UNIVERZITET SINGIDUNUM

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKA DISERTACIJA

UTICAJ KONTROLE I REVIZIJE INFORMACIONIH SISTEMA NA USPEŠNOST I EFIKASNOST UPRAVLJANJA I POSLOVANJA KOMPANIJA U SRBIJI

Mentor:
Prof. dr Milovan Stanišić

Kandidat:
mr Dalibor Radovanović

Beograd, 2010.

S A D R Ž A J

Popis slika

Popis tabela

UVOD

1. PREDMET I CILJEVI ISTRAŽIVANJA

Informacioni sistem (u daljem tekstu IS) je jedan od ključnih činilaca poslovanja svake kompanije. Upravljanje informacionim sistemom je aktivnost povezana sa korišćenjem naprednih tehnologija i visokim stepenom stručnih znanja, kao i opštim znanjima iz teorije upravljanja organizacionim sistemima. Svaka organizacija se u svom poslovanju susreće sa značajnom količinom nesigurnosti koja može da bude uzrok materijalnog rizika i gubitaka. Uspeh upravljanja celokupnim poslovanjem direktno je povezan sa upravljanjem rizicima, tj. rizici treba da budu prevaziđeni da bi se uspešno upravljalo organizacijom.

Revizija IS je proces kojim se prikuplja i procenjuju dokazi na osnovu kojih se procenjuje uspešnost IS, odnosno odredjuje se da li IS radi u funkciji održavanja celovitosti i integriteta podataka i očuvanja imovine. Takođese određuje da li IS omogućavauspešno ostvarivanje poslovnih ciljeva i da li su sistemski resursi koriste na svrsishodan način. Revizija informacionih sistema je postupak pomoću kojeg se procenjuje da li informacione tehnologije deluju u skladu sa ciljevima organizacije, kao i u kolikoj meri uspešno i svrsishodno podupiru ciljeve poslovanja. U današnje vreme ima savetodavnu ulogu i pomaže pri korporativnom upravljanju informacionim tehnologijama[1].

Revizijom se utvrđuje da li je sistem internih kontrola koji je uspostavljen u cilju upravljanja rizicima, kontrolisanja i rukovođenja procesima, adekvatan i da li funkcioniše na način kojim se obezbeđuje:

- da su rizici na odgovarajući način identifikovani i kontrolisani,
- da su međusobni odnosi članova rukovodstva uspostavljeni na odgovarajući način (horizontalna i vertikalna povezanost),

[1] *Engl. IT Governance*

- da su bitne finansijske, upravljačke i operativne informacije i izveštaji pravovremeni, tačni i potpuni,
- da zaposleni obavljaju poslove u skladu sa propisanim standardima i procedurama,
- da su sredstva ekonomično nabavljena, da se efikasno i racionalno koriste i da su adekvatno zaštićena,
- da su programi, planovi i ciljevi organizacije ostvareni,
- da su kontrolni procesi kvalitetni i da se stalo unapređuju,
- da su rukovodstvo i zaposleni pravovremeno upoznati sa zakonima, drugim propisima i opštim aktima koji su iz njihovih delokruga,
- da je poslovanje usklađeno s politikom, planovima, procedurama i propisima.

Problem koji se istražuje u ovom radu je unapređenje efikasnosti, efektnosti, sigurnosti i zaštite informacionog sistema kao zahtev procesa revizije IS. Objašnjenje pojma rizika, ocene rizika i upravljanja rizikom su ilustrovani primerima iz prakse da bi se dokazala prednost iz prakse i na taj način će se dokazati prednosti ovakvog načina razvoja i primene strategije revizije informacionog sistema. Planiranje i izvođenje konkretnih revizija obezbeđuje zaštitu i kontrolu poslovnog i informacionog sistema. Izveštavanje rukovodstva o rezultatima revizije i savetodavna funkcija revizije omogućuju da se uočeni nedostaci otklone i da se postojeći sistem poboljša.

Glavni cilj doktorske teze je da se utvrdi uticaj kontrole i revizije informacionog sistema na uspešnost i efikasnost upravljanja i poslovanje kompanija bi se stvorila teorijska osnova za primenu kontrole i revizije informacionih sistema u drugim privrednim subjektima u Srbiji.

Dodatni ciljevi istraživanja u radu se odnose na upoznavanje sa procesom revizije informacionog sistema, uključujući izradu godišnjeg plana, analizu rizika, izbor predmeta i ciljeva revizija, pripremu za svaku konkretnu reviziju, razgovore sa rukovodiocima i neposrednim izvršiocima, prikupljanje podataka, analiza postojećeg stanja, kao i projektovanje novog poboljšanog sistema kroz implementaciju datih preporuka.

Takođe, u radu su istraživani uzroci i posledice rizika kako bi stvorio opšti teorijski pristup upravljanju rizikom u organizaciji.

Poseban aspekt istraživanja se odnosi na definisanje međunarodnih standarda, smernica i procedura uz prikaz kompletnog procesa revizije informacionog sistema u svim njegovim fazama.

2. HIPOTEZE ISTRAŽIVANJA

Osnovne hipoteze u doktorskoj tezi

Generalna hipoteza:

- Udanašnjim tržišnim okolnostima broj poslova koji se odvijaju uz pomoć informacionih sistema je u stalnom porastu, kontrola i revizija informacionih sistema sve više dobija na važnosti i neophodnosti.

Posebna hipoteza:

- Korporativno upravljanje informacionim tehnologijama i IT revizija su imperativ za uspešno poslovanje.
- O informacionom sistemu menadžment često malo zna, a samim tim upravljanje i kontrolisanje je otežano.
- Uspešnost kompanije je u direktnoj korelaciji sa redovnom kontrolom i revizijom informacionih sistema.

Pojedinačna hipoteza:

- IT revizija, pored egzaktne i analitičke funkcije, u današnje vreme ima savetodavnu ulogu i pomaže pri korporativnom upravljanju informacionim tehnologijama.
- Rad informacionog sistema je u funkciji održavanja celovitosti i integriteta podataka, kao i korišćenja resursa sistema na efektivan i efikasan način.

- Revizijom se utvrđuje da li informacione tehnologije fukcionišu u skladu sa ciljevima organizacije, i u kojoj meri delotvorno i efikasno podupiru ciljeve poslovanja.
- Od ekonomske snage kompanije direktno zavisi uvođenje novih tehnologija.

3. METODE ISTRAŽIVANJA

Tokom istraživanja korišćene su metode primerene oblastima ekonomskih nauka odnosno revizije, poslovnih finansija, statistike, modelovanja. Osnovu istraživanja činile su sledeće metode:

- osnovne analitičke metode:
  - metoda analize,
  - metoda apstrakcije,
  - metoda specijalizacije i
  - metoda dedukcije;

- osnovne sintetičke metode:
  - sinteza,
  - konkretizacija,
  - generalizacija i
  - indukcija;

- opšte naučne metode:
  - hipotetičko-deduktivna,
  - analitičko-deduktivna,
  - komparativna,
  - statistička i
  - metoda modelovanja.

Primenom ovih metoda omogućeno je dostizanje naučnog i društvenog cilja istraživanja, a da pri tom ni jednom metodološkom postupku nije data isključiva prednost.

Za prikupljanje podataka prilikom istraživanja primenjena je anketa i metoda analize sadržaja dokumenata.

Analiza obuhvata sledeće nivoe:

- nivo izvornih podataka na osnovu originalnih podataka kompanija i
- nivo sekundarne analize rezultata prethodnih istraživanja i odgovarajuće literature.

4. OČEKIVANI DOPRINOS ISTRAŽIVANJA

Na osnovu sprovedenih istraživanja očekuje se rezultat u kome je dokazan uticaj kontrole i revizije informacionih sistema na uspešnost i efikasnost poslovanja kompanija, što dalje znači da može da se preporuči svim kompanijama da vrše periodičnu kontrolu i reviziju informacionih sistema i time postignu uspešnije poslovanje. Ciljevi ovog istraživanja su ukazivanje na značaj, koristi i neophodnost primene revizije informacionog sistema. Konkretan rezultat ovog istraživanja je sveobuhvatni prikaz procesa revizije informacionih sistema i primeri izvođenja revizije u praksi.

Svrha ovog istraživanja je upoznavanje sa procesom revizije informacionog sistema, uključujući izradu godišnjeg plana, analizu rizika, izbor predmeta i ciljeva revizija, pripremu za svaku konkretnu reviziju, razgovore sa rukovodiocima i neposrednim izvršiocima, prikupljanje podataka, analiza postojećeg stanja, kao i projektovanje novog poboljšanog sistema kroz implementaciju datih preporuka.

Sa naučnog stanovišta ovaj rad treba da napravi celovit, konzistentan teorijski i praktičan okvir za kontrolu i reviziju informacionih sistema u skladu sa najboljom svetskom praksom. Kao konačan rezultat i doprinos rada očekuju se veoma konkretne preporuke kompanijama za uvođenjem revizije informacionih sistema i korporativnog upravljanja informacionim tehnologijama.

PRVI DEO

KORPORATIVNO UPRAVLJANJE INFORMACIONIM TEHNOLOGIJAMA

1. UVOD

Korporativno upravljanje informacionim tehnologijama je podskup disciplina korporativnog upravljanja fokusiran na sisteme informacione tehnologije (u daljem tekstu IT), njihovim performansama i upravljanjem rizikom. Povećano interesovanje za IT upravljanje je delimično vezano za inicijative usaglašenosti, npr. Sarbanes-Oxley u SAD i Bazel II u Evropi, ali više zbog potrebe za većim stepenom odgovornosti prilikom donošenje odluka vezanih za korišćenje informacionih tehnologija u najboljem interesu svih zainteresovanih strana.

Uobičajena diskusija o upravljanju IT-em je da je kapacitet IT-a direktno povezan sa izborima investicija koje je doneo vrh menadžmenta i koje imaju dugoročne posledice na različite aktere. Korporativno upravljanje informacionim tehnologijom podrazumeva sistem u kojem svi akteri, uključujući bord direktora, izvršni menadžment, kupce i osoblje imaju odgovornost u procesu donošenja odluka koje utiču na IT. Ovo sprečava IT ili poslovne lidere da nezavisno donose odluke o IT-ju bez odgovornosti za svoje postupke i uticaja koji imaju na podršku postignuća strateških ciljeva.

Upravljanje informacionim tehnologijama određuje nivo integracije i kontrole koji organizacija ima nad svojim investicijama u IT. Informaciona tehnologija je sveprisutna u poslu danas. Suštinska vrednost informacione tehnologije mora biti u potpunosti integrisana u svaki aspekt posla, umesto da bude izdvojena kao posebna IT funkcija. Nivo IT integracije ima znatan efekat na to kako organizacija definiše svoju misiju, postiže strateške ciljeve i saopštavasvoju viziju razvoja. Revizija IT upravljanja uključuje najviše nivoe organizacionog menadžmenta i prelazi granice između odeljenja.

2. KORPORATIVNO UPRAVLJANJE INFORMACIONIM TEHNOLOGIJAMA

Disciplina korporativnog upravljanja informacionim tehnologijama se prvi put pojavila 1993. godine kao derivat korporativnog upravljanja i primarno se bavila vezom između strateških ciljeva i IT upravljanja organizacijom. Naglašava značaj pitanja vezanih za IT u savremenim organizacijama i navodi da bi strateške IT odluke trebao donositi bord direktora umesto direktora IT službe ili drugih IT menadžera.

Osnovni ciljevi upravljanja informacionim tehnologijama su:

- Osigurati da investicije u IT stvaraju poslovnu vrednost.
- Smanjiti rizike koji su povezani sa informacionim tehnologijama. Ovo može biti postignuto implementacijom organizacione strukture sa dobro definisanim ulogama za odgovornost informacija, poslovnih procesa, aplikacija, infrastrukture itd. Odgovornost je najveća briga IT upravljanja.

Posle kolapsa Enrona[2] 2000. godine i problema u Arthur Andersenu[3]i WorldCom[4]-u dužnosti i nadležnosti revizora i bordova direktora korporacija u javnom i privatnom vlasništvu su dovedene u pitanje. Kao odgovor na ovo, a i da bi bilo sprečeno da se slične stvari ponovo dogode, napisan je zakon Sarbanes-Oxley da bi istakao značaj kontrole posla i revizije. Iako

[2] Petrache, A., (2009), "The collapse of ENRON, a classic case of corporate social irresponsibility", The Ninth International Conference Investments and Economic Recovery

[3] Edelman, D., Nicholson, A., (2011), "Arthur Anderson Auditors and Enron: What happened to their Texas CPA licenses?", Journal of Finance and Accountancy

[4] Kuhn, R., Sutton, S., (2006), "Learning from WorldCom: Implications for Fraud Detection through Continuous Asurance", Journal of Emerging Techologies in Accounting, Vol 3., pp. 61-80

nisu direktno povezani sa IT upravljanjem Sarbanes-Oxley u SAD i Bazel II u Evropi su uticali na razvoj upravljanja informacionim tehnologijama od ranih 2000-ih godina.

Postoje uže i šire definicije upravljanja IT-jem:

- Upravljanje IT-jem je odgovornost rukovodilaca i borda direktora i čine ga vođstvo, organizacione strukture i procesi koji omogućavaju da IT odeljenje podržava i proširuje ciljeve i strategije organizacije[5].

- Upravljanje IT-jem: Određivanje okvira prava prilikom donošenja odluka i odgovornosti radi podsticanja poželjnog ponašanja prilikom korišćenja informacionih tehnologija[6].

- Korporativno upravljanje informacionim tehnologijamaje takvo strateško usklađivanje IT-ja sa poslom tokom kog dolazi do ostvarivanja maksimalne poslovne vrednosti kroz razvoj i održavanje efektivne IT kontrole i odgovornosti, upravljanja performansama i upravljanja rizikom[7].

- Van Grembergen i De Haes su koncentrisani na korporativno upravljanje IT-em i definišu ga kao: „integralni deo korporativnog upravljanja koji se bavi definicijom i implementacijom procesa, struktura i relacionim mehanizmima koji omogućavaju i poslovnim i IT ljudima da vrše svoje dužnosti u prilog poslovnom/IT poravnanju i stvaranju poslovne vrednosti iz investicija koje je omogućio IT“ [8].

---

[5] ITGI, (2007), CobiT 4.1 – Framework, Control Objectives, Management Guidelines and Maturity Models, IT Governance Institute

[6] Weill, P., and Ross, J. W., (2004), "IT governance – How top performers manage IT decision rights for superior results", Harvard Business School Press, 2004

[7] Webb, P., Pollard, C., and Ridley, G., (2006), "Attempting to define IT Governance: Wisdom or Folly" Proceedings of the 39th Hawaii International Conference on system Sciences, 2006

[8] S. De Haes, and W. Van Grembergen, (2009), "An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment", Information Systems Management, Vol. 26, 2009, pp.123–137.

AS 8015-2005 je standard za korporativno upravljanje informacionom i komunikacionom tehnologijom koji je objavljen 2005. godine od strane Standarda Australija. Standard navodi principe, model i terminologiju kao osnovni okvir za implementaciju efektivnog korporativnog upravljanja informaciono i komunikacionom tehnologijom (u daljem tekstu IKT[9]) u svakoj organizaciji.

- „Sistem kojim se upravlja i kontroliše sadašnja i buduća upotreba IKT-a. Uključuje procenu i upravljanje planovima za upotrebu IKT-a za podršku organizaciji i praćenje ove upotrebe da bi planovi bili postignuti. Uključuje strategiju i politiku za korišćenje IKT-a u organizaciji.“[10]

Tokom prethodnih decenija stvoreno je nekoliko okvira koji podržavaju implementaciju IT upravljanja. Cobit je okvir zasnovan na najboljoj praksi, fokusira se na procese IT organizacije i kako njihove performanse mogu biti procenjene i praćene.

Biblioteka IT infrastrukture (ITIL) navodi najbolje prakse na polju upravljanja uslugama i pružanja usluga, ali ne pokriva strateški uticaj IT-ja i odnos između IT-ja i posla. Standard o sigurnosti informacija ISO/IEC 27002 (nekadašnji ISO/IEC 17799) često se spominje u kontekstu upravljanja IT-jem. Ovde je zajednički sadržalac upravljanje rizicima IT-ja, razdvajanje problema i podela dužnosti. Vejl i Ros[11] su razvili okvir za procenu IT upravljanja zasnovan na svega nekoliko pitanja i on se koristi za mapiranje zadataka na najvišem nivou za IT nadležnosti u 250 kompanija širom sveta, ali se ne može koristiti za detaljnu procenu IT upravljanja[12].

---

[9]*Skr. IKT - Informaciono i komunikaciona tehnologija*

[10]AS8015-2005, (2005), "Australian Standard for Corporate Governance of Information and Communication Technology (ICT)", 2005.

[11]Weill, P., and Ross, J. W., (2004), "IT governance – How top performers manage IT decision rights for superior results", Harvard Business School Press, 2004

[12]M. Simonsson, P. Johnson, (2005), "Assessment of IT Governance - A Prioritization of Cobit", KTH Royal Institute of Technology, 2005

2.1 UPRAVLJANJE IT USLUGAMA

Upravljanje IT uslugama[13] (u daljem tekstu ITSM ili IT usluge) je disciplina filozofski centrirana prema znanju korisnika o doprinosu informacionih tehnologija unapređenju poslovnih procesa i uspešnom organizacionom poslovanju. ITSM predstavlja kontrast u odnosu na pristupe IT upravljanju i poslovnoj interakciji koji su tehnološki usmereni. Nijedan autor, organizacija ili prodavac ne poseduje pravo na termin „upravljanje IT uslugama“ i poreklo fraze je nejasno. Sledeća rečenica predstavlja karakterističnu izjavu iz ITSM literature:

- Pružaoci IT usluga se više ne mogu fokusirati na tehnologiju i njihovu unutrašnju organizaciju, već sada moraju uzeti u obzir i kvalitet usluga koje pružaju i da se fokusiraju na odnos sa kupcima[14].

ITSM je fokusiran na proces i u tom smislu ima veze i zajedničke interese sa okvirima i metodologijama za unapređenje procesa (npr. TQM, Six Sigma, Upravljanje poslovnim procesom i CMMI). Ova disciplina se ne bavi detaljima korišćenja proizvoda određenog prodavca ili tehničkim detaljima sistema kojima se upravlja. Umesto toga se fokusira na stvaranje okvira za strukturisane aktivnosti vezanih za IT i interakciju IT tehničkog personala sa poslovnim klijentima i korisnicima.

ITSM se uglavnom bavi pomoćnim osobljem i operativnim problemima upravljanja IT-jem (ponekad poznato kao arhitektura operacija), a ne sa razvojem tehnologije. Na primer, ova disciplina se ne bi bavila procesom pisanja kompjuterskog softvera za prodaju ili dizajniranjem mikroprocesora, ali bi se bavila kompjuterskim sistemima korišćenim od strane osoblja za marketing i razvoj posla u hardverskim i softverskim kompanijama. Mnoge ne tehnološke kompanije kao one koje se bave finansijama, maloprodajom ili putovanjima poseduju značajne IT sisteme koji se ne otkrivaju klijentima.

---

[13] *Engl. IT service management* (ITSM ili IT usluge)

[14] IT Service Management Forum, (2002), "IT Service Management: An Introduction", Van Haren Publishing, 2002, ISBN 9080671347.

U ovom pogledu ITSM se može posmatrati kao analog ERP[15]-u (planiranje resursa u korporacijama) za IT. Njegovi istorijski koreni u IT operacijama mogu ograničiti primenjivost na ostale značajne IT aktivnosti kao što su IT upravljanje portfoliom i softverski inženjering.

[15]*engl. ERP - Enterprise Resource Planning-* (planiranje resursa u korporacijama)

3. NEOPHODNOST UPRAVLJANJA INFORMACIONIM TEHNOLOGIJAMA

Upravljanje informacionim tehnologijamaje potrebno da bi se osiguralo da investicije u IT generišu vrednost i ublažavaju rizike vezane za IT, na taj način izbegavaju neuspeh. IT je ključan za uspeh organizacije – efektivno i efikasno pružanje usluga i dobara – pogotovo ako je IT koncipiran da uvede promenu u organizaciju. Ovaj proces promene, koji se uobičajeno naziva "poslovna transformacija" je glavni pokretač novih poslovnih modela i u privatnom i u javnom sektoru. Od poslovne transformacije može biti mnogo koristi, ali takođe ona sa sobom nosi i mnoge rizike koji mogu poremetiti operacije i imati nenamerne posledice. Dilema je kako balansirati između rizika i koristi prilikom korišćenja IT-ja da bi se omogućila organizaciona promena.

Slika 1 - Oblasti fokusa upravljanja IT-jem[16]

[16]Radovanović D., Šarac M., Adamović S., Lučić D., (2011), "Necessity of IT Service Management and IT Governance", IEEE, MIPRO 2011- DE, May 23-27, 2011, Opatija, Croatia, ISSN 1847-3938, p. 84-87

Uprkos naporima softverske industrije da identifikuje i usvoji najbolje prakse u razvoju IT projekata i dalje postoji visok nivo neuspeha i promašenih ciljeva. Većina IT projekata ne ispuni ciljeve organizacije.

Dobra praksa je implementacija organizacione strukture, uključujući okvir za efektivno upravljanje, sa dobro definisanim ulogama i nadležnostima za IT aktere uključujući revizore informacionih službi. Takav okvir osigurava da IT investicije budu usklađene i realizovane u skladu sa ciljevima i strategijom kompanije; bez ovog okvira IT projekti su podložniji neuspehu. Ali mnoge organizacije ne uzimaju u obzir značaj upravljanja IT-jem. Oni započinju IT projekte bez potpunog razumevanja šta su zahtevi organizacije za projekat, i kako je ovaj projekat vezan za ciljeve organizacije.

Identifikacija organizacionih ciljeva za IT je još jedna dobra praksa za upravljanje informacionim tehnologijama. Nekada su viši rukovodioci posmatrali IT projekte iz ograničene perspektive zadatih i ispunjenih ciljeva. Ova neefikasna i ne efektivna perspektiva proizašla je direktno iz nedostatka tehničkog znanja ovih menadžera da bi mogli da se nose sa kompleksnošću ovih projekata. Uz to, ovi menadžeri su nepravedno okrivljeni za veliku neefikasnost izazvanu propustom organizacije da integriše ciljeve IT projekata sa opštim ciljevima organizacije.

Da bi bila uspešna organizacija bi trebala uzeti u obzir sledeće faktore, koji vode ka najboljim praksama: okvir visokog nivoa, nezavisna potvrda kvaliteta, izveštavanje o upravljanju performansama, upravljanje resursima, upravljanje rizikom, strateško usklađivanje i davanje vrednosti[17]:

- *Okvir visokog nivoa* – uključuje definisanje vođstva, procesa, uloga i odgovornosti informacionih zahteva i organizacionih struktura – osigurava usklađenost IT investicija sa opštim strategijama organizacije maksimizirajući primenu raspoloživih IT prilika.

[17]R. Brisebois, G. Boyd, Z. Shadid, "What is IT Governance?", INTOSAI, Working Group on IT Audit, 2008

- *Nezavisna potvrda kvaliteta* – u obliku unutrašnje ili spoljne revizije (ili pregleda) pravovremeno može obezbediti povratnu informaciju o usaglašenosti IT sa politikom, standardima, procedurama i opštim ciljevima organizacije. Ove revizije moraju biti izvedene na nepristrasan i objektivan način da bi menadžeri dobili realnu procenu revidiranog IT projekta.

- *Upravljanje resursima* preko redovnih procena obezbeđuje da IT ima dovoljno resursa, i da su oni kompetentni i efikasni, da bi mogli zadovoljiti zahteve organizacije.

- *Upravljanje rizikom* je ugrađeno u nadležnosti organizacije i obezbeđuje da organizacija i IT redovno procenjuju i izveštavaju o rizicima vezanim za IT i o njihovom uticaju na organizaciju.

- *Strateško usklađivanje* – dogovor između menadžmenta organizacije i IT odeljenja koji omogućava bordu direktora i višim rukovodiocima da shvate strateška IT pitanja. IT strategija demonstrira uvid organizacije u tehnologiju i njene mogućnosti i osigurava da je IT investicija usklađena sa opštim strategijama organizacije, maksimizirajući korišćenje IT prilika.

- *Dobijanje vrednosti* – demonstrira korist koja može biti dobijena od svake IT investicije. Takva investicija bi uvek trebala da se isplati organizaciji i da bude vođena potrebama subjekta koji investira.

- *Izveštavanje o performansama menadžmenta*, uključuje tačni, pravovremeni i relevantni portfolio, program i podnošenje izveštaja o IT projektima višim rukovodiocima, omogućava detaljan pregled napretka ka identifikovanim ciljevima IT projekta. Kroz ovaj pregled organizacija može proceniti IT performanse u smislu šta je ostvareno, a koje nedostatke treba ispraviti. Merenje performansi je dobar način za dobijanje podataka potrebnih za performanse.

3.1 ZNAČAJ MERENJA PERFORMANSI IT PROJEKATA

Merenje performansi je osnova za čvrsto i rigorozno upravljanje informacionim tehnologijama. Da bi organizacija imala dobru upravu mora videti gde leži prava vrednost njenih IT projekata. Dobro definisan set mera performansi omogućava sredstva menadžmentu za merenje uspeha i određuje na koje se oblasti treba fokusirati da bi se povećala efektnost i efikasnost IT projekata. Bez mera performansi bilo bi teško izmeriti napredak koji su IT projekti postigli ka ostvarenju IT ciljeva. Koristi od mera performansi uključuju:

- Unapređenje kvaliteta IT usluga tokom vremena;
- Smanjenje IT rizika tokom vremena;
- Unapređena realizacija;
- Smanjenje troškova realizacije IT usluga tokom vremena.

Postoje dva tipa mera performansi:

- mere razvoja koje se koriste za merenje performansi IT projekata u razvoju,
- mere usluga koje se koriste za merenje uspeha stalnih ili repetitivnih IT usluga.

Za merenje performansi razvoja se koristi propisan set mera za praćenje razvoja projekata koji omogućava organizaciji da meri napredak projekta u svim fazama životnog ciklusa. Generalno se za merenje usluga sredstva za IT usluge dodeljuju programu na osnovu merenja aktivnosti IT usluga koje koristi program.

Nemoguće je nabrojati razne mere koje se koriste za efektivno merenje informacione tehnologije, ali mere koje slede su uobičajene u većini organizacija, i u zavisnosti od toga kada i gde podaci budu sakupljeni mogu biti korišćene i za razvoj projekata i za usluge[18]:

[18]ITIL, (2007), "An Introductory Overview of ITIL V3", London: The UK Chapter of the itSMF, 2007

- *Troškovi IT-ja po kategoriji i po aktivnosti.* - Organizacija može videti količinu investiranu u svaku aktivnost i odrediti dodatu vrednost finansijskih ulaganja.

- *Broj IT osoblja i troškovi analizirani po aktivnostima.* - Organizacija može izmeriti dodatu vrednost svake aktivnosti u poređenju sa količinom izdvojenih resursa.

- *Outsourcing razmere.* - Organizacija može odrediti efektnost sopstvenog osoblja i omogućiti im da ocene njihovo pouzdavanje u spoljne resurse.

- *Incidenti operacionog rizika vezani za IT (broj i vrednost).* - Organizacija može izmeriti kako se postupa sa rizikom tako što će identifikovati rizike, način kako ih smanjiti, i cenu propusta ukoliko ih ne smanji; rezultati ovih merenja bi trebali biti predstavljeni menadžmentu.

Drugi primeri uobičajenih mera uključuju poređenje IT osoblja koje ima puno radno vreme i saradnika, troškovi radnih stanica, incidenti operacionih rizika vezani za IT (broj i vrednost), IT bezbednosni incidenti (broj i vrednost), razna merenja IT projekata, nivo upravljanja IT investicijama određen na osnovu CMM[19] trenutni i projektovani.

[19]*Engl. CMM - Capability Maturity Model*

4. STRATEŠKO PLANIRANJE ZA ORGANIZACIONU KONTROLU

Da bi bio uspešan menadžment mora definisati strategiju i omogućiti efektivno korporativno upravljanje. *Strategija* je definisana kao „adaptacija ponašanja ili strukture sa razrađenim i sistematskim planom." Još jedna definicija strategije je „napraviti fundamentalne promene u načinu na koji organizacija vodi posao". Očigledno, druga definicija ukazuje na to da samo nekolicina ljudi ima tolika ovlašćenja. *Korporativno upravljanje* se često definiše kao „etičko ponašanje korporativnih rukovodilaca prema akcionarima da bi se maksimizirao povrate finansijske investicije[20]." Da bismo razjasnili ko je odgovoran za upravljanje korporacijom trebali bismo koristiti ovu definiciju „voditi na osnovu pozicije ili ovlašćenja." Tri cilja visokog nivoa koje treba da potvrde revizori su[21]:

- **Strateško usklađivanje između IT-a i korporativni ciljevi** (formalna strategija). Potrebno je pravilno planiranje radi raspoređivanja resursa na pravom mestu i s razlogom. Menadžment je uvek odgovoran za izvršavanje (upravljanje korporacijom, preventivne kontrole).

- **Proces praćenja praksi uveravanja izvršnog menadžmenta**. Viši rukovodioci moraju shvatiti šta se zaista događa u kompaniji.

- **Intervenisati po potrebi da bi se zaustavili, izmenili ili ispravili propusti (korektivni postupak)**. Svi imaju neki problem. Menadžment treba da radi na tome da odmah reši probleme umesto da sakriva istinu.

[20]Davis, C., Schiller, M., & Wheeler, K. (2011), IT Auditing: Using Controls to Protect Information Assets. McGraw-Hill Osborne Media, 2nd ed

[21] Isto.

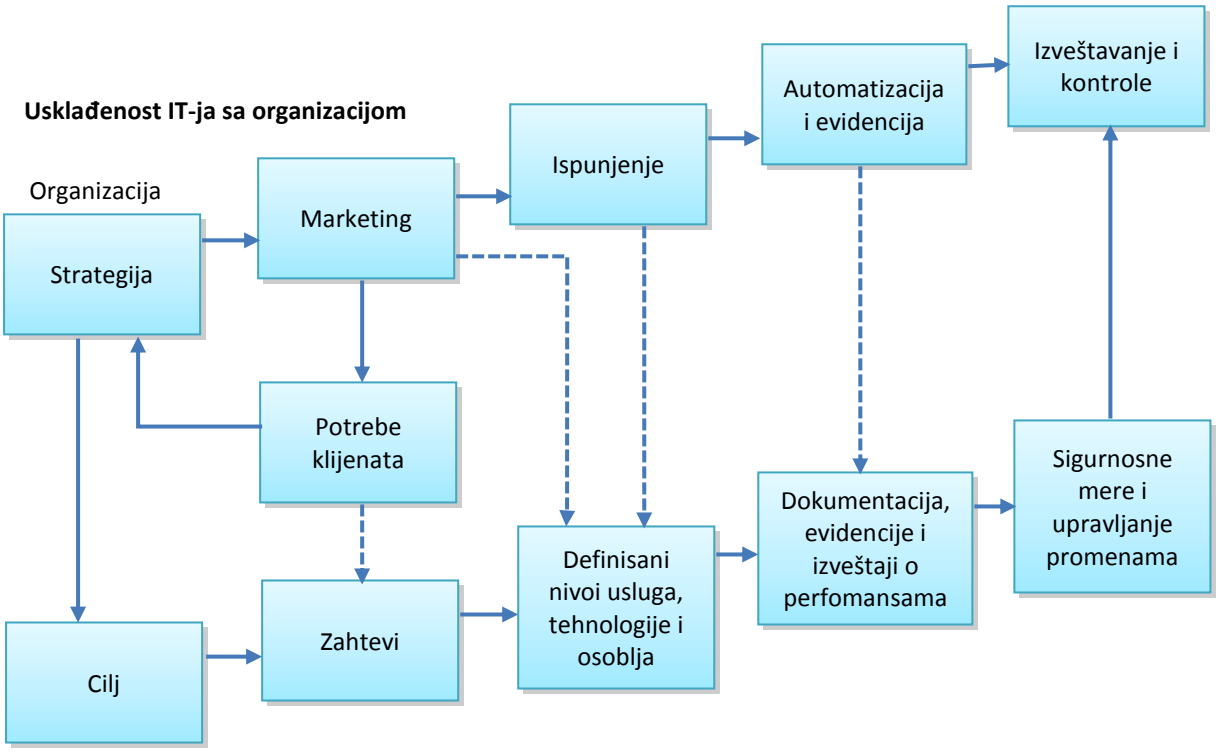
Svaka organizacija treba da razradi sopstvenu strategiju usmeravanja. U kom pravcu treba da krene biznis da bi ispunio svoje ciljeve? Izabrana strategija treba da se fokusira na potrebe klijenata i kako da zadovolji to tržište. Određuju se ključni faktori za uspeh. Marketinške inicijative su zamišljene tako da generišu prihode i zadovolje kupca. Slika 2 demonstrira put organizacionih zahteva u vezi sa IT zahtevima.

Proces zarade prate značajni troškovi administracije i vođenje evidencije. Očekivanja u svakom poslu su zarađivati novac, a ne biti sputan određenom tehnologijom ili vezan za određenog prodavca.

IT odeljenje traži jasno izražen cilj koji se očekuje da ispuni. Odeljenje traži uslove potrebne da bi bili uspešni. Strukturisani dogovor o nivou usluga može biti postignut, sa sve planovima za angažovanje novih kadrova i razvoj tehnologije.

Tehnološki planovi moraju ispuniti poslovne ciljeve. Na primer Amazon.com, ova uspešna on-line knjižara ne koristi samo Microsoft Windows, Macintosh ili Unix. Ono što rukovodioci žele da znaju je da je sav novac obrađen i da proizvod stiže na vreme u skladu sa očekivanjima mušterija. Upravljanje sistemima i revizija će na kraju potvrditi da njihovo računovodstvo i unutrašnje kontrole funkcionišu efektivno.

Na primer - prvi put u industriji Amazon je dodao opciju doplate u iznosu od 5 dolara za slanje istog dana za određene artikle sa lagera onim kupcima koje su geografski blizu skladištima kompanije. Amazon je konsultovao dnevni raspored kurirske rute, a zatim upoređivao raspored preuzimanja i isporuke sa adresom kupca. Porudžbine primljene ujutro mogu stići istog poslepodneva u nekim većim gradovima. Opcija za isporuku istog dana se automatski dodaje u korpu za kupovinu za podobne kupce. Amazon je na ovaj način demonstrirao odličnu integraciju poslovne i IT strategije.



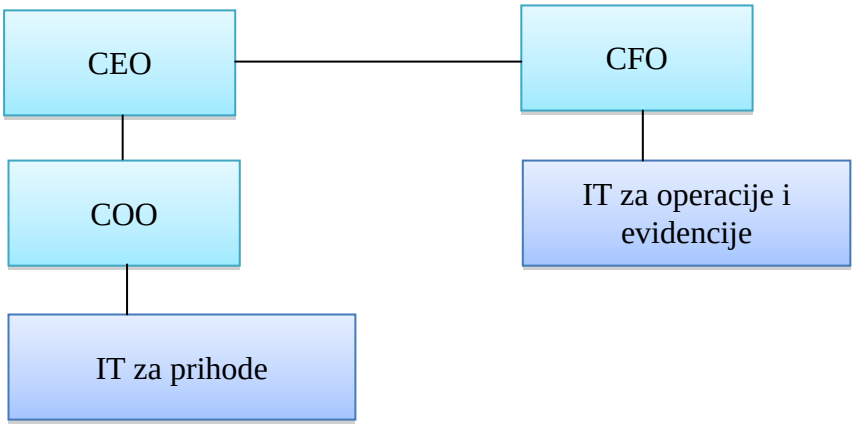
Slika 2- Usklađivanje IT-a sa ciljevima kompanije

Gornja strana ovog dijagrama predstavlja porast prihoda. Rukovodioci sračunato rizikuju da bi iskoristili nove mogućnosti za zaradu. S druge strane, od informacione tehnologije se očekuje da spreči servisne greške koje utiču na prihod i da se fokusira na aktivnosti koje omogućavaju prihod, ali istovremeno i na one aktivnosti koje sprečavaju gubitke na osnovu planova o upravljanju rizikom. Ovo otežava određivanje koji problem ili cilj su prioritet. Revizori mogu steći uvid pregledom IT strukture izveštavanja. IT funkcije izveštavanja operativnom direktoru[22] su usluge koji generišu zaradu. IT funkcije izveštavanja finansijskom direktoru[23] su interne funkcije izveštavanja i obrade kontrola.

Slika 3 prikazuje strukturu izveštavanja i demonstrira svrhu IT-ja.

[22]*Engl. COO – Chief Operating Officer*

[23]*Engl. CFO – Chief Financial Officer*



Slika 3 -Struktura izveštavanja

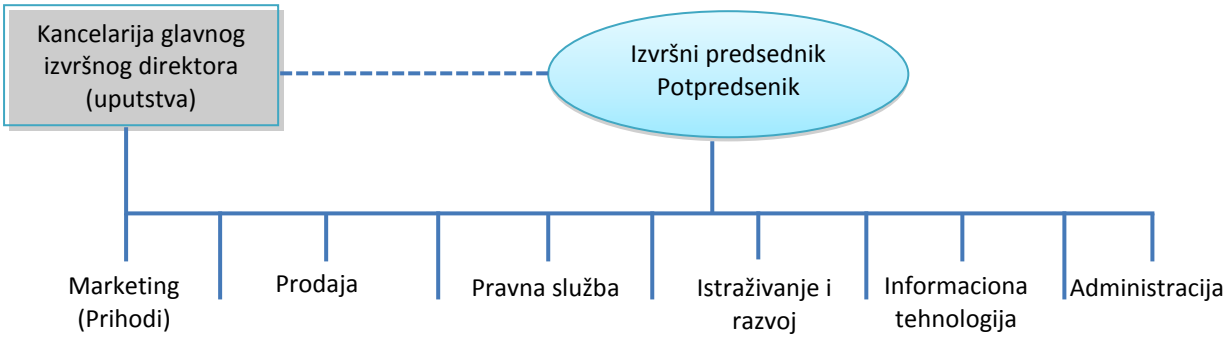
4.1 IT Upravni odbor

Većina organizacija koristi IT strategijski odbor ili IT Upravni odbor. *IT Upravni odbor* se koristi da prenese trenutne poslovne zahteve rukovodilaca posla do IT rukovodilaca. Ime odbora nije toliko bitno kao funkcija koju vrši. Odbor može obavljati više funkcija. IT Upravni odbor može biti i Upravni odbor poslovnog kontinuiteta, ali sa malo drugačijim fokusom. Ono što je bitno je da se posao upravljanja operacijama obavlja u skladu sa poslovnim zahtevima. Upravni odbori moraju imati formalan program koji određuje funkciju svakog člana. Ovaj program određuje odgovornosti i ovlašćenja na sličan način kao program revizije. Ukoliko ne postoji program Upravnog odbora to ukazuje na nedostatak formalnih kontrola – stanje koje zahteva proveru nadgledanja menadžmenta.

Odborom upravlja izvršni predsednik. CEO[24] treba da lično ili preko predstavnika (npr. COO) da saopšti smernice za identifikaciju ciljanih izvora prihoda. Od svakog člana odbora se očekuje da učestvuje u diskusijama vezanim za poslovna pitanja. Povremeno, odbor može pozvati na sastanak posmatrače i prezentere od poverenja da bi se povećala svest o određenoj

[24]*Engl. CEO- Chief Executive Officer*

oblasti. Pošto se identifikuju poslovni ciljevi sledeći korak je određivanje poslovnih ciljeva koje IT treba da ispuni. Upravni odbor se drži ciljeva visokog nivoa umesto da diktira tehničke detalje.



Slika 4- Organizaciona struktura Upravnog odbora

Organizaciona struktura IT upravnog odbora se sastoji od[25]:

- **Marketing** - Marketing treba imati predstavnika u Upravnom odboru. Svrha marketinga je da privuče kupce proizvoda i korisnike usluga organizacije. Čak i ako organizacija pravi najbolji proizvod na svetu to nije bitno dok god ne postoji postojan priliv kupaca.

- **Proizvodnja/Razvoj softvera** - Inputi iz proizvodnje ili razvoja softvera su potrebni radi usklađivanja proizvodnje i prodaje.

- **Prodaja** - Funkcija prodaje je pretvoriti povoljne prilike stvorene tokom marketinške kampanje u sigurnu prodaju. Rukovodioci prodaje su zainteresovani za korišćenje tehnologije da bi pospešili prodaju. Saradnja proizvodnje i tehnologije je neophodna da bi se doprinelo prodaji.

[25]Davis, C., Schiller, M., & Wheeler, K. (2011), IT Auditing: Using Controls to Protect Information Assets. McGraw-Hill Osborne Media, 2nd ed

- **Finansije** - Vođenje finansija i planiranje budžeta su ključni za pravilno korišćenje investicija. Bilo bi teško dobiti odobrenje za finansiranje projekata bez saradnje sa finansijskim kontrolorom.

- **Pravna služba** - Rukovodioci pravne službe moraju osigurati saglasnost sa zakonom. Kvalifikovani pravni savetnik daje pravne savete menadžmentu u nejasnim oblastima. Pravni saveti stručnjaka bi trebali zaštititi kompaniju od preterane odgovornosti ili nepotrebnog rizika kao posledica neuspeha kontrole.

- **Kontrola kvaliteta** - Proces kontrole kvaliteta obezbeđuje konzistentnost u operacijama, proizvodnji i smanjenju rizika. Dobro vođen proces značajno doprinosi opstanku kompanije. Propusti u kontroli kvaliteta mogu oštetiti tržišni imidž ili dovesti do problema sa odgovornošću.

- **Istraživanje i razvoj (R&D – Research & Development)** - Zaposleni u R&D stalno rade na stvaranju novih proizvoda i usavršavanju postojećih. Fokusirani su na razvoj.

- **Upravljanje projektima i programima** - Šef kancelarije za upravljanje projektima, ukoliko takva postoji, trebao bi da bude u Odboru radi savetovanja članova o trenutnim i predloženim projektima. Ideje kupaca mogu zahtevati izmene, stvarajući potrebu da novi projekti modifikuju postojeće programe. Da bi poslovni uspeh bio ostvaren potrebna je promena. Projekti privremeni, dok programi traju godinama ili stalno.

- **Poslovni kontinuitet** - Šef odeljenja za planiranje poslovnog kontinuiteta bi trebao uvek biti prisutan na sastancima Odbora. Ova osoba možda ima zvanje menadžera kontinuiteta ili programskog menadžera ili ima ovlašćenja potpredsednika ili glavnog direktora. Posao ove osobe je da proceni uticaj ili da pomogne iskorišćavanju prilika i tako pruži podršku organizacionoj strategiji. Bitno je da kontinuitet ne bude žrtvovan zarad kratkovidih odluka.

- **Informaciona tehnologija –** IT Direktor[26] ili potpredsednik IT-ja sluša poslovne ideje i ciljeve pokrenute od strane članova Odbora. Ova osoba je veza koja olakšava učešće IT-ja. IT član može poveriti planiranje i istraživanje članovima IT organizacije.

- **Ljudski resursi -** Upravljanje rastom personala se usložnjava svake nedelje. Poštovanje saveznih standarda o radu je obavezno. Internacionalnim organizacijama je potrebna pomoć koja je van stručnosti većine rukovodilaca koji se ne bave ljudskim resursima. Nepoštovanje može izazvati stroge kazne.

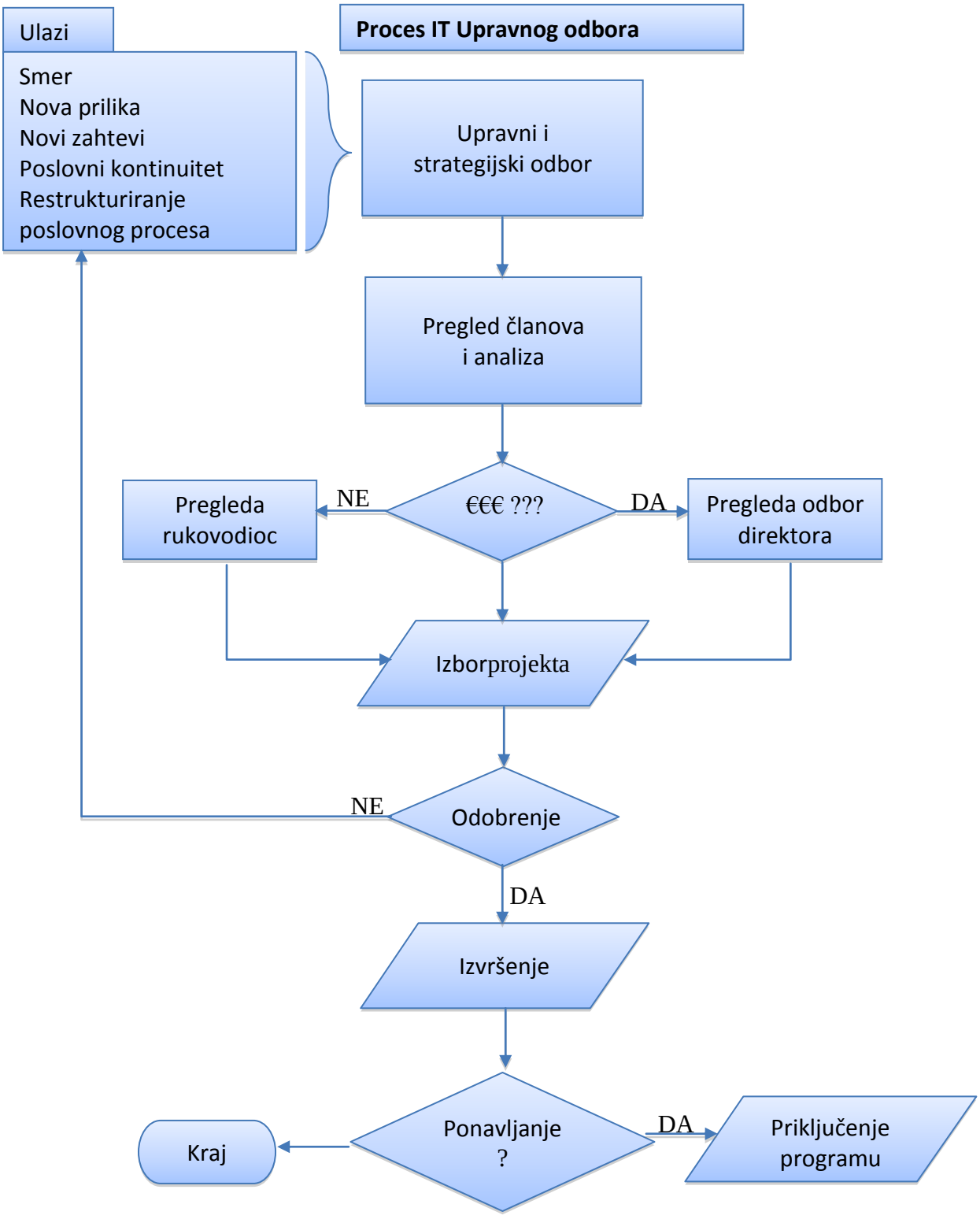
- **Upravljanje radom -** Izvršni predstavnik iz bilo koje radničke organizacije, kao što je radnički sindikat, mogao bi biti uključen u donošenje odluka vezanih za rad. Ovo može biti osetljiva tema u zavisnosti od organizacije.

- **Administracija -** Funkcije upravljanja kancelarijom uključuju računovodstvo, evidenciju i obradu papirologije. Svaki rukovodilac bi bio hendikepiran bez administrativnog asistenta.

Upravni odbor razmatra ideje i mogućnosti za predlaganje. Te predloge zatim razmatra bord direktora. Ukoliko ideja dobije preliminarno odobrenje izdvajaju se sredstva za planiranje projekta. Rukovodioci Upravnog odbora izvrše konačnu procenu poređenjem ukupnog troška i zarade da bi utvrdili da li će ili ne projekat dobiti zeleno svetlo.

Slika 5 predstavlja dijagram toka IT upravljačkog procesa.

[26]*Engl. CIO - Chief Information Officer*



Slika 5- Dijagram toka IT upravljačkog procesa.

Ukoliko projekat bude odobren organizacija specifikuje detalje, utvrđuje program projekta, izdvaja sredstva i resurse i sprovodi plan u delo. Ukoliko je predviđeno da projekat bude događaj koji se ponavlja tada mu se dodeljuje status programa. U suprotnom njime se upravlja kao projektom sa fiksnim vremenom trajanja i članovi tima koji rade na projektu će se razići posle završetka.

U strateškom planiranju, planovi uglavnom traju 3-5 godina. Taktički plan se izvršava u periodu 6 meseci do godinu dana, a može se produžiti i na 2 godine. Dnevni planovi su koraci u taktičkom planu. Kada organizacija planira 3-5 godina unapred onda zaista razvija strategiju.

4.2 Korišćenje Sistema uravnoteženih pokazatelja

Odrediti strateški cilj bez pravog planiranja i smislenih definicija bi bilo nemarno i nepromišljeno. Jedan od najmoćnijih alata za planiranje koji koriste rukovodioci je *Sistem uravnoteženih pokazatelja*[27][28] (BSC). BSC je strateška metodologija osmišljena za više rukovodioce.

Prvobitno BSC je nastao u univerzitetskom okruženju za poslovne rukovodioce za izveštavanje o pokazateljima. Najuspešniji rukovodioci koriste BSC da bi definisali unutrašnje uzrok-posledica veze između manjih planova njihovog posla, a ne za izveštavanje o pokazateljima kao što je zamišljeno.

Pristup uravnoteženih pokazatelja pretvara organizacione ciljeve percepcije potrošača, poslovne procese, rast broja zaposlenih i učenje i finansijske ciljeve u niz definisanih aktivnosti. Uglavnom ove aktivnosti se zovu *projekti* ili *programi*, a BSC ih često naziva inicijativama.

[27] *Engl. BSC - Balanced Scorecard*

[28] Kaplan, R., Norton, D., (2006), "Using the balanced scorecard as a strategic management system", Harvard Business Review

Tabela 1 - Metodologija uravnoteženih pokazatelja

Perspektiva	Isticanje
Kupci	Kakav je naš tržišni imidž? Šta nas čini posebnim? Kako bi organizacija trebala da se predstavi potrošaču? Zašto bi klijent želeo da posluje sa nama?
Poslovni proces	Koja je naša misija? Kako možemo stvoriti autentičnu konkurentnu prednost? Koji su ključni faktori uspeha? Koji su ključni pokazatelji performansi?
Finansije	Koji su finansijski ciljevi? Koji cu ciljevi akcionara? Da li smo krava muzara za investicije ili pioniri-inovatori?
Razvoj i učenje	Koje informacije su nam potrebne da bismo pobedili konkurenciju? Koji su planovi za razvoj organizacije? Kako ćemo čuvati ili steći znanje i radnike neophodne za izvršavanje planova organizacije?

Metodologija pokazatelja je uobičajena i van IT okruženja. IT može imati koristi od korišćenja uravnoteženih pokazatelja ukoliko ih implementiraju CEO ili CFO. Da bi bio efikasan sistemom pokazatelja se mora upravljati od gore ka dole.

4.2.1 Prednosti pokazatelja

Stavlja fokus na posebnu ako-onda (if-then) vezu između različitih ciljeva i njihovih budžeta. Cilj je direktna podrška organizacionim ciljevima. Ukoliko se promeni finansiranje ili strategija povezane inicijative (projekat ili program) to može uticati na pokazatelje. Zapravo, BSC se koristi da bi se stvorile dobro definisane i jasno izražene strategije.

Sve inicijative (programi i projekti) su povezani u tok procesa koji ignoriše odeljenja i tradicionalne granice. Nikada više strategija neće biti određena na jednom sastanku, a sredstva negde drugde.

Posledica pune implementacije biće da nijedno odeljenje neće imati sopstveni budžet. Rezultat je određivanje osoblja na osnovu programa ili projekta. Nije bitno da li je funkcija odeljenja interna ili eksterna.

