Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-588-594

REVIZIJA KONTROLA INFORMACIONIH SISTEMA

Mile Stanišić
Univerzitet Singidunum, Srbija

Abstract:
Revizija kontrola informacionih sistema obuhvata dve osnovne grupacije kontrola, opšte kontrole i aplikativne kontrole. Proces revizije se obavlja kroz tri faze, fazu planiranja, testiranja i izveštavanja. Na osnovu rezultata planiranja revizije i drugih obavljenih postupaka revizor treba da identifikuje kontrolne kategorije, kritične elemente, kontrolne aktivnosti, kao i tehnike kontrole koje su relevantne za IS reviziju. Pri tome, revizor razmatra ciljeve revizije i obim revizije, nivo rizika i preliminarno razumevanje IS kontrola. Nakon testiranja opštih i aplikativnih kontrola revizor donosi zaključak o nivou efektivnosti kontrola i utvrđenim slabostima u kontrolama.

Key words:
informacioni sistem,
opšte kontrole,
aplikativne kontrole,
revizija.

UVOD

IT revizija predstavlja proces sakupljanja i ocenjivanja dokaza radi utvrđivanja da li je kompjuterski sistem dizajniran tako da održava integritet podataka, zaštitu sredstava, omogućava da se na efikasan način postignu ciljevi organizacije i da se na efikasan način koriste resursi. Efikasan informacioni sistem vodi ka tome da organizacija postigne svoje ciljeve i da efikasan informacioni sistem koristi minimalna resurse za postizanje zahtevanih ciljeva. IT revizori moraju da budu upoznati sa karakteristikama informacionog sistema i okruženjem za donošenje odluka kod klijenta kada ocenjuju efikasnost određenog sistema.

Sve veća upotreba kompjutera za obradu podataka u organizacijama je povećala obim ispitivanja i ocenjivanja internih kontrola za svrhu revizije. Interne kontrole IT su od velikog značaja u svakom kompjuterskom sistemu i za revizora je značajan zadatak da vodi računa ne samo da postoje adekvatne kontrole već da one i funkcionišu na efikasan način da bi se obezbedili rezultati i postigli ciljevi. Takođe, interne kontrole treba da budu proporcionalne ocenjenom riziku tako da bi se smanjio uticaj utvrđenih rizika na prihvatljiv nivo. Revizori Informacionih sistema treba da ocene adekvatnost internih kontrola u kompjuterskom sistemu za ublažavanje rizika od gubitaka zbog grešaka, prevara i drugih radnji i nesreća ili incidenata koji prouzrokuju da sistem ne bude na raspolaganju.

Kontrole informacionih sistema se sastoje od onih internih kontrola koje zavise od obrade informacionih sistema i obuhvataju opšte kontrole (entiteta, sistema i nivoa aplikacija poslovnih procesa), kontrole aplikacija poslovnih procesa (ulaz, obradu, izlaz, matičnu datoteku, interfejs, i kontrole sistema za upravljanje podacima), i kontrole korisnika (kontrole koje obavljaju ljudi koji su u interaktivnoj vezi sa informacionim sistemima.[1]

U radu su prikazani rezultati istražena revizija opštih i aplikativnih kontrola informacionih sistema. Proces revizije se odbija kroz tri faze, fazu planiranja, testiranja i izveštavanja. Za svaku kontrolnu kategoriju u radu su utvrđeni značajni elementi – zadaci koji su bitni za uspostavljanje adekvatnih kontrola u okviru određene kategorije.

PRIRODA KONTROLA INFORMACIONOG SISTEMA

Ciljevi kontrole informacione i slične tehnologije (*The Control Objectives for information and related Technology - COBIT*) definišu kontrolu kao "politike, procedure, prakse i organizacione strukture, koncipirane tako da pružaju opravdano uveravanje da će se poslovni ciljevi ostvariti, a da će se neželjeni događaji sprečiti ili otkriti i korigovati." Ocenjivanje kontrola IS obično obuhvata opšte kontrole i kontrole aplikacija poslovnih procesa (takođe nazvane aplikativne kontrole). Entitet mora da ima efikasne opšte i kontrole aplikacija poslovnih procesa da bi postigao odgovarajuću poverljivost, integritet, pouzdanost i usaglašenost sa zakonima i propisima raspoloživost značajnih informacija i informacionih sistema.[2]

Poverljivost. Poverljivost se odnosi na zaštitu osetljivih informacija od neovlašćenog obelodanjivanja. Potrebno je razmotriti stepen osetljivosti podataka pošto će ovo

1 Stanišić, M., Stanojević, LJ., Revizija i primena kompjutera, Univerzitet Singidunum, Beograd, 2010, str. 315.
2 Razumevanje IT kontrola: Richards, D.A., Oliphant,A.S., Le Grand, C.H., Information Technology Controls, Global Technology Audit Guide, The Institute of Internal Auditors, USA, March 2005, pp.1-9.

određivati koliko striktne kontrole ovog pristupa treba da budu. Menadžmentu je potrebno uveravanje o sposobnosti organizacije da održi poverljivost informacija, pošto ugrožavanje poverljivosti može značajno da naškodi reputaciji u javnosti, naročito tamo gde se informacije odnose na osetljive podatke klijenta.

