REVIZIJA OPŠTIH KONTROLA INFORMACIONIH TEHNOLOGIJA

Mile Stanišić

Univerzitet Singidunum,
Beograd, Srbija

Rezime:

Opšte kontrole informacionih tehnologija su kontrole nad komjuterskim sistemima i služe da obezbede kontinuiran i pravilan rad aplikacionih kontrola. One obično sadrže kontrole rada računarskog centra, nabavke i održavanja sistemskog softvera, obezbeđenja pristupa i kontrole razvoja i održavanja sistema aplikacija. Istraživačko pitanje odnosi se na razvoj metodologije revizije ovih kontrola. Metodologija revizije opštih kontrola treba da obuhvati sledeće faze: upoznavanje sa poslovanjem entiteta i ključnim poslovnim procesima; utvrđivanje ključnih oblasti od interesa za reviziju; preliminarnu ocenu rizika informacionih sistema; utvrđivanje kritičnih/značajnih kontrolnih tačaka i nakon utvrđivanja kontrolih ciljeva i rizičnih oblasti dolazi faza razvijanja procedura revizije i ocenjivanje i testiranje postojanja adekvatnih kontrola i njihove efikasnosti.

Ključne reči:

revizija IT, opšte kontrole IT, proces IT revizije, program revizije IT, rizici informacionih tehnologija.

1. UVOD

Informacione tehnologije se menjaju rapidnim tempom i predstavljaju nove izazove sa kojima se sve organizacije moraju suočiti, čak i ako one odluče da ne prihvate takve izmene i način da razviju IT u svojoj organizacionoj strukturi. Za njihovo funkcionisanje nephodne su adekvatne i efikasne opšte i aplikacione kontrole. Zbog veoma raširenog oslanjanja na informacione sisteme, potrebne su kontrole svih takvih sistema: finansijskih, poslovnih, za usaglašavanje, velikih i malih. Kada je tehnologija ugrađena u poslovne procese entiteta, kao što je robotska automatizacija u pogonu za proizvodnju, kontrolne aktivnosti su potrebne da bi se smanjio rizik kojim sama tehnologija neće nastaviti da pravilno upravlja, da bi se podržalo postizanje ciljeva organizacije.

Stvari su se promenile početkom 1970-ih godina sa prevarom Equity Funding. Eksterni revizori su primenili svoje sopstvene revizijske softverske programe za pregled fajlova Equity Funding da bi otkrili veliku prevaru sa nevažećim podacima evidentiranim u datotekama sistema [1]. Kao posledica afere Equity Funding organizacije, kao što su American Institute of Certified Public Accountants (AICPA) i Institute of Internal Auditors (IIA) su počele da naglašavaju značaj obavljanja pregleda tada

Odgovorno lice:
Mile Stanišić

e-pošta:
mile.stanisic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2019-195-202

nazvanih kontrolama obrade podataka i aplikacionim kontrolama. Nova profesionalna specijalnost nazvana kompjuterskom revizijom je lansirana i svake godine metodologija IT revizije se sve više usavršava bilo da se obavlja finansijska ili poslovna revizija. Istraživačno pitanje upravo se odnosi na razvoj metodologije revizije opštih IT kontrola.

2. RAZUMEVANJE OPŠTIH KONTROLA INFORMACIONIH SISTEMA

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.

Kontrola se definiše kao proces uključen u upravljanje rizicima i obavljan od strane uprave u cilju ublažavanja rizika do prihvatljivog nivoa. Kontrole informacionih tehnologija (IT kontrole) se obično klasifikuju kao opšte ili aplikacione kontrole, opisane kao [2]:

- *Opšte kontrole,* koje se primenjuju na sve sistemske komponente, procese i podatke za datu organizaciju ili sistemsko okruženje.
- *Aplikacione kontrole,* odnose se na područje individualnih poslovnih procesa ili aplikacionih sistema i uključuju kontrole unutar aplikacije u vezi sa ulaznim podacima, obradom podataka i izlaznim rezultatima.