Svako odeljenje određuje u kojoj će meri podržati definisanu stratešku inicijativu. Novac iz budžeta se prebacuje odeljenju, pod uslovom da ispunjava svoje ciljeve. Izostanak podrške povezanim projektima znači nema novca, nema ljudi, nema posla.

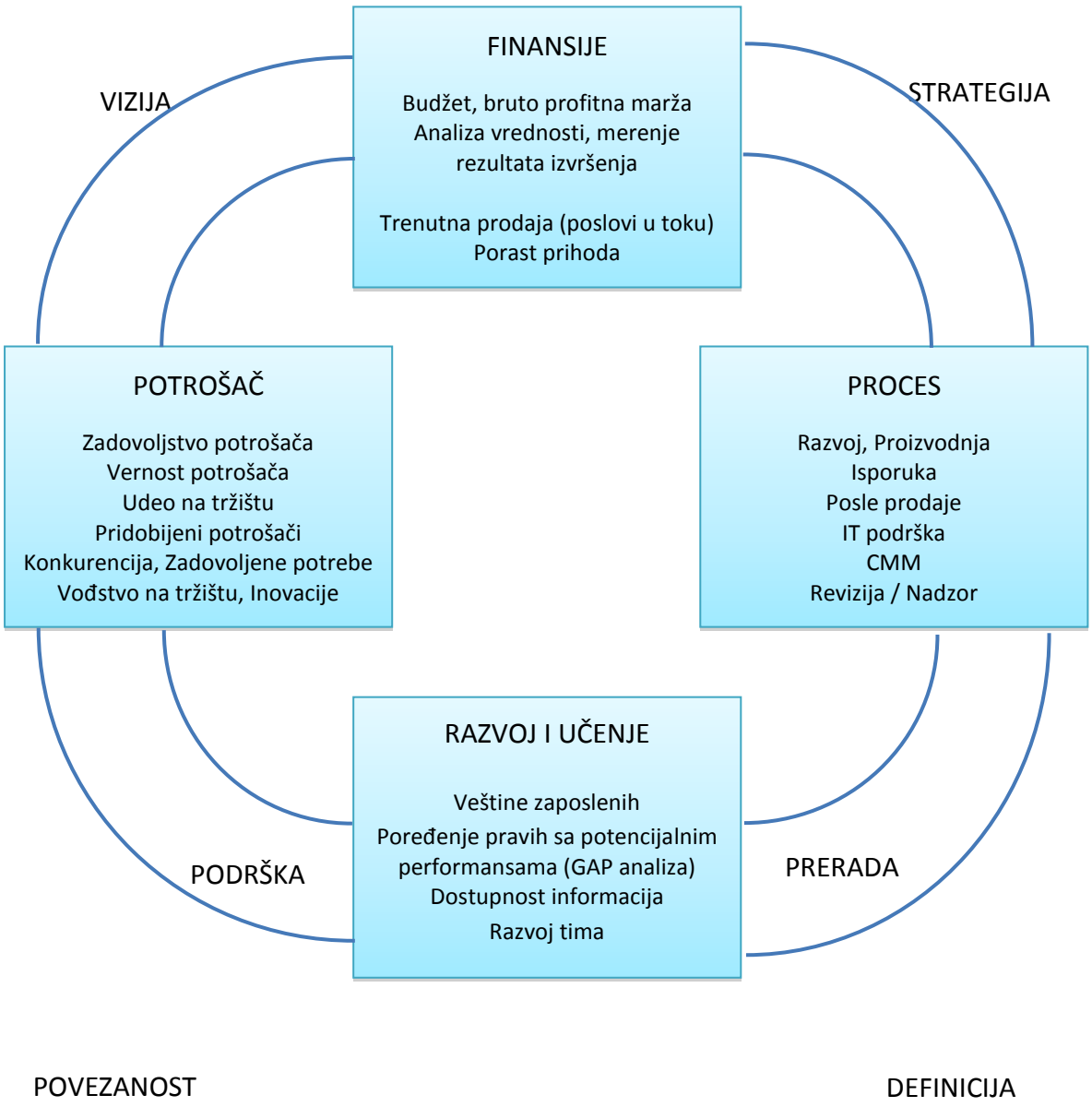
Svaki zaposleni ima lične pokazatelje koji su kreirani podelom BSC-a u specifične zadatke za izvršavanje. Kombinovani efekat ličnih pokazatelja će postići cilj njihovog odeljenja. Postignuće ciljeva odeljenja će pomoći ispunjenje organizacionih ciljeva.

4.2.2 Nedostaci pokazatelja

Pokazatelji zahtevaju pažljiv izbor inicijativa od strane glavnog izvršnog direktora i finansijskog direktora. Objavljeno je u žurnalima o izvršnoj trgovini da merenja dobijena od odbora stalno omanu. Zanimljivo je da opažanja ukazuju na to oni rukovodioci koji ne žele da se prilagode metodologiji pokazatelja takođe ne žele da budu timski igrači ili više žele da grade sopstveno okruženje u okviru organizacije. Politika može da razori BSC ukoliko sponzor ne ukloni ljude koji stvaraju politički konflikt.

Sistem uravnoteženih pokazatelja treba da bude definisano kroz više perspektiva. Može imati 3, 4 ili 5 perspektiva u zavisnosti od toga šta rukovodioci odluče da je potrebno.

Slika 6 je tipičan pristup sa 4 perspektive. Različite inicijative su povezane u kompletan proces.



Slika 6- Sistem uravnoteženih pokazatelja sa četiri perspektive

Strategija funkcioniše u oba pravca sa odličnim definicijama koje dele sve detalje u određene akcione stavke. Inicijative (projekti ili programi) se biraju, određuje im se obim i finansiraju se na osnovu toga koje generišu najviši povraćaj investicija[29] (ROI – Return on Investment).

Šta ako se dogodi da projekat ili program ne stvara zaradu? Jednostavno rečeno, bio bi povezan sa funkcijom koja stvara prihode, i koja se koristi za računanje kombinovanih operativnih troškova. Na primer, sigurnosni troškovi banke se udružuju sa profitom banke. Konačna ROI procena se primenjuje prilikom odlučivanja da li će ta oblast posla biti proširena ili zatvorena. Konačni cilj je naći najviši povraćaj investicija i prestati tračiti sredstva na marginalne aktivnosti ili aktivnosti koje donose gubitke.

Sistem uravnoteženih pokazatelja iz korena menja način na koji zaposleni određuju prioritet i izveštavaju o svom poslu. Aktivnosti i projekti se biraju na osnovu vrednosti stvorenih prema utvrđenim merilima. Ovo utiče i na način na koji se procenjuje zaposleni. Ključno je da menadžment i osoblje prođu odgovarajuću obuku pre implementacije. Bez potpunog prihvatanja na svim nivoima sistem uravnoteženih pokazatelja će biti neuspešan.

4.3 IT podgrupa BSC-a

IT uravnoteženi pokazatelji bi trebali biti podgrupa kompanijinog sistema uravnoteženih pokazatelja. Kada je na pravi način implementirana, metodologija pokazatelja podržava poslovne ciljeve najvišeg nivoa.

ISACA[30] opisuje pokazatelje koristeći tri sloja koji obuhvataju četiri perspektive (kupac, poslovni proces, finansije i razvoj i učenje). Tri sloja za ocenu IT-ja prema ISACA su[31]:

[29] *Engl. ROI – Return on Investment*

[30] Asocijacija za reviziju i kontrolu informacionih sistema

[31] Grembergen W.V., (2008),The Balanced Scorecard and IT Governance, IT Governance Institute

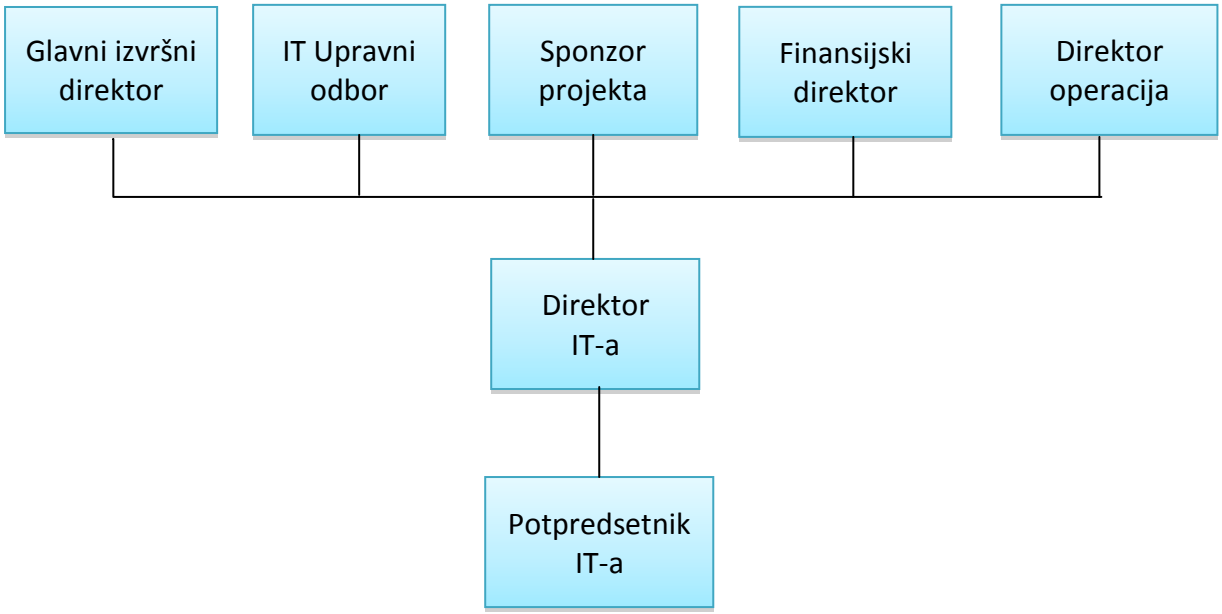
- **Misija -**Stvoriti mogućnosti za buduće potrebe. Obezbediti sredstva od poslovanja za IT investicije. Pružiti efektivne i ekonomične IT usluge. Cilj BSC-a je da pretvori nejasne izjave o misiji u jasne stavke o aktivnostima koje osoblje može da razume i zatim implementira.

- **Strategija -**Postići ciljeve kontrola IT-ja. Uspostaviti kontrolu nad troškovima IT-ja. Ostvarite poslovnu vrednost kroz IT projekte. Obezbedite IT obuku i edukaciju. Korišćenje sistema uravnoteženih pokazatelja može pomoći u definisanju ciljeva nižeg nivoa koji su potrebni misiji da bi bila funkcionalna. Preveliki broj rukovodilaca ne uspe da razradi dobro definisanu, artikulisanu strategiju. Potrebna je definicija koja mapira koordinaciju između odeljenja.

- **Pokazatelji -**Razviti i implementirati smislene IT pokazatelje zasnovane na ključnim faktorima uspeha i ključnim pokazateljima performansi.

5.IZBOR IT STRATEGIJE

Rukovodioci biraju IT strategiju radi ispunjenja poslovnih ciljeva. Strategija bi trebala biti odobrenasa vrha, po principu top – down. Strategija se zatim formalizuje u politiku i saopštava se celoj organizaciji. Slika 7prikazuje rukovodioce koji su uključeni na strateškom nivou (u kreiranju politike).



Slika 7- Rukovodioci uključeni na nivou IT strategije

Prva pretpostavka je da su rukovodioci prošli kroz proces sakupljanja zahteva. Njihova strategija može biti baziranje na kapacitetima korporacije, ili da poslove ustupaju spoljnom saradniku (outsource). Jedno od najbitnijih pitanja je utvrditi kako će strategija biti finansirana. Svaka od metoda ima svoje prednosti i nedostatke[32]:

[32] ITGI (2003),"Board Briefing on IT Governance", 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.

- **Zajednički troškovi** -Uobičajeno je da se najveći deo IT troškova tretiraju kao zajednički troškovi. Ovaj metod je relativno lak za implementaciju od strane finansijskog odeljenja. Nažalost, može dovesti do nezadovoljstva korisnika. Neki korisnici i njihovi menadžeri će osećati da plaćaju uslugu koju ne dobijaju.

- **Povraćaj novca** - Pojedinačna odeljenja dobijaju direktnu naknadu za korišćenje sistema. Ovo je smišljeno kao plati-usput način vođenja računovodstva za IT troškove. Šeme povraćaja novca su prilično uspešne ukoliko su implemetirane na pravi način.

- **Sponzor plaća** -Ovaj poslednji tip može predstavljati značajan izazov za upravljanje IT-jem. Sponzor projekta plaća sve račune. Zauzvrat sponzor može tražiti više ovlašćenja u donošenju odluka. Ovaj metod je ozloglašen po tome što stvara organizacije sa podrškom iz senke. Postojanje ovih organizacija ukazuje na nepoverenje među rukovodiocima. Uobičajeno je osnova grupa iz senke sebična agenda čiji planovi dovode do neuspeha. Dodatni sukobi izbijaju sa IT menadžmentom oko odgovornosti za budžet, ne implementacije svih potrebnih kontrola, nedovoljno efektivnog praćenja i nepravilnog prijavljivanje propusta. Najbolji način rešenja konflikta je potpuna primena podele dužnosti.

5.1. Određivanje politike poslovnih ciljeva

Izvršni menadžment ima obavezu određivanja ciljeva. Svaki cilj treba biti podržan sa definisanim skupom ciljeva. Da bi se ti ciljevi dostigli potrebna je strategija. Naredni korak je određivanje politike koja će biti saopštena podređenima.

Svaka politika treba da bude tako osmišljena da definiše pravac delovanja na visokom nivou. Svrha politike je da informiše zainteresovane strane o odabranom rešenju. Dobro osmišljena politika je bazirana na izjavi menadžmenta o važnosti politike. Izjava objašnjava kako ova

politika podržava poslovni cilj. Politiku zatim potpisuje osoba koja je visoko pozicionirana na hijerarhijskoj lestvici da bi dobila odobrenje.

Uspešna politika se sprovodi top-down u odnosu na sve podređene. Politika može odrediti direktora odeljenja da stvori standard za podršku politike. Konačne procedure stvaraju radnici na dnu hijerarhije. Uobičajene procedure bi trebale biti implementirane od dole ka gore. Procedura je odgovor u prilog politike rukovodilaca osobe sa nižeg nivoa.

5.2. Vrste politike

Politika je osmišljena da informiše zainteresovane strane o određenoj situaciji. Politika može biti savetodavna, regulaciona ili informaciona:

- **Savetodavna politika -** Savetodavna politika objašnjava stanje koje politika treba da spreči i daje obaveštenje o posledicama neuspeha. Zainteresovana strana može biti neko zaposlen u kompaniji. Tema može biti prihvatljiva upotreba interneta. U slučaju interneta savetodavna politika predviđa ili pridržavanje pravila ili otkaz.

- **Regulaciona politika -** Termin *regulacioni* ukazuje na to da je ova politika propisana nekom vrstom zakona. Od svih organizacija pod jurisdikcijom regulacije se očekuje poštovanje. Nepoštovanje će rezultovati krivičnom odgovornošću.

- **Informaciona politika -** Informaciona politika obaveštava javnost o operativnoj politici organizacije. Primeri uključuju zaštitu privatnosti kupaca, refundiranje novca kupcima i politika zamene artikala.

Pošto strategija bude odabrana, a ciljevi i politika određeni vreme je da se započne proces planiranja. Prilikom planiranja strategija se deli u upotrebljive definicije da bi se približila stvarnosti.

5.3. Implementacija planiranja IT strategije

IT strateški planovi moraju biti stvoreni da bi pomogli kratkoročnim i dugoročnim poslovnim ciljevima. Svaki IT plan trebao bi odgovarati određenom organizacionom cilju. Poslovni cilj može biti unapređenje kontakta sa kupcima, proširenje usluga e-trgovine ili poboljšanje brzine rada boljom softverskom integracijom. IT plan može definisati implementaciju i podršku za novi sistem upravljanja odnosima sa kupcima (CRM[33]). Uloga IT-ja je da bude posrednik i čuvar zahteva. Prava strateška vrednost biće određena u glavama poslovnih rukovodilaca. Trebalo bi da postoji zabrinutost ukoliko uticaj IT-ja nadjačava druge poslovne ciljeve nepovezane sa IT-jem. IT strategija će biti sačinjena od planova vezanih za podatke, softverske aplikacije, tehnologiju, personal i objekte.

5.3.1. Planovi o podacima

IT planovi o podacima se stvaraju u prilog planirane upotrebe podataka od strane organizacije. Primer je stvaranje novog sistema za anketiranje kupaca, sistema baze podataka marketinga ili finansijskog sistema za evidenciju. Ključno je utvrditi koji podaci su ti zaista potrebni i kako se zaštititi. Ovo se postiže implementacijom programa za klasifikaciju podataka sa administrativnom politikom i procedurama. Kada bude određena prava namena podatka sledeći korak je definisanje aplikacije koja će manipulisati podatkom.

5.3.2. Plan za upravljanje aplikacijom

Softverske aplikacije su u osnovi metode izvršenja posla. Zato je potreban plan upravljanja softverom da bi definisao vrstu posla koji će biti obavljen. Na primer, banka može biti u istoj industriji kao i kompanija za naplatu dugova. Međutim, obe organizacije koriste različite softverske aplikacije. Softverske aplikacije trebale bi biti skrojene da odgovaraju potrebama klijenta.

[33]*Engl. CRM - Customer Relationship Management*

Moguće je steći prednost nad konkurencijom koristeći drugačiji proizvod. Prednost podrazumeva viši nivo poslovne integracije i/ili manje operativne troškove. Upravo je pitanje razlike u ceni razlog zašto neke aplikacije koriste open source[34] MySQL za baze podataka umesto Oracle (komercijalno rešenje). I jedan i drugi su dobri proizvodi. Razlika u ceni može omogućiti dodatna sredstva za investiciju u razvoj veoma integrisanog softvera od strane tehnološkog stručnjaka koji može stvoriti prednost nad konkurencijom sa nižim operativnim troškom. Taj softver može imati jedinstvenu funkciju koju će konkurent imati teškoća da izdejstvuje zbog zahtevanog znanja, vremena za vođenje ili dodatnih investicija. Izbegavanje troškova može biti kompetetivna prednost. Rizik vezan za aplikaciju podrazumeva da do integracije ne dođe ili da je funkcija manjkava.

Kompjuterski softver predstavlja značajnu investiciju. Softver stvara poslovne rizike kojima se moramo baviti. Rizici podrazumevaju neuspeh procesa, povećan operativni rizik, ne efektivne rezultate, traćenje resursa kapitala, izgubljeno vreme i povećani operativni troškovi za isti efektivni učinak.

5.3.3 Tehnološki plan

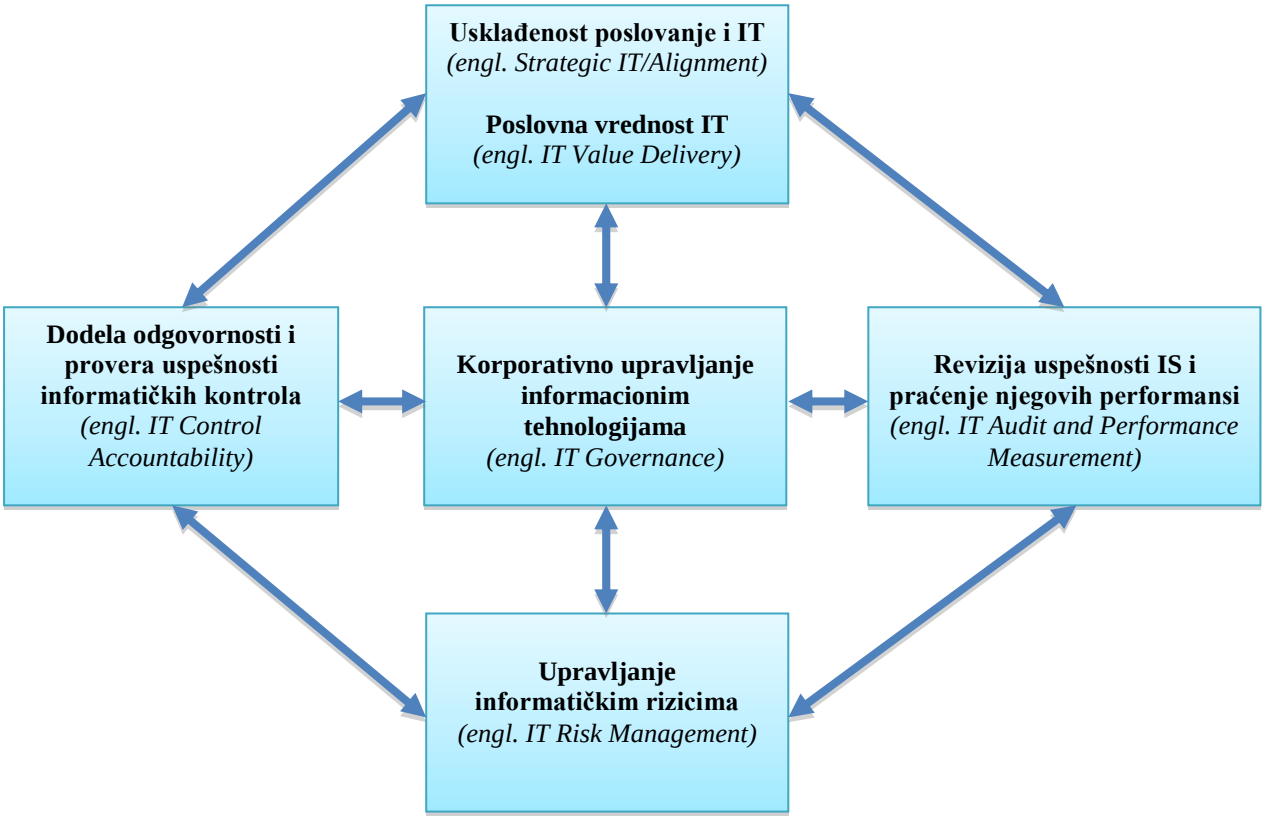
Tehnološki planovi se odnose na tehničko okruženje organizacije određujući vrste hardvera i softvera koje će biti korišćene. Nažalost, neke organizacije prvo počinju sa hardverom i zatim pokušavaju da povežu podatke i zahteve aplikacija sa željenom tehnologijom. Forsiranje tehnoloških planova može omesti rezultate.

5.3.4 Organizacioni plan

IT organizaciona struktura treba da budetako osmišljena da podržava poslovnu strategiju. Informaciona tehnologija se uglavnom smatra funkcijom unutrašnje administracije. Ovo bi svrstalo IT pod ingerenciju šefa unutrašnje kontrole (finansijski direktor, potpredsednik finansija ili kontrolora.

[34] Besplatan softver otvorenog koda

6. KOMPONENTE KORPORATIVNOG UPRAVLJANJA INFORMACIONIM TEHNOLOGIJAMA



Slika 8- Komponente korporativnog upravljanja IT-om

Slika 8 prikazuje osnovne komponentei područja primene koncepta korporativnog upravljanja informacionim tehnologijama. Sastoji se od 4 glavne komponente[35]:

[35]Panian, Z., & Spremic, M. (2007), Korporativno upravljanje i revizija informacijskih sustava. Zagreb, Zgombić & Partneri.

- **Strateško povezivanje poslovanja i IT-a**[36] u sklopu kojega se određuje strateška uloga i povezanost IT-a sa poslovanjem i **stvaranje nove (dodatne) vrednosti iz primene informatike**[37] koje će odnosi na to kako organizovati i upravljati IT-om tako da on postane sredstvo stvaranja nove vrednosti, a ne samo trošak i pozadinska poslovna funkcija. U ovom području posebno je važno uspostaviti korporativne mehanizme (odnosno, mehanizme korporativnog upravljanja) koji će se primenjivati na donošenje odluka o ulaganjima u informatiku i nadzoru i kontroli sprovođenja informatičkih projekata. Pri tome se za vrednovanje poslovnih učinaka investiranja u IT koriste operativne (analize troškova, studije izvodljivosti, stope povraćaja ulaganja, itd.) ali i strateške metode finansijske analize poput novije Val IT inicijative.

- **Upravljanje rizicima u IT-u**[38] predstavlja sastavni deo upravljanja korporativnim rizicima kojima se procenjuje izloženost organizacije raznim rizicima primene informacionih tehnologija u njenom poslovanju (poslovni rizik, rizik za finansijske izveštaje, rizik kontinuiteta poslovanja, reputacioni rizik, razni operativni rizici, itd.). Unutar ovoga područja potrebno je razraditi i plan upravljanja rizicima, stalno pratiti nivoe rizika, njihov uticaj na poslovne procese i odrediti efikasne protivmere (odgovarajuće kontrole). Metode i okviri koji se pri tome koriste su CobiT, ISO 27001 norma, ITIL (ISO 20000), Basel II, itd.

- **Dodela odgovornosti i provera uspešnosti informatičkih kontrola**[39] predstavlja okvir kojim se meri i proverava uspešnost IT kontrola. To se pre svega odnosi na jasnu i nedvosmislenu dodelu odgovornosti za sprovođenje informatičkih aktivnosti i proveru uspešnosti kontrola ugrađenih u informacioni sistem kako bi se poslovanje moglo odvijati neometano, uspešno i u skladu sa očekivanjima. Sarbanes-Oxley akt

[36] *Engl. Strategic IT/Alignment*

[37] *Engl. IT Value Delivery*

[38] *Engl. IT Risk Management*

[39] *Engl. IT Control Accountability*

propisuje da su članovi najvišeg menadžmenta odgovorni za tačnost, celovitost i pouzdanost informacija, kao i za kontrolu procesa finansijskog izveštavanja, koji je gotovo u svim kompanijama potpuno zavisan od automatizma rada informacionog sistema, pa njegova uspešnost i tačnost mahom zavisi od ugrađenih unutrašnjih kontrola. Osim toga IT menadžment treba da bude odgovoran za povraćaj ulaganja u informatiku i proveru (reviziju) rada informacionog sistema. U ovom području često koriste metode kao što su CobiT, ISO 27001 norma, ITIL, Basel II.

- **Revizija uspešnosti informacionog sistema i praćenje njegovih performansi**[40] predstavlja metrike kojima se kvalitativnim i kvantitativnim ocenama meri uspešnost sprovođenja raznih (informatičkih) procesa, čime se vrlo precizno i detaljno mogu meriti performanse informatike kao poslovne funkcije. Revizija informacionih sistema predstavlja postupak analize i provere njihove tačnosti, efikasnosti, delotvornosti i pouzdanosti. Rezultat tih koraka je izveštaj IT revizora.

[40] *Engl. IT Audit and Performance Measurement*

DRUGI DEO

REVIZIJA INFORMACIONIH SISTEMA

1. UVOD

Informaciona tehnologija je postala imperativ savremenog poslovanja, a informacioni sistemi (IS) su njegov sastavni deo i podrška poslovnom menadžmentu kompanijau kojima su tačne, pravovremene, precizne i sadržajne informacije oblikovane prema potrebama menadžmenta. Rad informacionih sistema i svi njegovih delova treba pratiti, kontrolisati i proveravati. Neophodan element za uspeh i održivost kompanija je efikasno korišćenje informacionih tehnologija. Sve je veća zavisnost od informacija i pridruženih sistema kao i stepen njihove ranjivosti.

Postoji više razloga zbog kojih se kontrola i revizija smatraju aktivnostima od presudnog značaja u nastojanjima za ostvarivanje očekivane delotvornosti i efikasnosti informacionih sistema.

2. SVRHA I ULOGA REVIZIJE INFORMACIONIH SISTEMA

Revizija IS[41] je proces za prikupljanje i procenu dokaza na osnovu kojih se potom procenjuje uspešnost i efikasnost informacionog sistema. Određuje se da li informacioni sistem radi u funkciji očuvanja imovine i održavanja celovitosti podataka i ocenjuje da li informacione tehnologije deluju u skladu sa ciljevima kompanije i da li efikasno podupiru ciljeve poslovanja. Revizijom se ispituje zrelost upravljanja i ocenjuje kontrola informacionih sistema na raznim hijerarhijskim nivoima.

Objekat revizije informacionih sistema je sistemsko, temeljno i pažljivo pregledanje kontrola unutar svih delova informacionog sistema, a osnovni zadatak je proceniti njegovo trenutno stanje, poput zrelosti i nivoa uspešnosti, otkrivanje rizičnihpodručja i nivoa rizika, kao davanje preporuka menadžmentu za unapređenjeprocesa upravljanja sistemom.

Revizijom se utvrđuje da li je sistem internih kontrola koji je uspostavljen radi upravljanja rizicima, kontrole i rukovođenja tim procesima adekvatan i da li funkcioniše na način kojim se obezbeđuje[42]:

- da su rizici na odgovarajući način identifikovani i kontrolisani,
- da su međusobni odnosi članova rukovodstva uspostavljeni na odgovarajući način (horizontalna i vertikalna povezanost),

[41] *Engl. Information system audit*

[42] Stanišić M., Radovanović D., Lučić D., "Revizija informacionih sistema", Singidunum revija, Vol. 6, No. 2, Beograd, 2010, ISSN 1820-8819, 72-81.

- da su bitne finansijske, upravljačke i operativne informacije i izveštaji pravovremeni, tačni i potpuni,
- da zaposleni obavljaju poslove u skladu sa propisanim standardima i procedurama,
- da su sredstva ekonomično nabavljena, da se efikasno i racionalno koriste i da su adekvatno zaštićena,
- da su programi, planovi i ciljevi organizacije ostvareni,
- da su kontrolni procesi kvalitetni i da se stalo unapređuju,
- da su rukovodstvo i zaposleni pravovremeno upoznati sa zakonima, drugim propisima i opštim aktima koji su iz njihovih delokruga,
- da je poslovanje usklađeno s politikom, planovima, procedurama i propisima.

Revizori informacionih sistema su malobrojni resurs. Informacione tehnologije se stalno unapređuju i razvijaju. Iz tog razloga, bitno je da revizori IS održavaju svoju stručnost kroz usavršavanje postojećih veština i znanja, kao i sticanje novih znanja vezanih za revizorske tehnike i IT. Neophodno je da revizor razume tehnike za upravljanje projektima revizije sa neophodnim brojem adekvatno obučenih revizora. Međunarodni standardi revizije zahtevaju da revizor informacionih sistema bude tehnički stručnjak, da ima veštine i znanje potrebne za obavljanje revizorskog posla. Takođe, on treba da održava svoju tehničku stručnost kroz odgovarajuće kontinuirano profesionalno usavršavanje. Prilikom planiranja revizije i dodele članova tima konkretnim revizijama treba uzeti u obzir njihova znanja, veštine i iskustva iz prethodnih revizija.

Poželjno je da postoji detaljan godišnji plan stručnog usavršavanja zaposlenih, koji je zasnovan na pravcu daljeg razvoja organizacije u pogledu tehnologije i rizika koji treba da se procene. Ovaj plan treba da se polugodišnje pregleda i ažurira kako bi se obezbedilo da su potrebe za usavršavanjem u skladu sa pravcem razvoja organizacije. Rukovodstvo revizije informacionih sistema treba da obezbedi potrebne IT resurse koji su potrebni za stručno izvođenje revizije IS (npr.: softver, skeneri za testiranje računarske mreže, itd.).

3. TIPOVI REVIZIJE

3.1 Revizija informacionih sistema nastala u kontekstu tradicionalne (ili konvencionalne) revizije

Izvorno, revizija je aktivnost usko usmerena na utvrđivanje ispravnosti računovodstvenih iskaza, odnosno finansijskih izveštaja neke organizacije. Tradicionalna revizija postoji u dva oblika – ekterna (spoljašnja) i interna (unutrašnja) revizija. Pri tome je eksterna revizija uglavnom fokusirana na oblast finansija, zbog čega se često naziva i finansijska revizija, i ima za cilj davanje objektivnog i nezavisno stečenog mišljenja o ispravnosti finansijkih iskaza (izveštaja) nekog pravnog lica (kompanije, javne ili državne ustanove itd), što se uglavnom odnosi na relevantnost, tačnost i celovitost predmetnih finansijskih izveštaja. Za razliku od eksterne, interna revizija se kreće u znatno širim okvirima i okreće se svim problemima koji generalno mogu da spreče određenu organizaciju u postizanju njenih ciljeva. Interna revizija sistematski i metodično preispituje sisteme internih kontrola u predmetnoj organizaciji i analizira sve poslovne procese i procedure sa ciljem da otkrije probleme, ukaže na njih i da preporuči odgovarajuće mere. Dok eksternu reviziju u nekoj organizaciji obavljaju zasebne, specijalizovane i za to ovlašćene firme, interna revizija se po pravilu nalazi unutar same organizacije čiju reviziju vrši i predstavlja njen sastavni deo.

Sa razvojem informacionih tehnologija, došlo je do njihove masovne primene u svim poslovnim sistemima. Svi poslovni procesi, uključujući i finansije, pritom dobijaju svoju implementaciju u odgovarajućim informacionim sistemima, čime se uspostavlja trajna i vrlo duboka zavisnost celokupnog savremenog sveta od informacionih tehnologija. Sve vrste biznisa, finansijske institucije, državne administracije, sistemi uprave, mediji i sve ostale organizacije zavise u ogromnoj meri od informcionih tehnologija koje koriste.

Prirodno, u novo nastalim uslovima, revizija (pre svega interna) vremenom biva prinuđena da se bavi i tehnologijom, razvijajući posebne aktivnosti unutar revizije koje su samo tome posvećene. Ona najpre kreće da analizu poslovnih procesa prilagodi novim uslovima primenjujući odgovarajuću aplikativnu logiku preko koje su ti poslovni procesi implementirani u informacionim sistemima. Dalje, revizija počinje da traži logiku tradicionalnih sistema internih kontrola unutar informacionih sistema i da pronalazi načine da se u okviru tih kontrola otkriju slabosti i praktične mogućnosti za njihovo prevazilaženje.

Ovaj pravac razvoja je danas dospeo do tačke u kojoj revizija informacionih tehnologija počinje da biva prepoznata kao zasebna disciplina u okviru konvencionalne interne revizije.

Mogu se izdvojiti sledeće karakteristike ovako uspostavljene revizije informacionih tehnologija:

- Revizori se biraju većinom iz redova stručnjaka za računovodstvo i finansije koji se dodatno obrazuju za informatičku oblast. Stručnjaci tehničkog profila su u manjini i mahom čine samo tzv „informatičku podršku" revizorima

- U većini slučajeva, fokus je uglavnom unutar dve grupe kontrola: prvo, tzv generalnih kompjuterskih kontrola i, zatim, kontrola u okviru aplikacija. Predmet revizije je ograničen uglavnom na one elemente informacionih sistema koji se mogu shvatiti kao digitalna analogija odgovarajućih konvencionalnih mehanizama kontrole: autentifikacija, autorizacija, potvrđivanje transakcija, validacija unosa podataka, validacija prikaza podataka, razdvajanje (segregacija) dužnosti i slično. U većini slučajeva, fokus ostaje zatvoren unutar aplikativnog sloja.

- Revizija je uglavnom interna. Nezavisnost i objektivnost u odnosu na druge delove organizacije se pritom postižu uspostavljanjem zasebne specijalizovane celine unutar organizacione strukture, što nije uvek moguće i dosta često i nije slučaj.

- Postoje preduslovi za razvoj formalnog i proceduralnog pristupa reviziji, pa čak i određeni pritisci unutar zakonske i profesionalne regulative za kretanje u tom smeru; u isto vreme, sloboda izbora je manja, najčešće nema istraživačkog i eksperimentalnog rada, skup korišćenih alata je vrlo ograničen.

- Favorizovani su revizorski pristupi koji polaze od organizacione šeme, od podele uloga i odgovornosti u organizaciji a u novije vreme i od prethodno procenjenog rizika; suprotno tome, pristupi koji uzimaju za polazište topološke, funkcionalne i druge složenije tehnološke karakteristike sistema retko se ili uopšte ne koriste.

3.2 Revizija informacionih sistema nastala u kontekstu samih informacionih sistema

Ovaj pravac razvoja je tekao potpuno nezavisno od konvencionalne revizije i bez ikakve veze sa profesijom tradicionalnog revizora. On je nastao kao sastavni deo samih informacionih tehnologija i to kao iskaz prirodne potrebe da se tehnologija sama po sebi mora podvrgavati reviziji u toku celog svog životnog ciklusa. Razvoj tehnologija i tehničkih rešenja koja se na njima zasnivaju oduvek je podrazumevao i potrebu za revizijom. Sve faze životnog ciklusa jednog IT rešenja obavezno uključuju detekciju, reakciju i korekciju, pa je tako, u ovom kontekstu, na prirodan način došlo do prepoznavanja potrebe da se revizija informacionih tehnologija izdvoji u posebnu disciplinu u okviru informatike i da bude prihvaćena kao zasebna profesija. Ovako shvaćena revizija informacionih tehnologija ima sledeće karakteristike:

- Revizori su uglavnom tehničkog stručnog profila – računarstvo, informatika, telekomunikacije i sl; dodatno obrazovanje i usavršavanje iz oblasti ekonomije, finansija, računovodstva, menadžmenta itd. vrlo se retko ili uopšte ne sprovodi.

- Predmet revizije je tehnologija u celini a ne samo pojedini delovi sistema ili izolovane aplikacije; prisutna je sklonost da se tehnologija posmatra kao isključivi

predmet revizije, pri čemu se tradicionalni predmeti revizije – finansijski, računovodstveni itd – često potpuno izuzimaju iz razmatranja.

- Revizor je pozicioniran izvan organizacije koja je predmet revizije – tehnologije su u privatnom vlasništvu klijenta revizije ili dobavljača/proizvođača, te je revizor najčešće u poziciji da nema sukoba interesa.

- Postoje izraziti preduslovi za nezavisnost i objektivnost u radu, kao i za istraživački i eksperimentalni pristup.

- Postoji veća sloboda u izboru postupaka, tehnika i alata, ali se često zaostaje u formalizaciji postupaka, dokumentovanju i proceduralnom pristupu reviziji.

- Pristupi koji podrazumevaju dublje poznavanje tehnologije se ovde ne zapostavljaju, što je prirodno s obzirom na kontekst koji je po sebi dominantno tehnički; naprotiv, topologija, funkcionalna podela, višeslojnost sistema i slično ovde su znatno prisutniji nego u tradicionalno shvaćenoj reviziji; u novije vreme, pored striktno tehnoloških, u prvi plan dospevaju personalni aspekti, socijalni inžinjering, etičko hakovanje i druge, često vrlo inventivne, tehnike revizorskog pristupa

4. PROCES REVIZIJE I REVIZORSKE AKTIVNOSTI

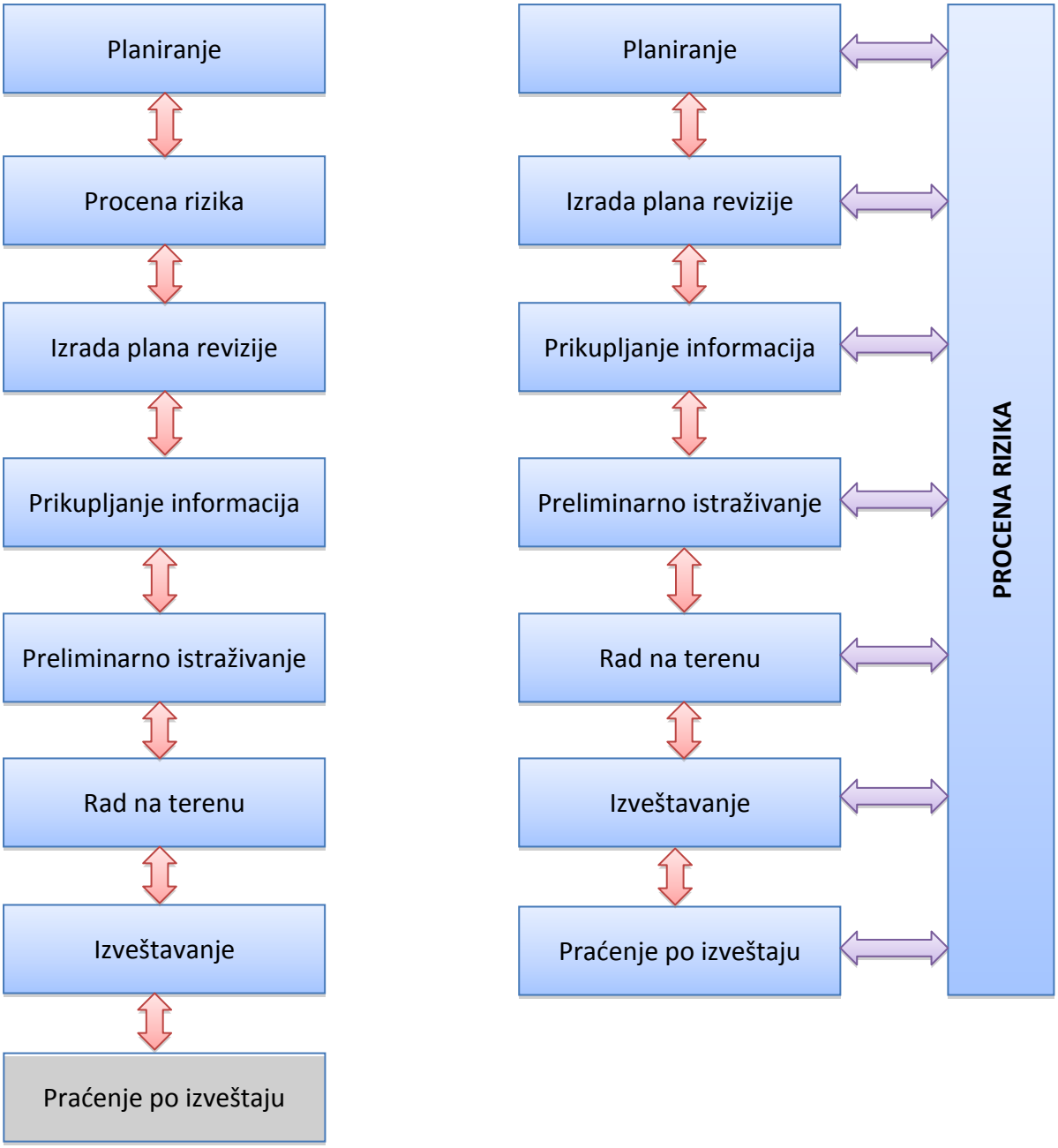
4.1. Životni ciklus procesa revizije

Proces revizije je neprekidan i ima kružni tok. On ima nekoliko prepoznatljivih faza koje se smenjuju u toku životnog ciklusa. Proces počinje planiranjem, nastavlja se nekom vrstom pripreme, neposrednim izvođenjem revizorskog zadatka (radom na terenu), izradom i predajom izveštaja i završava se daljim praćenjem po izveštaju. Ovaj ciklus se zatim kontinuirano ponavlja. U literaturi postoje razlike kod definisanja pojedinih faza. Najčešće, razlike su u rezoluciji detalja kojom se ciklus prikazuje: pojedine faze se prikazuju kao sekvenca od dve ili više detaljnijih faza ili obratno, što se svodi na različit broj faza u ciklusu. Pored toga, često srećemo i različite nazive pojedinih faza.

Međutim, povremeno se sreću različita shvatanja u pogledu mesta koje u revizorskom ciklusu treba da ima procena rizika.

4.2. Procena rizika

U savremenim organizacijama srećemo zasebne organizacione celine koje se bave tzv. upravljanjem rizikom *(engl. Risk Management).* Upravljanje rizikom je krajem prošlog veka pa do danas prošlo kroz ubrzan i snažan razvojni proces i dostiglo status veoma značajne komponente svakog poslovanja, pa čak i zasebne stručne grane sa samostalnom stručnom teorijom i praksom. Razvijeni su mnogi radni okviri i metodologije za kategorizaciju, identifikovanje, procenu i merenje, kao i za minimizaciju, izbegavanje, transfer i druge načine za kontrolu i upravljanje rizikom. Spremnost za reagovanje u situacijama kada dođe ili može doći do ishoda negativnih po poslovne ciljeve ugrađuje se danas u strateške i operativne planove svih uspešnih organizacija.



Slika 9- Životni ciklus revizije informacionih sistema

Iako upravljanje rizikom nije u oblasti direktne odgovornosti interne revizije, revizorski posao je neraskidivo vezan za procenu rizika. Uobičajeno je da se procena rizika smatra posebnom fazom u životnom ciklusu revizije, koja dolazi neposredno pre ili neposredno posle faze planiranja. U novije vreme često se koristi fraza Risk-based (ili Risk-driven) Auditing, čime se želi istaći da je određeni revizorski pristup zasnovan na riziku ili je vođen rizikom.

Dosledno gledano, ako se zaista želi da se revizorski posao odvija sa punom svešću o prisutnim rizicima, onda je verovatno najispravniji pristup kod kojeg sve faze životnog ciklusa revizije uključuju i procenu rizika kao svoj sastavni deo. Do saznanja o slabostima i nedostacima predmetnog sistema usled kojih smo izloženi rizicima, može se doći u svakoj fazi revizije. U svakoj od faza revizije procena ovih rizika može i treba da utiče na eventualne modifikacije u daljem toku odvijanja revizorskog ciklusa. Slika 9 ilustruje tok životnog ciklusa revizije i mesto procene rizika u njemu.

4.3. Planiranje

Planiranje revizije predstavlja prvi korak u svakom konkretnom revizorskom zadatku. Dugoročno planiranje se po pravilu odražava kroz izradu godišnjeg plana rada, u kojem se definišu ciljevi, predmet, resursi, opseg i trajanje za određeni broj konkretnih zadataka na kojima će revizori biti angažovani u predstojećem jednogodišnjem periodu. Ovaj plan predlaže rukovodilac interne revizije a usvaja ga odbor za reviziju, generalni direktor ili drugi organ najviše uprave kojem je interna revizija odgovorna. Godišnji plan mora da bude u skladu sa strategijom, poslovnim ciljevima i potrebama organizacije. Takođe, sadržaj godišnjeg plana rada se mora uskladiti sa prethodno procenjenim rizicima u organizaciji. Pošto su resursi po pravilu ograničeni, revizija nije u mogućnosti da "radi sve", već mora da se fokusira samo na najvažnije oblasti, tj. na one koje su prioritetne sa aspekta verovatnoće nastupanja i štetnosti posledica nepovoljnih ishoda.

Kratkoročno planiranje se odražava kroz izradu kratkoročnih planova i kroz planiranje pojedinačnih revizorskih projekata. Dok je izrada kratkoročnih planova neobavezna i ne tako česta, planiranje individualnih projekata je obavezna aktivnost za svaku internu reviziju. Tokom ove aktivnosti revizori dovode u vezu individualne stavke iz godišnjeg plana sa konkretnim uslovima u datom okruženju i u datom momentu (periodu vremena). Revizorski projekat se sinhronizuje sa tekućim aktivnostima klijenta revizije, ponovo se razmatraju ciljevi, resursi opseg i trajanje revizije, kako bi se uskladili sa realnošću tekućih poslovnih procesa.

Dugoročno i kratkoročno planiranje je karakteristično (i obavezno) za sistemski pristup reviziji. Za razliku od sistemskog, postoje i drugi pristupi, koji mogu biti primenjeni u zavisnosti od prirode konkretnog revizorskog zadatka.

Na primer, pored redovnih revizija, gde se zadaci planiraju unapred, postoji i mogućnost angažovanja revizora na vanrednim revizijama. Kod ovakvih zadataka vrlo često nije moguć sistemski pristup, već se poslu pristupa kao da je reč o pojedinačnoj, ad-hok istrazi.

Primeri su vrlo brojni – tu spadaju sve revizije otkrivenih ili nagoveštenih prevarnih radnji, sve revizije po incidentnim situacijama, revizije po dojavama *(engl.* žalbama korisnika itd. U oblasti IT revizije, zbog specifičnosti predmeta revizije, istražni pristup se veoma često koristi. Za sve takve slučajeve, po pravilu, postavljaju se visoki prioriteti realizacije i veoma kratki rokovi. Proces planiranja se tada nužno svodi na kratkotrajne taktičke pripreme, posle čega se prelazi na sledeću fazu – izradu programa revizije. Nije redak slučaj da kod ovakvih zadataka dođe do značajnog odstupanja od godišnjeg plana, preraspodele resursa, prekida tekućih ili odustajanja od planiranih (redovnih) revizorskih zadataka i drugih sličnih posledica. One u opštem slučaju dovode do uvećanja revizorskih rizika, ali se polazi od ocene rukovodstva (razumnog očekivanja) da će to, kroz rezultate revizije, da bude kompenzovano minimiziranjem nekog drugog poslovnog rizika, u ukupnom iznosu koji je pozitivan za organizaciju.

4.4. Izrada plana revizije

Za svaku pojedinačnu reviziju (konkretan revizorski zadatak) neophodno je prethodno izraditi detaljan plan. Ovaj plan se izrađuje kako za redovne (planirane) tako i za vanredne revizije. Svrha plana revizije je da obezbedi sređen i sistematičan pristup predmetu revizije, tako da se izbegne mogućnost da dođe do propusta, grešaka u postupku, odstupanja od zadatih ciljeva ili drugih revizorskih rizika. Plan revizije uspostavlja vezu između opštih revizorskih aktivnosti usaglašenih sa opsegom i ciljevima konkretne revizije sa jedne strane i raspoloživih stručnih i drugih resursa sa druge strane.

Plan revizije najčešće ima dva dela. U jednom, koji služi kao zaglavlje celog plana, identifikuju se i navode klijenti revizije, predmet revizije, opseg rada, ciljevi, ime odgovornog

revizora i članova revizorskog tima, vremena i rokovi. U drugom delu se sadrži konkretna sekvenca revizorskih aktivnosti. Ona povezuje revizorske aktivnosti planirane za svaku od faza revizije sa klijentima revizije, planiranim vremenskim okvirima, revizorima koji obavljaju tu aktivnost, eventualnim dodatno zahtevanim resursima i (po potrebi) sa drugim opštim napomenama.

Plan revizije do detalja prati tok odvijanja konkretnog revizorskog zadatka i služi revizoru kao kontrolno sredstvo – podsetnik za obavljanje revizije – kojim se dodatno obezbeđuje da revizija uspešno ispuni planirane ciljeve. Plan revizije uvažava rezultate prethodne procene rizika, tako što planira aktivnosti po prioritetima u skladu sa tom procenom.

4.5. Upoznavanje sa predmetom revizije

Cilj upoznavanja sa predmetom revizije jeste da se izvrši adekvatna priprema i prikupe sve polazne informacije koje su neophodne za uspešno izvođenje revizorskog zadatka. Takođe, u ovoj fazi, revizor je dužan da identifikuje predmetni sistem i njemu pripadajuće organizacione celine, kao i nosioce rukovodećih uloga i odgovornosti u tim celinama.

Konkretno, revizor je dužan da pribavi i pregleda sledeće:

- sve postojeće prethodne ocene, a koje se odnose na predmetni sistem. Ovo obuhvata prethodne izveštaje interne i/ili eksterne revizije, prethodne procene pripadajućih rizika, eventualne tehničke i administrativne kontrole, izveštaje inspekcija i sve druge izveštaje o stanju predmetnog sistema koji su relevantni za dati revizorski zadatak
- sve zakone, propise i podzakonska akta koji se odnose na predmetni sistem i primenljivi su na datom revizorskom zadatku
- internu regulativu – politike, pravilnike, procedure i drugo što je primenljivo na datom revizorskom zadatku; ukoliko je to primenljivo na konkretnom zadatku, potrebno je pribaviti i sve ugovore koji se odnose na predmetni sistem
- profesionalnu regulativu – smernice, standarde, radne okvire za najbolju profesionalnu praksu i drugo što je primenljivo na datom revizorskom zadatku

- druga relevantna dokumenta i informacije, primenljive na predmetni sistem, kao što su definicije graničnih linija predmetnog sistema, uzajamne veze sa drugim sistemima i sl.

