družbi KPMG. Na podlagi razgovora z revizorjem, ki ima tudi mednarodno licenco CISA, sem lahko potrdil nekatere predpostavke v zvezi s temo diplomske naloge.

Revizija IS v Sloveniji je v vzponu zaradi vedno večjega zanašanja podjetij na kvaliteten in učinkovit informacijski sistem. Podjetja v Sloveniji v vedno večji meri potrebujejo kvalitetno revizijo IS, da lahko svoj informacijski sistem primerno razvijajo z upoštevanjem napotkov revizorja IS.

Revizor zaznava problem uspešne revizije IS v nesodelovanju zaposlenih pri stranki, kar je povod neznanja in nevednosti o sami reviziji. Zaposleni se ne zavedajo, da so ključni razlogi za revizijo informacijskih sistemov v izboljšanju poslovanja in izboljšanju informacijskega sistema in ne samo v kontroli in preverjanju zaposlenih samih. Zaradi tega mora revizor dalj časa in predvsem večkrat razlagati smisel svojega dela, da da zaključka revizije pridobi zahtevane odgovore, na podlagi katerih lahko ustvari pravo revizijsko mnenje.

Prav tako bi izpostavil razvoj znanja revizorja informacijskih sistemov, ki mora biti stalno na tekočem z vedno novimi informacijskimi sistemi in se mora zato tudi stalno izobraževati. V Sloveniji je trenutno samo nekaj čez 50 revizorjev informacijskih sistemov z licenco CISA (*Certified Information System Auditor*), kar predstavlja morebitni problem ob visoki rasti revizij informacijskih sistemov. Dejansko bi moralo pri reviziji večjega informacijskega sistema sodelovati več revizorjev IS, vsak specializiran za svoje področje, da bi lahko na

koncu revizije večjega sistema prišli do boljših in predvsem bolj obsežnih zaključkov in napotkov upravi k izboljšanju svojega informacijskega sistema.

SKLEP

Revizija informacijskih sistemov je v Sloveniji vsako leto bolj prisotna in tudi bolj potrebna glede na nenehno naraščajoče potrebe večjih podjetij po večji učinkovitosti in s tem bolj kompleksnih in učinkovitejših informacijskih sistemih. V diplomski nalogi sem predstavil smisel revizije informacijskih sistemov, komu je namenjena in zakaj je le ta sploh potrebna. Nekoliko sem razjasnil zakone in standarde, ki jih uporabljajo revizorji informacijskih sistemov in delno predstavil dejanski primer.

Sodobne organizacije se z vsakim dnem bolj zanašajo na svoj delujoč informacijski sistem, ki olajšuje vse delovne naloge in omogoča uspešnejše poslovanje posamezne organizacije. Informacijski sistemi z vzpostavljenimi notranjimi kontrolami omogočajo poslovanje z manjšim številom napak in botrujejo redkejšim prekinitvam rednega poslovanja, zato lahko poteka bolj tekoče in tudi uspešnejše.

Vendar pa vzpostavitev zapletenega in predvsem obsežnega informacijskega sistema predstavlja določene možnosti napak, ki jih je treba številčno omejiti. Pri tem pomaga revizija IS. Z diplomsko nalogo sem razložil in pojasnil določena področja revizije IS in pojasnil delo revizorja IS na podlagi mednarodnih smernic, mednarodno priznane metodologije revizije IS Cobit in na podlagi zakonskih obveznosti v Sloveniji.

Revizija IS je veja revizije in pogosto, predvsem v Sloveniji, del bolj obsežne revizije, revizije računovodskih izkazov. Kljub temu je potreba po njej vsako leto večja zaradi napredka in vedno večjega zanašanja sodobne družbe na informacijsko tehnologijo.

Med proučevanjem dela revizorja IS v izbranem podjetju sem ugotovil, da je bila revizija IS opravljena v skladu z mednarodnimi smernicami organizacije ISACA in po metodologiji Cobit. Prav tako lahko zaključim, da je revizor IS proučevanega podjetja dejansko uspel najti nekatere nepravilnosti v informacijski tehnologiji in obravnavi le te, ter predstavil rezultate, ki bodo vodili k izboljšavi varnosti ter učinkovitosti informacijskega sistema.

