
UNIVERZITET SINGIDUNUM



Master akademski program Poslovna ekonomija

MASTER RAD

**INTERNA REVIZIJA SA POSVEBNIM OSVRTOM NA INTERNU
REVIZIJU INFORMACIONIH SISTEMA I TEHNOLOGIJA**

Mentor: Prof. dr Kosana Vićentijević

Student: Sofija Vukadinov

Br. indeksa 400128/2011

Beograd, 2012.

SADRŽAJ

1. Metodologija naučnog rada	5
2. Uvod	7
3. Interna revizija	8
3.1. Nastanak, pojam i funkcija interne revizije	8
3.2. Interna revizija i menadžment	10
3.3. Razgraničenje interne kontrole i interne revizije	12
3.3.1. Komponente i nedostaci interne kontrole	14
3.3.2. Odnos interne revizije prema sistemu interne kontrole u banci	18
3.4. Karakteristike internih revizora u Srbiji	20
4. Revizija informacionih tehnologija	24
4.1. Upravljanje informacionim tehnologijama	25
4.2. Interna revizija u oblasti informacionih tehnologija	28
4.3. Interne kontrole sa aspekta revizije infomacionih tehnologija	30
5. Pojam i svrha etičkog kodeksa i Međunarodnih standarda	33
5.1. Etička načela, principi i opšte prihvaćena pravila ponašanja	34
5.1.1. Etički kodeks za revizore informacionih sistema	37
5.2. Međunarodni standardi za profesionalnu praksu interne revizije	38
5.2.1. Pregled glavnih i karakterističnih standarda za internu reviziju	39
5.3. Najbitniji okviri i smernice za obavljanje IT revizije	45
5.4. Standardi ISO	47
5.4.1. ISO 9001 - Sistem menadžmenta za kvalitet	47

5.4.2. ISO 27001 - Sistem menadžmenta za bezbednost informacija	50
5.4.3. ISO 27002 - Kodeks prakse za upravljanje sigurnošću informacija	53
5.5. Sarbanes – Oxley zakon i COSO okvir	54
5.6. ITIL – informaciona biblioteka	56
5.7. COBIT – Kontrolni ciljevi za informacione i srodne tehnologije	58
6. Revizijski rizik i materijalnost	61
6.1. Mere rizika	63
6.2. Upravljanje rizikom	66
6.3. Upravljanje finansijskim rizikom	66
6.4. Uloga interne revizije u upravljanju rizicima	68
6.5. ERM pristup u upravljanju rizikom	70
6.6. Upravljanje rizicima informacionih sistema i tehnologija	73
7. Lažno finansijsko izveštavanje – istraživanje za 2012. godinu	76
7.1. Počinioci prevara i njihove karakteristike	79
7.2. Faktori na koje treba obratiti pažnju pri otkrivanju počinioca prevare	83
7.3. Trenutno stanje transparentnosti finansijskih izveštaja u Srbiji	86
Zaključak	88
Literatura	90

Tabele i grafikoni:

Tabela 1. - Starosna struktura ovlašćenih internih revizora u Republici Srbiji	20
Tabela 2. - Struktura ovlašćenih internih revizora u Srbiji prema fakultetskom obrazovanju	21
Tabela 3. - Pregled profesionalnih zvanja stečenih u inostranstvu, nostrifikovanih od strane Komore ovlašćenih revizora Srbije	22
Tabela 4. - Geografska struktura ovlašćenih internih revizora registrovanih u Republici Srbiji	23
Tabela 5. - Broj prevara i prosečan gubitak za 2012. po osnovu sektora počinioca	76
Tabela 6. - Broj prevara i prosečan gubitak za 2012. po osnovu odeljenja počinioca	79
Tabela 7. - Prosečan gubitak prouzrokovan prevareom po osnovu godišta počinioca	80
Tabela 8. - Broj slučajeva prevare i prosečni prouzrokovani gubici za 2012. godinu na osnovu nivoa obrazovanja počinioca	81
Dijagram 1. - Broj prevara u procentima prema poziciji počinioca u preduzeću	78
Dijagram 2. - Procenat slučajeva prevare po osnovu godišta počinioca	80
Dijagram 3. - Broj slučajeva prevare po osnovu pola počinioca	81
Dijagram 4. - Najčešće karakteristike počinioca prevare izražene u procentima	82
Dijagram 5. - Procenat učestalosti metoda za detekciju prevara	83

1. METODOLOGIJA NAUČNOG RADA

Predmet istraživanja ovog rada jesu karakteristike interne revizije, njen nastanak i razvoj, a akcenat je bačen na implementaciju revizije informacionih tehnologija. Analizirani su i okviri za profesionalnu upotrebu kako interne revizije tako i revizije informacionih tehnologija. Takođe, analizom je obuhvaćen odnos domaćeg sektora poput ministarstava i javnih preduzeća prema ovoj poslovnoj delatnosti koja je pretežno orijentisana na menadžment. Važan segment istraživanja je upravo i odnos menadžmenta prema internoj reviziji. Neshvaćenost i otpor prema ovoj profesiji nažalost su prisutni, a saveti i preporuke internih revizora potcenjeni. Ovakvo nezainteresovano ponašanje menadžmenta javlja se kao rezultat nerazvijenosti finansijskog tržišta i značajnog učešća preduzeća u društvenoj svojini. U radu je analiziran i problem netransparentnosti finansijskih izveštaja, značaj poštovanja propisanih zakona i principa, kao i značaj kontrole u borbi za transparentnost. U praksi važi stav da ono što nije kontrolisano, vremenom će se sigurno pogoršati. Posao revizora je da se uveri da finansijski izveštaji ne sadrže materijalno značajne pogrešne iskaze nastale usled kriminalne radnje ili greške tj. da su finansijski izveštaji transparentni i da daju istinit i tačan prikaz finansijskog stanja.

Naučni cilj ovog rada je da se prikažu karakteristike revizije informacionih tehnologija kroz upoznavanje sa najvažnijim profesionalnim standardima i smernicama.

Društveni cilj istraživanja je pokušaj da se približi značaj revizorskog rada, posebno sve veći značaj IT revizije, kroz pružanje adekvatnih informacija i znanja, u prepoznavanju prevara, otkrivanju prevaranata i drugih nezakonitih radnji, kao i merama zaštite u reviziji.

Generalna hipoteza:

Interna revizija čiji je zadatak da utvrdi da li su finansijske i operativne informacije pouzdane i precizne, rizici preduzeća identifikovani i minimizirani, eksterne regulative i interne politike i procedure ispoštovane, izvori korišćeni uspešno i ekonomski, a ciljevi organizacije postignuti je ekonomska disciplina koja je pretežno orijentisana na menadžment i koja svojom objektivnom procenom i nezavisnom kontrolom menadžmentu pruža podršku u vođenju uspešne poslovne organizacije.

Posebna hipoteza:

1. Prilično spor razvoj interne revizije i borba za profesionalni integritet i nezavisnost, rezultat su, kako ambijenta koji odiše netransparentnošću i otporom pojedinaca kojima ovo stanje odgovara, tako i neobaveštenosti, odnosno različitim, a često i pogrešnim shvatanjima funkcije ove profesije.
2. U današnje vreme kada su kompjuteri i informacione tehnologije postale sastavni deo života, pa tako i poslovanja, njihove stalne, sve dinamičnije promene i napredovanje, zavisnost velikih kompanija o informacionim sistemima i tehnologijama uslovile su potrebu za kontrolom i revizijom tih tehnologija. Nadgledanje i revizija informacionih sistema i tehnologija neophodni su za uspešno poslovanje i sprovođenje poslovnih aktivnosti preduzeća.
3. Pridržavanjem i promovisanjem etičkih načela, posebno principa nezavisnosti i političke neutralnosti, interna revizija će u isto vreme podstaći poverenje javnosti u svoj profesionalni i moralni integritet.

4. U praksi važi stav da dobra interna revizija mora otkriti prevaru.¹ Pa ipak, interni revizori često oklevaju u ispunjenju ove svoje obaveze, zbog određene vrste straha da će to naškoditi njihovom konsultantskom imidžu. Analizom poslovnih aktivnosti, procenom rizika, detaljnom i opsežnom kontrolom, interni revizori donose zaključke na osnovu kojih menadžmentu pružaju savete koji doprinose uspešnom poslovanju preduzeća. Iako je interna revizija orijentisana na menadžment, a njen osnovni zadatak je da mu pruži podršku i pomoć, otpor menadžmenta u Srbiji prema ovoj profesiji, je očigledan. S' jedne strane taj otpor se javlja kao posledica nerazumevanja razlike između interne kontrole i interne revizije i uopšte, funkcije interne revizije, a sa druge strane možemo primetiti da se javlja i kao posledica netransparentnog ambijenta i sputavanja od strane onih kojima to stanje odgovara. Brzi rezultati nisu mogući, ali podizanjem svesti pripadnika podređenih korupciji i promovisanjem etičkih načela, profesija će podstaći poverenje javnosti, a samim tim i svoj razvoj.

Metode i tehnike istraživanja:

Osnovne metode: U radu je pretežno korišćena metoda analize tj. rastavljanje predmeta istraživanja na njegove sastavne delove. Od osnovnih metoda naučnog rada korišćene su još i metoda apstrakcije, metoda indukcije koja predstavlja početnu fazu svakog mišljenja, metoda generalizacije, metoda specijalizacije gde se posebni i pojedinačni delovi saznaju posredstvom celine, posebno u obliku klasifikacije, gde se jedna klasa razvrstava po određenom kriterijumu i deduktivni metod koji možemo reći predstavlja oblik zaključivanja gde se iz opštih zakonskih stavova, sudova, premisa, logičkim putem izvode novi, posebni i pojedinačni zaključci.²

Opšte naučne metode: U radu su takođe donošeni zaključci na osnovu društvenog i naučnog iskustva mnogih subjekata u raznim vremenima i prostorima, dakle korišćena je hipotetičko- deduktivna metoda, kao i aksiomska metoda koja je neizbežno povezana sa hipotetičko- deduktivnom u procesima postavljanja aksioma. Od opšte naučnih metoda korišćene su i komparativna metoda koja je sastavni deo svakog mišljenja i bez čijeg istraživanja identičnosti, sličnosti i razlika pojava i procesa nije moguće oformiti bilo kakav sud, pojam, stav, uopšte zaključak³, a takođe i statistička metoda kada su posmatrane karakteristike ovlašćenih internih revizora kao identifikovane statističke mase.

Metode prikupljanja podataka:

U okviru metoda prikupljanja podataka, korišćene su sledeće metode: analiza naučne dokumentacije i studija slučaja koja je orijentisana na raznovrsnost izvora i podataka, kao i veliku prodornost i elastičnost obuhvata, a njen predmet istraživanja su celine realnosti koje se u ukupnoj realnosti mogu identifikovati i definisati kao celovite posebnosti u vremenu i prostoru.

1 Prof. dr Milovan Stanišić, "Revizija", Univerzitet Singidunum, Beograd 2009. str.66

2 Prof. dr Milan I. Miljević, "Metodologija naučnog rada", Univerzitet u Istočnom Sarajevu, Pale 2007. str.129

3 Prof. dr Milan I. Miljević, "Metodologija naučnog rada", Univerzitet u Istočnom Sarajevu, Pale 2007. str.188

2. UVOD

Nestabilni uslovi poslovanja, rast i razvoj preduzeća i samog finansijskog tržišta, poslovni rizici sa kojima se preduzeće suočava, uslovili su potrebu za formiranjem jedinice interne revizije u preduzeću. U praksi važi stav da poslovne aktivnosti koje nisu kontrolisane, vremenom će se sigurno pogoršati.⁴ Interna revizija je nezavisna ekonomska disciplina, nastala unutar organizacije i njen osnovni cilj je da svojom kontrolom, procenjivanjem, savetima, analizom i preporukama pomogne upravi u vođenju uspešne organizacije. Posao interne revizije obuhvata ocenjivanje ostvarenosti poslovnih ciljeva postavljenih od strane menadžmenta, ocenjivanje sistema interne kontrole i upravljanja, ispitivanje poslovnih transakcija, analiziranje rizika sa kojima se preduzeće suočava i sve to sa ciljem da pomogne menadžmentu u donošenju adekvatnih poslovnih odluka i u unapređivanju poslovanja preduzeća.

U toku obavljanja poslova revizije, interni revizori moraju očuvati svoju objektivnost i nezavisnost i u tom cilju treba da izbegavaju sve slučajeve koji mogu dovesti do sukoba interesa, sve odnose koji mogu uključiti rizik od korupcije, a svoju poziciju ne smeju koristiti u privatne svrhe. Prema Međunarodnim standardima profesionalne prakse Instituta internih revizora, interna revizija treba da bude organizovana samostalno, van poslovnih funkcija, a aktivnosti i odgovornosti menadžmenta i internih revizora moraju biti jasno definisane, radi obezbeđenja pune nezavisnosti prilikom izvršenja poslovnih aktivnosti. Interni revizori se moraju pridržavati Zakona o računovodstvu i reviziji, Okvira profesionalne prakse, Međunarodnih standarda i Kodeksa etike pri obavljanju svoje profesionalne dužnosti, to jest poslova revizije.

Veliku ulogu u poslovima interne revizije igra procena rizika. Interna revizija se pored ispitivanja knjigovodstvenih podataka, proveravanja usklađenosti sa zakonom, otkrivanja kriminalnih radnji i grešaka, sve više okreće procesu upravljanja rizicima, kako bi pomogla menadžmentu u vođenju uspešne poslovne organizacije. Dobro razvijen plan i program revizije usmerava se na ključne rizike i to ne samo one na nivou organizacije, već i u okviru pojedinačnih odeljenja, organizacionih jedinica ili procesa. Delokrug rada interne revizije obuhvata i „ljudske rizike“, a od revizora se očekuje da izveštava i o slabostima ljudskog faktora i da izvrši objektivnu, poštenu i nezavisnu procenu stanja internih kontrola uključujući i onu nad ljudima. Interni revizori pomažu menadžmentu da analizira rizike i uspostavlja kontrole što je ključna stavka za pozitivno to jest uspešno poslovanje preduzeća.

Iako je interna revizija poslovna disciplina orijentisana na menadžment, često smo svedoci nezainteresovanog ponašanja i otpora menadžmenta prema internoj reviziji. Ovaj stav menadžmenta proizilazi iz nedovoljne razvijenosti finansijskih tržišta i korporativnog upravljanja, značajnog učešća preduzeća u društvenoj svojini⁵, ali isto tako i zbog nerazumevanja ove profesije, posebno kroz razgraničavanje interne kontrole i interne revizije. U nastavku rada objašnjene su osnovne razlike između interne kontrole i interne revizije (takozvanog prethodnog i naknadnog nadzora), značaj ove ekonomske discipline, kao i uloga interne revizije u upravljanju rizicima preduzeća.

4 Prof. dr Milovan Stanišić, „Revizija“, Univerzitet Singidunum, Beograd 2009. str 66

5 <http://edukacija.ekof.bg.ac.rs/tema-meseca.php?temaId=3>, Prof. dr Kata Škarić Jovanović, Pouzdano finansijsko izveštavanje, maj 2009. , preuzeto dana 12.07.2012.

3. INTERNA REVIZIJA

3.1. Nastanak, pojam i funkcija interne revizije

Uspešnost poslovnosti nekog preduzeća prezentira se uglavnom kroz finansijske izveštaje i finansijski položaj preduzeća, što ima veliki značaj za korisnike tih izveštaja. Donošenje odlučujućih odluka o alokaciji resursa, investicionom ulaganju u budućnosti, prvenstveno zavisi baš od verodostojnosti tih izveštaja, njihovej tačnosti i preciznosti. Značaj i uloga tih izveštaja zadnjih decenija dobija na značaju.

Porast važnosti i uloga preciznog i realnog finansijskog izveštavanja zavisi od brojnih faktora a među njima se po snazi uticaja izdvajaju: razdvajanje vlasničke i upravljačke funkcije u korporativnim poslovnim entitetima, razvoj finansijskih tržišta i rast društvene odgovornosti preduzeća. Faktori kao takvi su svakako doveli ne samo do značajnog povećanja broja korisnika finansijskih izveštaja već su promenili i zahteve koje ti korisnici postavljaju pred finansijsko izveštavanje.

Zaštita interesa investitora je primarni cilj finansijskog izveštavanja, dok je zaštita interesa poverilaca, koja je decenijama determinisala formu i sadržinu finansijskih izveštaja izgubila prednost. Zadovoljavanje informacionih potreba investitora i pojava novih oblika ulaganja, ovde je pre svega reč o finansijskim instrumentima, doveli su do preispitivanja važećih pravila za priznavanje i vredovanje elemenata finansijskih izveštaja što je postalo primarno polje delovanja, kako profesionalnih računovodstvenih tela tako i regulatornih tela merodavnih za finansijsko izveštavanje.

Cilj svake revizije je formiranje revizijskog mišljenja o finansijskim izveštajima. S' obzirom da je često mišljenje revizora jedini deo revizije koji korisnici vide, izveštaj predstavlja proizvod revizora. Po standardima revizije zahteva se da se svi finansijski izveštaji revidiraju.

Osnovni zahtevi za izdavanje izveštaja revizije izvode se iz četiri opšte prihvaćena standarda revizije koji se odnose na izveštavanje. Poslednji standard zahteva izražavanje mišljenja o svim finansijskim izveštajima ili poseban izveštaj o tome da sveobuhvatno mišljenje nije moguće i o razlozima zbog kojih nije moguće izraziti mišljenje. Takođe se zahteva i jasan iskaz revizora o prirodi ispitivanja i stepenu u kome revizor ograničava svoju odgovornost.

Profesija priznaje i prihvata potrebu za jednoobraznošću u izveštavanju da bi se izbegla konfuzija. Da finansijski izveštaji nisu jednoobrazni i formalizovani svaki izveštaj bi izazivao dodatni napor i znanje korisnika da protumače njegovu sadržinu. Isto se odnosi i na revizijske izveštaje. Stručnim standardima se definišu i nabrajaju vrste izveštaja revizije koje bi trebalo uključiti u finansijske izveštaje. Tekst izveštaja revizije je relativno jednoobrazan iako različiti izveštaji revizije odgovaraju različitim situacijama.

Poslednji korak u celom procesu revizije predstavlja upravo izveštaj revizije. Izveštaj nezavisnog revizora predstavlja rezultat revizije i to je završni deo postupka prikupljanja i procene dovoljnih merodavnih dokaza u vezi sa realnošću i objektivnošću prikazivanja izjava uprave u finansijskim izveštajima.

Revizija je veoma stara finansijska disciplina, čiji su začeci vidljivi čak 3500 godina pre nove ere. Mesopotamija, Egipat, Kina, Persija, Grčka, svi ovi stari narodi verovali su u kontrolu finansija. U Starom Rimu se pojavljuje takozvano „slušanje računa“ ,odnosno funkcioneri usmeno međusobno

porede svoje zapise, kako ne bi počinili prevaru. Odatle i izraz „audit“ koji potiče od latinske reči „auditus“ što znači slušanje.

Revizija, koju mi danas poznajemo, nastaje tokom industrijske revolucije u Engleskoj, a tokom devetnaestog veka zajedno sa Britanskim investicijama stiže u Ameriku. Osnivanjem Instituta internih revizora u SAD-u, 1941. godine, interna revizija počinje da napreduje, a interni revizori se izjednačavaju sa eksternim po obuhvatu rada, ali nažalost još uvek ne i po statusu.

Interni revizori imaju širu i dublju funkciju od eksternih. Kroz nezavisno procenjivanje i merenje oni menadžere snabdevaju informacijama koje su im neophodne za efektivno i efikasno vođenje preduzeća. Interni revizori takođe moraju vršiti kontrolu svih finansijskih aktivnosti menadžmenta, moraju biti upoznati sa svim gubicima preduzeća, bilo da oni proizilaze iz neprofitabilne proizvodnje, inženjeringa ili čak iz finansijskih pronevera. Dakle, oni brinu o svim razlozima štete i prevare bez obzira na njihov izvor, uticaj i veličinu, za razliku od eksternih revizora koji se fokusiraju na greške i gubitke koji direktno utiču na tačnost finansijskih izveštaja.

Interna revizija je nezavisna ekonomska disciplina, nastala unutar organizacije i njen osnovni cilj je da svojom kontrolom, procenjivanjem, savetima, analizom i preporukama pomogne upravi u vođenju uspešne organizacije. Delokrug rada interne revizije obuhvata:

- Pregled celokupnosti finansijskih i operativnih informacija i sredstva koja su korišćena za identifikaciju, merenje, razvrstavanje kao i dostavljanje tih informacija;
- Pregled sistema koji su stvoreni da obezbede saglasnost sa takvom politikom, planovima, procedurama, zakonima i propisima koji bi mogli da imaju značajan uticaj na operacije i izveštaje i da utvrde da li je organizacija u saglasnosti;
- Pregled sredstava koja čine aktivu i ukoliko je moguće, da potvrde postojanje takve aktive;
- Procenu ekonomije i efikasnosti korišćenja resursa i kapitala;
- Pregled operacija ili programa kako bi ustanovili da li su rezultati dosledni osnovnim ciljevima i da li su izvršeni kako je i planirano.

3.2. Interna revizija i menadžment

Menadžment je proces planiranja, organizovanja, vođenja i kontrole ljudskih, fizičkih, finansijskih i informacionih resursa organizacije na efektivan i efikasan način, a menadžeri su osobe koje poseduju adekvatno znanje, sposobnosti i veštine, koje koordiniraju rad radnika kako bi ostvarili osmišljene ciljeve i zadatke organizacije.

Posao menadžera obuhvata:

Funkciju planiranja:

- Utvrđivanje vizije, misije, ciljeva organizacije na osnovu analize i predviđanja eksternih i internih faktora okruženja (situacione analize);
- Formulisanje strategije radi ostvarenja ciljeva i organizacione misije;
- Razvijanje planova u funkcije implementacije strategije (projekti, budžeti, programi, politike, pravila, procedure).

Funkciju organizovanja:

- Utvrđivanje i podela posla;
- Departmentalizacija (grupisanje poslova);
- Delegiranje autoriteta;
- Uspostavljanje lanca komandovanja i raspona (obima) menadžmenta (kontrole).

Funkciju vođenja:

- Motivacija;
- Liderstvo;
- Komuniciranje;
- Ponašanje i koordiniranje zaposlenih.

Funkciju kontrole:

- Utvrđivanje standarda;
- Merenje aktuelnih rezultata;
- Kompariranje rezultata sa standardima;
- Preuzimanje korektivnih akcija.⁶

⁶ Prof. dr Branislav Mašić, „Menadžment: principi, koncepti i procesi“, Univerzitet Singidunum, Beograd 2010. str. 36

Sredinom osamdesetih godina u našem privrednom prostoru počinje proces reformi sa ciljem da se na tržišnim osnovama izgradi privreda. Ovim reformama privrednog sistema dolazi i do promena u normativnoj osnovi finansijskog izveštavanja. Očekivalo se da će ove promene usloviti i promenu odnosa menadžmenta prema finansijskom izveštavanju, međutim veliki broj uprava preduzeća ne prihvata finansijske izveštaje kao izvore informacija ključne za procenu, unapređenje i uspešno poslovanje preduzeća, već kao “neugodnu obavezu” nametnutu od strane države.

Kada se pojavila, interna revizija je predstavljala dopunu nezavisnoj profesiji računovodstva, a vremenom je evoluirala do posebne discipline orijentisane na menadžment. Menadžment nije mogao bez podrške da se izbori sa sve kompleksnijim zadacima i poslovima, da na pravi način kontroliše sve poslovne aktivnosti i promene.

U praksi važi stav da aktivnosti koje nisu nadgledane, to jest ono što nije kontrolisano, vremenom će se sigurno pogoršati. Tu se javlja interna revizija, kao podrška menadžmentu, koja će odgovoriti na njegove potrebe i vršiti kontrolu poslovnih aktivnosti u skladu sa propisanim standardima i načelima. Nažalost nisu svi menadžeri svesni razlike između interne kontrole i interne revizije, kao ni pomoći koju im interni revizori nude, a to je pomoć u:

- Nadgledanju aktivnosti koje top menadžment ne može sam da nadgleda;
- Identifikovanje i umanjeње rizika;
- Validnost izveštaja starijem menadžmentu;
- Zaštita top menadžmenta u tehničkim oblastima sa kojima oni nisu upoznati;
- Obezbeđivanje informacija za proces odlučivanja;
- Kontrola kako za budućnost tako i za prošlost;
- Pomoćna linija menadžmenta za upravljanje tako što ukazuju na kršenje procedura i principa menadžmenta.⁷

Nezainteresovano ponašanje menadžmenta i njihov otpor prema računovodstvu i reviziji posledica je ne samo njihovog nerazumevanja ove profesije već i nerazvijenosti finansijskih tržišta i značajnog učešća preduzeća u društvenoj svojini. Međutim, ubrzani proces privatizacije, pojačani naponi na razvoju finansijskih tržišta i želja da se privuku strani investitori istakli u prvi plan pouzdanost, razumljivost i uporedivost finansijskih izveštaja naših preduzeća i banaka zbog čega je neophodno da menadžment pristupi unaprednju svojih računovodstvenih znanja ili bar da postane svestan vrste i dalekosežnosti uticaja donetih poslovnih odluka na sliku preduzeća prezentiranu u njegovim finansijskim izveštajima. Ovaj zadatak menadžment može ostvariti kroz unapređenje saradnje sa profesionalnim računovođama i postavljanjem odnosa menadžer - računovođa na paritetnu osnovu.⁸

7 Prof. dr Milovan Stanišić, “Revizija”, Univerzitet Singidunum, Beograd 2009. str.67

8 <http://edukacija.ekof.bg.ac.rs/tema-meseca.php?temaId=3>, Prof. dr Kata Škarić Jovanović, Pouzdano finansijsko izveštavanje, maj 2009. preuzeto dana 12.07.2012.

Interna revizija kao veoma mlada disciplina u Srbiji, susreće se sa problemima razgraničavanja pojmova i poslovnih aktivnosti. Upravo zbog nerazumevanja, to jest neshvaćenosti ove profesije, ona nailazi na snažan otpor od strane menadžmenta i uprave preduzeća. Ipak, čini se da se ta situacija polako menja. Prvo veliko preduzeće koje je shvatilo značaj i ulogu interne revizije u poslovanju i organizaciji poslovnih aktivnosti je Elektroprivreda Srbije. Kao rezultat lošeg iskustva sa Kolubarom, od prvog januara ove godine tendere EPS-a kontroliše čak 32 interna revizora, dok je u prošlosti to bio posao samo četiri lica.⁹

Igor Sholters, predsednik Državne revizorske institucije Slovenije, smatra da bi za Srbiju bilo dobro da država zakonski obaveže bar preduzeća u kojima je većinski vlasnik da uvedu internu reviziju, jer će tako biti otkriveni mnogi propusti i mnoge nepravilnosti će biti sprečene. On je ukazao na značaj objektivne i stručne interne revizije za poslodavstvo, jer prihvatanjem saveta i sugestija internih revizora, rad poslodavstva biva dosta poboljšán i olakšan.

3.3. Razgraničenje interne revizije i interne kontole

Interna kontrola je proces ustanovljen i sproveden od strane upravnog odbora preduzeća, uprave i drugog osoblja, a cilj mu je da obezbedi razumno uverenje vezano za postizanje ciljeva u sledećim kategorijama:

- efikasnost i uspešnost poslovanja;
- pouzdanost finansijskog izveštavanja;
- saglasnost sa postojećim zakonima i propisima;
- zaštita imovine od neovlašćenog prisvajanja ili otuđenja.

Interna kontrola, kao i interna revizija prevashodno je orijentisana na menadžment. Njen značaj leži u tome što ona menadžmentu pruža uverenje da će politike poslovanja biti ispoštovane, a poslovni ciljevi ostvareni (Napr. profitabilnost, sprečavanje nastanka gubitaka, sprečavanje pronevera i zloupotreba, sprovođenje budžeta..). Internu kontrolu mogu obavljati i nestručni ljudi, dok se interna revizija kao veoma profesionalan i zahtevan posao obavlja isključivo od strane stručnjaka.

Postoje dve osnovne vrste internih kontrola u preduzeću:

- 1) Administrativne – odnose se na funkcionisanje poslovnog sistema u neračunovodstvenim područjima (Poštovanje zakonskih propisa, statuta, pravilnika, poslovanje po odlukama organa upravljanja, područje prava zaposlenih..);
- 2) Računovodstvene – odnose se na zaštitu sredstava i pružanje uverenja da su finansijski izveštaji i računovodstveni sistemi pouzdani.

⁹ EPS ne želi više afera, Blic, Nedelja, 12.11.2011.