Nakon pregleda prikupljenih informacija, revizor priprema najavu revizije. Najava mora da sadrži:

- Predlog predmeta revizije – ciljeve i opseg revizije
- Vreme početka i procenu trajanja revizije
- Ime nadležnog revizora i podatke za kontakt

Direktor interne revizije odobrava najavu i šalje je klijentima.Sledeća aktivnost je zakazivanje i održavanje uvodnog sastanka sa svakim od klijenata, kako bi se diskutovalo i postigao dogovor o konačnom području i ciljevima revizije, eventualnim promenama u tom pogledu, ključnim kontaktima, vremenu revizije i osoblju koje će je obaviti. Revizor je u obavezi da sačini beleške sa ovih sastanaka.

4.6. Preliminarno istraživanje

Cilj preliminarnog istraživanja jeste da se postigne razumevanje predmetnog sistema, njegovih poslovnih i kontrolnih procesa, ciljeva, prateće regulative i područja odgovornosti. Tokom ove faze, revizor stiče osnovna saznanja o predmetu revizije, tako što prouči sva relevantna dokumenta koja je prikupio, sprovede potrebne razgovore i posmatra i analizira procese rada i funkcionisanje predmetnog sistema. U toku ove analize, revizor identifikuje osnovne procese predmetnog sistema, jake i slabe tačke svakog od tih procesa i označava ih za kasniju detaljnu proveru i testiranje prema procenjenom stepenu rizika koji im pripada.

U ovoj fazi, program revizije se dopunjava detaljima realizacije rada na terenu, koji sadrži pojedinosti o proverama i testovima koje treba obaviti. Tu se specificiraju metode, tehnike i alati, procenjeno trajanje i očekivani rezultati – konkretni ciljevi koje rad na terenu treba da ispuni.

4.7. Rad na terenu

Cilj ove faze je da se prikupi, analizira, protumači i dokumentuje svaka relevantna informacija kako bi se konačni rezultati revizije podržali argumentima i ispunili postavljeni ciljevi revizije.

Najvažnija aktivnost u ovoj fazi jeste obavljanje svih potrebnih provera i testiranja. Rezultate ovih provera i testova potrebno je prodiskutovati sa klijentom revizije, kako bi se izbegla eventualna neobaveštenost klijenta i obezbedila potvrda ispravnosti rezultata.

Operativno gledano, ovo je centralna aktivnost svake IT revizije. Tokom nje se formira konačna lista glavnih revizorskih nalaza. Na osnovu rezultata ove faze formiraju se zaključci, mišljenja, ocene i preporuke korektivnih mera, dakle svi najvažniji rezultati revizije.

Naziv „rad na terenu" vodi poreklo iz tradicionalne revizije. U kontekstu IT revizije ne treba ga shvatiti doslovno. U uslovima umreženosti, većina aktivnosti iz faze „rada na terenu" može se obaviti „na daljinu", uz upotrebu pogodnih tehnika i alata. Mapiranje mreža, enumeracija uređaja, enumeracija i identifikovanje servisa, operativnih sistema i aplikacija, otkrivanje slabosti i drugi postupci u ovoj fazi mogu biti obavljeni na automatizovan način i u većini slučajeva sa jedne centralne lokacije u mreži.

Rezultat ove faze jeste rezime nalaza i zaključaka. Oni se rangiraju prema stepenu pripadajućeg rizika i čine osnovu za izradu revizorskog izveštaja. Pre nego što se pristupi izradi izveštaja, rezime rada na terenu je poželjno prodiskutovati sa klijentima revizije, radi konačnog usklađivanja.

4.8. Izveštavanje

Cilj ove faze je da se saopšte krajnji rezultati revizije – nalazi, zaključci, mišljenja i preporuke.Izveštavanje u opštem slučaju ima dva koraka – izrada i odobrenje nacrta izveštaja i izrada konačnog izveštaja. Nacrt izveštaja se daje na pregled i odobrenje rukovodiocu interne revizije. Korekcije koje nakon pregleda naloži rukovodilac ulaze u konačan izveštaj.

Revizorski izveštaj ima dvodelnu strukturu. Prvi deo je rezime *(engl. executive summary)* u kojem se ukratko izlažu najvažniji rezultati revizije: zaključci, mišljenja, ocene i preporuke korektivnih mera. Rezime takođe može da sadrži i najvažnije revizorske nalaze ako je to potrebno, radi argumentacije u prilog iznesenih rezultata. Obim rezimea je po pravilu ne veći od dve do tri strane teksta. Drugi deo je detaljni revizorski izveštaj u kojem se detaljno izlažu nalazi revizije vezani za slabosti koje je potrebno korigovati. U kontekstu IT revizije, detaljni izveštaji mogu imati obim od više desetina, pa čak i više stotina strana teksta.

Jednostavno pravilo po kojem se razgraničava sadržaj ova dva dela izveštaja je sledeće: u rezime se stavljaju informacije koje su od interesa za najviše rukovodstvo i generalnog direktora, dok se u detaljni deo izveštaja stavljaju informacije od interesa za niže rukovodstvo i izvršioce neposrednih korektivnih mera.

Direktor interne revizije konačni izveštaj šalje naručiocu revizije (odbor za reviziju, generalni direktor i sl.) i klijentima revizije – rukovodiocima svih organizacionih celina koje su bile zahvaćene revizijom.

4.9. Praćenje po izveštaju

Završna, i u praksi najčešće zanemarivana faza jeste faza praćenja po izveštaju. Cilj ove faze jeste da se obezbedi uverenje da će preporučene korektivne mere iz revizorskog izveštaja zaista i biti sprovedene.

Nakon prijema izveštaja, klijent je u obavezi da sačini plan implementacije korektivnih mera i da ga dostavi revizoru. Na osnovu ovog plana, koji mora da bude usklađen sa raspoloživim resursima klijenta i sa procenom rizika, revizor planira rokove u kojima će obaviti kontrolu realizacije za svaku od preporučenih mera.

5. KONVENCIONALNI I STRIKTNO TEHNOLOŠKI PRISTUP – GLAVNE RAZLIKE I MOGUĆNOST INTEGRACIJE

Ovde je prisutna dvojnost pristupa reviziji informacionih tehnologija koja se ogleda u postojanju dve međusobno nezavisne „škole": jedna, poreklom iz tradicionalne revizije, finansijski orijentisana revizija i druga, poreklom iz informatike, tehnički i tehnološki orijentisana revizija. Razlike između ovih pristupa su najvidljivije u tretmanu internih kontrola i pojedinih revizorskih aktivnosti tokom životnog ciklusa interne revizije. Stoga kontekst internih kontrola i odgovarajućih revizorskih postupaka predstavlja i najpogodnije mesto za detaljnije razmatranje najbitnijih razlika.

Razmatranju najznačajnijih razlika pristupiće se sa idejom da se istaknu mogućnosti za njihovo kombinovanje i međusobno dopunjavanje i za izgradnju jednog modernog, integrisanog pristupa tehnološkoj reviziji, tj. reviziji informacionih tehnologija.

5.1 Razlike u tretmanu procene rizika

Konvencionalna revizija pokušava procenu rizika da prikaže kao jednu od faza u životnom ciklusu revizije. Često se procena rizika prikazuje kao faza koja prethodi fazi planiranja. Motivacija za to je jasna i logična – poželjno poznavati rizike pre donešenja bilo koje odluke o predmetu revizije – ciljevima i opsegu revizorskih projekata i zadataka. Pošto se ciljevi i opseg definišu upravo u fazi planiranja, jasno je da bi pre toga bilo uputno obaviti neku vrstu procene rizika.

Međutim, isto tako je jasno i logično da se i ciljevi i opseg, kao i drugi parametri utvrđeni planom mogu (često i moraju) menjati tokom kasnijih faza u životnom ciklusu revizije. Sa

svakom sledećom fazom raste opseg i kvalitet revizorskih saznanja o predmetu revizije. Nova zapažanja, zaključci i ocene mogu u značajnoj meri da odstupaju od inicijalnih procena i pretpostavki.

Tako se dolazi do ideje da se neka vrsta procene rizika mora vršiti tokom celog ciklusa. Svaka od faza mora da dozvoli promene u postavljenim prioritetima, bez obzira na inicijalni sadržaj plana. Ovaj koncept je odavno poznat tehnološkim revizorima koji rade u informatičkim okruženjima.

Na primer, pri skeniranju servisnih portova na serverima i radnim stanicama (što se, prema konvencionalnoj reviziji, događa tek u fazi rada na terenu) može se utvrditi da je na jednoj od radnih stanica koje pripadaju razvoju prisutna neka slabost koja može biti iskorišćena za napad na produkcioni sistem. Prema tome, procena rizika u fazi rada na terenu može nam dati sasvim drugačije rezultate od one procene rizika koja je prethodila planiranju. Sličnim primerima može se pokazati da isto važi i za sve ostale faze u ciklusu.

Integrisani pristup proceni rizika u tehnološkoj reviziji ilustruje dijagram desno na slici 9.

5.2. Sistemski pristup i pristup putem jednokratne probe (istrage)

Konvencionalna revizija favorizuje sistemski pristup. Svi revizorski projekti i zadaci se najpre planiraju, pa se prema usvojenom i odobrenom planu pristupa njihovoj realizaciji – prema dobro uhodanoj šemi životnog ciklusa. Međutim neki revizorski zadaci su po svojoj prirodi nepodesni za sistemski pristup. Incidentne, neočekivane situacije nalažu vanredan revizorski tretman, koji više liči na istragu nego na redovnu reviziju. Po pravilu, takvi zadaci su hitni, moraju biti obavljeni odmah, rezultati se očekuju u najkraćem roku, tako da ne mogu biti temeljno i sistematski planirani. Šta više, oni često iziskuju promptne izmene postojećeg plana, odlaganje ili čak otkazivanje drugih redovnih i planiranih revizija.

U informatičkim okruženjima ovakve situacije su relativno česte, dobro poznate pa čak i očekivane, pokrivene odgovarajućim kontrolama. Revizori koji rade u takvim okruženjima često dobijaju zadatke da izvrše neki pojedinačni test ili proveru.

Primeri su brojni: revizija informatičke bezbednosti određenog veb sajta, revizija izvornog koda neke aplikacije, test na proboj (penetration test) nekog produkcionog sistema, itd. Česte su i post-mortem revizorske analize, kao na primer nakon ispada nekog sistema ili neke njegove komponente, analize štete posle incidenta, utvrđivanje uzroka incidenta, odgovornosti za incident itd. Ovakvi zadaci često uključuju potrebu za posebnim znanjima, tehnikama i alatima (etičko hakovanje, digitalna forenzika i sl.).

Učestanost situacija koje iziskuju ovakav pristup i njegova nezamenljivost u takvim situacijama nameću potrebu da se revizorski profil proširi izvan konvencionalno – sistemskog i integriše sa vanredno – incidentnim pristupom.

5.3. Neformalna i kontinualna revizija

Potreba za odstupanjem od strogo planskog i sistematskog pristupa nije uslovljena samo vanrednim i incidentnim situacijama. Moderno poslovanje se odvija u uslovima stalnih promena. Brz tehnološki razvoj, konkurentska borba, nove usluge i proizvodi, imperativ za optimalno korišćenje resursa i niz sličnih faktora unose visok stepen dinamike i uslovljavaju brzo reagovanje i prilagođavanje promenama u svim poslovnim procesima. Kod rukovodilaca raste tzv. „apetit za rizik" *(engl. risk appetite)* – iznosi preostalog rizika u modernim i dinamičnim organizacijama u današnje vreme podižu se do nivoa koji su donedavno smatrani neprihvatljivim. Od toga nije pošteđena ni interna revizija.

Postoje dva načina da se odgovori na ovakvu vrstu izazova. Prvi je uvođenje elemenata neformalne revizije a drugi je tzv. kontinualna revizija. Oba načina su primerena tehnološkoj reviziji i vrlo primenljiva u nekim od njenih zadataka.

Ograničenja resursa su dovela do razvoja revizije koja se rukovodi rizikom, revizija koja „ne može da radi sve" usmerava se tako da radi ono što je najkritičnije u pogledu rizika kojima se organizacija izlaže. Međutim, tu postoji sledeći problem: ako se revizija u svome radu isključivo rukovodi rizikom, onda je očigledno da ona neke oblasti poslovanja nikada neće pregledati i analizirati. Jednostavno, na njih nikada neće doći red, pošto se nikada ne nalaze na listi najrizičnijih oblasti.

Pokazuje se da neformalna i kontinualna revizija mogu da budu od velike koristi i u rešavanju ovog problema.

Neformalna revizija je pristup u kojem se svesno odustaje od nekih elemenata discipline, sistematičnosti i detaljnosti koji su inače svojstveni konvencionalnoj reviziji. Ako je revizor stručno osposobljen i ima potrebna znanja, veštine i iskustvo, rukovodilac može da mu dozvoli da pojedine zadatke obavi bez prethodne procene rizika, bez detaljnog i dokumentovanog plana i bez obaveze da strogo i sistematično dokumentuje sve nalaze, formira radne papire i slično. Statističko formiranje uzoraka se takođe preskače i umesto toga uzorci se formiraju empirijski, prema prethodnim saznanjima i ličnom uverenju revizora. Radni nalog ga obavezuje da sačini kratak i koncizan izveštaj u zadatom roku, što predstavlja apsolutni minimum formalizma.

Ako se primeni pravilno i na mestima gde je odgovarajući, ovakav pristup može da pruži vrlo kvalitetne rezultate. Jasno, od neformalne revizije ne mogu se očekivati celoviti i sveobuhvatni izveštaji, ali praksa pokazuje da je upravo taj pristup uspevao da otkrije mnoge slabe tačke koje su prethodno promakle temeljno vođenim analizama rizika.

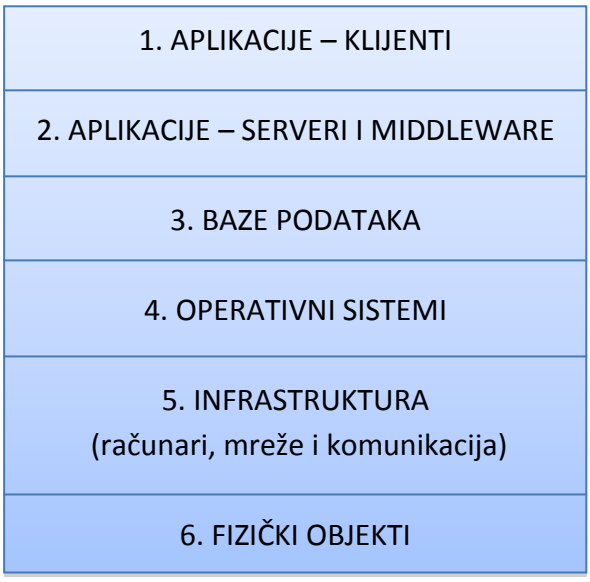
Kontinualna revizija je pristup u kojem se neke provere i testovi obavljaju neprekidno, po pravilu automatski, i to u ciklusima koji su nezavisni od redovnog ciklusa revizije. Ovakav način provera i testova veoma je primenljiv u raznim oblastima IT revizije, pod uslovom da revizori poseduju potrebne kompetencije i da su opremljeni potrebnim alatima. Najčešće, ovakav pristup se zasniva na primeni nekih softverskih senzora, agenata ili automatskih skenera, ali postoje i druga rešenja (hardverski uređaji – audit appliances). Njihovom primenom, IT revizija poprima neka svojstva stalnog praćenja (monitoringa). Pored tehničkih kompetencija, za kontinualnu reviziju je neophodno i vrlo detaljno razumevanje kontrolnog okruženja i svih pravila i izuzetaka u sistemima internih kontrola.

Kontinualnu reviziju ilustrovaćemo jednim primerom: u organizaciji koja ima implementiran sistem za upravljanje softverskim korekcijama *(engl. patch management),* tehnološki revizori često koriste softverski skener koji neprekidno testira sve računare u sistemu u pogledu primenjenih softverskih „zakrpa" i servisnih paketa aplikativnog i sistemskog softvera. Kratki izveštaji iz ovog programa mogu se dobiti na kraju svakog ciklusa testiranja, periodično, ili u realnom vremenu, u formi alarma.

5.4 Provere i testovi

Verovatno najbitnije razlike između konvencionalnog i striktno tehnološkog pristupa uočavaju se kod praktičnih provera i testova koji se odvijaju u fazi rada na terenu. U svom radu na terenu, konvencionalna revizija favorizuje posmatranje procesa i funkcionisanja sistema, razgovore sa odgovornim licima, upitnike, intervjue i slične metode za proveru. Egzaktna testiranja se najčešće vrše na statistički izabranim uzorcima, čijom analizom se dolazi do nalaza i pokazatelja na osnovu kojih se onda izvlače zaključci.

Aplikativne i opšte kontrole se redovno proveravaju i testiraju, ali uglavnom na nivou kontrola za koje odgovaraju rukovodioci – srednjeg ili najvišeg nivoa. U domenu tehničkih kontrola, konvencionalna revizija skoro da ne radi ništa. Koliko je ozbiljna i značajna ova "slepa tačka" vidi se sa slike 10, na kojoj je detaljno prikazana dubina i složenost područja u kojem se tehničke kontrole prostiru.



Slika 10 - Područja obuhvaćena tehničkim kontrolama

Oblast tehničkih kontrola koje uspeva da obuhvati konvencionalna revizija prema ovoj slici jedva da izlazi iz aplikativnog nivoa (slojevi 1 i 2). U oblasti generalnih kontrola, koje su najčešće zajedničke za ceo entitet i koje su po pravilu centralizovane, to može biti i nešto šire,

ali i tada se ne ide u potrebnu dubinu. Već je rečeno da nivo tehničkih kontrola ima fundamentalni značaj za celokupni sistem internih IKT kontrola. Dok viši nivoi kontrola daju usmerenje, propisuju mere i brinu o tome da li u sistemu internih kontrola „postoji sve što je potrebno", dotle tehničke kontrole brinu o tome da li zaista i „sve funkcioniše kako treba". Prema tome, odsustvo uvida interne revizije u detalje tehničke i tehnološke prirode predstavlja veliki nedostatak i izvor je izuzetno visokog inherentnog revizorskog rizika.

Ovo verovatno predstavlja najveći problem koji konvencionalna revizija ima u oblasti primene i korišćenja informacionih i komunikacionih tehnologija. Srećom, to je ujedno i oblast u kojoj postoji najveća prilika za razvoj integrisanog pristupa. Naime, za IT revizore koji dolaze iz informatičkog okruženja upravo ova oblast predstavlja centar profesionalnog interesovanja i domen u kojem dominantno dolaze do izražaja njihova stručna znanja, veštine i iskustva.

Ukoliko organizacija uspe da integriše konvencionalnu i informatičku reviziju u nivou revizije tehničkih kontrola i pritom postigne usklađenost i ravnotežu oba revizorska profila u svojim revizorskim timovima, time će biti ispunjen najvažniji od svih ključnih faktora uspeha za njene procese IT revizije i istovremeno otklonjen jedan od najznačajnijih izvora inherentnog revizorskog rizika.

6. POSEBNE OBLASTI REVIZIJE INFORMACIONIH TEHNOLOGIJA

6.1. Revizija informatičke bezbednosti

Revizija informatičke bezbednosti je tehnološka revizija koja se bavi bezbednošću informacionih i komunikacionih tehnologija i sistema koji su na njima zasnovani. U eri opšte informatizacije svih vidova poslovanja pitanja informatičke bezbednosti su po pravilu vezana za vrlo visoke poslovne rizike.

Sa druge strane, savremena IT revizija je upravo bazirana na riziku i teži tome da se u što većoj meri rukovodi procenom rizika. Zbog toga je revizija informatičke bezbednosti stalno prisutna i predstavlja neraskidivi, ako ne i najvažniji deo svake IT revizije. Praktično svaki zadatak tehnološkog revizora ima prisutne i bar neke elemente revizije informatičke bezbednosti.

Međutim, uprkos tome što se stalno prepliće sa opštom tehnološkom revizijom, zbog specifičnih znanja, veština, tehnika i alata koji se koriste u ovoj oblasti, ona se često razmatra i tretira potpuno odvojeno od ostatka IT revizije. Veliki broj organizacija se odlučuje da usluge revizije bezbednosti traži sa strane, od nezavisnih, eksternih specijalista, kojih u svetu ima sve više.

Slično opštoj IT reviziji, revizija informatičke bezbednosti takođe se bavi kontrolama i to u više nivoa: administrativnim (uprava i rukovodstvo), tehničkim i fizičkim. Postoji mnogo užih disciplina izdiferenciranih unutar revizije informatičke bezbednosti, posebno u nivou tehničkih kontrola. Tako postoje zasebne revizije bezbednosti veb aplikacija, baza podataka, mreža, mrežnog pristupa i demilitarizovane zone, operativnih sistema itd.

6.2. Revizija prevarnih radnji i mesto digitalne forenzike u IT reviziji

Iako mnoge organizacije imaju potrebu da uspostave zasebne organizacione celine specijalizovane za borbu protiv raznih prevarnih radnji[43], kod većine organizacija to ipak nije slučaj. Kada veličina, složenost ili priroda posla organizacije ne opravdava uvođenje posebnih službi za to, onda je sprečavanje, otkrivanje i reagovanje na otkrivene prevare prepušteno opštim sistemima internih kontrola u organizaciji.

Uloga revizije u ovim procesima je onda vrlo slična ulozi koju revizija inače ima u oceni sistema internih kontrola. Međutim, u nekim aspektima, revizija prevarnih radnji se ipak izdvaja kao dosta specifična. Pre svega, kod prevara je revizija po pravilu reaktivna, posebno tamo gde Fraud Management ne postoji. Iako postoji mogućnost da se preventivno deluje, na primer davanjem preporuka za unapređenje kontrola, ipak u većini slučajeva revizija deluje detektivno ili samo reaktivno – tek po nastalom incidentu. Obično se takve revizije vrše po vanrednom radnom nalogu i imaju nesistemski karakter, karakter jednokratne provere ili istrage. Kada je u slučajeve prevare uključena tehnološka komponenta, može se pojaviti i potreba za primenom digitalne forenzike. Treba imati u vidu da je primena digitalne forenzike u korporativnom okruženju bitno različita od one koja postoji kod istražnih i sudskih organa. Ta razlika se pre svega očitava u prirodi i težini učinjenog dela, što se onda odražava i na motivaciju i obim forenzičkih zahvata.

Korporativna forenzika je primenljiva isključivo onda kada je potpuno jasno da prevarna radnja spada u kategoriju koja se sankcioniše isključivo internim aktima (nema elemente krivičnog dela i sl.) i kada njene posledice ni u kom aspektu ne izlaze iz okvira kompanije.

Ova oblast je veoma osetljiva i mora biti tretirana sa posebnom pažnjom. Nikako se ne sme dozvoliti da se interna revizija upušta u bilo kakvu istragu prevare ili primenu digitalne forenzike bez eksplicitnog i preciznog naloga od strane ovlašćenog rukovodioca i ukoliko u svom sastavu nema odgovarajuće obučene i uvežbane specijaliste sa svim potrebnim znanjima i iskustvom za obavljanje takvih zadataka.

[43] *Engl. Fraud Management*

6.3. Revizija usklađenosti

Revizija usklađenosti[44] u širem smislu odnosi se na reviziju normativne usklađenosti, tj. na davanje mišljenja i ocene u pogledu poštovanja svake vrste regulative. Tu pre svega spadaju zakoni, zatim standardi, stručna i profesionalna regulativa, interna akta (politike, pravilnici, procedure) itd.

U kontekstu IT revizije, pod revizijom usklađenosti se pre svega podrazumeva revizija koja utvrđuje da li organizacija ispunjava norme propisane nekim konkretnim standardom. Ova vrsta revizije se ponekad naziva i sertifikaciona revizija, jer organizacija koja pri ovakvoj reviziji bude pozitivno ocenjena dobija odgovarajući sertifikat o usklađenosti. Nju obavljaju posebni, ovlašćeni revizori, specijalizovani za svaki određeni standard, po procedurama koje su strogo definisane i formalizovane. Neki primeri revizije usklađenosti su: ISO 9000, ISO 27001, Sarbanes-Oxley (SOX 302, SOX 404), Basel II, PCI DSS, ISO 15408 – Common Criteria itd.

6.4. Samoocenjivanje

Samoocenjivanje[45] je vrsta revizije kod koje svi nivoi uprave zajedno sa zaposlenima (rukovodstvom i operativnim osobljem) učestvuju u proceni rizika i njima pripadajućih kontrola u organizaciji. Izvorni naziv za ovu vrstu revizije je Control Risk Self Assessment (CRSA). Ona se izvodi posebnim tehnikama i alatima, obično u tzv. „radionicama" (CRSA Workshops), kojima rukovode posebno obučeni (najčešće tehnološki) revizori.

U osnovi samo ocenjivanja je ideja da se, u cilju otkrivanja slabosti, umesto uobičajenih provera i testova koje revizori vrše tokom rada na terenu, organizuje radionica u kojoj bi izvestan broj planski izabranih učesnika predmetnog poslovnog procesa bio u prilici da slobodno iznese sopstvenu ocenu o predmetu revizije.

---

[44] *Engl. Compliance Audit*

[45] *Engl. CRSA - Control Risk Self Assessment*

Tako na primer, umesto da se do revizorskog nalaza dolazi kroz razgovor sa šefom neke službe, u radionicu se pozovu svi radnici te službe i omogući im se da lično iznesu sopstvene nalaze. Pretpostavka od koje se polazi jeste da u velikom broju slučajeva zaposleni najbolje poznaju slabosti sistema u kojem rade, ali da se retko odlučuju da to iznesu u razgovoru sa trećim licima, posebno sa revizorima.

Da bi ovakva tehnika bila objektivna i dala autentičan rezultat, neophodno je ostvariti niz preduslova. Pre svega, potrebno je postići pouzdan nivo anonimnosti učesnika. To se najčešće postiže korišćenjem uređaja za anonimno glasanje, poput onih u parlamentarnim dvoranama, samo manjih i prilagođenih potrebama ovakvih radionica. Ti uređaji su obično prenosivi, čime se omogućava da se radionice organizuju u neposrednoj blizini radnih mesta učesnika. Takođe, neophodna je posebna obuka za voditelje tih radionica, budući da oni moraju imati posebna znanja i veštine iz raznih domena (tehnička, socijalna itd.). Od posebne važnosti je proces planiranja i pripreme u kojem se donose odluke o izboru učesnika, spisku pitanja koja će biti postavljena itd. Pitanja moraju biti postavljena tako da se odgovori daju izborom višestrukih opcija (tzv. test pitanja, gde se odgovori daju izborom – a, b, c ili d). Učesnik daje odgovor pritiskom na taster a rezultati su potpuno depersonalizovani i odmah se statistički obrađuju. Obrada se najčešće vrši u realnom vremenu, na licu mesta, tako da učesnici imaju mogućnost da se odmah upoznaju sa rezultatima. Na kraju, ali verovatno najvažnije, jeste da je za ovakav rad neophodna vrlo jaka podrška od strane rukovodstva.

Ova vrsta revizije ima mnoge nedostatke koji je čine neprimenljivom u mnogim situacijama. Jasno je da se samo ocenjivanje ne može primeniti u situacijama gde se radi o oceni veoma visokih poslovnih rizika, ili za istraživanje prevara, slučajeva korupcije i slično. Takođe, ako korporativna kultura nije odgovarajuća, učesnici radionica neće nikada davati iskrene odgovore, pa čak ni na najbezazlenija pitanja.

Međutim, u velikom broju primena se pokazalo da se ovakvim pristupom mogu ostvariti velike uštede u broju i radnom vremenu revizora, kao i u pouzdanosti i opštoj vrednosti revizorskih rezultata. Neke od oblasti u kojima se pokazalo da samo ocenjivanje može da bude vrlo uspešno su: revizija razvojnih projekata sistema i aplikacija, rada operativnih centara za nadzor tehnološke infrastrukture, pozivnih i uslužnih centara za brigu o korisnicima, ocena poznavanja raznih procedura i uvežbanosti njihove primene (na primer

reagovanje na incidente i sl.), ocena kvaliteta korisničke dokumentacije, prihvatljivosti aplikacija od strane korisnika itd.

TREĆI DEO

STANDARDI I METODOLOGIJE

1. UVOD

Već dugi niz godina informatička struka traži odgovarajuće, svetski priznate, specifične, a dovoljno opšte profesionalne standarde i okvire kojima će se opisati i propisati najbolja praksa u njenom korišćenju. Razvoj standarda korišćenja informacionih tehnologija može se dovesti u uzročno-posledičnu vezu sa njihovim ulogama u poslovanju.

Raniji informatički standardi su se mahom odnosili na korišćenje informatike kao tehnološke infrastrukture. Iz toga su razdoblja nastali brojni tehnološki propisi i norme kojima se uredilo ili propisalo kako koristiti tehnološku infrastrukturu. Ti su standardi bili gotovo isključivo orijentisani ka tehnologiji i vrlo su detaljno propisivali kako se neka tehnologija treba koristiti, ali vrlo su se retko odnosili na poslovnu stranu problema njihovog korišćenja. Često je njihova primena bila upitne isplativosti jer su bili slabo dostupni, skupi, a čak i njihova dosledna primena nije mogla garantovati uspešne rezultate. Upravo je ta činjenica bila presudna što se informatički standardi u toj fazi nisu razvili i nametnuli. Naime, često su propisivali koje aktivnosti treba sprovesti da bi se mogla koristiti neka tehnologija, a nisu se fokusirali na korist koju njena primena može doneti poslovanju i na rezultate koje primena standarda treba omogućiti. Taj strateški zaokret u razmišljanju o korišćenju informatike u poslovanju, a u skladu sa tim i korišćenju informatičkih standarda omogućio je razvoj većem broja vrlo kvalitetnih, svetski priznatih standarda i metodologija korišćenja informatike u poslovanju.

Novim načinom standardizacije, tehnologije dostižu svoju zrelost upotrebe i postaju kohezivan element u strukturi organizacije, pa dalji razvoj informatike u smeru procesnog (uslužnog) partnera i strateškog partnera poslovanju vodi i prema razvoju potpuno novih, sveobuhvatnih i u svetskim razmerima vrlo aktualnih standarda i normi. Današnji, u svetskim razmerama i na raznim nivoima organizacije najčešće korišćeni, informatički standardi i norme su:

- ITIL,
- Cobit,
- ISO 27001,
- Val IT,
- Basel II,
- Sarbanes-Oxley,
- CMMI, itd.

Tabela 2- Najvažniji i najčešće korišćeni standardi, norme i okviri

Način korišćenja IT-a	Zrelost IT-a i područje korišćenja	Okviri i norme
Informatika kao tehnološka infrastruktura i 'tehnološki sluga' poslovanju	- Pozadinska, tehnička funkcija. - Tretira se samo kao trošak tehnološki sluga poslovanju.	• OSI referentni model i razni ostali tehnološki standardi • ITIL (delomično) • CMMI
Informatika kao sredstvo povezivanja poslovanja *(upravljanje informatičkim uslugama)*	- Procesni (servisni) partner - Upravljanje informatičkim uslugama - Pouzdanost, dostupnost infrastrukture - Kvaliteta informatičke usluge	• ITIL (ISO 20000) • ITUP • CMMI • ISO 15408 i ISO 13335 • COBIT • ISO 17799, ISO 27001 -27005 • PRINCE2 • PMBOK

Informatika kao strateški resurs poslovanja *(IT Governance,korporativno upravljanje informacionim tehnologijama)*	- Strateška poslovna funkcija - Poluga inovativnosti poslovanja - Sredstvo konkurentske prednosti - Upravljanje rizicima	• COBIT • Val IT • ITIL • COSO • Sarbanes-Oxley zakon • ISO 27001 • ISO 27005 • Basel II (bankarstvo) • IT BSC (IT Balanced Scorecard)

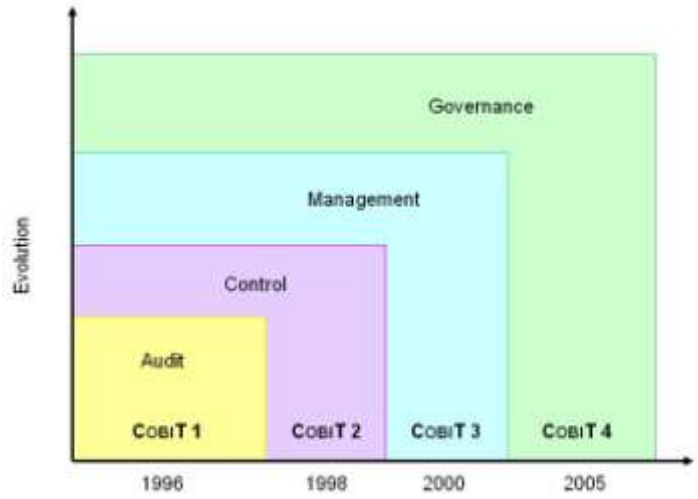
Oni su redom orijentisani prema koristima koje informacione tehnologije mogu doneti u poslovanju i prema dostizanju odgovarajućih merljivih ciljeva usklađivanja IT i poslovanja.

Tabela 2prikazuje najvažnije, i u svetu najčešće korišćene standarde, okvire i norme koje uređuju razna pitanja korišćenja informacionih tehnologija.

2. COBIT

COBIT[46] je opšte prihvaćeni standard za korporativno upravljanje informacionim tehnologijama i IT procesima. Neprofitne organizacije ISACA[47] i ITGI[48] su izdavači COBIT standarda.

Pomoću COBIT-a se spajaju poslovni i informatički ciljevi i pružaju mogućnosti za metričko praćanje zrelosti IS. Cobit pruža upravljačkim strukturama kompanije mogućnost za optimizacijuIT resursa, poput aplikacija, informacija, infrastrukture i ljudi. Uputstva koja daje standard su proizvod znanja mnogih stručnjaka, proizvod je dobre prakse koji je moguće primeniti u bilo kojoj kompaniji. Slika 11 prikazuje razvoj Cobit okvira i prikazuje uloge koje on preuzima svojim razvitkom i nadogradnjom.

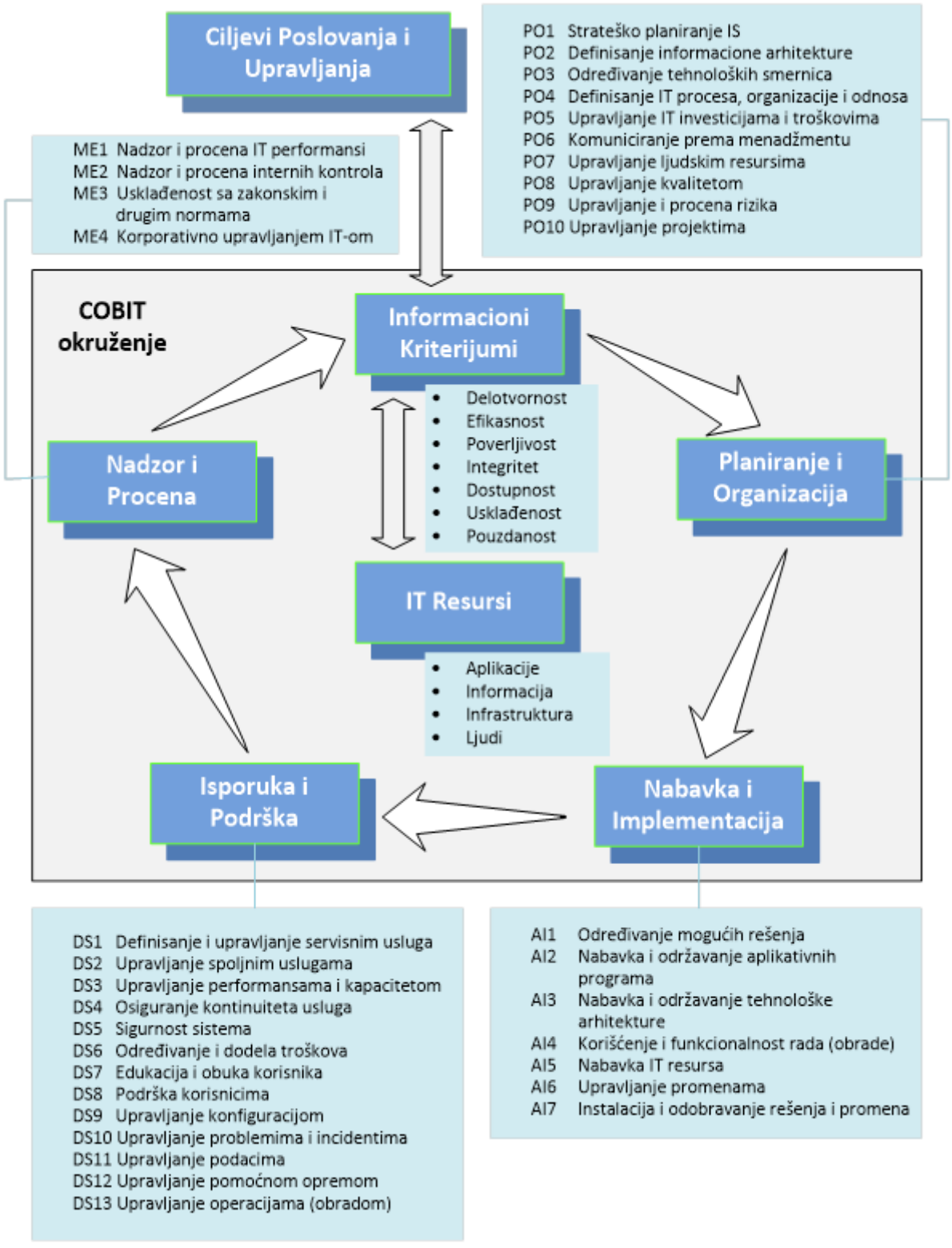


Slika 11 - Razvoj Cobit metodologije

[46]*Engl. Control Objectives for Information and Related Technologies*

[47]*Engl. Information System Audit and Control Association*

[48]*Engl. IT Governance Institute*



Slika 12- Cobit okvir[49]

[49]Stanišić M., Radovanović D., Lučić D., "Revizija informacionih sistema", Singidunum revija, Vol. 6, No. 2, Beograd, 2010, ISSN 1820-8819, 72-81.

Prva verzija Cobit-a je nastala kao alat za podršku izvođenja revizije finansijskih izveštaja. Pojavom druge verzije postao je u svetskim razmerama najkorišćenija metodologija za kontrolu informacionih sistema.

Daljim razvitkom i objavljivanjem treće verzije 2004. godine Cobit predstavlja integralni okvir upravljanja informacionim tehnologijama, dok trenutna zadnja verzija Cobit 4.1 prestavlja najvažniji okvir i metodologiju za korporativno upravljanje informatikom.

Standard sadrži 34 ključna poslovna kontrolna procesa i za svaki proces opisuje model zrelosti i ima preko 300 detaljnih informatičkih kontrola. Primarni kontrolni ciljevi podeljeni su u četiri domena[50] (slika 12):

- **PO - Planiranje i organizacija informatike**[51] uključuje procese za planiranje i dizajn organizacije namenjene postizanju poslovnih ciljeva organizacije. Ovaj domen obuhvata i procenu rizika.

- **AI - Nabavka i implementacija**[52] uključuje procese koji se odnose na nabavku i razvoj IT rešenja, kao i upravljanje promenama tih rešenja tokom vremena.

- **DS - Isporuka i podrška**[53] uključuje procese koji se odnose na aktuelne isporuke IT usluga organizaciji. Ovaj domen uključuje procese za upravljanje problemima i incidentima, upravljanje sigurnošću, i druge procese koji se odnose na izvršavanje IT.

- **ME - Nadzor i procena uspešnosti**[54] uključuje procese za proveru IT procesa i njihove uspešnosti u postizanju relativnih ciljeva IT kontrola.

---

[50]ITGI. (2007). CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models. Rolling Meadows, USA: IT Governance Institute.

[51]*Engl. PO - Planning and Organization*

[52]*Engl. AI - Acquisition and Implementation*

[53]*Engl.DS - Delivery and Support*

Aktivnosti \ Funkcije	Generalni direktor (CEO)	Finansijski direktor (CFO)	Izvršni direktor	Šef informatike (CIO)	Vlasnik poslovnog procesa	Glavni rukovodilac	Glavni arhitekta IS	Rukovodilac razvoja	Rukovodilac IT administracije	Rukovodilac projekta	Usklađenost, revizija, rizik i bezbednost
Uspostaviti IT organizacionu strukturu.	C	C	C	A		C	C	C	R	C	I
Dizajn okvira IT procesa	C	C	C	A		C	C	C	R	C	C
Identifikovanje vlasnika sistema.		C	C	A	C	R	I	I	I	I	I
Identifikovanje vlasnika podataka.		I	A	C	C	I	R	I	I	I	C
Uspostaviti i implementirati IT uloge i odgovornosti, uključujući nadzor i segregaciju dužnosti.		I	I	A	I	C	C	C	R	C	C

Slika 13 - RACI matrica – Planiranje i ogranizacija 04

Svaki od tih procesa nudi i tzv. RACI[55] matrice (slika 13), za svaki od datih procesa se određuje ovlašćena i odgovorna osoba za sprovođenje pojedinih kontrolnih aktivnosti, a koga samo treba obavestiti i konsultovati.

Cobit definiše za svaki od IT i poslovnih procesa (slika 14)[56]:

- modele zrelosti,
- kritične faktore uspeha - *CSF*[57],
- glavne indikatoreza ostvarenjivanje ciljave- *KGI*[58],
- smernice za nagledanje performansi i ključne indikatore - *KPI*[59],
- smernice za upravljanje rizicima - RACI Chart,
- ciljeve kontrole i kontrolne testove.

[54]*Engl. ME - Monitoring and Evaluation*

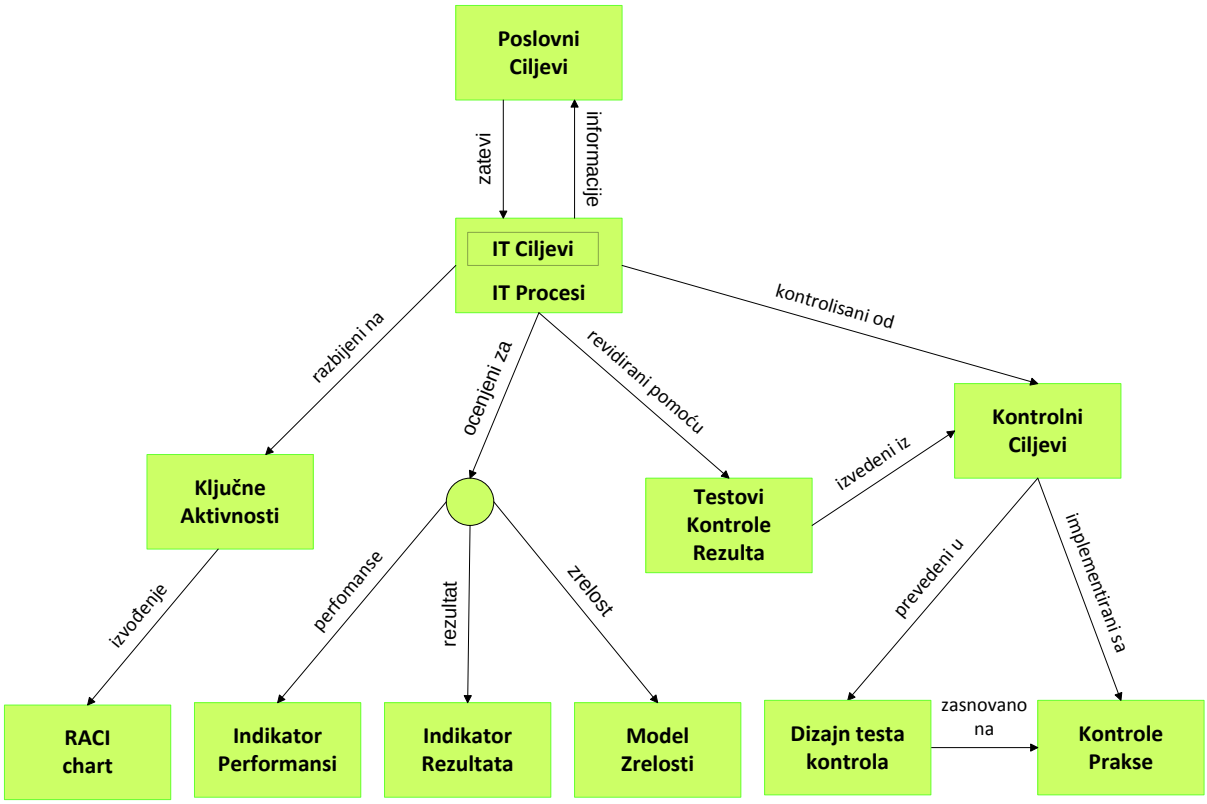
[55]*Engl. RACI, prema akronimu engleskih reči* ***R****esponsible*, ***A****ccountable*, ***C****onsulted*, ***I****nformed*

[56] Radovanović D., Šarac M., Lučić D., Adamović S., "Analiza metoda za kontrolu i reviziju informacionih sistema", INFOTEH 2010, Mart 17-19, 2010, Jahorina, Bosna, Vol. 9, Ref. E-III-2, p. 567-570

[57]*engl. CSF - Critical Success Factors*

[58]*engl. KGI - Key Goal Indicators*

[59]*engl. KPI - Key Performance Indicators*



Slika 14- Relacija između Cobit komponenti[60]

2.1 Model zrelosti

Ocene zrelosti procesa su zasnovane na poznatom CMM[61] modelu, samo što su u Cobit modelu ocene vrlo detaljno opisane i objašnjene za svaki proces. Ocene zrelosti procesa upravljanja informatikom na korporativnom nivou su u rasponu od 0 do 5[62]:

- **0 – Ne postoje procesi**; Procesi upravljanja informatikom na korporativnom nivou ne postoje. Menadžment nije prepoznao važnost tog koncepta. Odluke o ulaganjima u

[60]Stanišić M., Radovanović D., Lučić D., "Revizija informacionih sistema", Singidunum revija, Vol. 6, No. 2, Beograd, 2010, ISSN 1820-8819, 72-81.

[61]*engl. CMM - Capability Maturity Model*

[62]ITGI. (2007). CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models. Rolling Meadows, USA: IT Governance Institute.

informatiku potpuno su u rukama pojedinaca, stihijske, od slučaja do slučaja ('ad-hoc'), izvan su sistemskog nadzora i procene rizika.

- **1 – Početni procesi**; Menadžment nije svestan važnosti upravljanja informatikom. Iako nema nikakvih formalnih procedura, upravljanje i nadzor informatike se uglavnom zasniva na pojedinačnoj, stihijskoj bazi, a postupanje u tim prilikama je od slučaja do slučaja. Ne postoje standardi, korporativna pravila, obaveze i odgovornosti po tom pitanju. Ne koriste se nikakva uputstva. Menadžment uglavnom uopšte nije svestan važnosti informatičkih rizika. Upravljanje informatikom i merenje njene uspešnosti su procesi koji se sprovode samo unutar odeljenja informatike, a menadžment je po tim pitanjima pasivan i uglavnom neupućen i ne informisan.

- **2 – Ponovljivi procesi**; Procesi upravljanja informatikom postoje, ali su ne koordinisani i pokrenuti uglavnom od odeljenja informatike ili nekog drugog operativnog nivoa. Često se događa da veći broj ljudi obavlja iste zadatke i nema sistemskog nadzora, koordinacije, niti standardizovane procedure nad tim procesima. Odgovornost je prepuštena pojedincima, a politike na korporativnom nivou ne postoje ili nisu predstavljene zaposlenima.

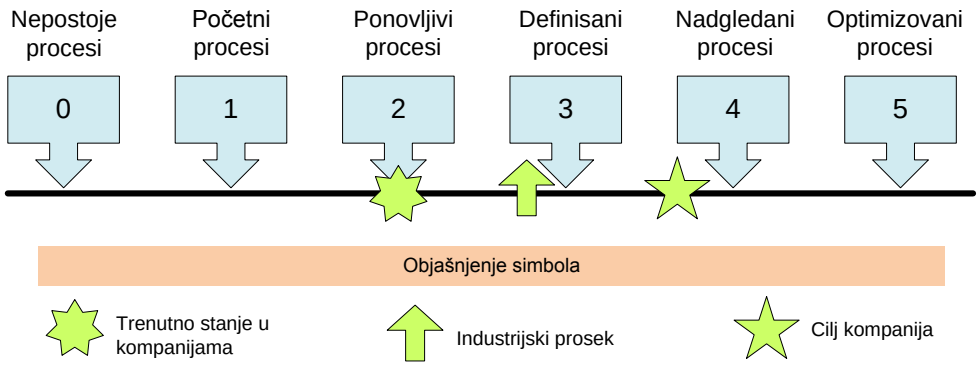
- **3 – Definisani procesi**; Procedure upravljanja informatikom su propisane i dokumentovane, stalno se usavršavaju formalnim treninzima i edukacijom. Procedure i korporativna pravila, iako formalno postoje, nisu sofisticirane, zrele niti prilagođene poslovanju organizacije, nego uglavnom predstavljaju formalizovanje postojećih procedura. Iako procedure postoje, odgovornost za njeno izvršenje je na pojedincima, a obzirom da nema sistemskog nadzora, malo je verovatno da neko može otkriti anomalije po tom pitanju.

- **4 - Nadgledani procesi**; Osim što korporativne politike i procedure postoje, moguće je i stalno nadzirati njihovo izvršenje i meriti uspešnost, pa prema potrebi i preduzimati potrebne korekcije. Procesi i aktivnosti se stalno unapređuju. Postavljaju se vrlo sofisticirani ciljevi upravljanja informatikom koji su usko usklađeni sa

poslovnim ciljevima. U merenju uspešnosti i reviziji obavezno se koriste aktuelne metodologije i okviri (Cobit, IT BSC, ITIL).

- **5 – Optimizovani procesi**; Procesi upravljanja informatikom su dovedeni na optimalan nivo, a kompanija je lider u tom području . Stalno se meri uspešnost i efikasnost informatike kao poslovne funkcije i rezultati se upoređuju sa najboljim iskustvima i drugim organizacijama. Vlada potpuna transparentnost u upravljanju informatikom. Korporativna tela imaju putem niza formalnih mehanizama stvarni nadzor nad informatikom. Informatika se koristi u strateške svrhe, kao ključan poslovni resurs, a informatičke aktivnosti (ulaganja, projekti, rizici,..) na optimalan se način odvijaju prema stvarnim poslovnim prioritetima.

Da bi rezultati ocene zrelosti procesa bili upotrebljivi menadžmentu na razumljiv način potrebno da prilikom prikazivanja upravljačkim strukturama organizacije budu grafički prikazani kao na slici 15. Na tako prikazan način menadžment u okviru kompanije, može lako uočiti stanje na kome se nalaze procesi u njihovoj kompaniji. Najbitnije je da mogu uočiti prosek ocena zrelosti u industrijskoj grani u kojoj se oni nalaze, i uporediti ga sa vlastitim. Menadžment kompanija može na takvom grafičkom prikazu videti u kom pravcu treba da nastavi sa unapređenjem procesa, tj. vidi cilj kome mora težiti.



Slika 15 - Grafički prikaz ocena zrelosti procesa[63]

[63]Stanišić M., Radovanović D., Lučić D., "Revizija informacionih sistema", Singidunum revija, Vol. 6, No. 2, Beograd, 2010, ISSN 1820-8819, 72-81.

2.2 Informacioni kriterijumi

Da bi zadovoljila poslovne ciljeve, informacija treba da bude u skladu sa određenim kontrolnim kriterijumima koji su u skladu sa Cobit okvirom i poslovnim potrebama za informacijama. Cobit okvir ističe sedam različitih kriterijuma informacije u odnosu na poslovne zahteve, i međusobno se preklapaju:

- **Delotvornost** – Informacija treba da bude relevantna i bitna za poslovni proces. Potrebno je da se isporučuju na vreme, tačno, konzistentno i na upotrebljiv način.

- **Efikasnost** – Informacija mora biti pružena putem optimalnog korišćenja resursa.

- **Poverljivost** – Osetljive informacije moraju biti zaštićene od neovlašćenog otkrivanja.