Integritet. Integritet se odnosi na tačnost i kompletnost informacija kao i na njihovu valjanost u skladu sa poslovnim vrednostima i očekivanjima. Ovo je jedan od važnih ciljeva revizije za dobijanje uveravanja zato što obezbeđuje i menadžmentu i eksternim korisnicima izveštaj da se na informacije koje obezbeđuju informacioni sistemi organizacije može osloniti i imati u njih poverenja za donošenje poslovnih odluka.

Raspoloživost. Raspoloživost se odnosi na to da su informacije na raspolaganju kada to zahteva poslovni proces u sadašnjosti i budućnosti. Takođe se odnosi na zaštitu potrebnih resursa i odgovarajućih sposobnosti. Imajući u vidu prirodu visokog rizika čuvanja važnih informacija u kompjuterskim sistemima značajno je da organizacije dobiju uveravanje da informacije koje su im potrebne za donošenje odluka su na raspolaganju kada je to potrebno. To podrazumeva da se obezbedi da u organizaciji postoje mere za obezbeđivanje kontinuiteta poslovanja i da se može izvršiti pravovremeni oporavak od nesreća tako da informacije budu na raspolaganju korisnicima kako i kada je to potrebno.

Pouzdanost. Pouzdanost se odnosi na stepen konzistentnosti sistema ili sposobnosti sistema (ili komponente) da obavlja svoju zahtevanu funkciju pod navedenim uslovima. Pouzdanost je značajan cilj revizije da bi se obezbedilo uveravanje da sistem funkcioniše na konzistentan način i obavlja svoje navedene funkcije u skladu sa očekivanjima.

Usaglašenost sa zakonima i propisima. Usaglašenost se odnosi na poštovanje zakona, propisa u ugovornih obaveza kojima poslovni proces podleže, tj., poštovanje eksternih poslovnih kriterijuma. Menadžment i ključni učesnici zahtevaju uveravanje da postoje potrebne procedure usaglašenosti sa propisima i zakonima, zato što postoji potencijalni rizik da bi organizacija mogla da se izloži kaznama ukoliko zakonske i regulatorne procedure nisu primenjene.

Kontrole informacionih sistema se sastoje od onih internih kontrola koje zavise od obrade informacionih sistema i obuhvataju opšte kontrole (entiteta, sistema, nivoa aplikacija poslovnih procesa), kontrole aplikacija poslovnih procesa (ulaz, obradu, izlaz, matičnu datoteku, interfejs i kontrole upravljanja podacima), i kontrole korisnika (kontrole koje obavljaju ljudi koji su u interaktivnom odnosu sa informacionim sistemima). Opšte kontrole i kontrole aplikacija poslovnih procesa su uvek IS kontrole. Kontrola korisnika je IS kontrola ukoliko njena efikasnost zavisi od obrade informacionih sistema ili pouzdanosti (tačnost, potpunost, valjanost, pouzdanost i usaglašenost) informacija koje su obradili informacioni sistemi. Suprotno tome, kontrola korisnika nije IS kontrola ukoliko njena efikasnost ne zavisi od obrade informacionih sistema ili pouzdanosti informacija koje su obradili informacioni sistemi.

Opšte kontrole su politike i procedure koje se primenjuju na sve ili veće segmente informacionih sistema entiteta i pomažu da se osigura njihovo pravilno funkcionisanje. Primeri primarnih ciljeva za opšte kontrole su zaštita podataka, zaštita aplikacionih programa poslovnih procesa, i da obezbedi kontinuirani rad kompjutera u slučaju neočekivanih prekida. Opšte kontrole se primenjuju na ceo entitet, sistem i nivoe aplikacija poslovnih procesa. Efikasnost opštih kontrola predstavlja značajan faktor prilikom utvrđivanja efikasnosti kontrola aplikacija poslovnih procesa koje se primenjuju na nivou aplikacija poslovnih procesa.

Bez efikasnih opštih kontrola kontrole aplikacija poslovnih procesa se obično mogu učiniti neefikasnim njihovim zaobilaženjem ili modifikovanjem. Na primer, automatska editovanja planirana da spreče korisnike da unesu nerazumno (neobjektivno) velike dinarske iznose u sistem za obradu plaćanja, mogu predstavljati efikasnu aplikativnu kontrolu. Međutim, ova kontrola nije efikasna (na nju se ne može osloniti) ukoliko opšte kontrole dozvoljavaju neovlašćeno modifikovanje programa koje može da omogući da neka plaćanja budu izostavljena iz editovanja ili neovlašćene promene budu izvršene u datotekama pošto je obavljeno editovanje. Zbog toga revizor mora da razume sledeće vrste opštih kontrola: upravljanje zaštitom, logički i fizički pristup, upravljanje konfiguracijama, podelu dužnosti i planiranje nepredviđenih događaja.