Pored navedene podele kontrola na opšte i aplikacione kontrole, COSO klasifikuje kontrole na automatizovane i manuelne. Mnoge kontrolne aktivnosti u entitetu su delimično ili u celini automatizovane korišćenjem tehnologije. Ovi postupci su poznati kao automatizovane kontrolne aktivnosti ili automatizovane kontrole. Automatizovane kontrole obuhvataju automatizovane transakcijske kontrole koje se odnose na finansijske procese, kao što je usaglašavanje na tri načina koje se obavlja u okviru ERP sistema koji podržava podprocese nabavki i plaćanja, i kompjuterizovane kontrole u operativnim procesima ili procesima usaglašavanja sa propisima i zakonima, kao što je provera da li pravilno funkcioniše pogon za električnu energiju (napajanje strujom). Ponekad je kontrolna aktivnost potpuno automatizovana, kao kad sistem otkriva grešku prilikom prenosa podataka, odbacuje prenos, i automatski zahteva novi prenos. Međutim, postoji nekad kombinacija automatizovanih i manuelnih postupaka. Na primer, sistem automatski otkriva grešku prilikom prenosa, ali neko mora ručno da ponovi prenos. U nekom drugom slučaju manuelna kontrola zavisi od informacija iz sistema, kao što su kompjuterski izveštaji kao podrška analizi planiranog u odnosu na ostvareno [3].

Većina poslovnih procesa koristi kombinaciju automatizovanih i manuelnih kontrola u zavisnosti od raspoloživosti tehnologije u entitetu. Automatizovane kontrole su pouzdanije, zavisno od toga da li su primenjene i funkcionišu opšte kontrole tehnologije, pošto manje zavise od ljudskog rasuđivanja i manje su podložne ljudskim greškama, i po pravilu su efikasnije. Pored ovih podela kontrola postoje i podele na preventivne, detektivne i korektivne kontrole, kao i podela svih kontrola na: kontrole upravljanja, menadžment kontrole i tehničke kontrole [4].

U revizorskoj profesiji se počelo da gleda na IT kontrole u smislu kontrola u okviru specifične aplikacije i onoga što nazivamo opštim kontrolama ili kontrolama infrastrukture, kontrolama koje se odnose na funkcionisanje svih informacionih sistema. IT opšte ili kontrole infrastrukture se odnose na celokupno IT poslovanje i obuhvataju [5]:

Kontrole rada računarskog centra. One sadrže grupu poslova i njihovo planiranje, operaterske poslove, procedure za backup i oporavak i planiranje za slučaj nepredviđenih okolnosti ili oporavak od katastrofičnih situacija. U kompleksnom okruženju, ove kontrole se odnose i na planiranje kapaciteta i raspodelu i korišćenje sredstava. U najsavremenijem tehnološkom okruženju, redosled izvršavanja poslova je automatizovan a jezik za upravljanje obradom je on-line. Alati za upravljanje memorisanjem podataka automatski učitavaju datoteke sa podacima na jedinice za memorisanje sa brzim pristupom u očekivanju sledećeg zadatka. Kontrolor smene više ne mora da ručno startuje protokol konzole zato što nije odštampan; protokol ostaje u sistemu. Stotine poruka bljesne svake sekunde na zajedničkoj konzoli koja opslužuje više centralnih računara. Miniračunari rade cele noći bez nadzora.

Kontrole sistemskog softvera. One se sastoje od kontrola za efikasnu nabavku, implementaciju i održavanje sistemskog softvera – operativni sistem, sistem za upravljanje bazama podataka, telekomunikacioni softver,

zaštitni softver i uslužni programi - koji upravlja sistemom i omogućuje funkcionisanje aplikacija. Glavni dirigent rada sistema, sistemski softver, takođe upravlja podizanjem sistema, i funkcijama trekinga i monitoringa. Sistemski softver izveštava o korišćenju uslužnih programa, tako da ako neko pristupi ovim moćnim funkcijama koje menjaju podatke, njihovo korišćenje će u najmanju ruku biti zabeleženo i prijavljeno da se ispita.