Glavne kontrole mogu se podeliti na različite kategorije, a jedan od načina je prema po profesoru Pickett-u:

- Usmeravajuće kontrole – kojima se obezbeđuje jasan pravac i smer aktivnosti za postizanje definisanih ciljeva;
- Preventivne kontrole – kojima se obezbeđuje funkcionisanje sistema;
- Detekcione kontrole – kojima se obezbeđuje otkrivanje grešaka u transakcijama koje nisu sprečene preventivnim kontrolama;
- Korektivne kontrole – kojima se obezbeđuje ispravnost akcija u vezi identifikovanih problema;
- Meke kontrole – kojima se obezbeđuje podsticanje svesti o odgovornosti.¹⁰

Kontrola predstavlja proces koji počinje postavljanjem standarda, a završava se pregledom stepena uspešne primene. Kontrole u praksi treba da budu “pametne” (SMART kontrole), a to znači da moraju biti:

- **Specific** – specifične;
- **Measurable** – merljive;
- **Achievable** – ostvarljive;
- **Result oriented** – orijentisane ka rezultatima;
- **Timely** – pravovremene.¹¹

Svoju funkciju nadgledanja u preduzeću menadžment lakše obavlja uz pomoć interne kontrole i interne revizije. U praksi važi stav da aktivnosti koje nisu nadgledane, to jest ono što nije kontrolisano, vremenom će se sigurno pogoršati. Tu se javlja interna revizija, kao podrška menadžmentu, koja će odgovoriti na njegove potrebe i vršiti kontrolu poslovnih aktivnosti u skladu sa propisanim standardima i načelima. Nažalost nisu svi menadžeri svesni razlike između interne kontrole i interne revizije, kao ni pomoći koju im interni revizori nude, a to je pomoć u:

- Nadgledanju aktivnosti koje top menadžment ne može sam da nadgleda;
- Identifikovanje i umanjenje rizika;
- Validnost izveštaja starijem menadžmentu;

10 http://uirs.rs/index.php?option=com_content&view=article&id=64:-8-9-2009&catid=32:2008-08-25-19-18-10&Itemid=40 , Bilten broj 8, (Informativno-teoretski list “Udruženja internih revizora Srbije”) , Maj 2009. preuzeto dana 13.07.2012.

11 http://uirs.rs/index.php?option=com_content&view=article&id=64:-8-9-2009&catid=32:2008-08-25-19-18-10&Itemid=40 , Bilten broj 8, (Informativno-teoretski list “Udruženja internih revizora Srbije”) , Maj 2009. preuzeto dana 13.07.2012.

- Zaštita top menadžmenta u tehničkim oblastima sa kojima oni nisu upoznati;
- Obezbeđivanje informacija za proces odlučivanja;
- Kontrola kako za budućnost tako i za prošlost;
- Pomoćna linija menadžmenta za upravljanje tako što ukazuju na kršenje procedura i principa menadžmenta.¹²

Možemo reći da je interna kontrola "prethodni nadzor", odnosno da je interna revizija "naknadni nadzor" funkcionisanja sastava internih kontrola i ostvarenja poslovanja u skladu sa usvojenim ciljevima. Kako interne kontrole nisu uvek toliko efektivne i efikasne, potrebno je vršiti kontinuiranu kontrolu nad njihovim funkcionisanjem. Između ostalog upravo je zadatak interne revizije da istražuje, ispituje i ocenjuje sastav internih kontrola i njihovu efikasnost u delovanju svakog pojedinačnog poslovnog sastava, da izveštava o nalazima i predlaže rešenja menadžmentu.

3.3.1. Komponente i nedostaci interne kontrole

Elementi odnosno komponente koje čine internu kontrolu su:

- Kontrolno okruženje;
- Procena rizika;
- Kontrolne aktivnosti;
- Informacija i komunikacija;
- Nadgledanje i praćenje.¹³

1) Kontrolno okruženje

Osnovu svakog poslovnog sistema čine brojni faktori kao što su ljudski resursi, proizvodi, tehnologije, ali svakako najbitniji faktor je čovek sa svojim radnim navikama, odnosima u poslovanju, shvatanjem i odnosom prema internoj kontroli. Odnos menadžmenta prema internoj kontroli uslovljava i odnos zaposlenih prema ovom sistemu i zato je veoma bitno da menadžment bude posvećen sprovođenju zakonitosti i sistema vrednosti, što je preduslov za ispravno poslovanje i finansijsko izveštavanje. Menadžment treba da obezbedi funkcionisanje sistema kontrole u preduzeću na nivou koji će revizora uveriti da preduslovi za ispravno poslovanje postoje.

Revizor treba da dođe do saznanja o kontrolnom okruženju koja su dovoljna da može da proceni ponašanje, stepen motivacije, aktivnosti direktora i uprave vezanih za sprovođenje internih kontrola i

¹² Prof. dr Milovan Stanišić, "Revizija", Univerzitet Singidunum, Beograd 2009. str 67

¹³ Prof. dr Milovan Stanišić, "Revizija", Univerzitet Singidunum, Beograd 2009. str 53

njihov značaj u preduzeću.¹⁴

Faktori na koje revizor treba da obrati pažnju pri proceni kontrolnog okruženja su :

- *Privrženost integritetu i etičkim vrednostima*

- Da bi interna kontrola dobro funkcionisala potrebno je da se na svim nivoima poštuju i primenjuju etičke i moralne norme i da se odnosi u preduzeću zasnivaju na njima.

- *Privrženost kompetentnosti i kvalitetu*

- Za svaki posao uprava treba da utvrdi nivoe stručnosti, potrebno znanje, iskustvo i inteligenciju i da to poštuje prilikom angažovanja i imenovanja zaposlenih.

- *Nezavisno funkcionisanje upravnog odbora*

- Upravni odbor koji pored ostalog kontroliše i nadgleda rad menadžmenta treba svojim primerom da obezbedi zaposlenima uverenje da su maksimalno okrenuti podizanju efikasnosti, efektivnosti, ekonomičnosti i da stvaraju adekvatni kontrolni ambijent. Odnos menadžmenta prema radu i obavezama, saradnicima i poslovnim aktivnostima, a posebno prema finansijskom izveštavanju, informacionom sistemu i osoblju angažovanom na ovim poslovima, takođe uslovljava i odnos zaposlenih prema ovim poslovnim aktivnostima.

- *Odgovarajuća organizaciona kultura*

- Organizaciona struktura kao osnova za planiranje, izvođenje i kontrolu poslovnih aktivnosti mora biti jasno definisana i konzistentno razvijena, mora postojati jasna raspodela ovlašćenja, jasno razgraničenje odgovornosti, jasno određeni nivoi odlučivanja i izveštavanja, kao i jasna pravila ponašanja.

- *Odgovarajuća podela ovlašćenja i odgovornosti*

- Između upravnog odbora i menadžmenta moraju postojati jasna razgraničenja prava i obaveza, kao i raspodela kontrolnih funkcija.

- *Odgovarajuća kadrovska i poslovna politika*

- Veoma je bitno da kadrovi budu kompetentni, pouzdani, poštteni i profesionalni i da uspešnim obavljanjem svojih dužnosti i posla olakšaju posao interne kontrole, odnosno da učine njene nedostatke zanemarljivim.

¹⁴ http://www.icisa.cag.gov.in/Background%20Material/RISK%20ASSt%20AND%20INTNL%20CONTROL%20ISA_400.pdf, ISA 400 – Risk Assessments and internal control, str 359, preuzeto dana 13.07.2012.

2) Procena rizika

Menadžment procenu rizika sprovodi u cilju razvoja i usavršavanja sistema interne kontrole, dok revizor procenu obavlja kako bi sagledao kontrolni rizik u sklopu rizika revizijskog angažmana. Menadžment ne mora biti zainteresovan za pravi izveštaj i može prihvatiti netačnu procenu rizika kako bi obezbedio slabo delovanje kontrole, da bi izvršio prevaru ili druge poslovne aktivnosti u svoju korist.

3) Kontrolne aktivnosti

Kontrolne aktivnosti obezbeđuju informacije neophodne za kontrolu rizika vezanih za postizanje ciljeva preduzeća. Postoje dve grupe kontrolnih aktivnosti: nalog šta treba kontrolisati i uputstvo kako treba sprovoditi kontrolu.

4) Informacija i komunikacija

Preduslov uspešne i savremene organizacije poslovnog sistema je dobar sistem informacija i dobra komunikacija između elemenata poslovnog sistema.¹⁵

Menadžment je dužan da zaposlenima pošalje jasnu poruku da se kontrolne aktivnosti moraju obavljati na odgovarajući način i da odstupanje od pravila nije dozvoljeno. Takođe, svi zaposleni moraju znati svoje mesto i ulogu u poslovnom sistemu, informacionom sistemu i sistemu interne kontrole.

U uspešnom preduzeću komunikacija ide u svim smerovima:

- *Komunikacija na dole* – kada se organizacione odluke donose na vrhu tj. na višim organizacionim nivoima ka dole odnosno ka zaposlenima koji će sprovesti tu odluku.
- *Komunikacija na gore* – kreće se od zaposlenih ka menadžmentu, gde zaposleni menadžere snabdevaju informacijama o tekućim problemima, aktuelnim trendovima, trenutnim rezultatima, šansama za unapređenje poslovnog procesa...
- *Horizontalna (lateralna) komunikacija* – se obavlja između zaposlenih na istom organizacionom nivou, u cilju deljenja informacija i koordiniranja zadataka, kao i lakšeg rešavanja složenih i teških problema.
- *Dijagonalna komunikacija* – koristi se kada je potrebno zameniti ostale vidove komunikacija i takođe u dinamičnom poslovnom okruženju kada je potrebno efikasno i brzo komuniciranje i razmena informacija. Ova komunikacija se odvija između zaposlenih i odseka koji nisu na istom organizacionom nivou.¹⁶

U adekvatnom sistemu informacija mora biti jasno definisano:

- Ko su izvori informacija;

¹⁵ Prof. dr Milovan Stanišić, "Revizija", Univerzitet Singidunum, Beograd 2009. str 58

¹⁶ Prof. dr Branislav Mašić, "Menadžment", Univerzitet Singidunum, Beograd 2010. str 325,326

- Ko generiše podatke i informacije;
- U kojoj se formi informacije prezentuju;
- U kojim rokovima se dostavljaju korisnicima;
- Ko su korisnici i koje informacije koriste.¹⁷

5) Nadgledanje

Funkcija nadgledanja je višestruka, a najbitnije funkcije su da se na vreme zapaze propusti u funkcionisanju sistema interne kontrole i da se utvrdi da li je sistem interne kontrole prilagodljiv zahtevima vremena, s' obzirom da poslovni sistem vremenom raste i menja se.

Termin nedostatak se odnosi na propuste u nekim aspektima interne kontrole i ima potencijal da negativno utiče na sposobnost subjekta da ostvari postavljene ciljeve.

Nedostaci interne kontrole podrazumevaju da ona ne obavlja funkciju koja joj je dodeljena, kao i slabosti u načinu na koji se primenjuje. Oni mogu biti prozrokovani aktivnostima unutar preduzeća, ali mogu nastati i delovanjem spoljnih subjekata koji su značajni za poslovanje preduzeća. Ovi nedostaci mogu prouzrokovati značajne gubitke u preduzeću.

Ozbiljni i značajni nedostaci se prijavljuju najvišim organima upravljanja ili potpunom upravnom odboru, dok se manje značajnim nedostacima bave niži nivoi upravljanja u preduzeću. Kada organizacija utvrdi da nedostaci postoje, menadžment mora da proceni uticaj nedostataka na delotvornost sistema interne kontrole. Obaveza organizacije je takođe i da izvrši identifikaciju i procenu nedostataka. Nije svaki nedostatak interne kontrole rezultat neefektivnosti sistema interne kontrole. Kao prvo, druge kontrole moraju biti prisutne i moraju da funkcionišu tako da svih pet komponenti interne kontrole takođe budu prisutne. Kada se nedostatak uoči procenjivač uzima u obzir uticaj kontrole na sve komponente. Procena ozbiljnosti nedostataka ili kombinacije nedostataka radi utvrđivanja potencijalnog uticaja na sistem interne kontrole zahteva detaljno razmatranje.¹⁸

Kako bi se nedostaci interne kontrole umanjili, bitno je da zaposleni odnosno ljudi koji ih sprovedu budu dovoljno obučeni i da adekvatno ispunjavaju svoje obaveze.

Interne kontrole nad finansijskim izveštavanjem

Interna kontrola nad finansijskim izveštavanjem ima svoje specifičnosti.

U ovom slučaju se koriste 3 nivoa nedostataka: nedostatak, značajni nedostatak i materijalna slabost.

Materijalna slabost podrazumeva da u internoj kontroli postoje nedostaci i definiše se kao stanje u kome postoji nedostatak ili kombinacija nedostataka u internim kontrolama, zbog čega postoji mogućnost da materijalno značajni pogrešni iskazi u finansijskim izveštajima neće biti sprečeni, otkriveni ili ispravljeni na vreme.

¹⁷ Prof. dr Milovan Stanišić, "Revizija", Univerzitet Singidunum, Beograd 2009. str 58

¹⁸ www.coso.org/ic-integratedframework-summary.htm, Internal control–Integrated Framework, Decembar 2011. str 16,17

Utvrđivanje postojanja materijalne slabosti zahteva rasuđivanje koje uzima u obzir sledeće:

- 1) Najverovatnije postoje materijalno značajni pogrešni iskazi koji neće biti sprečeni, otkriveni i ispravljani na vreme;
- 2) Razmeru potencijalnih ili postojećih materijalno značajnih pogrešnih iskaza u odnosu na finansijske izveštaje.¹⁹

Značajan nedostatak je nedostatak ili kombinacija nedostataka, koji je manje ozbiljan od materijalne slabosti, ali je ipak dovoljno važan da skrene pažnju upravnog odbora. Kada se višestruki značajni nedostaci zajedno razmatraju, može se otkriti da materijalna slabost postoji.

3.3.2. Odnos interne revizije prema sistemu interne kontrole u banci

Prve organizacione jedinice za internu reviziju počele su da se formiraju u SAD oko 1864. godine. Osnivanjem prvih Instituta internih revizora 1941. godine u SAD i 1958. godine u Nemačkoj, interna revizija dobija poseban razvojni trend kako u preduzećima tako i u bankama.

U Srbiji funkcija interne revizije prvi put je uspostavljena odlukom Narodne banke Jugoslavije 2002. godine i to Odlukom o osnovnim principima organizacije rada interne revizije banke i druge finansijske organizacije, sa ciljem da unapredi superviziju u bankama, donošenje smernica koje podstiču dobre prakse i da bi se povećala sigurnost rada banke. Ova odluka je bila na snazi sve do oktobra 2006. godine, kada se donošenjem Zakona o bankama utvrđuje funkcija interne revizije kao posebnog organizacionog dela banke. Ovim zakonom je utvrđeno da je banka obavezna da funkciju interne revizije obavlja i organizuje u skladu sa Međunarodnim revizijskim standardima, dok je interni revizor dužan da posao obavlja efikasno, kontinuirano, redovno i kvalitetno.²⁰

Interna revizija je nezavisna funkcija organizovana unutar banke u cilju ocene sistema kontrole i kvaliteta poslovanja u celini ili pojedinih delova.

Interni revizori su zaposleni u banci, a njihov posao obuhvata i pomoć menadžmentu u donošenju odluka i poboljšanju uspešnosti poslovanja banke kroz izradu izveštaja koji obezbeđuju analize, ocene, preporuke i savete. Dužnost internog revizora je da svojim ispitivanjem i analizom sagleda sve rizike vezane za ekonomski i finansijski položaj banke, bonitet sredstava, dinamiku likvidnosti i realnost bilansiranja.

Aktivnosti interne revizije u okviru banke:

- Revizija pravilnosti postupaka koja ima za cilj da utvrdi da li računovodstveni i sistem internih kontrole efikasno funkcionišu;
- Revizija poslovanja koja ima za cilj da utvrdi da li postoji mogućnost da se poslovanje banke ili

¹⁹ www.coso.org/ic-integratedframework-summary.htm, Internal control–Integrated Framework, Decembar 2011. str17

²⁰ www.kontroling.ftn.uns.ac.rs/skripte.html, Dr Branislav Nerandžić, Uloga interne revizije u korporativnom upravljanju rizicima, januar 2009., preuzeto dana 13.07.2012.

pojedinih njenih delova poboljša;

- Istraživanje pronevera koje se vrši u slučaju kada se pojavi sumnja da je pronevera izvršena;
- Ispitivanje primene propisa;
- Ostala ispitivanja na zahtev rukovodstva banke.²¹

Bankarstvo je dinamična ekonomska grana koja se brzo razvija, na čije poslovanje utiču brojni spoljni i unutrašnji faktori i zato banke moraju kontinuirano da nadgledaju svoje sisteme interne kontrole i moraju da unaprede te sisteme ako je to neophodno da bi se održala njihova efektivnost.²²

Uloga interne revizije u nadgledanju sistema internih kontrola definisana je sledećim principima koji su objavljeni od strane Bazelskog komiteta za bankarsku superviziju:

Princip 10

Celokupna efektivnost internih kontrola banke treba stalno da se nadgleda. Nadgledanje ključnih rizika treba da bude deo svakodnevnih poslova banke, kao i periodičnog ocenjivanja od strane poslovnih delova i interne revizije.

Princip 11

Treba da postoji efektivna i sveobuhvatna interna revizija sistema interne kontrole koju sprovodi osoblje koje je nezavisno od posla i koje je obučeno na odgovarajući način i kompetentno. Funkcija interne revizije kao deo nadgledanja sistema interne kontrole, treba da bude direktno odgovorna nadzornom odboru ili komitetu za reviziju i višem rukovodstvu.

Princip 12

O nedostacima interne kontrole, bilo da ih je identifikovala Uprava, interna revizija ili drugi kontrolni organ, treba blagovremeno da se izvesti odgovarajući nivo rukovodstva. O materijalno značajnim nedostacima interne kontrole treba da se izvesti više rukovodstvo ili nadzorni odbor.²³

21 Prof. dr Milovan Stanišić, Doc. dr Ljubiša Stanojević, "Revizija u bankarstvu", Univerzitet Singidunum, Beograd 2007. str. 21

22 Mr Mile Stanišić, Interna revizija i interna kontrola nad poslovanjem, str. 213

23 www.bis.org/publ/bcbs40.pdf, Framework for internal control systems in banking organisations, Basel, Septembar 1998. str. 4,5 preuzeto dana 14.07.2012.

3.4. Karakteristike internih revizora u Srbiji

Profesionalno zvanje ovlašćeni interni revizor može da stekne lice koje ima visoku školsku spremu, radno iskustvo na poslovima eksterne ili interne revizije u trajanju od 3 godine, odnosno radno iskustvo u trajanju od 5 godina na poslovima računovodstva, položen ispit za sticanje ovog profesionalnog zvanja i koje nije osuđivano za krivična dela koja ga čine nedostojnim za obavljanje ovih poslova.²⁴ Prema podacima koji su javno dostupni i nalaze se u registrima koje vodi Komora ovlašćenih revizora, u Republici Srbiji ima ukupno 56 ovlašćenih internih revizora.

U radu su posmatrane sledeće karakteristike populacije ovlašćenih internih revizora u Srbiji:

1) Starosna struktura ovlašćenih internih revizora:

Naredna tabela prikazuje starosnu strukturu ovlašćenih internih revizora u Republici Srbiji:

Godine života	Broj ovlašćenih internih revizora
Od 20 do 29	1
Od 30 do 39	16
Od 40 do 49	20
Od 50 do 59	22
Preko 60	2
Ukupno	56

Tabela 1 - *Starosna struktura ovlašćenih internih revizora u Republici Srbiji*

Na osnovu uvida u raspoložive podatke registara Komore ovlašćenih revizora, utvrđeno je da prosečna starost ovlašćenih internih revizora u Republici Srbiji iznosi 46 godina, najmlađi ovlašćeni interni revizor ima 29 godina, a najstariji 63 godine.

²⁴ Zakon o računovodstvu i reviziji 2006. godina, "Службени гласник РС" бр. 46/2006

2) Struktura ovlašćenih internih revizora prema prethodnom fakultetskom obrazovanju:

Član 4 Zakona o računovodstvu i reviziji i član 5 Pravilnika o uslovima za izdavanje sertifikata o sticanju profesionalnog zvanja ovlašćeni revizor i ovlašćeni interni revizor koji se bave prethodnim uslovima za sticanje profesionalnih zvanja zahtevaju visoku stručnu spremu, ali ne ograničavaju na određene vrste fakultetskog obrazovanja. i pored toga, ovlašćeni interni revizori su većinom završili Ekonomski fakultet (tabela 2.):

Završen fakultet	Broj ovlašćenih internih revizora
1.Ekonomski fakultet	55
2.Fakultet političkih nauka	1
Ukupno (1 + 2)	56

Tabela 2 - *Struktura ovlašćenih internih revizora u Republici Srbiji prema fakultetskom obrazovanju*

3) Struktura nostrifikovanih profesionalnih zvanja stečenih u inostranstvu

Prema članu 1. Pravilnika Komore ovlašćenih revizora o uslovima za nostrifikaciju profesionalnih zvanja stečenih u inostranstvu, Komora ovlašćenih revizora vrši nostrifikaciju profesionalnih zvanja “ovlašćeni revizor” i “ovlašćeni interni revizor”, a koje su izdate od strane sledećih inostranih organizacija i organa:

- 1) Association of Chartered Certified Accountants;
- 2) Institute of Certified Accountants of England and Wales;
- 3) Institute of Chartered Accountants of Scotland;
- 4) Institute of Chartered Accountants of Ireland;
- 5) Canadian Institute of Chartered Accountant;
- 6) Ministarstvo finansija Ruske Federacije;
- 7) American Institute of Certified Public Accountants;
- 8) Compagnie Nationale des Commissaires aux Comptes (Statutarni savet ovlašćenih revizora);

- 9) Wirtschaftsprüferkammer, Deutschland;
- 10) Australian Society of Certified Practising Accountants;
- 11) Institute of Chartered Accountants in Australia;
- 12) Institute of Internal Auditors Global;
- 13) Ordre des Experts-Comptables (Red stručnih računovođa).

Prema podacima Registra nostrifikovanih profesionalnih zvanja stečenih u inostranstvu, koji vodi Komora ovlašćenih revizora u skladu sa dodeljenim nadležnostima, u prethodnom periodu izvršena je nostrifikacija 47 sertifikata profesionalnih zvanja, od kojih je samo 7 sertifikata profesionalnog zvanja “ovlašćeni interni revizor” i to u sledećim inostranim profesionalnim organizacijama:

Strana profesionalna organizacija	Broj ovlašćenih internih revizora
1. The Institute of Internal Auditors (IIA)	6
2. The Association of Chartered Certified Accountants (ACCA)	1
Ukupno	7

Tabela 3 – Pregled profesionalnih zvanja stranih profesionalnih organizacija nostrifikovanih od strane Komore ovlašćenih revizora²⁵

²⁵ www.kor.rs/registri_nostr_zvanja.asp preuzeto dana 29.07.2012.

5) Geografska struktura ovlašćenih internih revizora

Naredna tabela prikazuje geografsku strukturu ovlašćenih internih revizora u Republici Srbiji:

Grad	Broj ovlašćenih internih revizora
1. Beograd	40
2. Novi Sad	7
3. Kragujevac	2
4. Pančevo	1
5. Čačak	1
6. Aranđelovac	1
7. Indija	1
8. Pirot	1
9. Subotica	1
10. Aleksinac	1
Ukupno (1 do 10)	56

Tabela 4 – *Geografska struktura ovlašćenih internih revizora registrovanih u Republici Srbiji*

Iz tabele je uočljivo da najveći broj ovlašćenih internih revizora živi u Beogradu, čak 71,43% njih. U Novom Sadu živi 12,5% ovlašćenih internih revizora, a 16.07% iznosi udeo ovlašćenih internih revizora u ostalim gradovima u Srbiji. Iz podataka je uočljiva nesrazmera, to jest koncentracija ovlašćenih internih revizora u glavnom gradu.

4. REVIZIJA INFORMACIONIH TEHNOLOGIJA

U prošlosti je bilo slučajeva da iako u finansijskim i poslovnim izveštajima nema nepravilnosti, ipak nije predstavljeno stvarno stanje u kojem se banke i kompanije nalaze. Nastanak revizije informacionih tehnologija usloveli su veliki, neočekivani skandali koji su potresli poslovno okruženje.

Barings, jedna od najstarijih banki u Londonu bankrotirala je usled jednog ovakvog incidenta. Naime, generalni direktor Barings-a uspeo je da zaobiđe organizacione strukture, regularne revizije i interne kontrole i uspeo da radi bez ikakvog nadzora. Do bankrota je došlo zbog njegovih takozvanih budućih ugovora a to je ugovor između dve strane, za prodaju ili kupovinu određene imovine standardizovanog kvaliteta i kvantiteta po cenama dogovorenim za taj dan (budućim cenama), a kojima se trguje na budućim razmenama.

Nakon ovog, usledio je i skandal u Enron korporaciji, jednoj od najvećih energetske kompanije u SAD-u. Korišćenjem računovodstvenih rupa i slabih finansijskih izveštaja, kao i pritisak na revizore Arthur Andersen-a, rukovodeće osoblje Enron korporacije uspeo je da sakrije dugove od milijardi dolara vezane za neuspele ponude i projekte. Posle ovog skandala došlo je i do raspada kompanije Arthur Andersen koja je uz PricewaterhouseCoopers, Ernst & Young, KPMG i Deloitte činila veliku petorku (Big Five).

Ponovo je dokazan stav da “ono što nije kontrolisano, vremenom će se sigurno pogoršati”²⁶

Rezultat ovih događaja bilo je pooštavanje revizije i kontrole. Uvedeni su novi zakoni i regulative kako bi revizorima osigurali nezavisnost i objektivnost, a finansijsko izveštavanje je prošireno i poboljšano.

Zbog ovih događaja i revizija informacionih sistema mora biti dobro revidirana. Informacioni sistemi i tehnologije ne mogu se smatrati odvojenim od ostatka kontrolne okoline i logično je da se pravna regulativa i zahtevi korporativnog upravljanja (Basel II) trebaju primeniti na tom delu poslovanja.

Revizija IT-a je procena informacionih tehnologija, praksi i operacija koje osiguravaju integritet informacionog subjekta. Ovakva procena uključuje procenu delotvornosti, učinkovitosti i ekonomičnosti praksi koje su računarski bazirane.

Revizorova procena uključuje:

- Procenu internih kontrola unutar ambijenta informacionih tehnologija kako bi osigurala validnost, pouzdanost i sigurnost informacija;
- Procenu efikasnosti i delotvornosti ambijenta informacionih tehnologija u ekonomskim terminima.

Tipovi IT revizije prema području delovanja:

- Tehnička IT revizija – pokriva infrastrukturu, prenos podataka i komunikacione podatke;
- Aplikaciona IT revizija – pokriva poslovne i finansijske delove;

26 Prof. dr Milovan Stanišić, Revizija, Univerzitet Singidunum, Beograd 2009. str. 66

- Organizaciona IT revizija – pokriva upravljanje kontrola nad informacionim tehnologijama;
- Razvojna i implementaciona IT revizija – pokriva specifikacije, zahteve, dizajn, razvoj i implementaciju;
- Zakonska IT revizija – pokriva nacionalne i međunarodne standarde.²⁷

U današnje vreme kada su kompjuteri i informacione tehnologije postale sastavni deo života, pa tako i poslovanja, njihove stalne, sve dinamičnije promene i napredovanje, zavisnost velikih kompanija o informacionim sistemima i tehnologijama uslovile su potrebu za kontrolom i revizijom tih tehnologija. Nadgledanje i revizija informacionih sistema i tehnologija neophodni su za uspešno poslovanje i sprovođenje poslovnih aktivnosti preduzeća. Uloga revizije je da osigura integritet informacionih sistema i finansijskog izveštavanja kako bi se na vreme sprečili finansijski problemi i umanjili potencijalni rizici. Uloga revizora je takode da proverava celovitost podataka i svih sistema koji procesuiraju, izveštavaju i održavaju podatke, da procene i evaluiraju stabilnost podataka i informacija koje su računarski generisane, posmatra sposobnost kontrola informacionih sistema kako bi garantovao pouzdanost sistema.

4.1. Upravljanje informacionim tehnologijama

Na uspešnost preduzeća utiče nivo raspoložljivosti, pouzdanosti, bezbednosti i IT sposobnosti. Time postaje značajna i zrelost upravljanja IT. Iako neke kompanije ne shvataju važnost informacionih tehnologija i njihov uticaj na ostvarivanje poslovnih ciljeva i poslovanje, informacione tehnologije predstavljaju budućnost poslovanja s obzirom da se danas gotovo svi poslovni procesi obavljaju korišćenjem različitih tehnologija.

Organizacija koja je podržana inovativnim IT uslugama sposobna je da brzo reaguje na promene na tržištu koje su sve češće, da se preusmerava, dostiže višu produktivnost, zadržava stare i pridobija nove stranke, kao i da povećava prihod, a uprava je sposobna da lakše donosi strateške odluke o budućnosti organizacije.²⁸

Upravljanje IT (IT Governance) sastoji se od rukovođenja, organizacione strukture i procesa koji obezbeđuju da informacione tehnologije podržavaju i proširuju organizacione ciljeve i strategije. Upravljanje informacionim tehnologijama je odgovornost kako rukovodstva tako i upravnog odbora. Osiguranje vrednosti informacionih tehnologija, upravljanje rizicima vezanim za IT, kontrola nad informacijama predstavljaju srž upravljanja informacionim tehnologijama. Samim razvojem informacionih tehnologija, raste i značaj revizije i kontrole u upravljanju ovim tehnologijama.

²⁷ <http://itrevizija.ba/informacione-tehnologije/tipovi-it-revizije>, preuzeto dana 01.08.2012.