Kontrole aplikacija poslovnih procesa su direktno povezane sa pojedinačnim kompjuterizovanim aplikacijama. One pomažu da se obezbedi da transakcije budu potpune, tačne, validne, poverljive i raspoložive. Kontrole aplikacija poslovnih procesa obuhvataju (1) programirane kontrolne tehnike, kao što su automatska editovanja i (2) manuelno praćenje kompjuterskih izveštaja, kao što su pregledi izveštaja kojim se utvrđuju odbijene ili neuobičajene stavke. U tom smislu revizor treba da razume definisane aplikacione kontrole, ili poslovne kontrole, kao one kontrole koje pomažu da se obezbede valjanost, kompletnost, tačnost i poverljivost transakcija i podataka za vreme obrade aplikacija.

CILJEVI REVIZIJE

Cilj IT revizije je da se oceni kompjuterski informacioni sistem (*Computerised information system* - CIS) klijenta radi uveravanja da li CIS proizvodi pravovremene, tačne, potpune i pouzdane informacije, kao i da se obezbedi poverljivost, integritet, raspoloživost i pouzdanost podataka, i usklađenost sa relevantnim zakonskim i regulatornim zahtevima. Ciljevi revizije će se razlikovati zavisno od prirode ili kategorije revizije.

Ciljevi obavljanja IT revizije kao komponente revizije finansijskih izveštaja su:

- Upoznati se sa tim koliko menadžment ima koristi od korišćenja IT za unapređenje značajnih poslovnih procesa;
- Upoznati se sa sveobuhvatnim uticajem IT na klijentove značajne poslovne procese, uključujući pripremu finansijskih izveštaja i poslovne rizike povezane sa ovim procesima;

- Upoznati se sa tim koliko klijentovo korišćenje IT za obradu, čuvanje i dostavljanje finansijskih informacija utiče na sisteme internih kontrola i naše razmatranje inherentnog rizika i kontrolnog rizika;
- Utvrditi i upoznati se sa kontrolama koje menadžment koristi da oceni, upravlja i kontroliše procese IT; i
- Doneti zaključak o efikasnosti kontrola procesa IT koji imaju direktan i značajan uticaj na obradu finansijskih informacija.

Tamo gde je revizija IT uključena u reviziju poslovanja ciljevi revizije su dalje definisani po tome koju ulogu IT ima u reviziji poslovanja.

- Ukoliko revizija poslovanja ima IT u fokusu cilj će biti da se traži uveravanje da se svi aspekti IT sistema, uključujući kontrole, primenjuju na efikasan način.
- Revizija poslovanja bi mogla u drugom slučaju da predstavlja ispitivanje efikasnosti i efektivnosti poslovnog procesa/vladinog programa i kao takva IT revizija se obavlja zato što se IT smatra značajnom u organizaciji pošto je u mogućnosti da pomogne kod pružanja tih usluga. Kao takva IT revizija je fokusirana da obezbedi uveravanje da se na IT sisteme može osloniti da pomogne u pružanju tih usluga. Efikasnost i efektivnost tih usluga se zatim ispituju iz perspektive koja nije IT posle razmatranja uticaja koji IT ima na sposobnost organizacije da obezbedi te usluge.

FAZE U OBAVLJANJU REVIZIJE KONTROLA INFORMACIONIH SISTEMA

Metodologija IT revizije koristi pristup baziran na riziku od višeg ka nižem nivou prilikom ocenjivanja kontrola. Sledeće faze obezbeđuju pregled zadataka koji su uključeni u ispitivanje IT kontrola: 1) planiranje, 2) testiranje i 3) izveštavanje.[3]

Planiranje. Ova faza pomaže revizoru IT da se upozna sa entitetom, njegovom organizacionom strukturom i poslovanjem. IT revizor se upoznaje sa kompjuterskim poslovanjem, kontrolama i odgovarajućim rizicima u vezi sa inherentnim IT rizicima. Na osnovu ovih saznanja revizor ocenjuje celokupno IT kontrolno okruženje i obavlja preliminarno ocenjivanje rizika. Rezultati ovog ocenjivanja će predstavljati smernice za nivo procedura (postupaka) koje treba primeniti u sledećim fazama revizije. Revizor utvrđuje efektivan i efikasan način da bi dobio dokaze potrebne za postizanje ciljeva revizije kontrola informacionih sistema i izveštaja o reviziji. Za finansijske revizije revizor razvija strategiju revizije i plan revizije. Za revizije poslovanja revizor razvija plan revizije.