Kontrole bezbednosti pristupa. Ove kontrole su dobile na važnosti sa razvojem telekomunikacionih mreža. Korisnici sistema mogu biti na drugom kraju zemlje ili u susednoj sobi. Efikasne kontrole bezbednosti pristupa mogu zaštiti sistem sprečavanjem neodgovarajućeg pristupa i neovlašćenog korišćenja sistema. Ako su dobro osmišljene mogu zaustaviti hakere i druge prestupnike.

Adekvatne mere za kontrolu pristupa, kao što su česta promena brojeva koji se pozivaju ili uvođenje povratnog pozivanja – gde sistem uzvraća poziv potencijalnom korisniku preko ovlašćenog broja, umesto da se dozvoli direktan pristup sistemu – mogu biti efikasne metode za sprečavanje neovlašćenog pristupa. Kontrole bezbednosti pristupa ograničavaju ovlašćene korisnike samo na pristup aplikacijama ili aplikativnim funkcijama potrebnim da obave svoj posao, što je podrška adekvatnoj podeli zaduženja. Treba da postoji učestalo i blagovremeno preispitivanje profila korisnika koji omogućuju ili zabranjuju pristup. Bivši ili nezadovoljni radnici veća su pretnja sistemu nego hakeri; lozinke i korisničko ime radnika koji tu više ne rade treba odmah ukinuti. Sprečavanjem neovlašćenog korišćenja i menjanja sistema, integritet podataka i programa je zaštićen.

Kontrole za razvoj i održavanje aplikacija. Razvoj i održavanje sistema aplikacija je po tradiciji veoma skupa oblast za većinu organizacija. Ukupni troškovi za MIS resurse, potrebno vreme, stručnost osoblja za obavljanje tih zadataka i potrebni hardver i softver su znatna stavka. Da bi kontrolisali ove troškove, mnogi entiteti imaju neku vrstu metodologije za razvoj sistema. Ona daje okvir za projektovanje i implementaciju sistema, navodeći u kratkim crtama specifične faze, zahteve u pogledu dokumentacije, odobrenja i kontrolne tačke za praćenje projekta razvoja ili održavanja. Ova metodologija treba da omogući adekvatnu kontrolu nad izmenama sistema što podrazumeva potrebno odobrenje za traženje izmena, razmatranje promena, odobrenja, rezultata testiranja i protokola za implementaciju da bi bilo sigurno da su izmene izvršene korektno.

3. TRETIRANJE OPŠTIH KONTROLA TEHNOLOGIJE U COSO 2013

Prema COSO-u opšte kontrole tehnologije obuhvataju kontrolne aktivnosti koje se odnose na infrastrukturu tehnologije, upravljanje zaštitom, i kupovinu, razvoj i održavanje tehnologije. One se primenjuju na sve tehnologije – od IT aplikacija na glavnom kompjuteru, do klijenta/servera, desktop-a, kompjutera krajnjih korisnika, portabl kompjutera, i okruženja mobilnih uređaja, do operativne tehnolgije, kao što su kontrolni sistemi pogona (fabrika) ili robotike za proizvodnju. Nivo i rigoroznost kontrolnih aktivnosti se razlikuju za svaku ovu tehnologiju zavisno od raznih faktora, kao što je kompleksnost tehnologije i rizik osnovnih poslovnih procesa koje podržavaju. Slično kontrolama poslovnih tarnsakcija opšte kontrole tehnologije mogu obuhvatati i manuelne i automatizovane kontrolne aktivnosti.