V bolj razvitih državah je revizija IS bolj samostojna kot v Sloveniji, zaradi večjih, bolj obsežnih, učinkovitejših informacijskih sistemov, ki potrebujejo večje zagotovilo integritete, vzdrževane s strani internih specialistov informacijskega oddelka posameznih organizacij. Revizorji IS pri tem pomagajo s pomočjo svojega znanja o specifični informacijski tehnologiji in lahko neodvisno ter objektivno ocenijo delovanje posameznih informacijskih sistemov. S tem bistveno pripomorejo k uspešnem delovanju le teh in tudi odkrijejo morebitne prevare, ki se dogajajo ob zlorabi informacijske tehnologije.

V Sloveniji se potreba po reviziji IS in revizorjih IS povečuje, saj revizorji računovodskih izkazov in notranji revizorji s svojim znanjem ne morejo zagotoviti, da informacijski sistem deluje v skladu s pričakovanji. Trenutno je le peščica pooblaščenih revizorjev IS, ki uspešno izvajajo revizijo IS v slovenskih podjetjih, vendar se bo glede na potrebe število moralo povečati. S tem bomo lahko nadgrajevali uspešen in tekoč razvoj informacijske tehnologije v slovenskih organizacijah.

LITERATURA IN VIRI

1. Botha, H. & Boon, J.A. (2002, 19. marec). The Information Audit: Principles and Guidelines. *Libri vol. 53*. Najdeno 20. julija 2007 na spletnem naslovu http://www.librijournal.org/pdf/2003-1pp23-38.pdf.
2. Brečko, V. (2001). *Sistem notranjih kontrol. Gradivo za izobraževanje za pridobitev strokovnega naziva preizkušeni notranji revizor*. Ljubljana: Slovenski inštitut za revizijo.
3. *COBIT 4.1. (2007).* [*organizacije ITGI (IT Governance Institute)*]. Najdeno 10. septembra 2007 na spletnem naslovu www.isaca.org/Template_cfm?Section=Downloads10&Template=/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742
4. *G10 Audit Sampling (2008).* [*organizacije ISACA*]. Najdeno 13. julija 2008 na spletnem naslovu http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=43069
5. *G3 – Use of computer-assisted audit techniques – CAATs (2008).* [*organizacije ISACA*]. Najdeno 16. julija 2008 na spletnem naslovu http://www.isaca.org/AMTemplate.cfm?Section=Standards,_Guidelines,_Procedures_for_IS_Auditing&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39261.
6. Gaudin, S. (2006, 13. december). Ex-Ubs systems admin sentenced to 97 months in jail. *InformationWeek*. Najdeno 27. aprila 2008 na spletnem naslovu http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=FXHUFQWXLN3VYQSNDLPCKHSCJUNN2JVN?articleID=196603888&_requestid=88797.
7. *Glosar*. [*Računsko sodišče republike Slovenije*]. Najdeno 31. julija 2007 na spletnem naslovu http://www.rs-rs.si/rsrs/rsrs.nsf/Glosar?OpenForm&start=131.
8. Goldwasser, L.D. (2005, november). The past and future of reasonable assurance. *The CPA Journal*. Najdeno 19. julija 2008 na spletnem naslovu http://www.nysscpa.org/cpajournal/2005/1105/special_issue/essentials/p28.htm.
9. Hahn, J. & Juergens, M. (1999, 27. april). SAP: Business Process Controls and AIS. *ISACA Spring Conference*, Najdeno 2. maja 2008 na spletnem naslovu http://www.auditnet.org/docs/erpsapbusproc.pdf.
10. Hulme, G.V.. (2002, 23. december). Guarding Against Threats From Within. *InformationWeek.* Najdeno 1. maja 2008 na spletnem naslovu http://www.informationweek.com/news/software/showArticle.jhtml;jsessionid=FXHUFQWXLN3VYQSNDLPCKHSCJUNN2JVN?articleID=6504584&_requestid=86530).
11. *Informacijska tehnologija – Kodeks varovanja informacij, BS ISO/IEC 27002:2005*, (2005). UK: British Standards Institution
12. KPMG Audit manual, 2007. Ljubljana: KPMG Slovenija d.o.o.
13. *Interni podatki revizijske družbe KPMG*, 2007.