²⁸ David L. Cannon, *CISA – Certified Information Systems Auditor, Study Guide Second edition*, Wiley Publishing, Indianapolis 2008. str.120

Upravljanje informacionim tehnologijama obuhvata sledeća područja :

- Strateško poravnanje (Strategic alignment) fokusira se na osiguravanje povezanosti poslovnih i IT planova, definisanje, održavanje i potvrđivanje IT vrednosti, vođenje IT poslovanja u skladu s poslovnim operacijama;
- Dostava vrednosti (Value delivery) fokusira se na izvršavanje vrednosti propozicija kroz ciklus dostave koji osigurava da IT dostavlja obećane prednosti kroz strategiju, a koncentrišući se na optimizaciju troškova i dokazivanje vlastite vrednosti IT-a;
- Upravljanje resursima (Resource management) se odnosi na optimalno ulaganje te pravilno upravljanje kritičnim IT procesima kao što su: aplikacije, informacije, infrastruktura i ljudi. Ključna pitanja odnose se na optimizaciju znanja i infrastrukture;
- Upravljanje rizicima (Risk management) zahteva podizanje svesti o rizicima od strane zaposlenih i višeg menadžmenta, jasno razumevanje kompanijinog "apetita za rizikom", razumevanje u skladu sa zahtevima, transparentnost o bitnim rizicima unutar kompanije i ugrađivanje mera odgovornosti za upravljanje rizicima u organizaciji;
- Mere izvođenja (Performance measurements) prate i nadziru primenu strategija, završetka projekata, korišćenja resursa, procesa rada i pružanja usluga koristeći npr. uravnoteženu karticu rezultata koja prevodi strategije u akcije kako bi postigli najbolje ciljeve merene izvan konvencionalnih računovodstvenih metoda.²⁹

Okvir upravljanja IT-jem kao što je naprimer COBIT može biti ključni element u obezbeđivanju odgovarajuće kontrole i upravljanja nad informacijama i sistemima.

COBIT podržava upravljanje IT-jem obezbeđivanjem okvira kako bi se osiguralo da:

- IT je usklađen sa poslovanjem;
- IT omogućava poslovanje i maksimizira koristi;
- IT resursi se koriste odgovorno;
- IT rizicima se upravlja adekvatno.

IT je od suštinske važnosti za upravljanje transakcijama, informacijama i znanjem neophodnim za pokretanje i održavanje socijalnih i ekonomskih aktivnosti. Dok mnoge organizacije prepoznaju potencijalne prednosti koje tehnologija donosi, one uspešne takođe razumeju, prepoznaju i upravljaju rizicima vezanim za implementaciju novih tehnologija.

²⁹ itrevizija.ba/okviri-it-revizije/upravljanje-it-it-governance, preuzeto dana 17.08.2012.

Među nedoumicama i izazovima sa kojima se preduzeće susreće su:

- Usklađivanje IT strategije sa poslovnom strategijom;
- Obezbeđivanje organizacione strukture koja omogućava realizaciju strategije i ciljeva;
- Insistiranje da IT kontrolni okvir bude usvojen i sproveden;
- Merenje IT performansi.³⁰

Rukovodstvo treba da:

- Bude upoznato sa konceptima i aktivnostima vezanim za informacioni sistem;
- Odredi člana koji će biti nadležan za nadzor i kontrolu procesa upravljanja informacionim sistemom;
- Uspostavi adekvatnu organizacionu strukturu, pripadajuće funkcije i odbore;
- Definiše kriterijume, načine i postupke izveštavanja;
- Usvoji strategiju informacionog sistema i nadzire njeno sprovođenje;
- Donese procedure kojima se uređuje upravljanje informacionim sistemima;
- Uspostavi proces upravljanja rizikom informacionog sistema.

Uprava treba da promoviše pravovremene, efikasne i efektivne mere usmerene na rešavanje ovih problema. Dakle izvršni odbori i menadžment treba da prošire već postojeće upravljanje nad preduzećem putem efikasnog upravljanja IT okvirom, koji se bavi strateškim poravnanjem, merenjem performansi, upravljanjem rizicima i upravljanjem resursima.

IT upravljanje je sastavni deo upravljanja preduzećem i sastoji se od liderskih i organizacionih struktura i procesa. Upravo zbog ovog, sve većeg značaja IT-ja na poslovanje preduzeća, veoma je bitno sprovesti aktivan nadzor nad upravljanjem IT-jem i tako obezbediti uspešno poslovanje kompanija. Uslov opstanka bilo koje organizacije je da raspolaže adekvatnim informacionim sistemom, u kojem su optimizovani poslovni procesi i tokovi informacija.

³⁰ www.itgi.org/template_ITGIa166.html?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657, preuzeto dana 18.08.2012.

4.2. Interna revizija u oblasti informacionih tehnologija

Napretkom informacione tehnologije do nivoa na kome se danas nalazi, raste i njen uticaj na poslovanje preduzeća. Sistem upravljanja nad informacionim tehnologijama veoma je bitan faktor za uspešne poslovne rezultate. On predstavlja sastavni deo opšteg sistema upravljanja kompanijom i sastoji se od rukovođenja, organizacione strukture i procesa koji obezbeđuju da IT podržava i proširuje strategiju i ciljeve kompanije.³¹

Kompanije treba da aktivno vrše nadzor upravljanja informacionim tehnologijama, da osiguraju da su IT operacije, rizici i mogućnosti vođeni tako da doprinose uspešnom poslovnom rezultatu organizacije, a ipak podaci Nacionalne asocijacije korporativnih direktora (NACD) pokazuju da mali broj preduzeća ima odbore za nadzor IT-a.

Ključni faktor za uspešno uvođenje i primenu novih tehnologija i informacionih sistema u odeljenje interne revizije predstavljaju kadrovi, koji moraju imati određeno znanje u vezi sa primenom informacionih sistema. Nema sumnje da poslednjih 10 do 15 godina, informaciona tehnologija i kompjuterski zasnovane tehnike, vrše invaziju na:

- konvencionalne revizijske procedure i procese;
- utvrđene revizijske tehnike koje revizori koriste.

Institut internih revizora (IIA), zbog velikog uticaja informacionih tehnologija na poslovanje preduzeća, 2008. godine Međunarodnim standardima prakse dodaje standard 2110.A2 koji glasi :

“Interna revizija mora proceniti da li upravljanje informacionim tehnologijama podržava organizacione strategije i ciljeve”³².

U okruženju informacionih tehnologija manje je papira dostupno za proveru i usklađivanje transakcija, pa revizor treba da:

- stekne dovoljno znanja o procesima i resursima informacionih tehnologija, kao i o ugrađenim informacionim sistemima u organizaciji;
- stekne uverenje da procesi i informacioni sistemi rade ispravno;
- razvije razumevanje kontrola i revizijski pristup koji će utvrditi da sistem internih kontrola preduzeća deluje efikasno;
- istraži i proveriti transakcije kroz sistem obrade kako bi utvrdio da su transakcije u potpunosti i ispravno obrađene.

31 uirs.rs/index.php?option=com_content&view=category&layout=blog&id=32&Itemid=40, Bilten broj 16, Novembar 2010. (Informativno-teoretski list “Udruženja internih revizora Srbije”), preuzeto dana 23.08.2012.

32 global.theiia.org/standards-guidance/mandatory-guidance/pages/standards.aspx, preuzeto dana 24.08.2012.

Kao što je propisano u Standardu 2110.A2, zadatak interne revizije je da procenjuje adekvatnost aktivnosti upravljanja informacionim tehnologijama sa stanovišta rizika i da planira revizijske angažmane kada je to potrebno. Kada ocenjuje adekvatnost upravljanja nad sistemom IT-a, revizor mora voditi računa o sledećem:

- Usklađivanje organizacione i IT strategije;
- Realizacija IT projekata i poslovna vrednost;
- Realizacija mogućnosti povezanih sa informacionim tehnologijama;
- Efektivno upravljanje i odgovorna upotreba IT resursa;
- Efikasno upravljanje poslovnim rizicima povezanim sa informacionim tehnologijama;
- Usklađenost sa važećim zakonima, propisima i korporativnim standardima.

Pored znanja koje revizori steknu u okviru odeljenja interne revizije postoje i drugi načini edukacije internih revizora za upotrebu informacionih tehnologija i razumevanje funkcionisanja informacionih sistema. Načini za sticanje neophodnih znanja i veština mogu biti opšta edukacija vezana za informacione tehnologije, obuka revizora kao korisnika informacionih tehnologija, obuka revizora kao menadžera informacionih sistema, obuka revizora kao dizajnera i projekatanta informacionih sistema i obuka revizora za podsticaje u ocenjivanju informacionog sistema u razvoju novih tehnologija³³.

Jedna od najuticajnijih internacionalnih organizacija za reviziju i kontrolu informacionih sistema je ISACA (Information Systems Audit and Control Association). Članovi ISACA -e su ljudi sa različitim iskustvima i znanjem, zaposleni u različitim poslovnim područjima kao što su finansijske i bankarske institucije, revizorske i računovodstvene kompanije, javni ili privatni sektor, proizvodni ili prodajni sektor. Slovenija i Hrvatska već imaju formirane odseke ISACA -e, dok Srbija i Bosna još uvek nemaju. Slovenački odsek osnovan je 1994. godine i broji 160 članova, a Hrvatski 2001. godine i broji 130 članova. Cilj ovih odseka je edukacija članova, unapređenje poslovnih i IT procesa i kontrola, kao i promovisanje odličnih rešenja zaštite informacionih sistema i visoko kvalitetne revizije informacionih tehnologija i sistema³⁴.

Primarna uloga revizora je pored savetodavne funkcije i da pruži razumno uverenje da će sve operativne kontrole biti u funkciji i da će raditi efikasno i efektivno. Revizor je kao i uprava tu kako bi zajednički osigurali pravilan rad informacionih tehnologija i operacija, kao i procesa i usluga koje se odnose na informacione tehnologije.

Široko poznavanje informacionih tehnologija potrebno je za reviziju informacijskih sistema. Neke posebne veštine koje su potrebne su:

33 Mijić Kristina, Jakšić Dejan, *Primena kompjuterskih alata i tehnika prema fazama procesa revizije finansijskih izveštaja*, Revizor 49/2010, Institut za ekonomiku i finansije, str. 84

34 www.itrevizija.ba/it-revizija/it-revizija-u-regionu, preuzeto dana 27.08.2012.

- Razumevanje očekivanja, uloga i celokupnog poslovanja u reviziji informacionih sistema, projektnog menadžmenta i software-a;
- Korišćenje CAAT alata i tehnika (computer-assisted audit tools);
- Sposobnost da proceni pitanja privatnosti i sigurnosti koja mogu doneti rizik organizaciji;
- Evolucija životnih ciklusa složenih sistema (SDLC - System Development Life Cycles);
- Razvoj novih tehnika koje uključuju brze izrade i prototipe sistema;
- Primena rizik-orijentisanog pristupa reviziji;
- Pregled i verifikacija organizacijskih informacionih tehnologija vezanih za pravna pitanja;
- Primenu nacionalnih i međunarodnih standarda kao što je ISO 9000 / 3, ISO 27001, ISO 27002;
- Izveštavanje i obavljanje pregleda kako bi se osiguralo da je posao adekvatno obavljen.

Od ukupno 56 ovlašćenih internih revizora u Republici Srbiji, čak 55 njih su ekonomisti dok je samo jedno lice politikolog.³⁵ Iz priloženog mozemo zaključiti da ne postoji ni jedan ovlašćeni interni revizor u Srbiji, koji je usmeren na informacione sisteme i tehnologije.

4.3. Interne kontrole sa aspekta revizije informacionih tehnologija

Interne kontrole predstavljaju politike, planove i procedure kao i organizacione strukture dizajnirane da omoguće realnu sigurnost kako bi poslovni ciljevi bili postignuti, a neželjeni događaji sprečeni, detektovani i ispravljeni.

Interne kontrole kreiraju organizacioni plan i sve koordinacione metode usvojene unutar preduzeća kako bi zaštitili svoju imovinu, proverili preciznost i pouzdanost računovodstvenih podataka, promovisali operacionu efikasnost i podsticali pridržavanje propisanih menadžerskih politika. Svaki sistem i proces unutar kompanije postoji kako bi zadovoljio određene poslovne svrhe. Revizor mora tražiti postojanje rizika za te svrhe a zatim osigurati da su interne kontrole na pravom mestu za ublažavanje tih rizika.³⁶

³⁵ www.kor.rs/registri_izdatih_sertifikatai_interni.asp, preuzeto dana 24.08.2012.

³⁶ www.itrevizija.ba/informacione-tehnologije/interne-kontrole, preuzeto dana 24.08.2012.

Osnovni ciljevi procesa internih kontrola informacionog sistema su:

- Čuvanje imovine informacionog sistema (sigurnosni ciljevi);
- Osiguravanje što višeg stepena integriteta informacionog sistema i njegovog neposrednog okruženja, uključujući delovanje sistemskog software-a, upravljanje mrežama i radom samog sistema;
- Osiguravanje što višeg stepena integriteta upravljanja informacijama i integriteta kritičnih delova aplikacionog softwarea (informacioni ciljevi);
- Autorizacija ulaza;
- Tačnost i potpunost transakcijskog dela sistema;
- Pouzdanost svih aktivnosti vezanih za obradu informacija;
- Tačnost, potpunost i sigurnost izlaznih vrednosti;
- Što viši integritet baza podataka;
- Osiguranje delotvornosti i učinkovitosti informacionog sistema;
- Usklađenost sa zahtevima korisnika, organizacionim procedurama i ciljevima, zakonskim i drugim aktima (ciljevi usklađivanja);
- Donošenje planova za arhiviranje (backup) sadržaja i ponovno pokretanje sistema nakon neželjenog događaja (disaster recovery) ;
- Razvoj procedura i pravila kojima se postupa u slučaju incidenta, čiji je osnovni zadatak da što pre omoguće neprekidnost poslovanja uz minimalne gubitke i troškove (business continuity).
Uspešne kompanije često propisuju i neke dodatne uslove ciljeva neprekidnosti poslovanja.³⁷

Postoje 3 osnovna tipa interne kontrole i to:

Preventivne kontrole njihov glavni zadatak je da utvrde probleme ili neželjene pojave pre nego što se pojave, da ih predvide i pokušaju da ih zaustave korišćenjem preventivnih mera, kao i da stalno prate rad informacionog sistema. Tipični primeri preventivnih kontrola su zapošljavanje obrazovanih i kvalifikovanih radnika, utvrđivanje organizacije tela koja se koriste za praćenje rada informacionog sistema (IT Upravnog odbora), stvaranje odseka za unutrašnju reviziju informacionog sistema, podizanje svesti o stalnim potrebama revizije i kontrole, dodeljivanje dužnosti i odgovornosti, kao i stvaranje priručnika o sigurnosnoj politici informacionog sistema.

Detektivne kontrole su one koje utvrđuju i detektuju greške i probleme bilo kog dela informacionog

³⁷ www.itrevizija.ba/informacione-tehnologije/interne-kontrole, preuzeto dana 30.08.2012.

sistema. Tipični primeri su razne osnovne kontrole informacionih sistema, kontrole ulaznih podataka, kontrole ovlasti, fizičke i logističke kontrole pristupa informacionom sistemu, provere dozvola za sisteme, kontrole tačnosti, kontrole procesa, kontrola podataka i sl.

Korektivne kontrole čiji je cilj da minimizira efekat pogreški i problema koji mogu ugroziti informacioni sistem. Čim se uoči pretnja ove kontrole izvršavaju specijalne instrukcije tako da detektovane pogreške ili pretnje mogu biti ispravljene. Procedure kopiranja i arhiviranja podataka, kontrole prenosa podataka, kontrole nad ključnom opremom su samo neke od čestih korektivnih kontrola.

Kontrole informacionih tehnologija mogu se podeliti prema specifičnim područjima koje obuhvataju, tako da imamo sigurnosne kontrole, informacione kontrole (kontrole podataka), kontrole kontinuiteta poslovanja, itd.

Primeri internih kontrola unutar informacionog sistema su:

Kontrole promene software-a:

- Programeri nemaju logičan pristup kako bi izvršili nadogradnje produkcionog koda;
- Ljudi koji imaju logički pristup kako bi izvršili nadogradnje produkcionog koda neće to uraditi bez dokaza o testiranju i odobrenja.

Pristupne kontrole:

- Potreba za unošenjem korisničkog imena i šifre kako bi pristupili sistemu je tip interne kontrole;
- Ograničen broj aplikacija za korisnika koje određuju sigurnosni administratori koji ujedno kontrolišu dodavanje novih korisnika u sistem je takođe tip interne kontrole.

Sigurnosne kopije i planovi oporavljanja nakon katastrofe sistema:

- Pravljenje kopija sistema i podataka periodično je interna kontrola;
- Dostavljanje kopija na drugo mesto je interna kontrola;
- Dokumentovanje plana za oporavljanje nakon katastrofe sistema je interna kontrola.

Interne kontrole predstavljaju skup postupaka koje oblikuje uprava, menadžment i ostali zaposleni sa svrhom sticanja razumnog uverenja da će se organizacijski ciljevi ostvariti, a neželjeni rizici predvideti, otkriti, i na vreme ukloniti. Zbog toga razvijaju brojne politike, procedure, prakse i postupke. Menadžment kompanije, u saradnji s menadžmentom informacionog sistema direktno je odgovoran za oblikovanje, primenu i ocenu efikasnosti sistema internih kontrola unutar informacionog sistema. U svetskim razmerama, već su prisutne koordinirane inicijative koje vode ka standardizaciji okvira internih kontrola pri čemu je čest zaključak da učinkovita primena sistema internih kontrola nije nikako moguća bez učinkovitog sistema internih kontrola informacionog sistema, poznat kao Sarbanes-Oxley Zakon.

5. POJAM I SVRHA ETIČKOG KODEKSA I MEĐUNARODNIH STANDARDA

Standardi predstavljaju kriterijume za procenjivanje i merenje poslovanja jedinice za internu reviziju, a namenjeni su predstavljanju prakse interne revizije onakvom kakva bi ona trebala da bude. Dakle namera standarda je da ocrtaju osnovne principe kakva praksa treba da bude, da omoguće okvir za sprovođenje i unapređenje aktivnosti koje doprinose povećanju vrednosti, ustanovi osnovu za merenje performansi i unapređenje organizacionih procesa i operacija.³⁸

Prve standarde za profesionalno obavljanje interne revizije (Standards for the Professional Practice of Internal Auditing) izdaje Institut internih revizora (IIA) SAD, 1978. godine. Oni su doneti kao nacionalni standardi, ali su ih kasnije preuzele mnoge druge zemlje, uz mala prilagođavanja. Zemlje koje su pravile svoje standarde morale su da obezbede usaglašenost sa američkim odnosno međunarodnim standardima.

Međunarodna grupa eksperata (GTF – Guidance Task Force) je pomoću informacija sakupljenih iz sopstvenih iskustava njenih članova i iz različitih istraživačkih studija i simpozijuma, formulisao novi okvir za profesionalnu praksu. Ove druge, nove standarde izdaje IIA 2002. godine pod nazivom Međunarodni standardi za profesionalnu praksu interne revizije. Novi standardi su bazirani na definiciji interne revizije i Kodeksu etike i sadrže savete i praktične smernice i takođe praktični savetnik i praktična uputstva.

Osnovna razlika između novih i starih standarda je naglasak na zahtevu za ocenom kvaliteta rada interne revizije kroz samoocenjivanje i ocenu od drugih nezavisnih tela.³⁹

Sadržaj standarda uključuje:

1. *Standarde atributa* koji se odnose na karakteristike organizacija i izvršilaca koji sprovode aktivnost interne revizije i obuhvataju 4 grupe:

- Svaha, ovlašćenja i odgovornost;
- Nezavisnost i objektivnost;
- Stručnost i profesionalna pažnja;
- Program osiguravanja i poboljšanja kvaliteta.

2. *Standarde rada* koji opisuju prirodu aktivnosti interne revizije i obezbeđuju kriterijume kvaliteta sa kojima se upoređuju performanse ovih aktivnosti. Obuhvataju 7 grupa:

- Upravljanje aktivnostima interne revizije;
- Priroda posla;

38 www.dgt.uns.ac.rs/download/kontrevhot_06.pdf, Dr Branislav Nerandžić, Međunarodni standardi interne revizije i Kodeks etike, prezentacija, novembar 2011. preuzeto dana 01.09.2012.

39 www.dgt.uns.ac.rs/download/kontrevhot_06.pdf, Dr Branislav Nerandžić, Međunarodni standardi interne revizije i Kodeks etike, prezentacija, novembar 2011. preuzeto dana 01.09.2012.

- Planiranje posla;
- Izvođenje posla;
- Izveštavanje o rezultatima;
- Nadgledanje napretka;
- Odluka menadžmenta o prihvatanju rizika.

3. *Standardi implementacije*

Proces interne revizije i etika su usko povezani i veoma je važno da izvršni menadžment svim zaposlenim licima posebno skrene pažnju na etičnost. Etički kodeks se sastoji iz načela koja su relevantna za profesiju i praksu interne revizije i pravila ponašanja odnosno normi ponašanja koje se očekuje od internih revizora.

Prvenstveno zbog različite zakonske regulative različitih zemalja, praćenje i poštovanje Standarda i Kodeksa etike je veoma važno kako bi revizori na pravi način ispunili svoje odgovornosti. Pridržavanje ovih principa, standarda i načela vodi ka uspehu, kako revizora tako i same organizacije, a bilo kakvo nepoštovanje istih dovodi do odgovarajućih disciplinskih mera, pa u ozbiljnim slučajevima čak i do gubljenja dozvole za rad.

5.1. Etička načela, principi i opšte prihvaćena pravila ponašanja

Prve moralne norme koje su usvojene 1968. godine, odnosile su se na sve interne revizore, članove Instituta internih revizora (IIA). Međutim, s'obzirom da ovlašćeni interni revizori nisu bili članovi ovog instituta, oni nisu bili u obavezi da se pridržavaju propisanih normi i zakona. Pravila ovlašćenih internih revizora takođe su se razlikovala od pravila Instituta internih revizora. Kako bi se ove razlike prevazišle, 1988. godine su usvojene nove Moralne norme koje zahtevaju poštovanje kako članova IIA, tako i ovlašćenih internih revizora.

Etički kodeks kao promoter etičke kulture, neophodan je u profesiji interne revizije i polazi od poverenja u njeno objektivno uveravanje o upravljanju rizicima, kontrolnim procesima i procesima upravljanja. Ovaj dokument postavlja smernice internim revizorima za obavljanje svoje dužnosti kroz dva bitna aspekta:

- Principi koji su relevantni za profesiju i praksu interne revizije;
- Pravila ponašanja koje se očekuje od internih revizora. Ova pravila pomažu u praktičnoj primeni principa i služe internim revizorima kao vodič za etički ispravne postupke.

Od internih revizora se očekuje poštovanje sledećih etičkih principa i pravila ponašanja:

1. Integritet

Svojim integritetom interni revizori grade poverenje što im obezbeđuje osnovu za pouzdavanje u njihove procene. Princip integriteta predstavlja osnovnu vrednost Kodeksa jer ovaj princip obavezuje revizora da postupa časno i ispravno u profesionalnim i poslovnim odnosima i samim tim obezbedi poverenje javnosti u integritet, nepristrasnost i efikasnost ove profesije.

Ovaj princip uslovljava sledeća pravila ponašanja internih revizora:

- Obaveza da svoj posao obavljaju časno, pažljivo i odgovorno;
- Da poštuju zakon i razotkrivaju nezakonite i neprofesionalne postupke;
- Ne smeju svesno biti uključeni u bilo kakve ilegalne aktivnosti, kao i aktivnosti koje vređaju profesionalni ugled interne revizije ili ugled organizacije kojoj pripadaju;
- Obaveza da poštuju i doprinose zakonitim i moralnim ciljevima organizacije kojoj pripadaju;

2. Objektivnost

Interni revizori iskazuju najvišu moguću meru objektivnosti prilikom prikupljanja informacija, prilikom njihove procene i izveštavanja o procesima i aktivnostima koje su predmet njihovog ispitivanja. Zaključci, mišljenja i izveštaji treba da budu sačinjeni nepristrasno i da su zasnovani isključivo na pribavljenim i prikupljenim dokazima u skladu sa standardima revizije.

Nezavisnost revizora ne sme biti ugrožena ličnim ili spoljnim interesima, jer njihova dužnost im nalaže da se uzdrže od uključivanja u sva pitanja u kojima imaju interes, a da o svakoj pretnji, spoljnom pritisku i uticaju obaveste rukovodstvo odnosno nadležna lica.

Dakle, ovaj princip obavezuje interne revizore da:

- Ne smeju učestvovati ni u kakvoj aktivnosti, niti stupati u odnose koji bi mogli da utiču, ili se za njih smatra da bi mogli da utiču, na njihovu nepristrasnost u procenjivanju ili da budu u konfliktu sa interesima organizacije kojoj pripadaju;
- Ne smeju da prihvate bilo šta što bi moglo da utiče ili da se smatra da bi moglo da utiče, na nepristrasnost u profesionalnim zaključivanjima;
- Moraju razotkriti svaku značajnu činjenicu koja im je poznata i koja bi, u slučaju da ostane neotkrivena, mogla da značajno izmeni izveštavanje o aktivnostima koje su predmet ispitivanja.

3. Poverljivost

Interni revizori su u obavezi da poštuju vrednost i vlasništvo nad informacijama do kojih su došli i da ih ne otkrivaju bez odgovarajućeg ovlašćenja ukoliko nisu u pravnoj ili profesionalnoj obavezi da to učine.

U obavezi su da budu savesni u korišćenju i zaštiti informacija do kojih su došli vršeci svoje dužnosti,

kao i da ne smeju koristiti dobijene informacije za ličnu dobit ili na način koji bi bio u suprotnosti sa zakonom, ili štetan po zakonite i moralne ciljeve organizacije kojoj pripadaju.

4. Kompetentnost

Obaveza revizora je da se uvek ponaša na profesionalan način i da primenjuje visoke profesionalne standarde, koji će im omogućiti kompetentno i nepristrasno vršenje dužnosti. Revizor ne sme preduzimati bilo koju aktivnost za koju nije kompetentan. Interni revizori primenjuju svo znanje, veštine i iskustvo koji su neophodni za pružanje usluga interne revizije.

Interni revizori su dužni da:

- Uzimaju učešće samo u onim aktivnostima za koje poseduju neophodna znanja, veštine i iskustvo;
- Pružaju usluge interne revizije u skladu sa Međunarodnim standardima profesionalne prakse interne revizije;
- Neprekidno unapređuju svoje veštine i efektivnost, kao i kvalitet usluga koje pružaju.⁴⁰

Pored ovih principa navedenih u Etičkom Kodeksu, veoma je bitno i da revizori očuvaju političku neutralnost, jer sarađuju sa zakonodavnim i izvršnim organima vlasti kao organima koji su po zakonu ovlašćeni da razmatraju njihove izveštaje. Revizori u javnoj praksi treba da preuzmu razumne korake u cilju identifikovanja slučajeva koji mogu dovesti do sukoba interesa. Sukob interesa revizori izbegavaju i sprečavaju odbijanjem primanja poklona ili bilo kakve usluge ili druge koristi za sebe ili drugo lice u vršenju svoje dužnosti. Revizori ne smeju koristiti svoju zvaničnu poziciju u privatne svrhe i treba da izbegavaju odnose koji bi mogli uključiti rizik od korupcije ili koji bi mogli dovesti u pitanje njihovu objektivnost i nezavisnost.

Interni revizori, ovlašćeni interni revizori i sva lica i organizacije koje pružaju usluge interne revizije dužni su da se pridržavaju Zakona o računovodstvu i reviziji, Okvira profesionalne prakse, Međunarodnih standarda i Kodeksa etike pri obavljanju svoje profesionalne dužnosti, to jest poslova revizije. Od velike važnosti je da revizori budu samostalni i nezavisni jer samo tako svoj posao mogu obavljati slobodno i objektivno. Kroz poštovanje propisanih standarda, moralnih principa i etičkih normi sačuvaće svoj samostalni stav i svoju objektivnost u odlučivanju od uticaja drugih, a to je osnova za sticanje odnosno jačanje poverenja među klijentima revizije.

⁴⁰ uirs.rs/index.php?option=com_content&view=category&layout=blog&id=55&Itemid=77 , Etički kodeks, preuzeto dana 03.09.2012.

5.1.1. Etički kodeks za revizore informacionih sistema

ISACA propisuje ovaj etički kodeks sa ciljem usmeravanja profesionalnog i ličnog ponašanja članova udruženja, kao i svih lica koja poseduju sertifikat ovog udruženja. Kodeks profesionalne etike u velikoj meri je usaglašen sa etičkim kodeksom IIA (Institute of Internal Auditors).

Svi nosioci ISACA sertifikata kao i svi članovi moraju da se pridržavaju sledećih načela:

1. Da pružaju podršku u sprovođenju i podsticanju usaglašenosti sa odgovarajućim standardima i procedurama za efikasno upravljanje i rukovođenje informacionim sistemom i tehnologijama preduzeća uključujući i reviziju, kontrole, bezbednost i upravljanje rizicima;
2. Obavljanje svoje dužnosti sa objektivnošću i dužnom profesionalnom pažnjom u skladu sa propisanim profesionalnim standardima;
3. Da rade u interesu klijenata na zakonit način, uz održavanje visokih standarda ponašanja. Moraju voditi računa da ne diskredituju ni svoju profesiju, ni udruženje;
4. Da održavaju privatnost i poverljivost informacija dobijenih u toku svojih aktivnosti, osim ako sudski organi zahtevaju drugačije. Ove informacije ne smeju biti korišćene u lične svrhe i za ličnu korist;
5. Održavanje nadležnosti u svojim oblastima i preduzimanje samo onih aktivnosti za koje su kompetentni, odnosno za koje poseduju odgovarajuće znanje, veštine i nivo stručnosti;
6. Obaveštavanje odgovarajućih strana o rezultatima rada i otkrivanje svih značajnih činjenica koje su im poznate;
7. Podržavanje profesionalne edukacije klijenata i zainteresovanih strana u cilju poboljšanja razumevanja upravljanja preduzećem, upravljanja informacionim sistemom i tehnologijama uključujući i reviziju, kontrole, bezbednost i upravljanje rizikom.⁴¹

Nepoštovanje ovog kodeksa dovodi do istrage člana ili lica koje poseduje sertifikat udruženja. Kada se istragom dokaže da je lice prekršilo neko od načela kodeksa, sprovode se odgovarajuće disciplinske mere.