Opšte kontrole informacionih tehnologija COSO razmatra u principu 11 COSO okvira postavljajući određena pitanja. Organizacija vrši izbor i razvija opšte kontrolne aktivnosti koje se odnose na tehnologiju kao podršku postizanju ciljeva. Sledeća pitanja mogu pomoći menadžmentu prilikom utvrđivanja da li je princip 11 prisutan i da li funkcioniše [6]:

- *Utvrđivanje zavisnosti između korišćenja tehnologije u poslovnim procesima i opštih kontrola tehnologije* - Menadžment se upoznaje i utvrđuje zavisnost i povezanost između poslovnih procesa, automatizovanih kontrolnih aktivnosti i opštih kontrola tehnologije.
- *Utvrđivanje relevantnih kontrolnih aktivnosti koje se odnose na infrastrukturu tehnologije* - Menadžment vrši izbor i razvija kontrolne aktivnosti koje se odnose na infrastrukturu tehnologije, koje su planirane i primenjuju se da bi pomogle da se obezbedi kompletnost, tačnost i raspoloživost tehnologije.
- *Utvrđivanje relevantnih kontrolnih aktivnosti koje se odnose na proces upravljanja zaštitom* - Menadžment vrši izbor i razvija kontrolne aktivnosti koje su planirane i primenjuju se da bi se ograničila prava pristupa tehnologiji ovlašćenim korisnicima proporcionalno njihovim odgovornostima za posao i da bi se zaštitila sredstva entiteta od spoljnih opasnosti.
- *Utvrđivanje relevantnih kontrolnih aktivnosti koje se odnose na proces nabavki, razvoja i održavanja* - Menadžment vrši izbor i razvija kontrolne

aktivnosti koje se odnose na akviziciju (nabavke), razvoj i održavanje tehnologije i njene infrastrukture da bi se postigli ciljevi menadžmenta.

Pouzdanost tehnologije u okviru poslovnih procesa, uključujući automatizovane kontrole, zavisi od prisustva i pravilnog funkcionisanja aktivnosti opštih kontrola koje se odnose na tehnologiju, i na koje se ovde poziva kao na opšte kontrole tehnologije. Opšte kontrole tehnologije se moraju rasporediti tako da automatizovane kontrole funkcionišu pravilno kada su prvi put razvijene i primenjene (na primer: pomenuta automatizovana kontrola vrši provere editovanja podataka usaglašavanja sa pravom datotekom transakcija ili stalnih podataka, svaka poruka o greškama odražava šta je pogrešno, i o svim izuzecima se izveštava u skladu sa politikama entiteta.) Opšte kontrole tehnologije takođe pomažu da informacioni sistemi i dalje pravilno funkcionišu pošto su primenjeni. Automatizovana kontrola za usaglašavanje transakcija će funkcionisati pravilno samo ako su opšte kontrole tehnologije planirane, primenjene i funkcionišu tako da se koriste prave datoteke u procesu usaglašavanja i da su datoteke kompletne i tačne. Takođe, pravilna zaštita omogućava pristup sistemu samo onima kojima je to potrebno, i smanjuje mogućnost neovlašćenog editovanja datoteka. Kontrolne aktivnosti koje se odnose na promene tehnologije pomažu da ona i dalje funkcioniše kako je planirano.

4. PLANIRANJE REVIZIJE KONTROLA INFORMACIONIH SISTEMA

Ciljevi planiranja su da se utvrde ciljevi revizije, upozna sa ključnim poslovnim procesima, utvrde ključne oblasti od interesa za reviziju, prelimiranrno oceni kontrolni rizik, utvrde kritične kontrolne tačke i sačini program revizije. Proces revizije kontrola informacionih tehnologija prolazi kroz nekoliko faza: faza planiranja, terenski rad i dokumentacija, otkrivanje problema i provera valjanosti, razvoj rešenja i praćenje problema [7].

A. Upoznavanje sa poslovanjem entiteta i ključnim poslovnim procesima

Revizor treba da se upozna i dokumentuje saznanja o entitetu dovoljna da planira i obavi reviziju u skladu sa primenjivim revizijskim standardima i zahtevima. Prilikom planiranja revizije revizor dobija informacije koje će obezbediti celokupnu sliku entiteta, kao što su: njegov zadatak (misija), veličina i lokacija, organizacija, poslovanje, strategije, rizici, i struktura internih kontrola. Upoznavanje sa poslovanjem entiteta prilikom planiranja procesa omogućava revizoru da utvrdi, reaguje i reši probleme u ranoj fazi revizije.