14. CISA Review manual 2006 (2006). ZDA: ISACA
15. *islovar*. [*organizacije Slovensko društvo Informatika*] Najdeno 1. maja 2008 na spletnem naslovu http://www.islovar.org/forumi/sporocila.asp?id=388&idk=5&debatestran=10.
16. Klitgaard, R. (1998, marec). International cooperation against corruption. *Finance & Development*. Najdeno 13. julija 2008 na spletnem naslovu http://www.worldbank.org/fandd/english/pdfs/0398/080398.pdf.
17. Kodeks poklicne etike revizorja IS. (2000). Ljubljana: Slovenski inštitut za revizijo.
18. Moškon, S. (2006). Revizija SAP – kaj mora revizor informacijskih sistemov vedeti o SAP sistemu. Najdeno 1. maja 2008 na spletnem naslovu www.osir.si/Db/osir/content/ppt/Predavanje_ISACA_2006_V2.ppt.
19. Mugerle, F. (1995). Revizija računovodstva in revizija informacijskih sistemov. *Zbornik posvetovanja: Dnevi slovenske informatike 1995*. Ljubljana: Slovensko društvo informatika.
20. *Osnovni pojmi revizije informacijskih sistemov*. [*organizacije Slovenski inštitut za revizijo*]. Najdeno 17. junija 2007 na spletnem naslovu http://www.si-revizija.si/isaca/revizija_IS.php.
21. Panian, Ž. (2001). *Kontrola i revizija informacijskih sustava*. Zagreb: Sinergija-nakladništvo Zagreb.
22. *Pomen revizije informacijskih sistemov pri upravljanju poslovnih sistemov*. [*organizacije Slovenski inštitut za revizijo*]. Najdeno 13. junija 2007 na spletnem naslovu http://www.si-revizija.si/isaca/revizija_IS.php.
23. Potočnik, B. (2003, 18. junij). Sodišče odločilo v prid Škulju. *24ur.com*. Najdeno 1. maja 2008 na spletnem naslovu http://24ur.com/novice/slovenija/sodisce-odlocilo-v-prid-skulju.html.
24. *Predstavitev virusov, črvov in trojanskih konjev*. [*podjetja Microsoft d.d.*]. Najdeno 2. maja 2008 na spletnem naslovu http://www.microsoft.com/slovenija/doma/varnost/virusi/predstavitev_virusov.mspx.
25. *Revizija IS [podjetja Audens d.o.o.*]. Najdeno 10. 10. 2007 na spletnem naslovu http://audens.si/index.php?option=com_content&task=view&id=24&Itemid=41;.
26. *Revizor informacijskih sistemov – priložnost za kariero?* [*organizacije Slovenski inštitut za revizijo*]. Najdeno 15. junija 2007 na spletnem naslovu http://www.si-revizija.si/isaca/revizija_IS.php.
27. Statut slovenskega inštituta za revizijo. (2001). Uradni list RS. (Št. 70/2001, 31. avgust 2001).
28. *Varnostna politika*. [*podjetja Astec d.o.o.*]. Najdeno 11. julija 2008 na spletnem naslovu http://www.astec.si/slo/index.php?option=com_content&task=view&id=27&Itemid=62.
29. Zakon o revidiranju (ZREv-2). (2008). Uradni list RS. (Št. 65/2008, 30. junij 2008).
30. Carlin, A. & Gallegos, F. (2007, julij). IT Audit: A critical business proces. *Computer*. Najdeno 24. avgusta 2008 na spletnem naslovu http://www.computer.org/portal/site/computer/menuitem.5d61c1d591162e4b0ef1bd108

bcd45f3/index.jsp?&pName=computer_level1_article&TheCat=1040&path=computer/homepage/July07&file=itsys.xml&xsl=article.xsl&;jsessionid=Ltc1hnvMppd1kD2DnS2bTgc3TfbkyntJ4QmZMkC7rG6mLc0RwsRv!1195711095.

PRILOGE

Priloga 1 Razgovor s pooblaščenim revizorjem IS

- Koliko časa delate kot revizor informacijskih sistemov?

5 let

- Ali potrebujete kakšno dodatno izobraževanje (poleg univerzitetne diplome) za opravljanje dela revizorja informacijskih sistemov?

Izobraževanje v okviru Slovenskega inštituta za revizijo – Preizkušeni revizor informacijskih sistemov. Potrebuješ tudi dodatna izobraževanja od poznavanja različnih sistemov – HW, SW, programiranja, konfiguracij sistemov, mrež, poznavanje področja organizacije informatike v podjetjih, poznavanje poslovnih procesov, itd.

- Ali je potrebno redno vzdrževati licenco CISA?

Licenco CISA je potrebno redno vzdrževati z dodatnim izobraževanjem, vsako leto je potrebno opraviti najmanj 20 ur strokovnega izobraževanja in 120 ur vsaka 3 leta. Dodatno je treba plačevati še članarino v ISACA 35 $ na leto.