Testiranje. Revizor testira efikasnost kontrola IS koje su relevantne za ciljeve revizije. Za vreme ove faze revizije IT revizori dobijaju detaljne informacije o kontrolnim politikama, procedurama i ciljevima i obavljaju testove kontrolnih aktivnosti. Ciljevi ovih testova su da se utvrdi da li kontrole funkcionišu na efikasan način. Opšte kontrole, kao i aplikativne kontrole, moraju biti efikasne da bi se pomoglo da se obezbedi poverljivost, integritet, raspoloživost i pouzdanost značajnih kompjuterskih podataka.

Izveštavanje. Za vreme faze izveštavanja IT revizor donosi zaključke i priprema izveštaj da bi informisao o ciljevima revizije, delokrugu revizije, usvojenoj metodologiji i nalazima, zaključcima i preporukama. Revizor donosi zaključak o uticaju utvrđenih slabosti u kontroli informacionih sistema na ciljeve revizije, i izveštava o rezultatima revizije, uključujući materijalno značajne slabosti i druge značajne nedostatke.

Za svaku od ove tri faze revizor priprema odgovarajuću revizijsku dokumentaciju.

PLANIRANJE REVIZIJE KONTROLA INFORMACIONIH SISTEMA

Prilikom planiranja revizije IS kontrola revizor koristi ekvivalentne koncepte materijalnosti (kod finansijskih revizija i angažmana za atestiranje - *in financial audits and attestation engagements*) i značajnosti/važnosti (*significance)* (kod revizija poslovanja - *in performance audits*) da bi se planirale efektivne i efikasne procedure revizije. Materijalnost (*materiality*) i značajnost su koncepti koje revizor koristi da utvrdi planiranu prirodu, vreme i nivo revizijskih procedura (postupaka). Osnovni princip je da se od revizora ne traži da potroši resurse na stavke od malog značaja, tj. one koje ne bi uticale na mišljenje ili ponašanje objektivnog (razumnog) korisnika izveštaja o reviziji u svetlu uslova (okolnosti) okruženja. Na bazi ovog principa revizor može da utvrdi da neke oblasti revizije IS kontrola (na primer: specifični sistemi) nisu od materijalnog značaja ili važni i zbog toga zahtevaju veoma malu ili nekakvu pažnju revizije.

Materijalnost i značaj obuhvataju kvantitativne i kvalitativne faktore kada je u pitanju predmet revizije. Čak iako sistem može da obrađuje transakcije od nematerijalnog značaja i važnosti sistem može da sadrži osetljive informacije ili obezbeđuje putanju pristupa drugim sistemima koji sadrže informacije koje su osetljive ili inače od materijalnog značaja ili važne. Na primer, aplikacija koja obezbeđuje javne informacije preko website-a, ukoliko je njena konfiguracija neodgovarajuća, može izložiti resurse interne mreže, uključujući osetljive sisteme, neovlašćenom pristupu.

Planiranje se odvija kroz celu reviziju kao iterativni proces. (Na primer, na bazi nalaza iz faze testiranja revizor može da promeni planirani pristup revizije, uključujući plan specifičnih testova.) Međutim, planiranje aktivnosti je skoncentrisano u fazi planiranja za vreme kojeg su ciljevi: upoznavanje sa entitetom i njegovim poslovanjem, uključujući njegovu internu kontrolu, da se utvrde značajni problemi, oceni rizik i planira priroda, obim i vreme procedura revizije. Da bi se ovo obavilo metodologija koja je prezentirana obuhvata smernice kao pomoć revizoru da uradi sledeće:

- Da se upozna sa svim ciljevima revizije i odgovarajućim delokrugom revizije kontrola IS

3 Panian, Ž., Spremić, M., Kontrola i revizija informacionih sustava, Sinergija-nakladništvo, Zagreb, Hrvatska, 2001, str. 24-30.

- Da upozna entitet i njegovo poslovanje i ključne poslovne procese[4]
- Da stekne opšta saznanja o strukturi mreža entiteta
- Da identifikuje ključne oblasti od interesa za reviziju (datoteke, aplikacije, sisteme, lokacije)[5]
- Da preliminarno oceni rizik informacionih sistema
- Da utvrdi kritične kontrolne tačke (na primer: spoljne pristupne tačke mrežama)
- Da se preliminarno upozna sa kontrolama IS
- Da obavi druge procedure planiranja revizije

Specijalista za IS kontrole skuplja informacije koje se odnose na gore navedene etapa kroz intervjue sa ključnim osobljem IT ili preko traženja podataka. Revizor obavlja planiranje da bi utvrdio efektivan i efikasan način da dobije dokaze potrebne da podrži ciljeve revizije IS kontrola i izveštaj o reviziji. Priroda i nivo procedura planiranja revizije se razlikuju za svaku reviziju zavisno od nekoliko faktora, uključujući veličinu i složenost entiteta, revizorovo iskustvo što se tiče entiteta i revizorovo poznavanje poslovanja entiteta.