⁴¹ www.isaca.org/Certification/Code-of-Professional-Ethics, preuzeto dana 05.09.2012.

5.2. Međunarodni standardi za profesionalnu praksu interne revizije

Međunarodni standardi revizije koje objavljuje Međunarodna federacija računovodja (IFAC), su profesionalni standardi za obavljanje revizije finansijskih izveštaja koji sadrže osnovne principe, bitne preporuke i smernice koje služe kao vodič za revizorsku praksu.⁴²

Kolike god da su pravne, kulturološke i strukturne razlike sredina i organizacija u kojima se interna revizija obavlja usklađenost sa Međunarodnim standardima je neophodna. Odstupanje od njih nije dozvoljeno, osim u specijalnim slučajevima gde prilikom profesionalnog rasuđivanja okolnosti to opravdavaju.

Svrha Standarda za profesiju interne revizije je da:

- Opišu osnovna načela koja predstavljaju praksu interne revizije;
- Obezbede okvir za obavljanje i promovisanje širokog spektra mogućnosti za dodavanje vrednosti putem interne revizije;
- Utvrde osnovu za vrednovanje učinka interne revizije;
- Unaprede procese i operacije organizacije.

Iako MSR predstavljaju osnovu profesionalne prakse, kako interne tako i eksterne revizije, jedan od najvećih problema njihove primene u Republici Srbiji bilo je njihovo prevođenje na srpski jezik. Ovaj problem je dodatno otežavao rešavanje netransparentnosti finansijskih izveštaja kroz samo pridržavanje standardima u Srbiji kao i u zemljama iz okruženja kao što su Crna Gora i Republika Srpska koje su delile ovaj problem. Dugo su se primenjivali Standardi zasnovani na prevodu Standarda iz 2006. godine, objavljeni od strane Saveza računovođa i revizora Srbije. S'obzirom da su MSR od 2006. pretrpeli značajne izmene, trebalo je što pre rešiti problem prevođenja i dostupnosti zvaničnih prevoda svim korisnicima, a u međuvremenu problem adekvatne primene postojećih standarda. Najveća revizorska društva u Srbiji, takozvana „velika četvorka“ (big4), koju čine KPMG, Deloitte, PricewaterhouseCoopers i Ernst & Young, koriste Standarde i druge materijale na engleskom jeziku, a radnu dokumentaciju sastavljaju na srpskom, dok manja revizorska društva koriste ranije prevode ili čak pokušavaju sami da prevedu Standarde na srpski jezik.

Posle dugogodišnjeg kašnjenja, po ovlašćenju Odbora za međunarodne standarde, Savez računovođa i revizora Srbije u saradnji sa Savezom računovođa i revizora Republike Srpske i Institutom sertifikovanih računovođa Crne Gore, izvršio je 2011. godine prevod najnovijih Standarda.

⁴² mfp.gov.rs/pages/article.php?id=7785, Nacrt, Nacionalna strategija za unapređenje kvaliteta korporativnog finansijskog izveštavanja i revizije, preuzeto dana 09.09.2012.

5.2.1. Pregled glavnih i karakterističnih standarda za profesionalnu upotrebu interne revizije 2011. godine

1000 - Svrha, ovlašćenja i odgovornost

- Svrha, ovlašćenja i odgovornost aktivnosti interne revizije moraju biti formalno definisani u povelji interne revizije u skladu sa Definicijom interne revizije, Etičkim kodeksom i Standardima. Izvršni rukovodilac revizije mora periodično da pregleda povelju interne revizije i da je podnosi višem rukovodstvu i odboru na odobrenje.

1000. A1- Priroda usluga uveravanja koje se obezbeđuju organizaciji mora biti definisana u povelji interne revizije. Ukoliko uveravanja treba da budu obezbeđena stranama izvan organizacije priroda ovih uveravanja takođe mora biti definisana u povelji interne revizije.

1000. C1- Priroda savetodavnih usluga mora biti definisana u povelji interne revizije.

1100 – Nezavisnost i objektivnost

- Aktivnost interne revizije mora da bude nezavisna, a interni revizori objektivni u obavljanju svojih poslova.

1110 – Organizaciona nezavisnost

- Izvršni rukovodilac revizije mora da izveštava onaj nivo rukovodstva u organizaciji koji aktivnosti interne revizije omogućava da ispuni svoje obaveze. Izvršni rukovodilac revizije mora, bar jednom godišnje, da potvrdi odboru organizacionu nezavisnost aktivnosti interne revizije.

1110. A1 – Aktivnost interne revizije mora biti slobodna od uticaja drugih kod određivanja obuhvata revizije, izvršenja posla i izveštavanja o rezultatima.

1111 – Neposredna saradnja sa odborom

- Izvršni rukovodilac revizije mora da izveštava odbor i da sa njim neposredno sarađuje.

1120 – Lična objektivnost

- Interni revizori moraju imati objektivni i nepristrasan stav i izbegavati svaki sukob interesa.

1130 – Narušavanje nezavisnosti i objektivnosti

- Ukoliko je nezavisnost ili objektivnost zaista ili naizgled narušena, detalji narušavanja moraju biti obelodanjeni odgovarajućim stranama. Sam način obelodanjivanja zavisiće od narušavanja.

1130. A1 – Interni revizori moraju da se uzdrže od ocenjivanja specifičnih poslova za koje su prethodno bili odgovorni. Smatra se da je objektivnost narušena ukoliko interni revizor pruža usluge uveravanja za aktivnost za koju je interni revizor bio odgovoran u toku prethodne godine.

1130. A2 – Angažovanja uveravanja za funkcije za koje je bio odgovoran izvršni rukovodilac revizije moraju biti nadzirane od strane izvan aktivnosti interne revizije.

1130. C1 – Interni revizori mogu pružati savetodavne usluge u vezi sa poslovima za koje su prethodno bili odgovorni.

1130. C2 – Ukoliko postoji mogućnost narušavanja nezavisnosti ili objektivnosti internog revizora u vezi sa predloženim savetodavnim uslugama, isto se mora obelodaniti klijentu pre prihvatanja angažovanja.

1200 – Stručnost i dužna profesionalna pažnja

- Angažovanja moraju biti obavljena stručno i uz dužnu profesionalnu pažnju.

1210 – Stručnost

- Interni revizori moraju posedovati znanje, veštine i druge sposobnosti neophodne za izvršavanje njihovih dužnosti. Aktivnost interne revizije kolektivno mora da poseduje ili da obezbedi znanja, veštine i druge sposobnosti potrebne za izvršavanje njenih dužnosti.

1210. A1 – Izvršni rukovodilac revizije mora da pribavi stručno mišljenje i pomoć ukoliko interni revizori nemaju znanje, veštine ili druge sposobnosti potrebne za obavljanje celokupnog ili dela angažovanja.

1210. A2 – Interni revizori moraju posedovati dovoljno znanja sa ocene rizik od prevara i način na koji organizacija upravlja tim rizikom, ali se od njih ne očekuje da imaju nivo stručnosti kao lice čija je primarna odgovornost otkrivanje i istraživanje prevara.

1210. A3 – Interni revizori moraju posedovati dovoljno znanja o ključnim informaciono – tehnološkim rizicima i raspoloživim na tehnologiji zasnovanim revizorskim tehnikama, kako bi izvršili dodeljene poslove. Ipak, ne očekuje se od svih internih revizora da imaju isti nivo stručnosti kao interni revizor čija je primarna dužnost revizija informacione tehnologije.

1220 – Dužna profesionalna pažnja

- Interni revizor mora da primenjuje pažnju i veštinu koja se očekuje od internog revizora koji je u razumnoj meri stručan i oprezan. Dužna profesionalna pažnja ne podrazumeva nepogrešivost.

1220. A1 – Interni revizori moraju praktikovati dužnu profesionalnu pažnju, tako što će razmotriti:

- Obim posla potreban za ostvarenje ciljeva angažovanja;
- Relativnu složenost, materijalnost ili značaj pitanja na koja se primenjuju procedure uveravanja;
- Adekvatnost i efektivnost procesa korporativnog upravljanja, upravljanja rizikom i kontrolnih procesa;
- Verovatnoću značajnih grešaka, prevara ili neusaglašenosti;
- Troškove revizije u odnosu na potencijalne koristi.

1220. A2 – Pri praktikovanju dužne profesionalne pažnje interni revizori moraju da razmotre korišćenje na tehnologiji zasnovanih revizorskih tehnika i drugih tehnika za analizu podataka.

1120. A3 – Interni revizori moraju biti spremni da prepoznaju značajne rizike koji mogu uticati na ciljeve, poslovanje ili resurse. Ipak, revizorske procedure same po sebi, čak iako su primenjene sa dužnom profesionalnom pažnjom, ne daju garanciju da će svi značajni rizici biti identifikovani.

1120. C1 – Interni revizori moraju obavljati savetodavna angažovanja sa dužnom profesionalnom pažnjom, tako što će razmotriti:

- Potrebe i očekivanja korisnika, uključujući prirodu, vreme i način saopštavanja rezultata angažovanja;
- Relativnu složenost i obim posla potreban za ostvarenje ciljeva angažovanja;
- Troškove savetodavnih angažovanja u odnosu na potencijalne koristi.

1230 – Kontinuirano profesionalno usavršavanje

- Interni revizori dužni su da unapređuju svoje znanje, veštine i ostale sposobnosti kroz kontinuirano usavršavanje.

1300 – Program obezbeđenja i unapređenja kvaliteta

- Izvršni rukovodilac revizije mora da uspostavi i održava program obezbeđenja i unapređenja kvaliteta koji pokriva sve aspekte aktivnosti interne revizije.

1311 – Interne ocene

Interne ocene moraju uključiti:

- Stalni nadzor učinka aktivnosti interne revizije;
- Periodične preglede izvršene kroz samoocenjivanje ili ocenjivanje od strane drugih lica u organizaciji, koja imaju dovoljno poznavanje praksi interne revizije.

1312 – Eksterno ocenjivanje

- Eksterna ocenjivanja moraju biti sprovedena bar jednom u pet godina od strane kvalifikovanog, nezavisnog ocenjivača ili tima ocenjivača. Izvršni rukovodilac revizije mora da razmotri sa odborom:

- Potrebu za češćim eksternim ocenjivanjem;
- Kvalifikacije i nezavisnost ocenjivača ili tima ocenjivača, uključujući i svaki potencijalni sukob interesa.

1322 – Obelodanjivanje neusklađenosti

Kada neusklađenost sa Definicijom interne revizije, Etičkim kodeksom i Standardima utiče na celokupan delokrug ili poslovanje aktivnosti interne revizije, izvršni rukovodilac revizije dužan je da obelodani neusklađenost i njen efekat višem rukovodstvu i odboru.

2000 – Upravljanje aktivnošću interne revizije

- Izvršni rukovodilac revizije mora efektivno da upravlja aktivnošću interne revizije kako bi osigurao da ona dodaje vrednost organizaciji. Aktivnost interne revizije dodaje vrednost organizaciji (i njenim interesnim stranama) kada obezbeđuje objektivno i relevantno uveravanje i doprinosi efektivnosti i efikasnosti korporativnog upravljanja, upravljanja rizikom i kontrolnih procesa.

2010 – Planiranje

- Izvršni rukovodilac revizije mora da ustanovi planove zasnovane na oceni rizika kako bi odredio prioritete aktivnosti interne revizije, koji su usaglašeni sa ciljevima organizacije.

2010. A1 – Plan angažovanja aktivnosti interne revizije mora da se zasniva na dokumentovanoj proceni rizika, koja se vrši bar jednom godišnje. U ovom procesu mora se uzeti mišljenje višeg rukovodstva i odbora.

2010. A2 – Izvršni rukovodilac revizije mora da identifikuje i razmotri očekivanja višeg rukovodstva, odbora i drugih interesnih strana u pogledu mišljenja i drugih zaključaka interne revizije.

2010. C1 – Izvršni rukovodilac revizije treba da odluči o prihvatanju predloženih savetodavnih angažovanja i na osnovu potencijalnog doprinosa tih angažovanja: unapređenju upravljanja rizicima, dodavanju vrednosti i unapređenju poslovanja organizacije. Prihvaćena angažovanja moraju biti uključena u plan.

2020 – Izveštavanje i odobravanje

- Izvršni rukovodilac revizije mora da dostavi višem rukovodstvu i odboru na razmatranje i odobrenje plan aktivnosti interne revizije i plan potreba za resursima, uključujući i sve značajne promene koje su se u međuvremenu desile. Izvršni rukovodilac revizije, takođe, mora da izvesti o efektima ograničenja resursa.

2030 – Upravljanje resursima

- Izvršni rukovodilac revizije mora da obezbedi da resursi interne revizije budu odgovarajući, dovoljni i efektivno korišćeni na ostvarenju odobrenog plana.

2040 – Politike i procedure

- Izvršni rukovodilac interne revizije mora da ustanovi politike i procedure za usmeravanje aktivnosti interne revizije.

2060 – Izveštavanje višeg rukovodstva i odbora

- Izvršni rukovodilac revizije mora periodično da izveštava više rukovodstvo i odbor o svrsi, ovlašćenju i odgovornosti aktivnosti interne revizije, kao i izvršenju u odnosu na plan. Izveštaji takođe moraju sadržati informacije o značajnim izloženostima riziku i pitanjima kontrole, uključujući rizike od prevara, o području korporativnog upravljanja i drugim pitanjima prema potrebi ili zahtevu rukovodstva i odbora.

2100 – Priroda posla

- Aktivnost interne revizije mora da vrednuje i doprinosi unapređenju korporativnog upravljanja,

upravljanja rizikom i kontrolnih procesa, primenjujući sistematičan i disciplinovan pristup.

2110 – Korporativno upravljanje

- Aktivnost interne revizije mora da ocenjuje i daje odgovarajuće preporuke za poboljšanje procesa korporativnog upravljanja, radi ispunjenja sledećih ciljeva:

- Promovisanja odgovarajuće etike i vrednosti u organizaciji;
- Obezbeđenja efektivnog upravljanja poslovanjem u organizaciji i polaganja računa;
- Saopštavanja informacija o rizicima i kontroli odgovarajućim delovima organizacije;
- Koordinacije aktivnosti i razmene informacija između odbora, eksternih i internih revizora i rukovodstva.

2110. A1 - Aktivnost interne revizije mora da oceni dizajn, primenu i efektivnost ciljeva, programa i aktivnosti povezanih sa etikom.

2110. A2 – Aktivnost interne revizije mora da oceni da li upravljanje informacionom tehnologijom u organizaciji podržava organizacione strategije i ciljeve.

2130 – Kontrola

- Aktivnost interne revizije mora da pomaže organizaciji u održavanju efektivnosti kontrola tako što ocenjuje njihovu efektivnost i efikasnost i promoviše njihovo kontinuirano unapređivanje.

2130. A1 – Aktivnost interne revizije mora da oceni adekvatnost i efektivnost kontola u odgovoru na rizike u korporativnom upravljanju, poslovanju i informacionim sistemima, a u vezi sa:

- Pouzdanošću i integritetom finansijskih i operativnih informacija;
- Efikasnošću i efektivnošću operacija i programa;
- Zaštitom imovine;
- Usaglašenosti sa zakonima, propisima, politikama, procedurama i ugovorima.

2130. C1 – Interni revizori moraju da uključe saznanja o kontrolama, stečena tokom savetodavnih angažovanja u ocenu kontrolnih procesa u organizaciji.

2200 – Planiranje angažovanja

- Interni revizori moraju da izrade i dokumentuju plan za svako angažovanje, uključujući ciljeve tog angažovanja, obuhvat, raspored vremena i alokaciju resursa.

2210 – Ciljevi angažovanja

- Za svako angažovanje moraju biti uspostavljeni ciljevi.

2210. A1 – Interni revizori moraju da obave preliminarnu ocenu rizika koji su relevantni za aktivnost

koja se ispituje. Ciljevi angažovanja moraju da odražavaju rezultate ove ocene.

2210. A2 – Kada utvrđuju ciljeve angažovanja, interni revizori moraju da uzmu u obzir verovatnoću pojave značajnih grešaka, prevare, neusaglašenosti i ostalih izloženosti riziku.

2210. A3 – Za ocenu kontola potrebni su adekvatni kriterijumi. Interni revizori moraju da utvrde stepen u kome je rukovodstvo uspostavilo adekvatne kriterijume za ocenu ostvarenja ciljeva i zadataka. Ukoliko su kriterijumi adekvatni, interni revizori ih moraju primenjivati prilikom sopstvene procene. Ukoliko su kriterijumi neadekvatni, interni revizori moraju da rade sa rukovodstvom na razvijanju odgovarajućih kriterijuma.

2210. C1 – Ciljevi savetodavnih angažovanja moraju da obuhvate korporativno upravljanje, upravljanje rizicima i kontrolne procese u meri u kojoj je to ugovoreno sa klijentom.

2210. C2 – Ciljevi savetodavnih angažovanja moraju biti konzistentni vrednostima, strategijama i ciljevima organizacije.

2220 – Obuhvat angažovanja

- Utvrđeni obuhvat mora da bude dovoljan za ispunjenje ciljeva angažovanja. Obuhvat angažovanja mora da uključi razmatranje relevantnih sistema, evidencija, zaposlenih i fizičke imovine, uključujući i onu koja je pod kontrolom trećih lica.

2230 – Raspodela resursa angažovanja

- Interni revizori moraju da se opredele za odgovarajuće i dovoljne resurse za ostvarenje ciljeva angažovanja, na osnovu ocene prirode i složenosti svakog angažovanja, vremenskih ograničenja i raspoloživih resursa.

2310 – Identifikovanje informacija

- Da bi ostvarili ciljeve angažovanja interni revizori moraju da identifikuju dovoljne, pouzdane, relevantne i korisne informacije.

2420 – Kvalitet izveštavanja

- Izveštaji moraju da budu tačni, objektivni, jasni, koncizni, konstruktivni, potpuni i blagovremeni.

2421 – Greške i propusti

- Ukoliko konačan izveštaj sadrži značajnu grešku ili propust, izvršni rukovodilac revizije mora da dostavi ispravljenu informaciju svim stranama koje su primile prvobitni izveštaj.

2440 – Saopštavanje rezultata

- Izvršni rukovodilac revizije mora da saopšti rezultate odgovarajućim stranama.

2440. A1 – Izvršni rukovodilac revizije je odgovoran za izveštavanje o konačnim rezultatima onih strana koje mogu osigurati da je rezultatima posvećena dužna pažnja.

2440. A2 - Ukoliko pravnim, zakonskim ili regulatornim zahtevima nije drugačije utvrđeno, pre izdavanja rezultata stranama izvan organizacije, izvršni rukovodilac revizije mora da:

- Oцени potencijalni rizik po organizaciju;
- Kada je to primereno da se konsultuje sa višim rukovodstvom i/ili pribavi pravni savet;
- Kontrolise obelodanjivanje rezultata ograničavanjem njihove upotrebe.

2440. C1 – Izvršni rukovodilac revizije odgovoran je za izveštavanje korisnika o konačnim rezultatima savetodavnih angažovanja.

2440. C2 – Tokom savetodavnih angažovanja mogu biti identifikovani problemi u vezi sa korporativnim upravljanjem, upravljanjem rizicima i kontrolama. Uvek kada su ti problemi od značaja za organizaciju, oni moraju biti saopšteni višem rukovodstvu i odboru.

2450 – Sveobuhvatna mišljenja

- Kada se izdaje sveobuhvatno mišljenje ono mora uzeti u obzir očekivanja višeg rukovodstva, odbora i drugih interesnih strana i mora biti potkrepljeno dovoljnim, pouzdanim i korisnim informacijama.

2600 – Razrešenje prihvatanja rizika od strane višeg rukovodstva

- Kada izvršni rukovodilac revizije veruje da je više rukovodstvo prihvatilo nivo rezidualnog rizika koji može biti neprihvatljiv za organizaciju, on mora da raspravi to pitanje sa višim rukovodstvom. Ukoliko se odluka koja se tiče rezidualnog rizika ne donese, izvršni rukovodilac revizije mora izvestiti odbor radi razrešenja situacije.⁴³

5.3. Najbitniji okviri i smernice za obavljanje IT revizije

Mala grupa pojedinaca koji su se bavili sličnim poslovima – revizorskim kontrolama kompjuterskih sistema čiji je uticaj na rad organizacija sve više rastao, 1967. godine razgovarala je o potrebi za centralizovanim izvorom informacija i potrebi za savetovanjem u tom polju. 1976. godine Udruženje je formiralo obrazovni osnov kako bi preduzelo velike istraživačke napore da proširi znanje i vrednost IT upravljanja i kontrola u praksi.⁴⁴ Danas ovu asocijaciju odlikuje raznovrsnost, odnosno više od 100 000 članova koji žive i rade u više od 180 zemalja i pokrivaju različite profesionalne pozicije vezane za IT (revizori informacionih sistema, konsultanti, edukatori, stručnjaci za bezbednost informacionih sistema, interni revizori, direktori informatičke službe...). Oni rade u gotovo svim industrijskim kategorijama, uključujući finansije i bankarstvo, javno računovodstvo, državni i javni sektor, komunalne usluge i proizvodnju. Ova raznolikost omogućava članovima da uče jedni od drugih i razmenjuju različite stavove i gledišta o profesionalnim temama. To je jedna od prednosti ovog udruženja. ISACA je postala globalna organizacija za informaciono upravljanje, kontrole, bezbednost i reviziju. Njene standarde za

⁴³ global.theiia.org/standards-guidance/mandatory-guidance/pages/standards.aspx, preuzeto dana 15.09.2012.

⁴⁴ www.isaca.org/About-ISACA/History/Pages/default.aspx, preuzeto dana 15.09.2012.

reviziju i kontrolu informacionih sistema slede praktikanti i stručnjaci širom sveta.

Asocijacija ISACA (Information Systems Audit and Control Association) formirala je svoje okvire za reviziju informacionih sistema koji se sastoje iz 2 dela:

1. Standardi, smernice, alati i tehnike za profesionalce u oblasti revizije, davanja uverenja i kontrole informacionih sistema (Standards, Guidelines and Tools and Techniques for Auditing and Assurance and Control Professionals);
2. Upravljačke smernice za informacione i srodne tehnologije (COBIT – Control Objectives for Information and Related Technologies).

Prvi deo okvira obuhvata:

- Kodeks profesionalne etike za revizore informacionih sistema;
- Standarde, uputstva, alate i tehnike za reviziju i davanje uverenja u oblasti informacionih tehnologija;
- Standarde za upravljanje informacionim tehnologijama.

Struktura drugog dela okvira je sledeća:

- Kratak pregled (Executive Summary);
- Upravljačko – kontrolni okvir (Governance and Control Framework);
- Uputstva za rukovodioce (Management Guidelines);
- Upravljačke smernice (Control Objectives);
- Upravljačka praksa (Control Practices – Implementation Guide);
- Uputstva za revizore (Audit Guidelines – IT Assurance Guide).

5.4. Standardi ISO

Međunarodna organizacija za standardizaciju - ISO (International Organization for Standardization) je najveća svetska organizacija koja se bavi razvijanjem međunarodnih standarda. Osnovana je 1947. godine i od tada je objavila više od 19 000 međunarodnih standarda koji pokrivaju skoro sve aspekte tehnologije i poslovanja. Međunarodni standardi daju vrhunsku specifikaciju proizvoda, usluga i dobrih praksi, i pomažu da industrija postane još efikasnija i efektivnija i pomažu da se probiju barijere u međunarodnoj trgovini.

ISO međunarodni standardi obezbeđuju sigurnost, pouzdanost i dobar kvalitet proizvoda i usluga.

Za poslovanje, oni predstavljaju strateške alate koji smanjuju troškove minimiziranjem grešaka i povećavanjem produktivnosti. Pomažu kompanijama da pristupe novim tržištima i omoguće slobodnu i fer globalnu trgovinu.⁴⁵

5.4.1. ISO 9001 - Sistem menadžmenta kvalitetom (Quality Management System)

Ovaj standard sadrži zahteve za uređenje sistema menadžmenta kvalitetom. To je jedinstveni model za uređenje organizacija bez obzira na njihovu veličinu ili oblast delatnosti. Dakle ISO 9001 je međunarodni standard kojim je definisan model za uređenje organizacija na dobrovoljnoj osnovi.

Kratak pregled sadržaja standarda ISO 9001:2008

Sekcija 1: Opseg - Govori o standardu i kako se primenjuje na organizacije;

Sekcija 2: Normativna Referenca - Literatura i drugi dokumenti koji treba da se koriste zajedno sa standardima, (uključujući i - Sistemi menadžmenta kvalitetom - Osnove i rečnik);

Sekcija 3: Termin i definicije - Daje definicije pojmova koji se koriste u standardu;

Sekcija 4: Opšti zahtevi - Daje pregled opštih zahteva za ukupan sistem menadžmenta kvalitetom;

Sekcija 5: Odgovornost za upravljanje - Daje zahteve za upravljanje i njihovu uloga u sistemu menadžmenta kvalitetom;

Sekcija 6: Upravljanje resursima - Daje zahteve za resurse, uključujući osoblje, obuku, postrojenja i radnu sredinu;

Sekcija 7: Realizacija proizvoda - Daje zahteve za proizvodnju proizvoda ili realizaciju usluge, uključujući stavke kao što su planiranje, kupac povezani procesi, dizajn, nabavka i kontrola procesa;

Sekcija 8: Merenje, analiza i poboljšanje - Daje zahteve za praćenje procesa i unapređenje tih procesa.⁴⁶

⁴⁵ www.iso.org/iso/home/about.htm, preuzeto dana 15.09.2012.

⁴⁶ www.cimgrupa.eu/sr/iso-9001.aspx, preuzeto dana 19.09.2012.

Mnoge organizacije se opredeljuju za implementaciju kvaliteta prema standardu ISO 9001 jer na taj način pokazuju svojim kupcima odnosno klijentima da mogu obezbediti ujednačen kvalitet svojih proizvoda odnosno usluga. Organizacije koje su implementirale ovaj standard, tokom godina su ostvarile i bolje poslovanje, poboljšale performanse i profitabilnost.

Dva glavna razloga za implementaciju sistema menadžmenta kvalitetom prema zahtevima standarda ISO 9001:2008:

- Poboljšana efikasnost rada - Niži proizvodni troškovi zbog manje neusaglašenih proizvoda (manji škart), manja dorada, niža stopa odbacivanja i manji broj grešaka zbog unapređenih poslovnih procesa;
- Pristup novim tržištima - Neka tržišta zahtevaju sertifikovan sistem menadžmenta kvalitetom prema zahtevima standarda ISO 9001, dok na drugim tržištima se podrazumeva da sertifikovan sistem prema zahtevima ISO 9001 može predstavljati samo korist za preduzeća koja ga poseduju. Ovo je zaista glavni cilj u primeni ISO 9001.

Dobro dizajniran i implementiran sistem menadžmenta kvalitetom zasnovan na ISO 9001 dokazano obezbeđuje organizacijama sledeće prednosti:

- Smanjenje troškova i povećanje dobiti preko poboljšanja pouzdanosti proizvoda odnosno usluga; bolje kontrole tokova procesa; bolje dokumentovanje procesa; povećane svesti zaposlenih; smanjenja neusaglašenih usluga i odbijanja.
- Dobro definisane i dokumentovane procedure koje poboljšavaju konzistentnost izlaza;
- Kvalitet se stalno meri i poboljšava;
- Manje stope defekata;
- Nedostaci su identifikovani na vreme i ranije se ispravljaju po znatno nižoj ceni;
- Definisanjem procedura koje identifikuju aktuelne prakse koje su zastarele i neefikasne;
- Dokumentovane procedure su lakše za primenu postupaka od strane novih zaposlenih;
- Organizacije zadržavaju i povećavaju udeo na tržištu, povećavaju prodaju i prihode.

Prednosti standarda ISO 9001 takođe su i:

- *Povećana efikasnost:* Organizacije koje imaju implementiran sistem menadžmenta kvalitetom u skladu sa zahtevima standarda ISO 9001, imaju ostvareno povećanje kvaliteta i ostvarena je veća efikasnost (pre svega uređenjem i poboljšanjem poslovnih procesa).