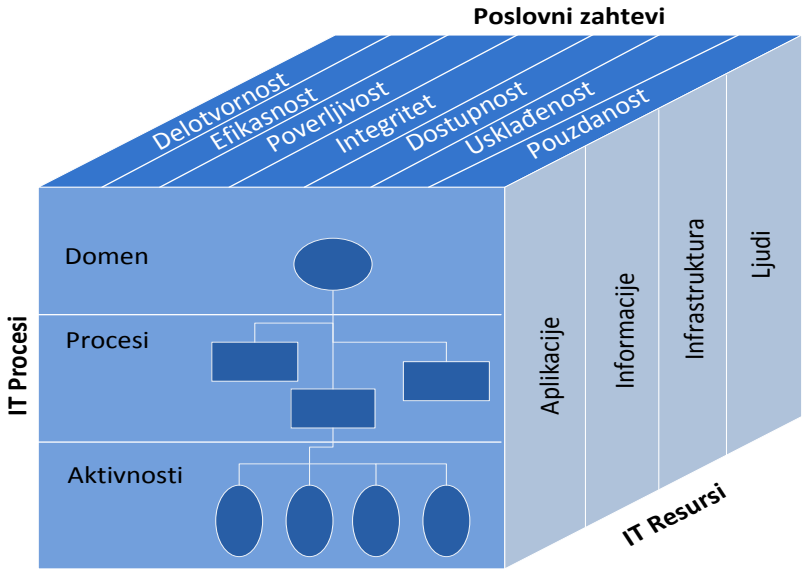
- **Integritet** – Informacija mora biti tačna, potpuna, i ispravna u skladu sa poslovnim vrednostima i očekivanjima.

- **Dostupnost** – Informacije moraju biti dostupne kada se to zahteva od poslovnih procesa, kako u sadašnjosti, tako i u budućnosti. Moraju se očuvati neophodni resursi.

- **Usklađenost** – Informacija mora biti u skladu sa zakonima, propisima i ugovornim aranžmanima koji su predmet poslovnih procesa, kao i sa unutrašnjim politikama.

- **Pouzdanost** – Odgovarajuće informacije moraju biti pružene menadžmentu za potrebe upravljanja i radi ostvarivanja poslovnih ciljeva.

Resursi informacione tehnologije koji su predmet kontrolnih aktivnosti su definisani kao ljudi, aplikacije, infrastruktura i informacije. Sumarno, IT resursima se upravlja preko IT procesa radi postizanja ciljeva koji odgovaraju poslovnim zahtevima organizacije. Ovaj bazni princip Cobit okvira je ilustrovan Cobit kockom na slici 16**.**



Slika 16- COBIT kocka

2.3 Cobit kontrolni ciljevi

Cobit metodologija je dosta korišćena u poslednjih nekoliko godina od strane velikog broja organizacija, odobrena je i testirana od strane stručnjaka širom sveta. U tabeli 1 su prikazani kontrolni ciljevi Cobit metodologije i informacioni kriterijumi koji podržavaju te kontrolne ciljeve. Cobit kontrolni ciljevi su namenjeni revizorima informacionih tehnologija, a za svaki kontrolni cilj definisana je važnost njegove primene, koja može biti velika, srednja ili mala.

U tabeli 3 važnost svakog cilja je obeležena početnim slovom važnosti; velikim slovom M, S ili M. Za informacione kriterijume svakog cilja definiše se uloga, koja može biti primerna ili sekundarna, u zavisnosti koji je informacioni kriterijum najbitniji, a koji je manje bitan.

Kontrolni ciljevi mogu imati više primarnih ili sekundarnih informacionih kriterijuma u okviru jednog cilja, a u tabeli su obeleženi početnim slovima uloge (važnosti), P ili S. Takođe, za svaki cilj su definisani i IT resursi potrebni za određeni cilj. Resursi mogu biti aplikacije,

informacije, infrastruktura i ljudi. Ciljevima mogu biti dodeljeni svi resursi, kao što je slučaj sa kontrolnim ciljem PO9, koji definiše upravljanje i procenu rizika, ili može biti dodeljen samo jedan resurs, kontrolni cilj PO7.

Tabela 3 - Cobit kontrolni ciljevi

Oznaka	COBIT KONTROLNI CILJEVI	**VAŽNOST**		Informacioni kriterijumi								IT resursi			
				Delotvornost	Efikasnost	Poverljivost	Integritet	Dostupnost	Usklađenost	Pouzdanost		Aplikacije	Informacije	Infrastruktura	Ljudi
PO - PLANIRANJE I ORGANIZACIJA															
PO1	Strateško planiranje IS	V		P	S							✓	✓	✓	✓
PO2	Definisanje informacione arhitekture	M		S	P	S	P					✓	✓		
PO3	Određivanje tehnoloških smernica	S		P	P							✓		✓	
PO4	Definisanje IT procesa, organizacije i odnosa	M		P	P										✓
PO5	Upravljanje IT investicijama i troškovima	S		P	P					S		✓		✓	✓
PO6	Komuniciranje prema menadžmentu	S		P					S				✓		✓
PO7	Upravljanje ljudskim resursima	M		P	P										✓
PO8	Upravljanje kvalitetom	S		P	P		S			S		✓	✓	✓	✓
PO9	Upravljanje i procena rizika	V		S	S	P	P	P	S	S		✓	✓	✓	✓
PO10	Upravljanje projektima	V		P	P							✓		✓	✓
AI - NABAVKA I IMPLEMENTACIJA															
AI1	Određivanje mogućih rešenja	S		P	S							✓		✓	
AI2	Nabavka i održavanje aplikativnih programa	S		P	P		S			S		✓			
AI3	Nabavka i održavanje tehnološke arhitekture	M		S	P		S	S						✓	
AI4	Korišćenje i funkcionalnost rada (obrade)	M		P	P		S	S	S	S		✓		✓	✓
AI5	Nabavka IT resursa	S		S	P				S			✓	✓	✓	✓
AI6	Upravljanje promenama	V		P	P		P	P		S		✓	✓	✓	✓
AI7	Instalacija i odobravanje rešenja i promena	S		P	S		S	S				✓	✓	✓	✓

DS - ISPORUKA I PODRŠKA															
DS1	Definisanje i upravljanje servisnim usluga	S		P	P	S	S	S	S	S		✓	✓	✓	✓
DS2	Upravljanje spoljnim uslugama	M		P	P	S	S	S	S	S		✓	✓	✓	✓
DS3	Upravljanje performansama i kapacitetom	M		P	P			S				✓		✓	
DS4	Osiguranje kontinuiteta usluga	S		P	S			P				✓	✓	✓	✓
DS5	Sigurnost sistema	V				P	P	S	S	S		✓	✓	✓	✓
DS6	Određivanje i dodela troškova	M			P					P		✓	✓	✓	✓
DS7	Edukacija i obuka korisnika	M		P	S										✓
DS8	Podrška korisnicima	M		P	P							✓			✓
DS9	Upravljanje konfiguracijom	S		P	S			S		S		✓	✓	✓	
DS10	Upravljanje problemima i incidentima	S		P	P			S				✓	✓	✓	✓
DS11	Upravljanje podacima	V					P			P			✓		
DS12	Upravljanje pomoćnom opremom	M					P	P						✓	
DS13	Upravljanje operacijama (obradom)	M		P	P		S	S				✓	✓	✓	✓
ME - NADZOR I PROCENA USPEŠNOSTI															
ME1	Nadzor i procena IT performansi	V		P	P	S	S	S	S	S		✓	✓	✓	✓
ME2	Nadzor i procena internih kontrola	S		P	P	S	S	S	S	S		✓	✓	✓	✓
ME3	Usklađenost sa zakonskim i drugim normama	V							P	S		✓	✓	✓	✓
ME4	Korporativno upravljanjem IT-om	V		P	P	S	S	S	S	S		✓	✓	✓	✓

Svaki kontrolni cilj u okviru Cobit metodologije sastoji se iz više definisanih aktivnosti. Broj aktivnosti u okviru kontrolnih ciljeva nije konstantan.

Postoji ukupno 197 definisanih aktivnosti u okviru četiri domena.

3. ITIL – POVEĆANJE EFIKASNOSTI IT U POSLOVNIM PROCESIMA

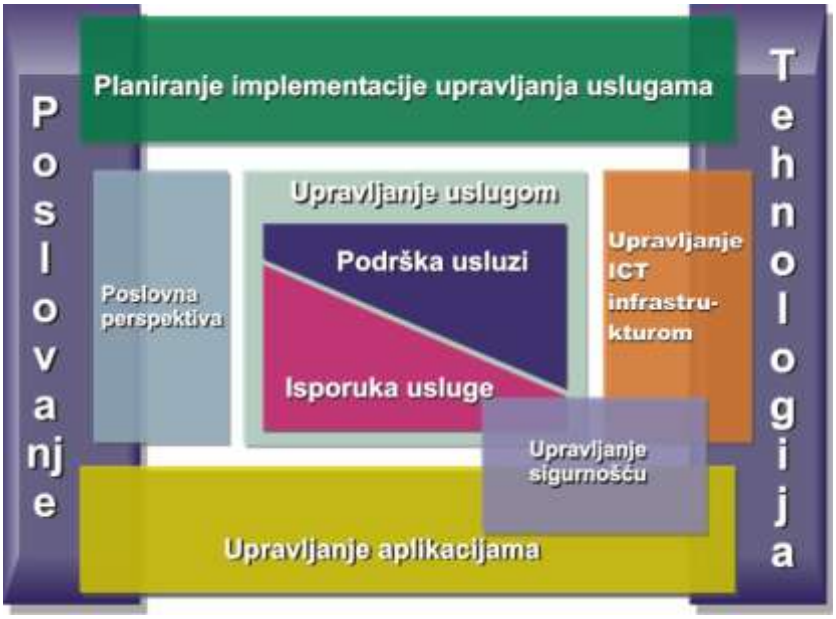
Mnoge IT organizacije se okreću IT menadžmentu uslugama (ITSM) za odgovor na ključna operativna pitanja iz njihovog delokruga rada. ITSM je fokusiran na isporučivanje i podržavanje IT usluga koje su usaglašene sa poslovnim zahtevima organizacije, i to postižu uspostavljanjem procesa opisanih u biblioteci IT infrastrukture. Koncept upravljanja IT uslugama za poboljšavanje sposobnosti poslovnih funkcija nije nov koncept, već on prethodi ITIL[64]-u. Ideja da se celokupna najbolja praksa upravljanja uslugama stavi pod jedan krov bila je i nova i radikalna.ITIL se pojavio kao inicijativa agencija Britanske vlade, kao odgovor na postavljeni zadatak da korišćenje IT u poslovnim procesima bude efikasno i efektivno. Verzija 1 je objavljena 1989. godine i sadrži 43 knjige, dok jeverziji 2 je sažeta u 7 knjiga i objavljena je u periodu 1999. - 2000. godine. U današnje vreme ITIL je postao de fakto standard za promociju poslovne efektivnosti i efikasnosti IT. Mnoge IT organizacije (Microsoft, HP, IBM i mnoge druge) iskoristile su ITIL kao osnovu za svoje modele ITSM kojima podržavaju integraciju svojih tehnoloških rešenja u celovita, sistemska rešenja. U cilju zadovoljenja naraslih potreba da bude i dalje osnova ITSM i omogućavajući faktor promena, planirana je i realizuje se (period 2006.-07.) velika revizija ITIL.

Međutim, ITIL formalno nije standard i stoga nije moguća sertifikaciona provera uspostavljenih mogućnosti i sposobnosti IT organizacije u isporuci usluga. Uvažavajući narastajuće potrebe i zahteve tržišta za formalnom sertifikacijom BSI[65] je objavio standarde BS 15000-1:2002 i BS 15000-2:2003. Standardi su prihvaćeni od tržišta, ali šira primena je uslovljena zahtevima za internacionalizacijom. Ova dva standarda su po ubrzanoj proceduri,

[64] *Engl.ITIL - IT Infrastructure Library*

[65] *Engl. BSI – British Standard Institute*

bez značajnih izmena, usvojena i objavljena kao standardi ISO 20000-1 i ISO 20000-2:2005. Standard ISO 20000-1 je po strukturi i sadržaju procesno orjentisan, potpuno kompatibilan sa ISO 9001:2000 i sadrži specifikaciju zahteva za sistem upravljanja IT uslugama. Drugi deo standarda je specifikacija najbolje prakse u isporuci IT usluga na visokom nivou, nezavisnom od raspoloživih tehnoloških rešenja i u celosti je zasnovan na ITIL.



Slika 17- ITIL – IT Infrastructure Library

Pokušaj da se primene ITIL smernice može biti obeshrabrujući, zato jer zahteva dalekosežne promene koje utiču na ljude, procese i tehnologiju. ITSM referentni model funkcioniše kao potpuno integrisana mapa IT procesa na najvišem nivou. Za razliku od organizacija u drugim privrednim oblastima, koje najčešće muku muče da identifikuju ključne procese i njihove međusobne veze, primenom kojih se realizuju proizvodi kojima se zadovoljavaju zahtevi kupca, IT servisne organizacije mogu sa puno poverenja prihvatiti i koristiti referentni model sistema menadžmenta specificiran u standardu ISO 20000-1:2005 i detaljno opisane ključne procese u ITIL. Dokazano je da je ITIL neprocenjivo koristan za kompanije širom sveta koje traže da razumeju svoje probleme sa ljudima, procesima i tehnologijom. Pored toga ITIL obezbeđuje koherentno predstavljanje IT procesa običnim jezikom, čineći ga korisnim u

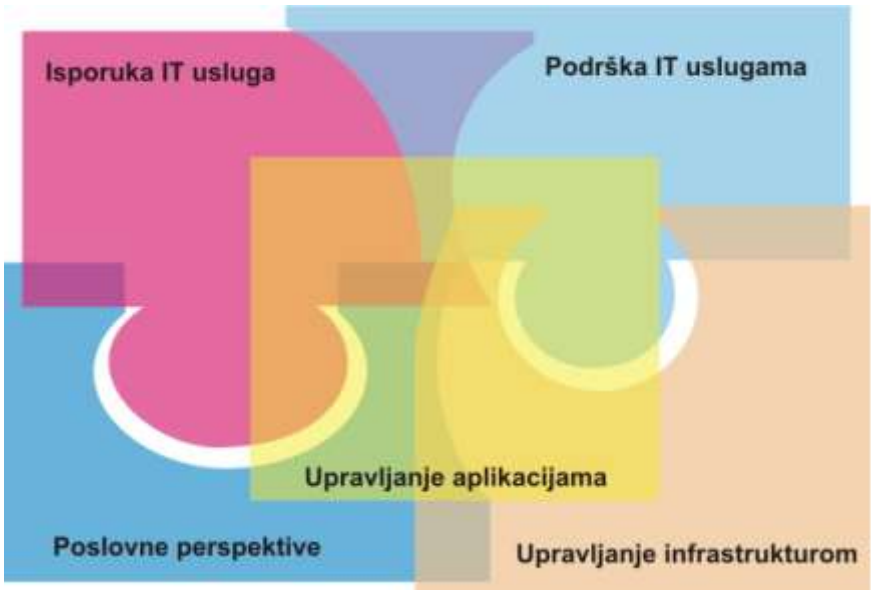
dijalogu između zainteresovanih strana koje učestvuju u definisanju zahteva i uspostavljanju IT procesa.

3.1 BIBLIOTEKA IT INFRASTRUKTURE – ITIL

U prvoj verziji objavljenoj 1989. godine ITIL je sadržao 43 knjige, dok je u drugoj verziji sažeto u 7 knjiga[66].

U nastavku je dat kratak prikaz svih sedam oblasti, od kojih procesi upravljanja uslugom predstavljaju osnovu kostura i obuhvataju dve oblasti:

- Isporuku usluge, i
- Podrška usluzi.



Slika 18- ITIL – Isporuka usluge i podrška usluzi

[66] ITIL, (2007),"An Introductory Overview of ITIL V3", London: The UK Chapter of the itSMF.

3.2 POSLOVNE KORISTI KORIŠĆENJA ITIL

Usvajanje i korišćenje ITIL - biblioteke IT infrastrukture omogućava IT organizaciji da[67]:

- **Umrežavanje IT usluga, zaposlenih, tehnologija i menadžmentau sistem** – bez širenja preduzeća. Isporuka end-to-end IT usluga ne može se kompletirati bez potpuno integrisanog ljudstva, procesa i tehnologije.

- **Pristupanje trenutnim i željenim stanjima i identifikovanje mogućih praznina –** ITIL se može koristiti da IT osoblje brzo identifikuje procese na radnom mestu i otpočne usaglašavanje sa drugim ključnim IT procesima. Kao brz referentni alat, model može da ukaže na željenu budućnost i krajnji cilj za IT organizaciju i obezbedi solidnu osnovu za strateško planiranje.

- **Prioritetni radni napori –** dok model predstavlja procese koje organizacija mora da ima da bi mogla da isporuči konzistentnu, kvalitetnu uslugu, operativni poslovi moraju fokusirati napore tamo gde su odmah potrebni. IT organizacija mora da odluči o prioritetu implementacije procesa. ITIL pomaže organizacijama da brzo odluče o prioritetima, naglašavanjem odnosa i veza unutrašnjih procesa, dozvoljavajući IT organizaciji da proceni značajnost i vrednost primene jednog pristupa u odnosu na drugi.

- **Početak diskusije o organizacionim promenama –** mada je model mapa međusobnih odnosa procesa, a ne organizacioni model, ITIL se može efikasno koristiti za početak diskusije i planiranje organizacionih promena unutar IT organizacije. Razmatranje uloga opisanih procesa u životnom ciklusu IT usluge, raspodela uloga i odgovornosti i potencijalni konflikti interesa pojedinih funkcija, mogu da budu korisna početna tačka i referenca za rekonstrukciju IT organizacije.

[67] ITIL, (2007),"An Introductory Overview of ITIL V3", London: The UK Chapter of the itSMF.

- **Identifikacija područja primene tehnologija koje omogućavaju procesni pristup** – ulazeći dublje u model da bi se analizirali detalji procesa i tačke integracije, ITIL omogućava IT specijalistima da izaberu tehnologije kojima će realizovati procesni pristup i obezbediti efikasno i efektivno postizanje postavljenih ciljeva u podršci poslovnim procesima.

- **Identifikacija sopstvenih slabosti i prednosti, benchmarking –** ITIL set oblasti i procesa sadržanih u njima može se upotrebiti ne samo za poboljšavanje postojeće prakse upravljanja IT uslugama, već i za uspostavljanje novih sposobnosti IT organizacije potrebnih da podrži, i u većini slučajeva da vodi promene u poslovnim procesima kupca da bi njegovo poslovanje bilo u skladu sa promenama u poslovnom okruženju, promenama zahtevanim za opstanak, ili održavanje konkurentnosti. Kao primer već par godina je IT svet konfrotiran sa novim poslovnim izazovom, takozvanom umreženom ekonomijom, u kojoj elektronsko poslovanje pokreće značajne IT investicije i podiže lestvicu kvaliteta i potrebnih sposobnosti i biznisa i podržavajući IT usluga na viši nivo. IT unutar elektronskog poslovanja nije samo podrška primarnim poslovnim procesima nego je deo primarnog poslovnog procesa, što dodatno proširuje i zaoštrava zahteve kvaliteta za raspoloživost, integritet i poverljivost informacija procesiranih/sadržanih u primarnom procesu.

3.3UPRAVLJANJE IKT INFRASTRUKTUROM

Upravljanje IKT infrastrukturom obuhvata sve aspekte informaciono komunikacione infrastrukture od identifikacije poslovnih zahteva preko tenderskog procesa do testiranja, instalacije, puštanja u rad i tekućeg održavanja IKT komponenata i IT usluga. Upravljanje IKT infrastrukturom opisuje glavne procese uključene u upravljanje u svim oblastima i aspektima tehnologije. Pored ostalih to uključuje:

- procese dizajniranja i planiranja usluge
- procese instalacije i puštanja u rad

- procese funkcionisanja
- procese tehničke podrške.

Pored nabrojanih tehničkih procesa ITIL u ovom poglavlju definiše i niz upravljačkih aktivnosti kojima se obezbeđuje funkcionisanje veza između procesa i odgovarajuću raspodelu odgovornosti za pojedine detalje i upravljanje IKT infrastrukturom u celosti.

3.3.1 Planiranje implementacije upravljanja sa IT uslugama

IT servis provajder prvo mora, kao i svaka druga organizacija definisati svoju misiju, viziju, principe kojima će se rukovoditi i izabrati strategiju postizanja vizije. Ukoliko i IT organizacija, i korisnik IT usluga, imaju uspostavljen i sertifikovan sistem menadžmenta kvalitetom tada je identifikacija prioriteta u uspostavljanju ITSM kod IT servis provajdera podržana prioritetima koje je definisao kupac. Ovi dokumenti omogućavaju IT servis provajderu da utvrdi svoju sveukupnu poziciju, skalu vrednosti – zasnovanu na rezultatima poslovnih procena – i generiše celovitu IT strategiju i plan arhitekture IT-a. Usklađivanje opštih (ISO 20000-1) i posebnih (kupci) zahteva za kompetentnost i svojih sposobnosti IT servis provajder treba da dokumentuje kroz razradu dokumentovanog strateškog plana. Ova razrada kao izlaz treba da dâ jasan plan postizanja pojedinačnih taktičkih i operativnih ciljeva, kojima se podržava realizacija vizije IT servis provajdera i obezbeđuje zadovoljavanje zahteva kupaca IT usluga.

Sledeće aktivnosti su deo IT strategije i planiranje arhitekture IT-a:

- usklađivanje dizajna IT organizacije sa tekućim biznis zahtevima
- definisanje i dokumentovanje IT vizije
- razvoj izjave o IT strategiji
- izvođenje strateških analiza
- ustanovljavanje IT budžeta
- identifikacija strateških ciljeva
- razvijanje i komuniciranje (saopštavanje) strateškog IT plana

- razvijanje definicije tržišnih usluga
- utvrđivanje rešenja za usluge
- definisanje IT arhitekture
- identifikacija omogućavajućih tehnologija
- preispitivanje budžeta i korekcije

Strategija postizanja vizije i strateški ciljevi moraju biti razrađeni i detaljno raščlanjeni na taktičke i operativne ciljeve, koji su osnova za projekte realizacije, od kojih svaki mora zadovoljiti osnovne principe projekta. Svaki projekt razvoja IT usluge mora imati svoj cilj/ciljeve i zadovoljiti zahteve za kvalitet, cenu i rok. S druge strane, marketing obezbeđuje tržišne procene što omogućava da se pri planiranju usluga pronalaze putevi da se maksimizira povratak investicija (ROI[68]) novih i postojećih usluga isporučenih kupcima kroz angažovanje poslovnih jedinica. Tokom planiranja usluga, IT verifikuje da se usluge poklapaju i sa biznis zahtevima i mogućnostima isporuke IT-a, i vredne informacije se primaju od procesa dizajna i menadžmenta uslugama. Ishodi uključuju detaljne specifikacije dizajna usluge koja se onda uklapa u procese razvoja i lansiranja usluga.

Sledeće aktivnosti su deo planiranja usluga[69]:

- planiranje za nove (standardne) usluge,
- sprovođenje analize rizika usluge,
- definisanje funkcionalnih potreba,
- analiziranje razlika sposobnosti i potreba,
- preispitivanje marketinga usluga „kupi ili napravi“,
- utvrđivanje ROI usluga,
- pravljenje specifikacije dizajna usluge,
- upravljanje vrednostima usluga,

[68]ROI – Return of investment, povraćaj investiranog, isplativost investicije

[69]Harryparshad N., (2012), "Best practices for implementing multiple concurrent IT frameworks (CMMI, ITIL, Six-Sigma, CobiT and PMBOK)", Graduate School of Business Leadership, University of South Africa, South Africa

- itd.

3.3.2 Projektovanje i testiranje usluge

Kada je završena specifikacija usluge, odnosno sklopljen ugovor o nivou IT usluga koje IT servis provajder treba isporučivati korisniku, proces projektovanja i testiranja usluge omogućava IT servis provajderu da razvije i potvrdi funkcionalnu verziju komponente, funkciju usluge, ili end-to-end uslugu. Kao deo ovog procesa, IT organizacija pribavlja ili pravi neophodne komponente, funkcije usluge – kao što su mogućnosti backup-a ili funkcionalnost Web-a – i čak end-to-end rešenja usluge – kao što je na primer SAP. Jednom sastavljena, komponenta, funkcija, ili end-to-end usluga mora biti temeljno testirana. Pravljenje i testiranje usluge je direktno povezano sa menadžmentom promenama, menadžmentom konfiguracije, i puštanjem u proizvodnju, kao i sa drugim procesima u modelu.

Sledeće aktivnosti su deo procesa pravljenja i testiranja usluge:

- pribavljanje komponenata usluge
- identifikovanje projektnog tima
- razvijanje smernica za pripremu usluge
- razvijanje smernica za upravljanje operativnim radom i infrastrukturom
- integracija primene i infrastrukture
- sertifikacija hardware-a i softver-a usluge
- konstruisanje mehanizama podrške i kontrole usluge
- sprovođenje testova usluge i podrške
- razvijanje planova obuke IT osoblja i osoblja korisnika
- dokumentovanje izrade usluge (ili glavnih šematskih planova) za izradu plana proizvodnje

Uvek važi posebna napomena: IT servis provajder mora imati sopstvenu infrastrukturu koja će obezbediti adekvatnu simulaciju realnog poslovnog okruženja i na kojoj će vršiti testiranja novih i/ili izmenjenih usluga. Sprovođenje testova u „živom okruženju“ može se dopustiti

samo u posebnim slučajevima uz preduzimanje adekvatnih mera koje će omogućiti siguran povratak na prethodno stanje. Ovo lakše reči nego realizovati, pogotovo danas, kada mnoge organizacije korisnici IT usluga poveravaju brigu o funkcionisanju svoje IKT infrastrukture IT entuzijastima koji najčešće nemaju adekvatno obrazovanje i nisu svesni rizika po poslovne procese korisnika.

3.4 SIGURNOST INFORMACIJA U IT INFRASTRUKTURI ORGANIZACIJE

Menadžment sigurnošću informacija zahteva da IT definiše, prati i kontroliše sigurnost korporativnih informacija i usluga. U posebnoj knjizi (jednoj od sedam knjiga) ITIL analizira svaki od Service Delivery i Service Support procesa sa stanovišta sigurnosti informacija[70]. I ITIL i ISO 20000-1 eksplicitno se pozivaju na standard ISO/IEC 17799:2005, koji sadrži specifikaciju najbolje prakse u zaštiti informacija. Organizacija je obavezna da uspostavi kompletnu infrastrukturu kojom obezbeđuje sigurnost informacija sa osnovnom napomenom da je to prvenstveno proces upravljanja koji započinje uspostavljanjem i objavljivanjem politika sigurnosti informacija i izjave o primenjivosti. Naime, organizacija ovom izjavom iskazuje svoje namere da implementira mere zaštite svojih informacija u određenim segmentima poslovanja. Ovaj proces je integralni deo šireg korporativnog plana sigurnosti, koji pored mera preduzetih na IT planu obuhvata organizacione i fizičke mere sigurnosti. Sve IT usluge se moraju pridržavati striktnih korporativnih standarda o sigurnosti informacija u kojima su definisani zahtevi za *raspoloživost, integritet i poverljivost* informacija sadržanih/procesiranih u IT infrastrukturi organizacije.

Sledeće aktivnosti su deo menadžmenta sigurnošću:

- definisanje korporativne politike sigurnosti, što obuhvata i politike sigurnosti koje se odnose na IT;
- promovisanje svesnosti o sigurnosti unutar IT-a;
- sprovođenje analize o nedostacima u pogledu sigurnosti;
- identifikacija mogućih pretnji po sigurnost informacija;
- sprovođenje procene rizika po sigurnost informacija;

[70] ITIL, (2007), "An Introductory Overview of ITIL V3", London: The UK Chapter of the itSMF

- procena uticaja incidenata sigurnosti informacija na poslovanje;
- odabir i implementacija kontrola kojima će se zadovoljiti zahtevi organizacije za sigurnost informacija;
- sprovođenje provera (audit) sigurnosti informacija.

4. ISO 27001/ISO 17799/BS 7799

Još od svog početka 1947. godine Međunarodna organizacija za standardizaciju (ISO[71]) je stvorila brojne standarde za upravljanje sigurnošću mreža, razvoj softvera i kontrolu kvaliteta, uz brojne druge standarde za poslovne i vladine funkcije. Niz identifikatora u naslovu ovog dela odnose se, u suštini, na isti osnovni set standarda koji se bave raznim aspektima praksi zaštite podataka, upravljanja zaštitom podataka i upravljanja rizicima zaštite podataka.

Prethodnik BS 7799[72] je prvi put objavljen kao standard za zaštitu podataka 1993. koji je objavilo britansko Ministarstvo za trgovinu i industriju. Dve godine nakon toga postao je formalno poznat kao Britanski standard 7799. Posle inicijalne publikacije BS 7799 je doživeo tri iteracije dodajući standarde za upravljanje zaštitom podataka od kojih je najnovija iz 2005, koja je dodala smernice za upravljanja rizicima zaštite podataka.

U decembru 2000. godine BS 7799 postao je ISO standard 17799[73]. Iako su unete promene pod uticajem međunarodnih standarda jezgro BS 7799 je ostalo u velikoj meri nepromenjeno, iako je sam BS 7799 obustavljen.

Nastavljajući niz ISO 27001[74] je objavljen oktobra 2005. Ovaj standard se pretežno bavio predmetom BS 7799-2, odnosno upravljanjem sistemima za zaštitu podataka. Ovaj ISO standard je stvoren da obezbedi smernice za efektivno funkcionisanje sistema za upravljanje podacima. Jedan od osnovnih principa u ovoj verziji standarda za zaštitu podataka je upotreba

[71] *Engl. ISO – International Organization for Standardization*

[72] BS 7799, (1995), The British Standards Insitution

[73] ISO, (2000), ISO/IEC 17799. Switzerland: International Organization for Standardization (ISO).

[74] ISO, (2005), ISO/IEC 27001. Switzerland: International Organization for Standardization (ISO).

principa OECD (Organizacija za ekonomsku saradnju i razvoj) u upravljanju sistemima zaštite podataka i mrežnim sistemima. ISO 27001[75] je prvi u nizu standarda za upravljanje zaštitom podataka. Ova serija standarda (27001) je stvorena radi usklađivanja sa drugim prihvaćenim međunarodnim standardima - konkretno ISO 9001[76] (upravljanje kvalitetom) i ISO 14001[77] (upravljanje okruženjem).

S obzirom na to koliko su zbunjujući nazivi standarda njihovo usvajanje i poštovanje takođe može predstavljati izazov. Neke organizacije koriste jednu ili više verzija standarda kao okvira za implementaciju da bi usmerile razvoj internih praksi za zaštitu podataka, procedura i kontrola. Saglasnost sa određenim standardima može biti potvrđeno posle revizije kvalifikovanog procenitelja koji radi za telo za sertifikaciju koje je priznato od strane lokalnih (u zavisnosti od zemlje) autoriteta za sertifikaciju.

Potpuno usvajanje ovih standarda nije trivijalan poduhvat, i trebao bi biti obavljen uz planiranje unapred i analizu. Konsultacije, obuka, kao i proizvodi koji podržavaju razne aspekte ovih standarda lako su dostupni.

Uprkos promenama naziva i obimu ova serija standarda je postala jedan od najprepoznatljivijih i međunarodno prihvaćenih setova o praksama, okvirima i smernicama za zaštitu podataka.

Koncepti ISO 17799

Takođe poznat kao *Kodeks prakse za upravljanje zaštitom podataka,* ISO 17799:2005 se odnosi na 11 bitnih oblasti u okviru kategorije zaštite podataka. Standard navodi 133 kontrole sigurnosti u sledećih 11 oblasti[78]:

[75] Isto.

[76] ISO, ISO/IEC 9001. Switzerland: International Organization for Standardization (ISO).

[77] ISO, ISO/IEC 14001. Switzerland: International Organization for Standardization (ISO).

[78] ISO, (2000), ISO/IEC 17799. Switzerland: International Organization for Standardization (ISO).

- Bezbednosna politika
- Organizacija zaštite podataka
- Upravljanje resursima
- Bezbednost ljudskih resursa
- Fizička bezbednost i bezbednost okruženja
- Upravljanje komunikacijama i operacijama
- Kontrola pristupa
- Akvizicija, razvoj i održavanje informacionih sistema
- Upravljanje incidentima vezanim za zaštitu podataka
- Upravljanje poslovnim kontinuitetom
- Usaglašenost sa standardom

5. COSO

Sredinom 80-ih godina Nacionalna komisija za lažne finansijske izveštaje je formirana kao odgovor na rastuću finansijsku krizu i na zahtev za uvid Vlade u računovodstvene i revizorske prakse. Ovaj nezavisni konzorcijum iz privatnog sektora je uobičajeno nazivan Tredvejeva komisija zato što ju je predvodio Džejms Tredvej Mlađi, izvršni potpredsednik i glavni savetnik u Paine Webber Incorporated i bivši komesar u Komisiji za hartije od vrednosti SAD. U prvom izveštaju iz 1987. grupa je predložila da organizacije koje bi bile sponzori komisije rade zajedno da bi ustanovile jasne smernice za unutrašnju kontrolu. Tako je stvoren Komitet sponzorskih organizacija (COSO)[79], koji su formirale pet velikih profesionalnih organizacija u SAD:

- *Američki institut ovlašćenih javnih računovođa* (AICPA)
- *Američka računovodstvena asocijacija* (AAA)
- *Institut finansijskih izvršioca* (FEI)
- *Institut unutrašnjih revizora* (IIA)
- *Institut računovođa menadžmenta* (IMA)

Komisija u potpunosti zavisi od organizacija pod čijim je pokroviteljstvom i čine je predstavnici iz industrije, javnog računovodstva, investitorskih firmi i sa Njujorške berze.

COSO je objavio prve smernice za unutrašnju kontrolu 1992. godine, *Unutrašnja kontrola – Integrisani okvir*[80]. Ova publikacija je ustanovila definiciju za unutrašnju kontrolu i okvir prema kojem bi organizacije mogle proceniti i unaprediti svoje kontrolne sisteme. Rad COSO

[79] *Engl. COSO -Committee of Sponsoring Organizations*

[80] Committee of Sponsoring Organizations of the Treadway Commission, Internal Control -- Integrated Framework; New York: COSO, 1992

je 1994. godine usvojen od strane *Kancelarije za opšte računovodstvo* Kongresa SAD[81]. Ove smernice za cilj su imale da pomognu javnim kompanijama da same sprovedu kontrolu i tako izbegnu regulaciju računovodstvenih i revizorskih industrija od strane Vlade.

COSO je 2001. započeo drugu veliku inicijativu sa ciljem da proširi prethodni rad na unutrašnjoj kontroli na sve naglašenije upravljanje rizikom. Otprilike u to vreme SAD su bile potresane spektakularnim neuspesima Enron-a[82], Tyco-a, Global Crossinga, Kmarta, Adelphia, Worldcom-a[83], HealthSouth-a i mnogih drugih. Vlada je reagovala donošenjem Sarbanes-Oxley akta 2002. Godine da bi ispunila zahtev da unutrašnja kontrola bude revidirana zajedno sa finansijskim izveštajima. Na vrhuncu ovih aktivnosti COSO je 2004. objavio *Korporativno upravljanje rizicima– Integrisani okvir*[84]. Ovaj drugi dokument je predstavio obimniji okvir za identifikaciju, procenu, i upravljanje rizicima.

Radovi COSO-a danas su prihvaćeni u SAD kao kamen temeljac praktikovanja moderne unutrašnje kontrole i upravljanja rizicima. COSO je uveo revoluciju u računovodstvo i reviziju uspostavljajući definiciju za unutrašnju kontrolu, korporativno upravljanje rizicima i još neke fundamentalne koncepte.

[81] *Engl. GAO -General Accounting Office*

[82] Petrache, A., (2009), The collapse of ENRON, a classic case of corporate social irresponsibility, The Ninth International Conference Investments and Economic Recovery, Vol.12, Nr. 2 special/2009

[83] Kuhn, R., Sutton, S., (2006), "Learning from WorldCom: Implications for Fraud Detection through Continuous Asurance", Journal of Emerging Techologies in Accounting, Vol 3., pp. 61-80

[84] Committee of Sponsoring Organizations of the Treadway Commission, (1992), "*Enterprise Risk Management-Integrated Framework COSO"*, New York.

COSO definicija unutrašnje kontrole

Unutrašnja kontrola je proces na koji utiče bord direktora kompanije, menadžment i drugo osoblje namenjena obezbeđivanju osnovanog uverenja u vezi sa postignućem ciljeva u sledećim kategorijama:

- Efektivnost i efikasnost operacija
- Pouzdanost finansijskih izveštaja
- Saglasnost sa važećim zakonima i propisima

Ključni koncepti unutrašnje kontrole

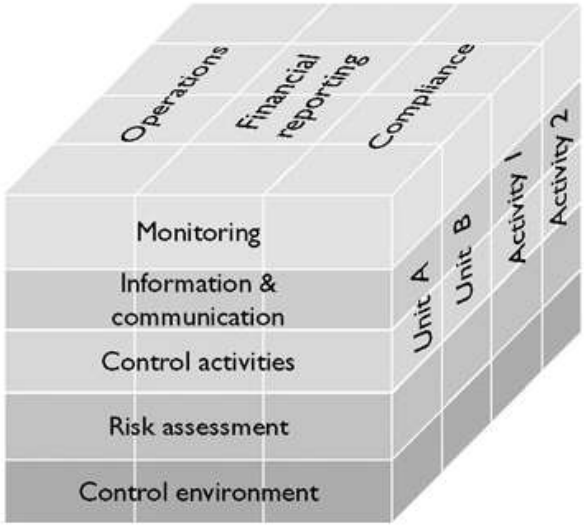
Slede ključni koncepti unutrašnje kontrole prema COSO[85]:

- Interna kontrola je proces, sredstvo kojim se postiže cilj, a nije cilj sam po sebi.
- Na internu kontrolu utiču ljudi. To nisu samo priručnici za postupanje i formulari, već ljudi na svim nivoima organizacije.
- Interna kontrola može obezbediti samo osnovano uverenje, ne i apsolutno uverenje menadžmentu i bordu subjekta.
- Unutrašnja kontrola je usmerena ka postizanju rezultata u jednoj ili više kategorija koje su odvojene ili preklapajuće.

[85] Committee of Sponsoring Organizations of the Treadway Commission, (1992), "*Enterprise Risk Management-Integrated Framework COSO"*, New York

5.1 Unutrašnja kontrola – Integrisani okvir

Publikacija *Unutrašnja kontrola – Integrisani okvir*[86] je uvela dobro poznati grafikon: COSO kocku (slika 19).



Slika 19- Prva COSO kocka (verzija 1992)

Kao što je COSO objasnio unutrašnja kontrola se sastoji od pet međusobno povezanih komponenti. One proizilaze iz načina na koji menadžment vodi posao i integrisane su u proces menadžmenta kompanije. Iako komponente važe za sve subjekte, male i srednje kompanije mogu ih sprovesti drugačije od velikih. Njihove kontrole mogu biti manje formalne i manje strukturisane, pa opet mala kompanija može imati efektivnu unutrašnju kontrolu. Komponente su sledeće:

- Okruženje kontrole
- Procena rizika
- Kontrolne aktivnosti

[86] Committee of Sponsoring Organizations of the Treadway Commission, (1992), "*Enterprise Risk Management-Integrated Framework COSO"*, New York

- Informacija i komunikacija
- Monitoring - praćenje

5.1.1 Okruženje kontrole

Okruženje kontrole utiče na svest o kontroli zaposlenih. To je temelj svih drugih komponenti unutrašnje kontrole i obezbeđuje disciplinu i strukturu. Faktori okruženja kontrole uključuju integritet, etičke vrednosti i znanja zaposlenih; filozofiju upravljačkih struktura, kao i stilove rada i način koji menadžment upravlja razvojemzaposlenih i uputstva od strane borda direktora.

5.1.2 Procena rizika

Svaka kompanija se suočava sa nizom rizika iz spoljnih i unutrašnjih izvora koji moraju biti procenjeni. Preduslov za procenu rizika je određivanje ciljeva koji bi trebali biti povezani na više nivoa i interno konzistentni. *Procena rizika* je identifikacija i analiza značajnih rizika za ostvarenje ciljeva na osnovu kojih se određuje kako bi se trebalo nositi sa rizicima. Zbog toga što će se ekonomski, industrijski, regulacioni uslovi i uslovi rada menjati potrebni su mehanizmi za identifikaciju i bavljenje posebnim rizicima povezanim sa promenom.

5.1.3 Kontrolne aktivnosti

Kontrolne aktivnosti su procedure koje treba da obezbede da se direktive menadžmenta izvršavaju. One omogućavaju da budu preduzete akcije protiv rizika da bi ciljevi kompanije bili ostvareni. Kontrolne aktivnosti se odvijaju u čitavoj organizaciji, na svim nivoima i na svim funkcijama. Uključuju niz aktivnosti poput odobrenja, ovlašćenja, overe, provere operativnih performansi, sigurnosti imovine i podelu dužnosti.

5.1.4 Informacija i komunikacija

Prema COSO važna informacija mora biti identifikovana, uhvaćena i razmenjena kroz komunikaciju u onakvom obliku koji bi zaposlenima omogućio da uspešno izvršavaju svoje dužnosti. Informacioni sistemi stvaraju izveštaje koji sadrže operacione, finansijske podatke, kao i informacije o usklađenosti koji omogućavaju vođenje i kontrolisanje biznisa. Ne bave se samo unutrašnjim podacima, nego i spoljnjim događajima, aktivnostima i uslovima potrebnim za donošenje poslovnih odluka i spoljno izveštavanje.

Efektivna komunikacija takođe mora da postoji u širem smislu, povezujući sve nivoe organizacije. Zaposleni moraju dobiti jasnu poruku iz vrha menadžmenta da se kontrolne dužnosti moraju shvatiti ozbiljno. Moraju razumeti svoju ulogu u sistemu unutrašnje kontrole i kako aktivnosti pojedinaca utiču na rad drugih. Takođe moraju imati sredstva za sprovođenje informacija ka vrhu. Mora postojati i efektivna komunikacija sa spoljnjim faktorima kao što su mušterije, snabdevači, regulatori i akcionari.

5.1.5 Monitoring - praćenje

Sistemi unutrašnje kontrole moraju biti praćeni – proces koji procenjuje kvalitet i performanse sistema tokom vremena. Ovo se ostvaruje kroz stalno praćenje, odvojenu procenu ili kombinaciju ova dva. Praćenje se događa tokom odvijanja operacija. Uključuje uobičajene menadžerske i supervizorske aktivnosti i druge akcije zaposlenih. Obim i učestalost odvojenih procena zavisi u prvom redu od procene rizika i efektivnosti procedura praćenja koje su u toku. Nedostaci unutrašnje kontrole bi trebali biti prosleđeni nadređenima, a ozbiljni problemi samom vrhu menadžmenta i bordu direktora.

5.1.6 Veze između komponenata

Postoji sinergija i povezanost između ovih komponenata koje stvaraju sistem koji dinamično reaguje na promenljive uslove. Sistem unutrašnje kontrole je isprepleten sa poslovnim aktivnostima kompanije i postoji zbog osnovnih poslovnih razloga. Unutrašnja kontrola je

najefikasnija kada su kontrole integrisane u infrastrukturu kompanije i kada su deo suštine preduzeća. „Ugrađene“ kontrole podržavaju inicijative za osnaživanje i kvalitet, i tako izbegavaju nepotrebne troškove i omogućavaju brz odgovor na promenljive uslove.

Postoji direktna veza između tri kategorije *ciljeva* koji predstavljaju ono što kompanija teži da ostvari i *komponenti* koje predstavljaju šta je potrebno uraditi da bi ciljevi bili ostvareni. Sve komponente su bitne za svaku od kategorija ciljeva. Kada bismo za primer uzeli efektivnost i efikasnost operacija (kao jedan od ciljeva) svih pet komponenti mora biti prisutno i mora funkcionisati da bismo mogli zaključiti da je unutrašnja kontrola nad operacijama efektivna.

Definicija unutrašnje kontrole – sa svojim osnovnim konceptima procesa na koji utiču ljudi, koja pruža osnovano uverenje – zajedno sa kategorizacijom ciljeva i komponenata i kriterijuma za efektivnost i povezane diskusije čini okvir unutrašnje kontrole.

5.2 Korporativno upravljanje rizicima– Integrisani okvir

COSO je objavio *Korporativno upravljanje rizicima– Integrisani okvir*[87] 2004. godine da bi kompanije imale reper za upravljanje rizikom unutar njihovih organizacija.

Korporativno upravljanje rizicima je proces na koji utiče bord direktora kompanije, menadžment i drugo osoblje strategijski primenjen širom preduzeća, koncipiran da odredi događaje koji bi mogli utiču na kompaniju i upravljaju rizicima u okviru svojih granica, da bi obezbedio osnovano uverenje u vezi sa ostvarenjem ciljeva kompanije.

Ova definicija odražava neke osnovne koncepte. Upravljanje rizicima je:

- Proces koji se odvija u celoj kompaniji
- Na njega utiču ljudi na samom nivou organizacije
- Primenjen u strategijskom okviru

[87] COSO, (2004), "*Enterprise Risk Management-Integrated Framework COSO"*, New York

- Primenjen na celo preduzeće, na svakom nivou, i uključuje sagledavanje problema na nivou kompanije
- Koncipiran tako da identifikuje potencijalne događaje koji bi, da se dogode, uticali na kompaniju i da upravlja rizikom u okviru svojih granica
- Može da obezbedi osnovano uverenje menadžmentu i bordu direktora kompanije

U publikaciji *Korporativno upravljanje rizicima– Integrisani okvir* originalna COSO kocka je proširena[88].

Slika 20- Proširena COSO kocka (verzija 2004)

Ovaj okvir za upravljanje rizicima je usmeren ka ostvarivanju ciljeva kompanije, raspoređenih u sledeće četiri kategorije:

[88] COSO, (2004), "*Enterprise Risk Management-Integrated Framework COSO"*, New York

- Mora biti usaglašen sa strateškim ciljevima visokog nivoa i da podržava njihovu misiju
- Operacije – efektivno i efikasno korišćenje resursa
- Izveštavanje – pouzdanost izveštavanja
- Usaglašenost sa važećim zakonima i propisima

Korporativno upravljanje rizicima sastoji se od osam međusobno povezanih komponenti. One proizilaze iz načina na koji menadžment vodi preduzeće i integrisani su u proces menadžmenta.

Ove komponente su:

- Unutrašnje okruženje
- Postavljanje ciljeva
- Identifikacija događaja
- Procena rizika
- Kontrolne aktivnosti
- Informacija i komunikacija
- Monitoring

Unutrašnje okruženje - Unutrašnje okruženje određuje stav organizacije i postavlja osnovu za percepciju rizika i kako se prema njemu odnose zaposleni u kompaniji. Uključuje filozofiju upravljanja rizikom, sklonost kompanije ka riziku, integritet i etičke vrednosti.

Postavljanje ciljeva - Ciljevi moraju postojati pre nego što menadžment identifikuje događaje koji mogu uticati na njihovo ostvarenje. Korporativno upravljanje rizicima osigurava postojanje procesa za postavljanje ciljeva, pokrenutog od menadžmenta, i da su odabrani ciljevi u saglasnosti sa misijom kompanije i u skladu sa sklonošću kompanije ka riziku.

Identifikacija događaja - Unutrašnji i spoljni događaji koji mogu uticati na ispunjenje ciljeva kompanije moraju biti identifikovani, pri tom bi trebalo razdvojiti rizike od dobrih prilika. Dobre prilike se sprovode ka procesima strategije menadžmenta ili postavljanja ciljeva.

Procena rizika - Rizici se analiziraju, u obzir se uzima verovatnoća i uticaj, kao osnova za njihovo tretiranje. Procenjuju se na osnovu važnosti.

Reagovanje na rizik - Menadžmentbira reakciju na rizik – izbegavanje, prihvatanje, redukcija ili deljenje – da bi rizike uskladili sa tolerancijom kompanije na rizike i kompanijinom sklonošću ka riziku.

Kontrolne aktivnosti - Uspostavljaju sei implementirajunačini postupanja i procedure da bi se obezbedila efektnost reakcije na rizik.

Informacija i komunikacija - Efektivna komunikacija takođe mora da postoji u širem smislu, povezujući sve nivoe organizacije.

Monitoring - Celokupan proces upravljanja rizikom se prati i modifikuje po potrebi. Praćenje se ostvaruje kroz aktivnosti menadžmenta, odvojenu procenu, ili i jedno i drugo.

Zbog činjenice da je *Unutrašnja kontrola – Integrisani okvir* podnela test vremena i osnova je mnogim pravilima, propisima i zakonima, ovaj dokument ostaje klasičan primer okvira za unutrašnju kontrolu. U isto vreme unutrašnja kontrola je integralni deo upravljanja rizicima preduzetništva. Celokupan sadržaj *Unutrašnja kontrola – Integrisani okvir* je integrisan u publikaciju *Korporativno upravljanje rizicima– Integrisani okvir*. Tako nastaje novi koncept i alatka za upravljanje.

5.3 Uticaj COSO na unitrašnju kontrolu korporacije

Principe zacrtane u COSO dokumentima postepeno implementiraju korporacije u javnom vlasništvu širom SAD. COSO je jedini okvir za unutrašnju kontrolu koju spominje *Komisija za hartije od vrednosti* (SEC) i *Nadzorni odbor za računovodstvo u javnim kompanijama* (PCAOB).

PCAOB je agencija u okviru SEC-a koja je osnovana posle donošenja zakona Sarbanes-Oxley 2002. s ciljem da nadgleda računovodstvo u kompanijama u javnom vlasništvu. U Standardu revizije br. 2 " Revizija unutrašnje kontrole finansijskog izveštavanja sprovedena zajedno sa revizijom finansijskih izveštaja" PCAOB spominje COSO.

Prilikom davanja uputstava vezanih za zakon Sarbanes- Oxley u Standardu revizije br. 2 stoji: "Od menadžmenta se zahteva da svoje procene o efektivnosti unutrašnje kontrole finansijskog izveštavanja bazira na prikladnom i priznatom kontrolnom okviru. Izveštaj COSO-a poznat kao *Unutrašnja kontrola – Integrisani okvir* daje pogodan i dostupan okvir za potrebe procene menadžmenta. Iz tog razloga uputstva vezana za performanse i izveštavanje su bazirana na COSO okviru."

Takođe, COSO principi prodiru u Vladine agencije, privatne kompanije, neprofitne organizacije i u druge subjekte širom sveta. Oni od kojih kompanije zavise su shvatili da su dobre prakse za javne kompanije dobre i za njih.

5.4 Efekat COSO-a na kontrole IT industrije

U publikaciji *Unutrašnja kontrola – Integrisani okvir* COSO ističe da je zbog sveprisutnog oslanjanja na informacione sisteme potrebna i kontrola značajnih sistema. COSO klasifikuje kontrolne aktivnosti informacionih sistema u dve velike grupe. Prva je *opšte kompjuterske kontrole*, koja podrazumeva kontrole IT menadžmenta, IT infrastrukture, sigurnosti, nabavke softvera, razvoja i održavanja. Ove kontrole se primenjuju na sve sisteme – od mejnfrejma do klijent-server i desktop kompjuterskih okruženja.

Druga grupa su *kontrole aplikacije* koje predstavljaju korake unutar softvera aplikacije s ciljem kontrole primene tehnologije. Kombinovane sa drugim ručnim kontrolama procesa ove kontrole osiguravaju celovitost, preciznost i validnost informacija.

6. SOX - SARBANES-OXLEY AKT

Akt Sarbanes-Oxley[89] iz 2002. godine formalno poznat kao Zakon o reformi računovodstva u javnim kompanijama i zaštiti investitora. To je bio odgovor Vlade SAD na izbijanje korporativnih skandala koji su počeli sa Enron-om i Arturom Andersenom, a zatim su usledili Tyco, Adelphia Communications, WorldCom, HealthSouth i mnogi drugi.