Revizorovo upoznavanje sa entitetom uključuje sledeće:

- menadžment i organizaciju entiteta,
- eksterne i interne faktore koji utiču na poslovanje entiteta, i
- ključne poslovne procese.

Da bi planirao reviziju revizor se upoznaje sa organizacionom strukturom entiteta i IT funkcijom, uključujući ključne članove entiteta i IT menadžmenta. Revizorov glavni cilj je da upozna kako se upravlja entitetom i kakva je organizaciona struktura.

B. Utvrditi ključne oblasti od interesa za reviziju

Revizor treba da utvrdi ključne oblasti od interesa za reviziju a to su one koje su značajne za postizanje cljeva revizije (na primer: opšti sistemi za podršku i sistemi i datoteke aplikacija poslovnih procesa (ili njihove komponente)). Za finansijsku reviziju to bi uključivalo ključne finansijske aplikacije i podatke i odgovarajuće *feeder* sisteme odnosno sisteme koji pružaju informacije ili podatke koji podržavaju glavnu aplikaciju. Na primer, u sistemu platnog spiska sistem za evidenciju radnog vremena i pisustva je sistem dodavanja za glavnu aplikaciju. Za reviziju poslovanja to bi obuhvatalo ključne sisteme koji će vervatno biti značajni za ciljeve revizije. Za svaku ključnu oblast od interesa za reviziju revizor treba da dokumentuje opšte sisteme za podršku i važnije aplikacije i datoteke uključujući (1) operativne lokacije svakog ključnog sistema ili datoteke, (2) značajne komponente odovarajućeg hardvera i softvera (na primer: zaštitni zid *(firewalls)*, ruteri, hostovi, operativni sistemi), (3) druge značajne sisteme ili resurse na nivou sistema koji podržavaju ključne oblasti od interesa, i (4) ranije prikazane probleme revizije.

C. Preliminarno ocenjivanje rizika informacionih sistema

Revizor treba da preliminarno oceni i dokumentuje prirodu i nivo IS rizika koji se odnosi na ključne oblasti od interesa za reviziju. Indikatori mogu da upozore na visok nivo rizika u procesima informacione tehnologije. Njih treba razmotriti prilikom ocenjivanja rizika opštih

IT kontrola [8]. IS rizik 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 materijalog 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. Globalni vodič za reviziju tehnologija (GTAG) je u svom dokumentu "Rizici i kontrole informacionih tehnologija dao analizu rizika informacionih sistema [9].

Preliminarni pregled IT opštih kontrola podrazumeva ocenjivanje kontrolnog rizika. Njegov cilj je da se revizor dobro upozna ili dobije opštu sliku okruženja IT kontrola. Brings prikazuje široki spektar ciljeva pregleda opštih kontrola IT sistema od kojih se ovde prikazuju samo neki [10]:

1. Utvrditi da li je IT oprema smeštena na bezbednom i kontrolisanom prostoru.
2. Prodiskutujte o procedurama za fizičku kontrolu i kontrolu okruženja sa menadžmentom informacionih sistema da biste utvrdili tekuće politike, važnije promene i druge buduće planove.
3. Obiđite prostor gde se nalazi serverska oprema i utvrdite koje su jake a koje slabe strane fizičke zaštite, uključujući:
   - » Postojanje mehanizama za zaključavanje radi omogućavanja pristupa kompjuterskom prostoru samo ovlašćenim licima
   - » Postavljanje opsežnih zidova i prozora u kompjuterskom prostoru da bi se ograničio pristup
   - » Postavljanje mrežnih transformatora, vodenog hlađenja, ukoliko je potrebno, i ventilacije radi pravilne zaštite
   - » Postojanje detektorske opreme, uključujući detektore za kontrolisanje toplote i dima, i lokalnu zaštitu.
4. Obavit kratak pregled evidencija o održavanju da biste se uverili da se fizičke i kontrole okruženja nadgledaju i održavaju.
5. Takođe preko intervjua opisati telekomunikacione mreže kompjuterskog sistema, uključujući rutere, povezanost sa radnim stanicama, kompjuterske centre.
6. Obaviti pregled standarda za dokumentaciju za ponovni početak (restart) i nastavak poslovanja
7. Obaviti pregled procedura, automatizovanih ili manuelnih, radi uvođenja novih aplikacija ili revidiranih aplikacija u proizvodnju da biste utvrdili da li postoji pregled poslovanja u skladu sa standardima.
8. Utvrditi da li politike zabranjuju kompjuterskom operativnom osoblju da obavljaju zadatke programiranja ili neovlašćene poslove.
9. Utvrditi procedure kojima se zabranjuje neovlašćeni unos ili pristup proizvodnim datotekama i programima.