- *Povećan prihod:* Organizacije koje imaju sertifikovan sistem kvaliteta prema zahtevima standarda ISO 9001 ostvarile značajna poboljšanja u oblasti produktivnosti i finansijskih performansi u odnosu na one organizacije koja nemaju sistem kvaliteta.
- *Moral zaposlenih:* Zaposleni su zadovoljni i motivisani kada postoje jasno definisane uloge i odgovornosti, odgovornosti upravljanja, obuke, propisane procedure, što čini neke od zahteva ovog standarda, i kada imaju jasnu sliku o tome kako njihova uloga utiče na kvalitet i ukupan uspeh organizacije.
- *Međunarodno priznanje:* Međunarodna organizacija za standardizaciju (ISO) je priznata u svetu kao najveći autoritet za upravljanje kvalitetom.
- *Činjenični pristup donošenju odluka:* Sistem menadžmenta kvalitetom prema zahtevima standarda ISO 9001, određuje jasna uputstva u vezi praćenja i merenja performansi poslovnih procesa. Ovo pomaže u prikupljanju informacija i donošenju odluka isključivo na osnovu podataka.
- *Dokumentacija:* Sistem menadžmenta kvalitetom prema zahtevima standarda ISO 9001, zahteva odgovarajuće dokumentovanje svih procesa, kao i evidenciju svih promena koje ste napravili, praćenje i evidentiranje grešaka ili odstupanja i bilo kojih neusaglašenosti. Na ovaj način se osigurava konzistentnost postupaka proizvodnje ili pružanja usluga koje pruža organizacija. Zbog toga zaposleni postaju odgovorniji. Vođenje dokumentacije daje garancije da će se identifikovati bilo koji uzrok, u slučaju pojave neprikladnog proizvoda ili usluge.
- *Doslednost:* Pošto su dokumentovani svi procesi, postoji minimalni obim grešaka. Proces, počevši od prava istraživanja i razvoja, koji pokrivaju proizvodnju i isporuku, su dobro dokumentovani. Čak i mala promena u bilo kom procesu treba da bude dokumentovana, da obezbedi da su promene dobro planirane i implementirane, i na najbolji mogući način da se obezbedi maksimalna efikasnost.
- *Zadovoljstvo klijenata:* Organizacije sada mogu lakše steći poverenje klijenata kako u zemlji tako i u inostranstvu, jer je ISO 9001 univerzalno prihvaćen standard. Sertifikovan sistem menadžmenta kvalitetom prema zahtevima standarda ISO 9001, osigurava efikasnost, doslednost i kvalitet proizvoda i usluga namenjen kompanijama koje na taj način obezbeđuju zadovoljstvo svojih kupaca odnosno klijenata.
- *Poboljšanje procesa:* Sistem menadžmenta kvalitetom prema zahtevima standarda ISO 9001 poseban značaj daje upravljanju, praćenju performansi i poboljšavanju poslovnih procesa, na osnovu prikupljenih podataka. Na osnovu prikupljenih činjenica tokom korišćenja dokumentacije i sprovedenih analiza, u procesima, omogućava se efikasno planiranje i sprovođenje svih neophodnih poboljšanja.⁴⁷

⁴⁷ www.cimgrupa.eu/sr/iso-9001.aspx, preuzeto dana 19.09.2012.

5.4.2. ISO 27001 - Sistem menadžmenta za bezbednost informacija (Information security management system)

Krajem dvadesetog veka informaciona tehnologija počinje svoj nagli razvoj sa kojim raste i njen uticaj na poslovanje preduzeća. Danas je toliko rasprostranjena da se informaciona rešenja koriste na svakom koraku u velikom delu ekonomski razvijenog sveta. Zbog njenog sve većeg uticaja na poslovanje, u uslovima visoke konkurentnosti veoma je bitno pružiti pravu i pravovremenu informaciju i održavati bezbednost informacija.

Standard ISO 27001 sadrži zahteve kojih se organizacija mora pridržavati kako bi uspostavila sistem za zaštitu informacija.

Britanski institut za standardizaciju BSI je početkom devedesetih godina postavio osnove za razvoj standarda za zaštitu informacija, a međunarodna organizacija za standardizaciju ISO u oktobru 2005. godine objavljuje standard ISO 27001 Informacione tehnologije – Sistemi upravljanja bezbednošću informacija – Zahtevi. Cilj standarda ISO 27001 je da osigura svu neophodnu zaštitu u vezi sa strogo poverljivim, verodostojnim i ograničenim za pristup informacijama, u cilju zaštite informacija i podataka "zainteresovanih strana". Zainteresovane strane kojima je ovaj sistem menadžmenta upućen mogu biti korisnici, razne vrste organizacija, zaposleni, saradnici, ali i društvo u širem smislu.

Standard ISO 27001 je koncipiran u pet poglavlja i to:

1. Sistem za upravljanje bezbednošću informacija (ISMS);
2. Odgovornost rukovodstva;
3. Interna provera ISMS;
4. Preispitivanje ISMS od strane rukovodstva i
5. Unapređenje ISMS.⁴⁸

Ovaj standard je usaglašen sa standardom ISO 9001 - Sistem upravljanja kvalitetom (Quality Management System) i u njemu je istaknut P-D-C-A (Plan-Do-Check-Act)⁴⁹ ciklus stalnog unapređivanja.

Plan-Planiraj deo sistema menadžmenta za bezbednost informacija sastoji se od politika, ciljeva i mera definisanim na unapređenju sistema u pogledu poboljšanja bezbednosti informacija. Na osnovu iskazanih zahteva korisnika i kroz uspostavljanje politike ISMS organizacija, dolazi faza uspostavljanja odnosno planiranja sistema za upravljanje bezbednošću informacija (ISO 27001). U ovoj fazi se sprovode i aktivnosti na definisanju kriterijuma za ocenu rizika, definiše se prilaz i metodologija za ocenu rizika, definišu se nivoi prihvatljivosti rizika i dr.

U sledećoj fazi (*Do - Uradi*) se sprovode akcije koje su planirane na osnovu odabranih upravljačkih mehanizama, ciljeva, izrada i primena plana snižavanja rizika, obuka za ostvarivanje svesti o primeni

⁴⁸ www.cimgrupa.eu/sr/iso-27001.aspx, preuzeto dana 19.09.2012.

⁴⁹ www.27000.org/iso-27001.htm, preuzeto dana 25.09.2012.

ISMS, upravljanje resursima ISMS.

Treća faza (*Check - Proveravanje*) je preispitivanje, merenje efektivnosti upravljačkih mehanizama, sprovođenja internih provera, ažuriranje planova za snižavanje rizika i dr. Ova faza se sastoji od praćenja i merenja, vrednovanja usaglašenosti, korektivnih i preventivnih akcija, upravljanja zapisima i internih provera sistema.

Poslednja faza, *Act (Deluj)* se sprovodi kroz uvođenje poboljšavanja, preuzimanje korektivnih i definisanje preventivnih mera, provera da li su sprovedena poboljšanja održiva itd.

Ovaj standard je posebno značajan za sve organizacije koje se bave uslugama vezanim za IT i potrebu za očuvanjem poverljivosti informacija. Prolongira princip sigurnosti, a korisnicima i ostalim zainteresovanim stranama skreće pažnju da je poslovna politika usmerena na stalna poboljšavanja u sistemu menadžmenta za bezbednost informacija i procesima pružanja usluga povezanih sa njim.

ISO 27001 predstavlja najbolju praksu za zaštitu i bezbednost informacija, a preduzeća koja odluče da ga implementiraju ostvaruju značajne koristi posebno u smislu poboljšanja svojih organizacionih performansi. Neke od ovih koristi su:

- kod potencijalnih ili postojećih korisnika se stvara poverenje u informacioni sistem u organizaciji čime se sa korisnicima ostvaruju poverljivije i čvršće relacije,
- obezbeđuje se da organizacija ima potpuno komplementaran sistem sa pravnom regulativom koja je vezana za informacione tokove jer se radi o standardu koji ima jasnu fleksibilnost u tom pravcu,
- obezbeđuje se sistem koji je usmeren na jasna kontinualna poboljšavanja procesa kojima se obezbeđuje informaciona sigurnost,
- ovim sistemom se ostvaruje transparentnost u pružanju usluga i menadžment na visokom nivou,
- obezbeđuje se i sistem koji je posebno orijentisan na upravljanje rizikom i kroz upravljačke aktivnosti, smanjenje rizika na dozvoljenu i minimalnu meru,
- obezbeđuje se naprednije razumevanje informacionih tokova u organizaciji čime se ostvaruje značajna dobit i u delu razumevanja i poboljšavanja poslovnih procesa,
- ostvaruje se mehanizam za jasno vidljive i opipljive dokaze o smanjenju troškova kroz bolji menadžment rizikom i smanjenje značaja uzročnika grešaka u organizaciji,
- ostvaruje se bolja analiza troškovi/dobiti,
- ostvaruje se lakši proces monitoringa kroz smanjenje radnih napora i primenu recimo sistema samo provere,
- moguće je povećati preventivno dejstvo kroz na primer smanjenje “uskih grla” u mreži ili kroz analizu zaštićenih i sačuvanih ranijih podataka o procesima,

- smanjenje incidenata i bolje razumevanje uzročnika,
- razvija se svest zaposlenih u smislu značaja zaštite informacija,
- obezbeđuje se jasan protok i raspoloživost informacija i dr.⁵⁰

SO/IEC 27001 sertifikovanje kao i ostala ISO sertifikacija obično imaju tri faze u procesu revizije:

1. faza – je preliminarni, neformalni pregled ISMS, kao npr. proveravanje postojanja i potpunosti ključne dokumentacije za politike informacione sigurnosti organizacije kao što su Statement of Applicability (SoA) i Risk Treatment Plan (Plan tretiranja rizika). Ova faza obično služi kako bi upoznala revizore sa organizacijom i strukturom.

2. faza - je detaljnija i spada u formalni segment revizije u kojem se nezavisno testira ISMS nasuprot zahteva ISO/IEC 27001. Revizori traže dokaze koji potvrđuju da menadžment sistem nezavisno funkcioniše, pravilno je dizajniran i implementiran i kao takav operativan. Revizije sertifikacije se obično obavljaju od strane Vodećih revizora ISO/IEC 27001 revizora. Uspešan “prolaz” ove faze rezultuje sertifikovanjem ISO/IEC 27001 standarda za postojeći ISMS.

3. faza - obično uključuje popratne provere ili revizije kako bi se potvrdilo da sistem i organizacija ostaje u skladu sa standardima. Održavanje sertifikacije podrazumeva periodične procene revizije koje potvrđuju da ISMS nastavlja da radi u skladu sa specifičnim zahtevima. Obično se revizije obavljaju godišnje (u dogovoru sa menadžmentom) ali mogu se obavljati i češće, pogotovo ako je sistem još u fazi sazrevanja.⁵¹

U savremenom poslovnom okruženju koje odlikuje brz rast količine informacija i znanja u organizacijama i u njihovoj komunikaciji sa korisnicima veoma je važno obezbediti poverenje korisnika kao i bezbednost informacija. ISO 27001 – Sistem menadžmenta za bezbednost informacija pomaže organizacijama u formiranju efektivnih i efikasnih sistema za menadžment u oblastima IT usluga. Samim tim organizacije koje primenjuju ove norme dobijaju konkurentsku prednost u odnosu na one koje ih ne primenjuju.

Primenom ISO 27001 obezbeđuje se odgovornost za bezbednost i zaštitu informacija na svim nivoima u organizaciji. Posledice izazvane lošim rukovanjem informacijama, kvarovima i izmenama izazvanim namerno ili greškom na sistemima u kojima su smeštene informacije, ili čak ubacivanjem virusa u nedovoljno zaštićene sisteme mogu da budu katastrofalne za neku organizaciju i da je dovedu do uništenja. Poznato je da, ukoliko informacije jedne organizacije nisu bezbedne, nije bezbedna ni njena budućnost i iz tih razloga je Međunarodna organizacija za standardizaciju ISO izdala standard ISO 27001 čijom primenom se postiže maksimalna zaštita informacija na svim kritičnim nivoima u organizaciji.

50 www.cimgrupa.eu/sr/iso-27001, preuzeto dana 29.09.2012.

51 www.itgovernance.co.uk/iso27001.aspx, preuzeto dana 29.09.2012.

5.4.3 ISO 27002 – Kodeks prakse za upravljanje sigurnošću informacija (Information technology - Security techniques - Code of practice for information security management)

Standard ISO 27002 je preimenovani standard ISO 17799, i on predstavlja kodeks za praksu informatičke bezbednosti. On u osnovi opisuje stotine potencijalnih kontrola i kontrolnih mehanizama koji se mogu primeniti u skladu sa smernicama u okviru standarda ISO 27001. Ovi standardi pomažu organizaciji da uspostavi validan Sistem upravljanja informacionom sigurnošću (Information Security Management System - ISMS) ISO 27002 i ISO 27001 standardi predstavljaju preporuke ili liste svih kontrola potrebnih za implementaciju u cilju smanjivanja sigurnosnog rizika na odgovarajući nivo. Standardi su jako popularni i često korišćeni a njihova implementacija može doprineti ispunjavanju glavnih ciljeva internih kontrola informacionog sistema (sigurnosni ciljevi, informacioni ciljevi kao i kontinuitet poslovanja).

Standard uspostavlja smernice i opšte principe za iniciranje, implementaciju, održavanje i unapređenje upravljanja informacionom sigurnošću u okviru organizacije. Kontrole sadržane u standardu imaju za cilj rešavanje specifičnih zahteva koji su identifikovani putem formalne procene rizika. Standard takođe ima za cilj da obezbedi vodič za razvoj organizacionih, bezbednosnih standarda i efektivnih praksi za upravljanje bezbednošću, kao i da pomogne da se izgradi poverenje u međuorganizacijske aktivnosti.⁵²

ISO/IEC 27002 standard obuhvata sledeće:

1. Procena rizika;
2. Sigurnosne politike – usmerene menadžmentu;
3. Organizacija informacione sigurnosti – upravljanje informacionom sigurnošću;
4. Menadžment imovine – popis i klasifikacija IT imovine;
5. Sigurnost ljudskih resursa – sigurnosni aspekti za ulazak, kretanje i izlazak zaposlenih;
6. Fizička sigurnost okoline – zaštita računara i računarskih komponenti;
7. Komunikacije i operacije upravljanja – upravljanje tehničkim sigurnosnim kontrolama u sistemima i mreži;
8. Kontrole pristupa – ograničavanje prava pristupa mrežama, sistemima i aplikacijama kao i podacima;
9. Razvoj, održavanje i adaptiranje informacionog sistema – sigurnost aplikacija;
10. Upravljanje sigurnosnim incidentima informacija – predvideti i reagovati na odgovarajući način na povrede informacione sigurnosti;
11. Upravljanje kontinuitetom poslovanja – zaštita, održavanje i oporavak kritičnih procesa i

⁵² www.27000.org/iso-27002.htm, preuzeto dana 02.10.2012.

sistema za poslovanje;

12. Usklađenost – osiguravanje usklađenosti s politikama informacione sigurnosti, standardima, regulativama i zakonima.

5.5. Sarbanes Oxley zakon i COSO okvir

Ovaj zakon nastaje 2002. godine na inicijativu američkih kongresmena Sarbanesa i Oxleya kao odgovor na korporativne skandale kao što su onaj u Enronu i WorldComu. Odredbe ovog zakona postale su obavezne za sve kompanije čije se deonice kotiraju na bilo kojoj berzi u USAu, a svrha ovog zakona je uvođenje delotvornog sistema internih kontrola nad procesom finansijskog izveštavanja. Ovim zakonom propisuju se nužne kontrole koje se moraju implementirati kako bi se rizik od netačnih i nepotpunih finansijskih izveštaja, odnosno njihovog pogrešnog prikazivanja sveo na prihvatljiv nivo. IT governance institute i ISACA su 2004. godine objavili preporuke o upotrebi informacionih tehnologija i informacionih sistema pri sprovođenju delotvornog sistema internih kontrola.

Cilj tog dokumenta odnosno skupa preporuka jeste dati odgovor na pitanje kakvo je stanje internih informatičkih kontrola u kompaniji, a zaključci i najčešći nalazi, su da informatičke kontrole imaju sveobuhvatan uticaj na ostale kontrole i ciljeve kontrola. Time informacione tehnologije i sistemi predstavljaju temelj delotvornog sistema internih kontrola poslovanja, odnosno, bez revizije delotvornosti kontrola, menadžment ne može imati garanciju da su finansijski izveštaji tačni, potpuni i da prikazuju stvarno finansijsko stanje kompanije.

Delotvornost SoX kontrola se meri istom mernom skalom kao i CobiT, ITIL, ili COSO norme (ocene zrelosti od 0 do 5). Osim toga Sarbanes-Oxley zakon u USA propisuje da su izvršni direktori odgovorni za sprovođenje sistema internih kontrola u poslovanju.⁵³

Ovaj zakon postavlja nove i poboljšava stare standarde za poslovanje svih računovodstvenih firmi i američkih deoničarskih društava. Zakon se ne odnosi na preduzeća koja su u privatnom vlasništvu. Po ovom zakonu osnovane su i nove, delimično javne agencije čiji posao je da nadziru, regulišu i vrše inspekciju i ukoliko je potrebno da kašnjavaju računovodstvene i konsultantske firme.

Američka komisija za nadzor finansijskih tržišta definiše COSO kao metodologiju za postizanje usklađenosti sa Sarbanes Oxley zakonom.

Osnovni principi unutrašnje kontrole zasnivaju se na dobro uspostavljenim organizacionim tehnikama i praksama, koje se izvode iz načina na koji rukovodstvo vodi određenu aktivnost, program i projekat i integrisane su u proces upravljanja. Primena unutrašnje kontrole je dinamična, pa se zato prakse zasnovane na ranijim okolnostima moraju menjati, kako bi se prilagodile izmenjenoj situaciji. Postoje različite metodologije i pristupi vezani za unutrašnju kontrolu, ali je najšire zastupljen COSO okvir. COSO predstavlja zajedničku definiciju internih kontrola, standarda i kriterijuma prema kojima preduzeća mogu proceniti kontrolne sastave.⁵⁴

53 www.sec.gov/news/studies/2009/sox-404_study.pdf, preuzeto dana 05.10.2012.

54 www.mf.gov.me/pretraga/94022/179629.html, preuzeto dana 05.10.2012.

Komitet sponzorskih organizacija COSO čine Američki Institut ovlašćenih javnih računovođa (CPA), Institut upravljačkih računovođa (IMA), Institut internih revizora (IIA), Međunarodni finansijski direktori i Američka asocijacija računovođa (AAA). COSO 1992. godine objavljuje okvir pod nazivom Unutrašnja kontrola - integrisani okvir koji internu kontrolu definiše kao proces sproveden od strane upravnog odbora, rukovodstva subjekta i drugih zaposlenih, osmišljen tako da pruža razumno uverenje vezano za ostvarivanje ciljeva preduzeća, i to u odnosu na 4 kategorije:

- Usklađenost sa važećim zakonima i propisima;
- Pouzdanost finansijskog i upravljačkog izveštavanja;
- Efektivnost i efikasnost poslovanja;
- Zaštita sredstava.⁵⁵

COSO definiše pet glavnih međusobno povezanih komponenti internih kontrola koje podržavaju zahteve koje postavlja zakon Sarbanes-Oxley.

Tih pet područja i njihov uticaj na odseke informacione podrške su sledeći:

- 1) Procena rizika. Pre nego što su primenjene potrebne kontrole, rukovodioci informacionih sektora moraju proceniti i shvatiti područja rizika koja utiču na kompletnost i ispravnost finansijskih izveštaja. Stoga se mora utvrditi kako se koriste sistemi preduzeća i koji je nivo tačnosti trenutno postojeće dokumentacije. Područja identifikovanog rizika definišu preostale četiri komponente COSO radnog okvira.
- 2) Kontrolno okruženje. Utiče na svest potrebe za kontrolom koju bi trebalo da imaju svi zaposleni u preduzeću i predstavlja osnovu svih drugih komponenti interne kontrole pružajući potrebnu strukturu. Činioci kontrolne okoline uključuju integritet, etičke vrednosti, znanja i sposobnosti zaposlenih, filozofiju uprave i operativni stil, odnosno način na koji uprava dodeljuje odgovornosti i autoritet upravljanja i organizuje i razvija ljudske resurse.
- 3) Kontrolne aktivnosti. To su politike i procedure koje osiguravaju da će uputstva uprave biti izvršena. One obezbeđuju preduzimanje potrebnih akcija kako bi se smanjili rizici ostvarenja ciljeva organizacije. Pojavljuju se u celoj organizaciji, na svim nivoima i funkcijama i uključuju niz aktivnosti u koja spadaju autorizacije, provere operativnih procedura, sigurnosti imovine i podele dužnosti. U informacionom okruženju, kontrolne aktivnosti tipično uključuju opšte kontrole, poput kontrola pristupa programima, promenama programa i zahvatima na računarskim sistemima.
- 4) Nadzor. Proces i raspored revizije trebaju biti razvijeni na taj način da primarno smanjuju područja visokog rizika unutar informacionih sistema. Zaposleni u informacionim odeljenjima

⁵⁵ www.mf.gov.me/pretraga/107135/Prirucnik-za-finansijsko-upravljanje-i-kontrole.html, preuzeto dana 05.10.2012.

trebali bi često vršiti interni nadzor. Ipak nadzori i revizije trebaju biti vršeni i od strane eksternih revizora po rasporedu koji odgovara nivoima percipiranog rizika. Za rezultate takvih revizija uprava mora imati jasnu odgovornost.

5) Informacija i komunikacija. Bez pravovremenih i tačnih informacija, rukovodioci informatičkih službi teško mogu proaktivno identifikovati i pratiti područja rizika. Moguć je i izostanak reakcije na novonastale probleme. Rukovodioci moraju pokazati razumevanje svih mera koje je potrebno preduzeti da bi se postigla uklađenost sa Sarbanes-Oxley zahtevima i načinima postizanja te usklađenosti.

COSO okvir naglašava da uspešno upravljanje poslovanjem nije moguće bez organizovanja efikasnog sistema internih kontrola, kojim se proverava delotvornost postupaka sprovođenja strategije poslovanja, ciljeva profitabilnosti poslovanja i upravljanja rizicima. Time je interna kontrola konačno dobila važno mesto u menadžerskim strukturama, a korporativno upravljanje rizicima postalo ključan prioritet savremenog vođenja poslova.

5.6. ITIL - Information Technology infrastructure library

ITIL je kreiran još pre 20 godina, tačnije kasnih 1980ih kada je britanska vlada zaključila da je kvalitet IT usluga pojedinih vladinih agencija nedovoljan i neujednačen. CCTA agencija (Central Computer and Telecommunications Agency) je kreirala ovaj okvir sa ciljem da struktuirala, standardizuje i ujednači IT sisteme, da klijentima poboljša upravljanje IT servisima a samim tim i njihovu efikasnost i delotvornost u ispunjavanju poslovnih ciljeva i poboljšanju profitabilnosti preduzeća. Pretežno se koristi u Evropi, najčešće u javnom sektoru za čije potrebe je i kreiran, ali isto tako se koristi i u privatnom sektoru, u velikim ili malim preduzećima i u centralizovanim ili distribuiranim poslovnim okruženjima.

ITIL predstavlja zbirku preporuka, uputstava, smernica. Vremenom smernice su proširene, unapređene i poboljšane, a okvir je tek nedavno zauzeo svoje mesto u praksi kao koristan i praktičan model u upravljanju IT servisima. U sebi objedinjuje smernice koje su bazirane na najboljim praksama menadžmenta IT usluga (pružanje, dostavljanje, podrška i upravljanje IT uslugama), odnosno instrukcije za pružanje kvalitetnih IT usluga i procedura, opreme i aktivnosti koje podržavaju IT.

ITIL je takozvani top-down pristup ili više orijentisan ka biznisu od strane IT menadžmenta koji stavlja naglasak na stratešku vrednost biznisa sa ITa i potrebu da “dostavi” njegove visokokvalitetne usluge. Kao dodatak tome ITIL pruža kompletne smernice i preporuke koje ciljaju na posao zaposlenih, funkcionisanje procesa i korišćenje informacionih tehnologija kao i pružanje kvalitetnih usluga.⁵⁶ Itil je dakle okvir pomoću koga preduzeća povećavaju kvalitet usluge prema svojim klijentima.

Uvođenjem ITIL preporuka i poboljšanjem procesa koje podržava IT, preduzeća i organizacije mogu da postignu:

- bolje iskorišćavanje izvora i sredstava;

⁵⁶ www.itrevizija.ba/okviri-it-revizije/itil, preuzeto dana 06.10.2012.

- povećanje konkurentnosti;
- smanjenje obima rada koji se ponavlja i otklanjanje nepotrebnog rada;
- poboljšanje kvaliteta projekata i završavanje projekata u kraćem vremenu;
- poboljšanje nivoa raspoložljivosti, pouzdanosti i bezbednosti usluga IT koje su od ključnog značaja za poslovanje;
- utemeljavanje investicija i troškova za obezbeđivanje kvaliteta usluge;
- obezbeđivanje usluga po meri potreba organizacije, stranaka i korisnika;
- dokumentovanje i posredovanje uloga i odgovornosti kod obezbeđivanja usluga;
- učenje iz ranijih iskustava;
- obezbeđivanje upotrebljivih pokazatelja funkcionalnosti i sposobnosti.⁵⁷

Na široku prihvatljivost i uspešnost ITIL sistema utiču tri ključna faktora.

Prvi je taj da je ITIL metodologija dostupna svima i da taj okvir ažurnim održavaju vladine, tj. neprofitne organizacije.

Drugi faktor uspeha ITIL-a je prihvaćenost ovog standarda od strane najvećih globalnih organizacija. Poslednji, a možda i najbitniji razlog uspešnosti je postojanje izuzetno velike količine poučnog materijala (web-sajtova i knjiga) za postizanje ciljeva koje ITIL postavlja.⁵⁸

Što se Itil sertifikata za fizička lica tiče postoje 3 stepena sertifikovanja.

Prvi stepen, ITIL Foundation Certificate, je neophodan za sticanje preostala dva ITIL sertifikata, ITIL Intermediate Certificate i ITIL Advanced Level Certificate. Posedovanje prvog sertifikata podrazumeva da osoba poseduje osnovno poznavanje ITIL standarda, pojmova i procesa. Osoba koja poseduje ITIL Intermediate Certificate poseduje znanje koje je potrebno za primenu ITIL okvira u organizaciji, dok treći sertifikat poseduju isključivo ITIL stručnjaci koji iza sebe imaju dugogodišnje iskustvo i brojne projekte.

⁵⁷ www.norips.org/itil-v3.html, preuzeto dana 08.10.2012.

⁵⁸ www.infotrend.hr/clanak/2012/2/poslovni-it-certifikati, preuzeto dana 08.10.2012.

5.7. COBIT – Kontrolni ciljevi za informacione i srodne tehnologije (Control Objectives for Information and Related Technologies)

COBIT je okvir koji propisuje ISACA (Information Systems Audit and Control Association) i organizacija ITGI (IT Governance Institute) sa ciljem da pomogne u upravljanju IT-jem. To je skup smernica i praksi koje pomažu menadžmentu da premosti razlike između kontrolnih zahteva, tehničkih pitanja i poslovnih rizika.

Prva verzija COBITa izdata je 1996. godine, a danas se koristi COBIT 5 verzija koja je objavljena u aprilu 2012. godine.

Osnovni zadatak COBITa je da istražuje, razvija, objavljuje i promoviše međunarodni skup opšte prihvaćenih ciljeva kontrole informacionih tehnologija za svakodnevno korišćenje od strane poslovnih menadžera, IT stručnjaka i stručnjaka za osiguranje. Ovaj okvir podržava upravljanje IT-jem tako što definiše i usaglašava poslovne ciljeve sa IT ciljevima i procesima. Poslovna orijentacija COBITa sastoji se od povezivanja poslovnih ciljeva sa IT ciljevima, pružajući pokazatelje i modele za merenje uspeha, identifikovanje poslovnih odgovornosti i IT procesa.⁵⁹

Primarni kontrolni ciljevi u COBITU dele se u 4 grupe:

1. Planiranje i organizacija;
2. Nabavka i sprovođenje (implementacija);
3. Isporuka i podrška;
4. Nadzor i evaluacija.

Ovaj okvir je na veoma visokom nivou i usklađen je sa drugim, detaljnijim IT standardima i dobrim praksama kao što su između ostalih i COSO, ITIL, ISO 27000. COBIT deluje kao integrator tih različitih okvira i smernica tako što sumira ključne ciljeve pod jedan okvir koji povezuje modele dobrih praksi sa upravljanjem i poslovnim zahtevima.

5 ključnih stvari o COBIT 5 verziji su:

1. Pomaže da se dobije više vrednosti iz podataka i tehnologije kroz poboljšano upravljanje IT vezanim rizicima, poboljšanje komunikacije između poslovnog sektora i ITa, poboljšanje IT isporuke poslovnih ciljeva, smanjivanje IT troškova i bolju poslovnu konkurentnost;
2. Bavi se potrebama poslovnih ljudi i IT lidera s poslovnim okvirom za upravljanje i menadžment korporativnog IT-a;
3. Bavi se potrebama deoničara kroz celu kompaniju i razjašnjava ciljeve za mnogo efektivnije donošenje odluka;

⁵⁹ www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx, preuzeto dana 10.10.2012.

4. Pruža end-to-end standard koji integriše druge pristupe i standarde i bavi se ostalim područjima kompanije;
5. Predstavlja “kolektivnu mudrost” više od 95 globalnih stručnjaka.⁶⁰

Ovaj okvir pomaže u postavljanju pravih pitanja i osigurava povraćaj investicija informacionih i tehnoloških sredstava.⁶¹

Uspesne organizacije razumeju prednosti informacione tehnologije, prepoznaju zavisnost mnogih poslovnih procesa od IT-a, koristi efektivnog upravljanja rizicima, potrebu da se pridržava rastućim regulatornim zahtevima usklađenosti. COBIT je okvir orijentisan na IT upravljanje i pruža set alata za podršku menadžmentu. Omogućava jasnu politiku razvoja i dobre prakse za IT kontrolu u organizacijama. Potencira usaglašenost, pomaže organizacijama da povećaju vrednost i pojednostavljuje implementaciju COBIT okvira.

COBIT:

- Poboljšava IT efikasnost i efektivnost;
- Pomaže IT-u da razume potrebe poslovanja;
- Dobrim praksama ispunjava poslovne potrebe što je efikasnije moguće;
- Obezbeđuje usklađivanje poslovanja i IT-a;
- Pomaže rukovodiocima da razumeju i upravljaju IT investicijama;
- Obezbeđuje da se IT resursi koriste odgovorno, a IT rizicima adekvatno upravlja.⁶²

Prednosti korišćenja COBIT-a uključuju:

- Zajednički jezik za direktora, menadžment i IT profesionalce;
- Bolje razumevanje kako biznis i IT mogu da rade zajedno za uspešno pružanje IT inicijativa;
- Poboljšana efikasnost i optimizacija troškova;
- Smanjenje operativnog rizika;
- Slobodan razvoj politike;

⁶⁰ www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx, preuzeto dana 12.10.2012.