SOX i Nadzorni odbor za računovodstvo u javnim kompanijama *(engl. PCAOB)* su stvoreni da bi povratili poverenje investitora u javna tržišta SAD. Osnovni cilj je bio povećanje korporativne odgovornosti, finansijske transparentnosti i smanjiti broj korporativnih i računovodstvenih prevara.

6.1 Uticaj Sarbanes-Oxley akta na javne kompanije

Monetarni udar na korporacije izazvan usklađivanjem politike sa ovim zakonom izazvao je puno neslaganja i lobiranje za manje stroge smernice. Male kompanije traže da budu izuzete od podnošenja obimne dokumentacije i izveštaja. Korekcije napravljene 2005 i 2006 godine su razjasnile do kog stepena kontrole tehnologije moraju biti testirane i koje kompanije moraju preduzeti adekvatne unutrašnje kontrole onih oblasti koje mogu uticati na finansijske transakcije i izveštavanje.

Zakon Sarbanes-Oxley zahteva od rukovodilaca kompanije da potvrde adekvatnost i efektivnost unutrašnjih kontrola vezanih za finansijske transakcije i izveštavanje uključujući i IT kontrole. Ove kontrole moraju biti revidirane spolja, a izveštaj o kontroli mora biti uključen u godišnji izveštaj korporacije podnet Komisiji za hartije od vrednosti *(engl SEC).* Glavni izvršni direktor *(engl. CEO)* i finansijski direktor *(engl. CFO)* su odgovorni za kvalitet

[89] *Engl. SOX - Sarbanes-Oxley*

i integritet informacija koje stvaraju kompanijine aplikacije i komunikacije, kao i za infrastrukturu koja podržava te aplikacije.

Kao rezultat ovoga od menadžera informacionih službi(IT menadžeri), koji ponekad nisu u potpunosti svesni mera koje zahteva zakon Sarbanes-Oxley, se zahteva da detaljno prouče sve rizike i testiraju sve kontrole. Ovo znači da mnogi IT menadžeri traže smernice ili konsultacije da bi bili sigurni da rade u skladu sa novim zakonima. Zbog različitih poslovnih politika u svetskim korporacijama i broja stranih investicija u američkim korporacijama bitno je da svetska IT zajednica bude svesna kakav uticaj finansijske revizije imaju na rad informacionih službi.

6.2 Ključne tačke Sarbanes-Oxley akta

Akt Sarbanes-Oxley ima mnogo odredaba. Članovi 101, 302, 404, 409 i 906 su ključni za značaj i uticaj na odeljenja informacionih službi[90].

6.2.1 Član 101

U članu 101. PCAOB je određena kao agencija za kreiranje standarda revizije i pravila za javne kompanije. PCAOB –u je takođe dat autoritet da reguliše računovodstvene firme koje vrše reviziju javnih kompanija. Pravila koje je objavio PCAOB, a odobrio SEC nazivaju se standardima revizije.

Primarna smernica PCAOB za reviziju unutrašnjih kontrola je navedena u Standardu revizije br. 2, na snazi od 17. juna 2004. naslovljen: „Revizija unutrašnje kontrole finansijskog izveštavanja sprovedena zajedno sa revizijom finansijskih izveštaja“.

[90] SOX ACT, Section 101, 302, 404, 409 i 906

6.2.2 Član 302

Član 302 određuje zakonsku odgovornost glavnog izvršnog direktora (CEO) i finansijskog direktora (CFO). Prema zakonu Sarbanes-Oxley CEO i CFO su odgovorni za unutrašnje kontrole i za kvartalna izveštavanja o bilo kakvim promenama unutrašnje kontrole koje bi mogle uticati na finansijski izveštaj kompanije. Ovi direktori moraju potvrditi svoju odgovornost i obaveštenost o svim finansijskim izveštajima koji se podnose kvartalno i godišnje. Moraju takođe potvrditi upućenost u koncepciju unutrašnjih kontrola i da su procenili njihovu efektivnost, i da ove kontrole garantuju kompletnost i tačnost informacija koje im se podnose u izveštajima. Značajne promene kontrola za razotkrivanje, i bilo koji nedostatak, slabost ili bilo kakve sumnjive radnje koje mogu uticati na preciznost izveštavanja moraju biti obelodanjeni.

Član 302 takođe definiše ulogu spoljnog revizora u finansijskom izveštavanju. Spoljni revizor procenjuje unutrašnje kontrole da bi utvrdio li su potrebne promene radi postizanja veće preciznosti i usaglašenosti. Spoljni revizor mora potvrditi da su on ili ona imali uvid u procene menadžmenta unutrašnjih kontrola i da su odobrili obradu i evaluaciju te procene.

6.2.3 Član 404

U članu 404 CEO i CFO moraju potvrditi da unutrašnje kontrole funkcionišu, da su dokumentovane i efektivne. Procena menadžmenta se sastoji iz četiri dela. Prva tri dela pokrivaju sledeće:

- Odgovornost menadžmenta za postojanje i rigidnost unutrašnjih kontrola
- Procena efektivnosti unutrašnjih kontrola
- Izveštaj okvira korišćenog za procenu efektivnosti kontrola

Menadžmentu je zabranjeno da prijavi da su unutrašnje kontrole efektivne ukoliko u njima postoji jedna ili više materijalnih slabosti.

Četvrti deo se odnosi na spoljnog revizora. Spoljni revizor mora posebno potvrditi da je izveštaj menadžmenta o efektivnosti unutrašnjih kontrola tačan.

PCAOB je 9. marta 2004. godine odobrio Standard revizije br. 2 naslovljen: „Revizija unutrašnje kontrole finansijskog izveštavanja sprovedena zajedno sa revizijom finansijskih izveštaja“. Ovaj standard revizije postavlja uslove za izvođenje revizije unutrašnje kontrole finansijskog izveštavanja i daje bitna uputstva o obimu i pristupu koji se zahteva od menadžmenta korporacije i spoljnih revizora. Takođe daje smernice o kontrolama koje bi trebale biti uzete u obzir uključujući razvoj programa, promene programa, kompjuterske operacije, i pristup programima i podacima. PCAOB Standard revizije br. 2 se posebno bavi kontrolama finansijskog izveštavanja koje bi trebalo da funkcionišu određeno vreme pre datuma potvrđivanja i kontrolama koje bi bile sprovedene i posle potvrđivanja.

6.2.4 Član 409

Član 409 navodi da bi CEO i CFO trebali da se postaraju da svaki materijalni događaj koji bi mogao uticati na finansijske ili operativne performanse kompanije bude brzo i ažurno objavljen u javnosti. Materijalni događaji uključuju bilo kakvo restrukturiranje kompanije, promene personala ili dužnosti ključnih osoba, prekoračenja budžeta na IT projektima, i prodaja akcija od strane korporativnih službenika. Možda je potrebno prijaviti i nove velike finansijske ili operativne aplikacije za koje je utvrđeno da ne rade. „Brzo i ažurno objavljivanje“ znači izveštavanje u gotovo realnom vremenu. Ovo može biti noćna mora za kompanije čije metode obrade zavise od količine podataka što zahteva više vremena.

6.2.5 Član 906

Član 906 se sastoji iz tri dela. Prvi je da uz svaki periodični izveštaj sa finansijskim podacima mora dolaziti i pisana izjava CEO i CFO. Drugi deo precizira da ovaj izveštaj mora pošteno prikazati finansijsko stanje kompanije. Poslednji deo navodi novčane i zatvorske kazne za namerno ili nenamerno podnošenje lažnog izveštaja. Takođe navodi krivične kazne za

neuspeh korporativnih službenika da overe finansijske izveštaje na vreme – 60 dana posle kraja godine u 2004, 45 dana posle kraja godine u 2005, i 30 dana posle kraja godine u 2006.

6.3 Uticaj zakona Sarbanes-Oxley na IT odeljenja

Za većinu organizacija IT službe su bitan deo procesa finansijskog izveštavanja. Aplikacije i servisi podržavaju stvaranje, čuvanje, obradu i izveštavanje o finansijskim transakcijama. I zbog toga, u skladu sa Sarbanes-Oxley zakonom, moraju postojati kontrole korišćenja tehnologije u baratanju sa podacima, obradi i izveštavanju. Opšte kompjuterske kontrole zbog toga su od kritičnog značaja za proces finansijskog izveštavanja tako što obezbeđuju integritet podataka i bezbednost operacija. IT odeljenja sada moraju formalno postupati sa konceptom, dokumentacijom, implementacijom, testiranjem, monitoringom i održavanjem IT unutrašnjih kontrola.

Izvršni i finansijski direktori očekuju od odeljenja Informacione službe da osiguraju da opšte i pojedinačne unutrašnje kontrole za sve aplikacije, podatke, mreže, ugovore, licence, telekomunikacije i fizičku sredinu budu dokumentovane i efektivne. Razmatranje rizika i kontrole se procenjuje na nivou odeljenja Informacione službe, a zatim na nivou kompanije. Razmatranje na nivou kompanije se razlikuje u zavisnosti od sledećih pitanja:

- Koliko je velika korporacija?
- Da li su ključne funkcije ustupljene spoljnim saradnicima (*engl. outsourcing*)?
- Kakva je podela procesa i dužnosti na geografski udaljenim lokacijama?
- Kako su kontrolne dužnosti podeljene među korisničkim grupama, funkcijama Informacione službe i saradnicima koji nisu direktno povezani sa kompanijom (*trećastrana*)?
- Kako se strategija za Informacionu službu (i aplikacije i infrastruktura) razvija, dokumentuje i kako se njome upravlja?

Revizori su do sada otkrili da su najveće slabosti korporacija konzistentnost, dokumentacija i komunikacija. Grupa u Informacionoj službi može pretpostavljati da su njena strategija,

taktičke procedure i aplikacije dobro kontrolisane. Međutim komunikacija sa drugim grupama može do te mere biti manjkava da nijedna grupa ne zna šta druge rade. Jedan od uobičajenih nedostataka organizacija je nepostojanje detaljnog strateškog plana vezanog za najbolji način na koji bi IT odeljenje moglo doprineti poslovnim ciljevima kompanije. Zajedno ovi propusti vode ka nekontrolisanoj i nekonzistentnoj konstrukciji.

6.3.1 Odnos Sarbanes-Oxley akta prema kompanijama sa više lokacija

Globalne organizacije i kompanije koje nemaju sedište u SAD bi trebalo da ispitaju tehnološke operacije svojih poslovnih jedinica da bi odredile njihov značaj za celu organizaciju. Procena poslovne jedinice Informacione službe zavisi od materijalnosti transakcija koje obrađuje ova jedinica, od potencijalnog uticaja na finansijsko izveštavanje ukoliko poslovna jedinica Informacione službe omane, i drugi kvalitativni faktori rizika.

Nekoliko primera ovih procena uključuju:

- Američka multinacionalna organizacija koja ima jednu poslovnu jedinicu koja nema dovoljno transakcija da bi bila finansijski materijalna, ali njena Informaciona služba obradi veliku količinu informacija i/ili konsoliduje finansijske izveštaje za druge lokacije
- Osiguravajuća kompanija sa sedištem u SAD koja prebacuje razvoj aplikacija, tehničku podršku i održavanje na IT poslovnu jedinicu u Indiji

6.3.2 Uticaj usluga treće strane na usaglašenost sa Sarbanes-Oxley aktom

Kontrole vezane za usluge treće strane trebale bi da garantuju da uloge i dužnosti treće strane budu jasno definisane, da ih se drže, i da zadovoljavaju postavljene uslove. Kontrolne mere su usmerene ka pregledu i praćenju postojećih ugovora i procedura da bi se utvrdila njihova efektivnost i usaglašenost sa politikom organizacije. Prekid značajnog ugovora može imati

značajan uticaj na finansijsko izveštavanje. I zato potpada pod smernice za razotkrivanje od strane službenika kompanije.

Za vreme revizije kompanije će često tvrditi da nisu odgovorne za određenu kontrolu zato što je funkcija ustupljena spoljnom saradniku ili da je softver kupljen i održavan od treće strane. Prema odredbama zakona kompanija može ustupiti usluge, ali ne i odgovornost za te usluge. Gotovo je nemoguće očekivati da kompanija ustupi problem poslovnom partneru, i da očekuje da taj problem nestane sam od sebe.

Dokumentacija o kontrolama treće strane je potrebna zbog potvrđivanja od strane nezavisnog revizora, i zbog toga procena mora utvrditi efektivnost i potpunost unutrašnjih kontrola službi organizacije. Ukoliko SAS 70 ili slične revizione opcije ne uključuju testiranje kontrola, rezultate testiranja i mišljenje revizora o efektivnosti kontrola koji je imao uvid u usluge treće strane izveštaji nisu u skladu sa Sarbanes-Oxley zakonom. Kompanije moraju obratiti pažnju da li su specifična okruženja, platforme i aplikacije korišćene u pružanju usluga od strane spoljnog saradnika obuhvaćeni SAS 70 (ili sličnim) revizorskim izveštajima.

Četiri funkcionalna cilja za reviziju usluga treće strane i značajnih usluga ustupljenih spoljnom saradniku, značajnih za kompanije, podružnice korporacija i multinacionalne kompanije su rezimirani na sledeći način:

- Pravila vezana za integritet podataka, dostupnost i poverljivost određuju viši rukovodioci i ona moraju biti održavana i potkrepljena ugovorom sa spoljnim saradnikom
- Uslovi zaštite dobara moraju biti jasno definisani i shvaćeni od strane potpisnika ugovora o ustupanju dela poslovnih aktivnosti
- Obaveze staranja o podacima i informacijama trebale bi biti dobro definisane i poštovane
- Nivoi službe bi trebali biti definisani, merljivi i prihvatljivi za obe strane. Nemogućnost da se ispune dogovori o nivou službe bi trebali biti kompenzovani na neki način. Obračuni i fakture bi trebali biti precizni, a troškovi u granicama budžeta.

6.4 Posebne IT kontrole potrebne za poštovanje Sarbanes-Oxley akta

Do sada PCAOB i spoljni revizori su, u skladu sa Sarbanes-Oxley zakonom, težili sigurnosti, upravljanjem promenama i problemima. Fokus revizije je na integritetu tehnološke infrastrukture za obradu, čuvanje i komunikaciju finansijskim podacima. Ovo se posebno odnosi na finansijske izveštaje koji nastaju iz skladišta podataka u koja se slivaju podaci iz više računovodstvenih i operativnih sistema.

Vlasništvo nad IT kontrolama može biti nejasno pogotovo za kontrole aplikacija. Zbog toga revizija u svakoj oblasti mora imati integrisane automatizovane i ručne kontrole na nivou biznis-procesa.

Generalno, sledeće IT kontrole moraju biti dokumentovane i procenjene kao efektivne da bi bile u skladu sa Sarbanes-Oxley zakonom:

- IT bezbednost
- Kontrola promene
- Upravljanje podacima
- IT operacije
- Mrežne operacije
- Upravljanje dobrima

6.4.1 IT bezbednost

Bezbednosna administracija mora imati efektivan, dokumentovani proces za praćenje i jačanje sigurnosnih pravila određenih od strane menadžmenta. Ova pravila i procesi moraju biti obznanjeni svim korisničkim grupama. Ukoliko se „rukovodioci korisničkih grupa“ koriste da bi rasteretili bezbednosnu administraciju, ti rukovodioci se moraju držati istih pravila i

procedura kao i osoblje informacionih službi. Oni takođe moraju detaljno i efektivno komunicirati sa korisničkim grupama.

Ko ima pristup aplikacijama i podacima? Ko odobrava pristup? Koliko često se proverava nivo pristupa? Koji je proces autorizacije? Šta se događa kada ovlašćena osoba napusti ili promeni posao? Da li se vodi računa o zaštiti podataka na osnovnom nivou? Da li se šifre koriste i redovno menjaju?

Izvršavanje finansijskih transakcija ili transakcija koje vode ka finansijskim transakcijama mora biti ograničeno na one osobe koje imaju ovlašćenje da to urade. Pristup podacima o finansijama i „zaštićenom personalu“ takođe mora biti ograničen na one osobe koje imaju ovlašćenje da to urade.

6.4.2 Kontrola promene

Da bi se osigurala preciznost, kompletnost i integritet finansijskog izveštavanja kompanije moraju imati dokumentovani, efektivni proces kontrole promene koji uključuje promene finansijskih aplikacija, svih interfejs aplikacija, operativnih sistema koji kontrolišu desktop i host servere, instrumente produktivnosti koji se koriste za kreiranje sažete analize, sisteme koji upravljaju bazama podataka i mreže. Proces promene mora sadržati sledeće:

- Tačke za pregled menadžmenta
- Autorizacija
- Migracija promenjenih komponenti
- Raspored promena
- Izveštavanje menadžmenta
- Saopštavanje promena zajednici korisnika

Ko može inicirati promenu? Ko odobrava promenu? Ko može da vrši promene? Koji testovi moraju biti obavljeni pre promena komponenti proizvodnje? Ko obavlja testiranje i potvrđuje

promene? Kako se testiranje dokumentuje? Koji proces se koristi za promociju komponenata razvoja u proizvodnju?

Kontrola promene se odnosi na aplikacije, instrumente produktivnosti i softver operativnih sistema. Saopštavanje promena infrastrukture nailazi na slab odziv. Personal informacionih službi je primetio da korisnici ne mare za to šta je promenjeno i kada, dok god to funkcioniše. Ali šta ako ne radi? Šta ako na izgled nepovezana promena aplikacije ili operativnog sistema utiče na to da deo transakcija ne bude prijavljen?

Kontrola promene finansijskih aplikacija je očigledan problem prilikom pregleda kontrola finansijskog izveštavanja. Često se događa da revizori koji proveravaju usaglašenost nisu procenili rizike neadekvatne kontrole promena interfejs sistema, infrastrukture baza podataka, operativnih sistema, mrežnih sistema ili hardverskih konfiguracija. Čak i interne grupe informacionih službi možda ne shvataju značaj dokumentovanih i sprovedenih kontrola u ovim oblastima vezanim za aktivnosti finansijskog izveštavanja.

Nedavne analize od strane stručnjaka za procenu rizika su pokazale da neadekvatni metodi kontrole promene mogu dovesti do gubitka integriteta informacija u finansijskim aplikacijama i sistemima podataka. Potencijalni rizici su netačno i nekompletno izveštavanje.

6.4.3 Upravljanje podacima

Upravljanje podacima obuhvata i logičko i fizičko upravljanje podacima, kao i identifikaciju i zaštitu ključnih podataka, pogotovo onih vezanih za finansijsku obradu i izveštavanje.

6.4.3.1 Prenos podataka između sistema

Tajming i učestalost prebacivanja podataka iz interfejs sistema u skladišta finansijskih podataka ili u ERP (planiranje resursa u korporacijama) sistem su predmeti revizije. Brzina odgovara na upite skladišta podataka nije stvar kojom se bavi Sarbanes-Oxley zakon, ali je

ključna za funkcionalnost skladišta podataka. Bitno pitanje je da li su preuzimanja konzistentna, pravovremena i u skladu sa rutinama potvrde. Greške uočene prilikom ekstrakcije, transformisanja i preuzimanja treba izdvojiti, prijaviti i ispraviti u razumnom roku da bi bilo osigurano tačno finansijsko izveštavanje.

6.4.3.2 Strukture baza podataka

Kompatibilnost sistema za upravljanje bazama podataka koje se koriste za čuvanje finansijskih podataka je bitno. Ukoliko se podaci o transakcijama koji se koriste za finansijsko izveštavanje čuvaju u drugačijim strukturama podataka, integritet zbira, interpretacije i analize može biti ugrožen. Ukoliko su potrebne različite strukture podataka tada kontrole za kompenzovanje moraju stupiti na snagu da bi potvrdile konačnu kompilaciju podataka.

6.4.3.3 Konzistentnost podataka i elemenata

Mnoge kompanije imaju više računovodstvenih sistema koji koriste različitu terminologiju da bi predstavile iste informacije ili istu terminologiju da bi predstavile različite informacije. Zato bi trebalo koristiti meta data fajlove i rečnike podataka da bi se osigurala konzistentnost ključnih podataka.

6.4.3.4 Fizička kontrola podataka

Fizička kontrola podataka je ključna za integritet finansijskog izveštavanja. Ukoliko objekti gde su smešteni serveri, radne stanice i izveštaji u štampanom obliku nisu obezbeđeni neovlašćeni uvid ili promena može ugroziti transakcije i/ili podatke.

6.4.3.5 Pravljenje rezervnih kopija podataka

Tajming i učestalost procesa pravljenja kopija trebao bi biti određen potrebom biznisa za kratkoročnim oporavkom podataka u problematičnim situacijama. Planovi za oporavak od katastrofa i poslovni kontinuitet nisu sastavni deo najnovijih uslova za saglasnost sa Sarbanes-Oxley aktom, ali su ključni za otpornost biznisa.

6.4.4 IT u kontroli operacija

PCAOB navodi da neefikasna okruženja IT kontrola predstavljaju indikaciju da postoji materijalna slabost u unutrašnjoj kontroli finansijskog izveštavanja. Kontrole IT operacija sežu dalje od upravljanja hardverom i data centra. Što se tiče stvaranja IT okruženja postoje kontrole definicije, akvizicije, instalacije, konfiguracije, integracije i održavanja IT infrastrukture. Tekuće dnevne kontrole operacija podrazumevaju:

- Svakodnevno upravljanje na nivou službe
- Upravljanje uslugama treće strane
- Dostupnost sistema
- Korisničke usluge
- Konfiguracija i upravljanje sistemima
- Upravljanje i rešavanje problema
- Utvrđivanje rasporeda upravljanja operacijama
- Upravljanje objektima

Softverska komponenta sistema operacija uključuje kontrole akvizicije, implementacije, konfiguracije i održavanja softvera operativnih sistema, sistema za upravljanje bazama podataka, posredničkog softvera, softvera za mrežnu komunikaciju, sigurnosnog softvera i uslužnih programa. Sistemski softver takođe uključuje praćenje incidenata, prijave i praćenje funkcija. Konačno, još jedan primer kontrole IT operacija podrazumeva detaljno izveštavanje menadžmenta o neovlašćenom pristupu funkcijama za izmenu podataka.

6.4.5 Mrežne operacije

Revizija mrežnih operacija uključuje proveru pristupnih tačaka WAN[91]-a i LAN[92]-a. Pravilno podešavanje firewall-a, rutera i modema je bitno da bi se izbegao neovlašćeni pristup i potencijalne izmene finansijskih aplikacija i podataka kompanije. Kompletni dijagram konfiguracije mreže uključujući sve servere, rutere i firewall-ove mora biti uključen u dokumentaciju predočenu revizoru. Modemske i VPN[93] konekcije predstavljaju posebno visok rizik za neovlašćen pristup. Sve spoljašnje telekomunikacione konekcije (Internet ili point-to-point) moraju ići preko kompanijinih mrežnih rutera i firewall-ova.

Pretnja koju predstavljaju hakeri, crvi, virusi i drugo maliciozno ponašanje nalaže da svaki server i radna stanica (pogotovo prenosivi računari) imaju antivirusni softver i najnovije definicije virusa. Potencijalna mogućnost gubitka ključnih finansijskih podataka je velika ukoliko antivirus nije ažuriran.

Bilo koji problem izazvan crvom ili virusom u radnoj stanici ili serveru u mreži kompanije mora biti dokumentovan. Ta dokumentacija mora sadržati procenu štete, i mere preduzete za rešenje problema.

6.4.6 Upravljanje dobrima

Revizija upravljanja dobrima uglavnom se bavi ovlašćenjem, finansijskim izdacima i odgovarajućom amortizacijom i izveštavanjem. Da li su ključna dobra (npr. softver, podaci, hardver, posrednički softver i objekti) popisana, a njihovi „vlasnici kompanija“ identifikovani? Sledeće stavke vezane za upravljanje dobrima se pregledaju prilikom revizije:

- Evidencija fiksnih dobara

[91] *Engl. Wide Area Network – regionalna računarska mreža*

[92] *Engl. Local Area Network – lokalna računarska mreža*

[93] *Engl. Virtual Private Network – virtuelna privatna mreža*

- Nabavna cena
- Isporuka
- Odvojena odgovornost za naručivanje
- Odobravanje kupovine
- Prijem i isplata
- Inventar
- Amortizacija
- Raspolaganje dobrima
- Upravljanje promenama inventara dobara
- Razumevanje procedura vezanih za dobra

Rezultat je da obrada evidencije predstavlja nezamenljiv deo plana za upravljanje dobrima.

U okviru upravljanja dobrima kompanije bi trebale da uzmu u obzir kontrole objekata. Da li su data centri opremljeni adekvatnim kontrolama okruženja za održavanje sistema i podataka, na primer sistem za gašenje požara, neprekidno napajanje (UPS), klimatizacija, izdignuti podovi, i dokumentacija za hitne slučajeve.

6.5 Finansijske posledice po kompanije nastale usled postupanja u skladu sa Sarbanes-Oxley aktom

Cena pregleda unutrašnjih kontrola i postupanja u skladu sa Sarbanes-Oxley aktom može biti visoka – i interni troškovi i troškovi za spoljne usluge. Većina osoblja internih informacionih službi nema pozadinu, znanje i iskustvo sa kontrolama da bi adekvatno procenili da li trenutne prilike zadovoljavaju uslove Sarbanes-Oxley zakona. Pojedinci nisu motivisani da proveravaju dokumentaciju i komunikaciju. Zbog toga se često u kompaniju dovode specijalni IT revizori da bi analizirali propuste – da bi utvrdili šta nedostaje ili šta je nepouzdano. Kompanije mogu odlučiti da je potrebna implementacija automatizovanih kontrola dokumentacije ili novog softvera za finansijsko izveštavanje. U zavisnosti od posvećenosti kompanije zavisiće i cena.

Uprkos visokoj ceni saglasnosti sa zakonom, neefikasne kontrole i nepridržavanje zakona imaju još višu cenu. Ukoliko bi spoljni revizor kompanije pronašao materijalnu slabost u kontrolama, kompetentnost i kredibilitet kompanije bi bili dovedeni u pitanje – što bi izazvalo pad vrednosti akcija i raspoloživosti kapitala. Investitori bi se zbog uvida u slabosti strukture menadžmenta i kontrola mogli povući. Strani emitenti mogu rizikovati primoravanje i ličnu odgovornost sa kojom se nisu ranije sreli.

U multinacionalnim korporacijama revizori bi možda bili pod pritiskom da pažljivije ispitaju sumnjive isplate koje podsećaju na mito. U prošlosti, korporativni rukovodioci nisu imali obavezu da prijave sumnjive uplate za ofšor usluge. Ovo više nije mogućnost.

7. BALANCED SCORECARD (BSC) – URAVNOTEŽENO MERENJE EFIKASNOSTI POSLOVANJA

BSC[94]predstavlja uravnoteženi koncept merenja efikasnosti poslovanja, posebno sa stanovišta sprovođenja strategije, kojeg su 1992. godine predstavili Robert S. Kaplan i David Norton[95]. Osnovno obeležje ovog koncepta je da se performanse poslovanja ne mogu meriti ili gledati samo sa finansijskog stanovišta, nego se trebaju uravnotežiti sa dodatnim metrikama poput zadovoljstva kupaca, uspešnosti internih poslovnih procesa i upravljanja znanjem i ljudskim resursima poslovanja. Rezultati postignuti merenjem i tih dodatnih, ne finansijskih pokazatelja, trebali bi garantovati (predvideti) da će i u budućnosti organizacija uspeti ostvariti svoje finansijske, ali pre svega i strateške ciljeve, imajući u vidu sve komponente poslovanja. Upravo radi svoje orijentacije na pokazatelje (metrike) uspešnosti poslovanja, BSC metoda je među menadžerima u svetskim nivoima postala jedna od najkorišćenija metoda strateškog upravljanja. Pokazatelji ili metrike uspešnosti u sve četiri kategorije (finansijski pokazatelji, kupci, interni poslovni procesi i pokazatelji budućeg rasta) često predstavljaju strateške ciljeve, odnosno indikatore uspešnosti poslovanja u budućnosti, čime je menadžmentu iz strategije moguće izdvojili ključne operativne aktivnosti, nadzirati njihovo sprovođenje i pokazateljima meriti uspešnost.

Osnovni smisao korišćenja BSC metode jeste da se složeni strateški ciljevi razlože u jasne operativne aktivnosti čiju je uspešnost sprovođenja moguće transparentno meriti uz pomoć već navedenih pokazatelja. Pokazatelji uspešnosti se određuju na svim strateškim nivoima (mrežni, korporativni, nivo poslovnih jedinica, funkcijski nivo), raspodeljuju na nosioce i ciljeve nižih hijerarhijskih nivoa. U BSC metodi gotovo svi zadani parametri su merljivi, a na

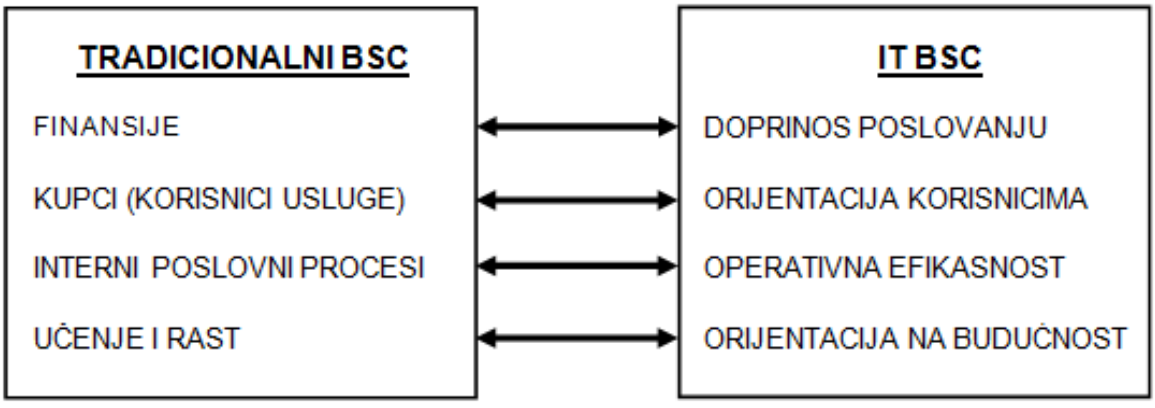
[94]*Engl. BSC - Balanced Scorecard*

[95] Kaplan, R.S., Norton, D.P., (1992): The Balanced Scorecard: Measures that Drive Performance, Harvard business review, Vol 70. Jan-Feb

osnovu njihovog praćenja menadžeri mogu i predviđati performanse poslovanja u budućnosti. Svi korporativni nivoi mogu razvijati sistem merenja uspešnosti poslovanja, ali je važno je da su pojedini merni sistemi hijerarhijski usklađeni.

Porastom važnosti primene informacione tehnologije u poslovanju BSC model upravljanja performansama se počinje primenjivati i na taj deo poslovanja *(engl. IT BSC).* Zbog toga IT BSC[96], uz Cobit, postaje krovni okvir sprovođenja koncepta korporativnog upravljanja informacionim tehnologijama. Na primer, Uprava i izvršni menadžment mogu postavljati sledeća pitanja, odnosno odabrati sledeće metrike za uspešno korporativno upravljanje informacionim tehnologijama[97]:

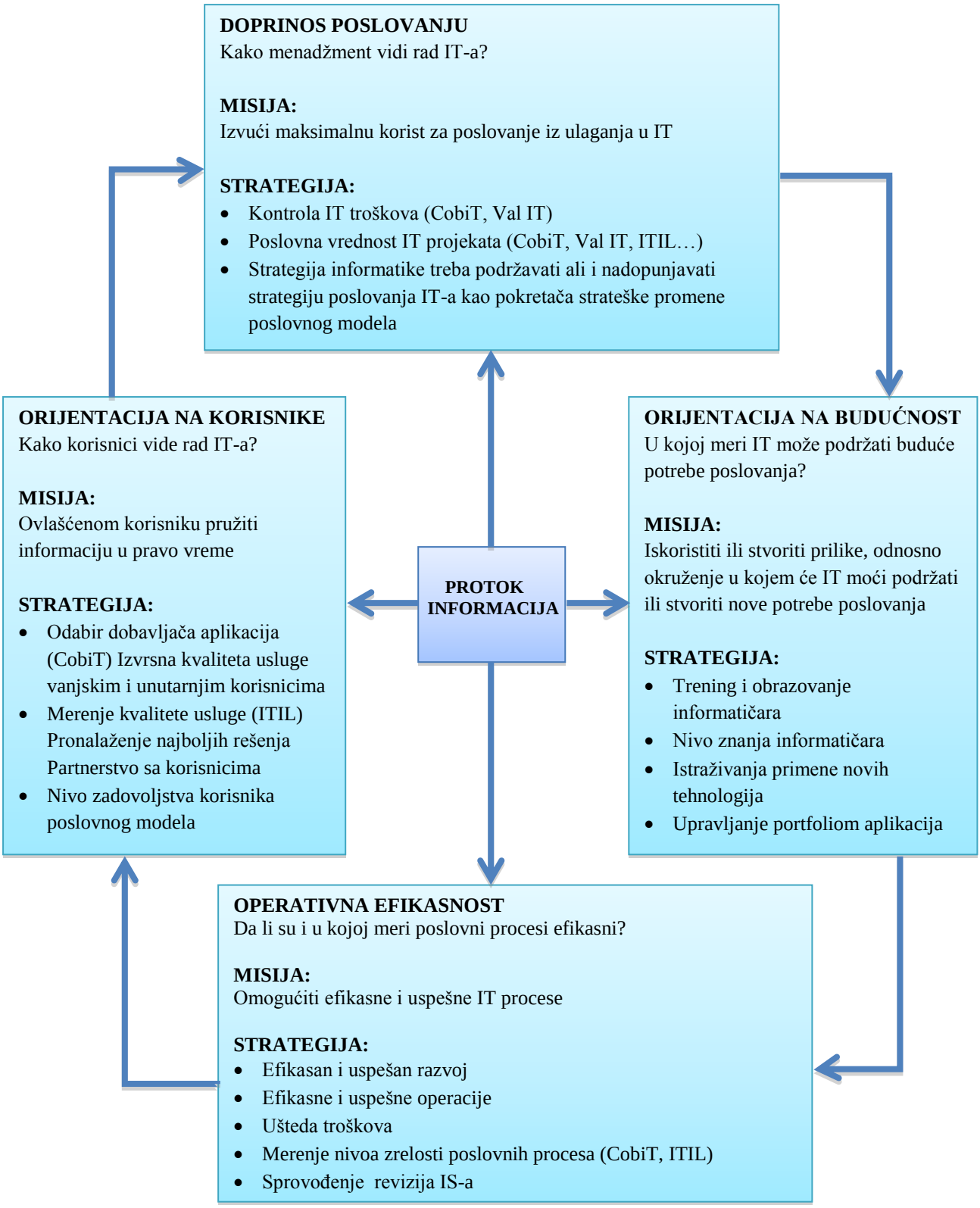
- Koju poslovnu vrednost IT treba dodati ili stvoriti?
- Kojim metodama najviši menadžment nadzire uspešnost ulaganja u IT? Kako biti siguran da ključni informatički projekti neće propasti ili izložiti poslovanje velikom riziku?
- Kako najviši menadžment nadzire rad informatike i CIO-a?
- Kojim metodama (i korporativnim telima) nadzirati sprovođenje strateških planova IT?



[96]*Engl. IT BSC - Information Technology Balanced Scorecard*

[97] Kaplan, R.S., Norton, D.P., (1996): The Balanced Scorecard: Translating Strategy into Action, Harvard Business School Press, Boston, SAD

Slika 21 - Odnos tradicionalnog BSC modela i IT BSC modela



Slika 22- Generički IT BSC model

Slika 21 prikazuje osnovna četiri područja tradicionalnog BSC modela i IT BSC modela. Jasno je vidljiva njihova međusobna povezanost, čiji se nivo može meriti uspostavom sistema merenja performansi (u tabelama 4 i 5 su prikazani mogući scenariji za izradu takvih metrika). Važno je istaknuti da su poveznice obostrane, što znači da i pojedina područja IT BSC modela mogu u znatnoj meri uticati na performanse područja unutar tradicionalnog BSC modela. Upravo te poveznice možemo smatrati temeljem korporativnog upravljanja informacionih tehnologija, odnosno vezom između menadžmenta i informacionih tehnologija.

Slika 222 prikazuje primenu BSC metode na IT, odnosno razrađen je generički IT BSC model. Metode i okviri se međusobno nadopunjuju sa osnovnim ciljem: kako pokriti odgovarajuće područje korporativnog upravljanja informacionim tehnologijama i menadžmentu pružiti što bolji alat za merenje performansi IT-a kao poslovne funkcije.

Postupak operativnog sprovođenja IT BSC modela odvija se u sledećim koracima (fazama):

- odrediti ključne strategije i metrike uspešnosti za svaku od 4 osnovna područja i zadužiti odgovorne osobe,
- temeljne ciljeve razdvojili po glavnih područjima,
- odredili uzročno-posledične veze među područjima i metrikama uspešnosti,
- unutar svakog područja odrediti metrike uspešnosti (primeri su u tabelama 4 i 5),
- odrediti obaveze i odgovornosti za sprovođenje zacrtanih ciljeva.
- primenom odgovarajućih okvira i metoda (Cobit, ITIL, ISO, ...) nadzirati sprovođenje i ocenjivati nivo uspešnosti,
- pratiti na koji način pojedinačni ciljevi i metrike utiču na glavne odnosno strateške ciljeve.

U tabelama 4 i 5 su primeri razrade metrika uspešnosti unutar pojedinih kategorija IT BSC modela.

Tabela 4- Razrada operativnih metrika uspešnosti IT BSC modela unutar područja Doprinos poslovanju

PODRUČJE: DOPRINOS INFORMATIKE POSLOVANJU	
Cilj: omogućiti maksimalni profit uz uspešno upravljanje informatičkim rizicima	
Pod-područja i njihovi ciljevi	
Strateško povezivanje poslovanja i informacionih tehnologija	
Metrike	• Sprovođenje koncepta korporativnog upravljanja informacionim tehnologijama • Koliko važnih informatičkih projekata u svim tačkama podupire i nadopunjuje strategiju poslovanja? • Koliko je % poslovnih ciljeva podržano od strane IT-a?
Stvaranje vrednosti	
Metrike	• Upravljanje performansama poslovnih jedinica • Poslovna vrednost važnih informatičkih projekata (studije izvodljivosti, ROI, NPV, IRR, vreme povratka ulaganja, Val IT ..) • Troškovi IT-a / ukupni troškovi • Način obračuna troškova IT-a - IT kao profitni centar
Upravljanje rizicima	
Metrike	• Broj novo-uvedenih inicijativa u vezi s kontrolom IS-a, revizijom i sigurnosti IS-a • Broj i nivo kritičnosti sigurnosnih incidenata • Izveštavanje menadžmenta o nivou informatičkih rizika • Broj izvršenih revizija informacionih sistema • Implementirane preporuke nakon revizija • Nadzor plana održavanja i upravljanja kontinuitetom poslovanja • itd. ..

Tabela 5 - Moguća razrada operativnih metrika uspešnosti IT BSC modela unutar područja Operativna efikasnost

PODRUČJE: OPERATIVNA EFIKASNOST	
Cilj: uspešno i delotvorno korporativno upravljanje informacionim tehnologijama	
Pod područja i njihovi ciljevi	
Strukture	
Metrike	• Broj sastanaka Odbora za strategiju IT-a • Sastav Odbora za upravljanje IT-a i Odbora za strategiju IT-a • Način rada i korporativna snaga tih Odbora • CIO član Uprave ili član izvršnog menadžmenta
Procesi	
Metrike	• Usklađenost strategije informatike i strategije poslovanja • Broj sati koje su izvršni menadžeri potrošili na pitanja usklađenosti poslovne strategije i IT-a • Metode praćenja poslovnih performansi informatike (IT BSC, Cobit,...) • Broj informatičkih procesa čije se performanse prate (mere) • Broj informatičkih procesa pokrivenih Cobit-om • Broj informatičkih procesa pokrivenih ITIL-om • Nivo zrelosti informatičkih procesa • % ciljeva IT koje podržavaju informatički procesi • Brzina sprovođenja poslovnih procesa i transakcija • Uštede u sprovođenju poslovnih procesa i transakcija
Zrelost	
Metrike	• Opšti nivo zrelosti korporativnog upravljanja informacionim tehnologijama • Nivo zrelosti kritičnih poslovnih i informatičkih procesa

8. POREĐENJE COBIT, ITIL I ISO17799 STANDARDA

Ove tri opisane metodologije su dosta korišćene u poslednjih nekoliko godina od strane pojedinih organizacija i predstavljaju najbolje prakse, odobrene, razvijene i testirane od strane stručnjaka širom sveta. Tabela 6. prikazuje korelaciju između kontrolnih ciljeva predstavljenih preko Cobit okvira sa standardom ISO 17799 i ITIL metodologijom. Nakon analize svake kontrole Cobit modela, u radu se predstavlja i predlog kategorizacije, u cilju grupisanja kontrolnih ciljeva, i to na tri nivoa[98]:

- Strateški nivo
- Taktički nivo
- Operativni nivo

Tabela 6- Poređenje Cobit-a, ITIL-a i ISO17799

	COBIT KONTROLNI CILJEVI		Ciljevi koji upućuju na ISO 17799	Ciljevi koji upućuju na ITIL
STRATEŠKI NIVO	PO - PLANIRANJE I ORGANIZACIJA			
	PO1	Strateško planiranje IS		
	PO2	Definisanje informacione arhitekture	✓	
	PO3	Određivanje tehnoloških smernica	✓	površno
	PO4	Definisanje IT procesa, organizacije i odnosa	✓	površno
	PO5	Upravljanje IT investicijama i troškovima		površno
	PO6	Komuniciranje prema menadžmentu	✓	

[98]Radovanović D., Radojević T., Lučić D., Šarac M., "Analysis of methodology for it governance and information systems audit", 6th International Scientific Conference Business and Management–2010 May 13-14, 2010, Vilnius, Lithuania, ISBN 2029-4441, p.943-949

	COBIT KONTROLNI CILJEVI		Ciljevi koji upućuju na ISO 17799	Ciljevi koji upućuju na ITIL
	PO7	Upravljanje ljudskim resursima	✓	
	PO8	Upravljanje kvalitetom	✓	
	PO9	Upravljanje i procena rizika	✓	
	PO10	Upravljanje projektima		
	PO11			
TAKTIČKI I OPERATIVNI NIVO	DS - ISPORUKA I PODRŠKA			
	DS1	Definisanje i upravljanje servisnim usluga	✓	✓
	DS2	Upravljanje spoljnim uslugama	✓	✓
	DS3	Upravljanje performansama i kapacitetom	✓	✓
	DS4	Osiguranje kontinuiteta usluga	✓	✓
	DS5	Sigurnost sistema	✓	
	DS6	Određivanje i dodela troškova		✓
	DS7	Edukacija i obuka korisnika	✓	
	DS8	Podrška korisnicima	✓	✓
	DS9	Upravljanje konfiguracijom	✓	✓
	DS10	Upravljanje problemima i incidentima	✓	✓
	DS11	Upravljanje podacima	✓	✓
	DS12	Upravljanje pomoćnom opremom	✓	
	DS13	Upravljanje operacijama (obradom)	✓	✓
	AI - NABAVKA I IMPLEMENTACIJA			
	AI1	Određivanje mogućih rešenja	✓	✓
	AI2	Nabavka i održavanje aplikativnih programa	✓	✓
	AI3	Nabavka i održavanje tehnološke arhitekture	✓	✓
	AI4	Korišćenje i funkcionalnost rada (obrade)	✓	✓
	AI5	Nabavka IT resursa	✓	✓
	AI6	Upravljanje promenama	✓	✓
	AI7	Instalacija i odobravanje rešenja i promena	✓	✓
STRATEŠKI NIVO	ME - NADZOR I PROCENA USPEŠNOSTI			
	ME1	Nadzor i procena IT performansi	✓	
	ME2	Nadzor i procena internih kontrola	✓	
	ME3	Usklađenost sa zakonskim i drugim normama		
	ME4	Korporativno upravljanjem IT-om		

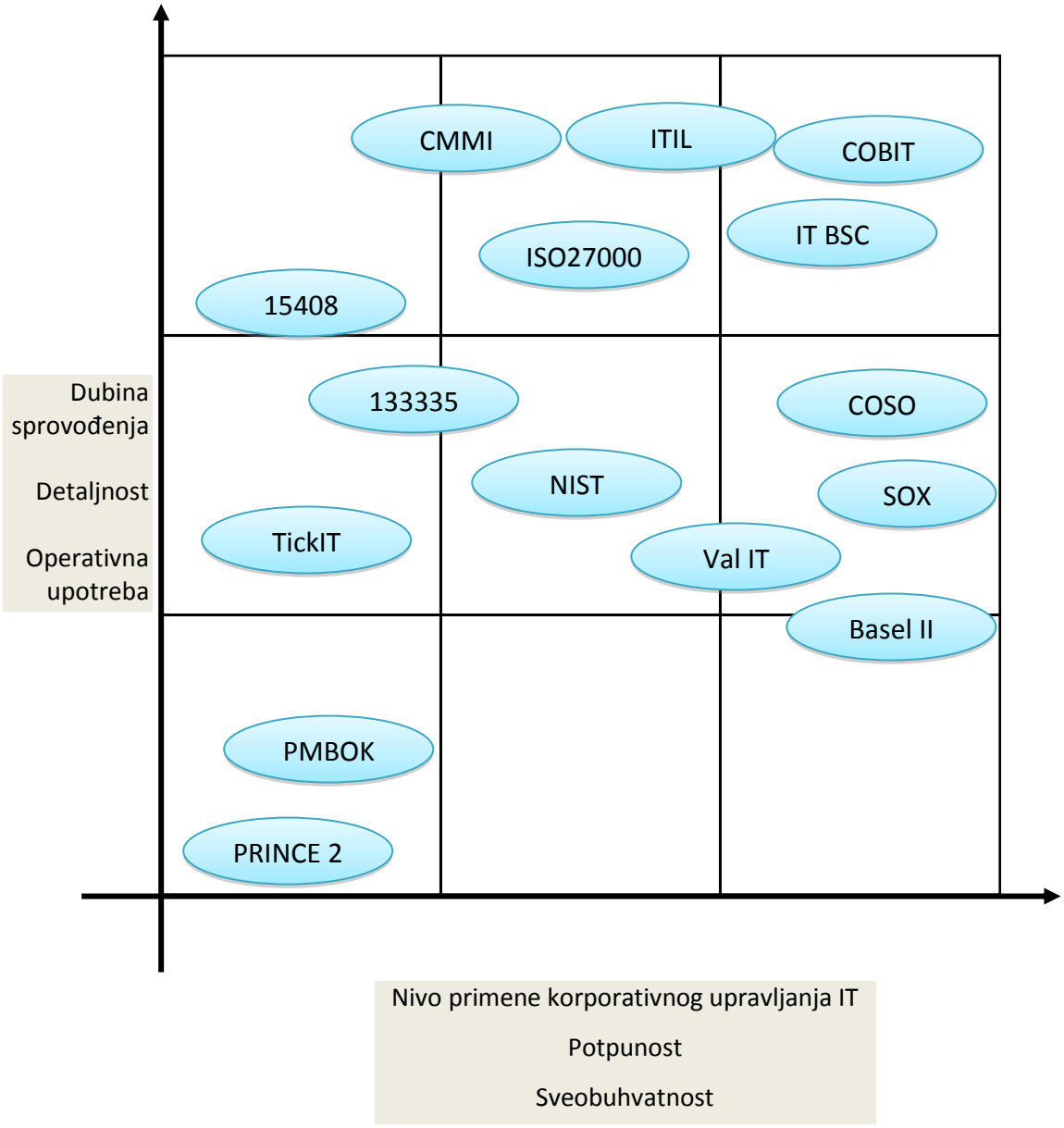
U odnosu na COBIT okvir, ITIL detaljno opisuje postupke za podršku i isporuku usluga (DS domen), ali ne podržava sve zahteve vezane za kontrolu i nadzor upravljanja informaciono

komunikacionim tehnologijama jedne organizacije. Pojedini kontrolni ciljevi Cobit modela u domenu planiranja i organizacije se površno tretiraju i prikazujeu kroz procese ITIL-a (PO domen). ITIL ne opisuje i ne objašnjava domen za nadzor i procenu uspešnosti u okviru Cobit modela. ITIL model nije fokusiran na opisivanje šta treba da bude razmotreno u upravljanju IKT. Procesi su detaljno strukturirani da ukažu ko i kako treba da ih primeni (uloge i odgovornosti).

Tabela 7- Pregled Cobit-a, ITIL-a, ISO27002

	COBIT	ITIL	ISO27002
Function	Mapping IT Process	Mapping IT Service Level Management	Information Security Framework
Area	34 Processes and 4 Domains	9 Processes	10 Domains
Issuer	ISACA	OGC	ISO Board
Implemen-tation	Information System Audit	Manage Service Level	Compliance with security standards
Consultant	Accounting Company, IT Consulting Company	IT Consulting Company	IT Consulting Company, Security Company, Network Consultant

Primena metoda, standarda i okvira u korporativnom upravljanju informacionim tehnologijama prikazana je na slici 25.



Slika 23 - Primena metoda, standarda i okvira u korporativnom upravljanju informacionim tehnologijama

ČETVRTI DEO

UPRAVLJANJE RIZICIMA

1. UVODNO RAZMATRANJE

Poslovanje je u svakom svom segmentu izloženo iskušenjima i opasnostima koje otežavaju upravljanje tim poslovanjem i dovode u pitanje ostvarenje zacrtanih poslovnih ciljeva. Kompanije i njeni poslovni procesi, sredstva kojima se ti procesi obavljaju i njihovi izvršitelji izloženi su stalnim rizicima. To su činjenice koje su više manje svakome iskustveno poznate i intuitivno razumljive. Savremeno shvatanje poslovnog (korporativnog) upravljanja se ne može zadovoljiti samo iskustvenim i intuitivnim spoznajama već će teži što je moguće egzaktnijem i naučno utemeljenom utvrđivanju svih relevantnih činjenica.

1.1. Upravljanje rizicima - osnovna značenja pojmova

U prošlosti najčešće korišćen pristup sigurnosnim aspektima poslovnih rizika je bilo izbegavanje rizika[99]. Taj se pristup odnosno model borbe protiv rizika fokusirao isključivo na prevenciju, tj. preuzimanje mera zaštite poslovanja od gubitaka ili šteta, nezavisno o stepenu njegove izloženosti određenim rizicima. Danas je, međutim, taj pristup zamenjen novijim pod nazivom upravljanje rizicima[100].

Za razliku od izbegavanja rizika, upravljanje rizicima nastoji da:

- otkrije i identifikujei slabosti u organizaciji ili sistemu (poput vodovodnog sistema, sistema napajanja električnom energijom, građevinskih konstrukcija ili informacionih sistema)

[99] *Engl. Risk Avoidance*

[100] *Engl. Risk Management*

- ponudi racionalnu i izvodljivu metodu odlučivanja o ulaganju finansijskih sredstava i izboru troškovno učinkovitih protivmera kojima će se štiti vredna imovina kompanije

- unapredi stepen uspešnosti napora koji se u organizaciji ulažu u povećanje sigurnosti i stabilnosti uslova poslovanja

- pomogne stručnjacima za bezbednost i donosiocima ključnih odluka u pronalaženju odgovora na pitanje svih pitanja koje glasi: Koji se stepen sigurnosti može smatrati dopustivim za ostvarenja održivog i racionalnog poslovanja kompanije?

Najjednostavnije rečeno, upravljanje rizicima je sistematičan analitički proces pomoću kojeg kompanija pronalazi, identifikuje, smanjuje i kontroliše potencijalne rizike kojima je izložena. Proces omogućavakompanijamaodređivanjenivoa ozbiljnosti i težine potencijalnih gubitaka, verovatnoću da li se takav gubitak može desiti, kao i protivmere koje treba koristiza smanjivanje verovatnoće ili iznosa gubitka. Treba pronaći prihvatljiv nivo rizika koji odražava najbolju kombinaciju sigurnosti i troškova.