Ukoliko se revizija IS kontrola obavlja kao deo finansijske revizije standardi za eksternu reviziju zahtevaju od revizora da se upozna sa internom kontrolom finansijskog izveštavanja u dovoljnoj meri da oceni rizik od značajnog lažnog prikazivanja finansijskih izveštaja bilo zbog grešaka ili prevara, i da planira prirodu, vreme i obim daljih revizijskih postupaka na bazi te ocene. Ovo uključuje obavljanje procedura ocenjivanja rizika da bi se ocenio plan kontrola relevantnih za reviziju finansijskih izveštaja i da se utvrdi da li su one primenjene. Kod ovog upoznavanja revizor razmatra na koji način korišćenje IT i manuelnih procedura od strane entiteta utiče na kontrole relevantne za reviziju.

Ukoliko se revizija IS kontrola obavlja kao deo angažmana dokazivanja (potvrđivanja) ispitivanja revizor treba da stekne dovoljno saznanja o internoj kontroli koja je od materijalnog značaja za ovaj predmet radi planiranja procedure angažmana i plana da bi se postigli ciljevi angažmana za dokazivanje (atestiranje).

Ukoliko se revizija IS kontrola obavlja kao deo revizije poslovanja, u standardima se navodi da kada se utvrdi da su IS kontrole značajne za ciljeve revizije revizori treba zatim da ocene plan i operativnu efikasnost takvih kontrola. Ovo ocenjivanje bi uključivalo i druge IS kontrole koje utiču na efikasnost značajnih kontrola ili pouzdanost informacija koje se koriste u obavljanju značajnih kontrola. Revizori treba da dovoljno upoznaju IS kontrole potrebne za ocenjivanje revizijskog rizika i planiraju reviziju u kontekstu ciljeva revizije.

Pored toga, revizori treba da utvrde procedure revizije koje se odnose na kontrole informacionih sistema koje su potrebne da bi se dobio dovoljan i odgovarajući dokaz kao podrška nalazima i zaključcima revizije.

Kada ocenjuju efikasnost IS kontrola koje direktno predstavljaju deo određenog cilja revizije revizori treba da testiraju IS kontrole potrebne za ispunjavanje ciljeva revizije. Na primer: revizija može da obuhvata efikasnost IS kontrola koje se odnose na izvesne sisteme, uređaje (kapacitete) ili organizacije.

Revizor treba da preliminarno oceni i dokumentuje prirodu i nivo rizika IS koji se odnosi na ključne oblasti od interesa za reviziju. Rizik IS se odnosi na verovatnoću da se može dogoditi gubitak poverljivosti, integriteta ili raspoloživosti što bi značajno uticalo na ciljeve revizije (na primer, za finansijsku reviziju, lažno prikazivanje od materijalnog značaja). Ocenjivanje IS rizika obuhvata ocenu verovatnoće da takav gubitak poverljivosti, integriteta ili raspoloživosti se može dogoditi, kao i materijalni značaj ili važnost gubitka poverljivosti, integriteta ili raspoloživosti za ciljeve revizije. Revizor treba da dokumentuje faktore koji značajno povećavaju ili smanjuju nivo IS rizika i njihov potencijalni uticaj na efikasnost IS kontrola.[6]

Revizorska ocena IS rizika utiče na prirodu, vreme i obim procedura revizije IS kontrola. Ako se IS rizik povećava revizor treba da obavi ekstenzivnije i/ili efikasnije testove IS kontrola. Na primer, značajan broj pristupnih tačaka Internetu koje nisu centralizovano kontrolisane povećava IS rizik. U ovom slučaju revizor bi proširio testiranje pošto postoji više potencijalnih putanja pristupa ključnim oblastima od interesa za reviziju.

Testiranje kontrola informacionih sistema

Prilikom faze testiranja IS kontrola u toku revizije revizor koristi informacije dobijene za vreme faze planiranja da bi testirao efikasnost IS kontrola koje su relevantne za ciljeve revizije. Pošto se dobije revizijski dokaz kroz obavljanje testiranja kontrola revizor treba da ponovo oceni plan revizije i razmotri da li su promene odgovarajuće.[7]

Istovremeno dok utvrđuje da li su IS kontrole na odgovarajući način planirane i primenjene i dok obavlja testiranja IS kontrola, revizor treba periodično da ocenjuje dobijene kumulativne revizijske dokaze da bi utvrdio da li je potrebno izvršiti izvesna revidiranja plana revizije. Na primer, ukoliko su utvrđene značajne slabosti revizor može da odluči da obavi manje testiranja u preostalim oblastima ukoliko su postignuti ciljevi revizije. U suprotnom slučaju, obavljanje testiranja može da otkrije dodatne oblasti koje je potrebno testirati.