⁶¹ www.itrevizija.ba/okviri-it-revizije/cobit, preuzeto dana 12.10.2012.

⁶² www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx, Cobit 4.1 Framework, preuzeto dana 15.10.2012.

- Efikasnija i uspešnija revizija;
- Slobodno vlasništvo i odgovornosti na osnovu procesa orijencije.⁶³

Strategija poslovanja obuhvata poslovne ciljeve i odluke, način na koji se organizacija bori sa sve dinamičnijim promenama. Kompanijama je potrebna dobra IT strategija koja je povezana sa potrebama poslovanja, s' obzirom na sve veći značaj informacionih sistema na poslovanje preduzeća.

COBIT je okvir koji pomaže usklađivanju IT strategije sa poslovnom strategijom preduzeća, određivanju veze IT procesa, IT resursa i informacija prema organizacionim ciljevima i strategijama. On sadrži i ističe brojne preporuke i postupke koje organizacije treba da primenjuju kako bi odabrale odgovarajuću i što ekonomičniju IT strategiju.

⁶³ www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx, Cobit 4.1 Framework, preuzeto dana 15.10.2012.

6. REVIZIJSKI RIZIK I MATERIJALNOST

Revizor treba da upotrebi profesionalni sud da bi procenio revizijski rizik i projektovao postupke revizije, kako bi osigurao da taj rizik bude ograničen na prihvatljivo nizak nivo.⁶⁴

Revizijski rizik tj. rizik revizijskog angažmana sastoji se od inherentnog, kontrolnog i rizika detekcije. *Inherentni rizik* je podložnost nekog salda računa ili vrste transakcija na pogrešne iznose (greške) koje bi mogle biti materijalno značajne, pojedinačno ili kada se saberu sa greškama u drugim saldima ili vrstama pod pretpostavkom da nije bilo potrebnih internih kontrola.

Kontrolni rizik je rizik da pogrešan iskaz – greška koja bi se mogla pojaviti u nekom saldu računa ili vrsti transakcija i koja bi mogla biti pojedinačno značajna, ili kada se sabere sa greškama u drugim saldima ili vrstama transakcija, neće biti blagovremeno sprečena ili otkrivena i ispravljena primenom računovodstvenog i sistema interne kontrole.

Detekcioni rizik je rizik da dokazni postupci revizora neće otkriti grešku koja postoji u saldu računa ili vrsti transakcija, a koja bi mogla biti značajna, pojedinačno ili kada se sabere sa greškama u ostalim saldima ili vrstama transakcija.

Materijalnost se definiše od strane Odbora za međunarodne računovodstvene standarde u Okviru za sastavljanje i prikazivanje finansijskih izveštaja: Informacija je materijalno značajna ako bi njeno izostavljanje ili pogrešno prikazivanje moglo uticati na ekonomske odluke koje bi korisnici doneli na bazi finansijskih izveštaja. Materijalnost zavisi od veličine stavke ili greške prosuđene u specifičnim okolnostima njenog izostavljanja ili pogrešnog prikazivanja. Otuda materijalnost pre obezbeđuje prag ili tačku razgraničenja nego kvalitativnu karakteristiku koju informacija mora imati da bi bila od koristi. Procena o tome šta je materijalno je stvar profesionalnog prosuđivanja revizora.

Prilikom izrade plana revizije, revizor postavlja prihvatljiv nivo materijalnosti kako bi otkrio kvantitativna, materijalno pogrešna prikazivanja. Takođe treba da budu razmotreni i iznos i priroda pogrešnog prikazivanja. Revizor treba da razmotri mogućnost pogrešnog prikazivanja relativno malih iznosa koji bi kumulativno mogli imati materijalno značajan efekat na finansijske izveštaje. Revizor razmatra materijalnost i na opštem nivou finansijskih izveštaja i u odnosu stanja na pojedinačnim računima, vrste poslovnih događaja i obelodanjivanja.

Revizor treba da razmotri materijalnost kada:

- Određuje prirodu, vreme i obim revizijskih postupaka i
- Vrednuje efekte pogrešnih iskazivanja - materijalnost ima direktan uticaj na vrstu mišljenja.⁶⁵

Revizorovo razumevanje klijenta revizije i njegovog okruženja uspostavlja referencijalni okvir za svrhe planiranja revizije i profesionalno prosuđivanje u vezi procene rizika materijalne greške u finansijskim izveštajima kao i odgovora na te rizike tokom revizije. Postoji obrnuto proporcijalan odnos između

⁶⁴ www.icisa.cag.gov.in/Background%20Material/RISK%20ASST%20AND%20INTNL%20CONTROL%20ISA_400.pdf, International Standards on Auditing (ISA) 400, Risk assessment and internal control, preuzeto dana 16.09.2012.

⁶⁵ Prof. dr Milovan Stanišić, Prof. dr Kosana Vićentijević, “Revizijski zaključni izveštaj”, Univerzitet Singidunum, Beograd 2009. str. 6

materijalnosti i nivoa revizijskog rizika, tj. što je viši nivo materijalnog značaja to je niži nivo revizijskog rizika i obrnuto. Kada revizor određuje prirodu, vreme i obim postupaka revizije, treba da uzme u obzir ovaj odnos između materijalnog značaja i revizijskog rizika.

Revizorova procena materijalnosti i revizijskog rizika može biti različita u vreme inicijalnog planiranja angažmana u odnosu na vreme vrednovanja rezultata primene revizijskih postupaka. Ovo može biti slučaj zbog izmenjenih okolnosti ili zbog promena u saznanjima revizora na osnovu rezultata revizije. Kod ocene istinitosti i objektivnosti finansijskih izveštaja revizor treba da proceni da li su ukupna nekorigovana pogrešna iskazivanja koja su bila identifikovana u toku revizije, materijalno značajna. Ukupna nekorigovana pogrešna iskazivanja obuhvataju:

1. Pojedinačna pogrešna iskazivanja identifikovana od strane revizora, uključujući neto efekat nekorigovanih pogrešnih iskazivanja identifikovanih u toku revizije prethodnih perioda i
2. Najbolje revizorske procene ostalih pogrešnih iskazivanja koja ne mogu biti pojedinačno identifikovana.

Ako revizor zaključi da pogrešna iskazivanja mogu biti materijalno značajna, treba da razmotri mogućnost smanjenja revizijskog rizika proširenjem revizijskih postupaka ili zahtevanjem od rukovodstva klijenta revizije da koriguje finansijske izveštaje. Ako rukovodstvo klijenta revizije odbije da izvrši korekcije finansijskih izveštaja, a rezultati proširenih revizijskih postupaka ne omoguće revizoru da zaključi da ukupna nekorigovana pogrešna iskazivanja nisu materijalno značajna, revizor treba da razmotri odgovarajuću modifikaciju revizijskog izveštaja u skladu sa MSR 700 Izveštaj nezavisnog revizora o kompletnom setu finansijskih izveštaja opšte namene.

Osnovni problem kod merenja materijalnosti kada se klijent ne pridržava opšte prihvaćenih računovodstvenih principa obično predstavlja ukupna novčana greška u računima, u poređenju sa nekom osnovom. Greške moraju da se uporede sa nekom orijentacionom osnovom pre nego što se donese zaključak o materijalnosti nepoštovanja opšte prihvaćenih računovodstvenih principa. Neto osnove obuhvataju neto prihod, ukupnu aktivu, obrtna sredstva i obrtni kapital.

Na odluku korisnika finansijskih izveštaja može uticati i vrsta greške u finansijskom izveštaju. Sledeći aspekti mogu u većoj meri od većine drugih grešaka uticati na odluke korisnika i na mišljenje revizora:

- Transakcije su nelegalne i nepoštene;
- Stavka može materijalno uticati na neki budući period čak iako nije materijalna samo u odnosu na tekući izveštajni period;
- Stavka ima "psiho" efekat;
- Stavka može biti važna sa aspekta mogućih posledica koje proističu iz ugovorenih obaveza.

Veličina potencijalnih grešaka gde postoji ograničenje delokruga rada, važna je kod odlučivanja koju vrstu mišljenja koristiti – nekvalifikovani izveštaj, kvalifikovani izveštaj ili uzdržavanje od mišljenja. Po prirodi stvari teže je oceniti materijalnost potencijalnih grešaka koje potiču od ograničenja delokruga rada nego od nepoštovanja opšte prihvaćenih računovodstvenih principa.

6.1. Mere rizika

U praksi postoje brojni metodi koji mogu direktno da uključe rizik u analizu donošenja odluka.

Najčešći način za uključivanje rizika jeste dizajniranje indeksa, koji bi direktno održavao rizik, i koji je po definiciji inherentan investicionoj odluci.

Moderna teorija investicija definiše rizik, kao disperziju mogućih prinosa, preciznije kao odstupanja od očekivanih prinosa.

Najčešće korišćeni metodi jesu očekivani profit (aritmetička sredina) kao indikator – mera anticipirane profitabilnosti i varijansa, kao mera tj. indikator rizika.

1. Očekivani profit

Očekivana vrednost profitabilnosti projekta je:

$$E(x) = \sum_{i=1}^n p_i x_i$$

$E(x)$ – očekivana vrednost

x_i - i-ti mogući rezultat (profit, dobit)

p_i – verovatnoća i-tog rezultata x_i

n – broj mogućih rešenja

2. Varijansa kao mera rizika

Varijansa (standardna devijacija) meri disperziju očekivane vrednosti profita u odnosu na očekivanu vrednost profita $E(x)$. Varijansa se izračunava sledećom formulom:

$$\sigma^2(x) = E(x - E(x))^2 = \sum_{i=1}^n p_i (x_i - E(x))^2$$

Izračunavanjem varijanse dobija se standardna devijacija kao koren iz varijanse i kao mera je adaptibilnija od varijanse jer može da meri različite monetarne jedinice.

Pravilo za primenu varijanse je sledeće:

Investicija A je preferabilnija od investicije B, ako $\sigma^2 A > \sigma^2 B \rightarrow \sigma A > \sigma B$.

3. Kovarijansa

Mera do koje diverzifikacija utiče na stabilizaciju prihoda je funkcija relacije između dve slučajne varijable, a njihovo izračunavanje se vrši putem kovarijanse i koeficijenta korelacije.

Po definiciji kovarijansa dve varijable x i y se izražava kao :

$$101$$

$$\text{Cov}(x,y) = E(x - E_x)(y - E_y)$$

Ako je $\text{Cov}(x,y)$ veća od nule tada x i y simultano teže da prevaziđu njihove respektivne proseke ili da budu ispod njih. Ako je $\text{Cov}(x,y)$ manja od nule, tada se dešava disperzija, koja uslovljava da vrednosti x i y imaju suprotne tendencije čime je zadovoljen uslov investitora, a to je da izbor plasmana investicija ima negativnu kovarijansu prinosa u relaciji sa drugom investicijom, koja može biti plasirana na drugu granu – oblast industrije.

4. Koeficijent korelacije

Mera koja određuje pravac kovarijacija i veličinu kovarijacije između dve ili više varijabli naziva se koeficijent korelacije:

$$R(x,y) = \text{Cov}(x,y) / \sigma(x) \sigma(y)$$

Koeficijent korelacije vrednosno se pozicionira uvek u granicama $-1 \leq R(x,y) \leq +1$ i nezavisan je od jedinica mere. Kada je R između 0 i 1 onda je relacija između dva sredstva u investicionoj opciji pozitivna, što je bliža 1 sve je veća da bi za 1 bila perfektno pozitivna korelacija. Drugim rečima, relacija je linearna što znači da su a i b takve da u linearnoj jednačini zadovoljavaju uslov $y=a+bx$, $b > 0$. Suprotno, za relaciju $0 \leq R \leq -1$ relacija je negativna i što je manje R veća je negativna korelacija. Za $R = -1$, dobijamo perfektno negativnu korelaciju tj. formalno – matematički i to je $y=a+bx$, za $b < 0$.

5. Pravilo varijansa – sredina

Jedno od najpoznatijih pravila za evaluaciju investicija uveo je Harry Marković, jedan od osnivača Portfolio teorije, bazirajući svoju ocenu na očekivanom prihodu i varijansi. Pravilo “očekivana prinos varijansa” ili “sredina - varijansa” definiše se:

Projekat A će biti preferabilniji od projekta B, ako sadrži jedan od dva uslova i to:

- Očekivani prinos A je jednak ili veći od očekivanog prinosa B i ako je varijansa projekta A manja od varijanse projekta B.

ILI

- Očekivani prinos A je veći od očekivanog prinosa B i ako je varijansa projekta A manja ili jednaka varijansi projekta B.⁶⁶

U ovom pravilu spojena su dva indikatora i to indikator profitabilnosti (sredina) i indikator rizika (varijansa) u jedinstvenu meru relacije prinos – rizik.

66 Prof. dr Milovan Stanišić, Doc. dr Ljubiša Stanojević, “Evalvacija i rizik”, Univerzitet Singidunum, Beograd 2010. str. 175

6. Varijansa NSV kao mera rizika

Preduzeće prilikom donošenja odluke o projektu može primeniti dve metode: diskontovati očekivani novčani tok putem troškova kapitala, ili diskontovati ekvivalent izvesnosti sa nerizičnom interesnom stopom. Pošto kapitalno budžetiranje uključuje više perioda kao i zavisnost projekata, očekivana neto sadašnja vrednost mora biti zamenjena za očekivani profit kao adekvatniju meru profitabilnosti i analogno tome varijansa neto sadašnje vrednosti se neophodno primenjuje kao indikator rizika.

Pretpostavićemo da investicioni projekat uključuje trenutne novčane utroške praćene sa pozitivnim novčanim prilivom u naredne dve godine. Pod ovom pretpostavkom, očekivana NSV predloženog projekta je suma SV očekivanih neto novčanih tokova u 1-oj i 2-oj godini umanjene za inicijalnu investiciju I_0 .

$$NSV = \alpha x_1 + \alpha^2 x_2 - I_0$$

$$E(NSV) = \alpha E x_1 + \alpha^2 E x_2 - I_0$$

$E x_1$ - očekivana vrednost neto novčanog toka u prvoj godini,

$E x_2$ - očekivana vrednost neto novčanog toka u drugoj godini,

I_0 – inicijalna investicija

$\alpha = 1 / (1+r)$ – koeficijent kapitalizacije novčanih tokova u vremenu gde je r -nerizična interesna stopa.

$$E(NSV) = \text{očekivana NSV}$$

7. Merenje rizika putem koeficijenta varijacije

Može se reći da standardna devijacija i varijansa ponekad ne pružaju dovoljno odgovarajuću meru rizika greške. Da bi se prevazišli ovi nedostaci neki ekonomisti se zalažu za primenu koeficijenta varijacije.

$$c = \sigma / E$$

Koeficijent varijacije se koristi umesto standardne devijacije kao mera investicionog rizika. Primenom koeficijenta varijacije ne prevazilaze se sve poteškoće proistekle iz primene pravila sredina-varijansa.

6.2. Upravljanje rizikom

Prisustvo rizika ne može se neutralisati, pa pojedinci i preduzeća traže puteve njegovog rešavanja. Posledice ostvarenja rizika rešavaju se na nekoliko načina, od kojih su najvažniji sledeći:

1. Upravljanje rizikom izbegavanjem - Rizik se izbegava kada pojedinac ne želi da prihvati rizik. Ovo se postiže neangažovanjem u akciji koja može dovesti do rizika. Po svojoj filozofiji ovo je negativan pristup. Napredak pojedinca i napredak privrede je situacija rizika.
2. Upravljanje rizikom zadržavanjem - Pojedinac je suočen sa gotovo neograničenim nizom rizika, u većini slučajeva se ništa ne preuzima u vezi njih. Zadržavanje rizika može biti svesno i nesvesno. Ako se rizik ne proceni, on je nesvesno zadržan. Po pravilu, rizici koji se zadržavaju su oni koji rezultiraju relativno malim gubicima.
3. Upravljanje rizikom prenosom - Rizik se može preneti sa jednog pojedinca na drugog koji je više spreman da snosi rizik.
4. Upravljanje rizikom podelom - Rizici se dele u velikom broju slučajeva. Primer podele rizika je organizacija akcionarskog društva.
5. Upravljanje rizikom umanjnjem - Rizik se može umanjiti na dva načina, i to: sprečavanjem i kontrolom. Većina gubitaka se može nekim naporima sprečiti. Bezbednosni programi i mere za sprečavanje nastanka gubitaka najpoželjnije su sredstvo za upravljanje rizikom. Praktično je nemoguće sprečiti sve gubitke.

6.3. Upravljanje finansijskim rizikom

Rizik možemo posmatrati dvojako. S' jedne strane, kao mogućnost da pretrpimo gubitak usled realizacije nepovoljnog događaja, a sa druge strane kao mogućnost da propustimo povoljnu priliku i ostvarimo neplanirane dobitke.⁶⁷

Upravljanje finansijskim rizikom je proces kojim se organizacija priprema da na najbolji mogući način preuzme rizik. Kada se biznis dobro vodi, kada se rizikom dobro upravlja, može se zaključiti da je biznis - uključujući tu i neprofitne organizacije, zapravo preuzimanje rizika. Sve organizacije akumuliraju resurse i investiraju ih u nesigurne poduhvate.

Uspešna organizacija preuzima rizike koji su neophodni za postizanje njenih ciljeva, a ostale izbegava. Sve organizacije se bave ulaganjem kapitala u rizične poslove da bi iz tih poslova ostvarile korist za sebe. Ovo se odnosi i na finansijske institucije, vladine organizacije, korporacije i neprofitne organizacije. Sve one imaju ciljeve, i sve raspoređuju resurse da bi težile tim ciljevima. Zbog činjenice

⁶⁷ Dr Jozefina Beke Trivunac, Jelena Vučinić i dr., Interna revizija – upravljanje, rizici, kontola, Institut za ekonomiku i finansije, Beograd 2012.godina, str. 45

da se sve organizacije suočavaju sa nesigurnošću, pri postizanju ciljeva, sve se suočavaju i sa rizikom. Preduzetničko upravljanje rizikom je zapravo preuzimanje rizika na najbolji način. Od 1990-tih ovo je postalo ključno pitanje zato što su organizacije počele da trpe velike gubitke – vrlo često zbog rizičnih situacija koje uopšte nisu trebale da se dese i na koje niko nije računao.

U prošlosti kompanije su mogle pretrpeti gubitke ili bankrotirati, ali ono što ih je dovelo u tu situaciju su makroekonomski faktori – konkurencija, pogrešno vođenje, ili negativne ekonomske prilike. Danas pojedinac može uzeti telefon i staviti milijarde dolara u rizičan poduhvat. To je ono što je novo i upravo zbog toga, proučavanju rizika i upravljanju rizikom posvećuje se sve veća pažnja.

Problem nisu finansijski alati već ljudi koji ih koriste. Za razliku od mnogih finansijskih alata, koji su novijeg datuma problem ljudi koji se ponašaju naivno ili neodgovorno oduvek je postojao. U prošlosti rizici su bili mali, tako da su mogući gubici bili ograničeni, i pojedinci su mogli izgubiti posao. Danas ljudi preuzimaju rizik istog tipa, ali gubici su porasli. Ne jača samo tržišni rizik. Sklapanjem pogrešnog ugovora povećavaju se i kreditni rizik, rizik likvidnosti, poslovni rizik i pravni rizik. Organizacije su fokusirane na sve ovo. Kroz preduzetničko upravljanje rizikom one traže razumna rešenja – ne zato što je ovo nov problem, već zato što su posledice neuspeha postale enormne. Osobe koje se bave upravljanjem i regulisanjem finansija podstiču tržišnu razmenu.

Svesni snage rizika oni teže:

- da otkriju listu mogućih vrsta rizika,
- da promovišu upravljanje korporativnim rizikom,
- da obezbede osiguranje, odnosno, da organizacije imaju dovoljno kapitala za rizik koji preuzimaju i
- da smanje sistemski rizik (odnosno rizične događaje koji mogu ugroziti poslovanje preduzeća kao organizacionog sistema).

Konačno, organizacije upravljaju rizikom zato što je to činilac dobrog poslovnog osećaja. Danas se aktivno donose odluke kojima se menjaju način i preuzimanja rizika. Implementiraju se inovativne procedure, instaliraju nove tehnologije, aktivno se restrukturiše korporativna kultura, da bi se na što bolji način prihvatio rizik. Izvršavanje aktivne strategije preduzetničkog upravljanja rizikom nije lako i različito je za svaku organizaciju.

6.4. Uloga interne revizije u procesu upravljanja rizikom

Standard 2120 – Upravljanje rizikom, jasno definiše ulogu interne revizije u procesu upravljanja rizikom: “Aktivnost interne revizije mora da procenjuje efektivnost i doprinosi poboljšanju procesa upravljanja rizikom”.

Aktivnost interne revizije mora da ocenjuje izloženost riziku koji je povezan sa korporativnim upravljanjem, poslovanjem i informacionim sistemima, a u vezi sa:

- Pouzdanošću i integritetom finansijskih i operativnih informacija;
- Efikasnošću i efektivnošću operacija i programa;
- Zaštitom imovine;
- Usaglašenosti sa zakonima, propisima, politikama, procedurama i ugovorima.

Aktivnost interne revizije mora da ocenjuje mogućnost pojave prevara i načina na koji se u organizaciji upravlja rizikom od prevara. Kada pomažu rukovodstvu u uspostavljanju ili unapređenju procesa upravljanja rizikom, interni revizori moraju da se suzdrže od preuzimanja bilo kakve rukovodeće odgovornosti za upravljanje rizikom.⁶⁸

Veoma je važno razdvojiti odgovornost rukovodstva i odgovornost interne revizije u sistemu upravljanja poslovnim rizicima tako da nezavisnost i objektivnost internih revizora ne bude ugrožena. Revizori su odgovorni za obavljanje sledećih aktivnosti:

- Pružanje uverenja o procesima upravljanja rizikom;
- Pružanje uverenja da se rizici korektno procenjuju;
- Procenjivanje odnosno vrednovanje procesa upravljanja rizikom;
- Procenjivanje izveštavanja o upravljanju rizicima;
- Ispitivanje upravljanja ključnim rizicima.

U poslove interne revizije takođe spadaju usluge konsaltinga kako bi pomogli rukovodstvu u upravljanju rizicima i organizacijom, a te usluge obuhvataju:

- Pomoć pri prepoznavanju i proceni rizika;
- Usmeravanje rukovodstva da reaguje na rizike;

68 global.theiia.org/standards-guidance/mandatory-guidance/pages/standards.aspx, preuzeto dana 19.10.2012.

- Koordinacija aktivnosti upravljanja poslovnim rizicima;
- Izrada konsolidovanih izveštaja o rizicima;
- Održavanje i razvoj okvira za upravljanje poslovnim rizicima;
- Rukovođenje procesom uspostavljanja sistema upravljanja poslovnim rizicima;
- Razvoj strategija upravljanja rizikom koje konačno odobrava upravni odbor.

Interna revizija ne sme prihvatati poslove koji bi ugrozili njenu nezavisnost i objektivnost, odnosno poslove koji su u nadležnosti rukovodstva, a u te poslove spadaju:

- Određivanje obima prihvatljivosti rizika;
- Nametanje procesa upravljanja rizikom;
- Status jedinog organa koji rukovodstvu pruža uveravanje da se rizicima efektivno upravlja;
- Odlučivanje o načinu reagovanja na rizike;
- Uvođenje kontrola nad rizicima umesto rukovodstva;
- Polaganje računa za upravljanje rizicima.

Određivanje nivoa rizika koji je prihvatljiv za preduzeće je obaveza menadžmenta, dok interna revizija svojim predlozima i korisnim informacijama stečenim nezavisnom procenom, menadžmentu pomaže u donošenju ove odluke.

Veliku ulogu u poslovima interne revizije igra upravo procena i upravljanje rizicima. Dobar sistem korporativnog upravljanja podrazumeva postojanje interne revizije u organizaciji. Njena uloga je da pruži upravi objektivno uveravanje o efektivnosti svih aktivnosti u organizaciji koje imaju za cilj da obezbede da se poslovnim rizicima upravlja na odgovarajuć način i da sistem internih kontrola deluje efektivno.⁶⁹

⁶⁹ uirs.rs/index.php?option=com_content&view=article&id=43:-2008&catid=32:2008-08-25-19-18-10&Itemid=40 , Bilten Novembar 2008. (Informativno-teoretski list "Udruženja internih revizora Srbije"), preuzeto dana 20.10.2012.

6.5. ERM pristup u upravljanju rizikom

Koncept ERM (Enterprise Risk Management) razvijen je sredinom 90-ih godina u industrijama sa menadžerskim fokusom. Potreba za nastankom ERM-a javlja se zbog mišljenja da ne treba praviti razliku između čistih (rizici koji rezultiraju gubitkom ili bez gubitaka, ali ne postoji mogućnost dobitaka) i spekulativnih rizika (postoji verovatnoća nastajanja i gubitaka i dobitaka), da upravljanje rizikom treba posmatrati kao opštu funkciju menadžmenta, kao i zbog shvatanja da je tradicionalno upravljanje rizikom orijentisano na zaštitu od gubitaka, ali ne i od neizvesnosti.

Poslednjih godina stvaraju se specijalizovane grane upravljanja rizikom uključujući projekte, energiju, finansije, operativne rizike i kliničko upravljanje rizicima. Takođe organizacije povećavaju zahteve za širim pristupima rizicima. Kao odgovor na ove zahteve javlja se Enterprise Risk Management – ultimativni pristup upravljanja rizicima, a COSO objavljuje okvir ERM 2004. godine. ERM je sistemski, integrisani pristup u upravljanju svim rizicima koji su prisutni u organizaciji, u cilju zaštite i poboljšanja vrednosti preduzeća. ERM pristup pokriva sve rizike i razmatra gledište da je većina rizika međusobno povezana, na osnovu činjenice da dva ili više rizika mogu imati uticaj na istu aktivnost ili cilj.

Enterprise Risk Management je proces koji se koristi od strane upravnog odbora organizacije, menadžmenta i ostalog osoblja, primenjen širom preduzeća u postavkama strategije, dizajniran kako bi se identifikovali potencijalni događaji koji bi mogli uticati na organizaciju, kreiran za upravljanje rizicima u skladu sa sklonošću prema riziku kako bi se pružilo razumno osiguranje u pogledu ostvarivanja ciljeva preduzeća.⁷⁰

Definicija reflektuje određene temeljne koncepte kao što su:

- Proces koji je u toku i teče kroz preduzeće;
- Izvršava se od strane ljudi na svim nivoima organizacije;
- Uključen je u postavkama strategije;
- Primenjuje se kroz celo preduzeće, na svakom nivou i u svakoj jedinici, i zahteva portfolio rizika na organizacionom nivou;
- Dizajniran radi identifikacije potencijalnih događaja koji, ako se dese, mogu ozbiljno uticati na organizaciju;
- U stanju je pružiti razumno uverenje organizacijskom menadžmentu i upravi direktora;
- Usmeren je na postizanje ciljeva u jednoj ili više pojedinačnih, preklapajućih kategorija.⁷¹

70 upravljanjerizicima.com/definicija-erma/3.1.4, preuzeto dana 20.10.2012.

71 upravljanjerizicima.com/definicija-erma/3.1.4, preuzeto dana 20.10.2012.

ERM se sastoji od osam međusobno povezanih komponenti. One su izvedene iz načina prema kome menadžment upravlja preduzećem i integrisane sa procesom upravljanja. ERM nije strogo serijski proces gde jedna komponenta utiče samo na sledeću, već bilo koja komponenta može uticati na drugu. Te komponente su:

- 1) *Interno okruženje* – obuhvata karakteristike organizacije i temeljno određuje načine na koje se posmatraju rizici, uključujući filozofiju upravljanja rizicima, sklonost riziku, integritet i etičke vrednosti, kao i okruženje u kojem deluju.
- 2) *Postavljanje ciljeva* – ciljevi moraju postojati pre nego što menadžment identifikuje potencijalne događaje koji utiču na njihovo ostvarenje. ERM osigurava da menadžment komponuje proces za postavljanje ciljeva i da izabrani ciljevi podržavaju misiju, te da su u skladu sa odredbama sklonosti riziku.
- 3) *Identifikacija događaja* – interni i eksterni događaji koji utiču na ostvarivanje ciljeva moraju biti identifikovani uz pravljenje razlike između rizika i mogućnosti. Prilike se razmatraju ponovo kroz strategiju menadžmenta ili ciljeve uspostavljene kroz proces ERM-a.
- 4) *Procena rizika* – rizici se analiziraju s obzirom na verovatnoću i uticaj, kao osnovu za određivanje načina kojim trebaju biti upravljani. Rizici se procenjuju preko inherentne i rezidualne osnove.
- 5) *Odgovor na rizik* – menadžment bira metodu odgovora na rizike – izbegavanje, prihvatanje, smanjenje ili deljenje rizika, razvijajući time skup akcija kako bi se uskladili rizici sa prihvaćenim nivoom tolerancije i sklonosti riziku.
- 6) *Kontrolne aktivnosti* – politike i procedure se uspostavljaju i sprovode kako bi se osiguralo efikasno sprovođenje odgovora na rizike.
- 7) *Informacije i komunikacija* – relevantne informacije su identifikovane, pohranjene i dostavljene u formi i roku koji omogućavaju osoblju da ispunjava svoje odgovornosti i obaveze. Efikasna komunikacija se takođe pojavljuje u širem smislu i teče u svim pravcima kroz organizaciju.
- 8) *Monitoring* – ukupnost primene ERM-a se prati i modifikuje po potrebi. Nadzor se ostvaruje kroz tok aktivnosti upravljanja ili odvojenom evaluacijom, ili na oba načina.⁷²

ERM je u nadležnosti upravnog odbora. ERM pomaže menadžmentu da postigne performanse i ciljeve profitabilnosti značajne za poslovanje uz sprečavanje gubitka resursa. Ovaj pristup osigurava efektivno izveštavanje u skladu sa zakonima i propisima, kao i izbegavanje narušavanja subjektive reputacije i pratećih posledica. Možemo reći da ERM pomaže subjektu da ispuni svoje zadatke i da izbegava “zamke” i iznenađenja na putu ka ostvarivanju postavljenih ciljeva.