Rizik je funkcija imovine, pretnje i ranjivosti. Navedeni se pojmovi u analitičkoj praksi često interpretiraju i koriste na različite načine. Zbog toga će biti korisno odrediti kako se oni koriste i koji su njihovi međusobni odnosi u kontekstu upravljanja rizicima.

Rizik je potencijal dešavanja nekog neželjenog događaja. Primeri neželjenih događaja su brojni, primeri nekih su:

- gubitak novčanih sredstava
- gubitak reputacije (ugleda) kompanije
- gubitak informacija
- neovlašćeni pristup sistemskim resursima

Rizik je funkcija verovatnoće pojave (zbivanja) nekog neželjenog događaja i njegove posledice. Polazeći od navedenog, može se zaključiti sledeće: što je veća verovatnoća nastupanja neželjenog događaja i što su teže njegove posledice, rizik je veći.

Verovatnoća dešavanja neželjenog događaja zavisi od pretnji i ranjivosti.

Pretnja je namera ili potencijalna mogućnost neke osobe da preduzmeaktivnosti koje nisu u saglasnosti sa interesima kompanije. Ona je u isključivoj ingerenciji napadača i po pravilu nad njom ni vlasnik niti korisnik imovine nemaju nikakve kontrole.

Ranjivost je svaka slabost ili nedostatak bilo kojeg od elemenata imovine ili određene zaštitne mere koju preduzimaju njegov vlasnik ili korisnik koju može iskoristili napadač ili tržišni konkurent da bi naneo štetu interesima kompanije. Nivo ranjivosti, a posledično i nivo rizika, mogu se smanjiti osmišljavanjem, izborom i sprovođenjem (implementacijom) odgovarajućih sigurnosnih protiv mera.

Imovina je sve ono što kompanije poseduje i što za nju ima neku poslovnu vrednost. To mogu biti, zgrade, oprema, finansijska sredstva, ljudi, informacije, patenti, idejna rešenja, računarski programi i znanje njenih stručnjaka. Isto tako i poslovna reputacija kompanije, njen ugled u javnosti, brendovi koje je stvorila, akcije koje je preduzela ili upravo preduzima poslovne operacije. Drugačije rečeno, imovina neke organizacije je sve ono što joj treba za obavljanje poslova i za ostvarenje misije koju je njen menadžment postavio.

Neki elementi su kritičniji sa stanovišta ostvarenja misije kompanije, veći su učinci i posledice njegovog oštećenja ili uništenja. Primer, kvar nekog računara moguće je razumno brzo otkloniti ili, u krajnjem slučaju, neispravan računar zameniti drugim, samim tim i šteta će biti razumno mala. Ipak, oštećenje ili uništenje sadržaja baze podataka može dovesti do nesagledivih posledice koje se neće moći otkloniti u kratkom vremenu, tako da će i štete biti proporcionalno trajne i velike. Veći deoorganizacija koje izgube kritične poslovne funkcije u vremenskom periodu koji je duži od deset dana nikada se ne oporave[101].

Protiv mere ili mere zaštite su aktivnosti, softverska rešenja ili uređaji koji mogu umanjiti rizike pre nego što oni počnu delovati na imovinu, pretnje ili na ranjivost sistema.

[101]Fulmer, K. L., (2005): Business Continuity Planning – A Step-by-Step Guide with Planning Forms, Third Edition, The Rothsein Catalog on Disaster Recovery, Brookfield, Connecticut, 2005., str. 7

2. OSNOVNI DELOVI MODELA UPRAVLJANJA RIZICIMA

Analizi rizika trebalo bi da prethode određene pripremne aktivnosti za koje analitičar, mora odvojiti dovoljno vremena. On bi pre svega, trebalo da intervjuiše vlasnika imovine odnosno nekih njenih elemenata ili jednostavno da neformalno porazgovara sa njime kako bi utvrdio da li postoje neka ograničenja, na koja bi u daljem radu trebalo računati, kao i da precizno utvrdi svrhu, ciljeve i fokus, odnosno predmet analize rizika kome pristupa. Naime, vlasnik imovine ili nekog njenog elementa najbolje zna u kakvom je stanju i gde se nalazi njegova imovina, kao i u kojoj su meri neki njeni elementi kritični sa stanovišta odvijanja poslovanja kompanije.

Analitičar bi takođe trebalo da identifikuje sve zainteresovane strane ili dionike (engl. Stakeholder) i utvrditi njihove stavove, interese i ciljeve u pogledu zaštite imovine. Ovde se radi o ljudima ili organizacijama koje imaju izražene, ali ne nužno i sasvim podudarne interese s obzirom na imovinu koju treba štititi.

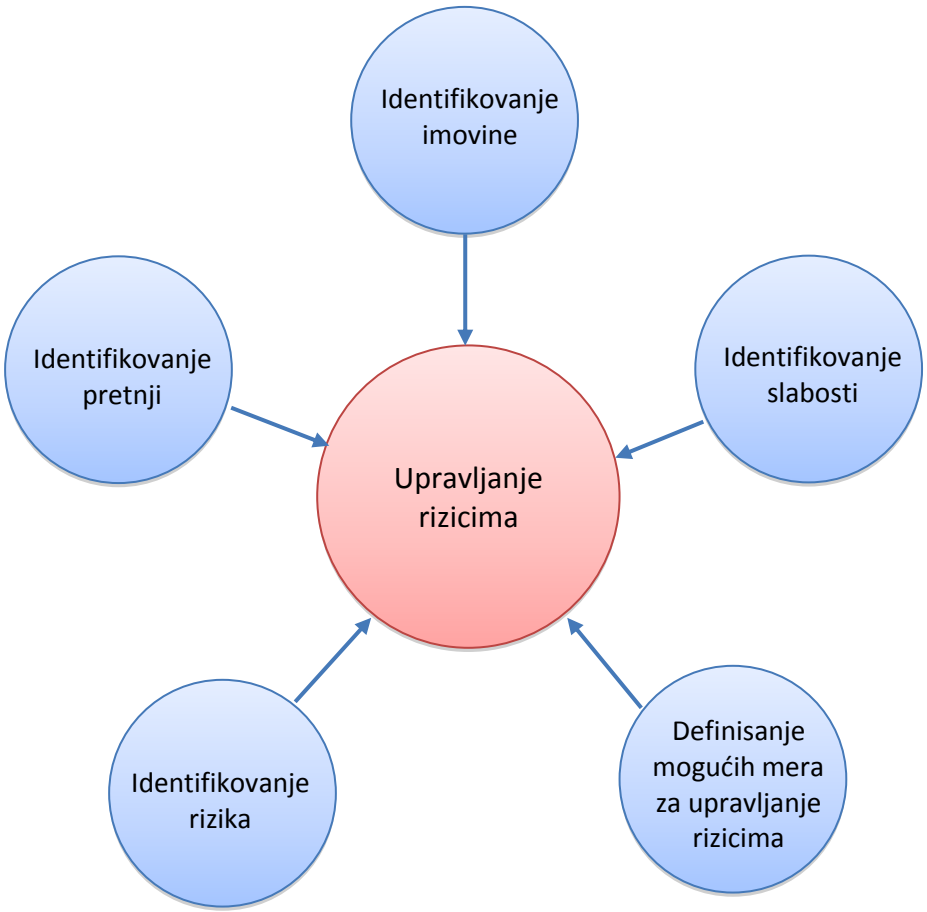
Primer, iako je administrator baze podataka nominalni „vlasnik" tog elementa ukupne imovine kompanije, za integritet (celovitost), ažurnost i tačnost sadržaja baze podataka zainteresovane su i mnoge druge strane, odnosno organizacione jedinice i pojedinci u kompaniji (pr. služba marketinga, osoblje pozivnog centra, računovodstvo, finansijski direktor, prodajna služba, projektanti informacionog sistema, tehnolozi, itd.). Svaka od tih organizacionih jedinica i svaki pojedinac imaju drugačije „gledanje" na ulogu i važnost korporativne baze podataka pa su, razumljivo, i njihovi interesi vezani uz zaštitu tog elementa imovine kompanije različiti.

Tek kad analitičar sakupi sve informacije, on može pristupiti osmišljavanju, razvoju i implementaciji modela upravljanja rizicima u konkretnoj poslovnoj sredini i situaciji.

Jakopeck[102] sugeriše da bi takav model trebao obuhvatati pet osnovnih delova:

1. identifikovanje imovine
2. identifikovanje pretnji
3. identifikovanje slabosti
4. identifikovanje rizika
5. definisanje mogućih mera za upravljanjerizicima

Na slici 24 može se naći grafički prikaz delova modela upravljanja rizicima.



Slika 24- Sastavni delovi modela upravljanja rizicima

[102] Jakopeck, E., (1997), "The Risk Assessment: Five Steps to Better Risk Management Decisions". Security Awareness Bulletin, br.3/1997, str. 515.

2.1. Identifikovanje imovine

Prilikom identifikovanja imovine stručnjak za bezbednost (u saradnji sa vlasnikom imovine) identifikuje i fokusira se samo na one elemente imovine koji su od važnosti za ostvarivanje misije kompanije i/ili obavljanje određenih poslovnih operacija. Utvrđivanje tih elemenata i njihove važnosti, odnosno prioriteta predstavlja osnovu za usmeravanje resursa prema bitnim elementima imovine, tj. onima najrelevantnijima sa stanovišta poslovanja koji samim tim zavređuju najveću pažnju.

Najveći deo imovine obično predstavljaju njeni materijalni „opipljivi“ elementi poput ljudi, mašina, građevinskih objekata, opreme, itd., dok manji deo njih otpada na nematerijalne „neopipljive" elemente imovine (informacije, znanje, patenti, brendovi, procesi, reputacija i ugled kompanije, itd.).

U infrastrukturnim operacijama, međutim, nematerijalni elementi imovine, poput informacija ili automatizovanih poslovnih procesa mogu biti, mada u ređem broju slučaja, čak i značajniji od „opipljivih" elemenata. Kompanije trebaju sa posebnom pažnjom štititi osetljive ili poverljive informacije, uključujući i informacije o funkcijama organizacije i njenih zaposlenih, u najmanju ruku podjednako pažljivo kao sto to čine onda kada se radi o kritičnim poslovnim procesima, poput osiguranja izvora energije, prečišćavanja otpadnih voda ili finansijskih transakcija.

Za svaki identifikovani značajan element imovine kompanije treba identifikovati neželjene događaje koji mogu na njih delovati, posledice koje bi nastale kada bi došlo do gubitka, oštećenja ili uništenja svakog od tih elemenata imovine. Ukupna vrednost imovine zavisna je o ozbiljnosti posledica neželjenih događaja.

Utvrđivanje imovine je najvažniji sastavni deo modela upravljanja rizicima, ostala četiri se oslanjaju na njega.

2.2. Identifikovanje pretnji

Prilikom identifikovanja pretnji stručnjak za zaštitu se usmerava na potencijalne napadače ili događaje koji mogu negativno uticati na prethodno utvrđene elemente imovine kompanije.

Pored iskustva i intuicije, on se ipak treba oslanjati prvenstveno na podatke, informacije i saznanja do kojih je došao prethodnim istraživanjem i intervjuisanjem relevantnih osoba u organizaciji.

Pojam pretnje veže se uz pojam napadača. Postoji nekoliko glavnih kategorija, odnosno tipova napadača, i to:

- klasične kriminalce koji uglavnom teže ostvarivanju materijalne koristi,
- poslovne konkurente koji pošto-poto žele ostvariti konkurentsku prednost i bolju tržišnu poziciju,
- hakere koji najčešće ne teže ostvarivanju nekih materijalnih koristi već ih više zanima neki oblik (samo)dokazivanja i potvrđivanja svoje tehnološko-intelektualne superiornosti pred „običnim" stručnjacima za zaštitu,
- organizovane i profesionalne obaveštajno-špijunske mreže koje deluju u skladu sa planovima i prema naredbama nalogodavaca iz određenih političkih, vojnih, industrijskih i drugih zainteresovanih društvenih krugova,
- teroriste kojima je prvenstveni cilj nanošenje štete određenoj organizaciji da bi joj stvorili probleme, otežali ili onemogućili rad, ili jednostavno širili paniku, strah i nemir u javnosti koja će saznati za posledice njihovih pretnji odnosno akcija,
- nezadovoljne često bivše zaposlene koji posežu za određenim metodama i sredstvima nanošenja štete organizaciji kojoj pripadaju (ili su pripadali) iz osvete ili da bi iskazali svoje negodovanje ili neslaganje sa nekim činjenicama, odnosima ili akcijama vezanima za organizaciju kojoj prete.

Da bi utvrdili da li neki potencijalni napadač zaista izvor pretnji po kompaniju, analitičari i stručnjaci za zaštitu moraju utvrditi postoji li namera i sposobnost napadača za stvaranje (uzrokovanje) neželjenog događaja koji bi mogao naneti štetu organizaciji.

Kao što se prirodne katastrofe i incidenti shvataju i tretiraju kao opšte sigurnosne pretnje, mada im se ne može utvrditi namera, neke informatičke pojave, poput računarskih virusa ili napada koji uzrokuju nemogućnost pružanja određene usluge *(engl. Denial-of-Service Attack, DoS Attack)*, takođe se mogu smatrati sigurnosnim pretnjama. Svaka organizacija koja svojim zaposlenima omogućuje pristup spoljnim računarskim mrežama, prvenstveno Internetu, a to su danas praktično sve savremene kompanije, ili spoljnim subjektima omogućuje pristup vlastitim informatičkim resursima i svojim unutrašnjim mrežama, takođe putem spoljne mreže (odnosno, najčešće, Interneta), mora biti svesna brojnih bezbednosnih pretnji ovog tipa čiji je izvor u njenom širem, pa i globalnom okruženju.

Kompanije koje su usmerene na primeni koncepta elektronskog poslovanja u tom smislu se smatraju najizloženijima i najugroženijima, jer su one praktički stalno „na Internetu" pa su potencijalno privlačnije sigurnosnim i bezbednosnim pretnjama od onih koje te koncepte poslovanja ne primenjuju.

Isto tako, savremena praksa pokazuje da u politički nestabilnim vremenima raste broj napada na infrastrukturne elemente imovine iz kategorije informatičke tehnologije, bilo da se radi o fizičkim napadima ili napadima za čije se izvršenje koriste informatička sredstva i metode. Zbog toga svaka kompanija, bez obzira je li sama zahvaćena nekim političkim (ili, još gore, ratnim) previranjima ili ne, tokom takvih događaja treba računati na povećanje sigurnosnih i bezbednosnih pretnji iz globalnog okruženja.

Pojedine kompanije, posebno one multinacionalne i one iz finansijskog sektora, česta su meta informatičkih bezbednosnih napada zbog toga što ih mnoge osobe, društvena udruženja i pokreti doživljavaju kao svojevrsni simbol globalizacije kojoj se protive i protiv koje se bore političkim pa i nekih drugim sredstvima.

2.3. Identifikovanje slabosti

Identifikovanje slabosti (ranjivosti) možda je od svih delova modela upravljanja rizicima najdublje ukorenjeno u tradicionalne pristupe problemima sigurnosti. Stručnjak za zaštitu identifikuje i određuje ranjivosti svojstvene određenim elementima imovine ili neželjenih

događaja. On nastoji da otkrije situacije koje se mogu zloupotrebiti zbog nedostatka odgovarajućih sigurnosnih mera, neprimerenog ponašanja ljudi, konstrukcionih grešaka u mašinama, uređajima i opremi, ili zbog neadekvatnih formalnih sigurnosnih procedura.

Primeri nekih tipičnih ranjivosti su sledeći:

- ne korišćenje usluga fizičko-tehničke zaštite u kompaniji, bez obzira da li to vlastito osoblje ili osoblje unajmljene organizacije
- slabe ili nepostojeće kontrole pristupa imovini kompaniji
- loše koncipirani i/ili nedorečeni ugovori o softverskim licencama ili kvalitetu usluga
- „šetnja“ neproverenih posetioca po sigurnosnim zonama odnosno područjima kompanije
- nedovoljno testiran računarski softver
- osoblje nedovoljno obrazovano i uvežbano za sprovođenje neophodnih sigurnosnih mera i procedura, itd.

Prilikom oblikovanja i instalacije sistema stručnjaci za sigurnost ne bi trebalo da oslanjaju samo u dobavljače i njihova obećanja odnosno garancije da će sistem pružati traženi nivo sigurnosti. Provera od strane nezavisnog stručnjaka ili organizacije specijalizovane za istraživanje i pronalaženje ranjivosti u sistemima će pružiti organizaciji objektivnu sliku i profil njenih sigurnosnih ranjivosti. Pritom je ipak najvažnije da stručnjak za sigurnost bude i ostane u punoj meri uključen u te procese i predan zadacima za koje je zadužen i odgovornostima koje su mu dodeljene.

Od stručnjaka se zahteva da na određeni element imovine kompanije gleda onako kako bi na njega gledao potencijalni napadač od spolja prema unutra, a ne obrnuto. Konkretno, stručnjak za sigurnost bi trebalo da analizira bitne element imovine kompanije postavljajući sam sebi pitanja poput sledećih:

- Kad bih želeo da fizički oštetim postrojenje X, šta bih prvo učinio?
- Da sam haker, u kojoj tački ili tačkama bih pokušao upasti u unutrašnju mrežu kompanije?
- Kada bih primetio da službe fizičko-tehničke zaštite ne funkcionišu kako bi trebalo, šta bih učinio?
- Da mi se kojim slučajem otvori mogućnost pristupa tajnim podacima, koje bi od njih i zašto bih kompromitovao?
- itd.

Ozbiljnost svake ranjivosti, razmatrana sa stanovišta napadača koji bi je mogao zloupotrebiti, kao i elemenata imovine kompanije koji bi mogli biti napadnuti može biti od veće ili manje važnosti za sveukupnu sigurnost kompanije. Utvrđivanjem važnosti svakog elementa imovine analitičar ili stručnjak za sigurnost će moći da utvrde koje od relevantnih ranjivosti će napadač najverovatnije pokušati da zloupotrebi.

3. RIZICI U OBLASTI PRIMENE I KORIŠĆENJA INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA

3.1. Poslovni rizici

Najopštije rečeno, rizik predstavlja mogućnost da dođe do nekog za nas nepovoljnog ishoda. Poslovni rizik se ogleda u mogućnosti da neki poslovni cilj ne bude ostvaren. Poslovni entiteti se neprekidno suočavaju sa mnoštvom različitih rizika, različitih po svojoj prirodi i po svom intenzitetu (tj. po verovatnoći realizacije nepovoljnog ishoda i visini štete koja bi nastala u slučaju realizacije nepovoljnog ishoda).

Da bi se poslovni entitet zaštitio od rizika, potrebno je uspostaviti proces upravljanja rizikom. Rukovodioci (i revizori) ne mogu nikada otkloniti rizik, jednostavno zato što je svaki poslovni poduhvat uvek rizičan. Kako se to već kaže u poslovnom svetu – „bez rizika nema dobitka". Prema tome, radi se na tome da se rizici identifikuju, izmere, predvide i (ako je moguće) spreče (ili da se minimizuju njihove posledice).

Kategorizacija rizika nam pomaže da rizike identifikujemo i kvantifikujemo (ocenimo, tj. izmerimo). Takođe, kategorizacija rizika nam pomaže da uspostavimo odgovarajuće kontrole – upravljačke, operativne i tehničke mere koje imaju za cilj prevenciju i minimizaciju poslovnih rizika.

3.2. Revizorski rizici

Revizorski rizik je mogućnost da dođe do greške u revizorskim nalazima, ocenama i mišljenjima. Greške mogu da se pojave u dva smera – mogući su previdi *(engl. false negatives)*, kada se konstatuje da je u redu nešto što zapravo nije u redu, ili „lažni alarmi" *(engl. false positives)*, kada se utvrdi da ne valja nešto što je zapravo bilo u redu. Previdi su znatno opasniji i predstavljaju glavninu revizorskih rizika.

Revizorski rizici su složeni i mogu da se kategorizuju u tri grupe – inherentni rizici, kontrolni rizici i rizici otkrivanja (rizici detekcije).

Inherentni rizici *(engl. inherent risks)* su oni koji su vezani neposredno za samu prirodu posla. Naime, kao što je već rečeno, svaki posao je rizičan. Međutim, neki oblici poslovanja su rizičniji od drugih. Na primer, vođenje poslova na globalnom nivou (internacionalno) je rizičnije od vođenja poslova na lokalnom tržištu.

Kontrolni rizici *(engl. control risks)* su oni koji su vezani za nesavršenosti u sistemima internih kontrola. Oni predstavljaju mogućnost da upravljačko – kontrolni mehanizmi jedne organizacije neće biti u stanju da na vreme spreče ili otkriju neki od poslovnih rizika.

Rizici otkrivanja (rizici detekcije – *engl. detection risks*) predstavljaju mogućnost da revizija neće na vreme otkriti materijalne greške, prevarne radnje itd.

Ove tri vrste rizika nisu međusobno nezavisne. U procesu procene rizika, sve tri moraju biti razmotrene kako bi se utvrdio njihov prihvatljivi nivo. Ne postoji mogućnost da se ovi rizici otklone u potpunosti, ali je moguće uspostaviti takav sistem kontrola koji će ih držati na prihvatljivom nivou i to na troškovno efikasan način.

Rizik koji preostane nakon primene kontrolnih mera naziva se rezidualni rizik.

3.3. Informatički rizici

Rizici od prisustva informacionih tehnologija su dvojaki. Jedna grupa se odnosi na mogućnost da se naruši tajnost, dostupnost ili integritet informacija (bezbednosni rizik – *engl. security risk),* dok je druga *(engl. IT deployment risk)* vezana za mogućnost da se informacione tehnologije uvedu, primene i koriste ili da se njima upravlja na način koji je generalno nepovoljan po realizaciju poslovnih ciljeva (rizik od umanjene efektivnosti, efikasnosti i ekonomičnosti informatičkih rešenja).

Tajnost (privatnost, poverljivost) informacija se odnosi na potrebu da se pristup informacijama ograniči samo na ovlašćene korisnike ili procese. Svaka informacija se kategorizuje (klasifikuje) po stepenu tajnosti, čime se u stvari definiše grupa korisnika i procesa koji imaju pravo pristupa toj informaciji. Procesi po pravilu nasleđuju pristupna

ovlašćenja onog korisnika koji je pokrenuo proces (ovlašćenja vlasnika procesa). Pristup se može ograničavati logički i fizički. Fizički pristup se odnosi na pristup prostorijama, računarima i drugoj opremi na kojoj se čuvaju, prenose ili obrađuju podaci. Logički pristup se odnosi na pristup informacionim sistemima, aplikacijama, bazama podataka bilo lokalno (nakon ostvarenog fizičkog pristupa), bilo udaljeno (bez fizičkog pristupa, preko mrežnih i drugih komunikacionih puteva). Fizički pristup se ograničava fizičko – tehničkim sredstvima, dok se logički pristup ograničava mehanizmima autentifikacije i autorizacije ugrađenim u operativne sisteme i aplikacije.

Integritet informacija se odnosi na tačnost, celovitost (kompletnost), ažurnost i pouzdanost podataka i informacija koje informacioni sistem proizvodi na osnovu tih podataka. Integritet može biti ugrožen u toku prikupljanja, skladištenja i prenosa podataka ili u toku obrade informacija i generisanja izveštaja.

Raspoloživost informacija se odnosi na potrebu da informacija uvek mora da bude dostupna ovlašćenim korisnicima i procesima. Pojam raspoloživosti je na izvestan način komplementaran pojmu tajnosti – obezbeđivanje pristupa se mora dešavati po principu „bez ovlašćenja nikad, ali sa ovlašćenjem uvek". Rizici od pojave problema sa raspoloživošću rangiraju se od jednokratnih i sporadičnih, preko trajnih ali povremenih *(engl. Denial of Service Risks),* sve do fatalnih, koji imaju katastrofalne razmere *(engl. Business Continuity and Disaster Risks).*

Efektivnost, efikasnost i ekonomičnost informatičkih rešenja može biti ugrožena u bilo kojoj fazi životnog ciklusa. Kao prvo, greške mogu biti učinjene u fazi strateškog planiranja. Strateški plan informatičkog razvoja mora da bude usklađen sa opštom strategijom organizacije, tako da se uklapa u viziju, misiju, ciljeve i politike koje je organizacija definisala. Svako odstupanje informatičke strategije od generalne strategije izlaže organizaciju visokom poslovnom riziku.

Ključni indikatori rizika u ovoj fazi su: odsustvo strateškog planiranja, odsustvo procene informatičkih rizika, odsustvo investicione analize, odsustvo kontrole kvaliteta, neadekvatna infrastruktura, nedovoljna komunikacija i informisanje u organizaciji itd.

Planiranje i projektovanje takođe unose specifične informatičke rizike. Organizacija mora jasno da definiše uloge i odgovornosti svih subjekata uključenih u ovu fazu. Izrada plana podrazumeva postavljanje rokova, definisanje obima projekta (graničnih uslova), tehničkih zahteva i drugih preduslova za kvalitetno projektovanje.

Projekat generalno mora da pruži tzv.predmet i predračun - „koliko nam čega treba i koliko će to da košta". Greške u ovoj fazi unose visoke poslovne rizike. U principu, greške u strateškim odlukama, planiranju i projektovanju dešavaju se ređe, ali ostavljaju po pravilu daleko najteže posledice. Šteta je po pravilu velika i teško se nadoknađuje.

Ključni indikatori rizika u fazi projektovanja su: izostanak odgovarajuće metodologije, nedovoljno iskustvo i znanje rukovodstva, timova i pojedinaca, izostanak podrške najvišeg rukovodstva, propusti u prikupljanju polaznih informacija i zahteva od svih relevantnih strana, nedovoljni resursi (novčana sredstva, vreme, ljudstvo) itd.

U fazi nabavke ili razvoja informacionih sredstava i sistema i njihove kasnije implementacije potrebno je takođe primeniti striktne mere kontrole i nadzora, kako bi se izbegli karakteristični rizici.

Ako se radi o nabavci, ključni indikatori rizika su: odstupanje od strategije, nedostatak dokumentovanih politika za nabavku softvera i hardvera, nabavka bez prethodne analize mogućnosti za sopstveni razvoj, propusti u prikupljanju korisničkih zahteva, propusti u oceni bezbednosti rešenja, odsustvo analize u domenu integracije i skalabilnosti rešenja, previdi u domenima obuke korisnika, modela licenciranja, potrebne podrške i održavanja, budućih nadogradnji (upgrade) i modifikacija itd.

Ako se radi o razvoju, ključni indikatori rizika su: odstupanje od strategije, izostanak prethodne studije izvodljivosti, izostanak prethodne analize poslovnih procesa, propusti u prikupljanju zahteva od rukovodstva i/ili korisnika, propusti u razdvajanju razvoja, testiranja i produkcije sistema, odsustvo mehanizama zaštite i nepoštovanje principa informatičke bezbednosti u razvoju itd.

U fazi implementacije sistema najznačajniji indikatori rizika su: izostanak razmatranja alternativnih metoda implementacije, nepostojanje dokumentovanog plana implementacije, slabosti u koordinaciji uključenih timova i pojedinaca, nerazvijene procedure za upravljanje

promenama, nedovoljna ili neadekvatna obuka korisnika, izostanak ili neadekvatnost postupka finalnog testiranja itd.

U svim fazama uvođenja informatičkih rešenja neophodne su adekvatne upravljačko – kontrolne mere i stalni nadzor (monitoring, supervision) od strane rukovodstva.

Revizija IS ima veoma važnu ulogu u ovim procesima koja se sastoji u oceni adekvatnosti ovih kontrola, doslednosti njihove primene i njihove efektivnosti u pogledu umanjenja specifičnih rizika.

3.4. Mrežni i komunikacioni rizici

U uslovima umrežavanja, koji su danas praktično svuda prisutni, dolazi do pojave niza specifičnih rizika, kojih kod zasebnih računarskih sistema nema ili su znatno slabije izraženi.

Pre svega, u mrežnim okruženjima, pored običnih računara (radnih stanica) postoji niz različitih uređaja koji su neizbežni deo mrežne i telekomunikacione infrastrukture: modemi, kablovi ili radio uređaji za prenos signala, ruteri, svičevi, pristupni serveri, aplikativni serveri, serveri baza podataka, mrežni štampači itd.

Takođe, softver je složeniji jer sadrži podršku za rad u mreži – implementaciju brojnih mrežnih protokola i servisa. Prema tome, mrežna okruženja sadrže znatno veći broj potencijalnih pretnji. Realni rizici su samim tim brojniji i raznovrsniji.

Pretnje kojima su izloženi umreženi sistemi mogu se podeliti u nekoliko grupa.

Prva grupa su pretnje fizičkoj infrastrukturi, kao što su elementarne nepogode i prirodne katastrofe (poplava, požar, zemljotres i slična razorna dejstva). Iako ove pretnje mogu da ugroze i zasebne, ne umrežene računarske sisteme, one su kod umreženih sistema znatno rizičnije, zbog prostorne distribucije i fizičke razuđenosti koja karakteriše većinu računarskih mreža. Treba napomenuti da pretnja fizičkoj infrastrukturi može da nastupi i od ljudskog faktora – sabotaže, diverzije itd.

Sledeća grupa su tzv. programske (ili programirane) pretnje. Takvu pretnju predstavljaju sve vrste malicioznog softvera – virusi, crvi, trojanski konji, špijunski i reklamnisoftver *(engl. spyware, adware)*, „rutkitovi" (rootkits), „botovi" (bots, botnets), itd.

U treću grupu spadaju pretnje koje sprečavaju rad sistema, njihovih pojedinih delova ili servisa *(engl. Denial of Service - DoS)*. Iako mogu postojati i na lokalnom nivou (local DoS), ove pretnje su posebno izražene u mrežama, gde slabosti u implementaciji ili konfiguraciji sistema mogu da budu iskorišćene za napade sa udaljenih tačaka.

Posebno su opasni distribuirani DoS napadi, kod kojih se javlja tzv. amplifikacioni (pojačavački, lavinski) efekat – mala količina mrežnog saobraćaja se usmerava ka velikom broju tačaka u mreži, sa kojih se onda sinhronizovano, u isto vreme, pokreće mnoštvo napada koji u zbiru rezultiraju saobraćajnim preopterećenjem napadnutog sistema.

Druga i treća grupa su direktno uslovljene egzistencijom tzv. softverskih *slabosti (engl. software vulnerabilities)*. Slabe tačke operativnih sistema, mrežnih protokola, servisa i aplikacija potiču od grešaka učinjenih tokom njihovog projektovanja, kodiranja ili kasnije prilikom instalacije i konfigurisanja. Greške u kodiranju su vrlo česte i praktično neizbežne, toliko da većina proizvođača softvera redovno publikuje ispravke za svoje proizvode (softverske korekcije, „zakrpe" - engl. patch). Korisnici pritom preuzimaju odgovornost za primenu ovih korekcija, često uvodeći posebne kontrolno – upravljačke procese koji služe samo za te potrebe *(engl. Patch Management)*. Na taj način se vrši transfer rizika sa slabosti softvera na slabosti u kontrolnom procesu. Slično tome, slabosti u instalacijama i konfiguracijama kontrolišu posebni upravljački procesi *(engl. Configuration and Change Management)*, tako da se pripadajući rizici mogu tretirati kao da potiču od nedostataka kontrolnog procesa. Rizici od ne otklonjenih softverskih nedostataka često se navode kao zasebna grupa rizika, premda su u tesnoj vezi i međuzavisnosti sa prethodne dve grupe. Ovi rizici su neposredno vezani za pretnje od moguće zloupotrebe ne otklonjenih softverskih nedostataka. Pored zlonamernog softvera koji automatski (programirano) zloupotrebljava „rupe" u sistemima, servisima i aplikacijama, zloupotrebe mogu biti učinjene i neposredno od strane ljudskog faktora. Napadači različitih profila, interesa i motivacije predstavljaju pretnju koja direktno ugrožava bezbednost (tajnost, integritet, raspoloživost), ometa funkcionisanje

sistema, narušava ugled organizacije, čini materijalnu štetu (uvećava troškove) i izlaže organizaciju nizu drugih poslovnih rizika.

Posebna grupa rizika vezana je za zloupotrebu slabosti koje su svojstvene ljudskom faktoru. Lakovernost, neupućenost, predvidljivost ljudskih reakcija i ponašanja i druge osobine karakteristične za prosečnu ličnost mogu biti zloupotrebljene od strane napadača. Prevare, manipulacije, dezinformacije, lažno predstavljanje i slično, u uslovima umreženog poslovanja, gde je čest slučaj poslovnih kontakata sa osobama sa kojima se nikada nismo fizički susreli i upoznali, dobijaju vrlo povoljne mogućnosti za uspeh. U novije vreme, o ovoj vrsti rizika se dosta piše, najčešće pod nazivom „socijalni inženjering" *(engl. social engineering).* Međutim, u ovu grupu mogu da se svrstaju i neke pretnje koje usko gledano ne spadaju u socijalni inženjering, ali se takođe baziraju na zloupotrebi ljudske slabosti, kao što su širenje dezinformacija *(engl. hoax),* podmetanje lažnih adresa, servera i servisa *(engl. phishing)* i slično.

Izložena kategorizacija rizika u velikoj meri pojednostavljena i da nikako ne može biti uzeta kao konačna ili jedina moguća. Ipak, ona može da posluži ne samo kao ilustracija osnovnog pojma rizika, već čak i da olakša identifikaciju glavnih rizika usled prisustva IKT u nekom realnom poslovnom okruženju.

4. KLASIFIKACIJA INTERNIH IKT KONTROLA

Potreba za kontrolom u poslovnim procesima stara je koliko i samo poslovanje. Međutim, teorijske osnove i prva sistematizovana praktična uputstva postavljaju se tek u novije vreme. U svom izveštaju iz 1992. godine, organizacija COSO postavlja teorijsku osnovu za sisteme internih kontrola. Iako izvorno američki, ovaj materijal ubrzo postaje internacionalno prihvaćen. Slede slični poduhvati u nizu drugih zemalja: Velikoj Britaniji (Cadbury Report), Kanadi (CoCo), Francuskoj (Vienot Report), Južnoj Africi (King Report) itd.

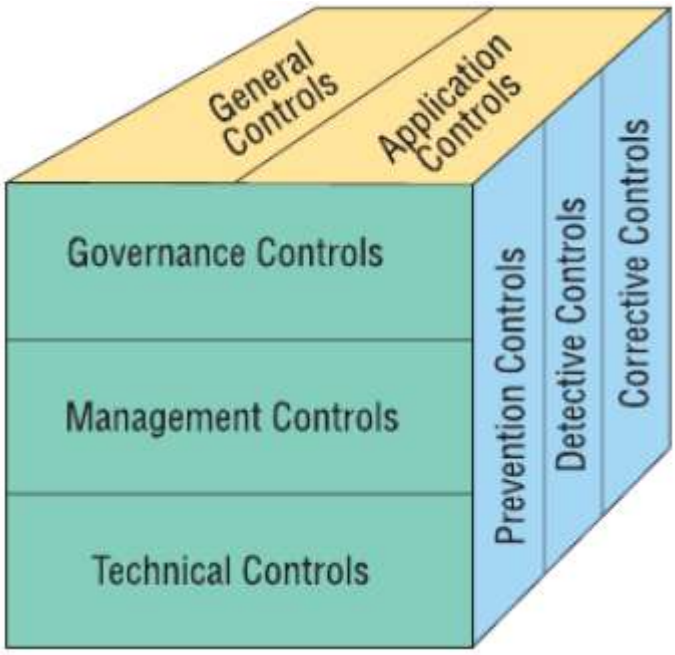
U svim ovim izveštajima daju se najopštije definicije interne kontrole kao procesa koji ima za cilj održavanje i unapređenje efektivnosti i efikasnosti poslovnih operacija, pouzdanosti finansijskog izveštavanja i usklađenosti sa zakonima i drugom regulativom. Veoma značajno je i to što se interne kontrole u svim ovim dokumentima jasno postavljaju u okvire neposredne odgovornosti rukovodstva. Kontrola je prepoznata kao sastavni deo procesa upravljanja i ne može biti delegirana drugim entitetima, pa tako ni internoj reviziji.

Pored ovih najopštijih okvira, razvijaju se i okviri za pojedine uže oblasti kontrole, kao što su kontrola rizika, kontrola kvaliteta itd.

U oblasti primene i korišćenja informacionih i komunikacionih tehnologija najdetaljniju razradu poslovnih procesa i pripadajućih kontrolno – upravljačkih mehanizama daje organizacija ISACA u svojim smernicama Cobit.

Interne kontrole u oblasti primene i korišćenja tehnologija mogu da se klasifikuju na više načina. Jedna veoma uprošćena podela već je korišćena ranije u ovom radu. To je podela na opšte (generalne) i aplikativne kontrole. Ta podela ilustruje osnovnu dvojnost internih kontrola u oblasti IKT. Naime, jednim delom IKT kontrole služe kao podrška upravljanju i upravljanju poslovnim procesima koji su implementirani u informacionim sistemima i poslovnim aplikacijama, dok drugim delom ove kontrole služe za upravljanje samom

tehnološkom infrastrukturom, kao podrška delu organizacije koji je odgovoran za primenu i korišćenje informacionih i komunikacionih tehnologija.



Slika 25- Interne kontrole u IKT sistemima

Ostali primeri moguće klasifikacije internih kontrola su podele na ručne i automatske, obavezne i opcione, komplementarne (redundantne) i kompenzacione *(engl. complementary, redundant, compensating)*, neprekidne, „na zahtev" i „po događaju" *(engl. continuous, on-demand, eventdriven)* itd.

Jednostavnija klasifikacija, ali dovoljno elaborirana da omogući dobar uvid i pravilno razumevanje internih kontrola u kontekstu IKT je data u publikaciji Instituta internih revizora (IIA) pod nazivom Information Technology Controls (GTAG-01)[103]. Ta klasifikacija daje trostruku podelu, pa se kao ilustracija koristi grafički prikaz u tri dimenzije (kocka).

[103] The Institute of Internal Auditors, (2012), Information Techology Risk and Controlos, IIA, 2nd Edition

Na slici 25 je prikazana trostruka podela: u jednoj ravni je podela na generalne i aplikativne kontrole, u drugoj na preventivne, detektivne i korektivne, dok je u trećoj podela prema nivou ovlašćenja i odgovornosti za uspostavljanje i primenu kontrola: najviše upravljačke kontrole, kontrole u nivou rukovodstva i tehničke kontrole.

4.1 Opšte (generalne) kontrole

Ove kontrole su poznate i pod nazivom infrastrukturne kontrole. One se odnose na sve sistemske komponente i procese u primeni i korišćenju IKT i pripadajuće podatke relevantne za datu organizaciju ili okruženje. One, između ostalog, uključuju politike informatičke bezbednosti, administraciju sistema, pristup sistemu i njegovim komponentama, razdvajanje (separaciju, segregaciju) dužnosti kod ključnih IKT funkcija, upravljanje nabavkom, razvojem, implementacijom i konfiguracijom, upravljanje promenama u sistemu, upravljanje primenom sistemskih korekcija, kontrole za kontinuitet poslovanja i oporavak od incidenata, izrada rezervnih kopija (backup), procedure za njihovu primenu kod sistemskog oporavka (recovery) itd.

4.2 Aplikativne kontrole

Kao što je već pominjano, aplikativne kontrole se odnose na mehanizme ugrađene u informacione sisteme i aplikativnu logiku, a koji služe kao podrška upravljanju i kontroli poslovnih procesa. Tu spadaju, između ostalog, kontrole za validaciju polja za unos podataka, kontrole autorizacije za pristup segmentima poslovnih aplikacija, razdvajanje (segregacija) poslovnih funkcija, kontrole tačnosti raznih obračuna, registrovanje tragova o transakcijama, izveštaji o greškama itd.

4.3 Preventivne kontrole

Preventivne kontrole imaju za cilj da spreče nastajanje događaja nepovoljnih po organizaciju i njene ciljeve. Primer preventivnih kontrola su kontrole za validaciju unosa podataka. U polja

za unos numeričkih podataka ne sme se dozvoliti unos znakova koji nisu cifre – slova, interpunkcija, kontrolni znakovi i sl. Drugi primer su kontrole za autorizaciju pristupa koje sprečavaju pristup neautorizovanim korisnicima itd. U preventivne kontrole takođe spadaju i kompleksni korisnički softver, uređaji i sistemi, kao što su anti-virusni softver, mrežne barijere, sistemi za prevenciju upada (IPS[104]).

4.4 Detektivne kontrole

Detektivne kontrole otkrivaju nepovoljne događaje (greške, incidente i sl.) nakon što su se oni već desili. Cilj ovih kontrola je da otkrije nastale probleme i ukaže na njih pre nego što dođe do eskalacije njihovih štetnih posledica. Na primer, detektivne kontrole mogu da identifikuju neaktivne račune ili račune sa sumnjivim aktivnostima. Takođe, detektivne kontrole mogu da budu zadužene za praćenje raznih indikatora prevarnih radnji, probijanja limita kod transakcija, netačnosti u obračunima itd. Pored aplikativnih, detektivne kontrole mogu da budu i u grupi opštih kontrola – detekcija grešaka u komunikaciji, detekcija narušenog integriteta sistema fajlova, detekcija upada u sistem (IDS[105]), detekcija upotrebe neautentifikovanih, isteklih ili povučenih digitalnih sertifikata, itd.

4.5 Korektivne kontrole

Korektivne kontrole služe da se otklone slabosti, greške i propusti koje su dovele do nepovoljnih događaja. One se kreću od vrlo jednostavnih, kao što su prosto otklanjanje grešaka na unosu podataka, preko ukidanja naloga za pristup korisnicima koji su pokušali ili realizovali neautorizovani pristup, oporavka greškom izbrisanih podataka primenom rezervne kopije, pa sve do najsloženijih, kao što je aktiviranje rezervnih sistema za neprekidnost poslovanja u slučaju ozbiljnijih incidenata, otkaza pojedinih komponenti ili potpunog uništenja sistema.

[104] *Engl. Intrusion Prevention Systems – IPS*

[105] *Engl. Intrusion Detection Systems – IDS*

4.6 Kontrole na nivou najviše uprave (Governance)

Ova grupa obuhvata kontrole za čije uspostavljanje, primenu i funkcionisanje odgovara najviši nivo uprave u organizaciji: upravni odbor, generalni direktor, rukovodioci najvišeg nivoa i drugi organi uprave sa najvišim nivoom ovlašćenja i odgovornosti. U domenu primene i korišćenja tehnologija, kontrole ovog nivoa obuhvataju, pored ostalog, i sledeće: strateške smernice, politike za primenu i korišćenje tehnologija, politike za informatičku bezbednost, mere kojima se obezbeđuje nadzor nad odvijanjem poslovnih procesa, merenje i ocene rizika, merenje i ocene uspešnosti poslovanja itd. U najopštijem smislu, čitava poslovna funkcija interne revizije predstavlja takođe jednu iz ove grupe kontrola.

4.7 Kontrole na nivou rukovodstva (Management)

Ovde spadaju kontrole za čije uspostavljanje, primenu i funkcionisanje odgovaraju izvršni rukovodioci u organizaciji. Na prvi pogled je teško povući granicu između ove i prethodne grupe. Međutim postoji jednostavno pravilo za distinkciju: za rukovodioce iz prethodne grupe u pogledu internih kontrola važi pravilo „Noses in – fingers out", što je žargonski izraz za princip po kome je rukovodstvo iz grupe na nivou najviše uprave zaduženo za nadgledanje, praćenje i davanje opšteg usmerenja ali ne i za realizaciju. Za razliku od izvršnog rukovodstva, koje ima ovlašćenja i odgovornosti i za donošenje i za sprovođenje konkretnih poslovnih odluka, najviša uprava u sprovođenju uopšte ne učestvuje. U domen ovih kontrola spadaju upravljanje rizikom, kontrola usklađenosti sa zakonima,ostalom internom, eksternom regulativom i ugovorima, sprovođenje politika, procedura, kontrole radnog okruženja i bezbednosti na radu, upravljanje projektima, itd.

4.8 Tehničke kontrole

Tehničke kontrole predstavljaju najniži i u isto vreme osnovni nivo kontrola u oblasti primene i korišćenja tehnologija. One su temelj svakog sistema internih IKT kontrola i obezbeđuju osnovu za pouzdanost funkcionisanja praktično svih ostalih kontrola u jednoj organizaciji.

Na ovom nivou se zapravo ostvaruje neposredna (fizička i/ili logička) realizacija svih kontrola koje su kreirane i propisane na višim nivoima. Treba napomenuti da su ove kontrole zavisne od individualnih tehnologija i tehničkih rešenja koja su na njima zasnovana, što sa kontrolama višeg nivoa najčešće nije slučaj. Ukoliko organizacija obezbedi efektivan i efikasan sistem kontrola na tehničkom nivou, ispunjen je jedan od najkritičnijih faktora uspeha za ukupan sistem internih kontrola. Takođe, po samoj svojoj prirodi, tehničke kontrole se mogu u velikoj meri automatizovati. Isključenjem ručnih kontrola sa tehničkog nivoa i optimizovanjem automatskih kontrola, organizacija može da postigne veoma visok stepen zaštite od rizika.

Pored toga, prepoznavanjem značaja kontrola tehničkog nivoa i njihovim uključenjem u predmet revizije, IT revizija može da dodatno i vrlo značajno uveća svoj doprinos ukupnim vrednostima organizacije.

PETI DEO

ISTRAŽIVANJE

1. UVOD

Informacioni sistemi imaju izuzetno značajnu ulogu u svakodnevnom poslovanju i upravljanju kompanijama. Saglasno tome, kompanije u Srbiji danas, naročito one koje su u potpunom ili većinskom stranom vlasništvu, ulažu značajna sredstva (novac, vreme, osoblje) u informacione sisteme kako bi unapredile efektivnost i efikasnost svoga poslovanja, bile konkurentne ili ostvarile konkurentsku prednost i imale bolji imidž. Pored značajnih benefita, korišćenje informacionih tehnologija izlaže kompaniju i IT rizicima. Tako na primer, jedno malo preduzeće koje se bavi razvojem i prodajom aplikacija za mobilne telefone putem interneta, izloženo je brojnim IT rizicima koji se odnose, pre svega, na sigurnost i privatnost podataka, stabilnost IT infrastrukture, korišćenje društvenih medija od strane zaposlenih, ali i mnogim drugim.

U takvom okruženju, razumevanje IT rizika, uspostavljanje sistema IT kontrola kao odgovora na te rizike, sprovođenje revizije efektivnosti i efikasnosti funkcionisanja sistema IT kontrola, odnosno uspostavljanje dobre prakse korporativnog upravljanja informacionim sistemima je od izuzetnog značaja za uspešnost poslovanja kompanija.

1.1 Metodologija korišćena u istraživanju

Istraživanje je imalo za cilj da ispita uticaj kontrole i revizije informacionih sistema na uspešnost i efikasnost upravljanja i poslovanja kompanija u Srbiji. Sprovedeno je u periodu od juna 2013. godine do decembra 2014. godine. U cilju postizanja što veće reprezentativnosti uzorka istraživanjem su obuhvaćene kompanije različitog tipa, vlasničke strukture, veličine, kao i mnogobrojne oblasti poslovanja.

Osnovni metod prikupljanja podataka bila je anonimna anketa koja se sastojala od 40 pitanja sa više ponuđenih odgovora. Radi boljeg razumevanja dobijenih odgovora i prikupljanja

dodatnih informacija za analizu, sa skoro trećinom ispitanika obavljeni su i razgovori. Anketa je kreirana pomoću Lime survey aplikacije sa idejom jednostavnog korišćenja i popunjavanja upitnika. Korišćenje ovog alata omogućilo je brže popunjavanje upitnika. Linkovi za upitnik poslati su ispitanicima putem mejla ili privatnim porukama preko LinkedIn profesionalne društvene mreže. Kako bi se utvrdio stav različitih grupa o nivou razvoja, značaju i doprinosu kontrola i revizije informacionih sistema na uspešnost i efikasnost upravljanja i poslovanja kompanija u Srbiji ispitanici su bili podeljeni u dve grupe. Dodatno, na pojedina tehnička pitanja odgovore su bili stručni daju samo ispitanici iz IT oblasti i oblasti IT revizije:

- **I grupu ispitanika** činili su: IT direktori ili lica odgovorna za upravljanje informacionim tehnologijama, direktori interne revizije, IT revizori i revizori.
- **II grupu ispitanika** činili su: izvršni direktori i srednji menadžeri koji koriste IT usluge u kompanijama koje su bile u uzorku.

Ukupno je poslato 95 upitnika ispitanicima I grupe i 86upitnika ispitanicima druge grupe. Dodatno, dve ankete su poslate poštom ispitanicima prve grupe. Ankete su poslate ispitanicima iz 109 kompanija. Od ispitanika traženi su iskreni odgovori na postavljena pitanja.

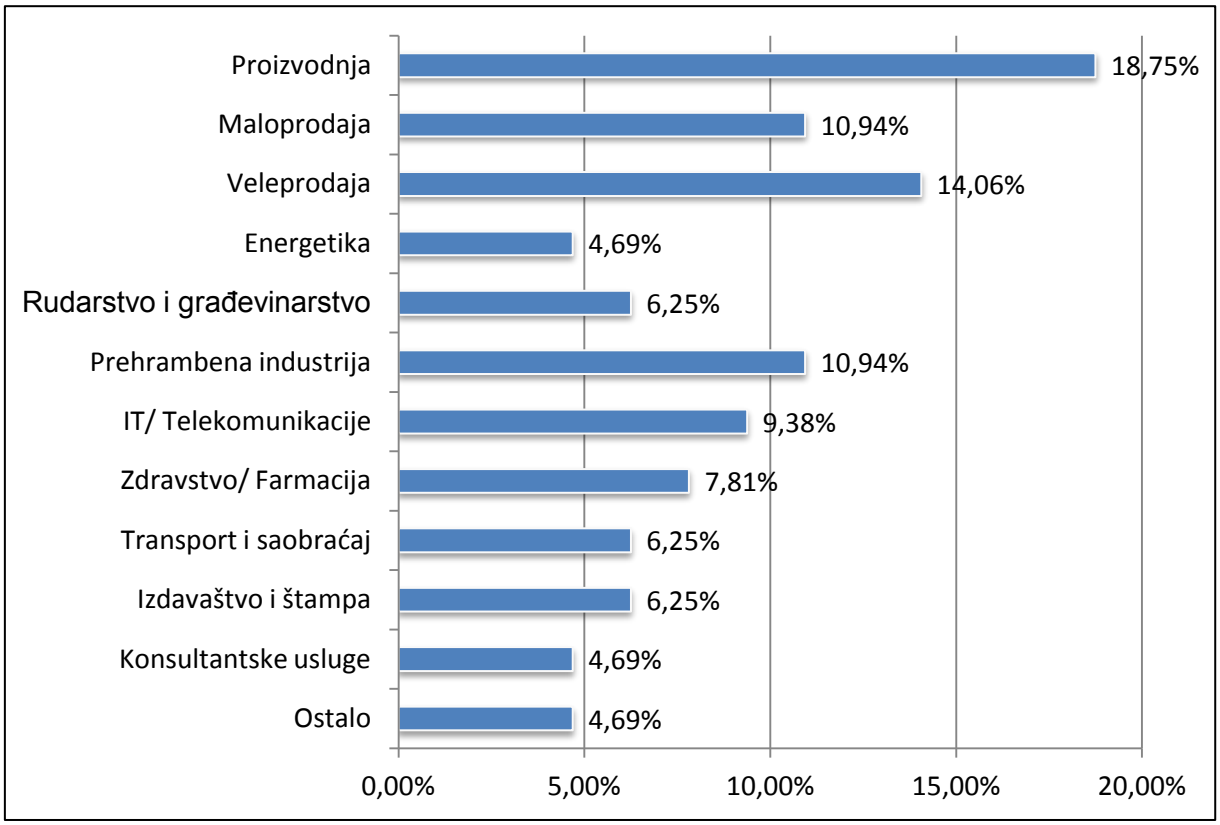
Od ukupno 183 poslate ankete, odgovor je dobijen na 96 anketa. Od tog broja, 5 anketa nije uključeno u analizu jer su ispitanici delimično dali odgovore na pitanja. Drugim rečima, predmet analize bio je 91 uredno popunjen upitnik, što čini stopu odgovora od 49,73%.