Za one IS kontrole za koje revizor utvrdi da su pravilno/prikladno planirane i primenjene, revizor odlučuje da li da obavi testove efikasnosti funkcionisanja takvih kontrola. Prilikom odlučivanja da li da testira efikasnost funkcionisanja IS kontrola revizor treba da utvrdi da li je moguće i izvodljivo da se dobiju dovoljni i odgovarajući revizijski dokazi bez testiranja IS kontrola. Za revizije finansijskih izveštaja i za pojedinačne revizije (usaglašenost sa propisima i zakonima) od revizora se zahteva da obavi testiranje da su kontrole planirane i primenjene na pravilan način da bi se postigao nizak ocenjeni nivo rizika kontrola.

Postoji pet opštih kategorija kontrole i četiri kategorije aplikativnih kontrola. Opšte kontrole su sledeće:

4 Videti više: GAIT for Business and IT Risk (GAIT-R), The Institute of Internal Auditors, 2008, pp. 10-11.

5 Ibid., pp. 6-7, 11-12.

6 GAIT Methodology, A risk-based approach to assessing the scope of IT general controls The Institute of Internal Auditors, 2007, pp. 7-34.

7 Videti analizu rizika: Global Technology Audit Guide (GTAG) 1, Information Technology Risk and Controls, The Institute of Internal Auditors, 2012, pp. 10-11.

- upravljanje bezbednošću,
- kontrola pristupa,
- upravljanje konfiguracijom,
- razdvajanje dužnosti, i
- planiranje za nepredviđene događaje.

Kontrole na nivou aplikacija poslovnih procesa su:

- opšte kontrole poslovnog procesa na nivou aplikacija,
- kontrole poslovnih procesa,
- kontrole interfejsa i konverzija, i
- kontrole sistema upravljanja podacima.

Poslednje tri kategorije kontrola na nivou aplikacija poslovnih procesa su zajedno objašnjene "kao kontrole aplikacija poslovnih procesa".

Za efikasno obavljanje revizije kontrola revizor treba da koristi priručnik gde je obrađena svaka kategorija kontrola i utvrđeni značajni elementi – zadaci koji su bitni za uspostavljanje adekvatnih kontrola u okviru kategorije. Za svaki značajni element treba da postoji objašnjenje o odgovarajućim ciljevima, rizicima i kontrolnim aktivnostima, kao i odgovarajućim potencijalnim kontrolnim tehnikama i predloženim revizijskim procedurama.[8]

Zavisno od IS rizika i ciljeva revizije priroda i nivo kontrolnih tehnika potrebnih da se postigne poseban kontrolni cilj će se razlikovati.

Revizor utvrđuje kontrolne tehnike i efikasnost kontrola na svakom od sledećih nivoa:

- Na nivou entiteta ili komponenata (opšte kontrole). Kontrole na nivou entiteta ili komponenata se sastoje od procesa na nivou entiteta ili komponenata planiranih za postizanje kontrolnih aktivnosti. One su fokusirane na to kako entitet ili komponenta upravlja informacionim sistemom koji se odnosi na svaku opštu kontrolnu aktivnost. Na primer, entitet ili komponenta mogu imati proces na nivou entiteta za upravljanje konfiguracijom, uključujući uspostavljanje zaduženosti i odgovornosti za upravljanje konfiguracijom, šire politike i procedure, razvoj i primenu programa za monitoring, i moguće alate za centralizovano upravljanje konfiguracijom. Odsustvo procesa na nivou entiteta može biti glavni uzrok slabih ili nekonzistentnih kontrola; na primer, povećanjem rizika da se IS kontrole ne primenjuju konzistentno u organizaciji.
- Na nivou sistema (opšte kontrole). Kontrole na nivou sistema se sastoje od procesa za upravljanje specifičnim sistemskim resursima koji se odnose na opštu podršku sistema ili značajne aplikacije. Ove kontrole su specifičnije od onih na nivou entiteta ili komponente i obično se odnose na jednu vrstu tehnologije. U okviru nivoa sistema postoje tri dalja nivoa koja revizor treba da oceni: mreža, operativni sistem i aplikacija infrastrukture. Ova tri podnivoa se mogu definisati na sledeći način:
  - *Mreža*. Mreža je konfiguracija ili sistem međusobno povezanih komponenata. Na primer, kompjuterska mreža omogućava komuniciranje aplikacija sa raznih kompjutera.
  - *Operativni sistem*. Operativni sistem je softver koji kontroliše obavljanje kompjuterskih programa, i može da obezbeđuje razne usluge. Na primer, operativni sistem može da obezbeđuje usluge kao što su: alociranje (raspoređivanje) resursa, planiranje vremena, kontrola input-a/output-a, i upravljanje podacima.
  - *Aplikacije infrastrukture*. Aplikacije infrastrukture su softver koji se koristi da se pomogne funkcionisanje sistema, uključujući upravljanje mrežnim uređajima. Ove aplikacije uključuju baze podataka, e-mail, browsers, plug-ins, uslužne programe (utilities) i aplikacije koje nisu direktno povezane sa poslovnim procesima. Na primer, aplikacije infrastrukture omogućavaju više procesa koji se obavljaju na jednoj ili više mašina radi međusobnog delovanja u okviru mreže.
- Na nivou aplikacija poslovnih procesa. Kontrole na nivou aplikacija poslovnih procesa se sastoje od politika i procedura za kontrolu specifičnih poslovnih procesa. Na primer, upravljanje entiteta konfiguracijom treba objektivno da obezbedi da sve promene aplikacionih sistema u potpunosti budu testirane i odobrene.