- Katere probleme najpogosteje opažate pri revidiranju informacijskih sistemov?

Nepoznavanje pomena in ciljev revizije v podjetju, ki se revidira. Nepoznavanje ciljev vodi k nezaupanju in posledično se stanje prikazuje drugačno, kot je v resnici. Zaradi nepoznavanja in nezaupanja pa se podaljša čas, ki ga revizor potrebuje, da pride do pravih informacij. Nepoznavanje internih aktov, ki urejajo področje informatike.

- Kako pridobivate stranke, ki potrebujejo revizijo informacijskih sistemov?

Stranke večinoma kontaktirajo nas, za nas izvedo od sorodnih podjetij ali preteklih stikov. Včasih se javimo tudi na kakšen javni razpis. Marketinga ne izvajamo.

- Ali mislite, da je panoga revizije informacijskih sistemov v vzponu oz. ali so potrebe po njej zvišujejo glede na trenutne tržne razmere?

Menim, da je panoga v vzponu, potrebe se povečujejo. To dokazuje tudi naš plan, ki je zapolnjen do vsaj pol leta vnaprej in moramo stranke zato odklanjati. Poleg tega je še veliko

področij revizije informacijskih sistemov, katera bi se lahko izvajala v Sloveniji, vendar zaradi pomanjkanja kvalitetnega kadra to ni mogoče.

- Kaj menite o kvaliteti revizije informacijskih sistemov v Sloveniji? Ali je v svetu revizija informacijskih sistemov bolj cenjena oz. tudi bolje izvedena v primerjavi s slovenskimi razmerami?

Moja ocena je, da v Sloveniji ni veliko kvalitetnih revizorjev informacijskih sistemov. Do tako širokega spektra znanj, kot ga revizor informacijskih sistemov potrebuje za kvalitetno opravljanje dela, je težko priti. Zato je revizija informacijskih sistemov lahko uspešna le, če posamezen revizor pregleduje del, ki ga obvlada ali pa če se združi več revizorjev.

V svetu se v okviru revizije informacijskih sistemov ponuja več storitev, pri nas podjetja večinoma še niso na takšnem nivoju poznavanja in zavedanja poslovanja, da bi lahko uporabili revizijo informacijskih sistemov za izboljšanje nivoja poslovanja ter tudi zmanjšali tveganja pri poslovanju.
Glede nivoja storitve se moram navezati na prvo vprašanje. Za svoje storitve lahko rečem, da smo jih primerjali s tujimi in smo prišli do zaključka, da jih opravljamo zelo kvalitetno. Vendar je to veliko lažje v veliki družbi, kjer se znanje tudi svetovno pretaka in lahko hitreje prideš do informacij, ki jih potrebuješ. Zato imajo posamezni revizorji lahko tudi težave pri revidiranju.

- Koliko je revizorjev informacijskih sistemov (CISA licenca) v Sloveniji?

V Sloveniji je nekaj čez 50 preizkušenih revizorjev informacijskih sistemov s CISA licenco.

- Kaj mislite, da bi lahko v Sloveniji naredili v smeri boljše zaščite informacijskih sistemov v zvezi z zaposlenimi v podjetju?

Več izobraževanja in treningov dvigovanja zavedanja o zaščiti IS. Začeti bi morali pri vodstvu in širiti zavedanje in znanje s pomočjo zgleda tudi navzdol.

- Ali vam je vaše delo všeč oz. ali vidite perspektivo in razvoj vašega znanja kot revizor informacijskih sistemov?

Delo mi je všeč, je zelo pestro in raznoliko. Velikokrat je potrebno razmišljati o različnih možnostih in rešitvah pri reviziji npr. programskih rešitev ali pa tudi celotnih sistemov. Glede znanja obstaja še zelo veliko stvari, ki se jih lahko naučiš kot revizor, od novih sistemov, programskih rešitev, novih naprav, itd.

- Ali strankam tudi svetujete glede boljše zaščite in kvalitete informacijskih sistemov ali samo ocenite trenutno stanje v podjetju?

V okviru revizije skušamo podjetjem s priporočili pokazati kako naj se različnim tveganjem izognejo ali jih zmanjšajo. Končno odločitev in način, kako bodo podjetja tveganja zmanjšala ali se jim izognila, ostaja na strani podjetja.
Pri svetovanju pa poskušamo ponuditi najboljšo možno rešitev glede na tveganja in možnosti v podjetju.