Struktura prihvaćenih odgovora

Prihvaćeni odgovori dobijeni su od ispitanika iz 64 kompanije, što posmatrano po kompanijama čini stopu odgovora od 58,72%. Od 91 prihvaćenog upitnika, 48 upitnika ili 52,75% dobijeno je od ispitanika I grupe, dok je 43 upitnika ili 47,25% dobijeno od ispitanika II grupe. Navedeni odnos dobijenih odgovora od 52,75% prema 47,25% od strane ispitanika I grupe naspram ispitanika II grupe je blizu odnosa 50% prema 50%. Takav odnos između IT i biznis ispitanika doprineo je relevantnosti zaključaka do kojih se došlo istraživanjem.

Dodatno, 67,19% ispitanika bili su članovi izvršnog rukovodstva što je takođe doprinelo relevantnosti zaključaka.

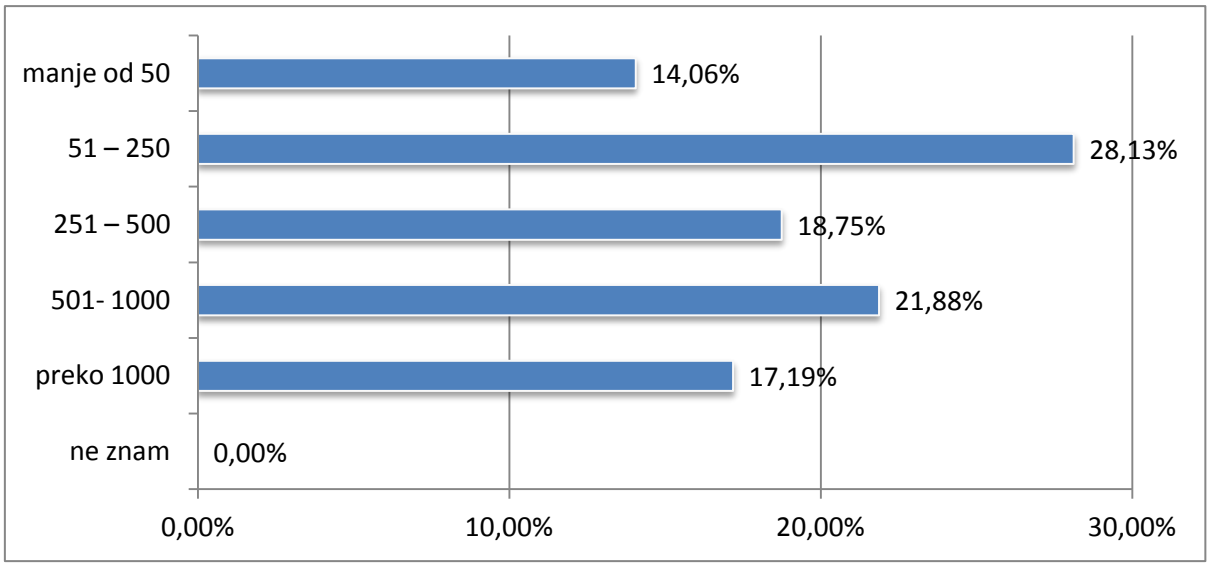
Na grafiku (slika 26) je prikazana struktura odgovora po oblastima poslovanja kompanija u kojima su ispitanici zaposleni.



Slika 26 - Struktura odgovora po oblastima poslovanja kompanija u kojima su ispitanici zaposleni

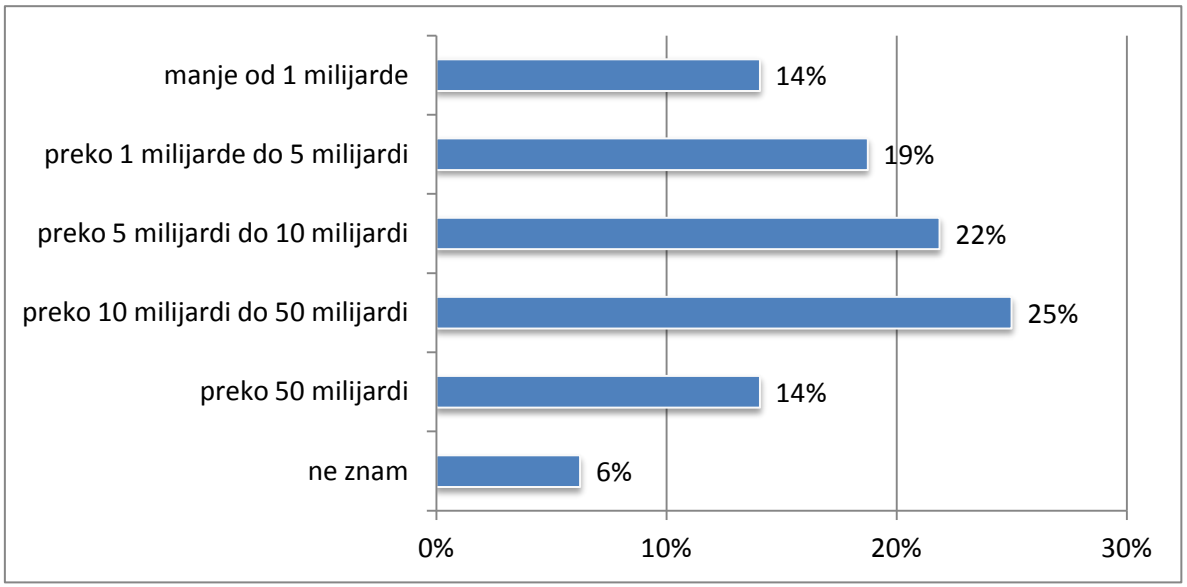
Neke od kompanija aktivne su u više oblasti poslovanja, pa je zbir procenata dobijenih odgovora veći od 100%. Najviše kompanije je bilo iz oblasti proizvodnje, veleprodaje, maloprodaje i prehrambene industrije.

Posmatrajući veličinu kompanije u kojima su ispitanici zaposleni, na osnovu faktora broj zaposlenih, najveći broj ispitanika radi u kompanijama koje zapošljavaju između 50 i 1000 zaposlenih, preko 50%. Na grafiku broj 27 prikazana je struktura odgovora po većini kompanija, na osnovu broja zaposlenih.



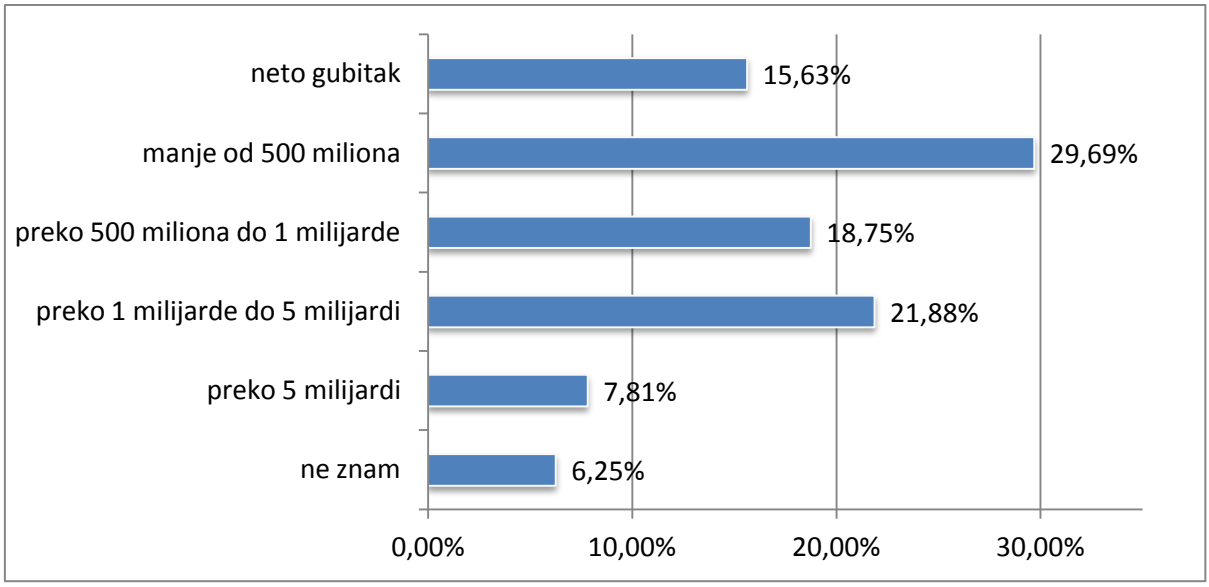
Slika 27- Struktura odgovora po veličini kompanija (posmatrano po broju zaposlenih)

Grafik broj 28 prikazuju strukturu odgovora ispitanika na osnovu kriterijuma prihodi kompanije u kojima su zaposleni. Najveći broj kompanija je ostvario prihod preko 5 milijardi u posmatranom periodu.



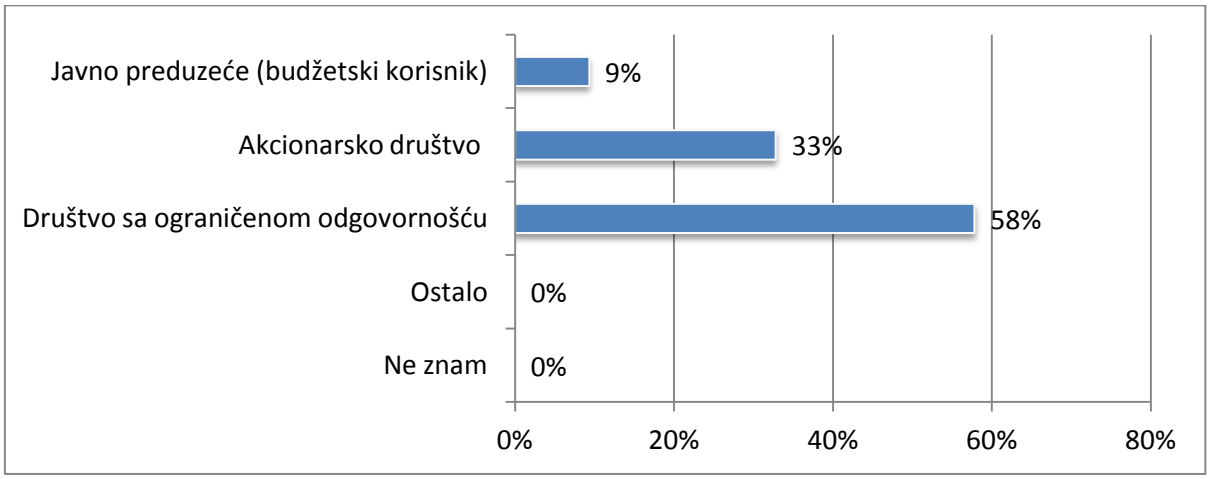
Slika 28 - Struktura odgovora po prihodima kompanija u kojima su ispitanici zaposleni

Posmatrajući neto finansijski rezultat kompanija u posmatranom periodu preko 45% kompanija je zabeležio neto gubitak ili finansijski rezultati manji od 500 miliona dinara. Samo 8% kompanija ima zabeležen neto finansijski rezultati veći od 5 milijardi dinara. Slika 29 prikazuje detaljnu struktura odgovora po neto finansijskom rezultatu kompanija.



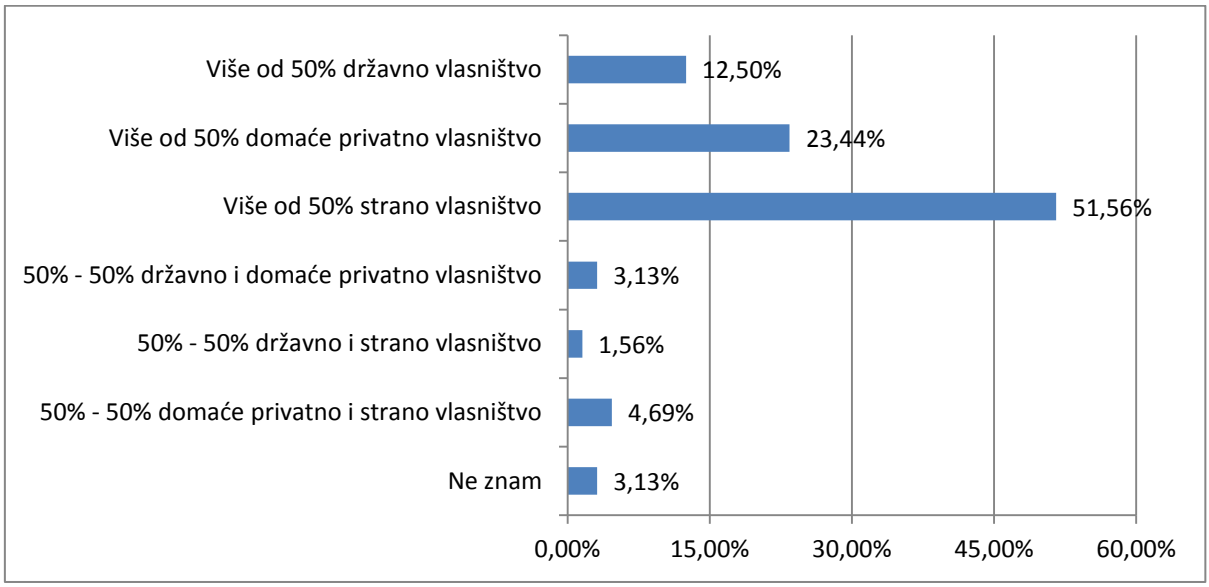
Slika 29 - Struktura odgovora po neto finansijskom rezultatu kompanija u kojima su ispitanici zaposleni

Najveći broj posmatranih kompanija su društva sa ograničenom odgovornošću 58% sa više od 50% stranog vlasništva u vlasničkoj strukturi. Slika 30 prikazuje struktura odgovora po tipu kompanija u kojima su ispitanici zaposleni.



Slika 30 - Struktura odgovora po tipu kompanija u kojima su ispitanici zaposleni

Grafik 31 prikazuje strukturu odgovora po vlasničkoj strukturi kompanija u kojima su ispitanici zaposleni.



Slika 31- Struktura odgovora po vlasničkoj strukturi kompanija u kojima su ispitanici zaposlenih

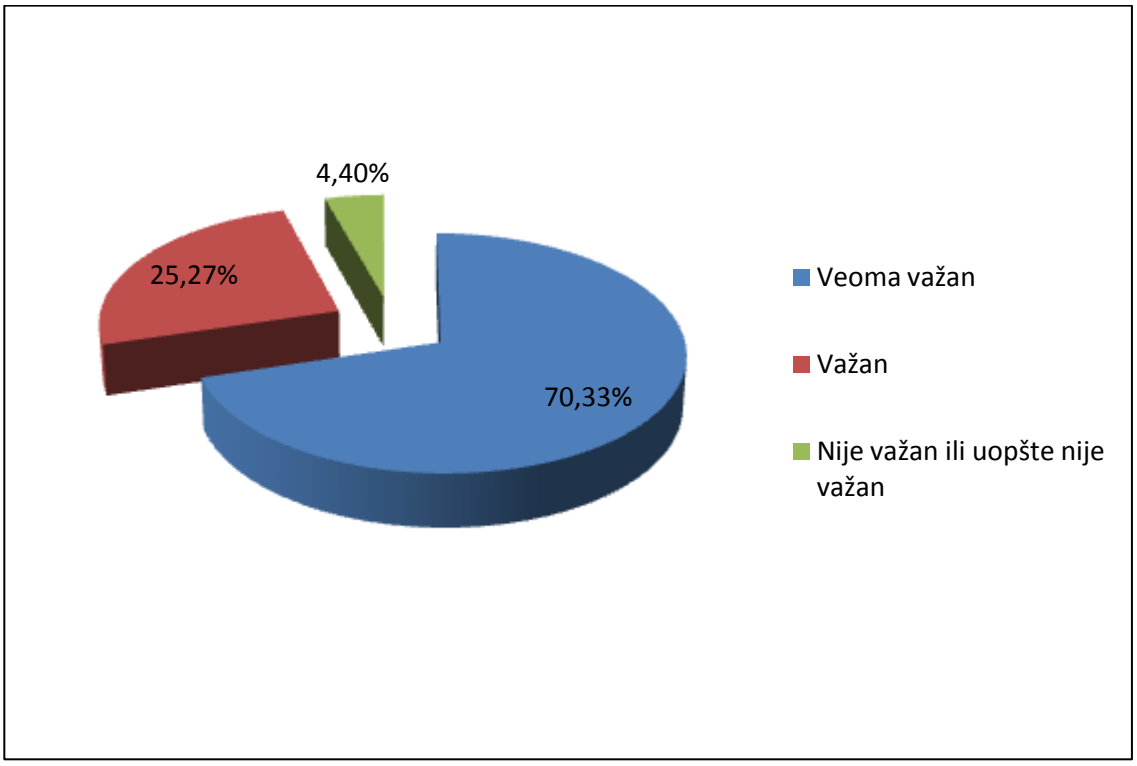
Kao što je prikazano na prethodnihpet grafika, odgovorima su u dovoljnoj meri pokrivene kompanije različith oblasti poslovanja, svih veličina (posmatrano po broju zaposlenih), različite visine prihoda, neto finansijskog rezultata odnosno nivoa efektivnosti i efikasnosti poslovanja, različitog tipa i vlasničke strukture. Takva struktura odgovora omogućila je realno sagledavanje stanja i doprinela relevantnosti zaključaka o predmetu istraživanja.

2. ANALIZA I REZULTATI ISTRAŽIVANJA

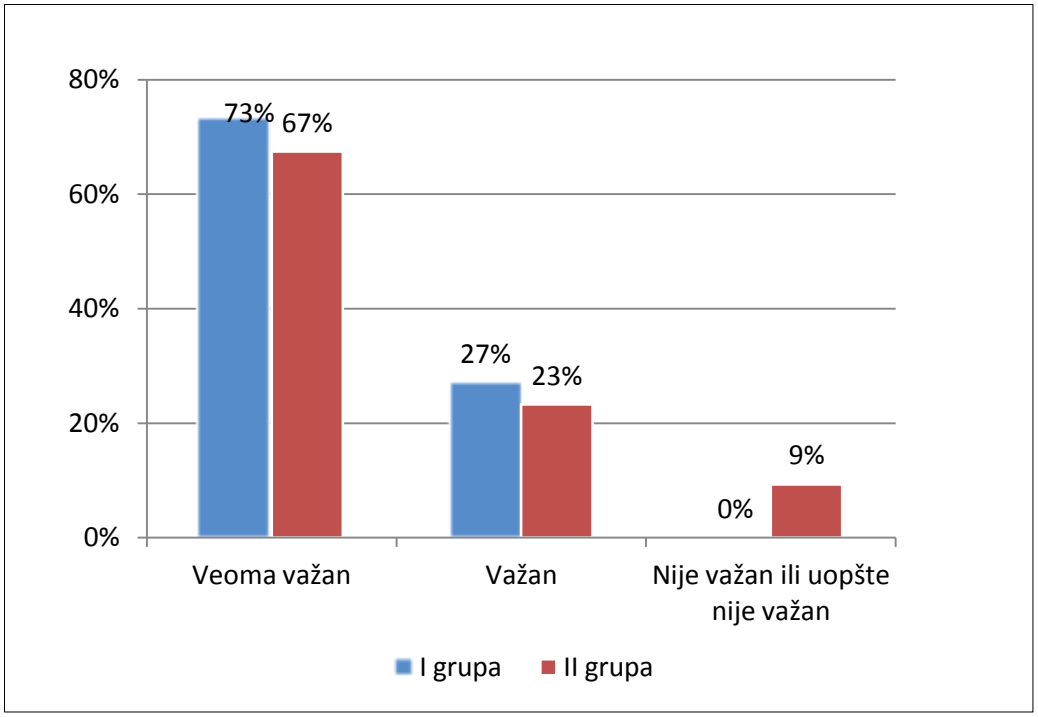
Značaj i uloga IT-a u kompaniji

2.1 Značaj IT-a za uspešno ostvarenje celokupne poslovne strategije

Kao što je prikazano na grafiku 32, većina ispitanika smatra da je IT veoma važan (70,33%) ili važan (25,27%) za ostvarenje celokupne poslovne strategije. Pri tome nisu značajna odstupanja u odgovorima između ispitanika I i II grupe (grafik 33): 72,92% ispitanika I grupe u odnosu na 67,44% ispitanika II grupe smatra da je IT veoma važan, dok 27,08% ispitanika I grupe u odnosu na 23,26% ispitanika II grupe smatra da je IT važan. To govori da je strateški značaj IT-a u savremenom poslovanju i razvoju poslovanja široko prepoznat u kompanijama u Republici Srbiji.



Slika 32- Značaj IT-a za uspešno ostvarenje celokupne poslovne strategije



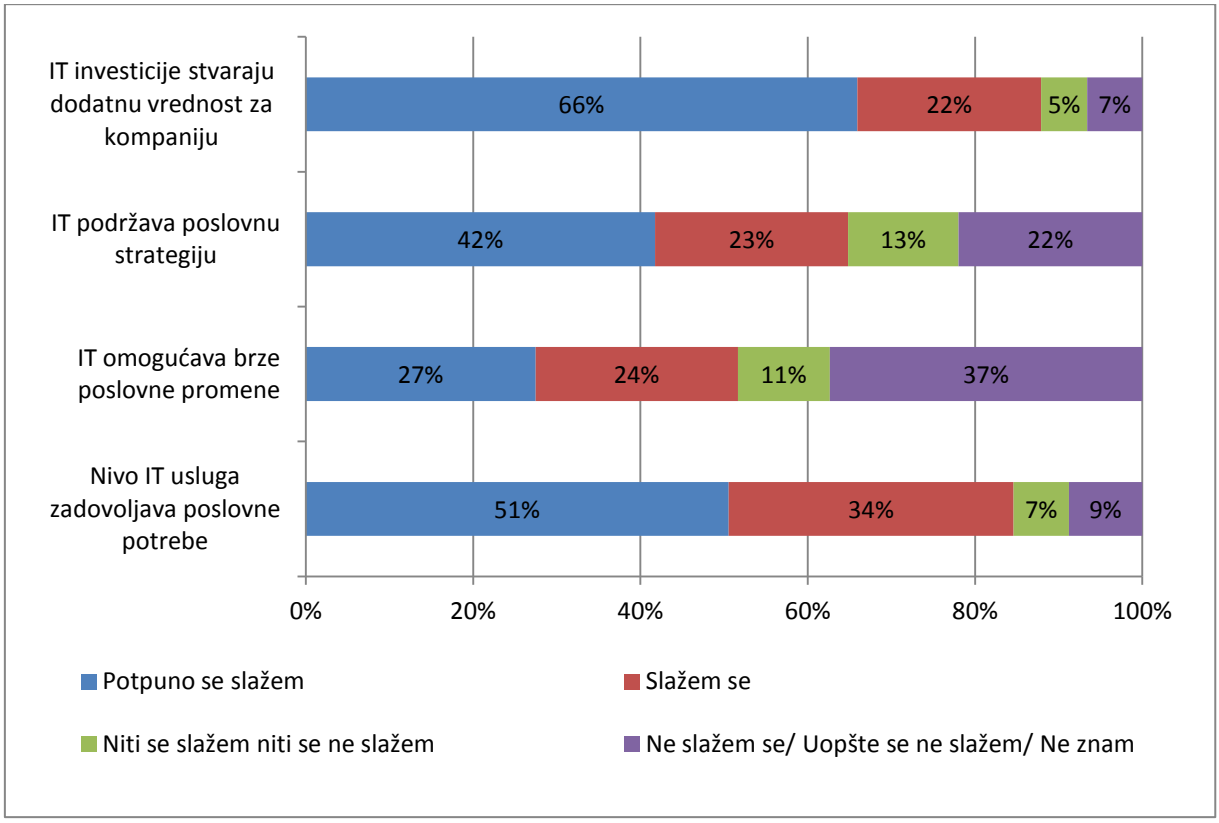
Slika 33- Značaj IT-a za uspešno ostvarenje celokupne poslovne strategije

Dodatno, analiza rezultata istraživanja pokazuje da je verovatnije da se IT smatra kao veoma važan ili važan za ostvarenje poslovne strategije kod kompanija čiji su ispitanici naveli da IT ima proaktivnu ulogu (pomaže biznisu da inovira i postigne strateške ciljeve) u odnosu na reaktivnu ulogu (reaguje na poslovne potrebe; IT je tehnički fokusiran da održava okruženje aktivnim i dostupnim). Navedeno je prikazano na slici 38.

2.2 Doprinos IT-a poslovanju

Rezultati istraživanja pokazuju da je doprinos IT-a poslovanju široko prepoznat. Prema mišljenju ispitanika, taj doprinos se najviše ogleda u stvaranju dodatne vrednosti za kompaniju putem IT investicija, što je najveća dimenzija na grafiku iznad. Sa druge strane, omogućavanje brzih poslovnih promena od strane IT-a je najmanja dimenzija na grafiku iznad. Ispitanici navode da je nemogućnost omogućavanja brzih poslovnih promena prouzrokovana, u najvećoj meri, lošom ili zastarelom IT infrastrukturom, nedostatkom

budžeta za IT investicije, dugotrajnim procedurama nabavke (izbora i usaglašavanja ugovora sa IT konsultantima), nepreciznim zahtevima korisnika i nedovoljnim razumevanjem poslovnih potreba od strane IT-a.



Slika 34 - Doprinos IT-a poslovanju

Tabela 8 - Uporedni pregled procenata odgovora IT ispitanika i biznis ispitanika koji su odgovorili sa "potpuno se slažem" ili "slažem se" po svakoj od tvrdnji o doprinosu IT-a poslovanju

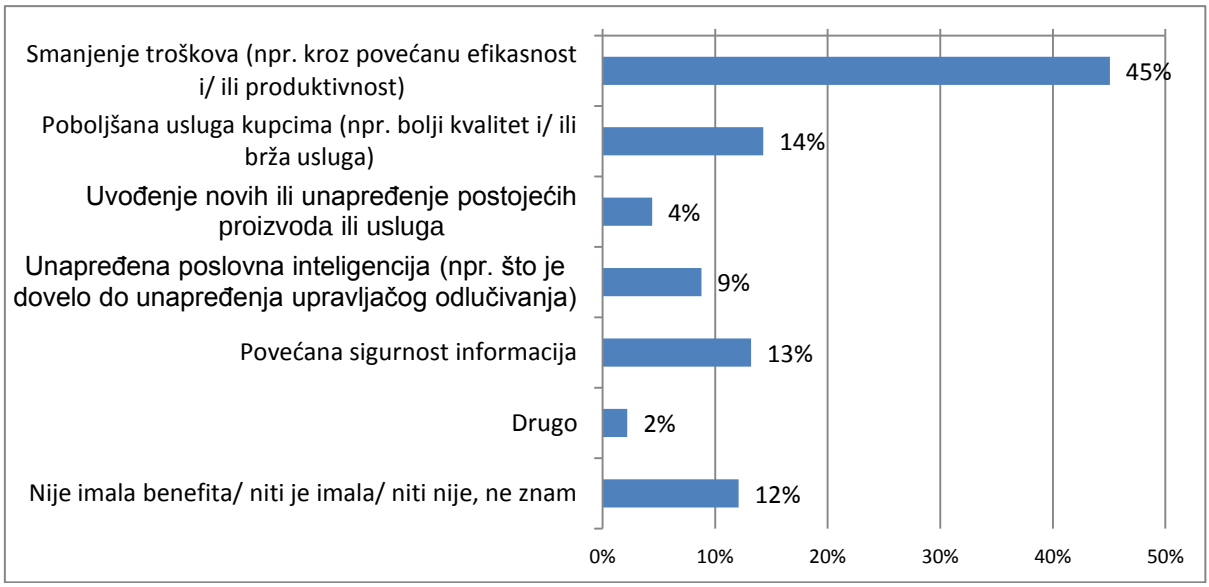
Doprinosa IT-a poslovanju	IT ispitanici	Biznis ispitanici
IT investicije stvaraju dodatnu vrednost za kompaniju	93,75%	81,40%
IT podržava poslovnu strategiju	79,17%	62,79%
IT omogućava brze poslovne promene	58,33%	44,19%
Nivo IT usluga zadovoljava poslovne potrebe	89,58%	79,07%

Kao što je prikazano u prethodnoj tabeli, kod svih tvrdnji IT ispitanici su pozitivniji od biznis ispitanika. Najveća razlika se javlja kod tvrdnje da IT podržava poslovnu strategiju, gde se skoro 80% IT ispitanika potpuno slažu ili slažu sa tvrdnjom, dok 62,79% biznis ispitanika,

odnosno 16,78% manje, ima isto mišljenje. Dodatno, analiza rezultata istraživanja pokazala je da su u preko 80 slučajeva biznis ispitanici koji smatraju da IT podržava poslovnu strategiju iz velikih i srednjih preduzeća sa većinskim stranim vlasništvom. Prema mišljenju ispitanika, razlog tome je što navedene kategorije preduzeća zbog obima poslovnih transakcija i višeg nivoa zrelosti IT korporativnog upravljanja imaju veću svest o značaju i neophodnosti razvoja IT-a i ulažu više novca u IT resurse. Dodatno, vezano za tvrdnju da IT podržava poslovne potrebe, pozitivniji stav je prisutan kod biznis ispitanika u preduzećima koja outsorsuju IT usluge u odnosu na ona koja imaju interno IT odeljenje ili zaposlenog.

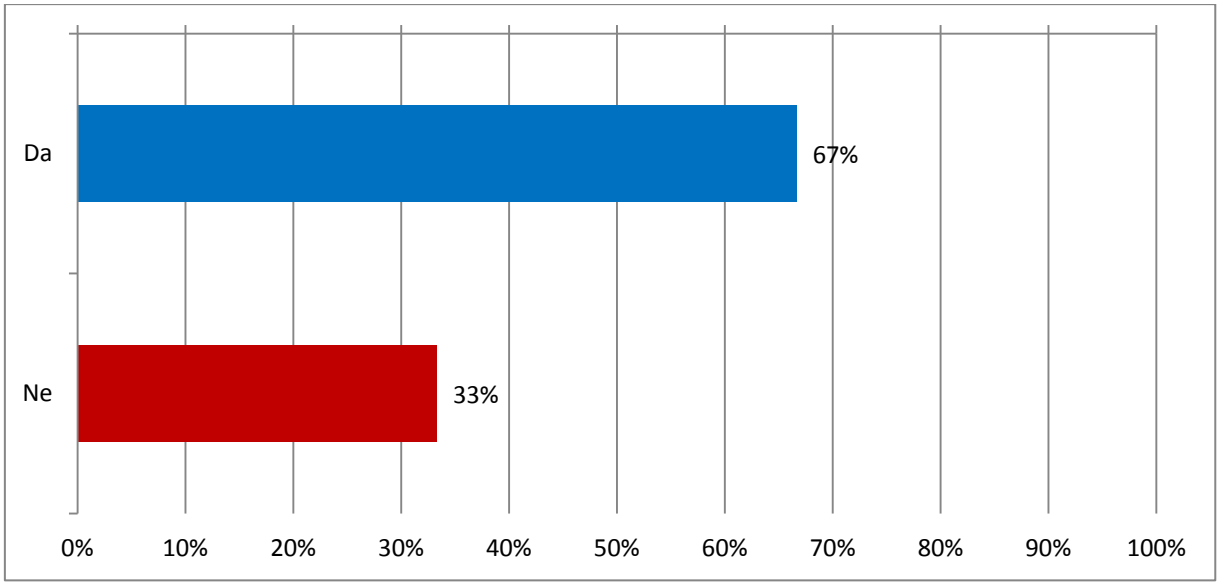
2.3 Benefiti od IT investicija

Rezultati istraživanja pokazuju da oko 87% ispitanika prepoznaje da je preduzeće imalo benefita od IT investicija (slika 35). Najviše ispitanika je kao glavni benefit prepoznalo smanjenje troškova (kroz povećanu efikasnost i/ ili produktivnost). Taj benefit je kao i benefit poboljšana usluga kupcima naročito prepoznat među velikim i srednjim preduzećima (i to naročito maloprodaja, IT/telekomunikacije), dok je među manjim preduzećim kao najznačajniji benefit prepoznata povećana sigurnost informacija. Takva struktura odgovora je u skladu sa brojem poslovnih transakcija koji ta preduzeća imaju.



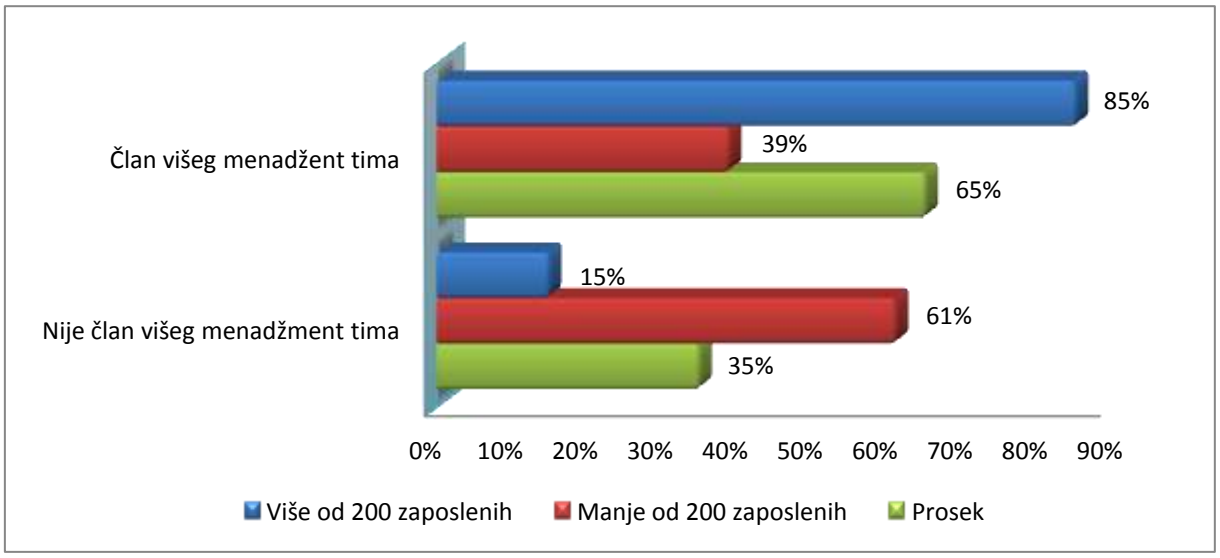
Slika 35 - Benefiti od IT investicija

Većina ispitanika (67%) smatra da su teškoće implementacije aplikacija i organizaciona kultura najčeće barijere koje su onemogućile da se ostvari pun benefit od IT investicija



Slika 36 – Ostvarenje punog benefita od IT investicija

Šestdeset procenata ispitanika je ukazalo da je u njihovim kompanijama IT direktor član starijeg menadžment tima (slika 37). Ova pozicija na starijem menadžment timu će se verovatnije desiti u preduzećima sa 200 ili više zaposlenih (85%) nego u onima sa manje od 200 zaposlenih (15%).

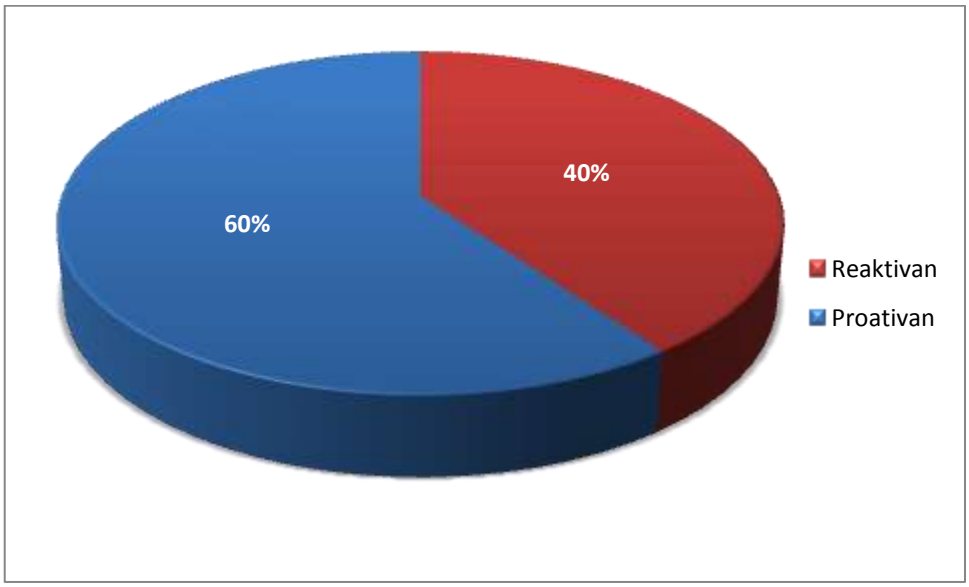


Slika 37 - IT direktor kao član višeg menadžement tima

Ovi rezultati potvrđuju veliku važnost IT-a u mnogim kompanijama. Oni ispitanici koji ukazuju da IT direktor nije član starijeg menadžment tima u njihovim kompanijama ukazuju na malu veličinu starijeg menadžment tima kao glavni razlog za to (53 %). Ovo se poklapa sa otkrićem da je češće u malim kompanijama da IT direktor ne bude član starijeg menadžment tima. Drugi razlozi često uključuju da je IT potporna funkcija i da je IT adekvatno predstavljen od strane drugog člana starijeg izvršnog time (28% i 23% za svaku opciju).

2.4 Reaktivna ili proaktivna uloga IT

IT ima reaktivnu ulogu u organizaciji kada IT odgovora na poslovanje kada poslovanje ima formalan zahtev. U reaktivnoj ulozi IT je obično fokusiran i koncentriše se na održanje postojećih sistema operativnim i dostupnim. IT ima proaktivnu ulogu u organizaciji kada je IT partner poslovanja i preuzima inicijativu kako bi pomogao u IT inovaciji i postizanju strateških ciljeva. Na osnovu odgovora ispitanikamože se zaključiti da proaktivnu ulogu IT ima u 60% kompanija, a reaktivnu u 40%.



Slika 38 - Reaktivna i proaktivna uloga IT

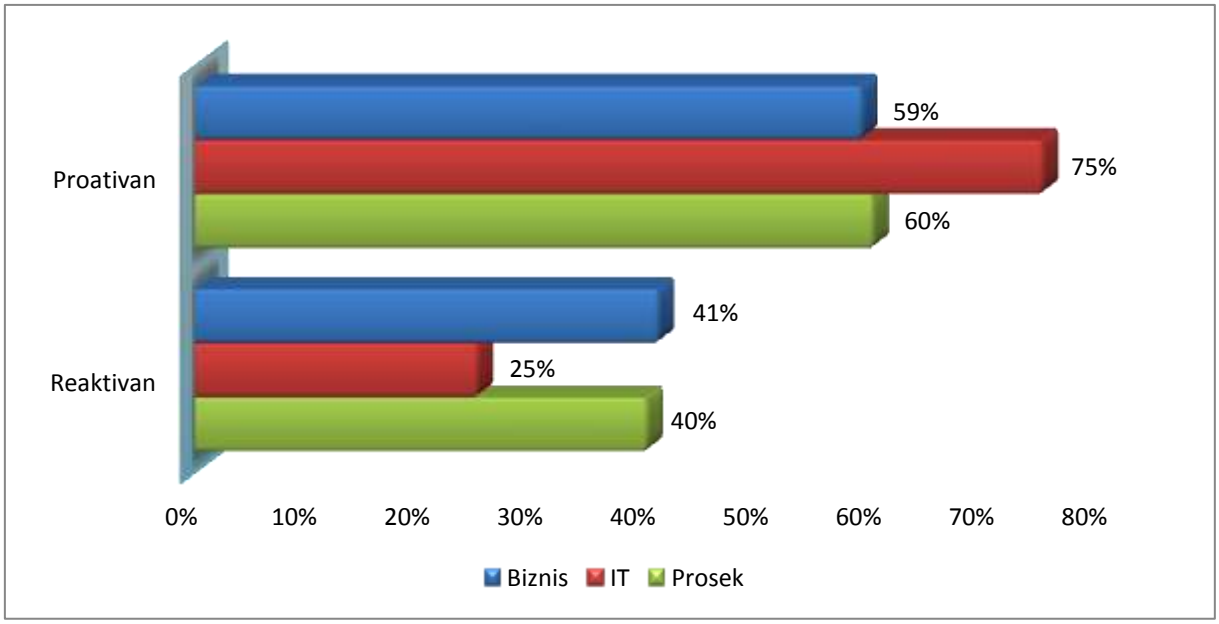
Odgovori učesnika u vezi uloge IT u kompaniji (proaktivna i reaktivna) su poređeni sa njihovim odgovorima na pitanje u vezi članstva njihovog IT direktora u starijem menadžment

timu. Jasna korelacija je nađena između ta dva pitanja. Od svih ispitanika koji su spomenuli da IT ima proaktivnu ulogu u njihovim organizacijama, 80% je takođe napomenulo da je IT direktor član višeg menadžment tima. Suprotno je takođe tačno: reaktivna uloga teži da bude povezana sa IT direktorom koji nije član višeg menadžment tima.

2.5 Uloga IT u Organizaciji

Od ispitanika je zatraženo da okarakterišu trenutnu ulogu IT u njihovim kompanijama ili kao proaktivnu ili kao reaktivnu. Većina ispitanika je opisala trenutnu ulogu kao proaktivnu (60% nasuprot 40%), kao što je prikazano na slici 39. Međutim, učesnici istraživanja koji su povezani sa IT i oni koji nisu direktno povezani se ne slažu oko uloge koju ima IT. Osobe povezane sa IT će verovatnije opisati trenutnu ulogu IT kao proaktivnu (75% od osoba povezanih sa IT, nasuprot 25%), dok osobe koje nisu direktno povezane sa IT vide ulogu IT kao reaktivnu (59% nasuprot 41% kod IT ispitanika).

Ovo ukazuje na značaj uticaja poboljšanje komunikacije i transparentnosti između poslovanja i IT. Dobra komunikacija omogućava i osigurava da IT može da ima proaktivniju ulogu u kompanijama.

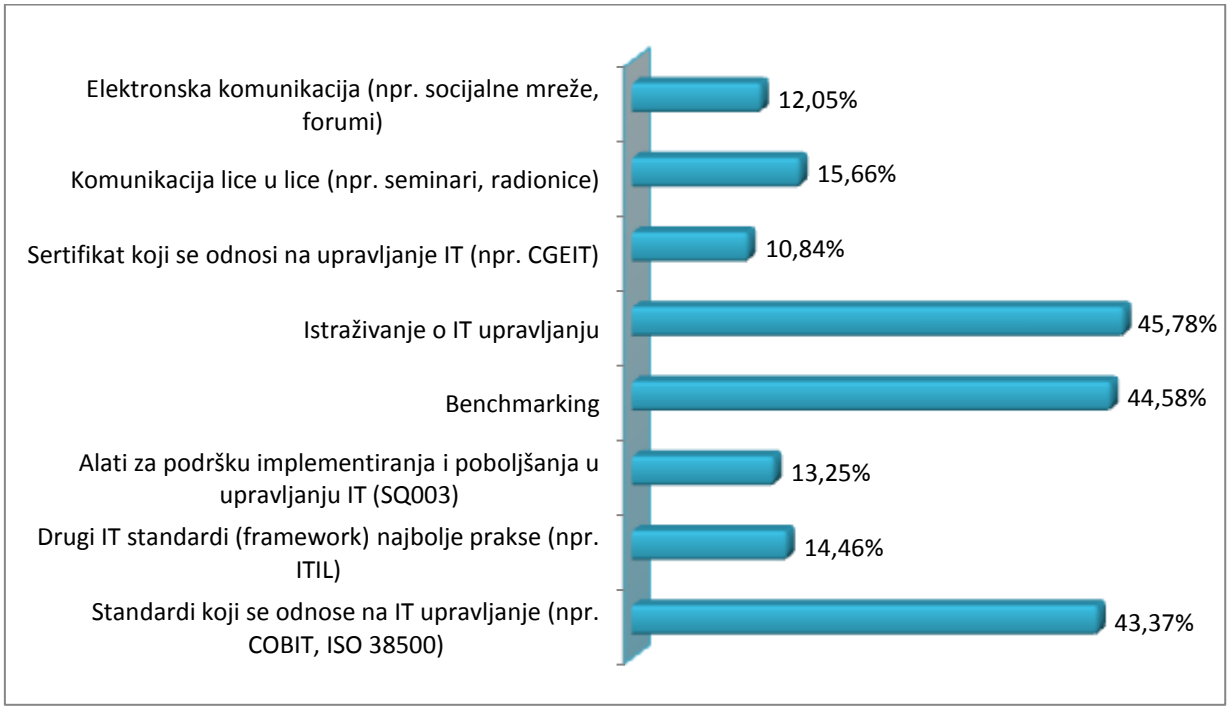


Slika 39 - Korelacija između uloge IT i osoba povezanih sa IT

2.6 Efikasno IT upravljanje

Prema mišljenju ispitanika, za efikasno IT upravljanje najvažniji su standardi koji se odnose na IT upravljanje 43%, benchmarking 45% i feedback od strane korisnika 46%. Učesnici su imali mogućnost da odaberu više odgovora i oni su prikazani na slici 40.

Prema njihovom mišljenju najmanje značajno za efikasno IT upravljanje su sertifikati koji se odnose na upravljanje i elektronska komunikacija putem socijalnih mreža i foruma.

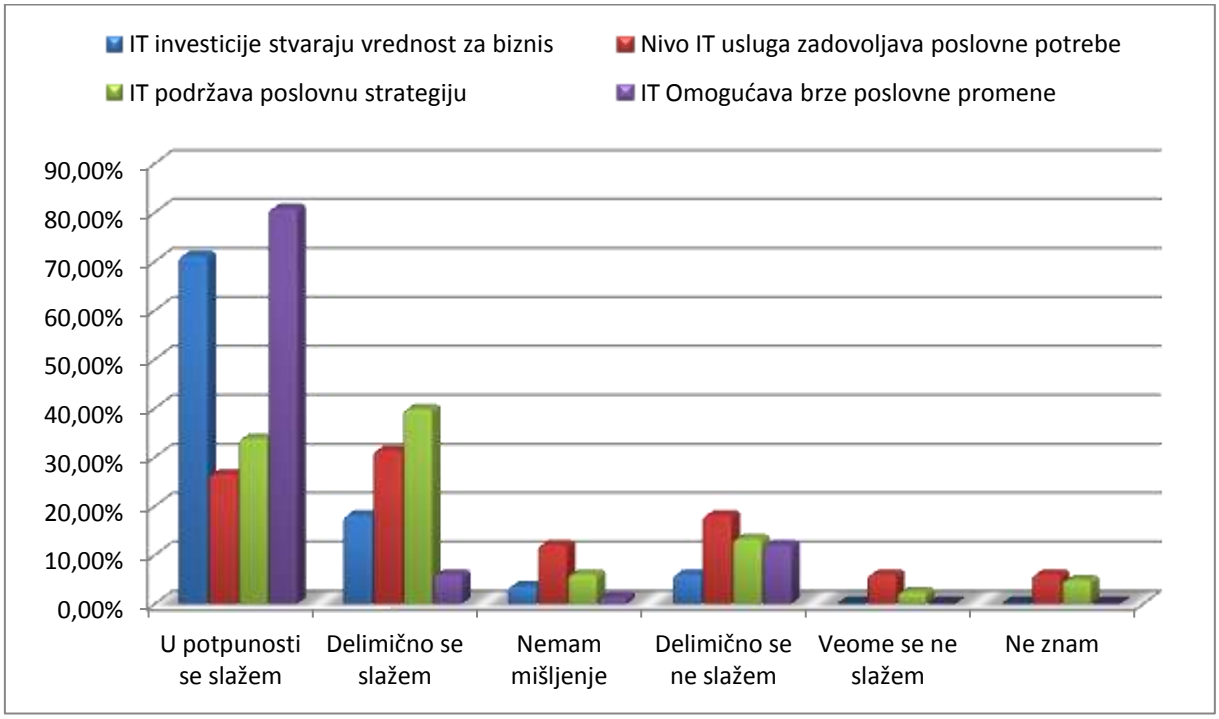


Slika 40 - Efikasno IT upravljanje

2.7 Doprinosi IT poslovanju

Istraživanjima je utvrđeno da je doprinos IT unapređenju poslovanja prepoznat kao prednost i investicija kojom se stvara nova poslovna vrednost. IT je obično shvaćen i viđen kao veliki doprinosni poslovanju, kako što je ukazano na slici 41. Tvrdnja da IT investicije stvaraju vrednost za biznis je u potpunosti podržana od strane 71% ispitanika, a 80% ispitanika je u potpunosti saglasno da IT omogućava brze poslovne promene. Nemogućnost brzih poslovnih promena često može biti pripisana problemima i sporim promenama kompanijske IT

infrastrukture. To podstiče mnoge kompanije da se bave lansiranjem inicijativa i permanentnom afirmacijom korporativnog upravljanja informacionim tehnologijama.



Slika 41 - Doprinos IT-a poslovanju

U tabeli 9. je prikazana kompletna struktura odgovora. U većini dimenzija, IT ispitanici su obično pozitivniji od njhovih kolega iz domena biznisa. Najupečatljivija razlika se može videti za tvrdnju "IT podržava poslovnu strategiju" gde oko 90% IT ispitanika se u potpunosti ili delimično slaže sa izjavom, dok se mnogo manje (75%) poslovnih ispitanika drži istog stanovišta.

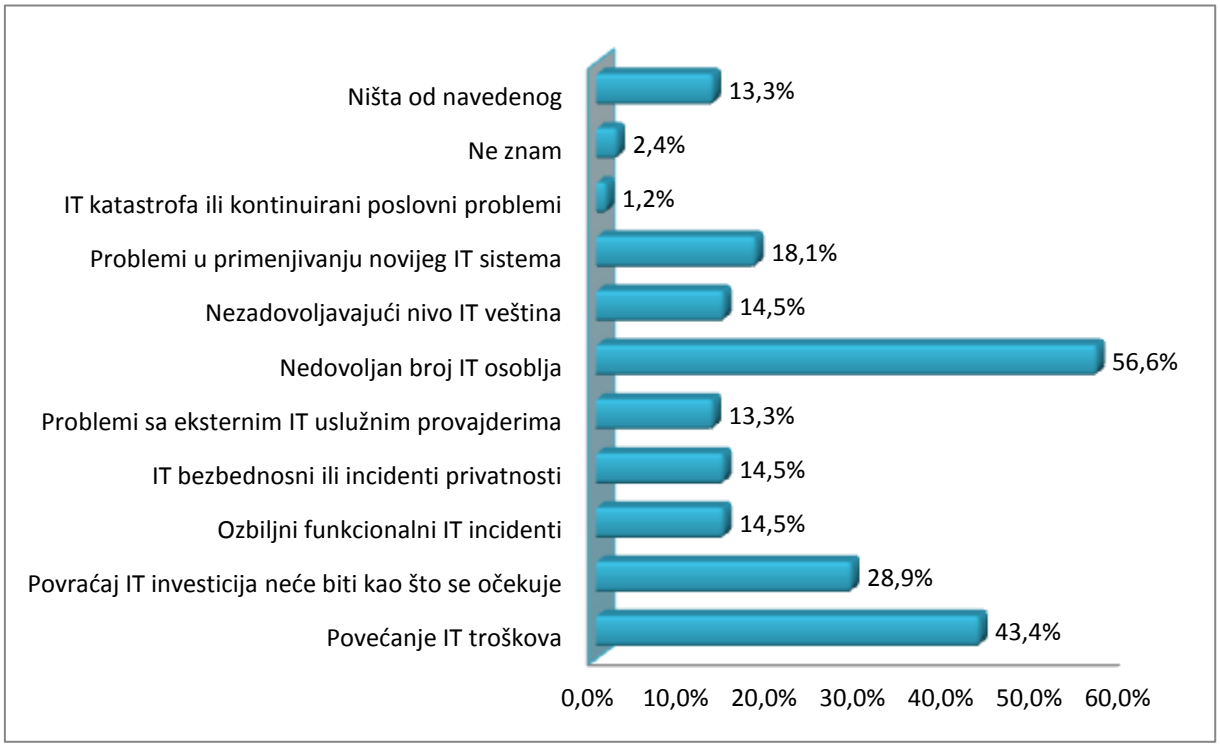
Takođe je interesantno napomenuti da kod pitanja vezanog za nivo IT usluga koji zadovoljava i uspunjava poslovne potrebe, pozitivniji pogled je reflektovan među kompanijama koja rade outsorcing IT usluge nasuprot onih koja se time ne bave.