Revizor treba da planira i obavi testove relevantnih kontrolnih tehnika koje su efikasne što se tiče njihovog planiranja da bi se utvrdila i njihova efikasnost u funkcionisanju.

IZVEŠTAVANJE O REZULTATIMA REVIZIJE

Posle završetka faze testiranja revizor sumira rezultate revizije, donosi zaključke o pojedinačnom zbirnom efektu svih utvrđenih slabosti IS kontrola na rizik revizije i ciljeve revizije i izveštava o rezultatima revizije. Takvo ocenjivanje obuhvata razmatranje (1) efekta slabosti utvrđenih revizorovim tekućim testiranjem, (2) praćenja slabosti prikazanih u prethodnim revizijama ili ocenjivanja koja su relevantna za ciljeve revizije, i (3) drugih nekorigovanih slabosti koje su utvrđene i/ili prikazane od strane menadžmenta ili drugih koji su relevantni za ciljeve revizije. Revizor ocenjuje efekat svih slabosti na sposobnost entiteta da postigne svaki od značajnih elemenata opštih i aplikativnih kontrola, i na rizik od neovlašćenog pristupa ključnim sistemima ili datotekama. Takođe, revizor ocenjuje potencijalne kontrolne zavisnosti.

Za svaki značajni element revizor treba da donese zaključak da li je značajni (kritični) element postignut uzimajući u obzir nivoe entiteta, sistema i aplikacija poslovnih procesa.

Revizor treba da oceni efekat odgovarajućih osnovnih kontrolnih aktivnosti koje nisu postignute. Pored toga, na bazi utvrđenih slabosti revizor treba da utvrdi efikasnost IS kontrola za svaku od pet kategorija opštih kontrola ili

8 Global Technology Audit Guide (GTAG) 8, Auditing Application Controls, The Institute of Internal Auditors, 2007, pp. 7-25.

četiri kategorije kontrola na nivou aplikacija. Ukoliko nije postignut kritični (značajan) element, u tom slučaju (1) nije verovatno da će biti postignuta odgovarajuća kategorija kontrola i (2) u odsustvu jakih kompenzirajućih kontrola verovatno je da će sve kontrole biti neefikasne. Ukoliko jedna ili više od devet kontrolnih kategorija nisu efikasno postignute, IS kontrole su neefikasne, sem ukoliko drugi faktori ne smanje rizik u dovoljnoj meri. Revizori koriste profesionalno rasuđivanje u donošenju takvih odluka.

Takođe, revizor treba da oceni da li bi ukupne slabosti mogle da imaju za rezultat neovlašćeni pristup sistemima ili datotekama koji podržavaju ključne oblasti od interesa za reviziju, što bi imalo za rezultat značajan nedostatak u internim kontrolama.

Na primer, niz slabosti može imati za rezultat da je pojedincima omogućeno da dobiju neovlašćeni eksterni pristup sistemima entiteta, da povećaju svoje privilegije da dobiju značajan nivo pristupa kritičnim kontrolnim tačkama, i shodno tome postignu pristup ključnim oblastima od interesa za reviziju. Revizori mogu da koriste pojednostavljenu mrežnu šemu sa označenim slabostima koje se odnose na ključne komponente sistema da bi dokumentovali uticaj tog niza slabosti.

Takva dokumentacija se može razvijati kako se revizija odvija što omogućava revizoru da pokaže na sistemu da slabosti u stvari postoje i može se koristiti da bi se postigao očekivani rezultat. Takođe, takva dokumentacija može da pomogne u obaveštavanju menadžmenta entiteta o odgovarajućim rizicima.

Dalje, revizor treba da oceni potencijalni uticaj utvrđenih slabosti na potpunost, tačnost, valjanost (važnost), i poverljivost podataka aplikacija relevantnih za ciljeve revizije.

ZAKLJUČAK

Kako je informaciona tehnologija napredovala organizacije su sve više postajale zavisne od kompjuterizovanih informacionih sistema u obavljanju svojeg poslovanja i u obradi, održavanju i izveštavanju o bitnim informacijama. Kao rezultat toga pouzdanost i sigurnost kompjuterskih podataka i sistema koji obrađuju, održavaju i izveštavaju o ovim podacima su postali značajni aspekt i za menadžment i revizore organizacija. Informacioni sistemi podrazumevaju specijalne vrste kontrolnih aktivnosti. Zbog toga kontrole informacione tehnologije se sastoje od dve velike grupacije: 1) opšte kontrole i 2) aplikativne kontrole.