⁷² www.upravljanjerizicima.com/komponente-erma/3.1.6, preuzeto dana 20.10.2012.

ERM obuhvata:

- Usklađivanje strategije i apetita za rizicima - Menadžment razmatra apetit za rizik u evaluaciji strateških alternativa, postavljanje ciljeva i razvoj mehanizama za upravljanje rizicima;
- Jačanje odluka kroz odgovore na rizike – ERM daje strogi pristup identifikacije i selekcije između alternativa odgovora na rizike –izbegavanje, smanjenje, deljenje i prihvatanje rizika;
- Smanjenje operativnih iznenađenja i gubitaka – Entiteti dobijaju poboljšane sposobnosti da identifikuju potencijalne događaje i uspostave odgovore na njih smanjujući iznenađenja i pripadajuće troškove ili gubitke;
- Identifikacija i upravljanje višestrukim i zajedničkim rizicima preduzeća – Svako preduzeće se suočava sa bezbroj rizika koji utiču na različite delove organizacije. ERM olakšava pružanje delotvornog odgovora na međusobne uticaje kao i integrisane odgovore na višestruke rizike;
- Iskorišćavanje prilika – Uzimajući u obzir čitav niz potencijalnih događaja menadžment je postavljen za identifikaciju i proaktivnu realizaciju prilika;
- Poboljšanje raspoređivanja kapitala – Dobijanje snažne informacije o riziku omogućava menadžmentu da efikasno proceni ukupne potrebe kapitala i poboljša alokaciju kapitala.⁷³

Neke od prednosti korišćenja ERM koncepta jesu bolje razumevanje ključnih rizika i njihovih širih posledica, veća fokusiranost na pitanja koja su zaista bitna, smanjena su iznenađenja ili krize, veća izvesnost u ostvarivanju ciljeva, konsolidovano izveštavanje o potpuno različitim rizicima od strane odbora, posedovanje više informacija pri donošenju odluka i prihvatanju rizika, veći interni fokus na bavljenje pravim stvarima na pravi način i dr.⁷⁴

⁷³ upravljanjerizicima.com/uvod-u-coso-erm/3.1.2, preuzeto dana 20.10.2012.

⁷⁴ Dr Jozefina Beke Trivunac, Jelena Vučinić i dr., Interna revizija – upravljanje, rizici, kontola, Institut za ekonomiku i finansije, Beograd 2012.godina, str. 48

6.6. Upravljanje IT rizicima

Organizacije koje se u svom poslovanju oslanjaju na informacione sisteme, koje imaju potrebu za obradom masovnih transakcija i kontinuirane dostupnosti IT servisa, upravo ove organizacije su najviše izložene rizicima informacionih sistema. Istraživanje kompanije KPMG pokazuje da se preduzeća često suočavaju sa hakerskim napadima, virusima, sa odavanjem poverljivih podataka, ugrožavanjem bezbednosti informacionih sistema i špijunažom što dovodi do značajnih gubitaka. Kako se bez nadzora stanje pogoršava, uspostavljanje adekvatnih IT kontrola je krucijalno za borbu sa IT rizicima.

Primeri IT rizika:

- Oslanjanje na sisteme i programe koji netačno obrađuju podatke;
- Neuautorizovan pristup podacima;
- Kršenje pravila podele dužnosti;
- Propust da se naprave neophodne izmene u sistemima ili programima;
- Potencijalni gubitak ili nemogućnost pristupa podacima, softveru ili hardveru;
- Nedostupnost potrebnih ljudskih resursa.⁷⁵

Upravljanje rizikom treba da obuhvati celokupni informacioni sistem organizacije i sve IT resurse. To je kontinuirani proces upoređivanja procenjenih rizika s prednostima i troškovima predloženih mera u skladu s poslovnim ciljevima.

Ključne faze procesa upravljanja rizicima obuhvataju:

- Planiranje - Priprema za uvođenje procesa upravljanja rizicima unutar koje se definišu ciljevi koje proces mora ispuniti, određuje opseg procesa, prikupljaju informacije o pređašnjim neželjenim događajima i incidentima unutar sistema pa se određuju granice prihvatljivih rizika.
- Identifikacija pretnji i procena rizika - Faza u kojoj se identifikuju svi resursi ključni za funkcionisanje sistema i procenjuje na koji način realne pretnje utiču na njihovo kompromitovanje. Procenom ostvarivanja pojedine pretnje dolazi se do definisanja konačnog rizika za ispravno i neprekinuto funkcionisanje sistema. Organizacija treba da utvrdi nivo rizika kojem je informacioni sistem izložen i da predloži zaštitne mere kako bi rizik bio smanjen na prihvatljiv nivo. Kako bi se utvrdila verovatnoća pojave nekog štetnog događaja, potrebno je

⁷⁵ www.infotech.org.rs/blog/download-sekcija/, KPMG, IT kontrole i upravljanje rizicima informacionih sistema, preuzeto dana 21.10.2012.

analizirati pretnje informacionom sistemu zajedno sa ranjivostima i kontrolama koje su primenjene. Uticaj se odnosi na prirodu i veličinu štete koju pretnja može uzrokovati ako iskoristi ranjivost.

Procena rizika informacionih sistema trebalo bi da obuhvati sledeće korake:

1. Analiza karakteristika sistema;
 2. Identifikacija mogućih pretnji;
 3. Identifikacija mogućih ranjivosti;
 4. Analiza trenutnog sistema kontrole;
 5. Određivanje verovatnoće;
 6. Analiza uticaja na informacioni sistem;
 7. Utvrđivanje rizika;
 8. Predlaganje korektivnih i zaštitnih mera.
- Preporuke za smanjivanje rizika - Preporuke se temelje na analizi postojećih mera za smanjivanje rizika pa se procenjuje koje od njih su prihvatljive, a koje je potrebno zameniti ili nadograditi. Takođe, u slučajevima kada umanjivanje rizika nije finansijski opravdano, razmatraju se opcije za izbegavanje ili prebacivanje rizika.

U osnovne mogućnosti smanjivanja identifikovanih rizika spadaju:

1. Izbegavanje rizika;
2. Ograničavanje rizika;
3. Prenosjenje rizika

Pri odabiru bilo koje od ovih mogućnosti potrebno je uzeti u obzir poslovne ciljeve i zadatke kao i potrebu za očuvanjem osnovnih principa sigurnosti informacionog sistema.

Smanjivanje rizika obuhvata sledeće korake:

1. Utvrđivanje prioriteta;
2. Procenu zaštitnih mera;
3. Sprovođenje cost - benefit analize;
4. Izbor mera za smanjenje rizika;
5. Raspodela odgovornosti;
6. Izrada plana sprovođenja;
7. Utvrđivanje rezidualnih rizika.

- Odabir sigurnosnih mera - Rizici koji nisu adresirani postojećim merama, a odlučeno je da se moraju umanjiti, tretiraju se odabirom novih tehničkih ili proceduralnih sigurnosnih mera. U ovoj fazi biraju se konkretne mere, određuje se budžet i rokovi njihove implementacije.
- Konstruisanje i implementacija sigurnosnih mera – Stručnjaci treba da konstruišu i implementiraju sve sigurnosne mere vezane za IT sisteme i na taj način umanje sve rizike koji im prete.
- Provera uspešnosti implementiranih mera - Osim konstruisanja i implementacije sigurnosnih mera, izrađuju se i procedure za testiranje mera i merenje njihove uspešnosti kroz duži vremenski period.

7. LAŽNO FINANSIJSKO IZVEŠTAVANJE – ISTRAŽIVANJE ZA 2012. godinu

Revizijska smernica - Odgovornost revizora kod otkrivanja prevare i izveštavanja o prevari i drugim nezakonitim postupcima - pravi razliku između sledećih kategorija:

- Omaška - nenamerni netačno prikazani izveštaji u računovodstvenim evidencijama ili računovodstvenim izveštajima;
- Nepravilnost - namerno prikazivanje netačnih izveštaja i pronevera / utaja sredstava određenog tela;
- Prevara - nepravilnost gde ima i krivičnih prevara da bi se nepravedno ili nezakoniti stekla neka korist;
- Nezakoniti postupci - počinjena dela, ili transakcije preduzete, od strane ili u ime revizorskog klijenta ili u korist preduzeća od strane zaposlenih, koji su u suprotnosti sa zakonom. Nezakoniti postupci mogu biti namerni ili nenamerni / iz nesmotrenosti počinjeni, i neki nezakoniti postupci mogu biti nepravilnost.⁷⁶

Revizori bi trebalo da znaju dovoljno o prevari kako bi uočili njene znake i signale, da ocene kada im je potrebna pomoć od strane iskusnijih istražitelja. Revizori finansijskih izveštaja treba da razumeju prevaru i moguće situacije prevare i treba da znaju da postavljaju odgovarajuću vrstu pitanja tokom revizije. Revizor treba da zadrži profesionalnu sumnju u sve pozicije, dok se ne dokaže da li su tačne ili netačne. Profesionalnu sumnju ne treba da iskazuje javno kako ne bi izvršio uticaj na ponašanje poslovnog okruženja.

Udruženje ovlašćenih istražitelja nezakonitih radnji (The Association of Certified Fraud Examiners) pod pogrešnim prikazivanjem finansijskih izveštaja prihvata jednu od definicija prevare koja pod prevarom podrazumeva namerno, osmišljeno pripremanje dokumenata, činjenica i informacija, tako da one utiču na pogrešno prikazivanje ili izostavljanje materijalno značajnih činjenica ili računovodstvenih podataka, koje će dovesti do toga da čitalac finansijskih izveštaja poveruje u neistinu i na osnovu toga promeni svoj sud ili donese odluku. Pogrešno finansijsko prikazivanje ili lažno finansijsko izveštavanje (Fraudulent financial reporting) je ono koje namerno ili nesmotreno, unapred smišljenim činom ili u ovom drugom slučaju propustom, rezultira materijalno netačnim iznosima u finansijskim izveštajima. Mnogi finansijski kolapsi su nastali kao posledica lažnog finansijskog izveštavanja, namernog povećanja prihoda, prikrivanja dugova i manipulisanja rukovodstva sa zaradama zaposlenih.

Najčešći motiv za pripremanje lažnih finansijskih izveštaja odnosno pogrešnog finansijskog prikazivanja je pribavljanje određene lične koristi za sebe ili kompaniju, kao i da bi se finansijsko stanje kompanije prikazalo boljim nego što zaista jeste. Iako se najčešće smatra da su računovođe i revizori odgovorni za istinitost i tačnost finansijskih izveštaja, taj posao spada pod odgovornost rukovodstva. Prema Zakonu o računovodstvu i reviziji i Okvirima profesionalne prakse, rukovodstvo preduzeća je odgovorno za sastavljanje finansijskih izveštaja preduzeća. To nas dovodi do zaključka da

⁷⁶ Prof. dr Milovan Stanišić, Revizija, Univerzitet Singidunum, Beograd 2008. str. 189

iako se prevare dešavaju u svim sektorima, da su najrasprostranjenije među rukovodstvom, menadžmentom, upravom preduzeća. Upravo ljudi zaposleni na najvišim pozicijama, koji raspolažu najvećim količinama novca i svojim profesionalnim statusom i pozicijom imaju moć da zaobiđu i nadjačaju kontrole, takozvani "zločinci belog okovratnika".

Sektor	Broj slučajeva	Slučajevi u procentima	Prosečan gubitak
Bankarstvo i finansije	229	16,7%	\$232,000.00
Vlada i državna uprava	141	10,3%	\$100,000.00
Proizvodnja	139	10,1%	\$200,000.00
Zdravstvo	92	6,7%	\$200,000.00
Prosveta	88	6,4%	\$36,000.00
Maloprodaja	83	6,1%	\$100,000.00
Osiguranje	78	5,7%	\$95,000.00
Usluge (profesionalne)	55	4,0%	\$115,000.00
Verske, dobrotvorne ili socijalne usluge	54	3,9%	\$85,000.00
Usluge (druge)	48	3,5%	\$150,000.00
Građevinarstvo	47	3,4%	\$300,000.00
Nafta i gas	44	3,2%	\$250,000.00
Telekomunikacije	43	3,1%	\$135,000.00
Tehnologija	38	2,8%	\$100,000.00
Transport i skladištenje	36	2,6%	\$180,000.00
Umetnost, zabava i rekreacija	32	2,3%	\$71,000.00
Nekretnine	28	2,0%	\$375,000.00
Veleprodaja	27	2,0%	\$50,000.00
Komunalne usluge	24	1,8%	\$38,000.00
Poljoprivreda, šumarstvo, lov i ribolov	20	1,5%	\$104,000.00
Rudarstvo	9	0,7%	\$500,000.00
Komunikacije i izdavaštvo	9	0,7%	\$150,000.00

Tabela 5. - Broj prevara i prosečan gubitak za 2012. godinu po osnovu sektora počinioca⁷⁷

⁷⁷ www.acfe.com/uploadedFiles/ACFE_Website/Content/rtn/2012-report-to-nations.pdf, preuzeto dana 26.10.2012.

Prema istraživanju ACFE - Association of Certified Fraud Examiners iz 2012.godine najviše prevara počinjeno je u sektoru za finansije i bankarstvo 16,7%, dok su na sledećem mestu zaposleni u vladi i državnoj upravi 10,3%. Iako najveći broj slučajeva prevare postoji u ovim sektorima, u njima nije pronevereno najviše novca. Naime najveće količine novca proneverene su u rudarskoj delatnosti, čak 500 hiljada dolara, kao i u građevinarstvu 300 hiljada dolara. Prema količini proneverenog novca oblast sa najviše slučajeva prevare, finansije i bankarstvo nalazi se na petom mestu sa 232 hiljade dolara, dok se državna uprava i vlada nalaze na petnaestom mestu sa 100 hiljada dolara.

Veoma je važno identifikovati faktore koji pružaju mogućnost za prevaru kako bi se sprečila slična dešavanja u budućnosti. Najčešći faktor je nedostatak kontrola čak u 35% slučajeva. U praksi važi stav da ono što nije kontrolisano vremenom će se sigurno pogoršati. U ovom se ogleda značaj kontola u sprečavanju prevara. Organizacije sa nedostatkom kontrole imaju gubitke veće za 45% od organizacija koje su imale odgovarajuće kontrole.

U 19% slučajeva počinilac je taj koji poništava postojeće kontrole kako bi mogao da izvrši prevaru. Ostali faktori koji mogu uticati na pojavu prevara su i loše upravljanje, nedostatak etičnosti i slabo procenjivanje od strane menadžmenta. Svi ovi faktori utiču na reputaciju i finansijsko stanje presuzeća.

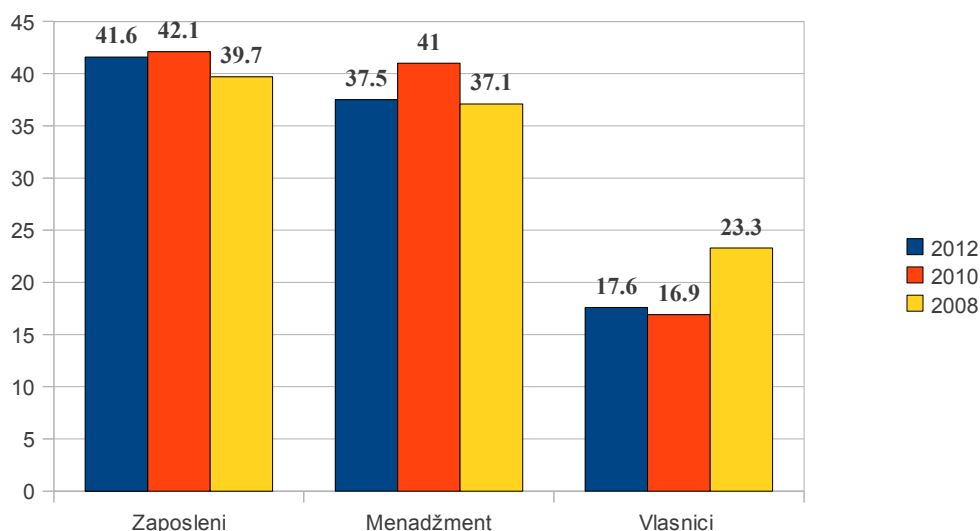
Lažno finansijsko izveštavanje može imati značajne posledice na organizacije i njene klijente, kao i na poverenje javnosti u tržište kapitala. Važni, periodični slučajevi lažnog finansijskog izveštavanja stvaraju određenu zabrinutost o kredibilitetu finansijskog izveštavanja u SAD i dovode u pitanje uloge menadžmenta, revizora, regulatora i analitičara. Jedan od najvećih finansijskih skandala je onaj u Enron korporaciji kada je rukovodeće osoblje Enron korporacije uspeo da sakrije dugove od milijardi dolara vezane za neuspele ponude i projekte, uz pomoć računovodstvenih rupa i slabih finansijskih izveštaja, kao i pritiska na revizore Arthur Andersen-a. Nakon otkrivanja prevare nije propala samo Enron korporacija, već je došlo i do raspada Arthur Andersen-a koji je do tada uz PricewaterhouseCoopers, Ernst & Young, KPMG i Deloitte činila veliku petorku (Big Five).

7.1. Počinioci prevara i njihove karakteristike

Neke kompanije koje su počinile prevaru su iskusile neto gubitke ili su bile blizu prelomne pozicije u periodu pre nego što je počinjena prevara. Pritisci koji prate sve dinamičnije finansijsko okruženje kao i uznemirenost koju kompanije osećaju pod ovim pritiscima, u nekim slučajevima kompanijama daju podsticaje za prevaru.

Kako bi se bolje razumeli faktori koji prouzrokuju prevaru potrebno je i bolje razumevanje psihe i ponašanja pojedinaca koji su do tada bili poznati po visokom integritetu i snažnim etičkim vrednostima. Takođe je veoma bitno i upoznati se sa karakteristikama prevaranata, kako bi ih bilo lakše prepoznati i sprečiti ili otkriti prevaru.

Grafikon koji sledi pokazuje procenat prevare prema poziciji koju počinioci zauzimaju u preduzeću. U 2012. godini 42% počinioca bili su zaposleni na nižim nivoima u preduzeću, 38% činili su menadžeri, a 18% rukovodioci ili vlasnici preduzeća. Ovi rezultati su upoređeni sa nalazima iz 2010. i 2008. godine.



Dijagram 1. - Broj prevara u procentima prema poziciji počinioca u preduzeću

Što se tiče novčanih gubitaka prouzrokovanih prevarama situacija je drugačija. Vlasnici su prouzrokovali skoro 3 puta veće gubitke od menadžera, dok su menadžeri prouzrokovali 3 puta veće gubitke od zaposlenih u nižim sektorima. Ovi rezultati su svakako očekivani s obzirom da zaposleni na rukovodećim pozicijama imaju veći pristup sredstvima jedne organizacije, kao i bolju poziciju kako bi zaobišli kontrole. Prevare koje su počinili menadžeri, rukovodioci i vlasnici trajale su u proseku 2 godine pre nego što su otkrivene. To je dva puta duže nego što su trajale prevare zaposlenih na nižem nivou, što je jedan od dokaza da više pozicije lakše zaobilaze kontrole ili prikrivaju prekršaje. U 2012. godini zaposleni su prevarama prouzrokovali gubitke preduzeća u iznosu od 60 hiljada dolara, menadžment 182 hiljade, a vlasnici čak 573 hiljade dolara.

Više od tri četvrtine prevara koje su obuhvaćene studijom počinili su pojedinci zaposleni u sledećim odeljenjima: računovodstvo, prodaja, izvršni menadžment, nabavka i korisnički servis.

U sledećoj tabeli prikazan je broj slučajeva prevare i količina proneverenog novca prema odeljenju u kojem su počinilioci zaposleni.

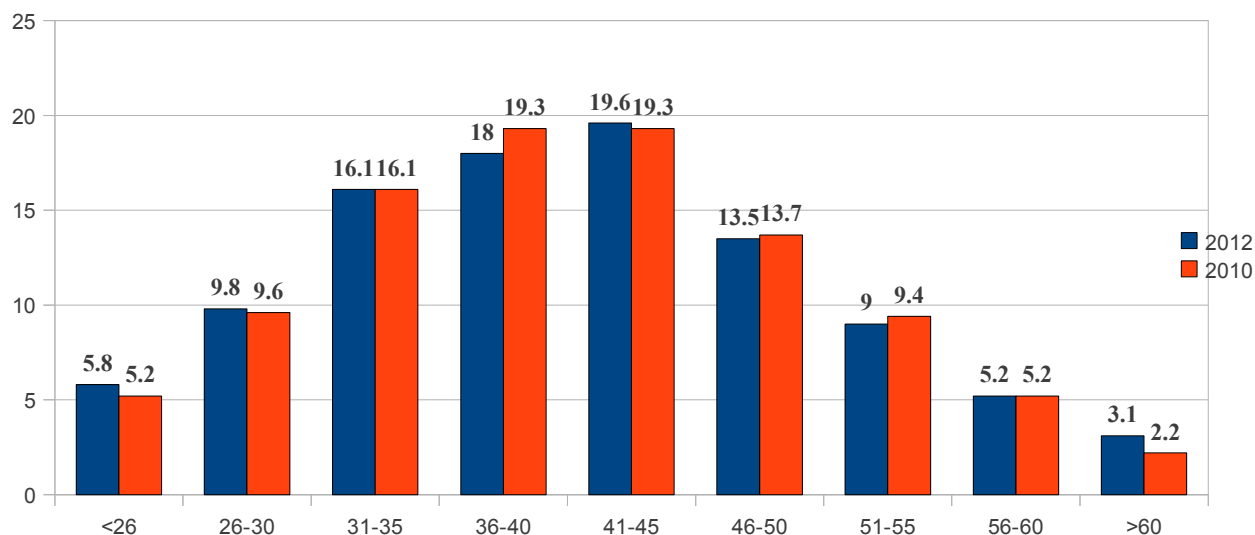
Odeljenje	Broj slučajeva	Procenat slučajeva	Prosečni gubitak
Izvršni menadžment	159	11,90%	\$500,000.00
Finansije	49	3,7%	\$250,000.00
Upravni odbor	19	1,4%	\$220,000.00
Nabavka	76	5,7%	\$200,000.00
Računovodstvo	293	22,0%	\$183,000.00
Pravni sektor	8	0,6%	\$180,000.00
Marketing/odnosi sa javnošću	14	1,1%	\$165,000.00
Proizvodnja	25	1,9%	\$160,000.00
Ljudski resursi	16	1,2%	\$121,000.00
Istraživanje i razvoj	9	0,7%	\$100,000.00
Informacione tehnologije	27	2,0%	\$100,000.00
Operacije	232	17,4%	\$100,000.00
Prodaja	170	12,8%	\$90,000.00
Skladištenje/zalihe	56	4,2%	\$67,000.00
Interna revizija	8	0,6%	\$32,000.00
Korisnički servis/usluge za potrošače	92	6,9%	\$30,000.00

Tabela 6. - Broj prevara i prosečan gubitak za 2012. godinu po osnovu odeljenja počinioaca⁷⁸

Najveći broj slučajeva prevare zabeležen je u računovodstvenom sektoru čak 293 slučaja, ali ovde nisu zabeleženi najveći gubici za preduzeće. Najviše novca proneverio je izvršni menadžment, čak 500 hiljada dolara. Najmanje slučajeva prevare u 2012. godini zabeleženo je u pravnom i sektoru za internu reviziju, samo 8 slučajeva. Najmanji gubici registrovani su u korisničkom servisu i odeljenju za internu reviziju, oko 30 hiljada dolara.

⁷⁸ www.acfe.com/uploadedFiles/ACFE_Website/Content/rtn/2012-report-to-nations.pdf, preuzeto dana 26.10.2012.

Zanimljivo je da najveći broj počinioca ima između 35 i 45 godina, njih oko 38%, a taj procenat je prilično konzistentan u protekle 2 godine. Međutim gubici nastali prilikom prevare, odnosno količina proneverenog novca raste sa godinama počinioca (Tabela 3). Mlađi od 26 godina u 2012. godini proneverili su 25 hiljada dolara, dok su najviše novca proneverili počinioci između 50 i 55 godina, čak 600 hiljada dolara, što je 2,5 puta više od gubitaka prouzrokovanih od strane počinioca drugih starosnih rangova. Sledeći dijagram pokazuje procenat slučajeva prevare na osnovu godišta počinioca i poređenje rezultata iz 2012. sa 2010. godinom.



Dijagram 2. - Procenat slučajeva prevare po osnovu godišta počinioca

Godište počinioca	Ostvareni gubici
<26	\$25,000.00
26-30	\$50,000.00
31-35	\$100,000.00
36-40	\$150,000.00
41-45	\$183,000.00
46-50	\$200,000.00
51-55	\$600,000.00
56-60	\$232,000.00
>60	\$250,000.00

Tabela 7. - Prosečan gubitak za 2012. prouzrokovan prevarom po osnovu godišta počinioca

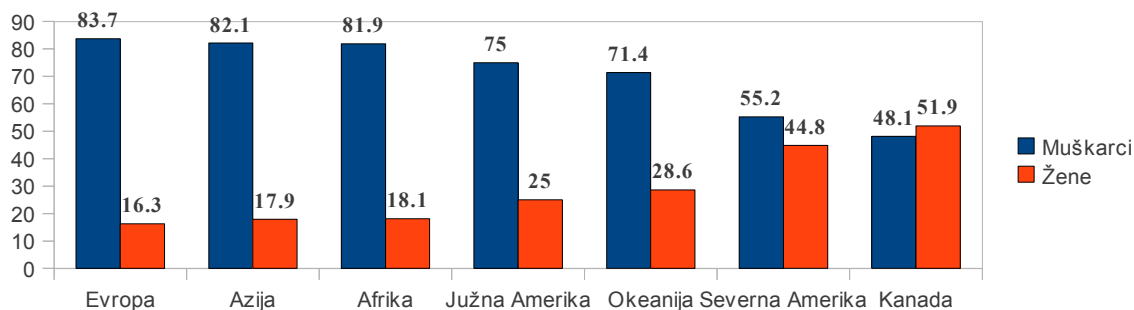
Nivo obrazovanja počinioca

Sledeća tabela prikazuje nivo obrazovanja koji poseduju počinioci prevare. Otprilike 54% počinioca poseduje diplomu koledža, univerziteta, ili čak master i doktorat. Oko 20% njih poseduje diplomu koledža, a 25% je završilo srednju školu ili ima niži nivo obrazovanja. Iako je očekivano da osobe sa višim nivoom obrazovanja imaju i viši nivo etičke kulture, rezultati su pokazali suprotno. Što počinilac ima veći nivo obrazovanja, to su i gubici prouzrokovani prevarom veći. Ovu povezanost možemo objasniti time što su obrazovaniji pojedinci zaposleni na višim položajima, imaju veći nivo vlasti odnosno autoriteta u svojim organizacijama, i samim tim lakše mogu da zaobiđu kontrole, a takođe raspolazu i većim količinama novca. Oni takođe poseduju bolje tehničke mogućnosti da osmisle i sprovedu šemu prevare. Pojedinci sa postdiplomskim stepenom odnosno diplomama u 2012. godini prouzrokovali su gubitke od 300 hiljada dolara, oni sa diplomom koledža 200 hiljada, a pojedinci sa nižim nivoom obrazovanja, odnosno oni sa završenom srednjom školom 75 hiljada dolara.