Pre direktnog upuštanja u detaljnu ocenu opštih kompjuterskih kontrola, korisno je razumeti rizike povezane sa IT i ciljeve kontrole na relativno visokom nivou. Neka od pitanja na koja treba da odgovorite uključuju:

- Da li je bilo značajnih pormena u sistemu IT u subjektu, uključujući promene na hardveru, softevru, u procesima i osoblju? Ako jeste, koje opšte rizike te promene stvaraju? Ako nije bilo značajnih promena, koji su raniji rizici ostali? Kako se rizici identifikuju i kako se njima upravlja?
- Koliko različitih kompjuterskih platformi ili okruženja postoji u subjektu? Kakav je interfejs višestrukih sistema, na primer, kako se razmenjuju podaci i kako se ta razmena kontroliše?
- Šta može da umanji pouzdanost sistema IT u subjektu ili da na drugi način negativno utiče na sposobnost subjekta da prikupi, obradi i drži podatke?
- Kako se može ugroziti integritet sistema IT u subjektu? Koji postojeći rizici mogu da utiču na sposobnost subjekta da zaštiti svoje podatke i sisteme od neovlašćenog pristupa, oštećenja ili gubitka?

Ocenjivanje IS rizika koje se odnosi na reviziju se razlikuje od ocenjivanje rizika menadžmenta. Prilikom ocenjivanja IS rizika od revizora se ne zahteva ili očekuje da ponovo obavi ocenjivanje rizika menadžmenta. Radije će revizor preliminarno ocenjivati IS rizik korišćenjem podataka koji će biti sakupljeni za vreme planiranja revizije, to uključuje korišćenje ocena rizika entiteta i obavljanje drugih procedura revizije. Revizorova ocena rizika treba da odražava uticaj efikasnosti IS kontrola na ciljeve revizije.

Za svaki utvrđeni rizik revizor treba da dokumentuje prirodu i nivo rizika; uslove koji povećavaju taj rizik; i (specifične infomacije ili poslovanje na koje utiče).

Revizor takođe treba da dokumentuje kompenzirajuće kontrole ili druga razmatranja koja mogu da ublaže efekte utvrđenih rizika.

D. Utvrditi kritične kontrolne tačke

Revizor treba da utvrdi i dokumentuje kritične kontrolne tačke prilikom planiranja informacionih sistema entiteta na bazi revizorovog upoznavanja sa takvim sistemima, ključnim oblastima od interesa za reviziju i IS rizikom. Značajne kontrolne tačke su one kontrolne tačke sistema koje, ukoliko su dovedene u pitanje (kompromitovane), omogućavaju pojedincima neovlašćeni pristup ili da obavljaju neodobrene ili neodgovarajuće aktivnosti na sistemima ili podacima entiteta što može voditi direktno ili indirektno ka neovlašćenom pristupu ili ka modifikovanjima ključnih oblasti od interesa za reviziju. Kontrolne tačke po pravilu obuhvataju eksterne tačke pristupa mrežama, međusobnu povezanost sa drugim eksternim i internim sistemima, komponente sistema koje kontrolišu tok informacija kroz mreže entiteta ili do ključnih oblasti od interesa za reviziju, značajne uređaje za čuvanje i obradu, i odgovarajuće operativne sisteme, aplikacije infrastrukture, i relevantne aplikacije poslovnih procesa.