Opšte i aplikacione kontrole su u korelaciji i potrebne su obe da bi se osigurala potpuna i tačna obrada informacija. Pošto se informaciona tehnologija brzo menja, odgovarajuće kontrole moraju da se konstantno razvijaju da bi bile efikasne.

Efikasnost opštih i aplikativnih kontrola ocenjuju revizori kroz postupke planiranja, testiranja i izveštavanja, bilo da se radi finansijska revizija ili revizija poslovanja.

LITERATURA

[1] Cascarino, R.E. (2012), Auditor's Guide to IT Auditing, 2nd ed, John Wiley & Sons Inc., Hoboken, NJ, USA

[2] Cater-Steel A. (2009), Information Technology Governance and Service Management: Frameworks and Adaptations, IGI Publishing, Hershey, PA, USA

[3] *COSO Internal Control-Integrated Framework Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commission (1992)

[4] Davis C., Schiller M., Wheeler K. (2011), IT Auditing Using Controls to Protect Information Assets, 2nd ed, Mc Graw Hill, USA

[5] GAIT for Business and IT Risk (GAIT-R), The Institute of Internal Auditors, 2008

[6] GAIT Methodology, A risk-based approach to assessing the scope of IT general controls The Institute of Internal Auditors, 2007

[7] Global Technology Audit Guide (GTAG) 1, (2012), Information Technology Risk and Controls, The Institute of Internal Auditors

[8] Global Technology Audit Guide (GTAG) 14, (2010), Auditing User-developed Applications,

[9] Global Technology Audit Guide (GTAG) 15, (2010), Information Security Governance, The Institute of Internal Auditors

[10] Global Technology Audit Guide (GTAG) 17, (2012), Auditing IT Governance, The Institute of Internal Auditors

[11] Global Technology Audit Guide (GTAG) 2, (2012), Change and Patch Management Controls: Critical for Organizational Success, The Institute of Internal Auditors

[12] Global Technology Audit Guide (GTAG) 4, (2013), Management of IT Auditing, The Institute of Internal Auditors

[13] Global Technology Audit Guide (GTAG) 8, (2007), Auditing Application Controls, The Institute of Internal Auditors

[14] Global Technology Audit Guide (GTAG)12, (2009), Auditing IT Projects, The Institute of Internal Auditors

[15] Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, COSO, September 2012.

[16] ISACA (2009), Implementing and Continually Improving IT Governance, Information Systems Audit and Control Association, Rolling Meadows, IL, USA

[17] ISACA (2009.), The Risk IT Framework, Information Systems Audit and Control Association, Rolling Meadows, IL, USA

[18] ISACA (2012), COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT, Information Systems Audit and Control Association, Rolling Meadows, IL, USA

[19] IT Governance Institute, (2006), IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, USA

[20] ITGI (2007.), COBIT Control Practices – Guidance to Achieve Control Objectives for Successful IT Governance, IT Governance Institute, Rolling Meadows, IL, USA

[21] ITGI (2007.): IT Assurance Guide using COBIT, IT Governance Institute, Rolling Meadows, IL, USA

[22] Izvršni odbor Narodne banke Srbije (NBS), (2013), Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, „Službeni glasnik RS", br. 23/2013 i 113/2013
[23] Nolan, R., McFarlan, F.W., (2005): Information Technology and the Borad of Directors, Harvard Business Review, USA
[24] Panian, Ž., Spremić, M. (2001), Kontrola i revizija informacionih sustava, Sinergija-nakladništvo, Zagreb, Hrvatska
[25] Richards, D.A., Oliphant,A.S., Le Grand, C.H., *Information Technology Controls,* Global Technology Audit Guide, The Institute of Internal Auditors, USA, March 2005.
[26] Stanišić, M., Stanojević, LJ., Revizija i primena kompjutera, Univerzitet Singidunum, Beograd, 2010.
[27] The Institute of Internal Auditors, (2009), International Professional Practices Framework (IPPF), The Institute of Internal Auditors (IIA)

INFORMATION SYSTEM CONTROLS AUDIT

Abstract:
Auditing controls of information systems includes two main groups of controls, general controls and application controls. The review process is carried out in three stages, the planning, testing and reporting. Based on the results of audit planning and other procedures performed, the auditor should identify the control categories, critical elements, control activities, and control techniques that are relevant to the IS audit. In doing this, the auditor considers the audit objectives and audit scope, the extent of IS risk and the preliminary understanding of IS controls. After testing the general and application controls the auditor shall make a conclusion about the level of effectiveness of controls and established weaknesses in controls.

Key words:
information systems, general controls, application controls, audit.