Tabela 9 - Doprinos IT-a poslovanju

	U potpunosti se slažem	Delimičmno se slažem	Nemam mišljenje	Delimično se ne slažem	Veome se ne slažem
IT investicije stvaraju vrednost za biznis	71,08 %	18,07%	3,61%	6,02%	0%
Nivo IT usluga zadovoljava poslovne potrebe	26,51%	31,33%	12,05%	18,07%	6,02%
IT podržava biznis strategiju	33,73%	39,76%	6,02%	13,25%	4,82%
IT omogućava brze poslovne promene	80,72%	6,02%	1,20%	12,05%	0%

2.8 Povezani problemi sa IT nastali u 2012. i 2013. godini

Povećanje IT troškova i nedovoljan broj IT osoblja su bili glavni problem koji su povezani sa IT sa kojim su se susretali ispitanici proteklih 12 meseci. Povećanje IT troškova je spomenuto od strane četiri od 10 ispitanika kao posledica naglašavanja na troškove tokom globalne ekonomske krize.



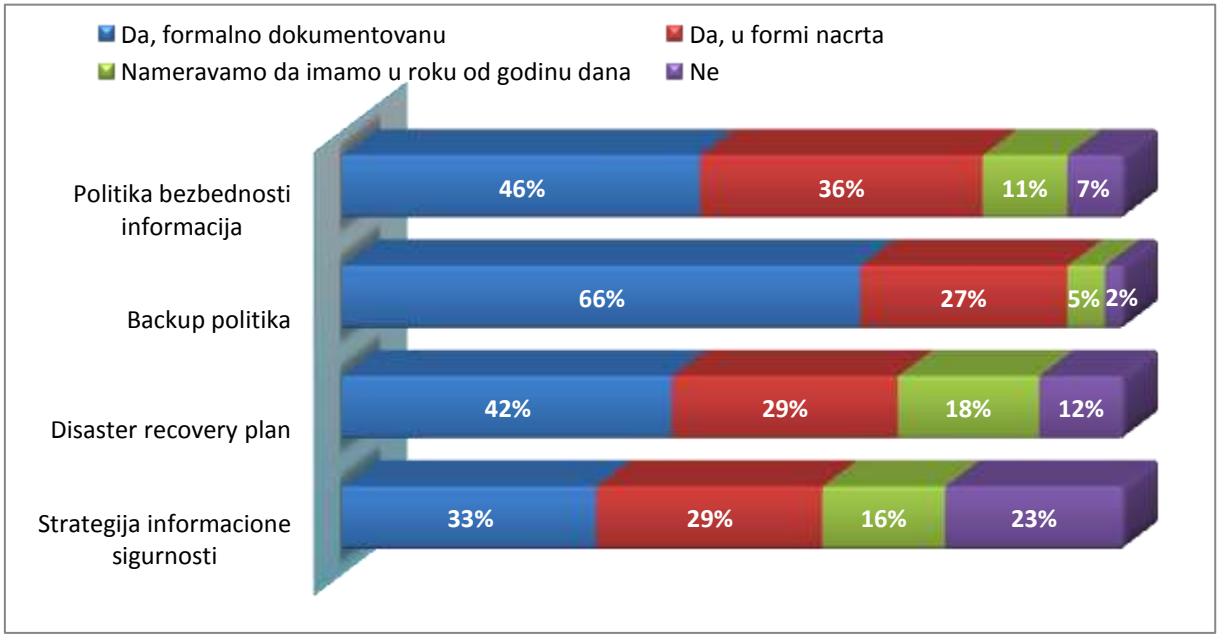
Slika 42 - Problemi povezani sa IT nastali u proteklih 12 meseci

Drugi relevantni problemi uključuju nedovoljne IT sposobnosti i veštine zaposlenih (moguće, ali ne mora da znači, da je povezano sa nedovoljnim brojem IT osoblja), poteškoće prilikom implementacije novih IT sistema i problema sa eksternim IT provajderima usluga (Slika 42). Poređenjem ovih odgovora na velike planirane inicijative, postoje neke jasne veze između određenih problema i inicijativa. Na primer, inicijative za smanjenje IT troškova su odgovor na rastuće IT troškove i velike IT sistemske implementacije.

Analiziranje ovih IT problema u vezi stanovišta kompanija o IT outsourcingu otkriva da outsourcing može delimično da pomogne sa nedovoljnim brojem IT osoblja. To je spomenuto kao problem od strane 28% ispitanika koji nisu za outsoucing nasuprot 12% onih rade outsourcing nekih IT usluga. Sa druge strane, problemi sa implementiranjem novih IT sistema su spomenuti od strane samo 5% ispitanika koje ne rade outsourcing.

2.9 Bezbednosne politike i procedure

Odgovori na pitanje da li organizacija ima dokumentovanu neku od sledećih strategija, planova ili politika prikazani su na slici 43.



Slika 43 - Bezbednosne politike i procedure

Najveći broj kompanija 93% ima backup procedure formalno dokumentovane 66% ili u formi nacrta 27%. Samo 7% kompanija nema definisane backup politike.

Tabela 10 - Bezbednosne politike i procedure

	Da, formalno dokumentovanu ili u formi nacrta	Ne ili nameravamo da imamo u roku od godinu dana
Politika bezbednosti informacija	82%	18%
Backup politika	93%	7%
Disaster recovery plan	71%	29%
Strategija informacione sigurnosti	62%	38%

Zabrinjavajuća je činjenica da 38% kompanija nije još usvojilo strategiju informacione sigurnosti i da je ista u procesu kreiranja.

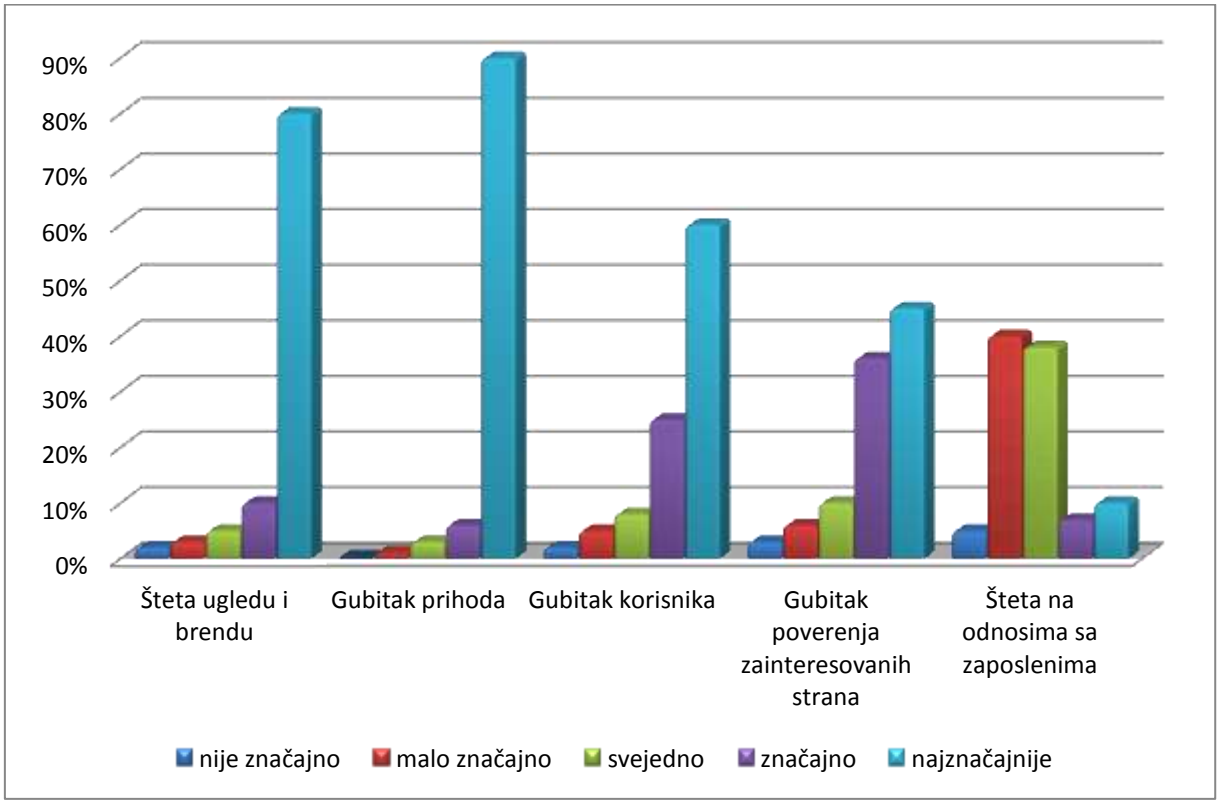
2.10 Uticaj gubitka ili krađe informacija

Uticak gubitka ili krađe informacije i značaj njihovih posledica prikazane su u tabeli 11.

Tabela 11 - Uticaj gubitka ili krađe informacije

	Nije značajno	Malo značajno	Svejedno	Značajno	Najznačajnije
Šteta ugledu i brendu	2%	3%	5%	10%	**80%**
Gubitak prihoda	0%	1%	3%	6%	**90%**
Gubitak korisnika	2%	5%	8%	25%	**60%**
Gubitak poverenja zainteresovanih strana	3%	6%	10%	36%	**45%**
Šteta na odnosima sa zaposlenima	5%	**40%**	38%	7%	10%

Rezultati istraživanja pokazuju da najveći broj kompanija ispoljava strah od gubitka prihoda (90%) koji nastaje kao posledica krađe informacija. Takođe se smatra da, iz istog razloga, šteta po ugled i brend kompanije može da bude do 80%.



Slika 44 - Značaj štete u slučaju gubitka ili krađe informacije

Šteta na odnosima sa zaposlenima im je najmanje značajna i prema istraživanju iznosi 10%.

2.11 Upotreba IT tehnologija

Nadgledanje sadržaja i filtriranje internet saobraćaja zastupljeno je kod preko 90% kompanija što je u vezi sa korišćenjem interneta i Wireless konekcija. Smanjenje troškova je uticalo na povećanje korišćenje serverske virtuelizacije 89% i VOIP komunikacije 25%.

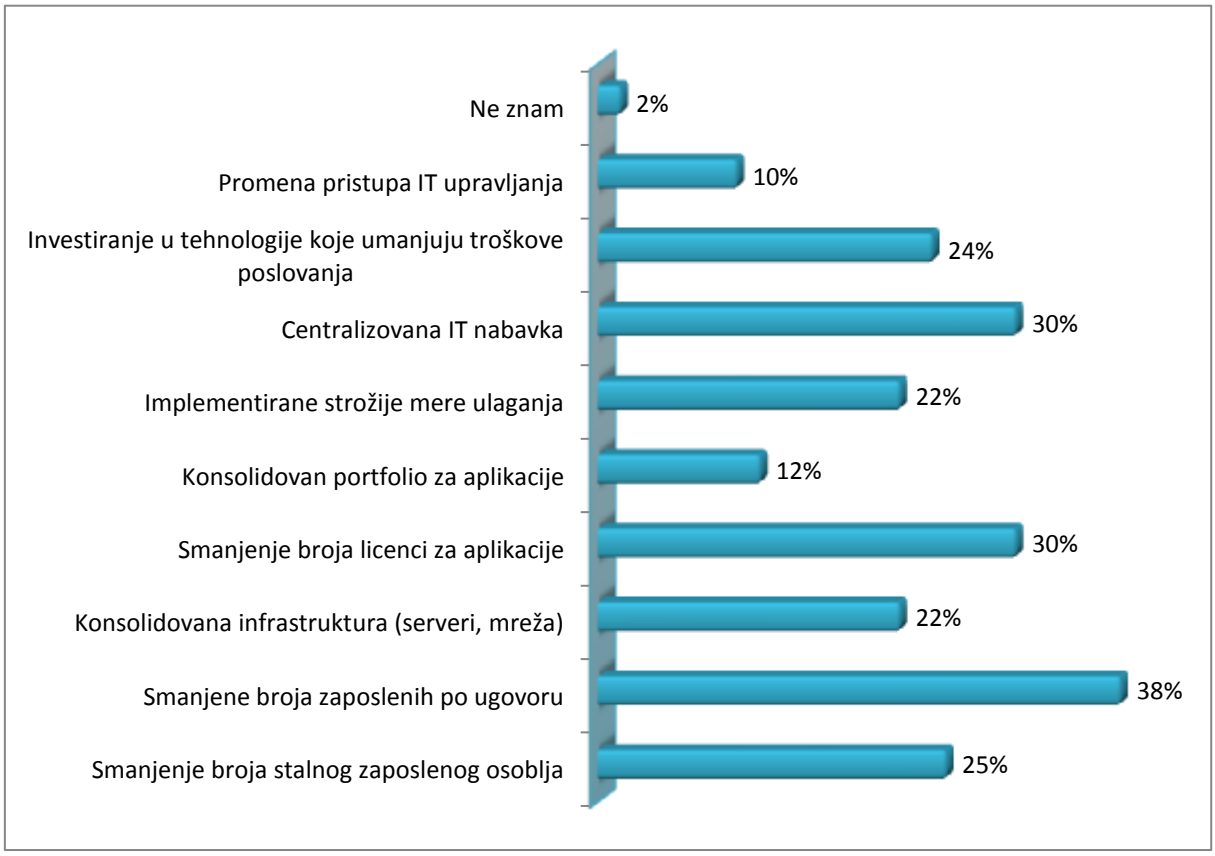
Slabo je zastupljeno šifrovanje podataka na desktop i laptop računarima, upotreba biometrije, RFID i PKI infrastrukture ispod 20%. Upotreba tehnologija koje su povezane sa internetom je stalnom porastu.

Tabela 12 - Upotreba IT tehnologija

	Trenutno koristimo	Planiramo u narednih 12 meseci	Još uvek razmišljamo
Nagledanje sadržaja i filtriranje	92%	5%	3%
Serverska virtuelizacija	89%	9%	2%
Wireless	85%	12%	3%
VOIP (Voice over IP)	25%	35%	30%
Poboljšana autentifikacija (802.1x, tokeni...)	25%	26%	49%
Šifrovanje podataka na laptop računarima	15%	3%	82%
Šifrovanje podataka na desktop računarima	10%	9%	81%
Šifrovanje prenosivih medija	10%	11%	79%
Radio Frequency Identifiers (RFID)	4%	6%	90%
PKI infrastruktura	3%	2%	95%
Šifrovanje email poruka	0%	3%	97%
Biometrija	0%	1%	99%

2.12 Inicijative implementirane kao odgovor na ekonomsku krizu

Smanjenje broja zaposlenog osoblja, centralizovana nabavka, smanjenje broja licenci za aplikacije i konsolidacija infrastrukture su bile glavne inicijative koje su učesnici istraživanja odabrali kako bi se borili sa ekonomskom krizom u protekla dve godine (slika 45). Skoro četvrtina ispitanika je takođe investirala u tehnologije koje mogu da smanje procesne i poslovne troškove.



Slika 45 - Implementirane inicijative kao odgovor na krizu

ZAKLJUČAK

ZAKLJUČNA RAZMATRANJA

Revizija informacionih sistema je u kratkom vremenskom periodu prošla kroz dinamičan razvojni put. Izvorno ona je bila podrška reviziji finansijskih izveštaja. Danas, revizija informacionih sistema sve češće predstavlja nezaobilaznu analitičku kariku u procesu korporativnog upravljanja informacionom tehnologijom i "most" između menadžmenta i informacione tehnologije. Takođe predstavlja važnu komponentu koncepta korporativnog upravljanja informacionom tehnologijom. Pomoću nje se ocenjuje da li informaciona tehnologija deluju u skladu sa poslovnim ciljevima, u kojoj meri delotvorno i svrsishodno podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacionog sistema na raznim hijerarhijskim nivoima.

Finalni rezultat tih postupaka je izveštaj revizora informacionih sistema, koji se prema područjima analize, zasnovane na Cobit metodologiji, sastoji od sledećih koraka:

- analiza stanja (zrelosti) primene informacionih sistema i tehnologija u poslovanju prema posmatranim područjima;
- procena poslovnih rizika koji proizlaze iz zatečenog stanja;
- preporuke menadžmentu za poboljšanje tog stanja

Ključna otkrića do kojih se došlo na osnovu sprovedenog istraživanja uključuju sledeće zaključke:

- IT je smatran kao bitan ili veoma bitan za isporuku celokupne poslovne strategije i vizije od strane više od 95 procenata učesnika.

- Doprinosi IT-a poslovanju su prepoznati, dok je stvaranje vrednosti od IT investicija jedan od najvažnijih dimenzija (potvrdan odgovor je dalo devet od deset učesnika).

- 66 procenata učesnika je spomenulo da je IT direktor član višeg menadžment tima, potvrđujući rastuću važnost IT u mnogim kompanijama. Ova pozicija na starijem menadžment timu će se verovatnije desiti u preduzećima sa 200 ili više zaposlenih (85%) nego u onima sa manje od 200 zaposlenih (15%).

- Više učesnika opisuje trenutnu ulogu IT u njihovim kompanijama kao proaktivnu više nego reaktivnu (60 procenata nasuprot 40 procenta), ali je procenat sa proaktivnom ulogom je veći (68 procenta) u kompanijama gde su neke IT usluge autsorsovane u poređenju sa onima koje nisu autsorsovane.

- Odgovori učesnika u vezi uloge IT u kompaniji (proaktivna i reaktivna) su poređeni sa njihovim odgovorima na pitanje u vezi članstva njihovog IT direktora u starijem menadžment timu. Jasna korelacija je nađena između ta dva pitanja. Od svih ispitanika koji su spomenuli da IT ima proaktivnu ulogu u njihovim organizacijama, 80% je takođe napomenulo da je IT direktor član višeg menadžment tima. Suprotno je takođe tačno: reaktivna uloga teži da bude povezana sa IT direktorom koji nije član višeg menadžment tima.

- Glavne inicijative planirane od učesnika u sledećih 12 meseci imaju veze sa velikim sistemskim implementacijama ili nadogradnjama, IT smanjenem troškova, podacima ili informacijama.

- Povećanje IT troškova i nedovoljan broj IT osoblja su glavni problemi povezani sa IT-jem koje su osetili učesnici istraživanja u proteklih 12 meseci.

- Autsorsing je često korišćen: 65 procenata ispitanika je u potpunost autsorsovalo neke od njihovi IT aktivnosti a drugih 15 procenata korist delimičan autsorsing. Potpuni

autsorsing nekih IT aktivnost je češći i velikim kompanijama i ona u kojima se IT smatra bitan ili veoma bitan za isporuku poslovne strategije i vizije.

- Primarne inicijative implementirane u odgovor na ekonomsku krizu smanjenje broja zaposlenih, konsolidacija infrastrukture, centralizovana nabavka i smanjenje broja licenci za aplikacije

- Nadgledanje sadržaja i filtriranje internet saobraćaja zastupljeno je kod preko 90% kompanija što je u vezi sa korišćenjem interneta i Wireless konekcija. Smanjenje troškova je uticalo na povećanje korišćenje serverske virtuelizacije 89% i VOIP komunikacije 25%.

- Kompanije se najviše plaše gubitka prihoda 90 procenata kao posledice gubitke i krađe infromacije i štete po ugled i brend kompanije koje mogu pretrpeti na osnovu toga u iznosu od 80 procenata.Šteta na odnosima sa zaposlenima im je najmanje značajna i prema istraživanju iznosi 10 procenata.

- Tvrdnja da IT investicije stvaraju vrednost za biznis je u potpunosti podržana od strane 71 procenta ispitanika, a 80 procenata ispitanika je u potpunosti saglasno da IT omogućava brze poslovne promene. Nemogućnost omogućavanja brzih poslovnih promena često može biti pripisana problemima sa kompanijskom IT infrastruktorom, problem sa kojim se mnoge kompanije bave putem lansiranjem inicijativa za korporativno upravljanje informacionim tehologijama.

- U većini dimenzija, IT ispitanici su obično pozitivniji od njhovih kolega iz domena biznisa. Najupečatljivija razlika se može videti za tvrdnju "IT podržava poslovnu strategiju" gde oko 90 procenata IT ispitanika se u potpunosti ili delimično slaže sa izjavom, dok se mnogo manje (75%) poslovnih ispitanika drži istog stanovišta.

- Takođe je interesantno napomenuti da kod pitanja vezanog za nivo IT usluga koji zadovoljava i uspunjava poslovne potrebe, pozitivniji pogled je reflektovan među kompanijama koja rade outsorcing IT usluge nasuprot onih koja se ne bave autsorsingom.

- Stvaranje vrednosti u IT investicijama je jedna od najvažnijih dimenzija IT doprinosa poslovanju. Povećanje IT troškova i nedovoljan broj IT osoblja je najčešći IT povezan problem sa kojim su se susretale kompanije u proteklih 12 meseci.

- Postoji veza između pozicije direktora IT u hijerarhiji preduzeća i proaktivne prirode IT odeljenja. Celokupno, 70 procenata učesnika istraživanje je primetilo da je IT direktor član starije menadžment tima, ali ova cifra se povećava na 80 procenata za ona preduzeća gde IT ima proaktivnu ulogu.

- Efikasno IT upravljanje je prioritet kod većine kompanije - samo je šest procenata ukazalo da oni to ne smatraju bitnim.

- Najveći broj kompanija 93 procenata ima backup procedure formalno dokumentovane (66 procenata) ili u formi nacrta (27 procenata). Samo 7 procenata kompanija nema definisane backup politike.

- Najveći uočeni nedostatak u pogledu korišćenja IT za unapređenje poslovanja je u činjenici da 38 procenata kompanija nema usvojenu strategiju informacione sigurnosti ili je proces njenog donošenja u toku.

LITERATURA

SPISAK KORIŠĆENE LITERATURE

1. Beulen, E., & Ribbers, P. (2007). *Control in outsourcing relationships: governance in action*. Proceedings of the 40th Hawaii International Conference on System Sciences. Hawaii.
2. Calder, A., & Watkins, S. (2008). *A Manager's Guide to Data Security and ISO 27001 / ISO 27002.* Kogan Page.
3. Cannon, D. L. (2008). *CISA Certified Information Systems Auditor Study Guide.* Sybex.
4. Cascarino R. (2007), *Information Systems Auditing*, John Wiley & Sons Inc., USA
5. Champlain J. (2002), *Practical IT Auditing*, Warren Gorham & Lamount, USA
6. Champlain J. (2003), *Auditing Information Systems*, John Wiley & Sons Inc., USA
7. Clarke R. (2006), *Building, Managing, and Auditing Information Security,* Institute of Internal Auditors, USA
8. Coderre D. (2004), *Fraud Detection*, Ekaros Analytical Inc., Canada
9. Davis, C., Schiller, M., & Wheeler, K. (2007). *IT Auditing: Using Controls to Protect Information Assets.* McGraw-Hill Osborne Media.
10. Ernst&Young. (2009). *Ernst & Young's 2009 Global Information Security Survey.*
11. Ferraiolo D., Kuhn R., Chandramouli R. (2007), *Role-Based Access Control*, Artech House, USA

12. Garfinkel S., Spafford G. (2002), *Web Security, Privacy and Commerce*, O'Reilly & Associates, USA
13. Goldman, J.E., Christie, V.R. (2004). *Metrics based Security Assessment. In Information Security and Ethics*: Social and Organizational, IRM Press.
14. Graham L., Parker X. (2007), *Information Technology Audits*, CCH Group, USA
15. Grembergen, W. V., & Haes, S. D. (2009). *Enterprise Governance of Information Technology*. New York: Springer Science + Business Media.
16. Hunton, J.E., Bryant, S.M., Bagranoff, N.A.: (2004): *Core Concepts of Information Technology Auditing*, John Wiley &Sons Inc., SAD.
17. ISO. (2000). *ISO/IEC 17799*. Switzerland: International Organization for Standardization (ISO).
18. ISO. (2005). *ISO/IEC 27001*. Switzerland: International Organization for Standardization (ISO).
19. ISO. (2007). *ISO/IEC 27002*. Switzerland: International Organization for Standardization (ISO).
20. ITGI (2003): *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.
21. ITGI. (2007). *CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models*. Rolling Meadows, USA: IT Governance Institute.
22. ITIL. (2007). *An Introductory Overview of ITIL V3*. London: The UK Chapter of the itSMF.
23. Kaplan, R. S., Norton, D. P., (1992): The Balanced Scorecard: Measures that Drive Performance. Harvard business review, Vol 70. Jan-Feb

24. Kaplan, R.S., Norton, D.P., (1996): The Balanced Scorecard: Translating Strategy into Action, Harvard Business School Press, Boston, SAD
25. Kaufman, C., Perlman, R. and Spicier, M.,: *Network security* (Private Communication in a Public World), 2nd edition, Prentice Hall 2002.
26. Kaye D., Graham J. (2006), *Risk Management Approach to Business Continuity*, Rothstein Associates Inc., USA
27. Keele A., Mortier K., (2005), *Exam Cram 2: CISA*, Que Publishing, USA
28. Kotlica, S, (1996): *Informaciono tehnološka paradigma i ekonomski razvoj"*, Institut ekonomskih nauka, Beograd, 1996.
29. Krist M. (1999), *Standard for Auditing Computer Applications*, Auerbach, USA
30. Layton T., (2006), *Information Security: Design, Implementation, Measurement and Compliance*, Auerback Publications, USA
31. Malina, A.M. and Selto, F. H. (2001). *Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard Approach*. Journal of management accounting research
32. Mandia K., Prosise C., Pepe M. (2003), *Incident Response*, McGraw-Hill/Osborne, USA
33. McNamee David, (2003): *Risk Management & Risk Assessment*, Information System Audit and Control Association, USA
34. Microsoft (2007). *Balanced Scorecard for Information Security Introduction*, Microsoft TechNet – Security TechCenter.
35. Min, Y. W. (2009). *Understanding and Auditing IT Systems.* Peking: Lulu.
36. Natan R., (2005), *Implementing Database Security and Auditing*, Elsevier digital press, USA

37. Nolan, R. and McFarlan, F.W., (2005): Information Technology and Board of Directors, Harvard Business Review, October, 2005.
38. Oliphants A., (2004), *Auditing IT Infrastructures*, Mair International Ltd, USA, 2004
39. Panian, Z., & Spremic, M. (2007). *Korporativno upravljanje i revizija informacijskih sustava.* Zagreb: Zgombić & Partneri.
40. Peltier T. (2005), *Information Security Risk Analysis*, Auerbach, USA
41. Peltier T., Peltier J., Blackey J., (2004), *Information Security Fundamentals*, CRC Press, USA
42. Pickett S. (2006), *Audit Planning*, John Wiley & Sons Inc., USA
43. Pleskonjić, D, Đorđević, B, Maček, N, Carić, M, (2006): *Sigurnost računarskih mreža*, Viša elektrotehnička škola, Beograd, 2006.
44. Publishing, V. H. (2008). *IT Governance based on Cobit 4.1 - A Management Guide.* Van Haren Publishing.
45. Raval V., Fichadia A.,(2007), *Risks, controls, and security*, John Wiley & Sons, USA
46. Rigby, D. (2009). *Management Tools and Trends 2007*. Bain & Company Publication.
47. Rohm, H., Halbach, L. (August 2005). *Developing and Using Balanced Scorecard Performance Systems*. The Balanced Scorecard Institute.
48. Sallé, M. & Rosenthal, S. (2005), *Formulating and Implementing an HP IT Program Strategy Using COBIT and HP ITSM*, the 38th Hawaii International Conference on System Sciences;
49. Sawyer L. (2003), *Sawyer's Internal Auditing*, Institute of Internal Auditors, USA
50. Schneier, B.,(1996): *Applied cryptography*, John Willey & Sons, Inc., 1996.
51. Schwarz, A., & Hirschheim, R. (2003). An extended platform logic perspective of IT governance. *The Journal of Strategic Information Systems* , 129-166.

52. Selig, G.J. (2008), *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*, Van Haren Publishing;
53. Senft, S., & Gallegos, F. (2009). *Information Technology Control and Audit* (Third ed.). Boca Raton, USA: Taylor & Francis Group.
54. Simonsson, M., Johnson, P. and Wijkström, H. (2007): *Model-based IT Governance Maturity Assessments with COBIT*, KTH Royal Institute of Technology - Publications and Reports of School of Electrical Engineering.
55. Spremic, M. (2007). *Methods of auditing infromation systems*. Zbornik Ekonomskog fakulteta u Zagrebu
56. Stamp M. (2005), *Information Security: Principles and Practice*, John Wiley & Sons, USA
57. Stephenson P. (2000), *Investigating Computer-related Crime*, CRC Press, USA
58. Tarantino, A. (2008): *Governance, Risk and Compliance Handbook:Technology, Finance, Environmental, and International Guidance and Best Practices*, New Jersey, John Wiley & Sons Inc.;
59. The Balanced Scorecard Institute. (2008). http://www.balancedscorecard.org/
60. Toigo Jon William, (2003), *Disaster Recovery Planning*, Prentice Hall, USA
61. Turner, M.J., Oltsik, J., McKnight, J. (2008). *ISO, ITIL and COBIT triple play fosters optimal security management execution*. SC Magazine Awards 2009 - USA.
62. Van Grembergen, Guldentops, D.R., (2004): *Structures, Processes and Relational Mechanisms for IT Governance*, Idea Group
63. Van Grembergen, W. & De Haes. S. (2008), *Implementing InformationTechnology Governance: Models, Practices and Cases*, London, IGI Publishing;

64. Van Grembergen, W., (2004): *Strategies for Information Technology Governance*, Idea Group.
65. Venkatraman, N., (1999): *Valuing the IS Contribution to the Business*, Computer Sciences Corporation.
66. Von Roessing Rolf, (2002) *Auditing Business Continuity*, Rothstein Associates Inc., USA
67. Von Solms, B. (2001). *Corporate Governance and Information Security*. Computers & Security,
68. Weill, P., Ross, J.W., (2004): ITGovernance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.
69. William Stallings (2007): Network security essentials, Prentice, Third Edition, 2007.
70. Petrache, A., (2009), The collapse of ENRON, a classic case of corporate social irresponsibility, The Ninth International Conference Investments and Economic Recovery, Vol.12, Nr. 2 special/2009
71. Grembergen W.V., (2008),The Balanced Scorecard and IT Governance, IT Governance Institute
72. Fulmer, K. L., (2005): Business Continuity Planning – A Step-by-Step Guide with Planning Forms, Third Edition, The Rothsein Catalog on Disaster Recovery, Brookfield, Connecticut, 2005.
73. Jakopeck, E., (1997), "The Risk Assessment: Five Steps to Better Risk Management Decisions". Security Awareness Bulletin, br.3/1997,
74. Kuhn, R., Sutton, S., (2006), "Learning from WorldCom: Implications for Fraud Detection through Continuous Asurance", Journal of Emerging Techologies in Accounting, Vol 3., pp. 61-80

75. Edelman, D., Nicholson, A., (2011), "Arthur Anderson Auditors and Enron: What happened to their Texas CPA licenses?", Journal of Finance and Accountancy
76. Zakon o računovodstvu i reviziji, "Službeni glasnik RS", br. 46/2006, 111/2009 i 99/2011)
77. Zakon o privrednim društvima, ("Službeni glasnik RS", br. 36/2011, 99/2011, 83/2014 - dr. zakon i 5/2015)
78. Zakon o računovodstvu, "Službeni glasnik RS", br. 62/2013
79. Zakon o reviziji, "Službeni glasnik RS", br. 62/2013

OBJAVLJENI NAUČNI RADOVI

1. Radovanović D., Šarac M., Adamović S., Milenković M., "Analysis and classification of attacks on the security of smart cards with additional emphasis on security pin code", UNITECH 2009 - International Scientific Conference, 20 – 21 November 2009, Gabrovo, Bulgaria
2. Adamović S., Radovanović D., Šarac M., Milenković M., "Data protection in databases at the localand server level", UNITECH 2009 - International ScientificConference, 20 – 21 November 2009, Gabrovo, Bulgaria
3. Radovanović D., Šarac M., Lučić D., Adamović S., "Analiza metoda za kontrolu i reviziju informacionih sistema", INFOTEH 2010, Mart 17-19, 2010, Jahorina, Bosna, CD Zbornik radova, ISBN-99938-624-2-8, INFOTEH-JAHORINA Vol. 9, Ref. E-III-2, p. 567-570
4. Šarac M., Radovanović D., Adamović S., Radojević T., "Analiza bezbednosnih i sigurnosnih rešenja u mrežnom okruženju virtuelnih Datacentera", INFOTEH 2010, Mart 17-19, 2010, Jahorina, Bosna, CD Zbornik radova, ISBN-99938-624-2-8, Vol. 9, Ref. E-II-7, p.525-528
5. Adamović S., Šarac M., Milenković M., Radovanović D.,"Generatori slučajnih sekvenci i njihov uticaj na sigurnost", INFOTEH 2010, Mart 17-19, 2010, Jahorina, Bosna, CD Zbornik radova, ISBN-99938-624-2-8, Vol. 9, Ref. E-VI-1, p.820-822

6. Adamović S., Šarac M., Milenković M., Radovanović D., "Generatori slučajnih sekvenci i njihov uticaj na sigurnost", INFOTEH 2010, Mart 17-19, 2010, Jahorina, Bosna, CD Zbornik radova, ISBN-99938-624-2-8, Vol. 9, Ref. E-VI-1, p.820-822
7. M. Šarac, S. Adamović, D. Radovanović, "Analysis of Security and Safety Solutions in Network Environment of Virtual Datacenter", Kaunas & Vilnius - ELECTRONICS 2010, Lithuania, May, 2010.
8. M. Šarac, D. Radovanović, S. Adamović, J. Raković, "Smart Card Security", Kaunas & Vilnius - ELECTRONICS 2010, Lithuania, May, 2010.
9. M. Šarac, D. Radovanović, S. Adamović, „Secret Key Agreement and Privacy Amplification by Public Discussion", Kaunas & Vilnius - ELECTRONICS 2010, Lithuania, May, 2010.
10. Radojević T., Radovanović D.,"E-bankingimplementation in Serbia"- 6th International Scientific Conference Business and Management–2010May 13-14, 2010, Vilnius, Lithuania, ISBN 2029-4441, p.936-942
11. Radovanović D., Radojević T., Lučić D., Šarac M.,"IT audit in accordancewith Cobit standard" – IEEE Conference, MIPRO 2010 - DE, May 24-28, 2010, Opatija, Croatia, ISBN 978-1-4244-7763-0, p.1137-1141
12. Radojević T., Radovanović D., "The impact of electronic banking on offer of financial services" – IEEE Conference, MIPRO 2010- DE, May 24-28, 2010, Opatija, Croatia, ISBN 978-1-4244-7763-0, p.1131-1136
13. Radovanović D., Šarac M., Adamović S., "Cobit pristup reviziji informacionih sistema", XII međunarodni simpozijum Fakulteta organizacionih nauka, SYMORG 2010, Zlatibor, Jun 9 - 12, 2010

14. Šarac M., Radovanović D., Adamović S., "Analiza poslovne vrednosti serverske virtuelizacije", XII međunarodni simpozijum Fakulteta organizacionih nauka, SYMORG 2010, Zlatibor, Jun 9 - 12, 2010
15. Adamović S., Šarac M., Radovanović D., "Generatori slučajnih brojeva i njihov uticaj na sigurnost", XII međunarodni simpozijum Fakulteta organizacionih nauka, SYMORG 2010, Zlatibor, Jun 9 - 12, 2010
16. Radovanović D., Radojević T., Adamović S., Šarac M., "One concept for IT audit" UNITECH 2010 - International ScientificConference, 19 – 20 November 2010, Gabrovo, Bulgaria, ISBN 1313-230X, Vol. I, p.477-482
17. Radojević T., Radovanović D., "Managing risks of electronic banking" UNITECH 2010 - International ScientificConference, 19 – 20 November 2010, Gabrovo, Bulgaria, ISBN 1313-230X, Vol. III, p.107-113
18. Adamović S., Šarac M.,Radovanović D., Radojević T., "Secret key extraction over unauthenticated public channels" UNITECH 2010 - International ScientificConference, 19 – 20 November 2010, Gabrovo, Bulgaria, ISBN 1313-230X, Vol. I, p.472-476
19. Šarac M., Adamović S., Radovanović D., "Analiza sigurnosti bežičnih mreža IEEE 802.11. na teritoriji grada Beograda",Infoteh 2011, Mart 16-18, Jahorina, Bosnia, ISBN-99938-624-2-8, Vol. 10, Ref. B-III-1, p. 191-194
20. Radovanović D., Lučić D., Radojević T., Šarac M.,"Information technology governance – COBIT model" – IEEE Conference, MIPRO 2011 - DE, May 23-27, 2010, Opatija, Croatia, ISSN 1847-3938, p. 80-83

21. Radovanović D., Šarac M., Adamović S., Lučić D., "Necessity of IT Service Management and IT Governance" – IEEE Conference, MIPRO 2011- DE, May 23-27, 2011, Opatija, Croatia, ISSN 1847-3938, p. 84-87
22. Šarac M., Veinović M., Adamović S., Radovanović D., Jevremović A. "Analiza sigurnosti SSL saobraćaja u bežičnim računarskim mrežama", Infoteh 2012, ISBN-99938-624-2-8, Vol. 11, Ref. B-III-1, Jahorina, Bosnia
23. Radojević T., Radovanović D., Šarac M., Stanišić N., Radović N. "The impact of franchising on the development of tourism in Serbia", EBES 2012 Conference, May 24-26, 2012, Istanbul, Turkey, pp.168-169
24. Šarac M., Radojević T., Veinović M., Adamović S., Radovanović D., "Safety of e-business applications, applied knowledge based on SSL traffic" - 10th Annual International Conference on Finance, 2-5 July 2012, Athens, Greece
25. Radovanović D., Lučić D., Adamović S., Šarac M., "What is IT Governance?", UNITECH 2012 - International Scientific Conference, 16 – 17 November 2012, Gabrovo, Bulgaria
26. Radojević T., Šarac M., Radovanović D., Stanišić N., Adamović S., Jovanović J., "Penetration analysis of security in wireless networks", 9th Annual International Conference on Information Technology & Computer Science, May 2013, Athens, Greece
27. Radovanović D., Lučić D., Šarac M., Milenković M., "Klasifikacija i analiza napada na sigurnost mikroprocesorskih smart kartica na fizičkom nivou, sa posebnim osvrtom na verovatnoću pogađanja PIN koda", Telfor 2009, Novembar 24-26, 2009, Beograd, Srbija, CD Zbornik, 1237-1240

28. Stanišić M., Radovanović D., Lučić D., Šarac M., "Upravljanje informacionim tehnologijama i IT revizija", YU INFO 2010, Mart 7-10, 2010, Kopaonik, Srbija
29. Stanišić M., Radovanović D., Lučić D., "Analiza koncepta revizije informacionih sistema prema Cobit metodologiji", Sinergija 2010, 19 mart 2010, Bijeljina, Bosna, p.154-161
30. Veinović M., Šarac M., Radovanović D., "Analiza procesa virtualizacije", Sinergija 2010, 19 mart 2010, Bijeljina, Bosna, p. 131-137
31. Milenković M., Adamović S., Šarac M., Radovanović D., "Upravljanje X.509 sertifikatima u PKI sistemu", ZITEH 10, Beograd, Mart 5-6, 2010, CD Zbornik, ISBN 978-86-90951111-6
32. Mihailović V., Šarac M., Adamović S., Radovanović D.,"Video konferencijski sistemi i njihova primena u obrazovnom sistemu", Sinergija 2010, 19 mart 2010, Bijeljina, Bosnia, ISBN 978-99955-26-21-4, p. 122-128
33. Stamenković D., Šarac M., Adamović S., Radovanović D., "Energetska efikasnost u primeni virtualnog datacentra i upotreba ekoloških računara u edukativnim ustanovama", Sinergija 2012
34. Radojević, T., Šarac, M., Radovanović D., Srejić, J.,: "Uticaj uvođenja elektronskih servisa na poboljšanje kvaliteta usluga u lokalnoj samoupravi", XII Međunarodni naučni skup Sinergija 2013, Univerzitet Sinergija, Bjeljina, Zbornik radova str.97-105
35. D. Stamenković, M. Šarac, D. Radovanović, A. Simićević, „Privacy Policy and Data Archiving in Organizations of the Republic of Serbia and the Countries of the European Union“, SYNTHESIS 2015, International Scientific Conference of IT and Business-Related Research, Belgrade, Serbia, Apr, 2015.

36. Dalibor Radovanović, Marko Šarac, Tijana Radojević, Saša Adamović, "Information technology audit process and Cobit", Vol. XVIII, No. 7, pp. 110-113, Jan, 2013.
37. Marko Šarac, Tijana Radojević, Nemanja Stanišić, Saša Adamović, Dalibor Radovanović, „Safety of e-business Applications in Serbia: Applied Knowledge Based on SSL Traffic", Journal of Internet Banking and Commerce, Vol. 17, No. 3, pp. 1-18, Dec, 2012.
38. Radovanović D., Veinović M., Šarac M., "Klasifikacija napada i ugrožavanje bezbednosti smart kartica", Singidunum revija, Vol. 6, No. 1, Beograd, 2009, ISSN 1820-8819, 82-93
39. Stanišić M., Radovanović D., Lučić D., "Revizija informacionih sistema", Singidunum revija, Vol. 6, No. 2, Beograd, 2010, ISSN 1820-8819, 72-81.
40. Radovanović D., Šarac M., Adamović S., "Rešavanje problema uskog grla virtuelnih servera, virtuelnim iSCSI uređajima za skladištenje podataka" Singidunum rev., Vol. 7, No. 1, Beograd, 2010, ISSN 1820-8819, 193-198

CITIRANOST OBJAVLJENIH RADOVA

80. D., Radojević T., Lučić D., Šarac M., "IT audit in accordance with Cobit standard", IEEE Conference, MIPRO 2010 - DE, May 24-28, 2010, Opatija, Croatia, ISBN 978-1-4244-7763-0, p.1137-1141
81. Daniel Santiago Ramírez, (2010), SPAIN, "Análisis y estudio sobre el gobierno y gestión de los servicios ti en el mercado Español - Analysis and study on the government and it services management in the Spanish market", Universidad Carlos III de Madrid, Spain
82. Siti Syaroh, (2010), JACARTA, "Audit Sistem Informasi Call Center Studi Kasus ESQ Leadership Center dengan Menggunakan Metode COBIT", 2010, Fakultas Sains dan Teknologi, Unversitas Islam Negeri, Syarif Hidayatullah, Jakarta
83. J Ferri, JD Brancher, R Miranda, (2011), BRASIL, "Proposal for a Framework Focus On Sustainability (A Template to Software Factories)", XXX International Conference of the Chilean Computer Science Society (SCCC'2011), Curicó, Chile
84. David Wahlström, Lars Lindvall, (2011), SWEDEN, "Åtgärdsplaner vid informationssystemhaveri - Action plans for information systems failure", Department of Informatics, Lund University School of Economics and Management, LUSEM, Sweden
85. Ruben Pereira, Miguel Mira da Silva, (2012), PORTUGAL, "A literature review: guidelines and contingency factors for IT governance", European, Mediterranean &

Middle Eastern Conference on Information Systems 2012 (EMCIS2012), June 7-8, Munich, Germany

86. Al Omari, Loai, Barnes, Paul H., & Pitman, Grant (2012) AUSTRALIA "An exploratory study into audit challenges in IT governance : a Delphi approach", Symposium on IT Governance, Management and Audit (SIGMA2012), Universiti Tenaga Nasional, Malaysia, University of Tenaga Nasional, Kuala Lumpur.
87. Harryparshad Nirvasha, (2012), SOUTH AFRICA, "Best practices for implementing multiple concurrent IT frameworks (CMMI, ITIL, Six-Sigma, CobiT and PMBOK)", Graduate School of Business Leadership, University of South Africa, South Africa
88. Ruben Pereira, Miguel Mira da Silva, (2012), PORTUGAL, "IT Governance Implementation: The Determinant Factors", Volume 2012 (2012), Article ID 970363, Communications of International Business Information Management Association, 16 pages, DOI: 10.5171/2012.970363
89. Alves Victor, Ribeiro Jorge, Castro Pedro, (2012), PORTUGAL, "Information technology governance — A case study of the applicability of ITIL and COBIT in a Portuguese Private School", CISTI 2012 (7th Iberian Conference on Information Systems and Technologies), ISSN: 2166-0727, Print ISBN: 978-1-4673-2843-2, Date of Current Version: 30 August 2012, Issue Date: 20-23 June 2012
90. Tiago Miguel Lopes do Rosário, (2012), PORTUGAL, "Formalization of the IT Audit Management Process", Dissertação para obtenção do Grau de Mestre em, Engenharia Informática e Computadores, Instituto Superior Técnico, Lisboa, Portugal
91. Tanovic A., Orucevic F., Androulidakis I, (2012), "Development of a new improved model of the ITIL V3 framework for the information system of Telecom operator", 11th WSEAS International Conference on Data Network, Communications,

Computers (DNCOCO'12), ISBN: 978-1-61804-118-0, September 7-9, 2012, Sliema, Malta

92. Azalia Shamsaei, Daniel Amyot, Alireza Pourshahid, (2011), CANADA, "A Systematic Review of Compliance Measurement Based on Goals and Indicators", Advanced Information Systems Engineering Workshops, Lecture Notes in Business Information Processing, Volume 83, Part 4, 2011, ISBN:978-3-642-22055-5, DOI: 10.1007/978-3-642-22056-2_25, pp 228-237, London, UK
93. Abdellatif I., April A., (2012), CANADA, "Multiperspective Representation of Internal Controls in Business Processes", Journal of Software Engineering and Applications, Vol. 5 No. 12, 2012, pp. 971-982. doi: 10.4236/jsea.2012.512112, ISSN Print: 1945-3116, ISSN Online: 1945-3124, USA
94. Abdellatif I., April A., (2012), CANADA, "Multiperspective Representation of Internal Controls in Business Processes", Journal of Software Engineering and Applications, Vol. 5 No. 12, 2012, pp. 971-982. doi: 10.4236/jsea.2012.512112, ISSN Print: 1945-3116, ISSN Online: 1945-3124, USA
95. Al Omari, Loai, Barnes, Paul H., & Pitman, Grant, (2013), AUSTRALIA, "A Delphi study into the audit challenges of IT governance in the Australian public sector", Electronic Journal of Computer Science and Information Technology (eJCSIT), Vol. 4, No. 1, 2013, Australia
96. Tiago Rosário, Rúben Pereira, Miguel Mira da Silva, (2013), PORTUGAL, "IT Audit Management Architecture and Process Model", 16th International Conference, BIS 2013, Poznań, Poland, June 19-21, 2013. Proceedings, pp 187-198, Springer Berlin Heidelberg, Poland

97. Abdellatif, I., & April, A. (2014), CANADA, "A Comparative Evaluation on Multi-perspective Representations of Business Controls: An Experimental Case Study", Proceedings of the 2014 Industrial and Systems Engineering Research Conference

98. Syaroh, Siti, (2011), INDONESIA, "Audit sistem informasi call center pada PT. Arga Bangun Bangsa (Esq leadership center) dengan menggunakan framework cobit).", UIN Syarif Hidayatullah Jakarta: Fakultas Sains dan Teknologi, 2011, Indonesia
99. DWI, WIBOWO AJI, (2014), INDONESIA, "Self Assessment Service Design Pada PT. Dinustek Menggunakan Framework ITIL V. 3 Studi Kasus: Pelayanan Pengadaan Fasilitas Hotspot di Universitas Dian Nuswantoro." Skripsi, Fakultas Ilmu Komputer, 2014, Indonesia
100. Hakim, Abdul, Hoga Saragih, and Agus Suharto, (2015), INDONESIA, "EVALUASI TATA KELOLA TEKNOLOGI INFORMASI DENGAN FRAMWORK COBIT. 5 DI KEMENTERIAN ESDM." Jurnal Sistem Informasi 10.2 (2015): p105-117, 2015, INDONESIA
101. Rezeq Khalil Mohammed Harb, (2014), GAZA, "The Impact of Information Systems Audit on Improving Bank's Performance", Applied Study at Banks Working in Gaza, Islamic University of Gaza, Master Thesis, 2012, Gaza, PALESTINA
102. Shamsaei Azalia, (2012), CANADA, "Indicator-based Policy Compliance of Business Processes", PhD Thesis, University of Ottawa, 2012, Canada
103. R. Janeliūnienė, G. Liberytė, V. Davidavičienė, (2011), "IT auditas Lietuvos smulkaus ir vidutinio dydžio įmonėse - Possibilities of IT audit in small and medium size companies in Lithuania", Science – Future of Lithuania / Mokslas – Lietuvos Ateitis, Vilnius Gediminas Technical University, Vilnius, Lithuania

104. Davidavičienė V., Tolvaišas J., (2011), "Measuring quality of e-commerce web sites: Case of Lithuania", EKONOMIKA IR VADYBA - Economics and Management 2011 Nr.16, Kauno Technologijos Universitetas, Lithuania

105. Vida Davidavičienė, Ieva Meidutė, (2011), "Quality of e-Logistics in e-Commerce: Consumer Perception", Technical University of Liberec, Faculty of Economics, Liberec Economic Forum 2011, Liberec, Czech Republic

106. Boyke Nurhidayat, (2011), "Evaluasi Integrated Toll Collection System Dengan Menggunakan Framework Cobit", Sekolah Pascasarjana, Institut Pertanian Bogor, Bogor, Indonesia

107. N. K. Paliulis, J. Sabaitytė, (2011), "E. Verslo modelių panaudojimas verslo plėtrai (eng. E-business models for business development)", Contemporary Issues in Business, Management and Education ‘2011, Vilnius Gediminas Technical University (Faculty of Business Management), Vilnius, Lithuania

108. Herri Setiawan, Khabib Mustofa, (2013), INDONESIA, "Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia", IPTEK-KOM, Vol. 15 No. 1 Juni 2013: 1-15, ISSN 1410 - 3346, 2013, Indonesia

109. Amelia Setiawan, (2012), INDONESIA, "Possibility Of Cobit Quickstart Utilization For Small And Medium Enterprises To Assess It Control Objectives", Proceedings of The 1st International Conference on Information Systems For Business Competitiveness (ICISBC) 2011, ISSN 978-979-097-198-1, Indonesia

110. Slindile Khanyile, Hanifa Abdullah, (2012), SOUTH AFRICA, "COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT",

111. Alves Victor, Ribeiro Jorge, Castro Pedro, (2012), PORTUGAL, "Information technology governance — A case study of the applicability of ITIL and COBIT in a Portuguese Private School", CISTI 2012 (7th Iberian Conference on Information Systems and Technologies), ISSN: 2166-0727, Print ISBN: 978-1-4673-2843-2, Date of Current Version: 30 August 2012, Issue Date: 20-23 June 2012

112. Huda Al Skafy, Zeyad Abdel Halim Al- Theebeh, (2012), JORDAN, "The level of information technology governance in KULACOM-Jordan Company", Basic Research Journal of Business Management and Accounts ISSN 2315-6899 Vol. 1(5) pp. 84-93 December 2012