Nivo obrazovanja	Broj slučajeva u procentima	Prosečni gubitak
Postdiplomski stepeni	16,9%	\$300,000.00
Diploma koledža	36,9%	\$200,000.00
Neki koledž	20,5%	\$125,000.00
Završena srednja škola ili manje	25,3%	\$75,000.00
Drugo	0,5%	\$38,000.00

Tabela 8. - Broj slučajeva prevare i prosečni prouzrokovani gubici za 2012. godinu na osnovu nivoa obrazovanja počinioca

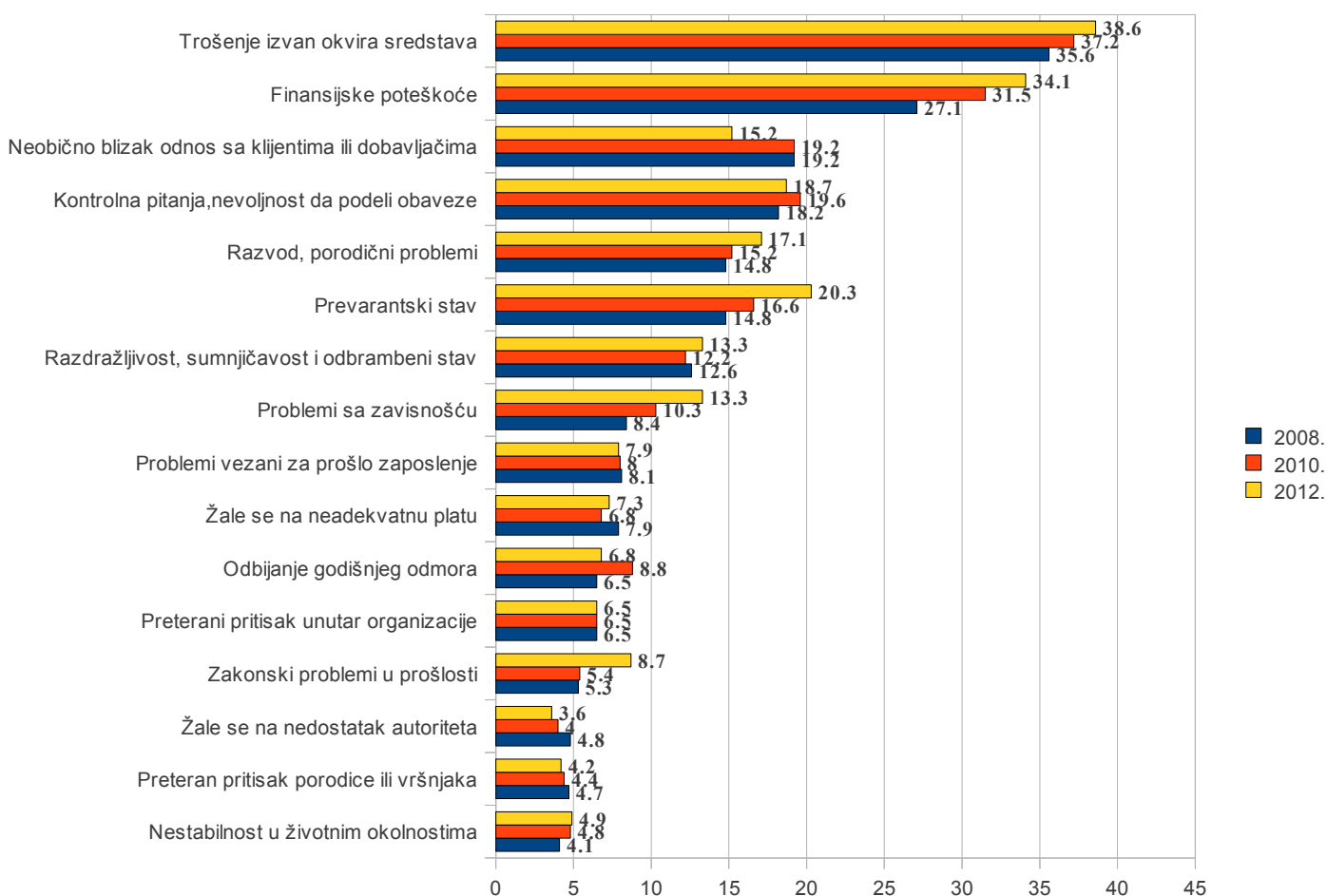
Interesantan je i podatak da su najčešće muškarci počinioci prevara, skoro duplo više slučajeva je registrovano nego kod žena. Registrovano je 65% slučajeva prevare gde su počinioci muškarci i 35% sa počiniocima ženskog pola. Ovi rezultati su prilično konzistentni kada se uporede sa studijama iz 2010. (M: 66,7% Ž: 33,3%) i 2008. godine (M: 59,1% Ž: 40,9%). Dolazimo do zanimljivog podatka i kada posmatramo regije pojedinačno. Napr. u Evropi je najuočljivija razlika između ženskih i muških počinioca, tačnije muškarci varaju u 83,7% slučajeva, a žene u 16,3%. Jedino je u Kanadi zabeležen veći broj slučajeva sa ženskim počiniocima 51,9%.



Dijagram 3. - Procenat slučajeva prevare po osnovu pola počinioca

7.2. Faktori na koje treba obratiti pažnju pri otkrivanju počinioca prevare

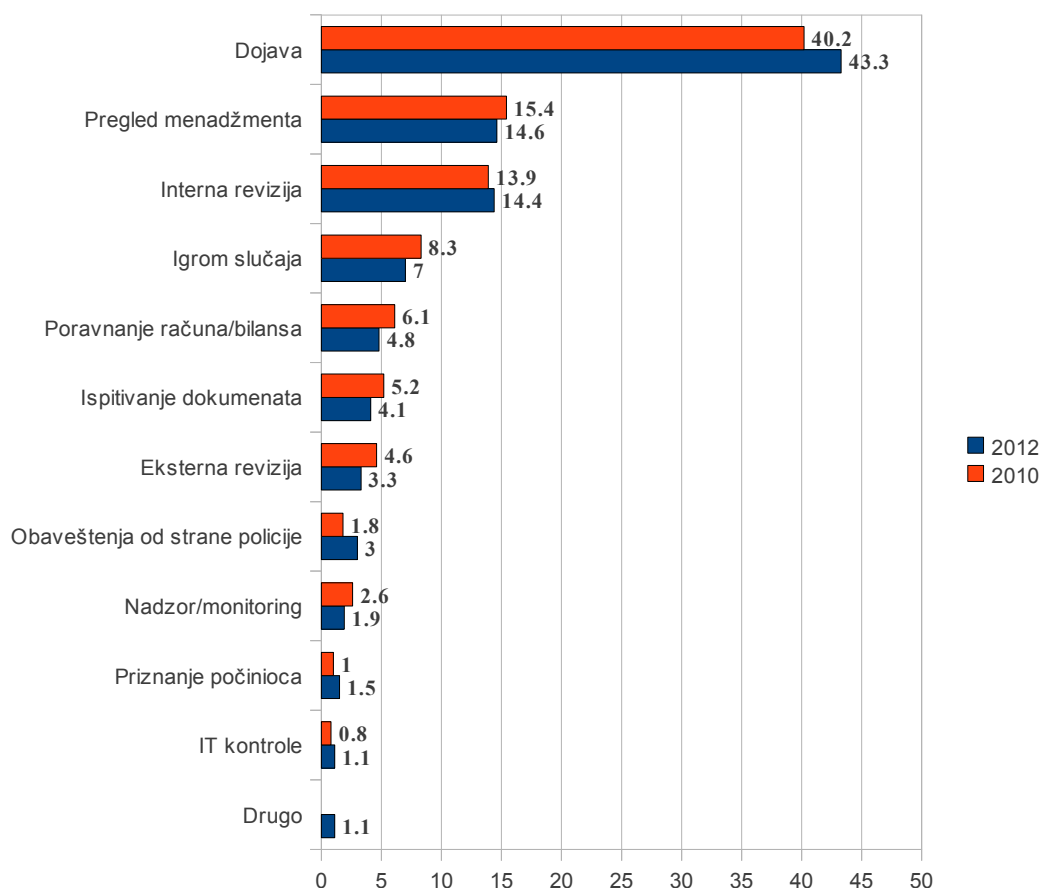
Većina počinioca motivisana je barem delimično nekom vrstom finansijskog pritiska. Pri tom, u toku izvršenja prevare, pojedinca često odaju određene karakteristike ponašanja, najčešće stres ili strah da će biti uhvaćeni. Ove karakteristike predstavljaju znak upozorenja da se prevara možda događa. Istraživanje obuhvata 16 najčešćih faktora odnosno karakteristika po kojima lakše možemo prepoznati prevarante. U 81% slučajeva, u 2012. godini, počinioci su imali barem jednu od navedenih karakteristika, a često i više njih. Sledeći dijagram pokazuje učestalost ovih karakteristika, odnosno procenat slučajeva u kojima je neka od karakteristika primećena, kao i poređenje sa rezultatima istraživanja iz 2010. i 2008. godine. Prema istraživanju iz 2012. godine, prevarante najčešće možemo prepoznati tako što žive na način koji prevazilazi okvire njihovih sredstava (36%), doživljavaju finansijske poteškoće (27%), imaju neobično blisku vezu sa dobavljačima ili klijentima (19%), prikazuju prekomerne kontrolne probleme (18%).



Dijagram 4. - Najčešće karakteristike počinioca prevare izražene u procentima⁷⁹

⁷⁹ www.acfe.com/uploadedFiles/ACFE_Website/Content/rtn/2012-report-to-nations.pdf, preuzeto dana 26.10.2012.

Početno otkrivanje prevare često je najvažniji trenutak u procesu ispitivanja prevara, trenutak kada se odluke moraju doneti brzo, gubici ublažiti i izabrati najbolja strategija koja je na raspolaganju. Analizirajući načine na koje organizacija otkriva slučajeve prevare, dobijamo uvid u efikasnost kontrola i drugih mera za sprečavanje prevara. Iznenadjuće je da su prevare najčešće otkrivene uz pomoć dojava, a najmanje uz pomoć IT kontola. Posle dojava koje pomažu otkrivanje čak 43,3% slučajeva, sledeće najefikasnije metode detekcije su procena i proveravanje od strane menadžmenta 14,6% i interna revizija sa 14,4% slučajeva u 2012. godini.



Dijagram 5. - Procenat učestalosti metoda za detekciju prevara⁸⁰

Najčešći izvori dojava su zaposleni u preduzeću, 50,9%. Izvori dojava mogu biti i dobavljači sa 9% i klijenti sa 22,1%. U podacima o izvoru dojava o prevarama našli su se čak i konkurenti, mada od je od njih u 2012. godini primljeno najmanje dojava, samo 1,5%. Iznenadjuće malo dojava dolazi od akcionara odnosno vlasnika samo 2,3%. Postoji nekoliko razloga zbog kojih osoba želi da ostane

80 www.acfe.com/uploadedFiles/ACFE_Website/Content/rtn/2012-report-to-nations.pdf, preuzeto dana 26.10.2012.

anonimna prilikom pružanja dojava, a upravo to pokazuju i podaci istraživanja, značajan broj dojava (12%) dolaze od anonimnog izvora. Alati kao što su anonimni sos telefoni ili veb bazirani portali, koji omogućavaju pojedincima da prijave prekršaj bez straha od odmazde ili da budu identifikovani, može pomoći da se olakša ovaj proces.

U više od dve trećine slučajeva, organizacije koje su žrtve prevaranata predmet prosleđuju organima za sprovođenje zakona, kako bi počinitelj bio krivično gonjen. Prosečni gubitak u slučajevima koji su prijavljeni je 200 hiljada dolara, dok je prosečni gubitak za slučajeve koji nisu prosleđeni 76 hiljada. U 390 slučajeva za koje je poznat ishod krivičnog postupka, oko 16% počinioca osuđeni su na suđenje, a u 56% slučajeva počinitelj se izjasnio krivim. Bilo je samo 6 slučajeva u kojima je počinioc oslobođen. U 454 slučaja koji nisu prosleđeni organima za sprovođenje zakona, kao najčešći razlozi za ne podnošenje krivičnih prijava navode se strah od lošeg publiciteta i odlučnost organizacije da sprovede unutrašnje sankcije koje su po njihovom mišljenju dovoljna kazna za nedolično ponašanje.

Iako se najčešće smatra da su računovođe i revizori odgovorni za istinitost i tačnost finansijskih izveštaja, zbog svojih kvalifikacija, veština i sistema kontrole taj posao spada pod odgovornost rukovodstva. Prema Zakonu o računovodstvu i reviziji i Okvirima profesionalne prakse, rukovodstvo preduzeća je odgovorno za sastavljanje finansijskih izveštaja preduzeća. Poslovne aktivnosti se zasnivaju na poverenju da svi učesnici tog procesa svoj posao obavljaju korektno i pošteno. Ipak samo poverenje nije dovoljno pa su sistemi kontrole neophodni. Mere za sprečavanje nezakonitih radnji su kompleksne, teško se sprovode i u osnovi su svedene na eliminisanje rizika nezakonitih radnji, uglavnom putem smanjenja prostora za motivaciju, šansi za pronevere i nedostatak integriteta.⁸¹

Veoma je važno očuvati integritet preduzeća. Najbolji način za to je poštovanje internih etičkih pravila koja postoje u svakoj organizaciji. Neka od tih pravila su jednostavna, dok su druga vrlo obimna i složena. Ovaj način je efikasan i efektivan ukoliko menadžment odnosno organi uprave podržavaju i promovišu propisana etička načela. Kada najviši organi kao što su predsednik upravnog odbora ili predsednik kompanije pokažu na ličnom primeru da se pridržavaju etičkih normi, ostali zaposleni će poverovati da je reč o realnim pravilima ponašanja. Važno je da viši menadžment promoviše etičke principe i norme ponašanja kako bi i zaposleni sledili njegov primer. Nažalost, rezultati istraživanja pokazuju da su upravo menadžeri i ostali zaposleni na visokim položajima ti koji vrše najveće prevare. Takozvani "zločinci belog okovratnika" zaposleni na visokim položajima, koji raspolažu sa najvećim količinama novca i s' obzirom na svoju poziciju lakše zaobilaze kontrole.

Postoji mnogo oblika prevare. Jedan od najčešćih oblika je korupcija. Sa korupcijom se najviše susreću u bankarskom i finansijskom sektoru, vladi i državnoj upravi, proizvodnji i naftnoj industriji. Prema istraživanju ACFE (Association of Certified Fraud Examiners), korupcija je najzastupljenija u Aziji i Južnoj Americi. Na trećem mestu je Evropa, zatim Okeanija i Afrika, a kontinent sa najmanje slučajeva korupcije je Severna Amerika. U nastavku rada govorićemo o stepenu korupcije u Srbiji, koji je toliko učestao da je čini se postao "oblik normalnosti".

81 Dr Dušan S. Milojević, Finansijska revizija i kontrola, Beogradska poslovna škola, Beograd, 2006.

7.3. Trenutno stanje transparentnosti finansijskih izveštaja u Srbiji

Cilj revizije je otkrivanje materijalno značajnih grešaka u finansijskim izveštajima čiji uzroci su mnogobrojni, a među njima kao uzrok navodi se i prevara.

Prevara se sastoji u osmišljenom i namernom pripremanju dokumenata, činjenica, informacija i situacija da bi se stvorili preduslovi da se neko na bazi pogrešnog predstavljanja činjenica u osmišljenim situacijama i okolnostima, podstakne da poveruje u neistinu i u skladu sa njom da se ponaša i prema tome, trpi gubitak ili štetu.⁸²

Revizor mora zadržati objektivnu i profesionalnu nepoverljivost u sve pozicije, dok ne utvrdi da li su tačne ili netačne. Profesionalnu sumnju revizor treba da zadrži za sebe, jer izražavanjem sumnje u javnosti može da utiče na ponašanje poslovne sredine i da sebi oteža prikupljanje informacija i dokaza. Mora uzeti u obzir sve faktore, kao što su ljudski faktor, ponašanje u organizaciji, poznavanje uobičajenih šema prevara, dokaz i njegove izvore, standarde dokaza. Iako ovaj, takoreći “detektivski” posao deluje prilično uzbudljivo, reč je o veoma složenom i naporanom, a ponekad čak i neprijatnom poslu jer najčešće ljudi na visokim izvršnim pozicijama čine najveće prevare.

Iako se polazi od činjenice da dobra interna revizija mora otkriti prevaru, zbog averzije javnog sektora nastale usled nerazumevanja ove profesije, kao i zbog neke vrste straha da će to naštetiti njihovom imidžu i efektivnosti internih konsultanata, mnogi interni revizori oklevaju sa ispunjenjem svojih obaveza vezanih za prevaru.

“Fenomen korupcije kod nas je u poslednjih 15 godina metastazirao, postao gotovo način života, a mnogi u tome vide i model za rešavanje raznih, kako većih tako i manjih problema. Stanje u kome je korupcija postala neki novi oblik 'normalnosti' samo pokazuje koliko je poremećen sistem društvenih vrednosti. Brzi rezultati međutim nisu mogući, a uspehom se može smatrati i podizanje svesti pripadnika podređenih korupciji najpodložnijih profesija u borbi za profesionalni integritet.

Polazi se od pretpostavke da se unapređenjem profesionalne etike može doprineti obuzdavanju korupcije u pojedinim delatnostima. U Srbiji nizak nivo profesionalne etike, praznine u pravnom sistemu, srozan položaj pojedinih delatnosti ali i uništene, a neizgrađene institucije doprinose raširenosti korupcije.

U razgovorima sa pripadnicima raznih profesija primećena je sa jedne strane obeshrabrenost onih koji su protiv korupcije, ali i otpor onih kojima takvo stanje odgovara.

U revizorsku profesiju ne baš mali broj njenih pripadnika stiže iz ministarstava, sudstva i policije, ali napuštanjem ranijih poslova nastavljaju da koriste svojevremene veze i povlašćen položaj a i stranke se rado opredeljuju za takve misleći da će time lakše rešiti svoje probleme.”⁸³

Čak i kada revizori svoj posao obave na adekvatan način i pravilno utvrde nepravilnosti u poslovanju revidiranog subjekta, sud je nezavisni državni organ na kome je da donese krajnu odluku o krivici subjekta. Međutim, korupcija i neprofesionalizam u sudstvu, prisutni su u velikoj meri, pa smo često svedoci “prilično sporog procesuiranja prijava” i “oslobađajućih presuda”⁸⁴, iako je utvrđeno da prekršaji postoje.

82 Prof. dr Milovan Stanisic, “Revizija”, Univerzitet Singidunum, Beograd 2009. str.191

83 www.transparentnost.org.rs/ts_mediji/stampa/2005/02FEBRUAR/2102-05.html, preuzeto dana 28.10.2012.

84 Radoslav Sretenović za Večernje novosti, Ponedeljak, 29.08.2011.

Predsednik organizacije “Transparency Serbia”, Vladimir Goati ukazao je na nedodirljivost političke korupcije u Srbiji i nedostatak hrabrosti, volje i profesionalizma u njenom suzbijanju. Ako pogledamo indeks korupcije⁸⁵ organizacije “Transparency International” možemo zaključiti da iako se stanje korupcije u zemlji od 2003. godine popravilo, od 2007. godine stanje je ostalo gotovo nepromenjeno i još uvek se nalazimo u “crvenoj zoni” koja označava visok stepen korupcije. U 2011. godini Srbija se našla na 86. mestu ove liste, što nam pokazuje da se stanje čak pogoršalo od 2010. godine kada je zauzimala 78 mesto. Ako ove rezultate uporedimo sa zemljama iz okruženja primetićemo da veći stepen korupcije ima samo Bosna, dok su Slovenija, Hrvatska i Crna Gora ispred nas u borbi za transparentnost. Švedska i Norveška u kojima je revizorska profesija mnogo razvijenija nego u Srbiji nalaze se na 4. i 6. mestu. Smatram da je ovo pravi pokazatelj koliko je revizorska profesija potrebna i značajna, ali isto tako i koliko je ona u Srbiji potcenjena i sputavana.

Elementi političkih pritisaka na rad nezavisnih državnih organa su više nego očigledni. Otkriveno je da Ministarstva krše Zakon o budžetu tako sto ne vrše popis imovine i obaveza kako je regulisano zakonom o budžetskom računovodstvu, ne vode evidencije o potraživanjima u svojim knjigama kao ni evidencije nefinansijske i finansijske imovine u skladu sa propisima Zakona o budžetskom sistemu, da se javna preduzeća ne pridržavaju odredaba primene Zakona o javnim nabavkama, Zakona o sredstvima u svojini Republike Srbije i Zakona o računovodstvu i reviziji. Pa ponovo kao i 2009. godine, kada su podnete prijave zbog kršenja propisa o trošenju sredstava iz budžeta za 2008. godinu, nisu napisane krivične prijave već samo prekršajne.

Kažnjavanje je bitno koliko i kontrola. Prema mišljenju Dragomira Jovanovića iz Evropskog ekonomskog instituta “potrebno je uvesti ozbiljne zakonske i moralne kazne za prekršiće zakona”⁸⁶. Predugi niz godina se u Srbiji pogled sklanja na stranu od nezakonitosti i korumpiranosti u javnom sektoru, i vremenom se čini kao da je zaboravljeno da u demokratskom društvu niko nije iznad zakona.

U Republici Srbiji, visok nivo korupcije, zloupotreba javnih sredstava i visok nivo finansijskog kriminala, posledica su ambijenta sa slabom kontrolom i skoro nikakvim funkcijama revizije. Kao rezultat iskrivljenog sistema vrednosti, nedostatka svesti i volje za promenama, ljudi su zaboravili etičke i moralne norme, norme ponašanja, a korupcija je postala sastavni deo života i možemo je naći u svakom segmentu poslovanja. Revizija, kao relativno mlada poslovna disciplina u našoj zemlji, dosta trpi zbog ambijenta i atmosfere u kojoj živimo. Kada su moral i poštenje potcenjeni, nadzor, disciplina i kažnjavanje su jedini elementi koji doprinose postizanju reda i istrebljenju korupcije.

85 www.transparency.org/policy_research/surveys_indices/cpi/2010/results, preuzeto dana 21.10.2012.

86 www.b92.net/biz/vesti/srbija.php?yyyy=2011&mm=02&dd=09&nav_id=491460, preuzeto dana 22.10.2012.

ZAKLJUČAK

Odlika današnjeg, savremenog poslovnog okruženja su stalne, sve dinamičnije i složenije promene koje utiču na poslovanje svakog preduzeća. U vreme kada su preduzeća svakodnevno izložena raznim rizicima, vrlo je važno da menadžment preduzeća posveti pažnju nadzornim mehanizmima, a posebno internoj kontroli i internoj reviziji i da osigura da zaposleni na ovim poslovima budu kompetentni odnosno osposobljeni i stručni.

Interna revizija i interna kontrola su prevashodno okrenute sprečavanju grešaka, prekomernih troškova i prevara. Njihov posao je da proveravaju i obezbede pouzdanost informacija. One kontrolišu preduzeće kao celinu i sve njegove delove pojedinačno, proveravaju da li su primenjene propisane politike i procedure i podnose izveštaj menadžmentu na osnovu analize prikupljenih informacija i dokaza. Interna kontrola, kao i interna revizija u savremenom poslovnom okruženju, imaju sve veći značaj i uticaj na uspešnost poslovanja preduzeća. Zato je potrebno fokusirati se na izgradnju dobrog sistema interne kontrole – preventivnog nadzora koji za cilj ima da ukloni potencijalne greške i nepravilnosti, i interne revizije – naknadnog nadzora, koja organizaciji pomaže u ostvarivanju postavljenih ciljeva kroz procenjivanje delotvornosti kontrole, korporativnog upravljanja i upravljanja rizicima preduzeća.

Prilikom upravljanja rizicima interna revizija treba da razume proces upravljanja rizikom, metode i tehnike upravljanja, da razvije strategiju kojom će zauzeti stav prema riziku. Uloga interne revizije nije samo ocenjivanje funkcionisanja procesa upravljanja rizikom koji je definisao menadžment, već i predlaganje mera za poboljšanje ovog procesa i uklanjanje slabosti i nedostataka kako bi se rizik sveo na nivo prihvatljiv za preduzeće. Odgovornost menadžmenta je da odredi nivo rizika koji je prihvatljiv za preduzeće, da donese odluku kako će upravljati rizikom, da odluči kako će ukloniti nedostatke i poboljšati odnosno unaprediti proces upravljanja rizikom. Interna revizija prikupljenim dokazima, korisnim informacijama i svojim savetima i predlozima, menadžmentu pomaže u donošenju ovih odluka, a njena odgovornost u procesu upravljanja rizicima je izražavanje mišljenja o delotvornosti primenjenog načina upravljanja rizicima.

U savremenom poslovanju koje odlikuju nestabilni uslovi poslovanja, rast i razvoj preduzeća i samog finansijskog tržišta povlači sve više poslovnih rizika sa kojima se preduzeće suočava, pa je upravljanje rizikom postalo neophodno. Čak i preduzeća koja nemaju organizovanu internu reviziju upravljaju rizikom, kako bi osigurali uspešno poslovanje, a takođe i zato što je to činilac dobrog poslovnog osećaja.

Napretkom informacione tehnologije do nivoa na kome se danas nalazi, raste i njen uticaj na poslovanje preduzeća. Sistem upravljanja nad informacionim tehnologijama veoma je bitan faktor za uspešne poslovne rezultate. On predstavlja sastavni deo opšteg sistema upravljanja kompanijom i sastoji se od rukovođenja, organizacione strukture i procesa koji obezbeđuju da IT podržava i proširuje strategiju i ciljeve kompanije.

Na uspešnost preduzeća utiče nivo raspoložljivosti, pouzdanosti, bezbednosti i IT sposobnosti. Time postaje značajna i zrelost IT upravljanja. Iako neke kompanije ne shvataju važnost informacionih tehnologija i njihov uticaj na ostvarivanje poslovnih ciljeva i poslovanje, informacione tehnologije predstavljaju budućnost poslovanja s obzirom da se danas gotovo svi poslovni procesi obavljaju korišćenjem različitih tehnologija.

IT upravljanje je sastavni deo upravljanja preduzećem i sastoji se od liderskih i organizacionih struktura i procesa. Upravo zbog ovog, sve većeg značaja IT-ja na poslovanje preduzeća, veoma je bitno sprovesti aktivan nadzor nad upravljanjem IT-jem i tako obezbediti uspešno poslovanje kompanija. Uslov opstanka bilo koje organizacije je da raspolaže adekvatnim informacionim sistemom, u kojem su optimizovani poslovni procesi i tokovi informacija.

Kompanije treba da aktivno vrše nadzor upravljanja informacionim tehnologijama, da osiguraju da su IT operacije, rizici i mogućnosti vođeni tako da doprinose uspešnom poslovnom rezultatu organizacije.

Revizija je veoma važna poslovna disciplina, na osnovu koje se donose bitne finansijske odluke, od koje korist imaju vlasnici preduzeća, menadžeri, poverioci, poreski organi, šira javnost, pa i sama država. Revizija je odgovoran posao koji zahteva veliku odgovornost, koncentraciju, visok stepen etičnosti, poštovanje zakona, načela i standarda, a revizori moraju biti poštjeni i časni ljudi koji će opravdati poverenje javnosti.

LITERATURA

1. Andrić Mirko, Krsmanović Branko, Jakšić Dejan, *Revizija-teorija i praksa*, „Proleter“ a.d. Bečej, Subotica 2004.
2. Prof. dr Branislav Mašić, *Menadžment*, Univerzitet Singidunum, Beograd 2010.
3. David L. Cannon, *CISA – Certified Information Systems Auditor, Study Guide Second edition*, Wiley Publishing, Indianapolis 2008.
4. Prof. dr Dušan S. Milojević, *Finansijska revizija i kontrola*, Beogradska poslovna škola, Beograd, 2006.
5. Harry T. Magill, Gary John Previts, *Professional Responsibilities - An Introduction*, South-Western Publishing, Cincinnati 1991.
6. Dr Jozefina Beke Trivunac, Jelena Vučinić, dr Dragan Milačić i dr., *Interna revizija - upravljanje, rizici, kontrola*, Institut za ekonomiku i finansije, Beograd 2012.
7. Kristina Mijić, Dejan Jakšić, *Primena kompjuterskih alata i tehnika prema fazama procesa revizije finansijskih izveštaja*, Revizor 49/2010, Institut za ekonomiku i finansije 2010.
8. Prof. dr Milan I. Miljević, *Metodologija naučnog rada*, Univerzitet u Istočnom Sarajevu, Pale 2007.
9. Prof. dr Milovan Stanišić, *Revizija*, Univerzitet Singidunum, Beograd 2009.
10. Prof. dr Milovan Stanišić, Doc. Dr Ljubiša Stanojević, *Evaluacija i rizik*, Univerzitet Singidunum, Beograd 2010.
11. Prof. dr Milovan Stanišić, Doc. Dr Ljubiša Stanojević, *Revizija i primena kompjutera*, Univerzitet Singidunum, Beograd 2008.
12. Prof. dr Milovan Stanišić, Doc. Dr Kosana Vićentijević, *Revizijski zaključni izveštaj*, Univerzitet Singidunum, Beograd 2009.
13. Prof. dr Milovan Stanišić, Doc. dr Ljubiša Stanojević, *Revizija u bankarstvu*, Univerzitet Singidunum, Beograd 2007.
14. Soltani Baharam, *Revizija-međunarodni pristup*, prevod Mate d.o.o. Zagreb, 2010.
15. William F. Messier, *Revizija - Priručnik za revizore i studente*, Zagreb 2000.
16. Prof. dr Zoran Petrović, *Međunarodni standardi revizije*, Univerzitet Singidunum, Beograd 2010.

INTERNET IZVORI

www.acfe.com, 2012 Report to the nations on occupational fraud and abuse

www.astuteconsulting.com, Internal audit and risk management

www.bis.org, Framework for internal control systems in banking organisation

www.coso.org, Internal control – Integrated Framework

www.ekof.bg.ac.rs, Prezentacija – Revizija, Međunarodni standardi revizije i kodeks etike

www.globaliia.org, Standards 2011 – Serbian

www.icisa.cag.gov.in, ISA 400 – Risk assessment and internal control

www.isaca.org, COBIT Framework

www.iso.org, ISO 9001

www.itgovernance.co.uk, ISO 27001

www.itrevizija.ba, ITIL okvir

www.kontroling.ftn.uns.ac.rs, Uloga interne revizije u korporativnom upravljanju rizicima

www.kor.rs, Registri ovlašćenih revizora

www.mf.gov.me, Priručnik za finansijsko upravljanje i kontrole

www.mfin.gov.rs, Nacrt Nacionalne strategije za unapređenje kvaliteta korporativnog finansijskog izveštavanja i revizije

www.sec.gov, Sarbanes Oxley Act of 2002.

www.theiia.org, Glossary

www.uirs.rs, Bilten (Informativno – teoretski list "Udruženja internih revizora Srbije"), Kodeks etike

www.upravljanjerizicima.com, Enterprise Risk Management

www.2700.org, ISO 27001, ISO 27002