E. Upoznavanje sa IS kontrolama

Revizor treba da se upozna sa i dokumentuje plan IS kontrola entiteta, uključujući organizaciju, osoblje, odgovornosti, ovlašćenja i resurse funkcije za upravljanje zaštitom. Revizor treba da dokumentuje preliminarna saznanja o kontrolama u entitetu (ili kontrolama komponeneta ukoliko se vrši revizija samo određene komponente), odgovarajućem upravljanju zaštitom, kontrolama pristupa, upravljanju konfiguracijama, podeli dužnosti, i planiranju nepredviđenih događaja.

Revizor treba da se upozna sa planom svake od dve vrste IS kontrola (opšte i kontrole aplikacija poslovnih procesa) do stepena potrebnog za privremeno zaključivanje da li je verovatno da su ove kontrole efikasne. Ukoliko je verovatno da su efikasne revizor treba da razmotri odnosno uzme u obzir specifične IS kontrole prilikom utvrđivanja da li su postignuti relevantni kontrolni ciljevi. Ukoliko nije verovatno da su efikasne revizor treba da se u dovoljnoj meri upozna sa kontrolnim rizikom koji je rezultat IS kontrola, da bi ocenio revizijski rizik, planirao odgovarajuće procedure za reviziju i pripremio odgovarajuće nalaze.

Na bazi ovih saznanja revizor treba da preliminarno oceni da li je verovatno da su IS kontrole efikasne da bi utvrdio prirodu, vreme i obim testiranja. Ova ocena je bazirana pre svega na diskusijama sa osobljem u entitetu, uključujući menadžere za programe, operatore sistema, menadžere za informacione resurse, i menadžere za zaštitu sistema; na posmatranjima IT poslovanja i kontrola; na pregledu primera dokaza obavljanja kontrola; na ranijim revizijama ili radu drugih.

5. TESTIRANJE KONTROLA INFORMACIONOG SISTEMA

Revizor treba da planira i obavi testove ključnih kontrola, da proveri da li su adekvatno planirane i da li efikasno funkcionišu. Obično je efikasnije da revizor testira IS kontrole slojevito počev od opštih kontrola na nivou entiteta i sistema, zatim opšte kontrole na nivou aplikacija poslovnih procesa, i da zaključi sa testovima kontrola aplikacija poslovnih procesa, interfejsa i sistema za upravljanje podacima na nivou aplikacija poslovnih procesa. Takvo testiranje strategije se može koristiti zato što neefikasne IS kontrole na svakom nivou (sloju) uglavnom isključuju efikasne kontrole na sledećem nivou.

Ocenjivanje opštih kontrola uključuje sledećih pet kategorija opštih kontrola:

- upravljanje zaštitiom kojim se obezbeđuje okvir i kontinuirani ciklus aktivnosti za upravljanje rizikom, razvoj politika za zaštitu, podelu odgovornosti, i monitoring adekvatnosti kompjuterskih kontrola u entitetu;
- kontrole pristupa koje ograničavaju ili otkrivaju pristup kompjuterskim resursima (podacima, programima, opremi i drugim kapacitetima), i time ih štite od neovlašćenog modifikovanja, gubitka i obelodanjivanja;
- upravljanje konfiguracijama koje sprečava neovlašćene promene resursa informacionih sistema (na primer: softverskih programa i hardverskih konfiguracija) i obezbeđuje objektivno uveravanje da su konfiguracije i funkcionisanje bezbedni kako je planirano;
- podela dužnosti koja obuhvata politike, procedure i organizacionu strukturu za upravljanje ko može da kontroliše ključne aspekte rada kompjutera; i
- planiranje nepredviđenih događaja tako da kada se desi neočekivani događaj značajno poslovanje se nastavlja bez prekida ili se brzo nastavi, i značajni i osetljivi podaci su zaštićeni.

Za svaki značajni element revizor donosi zaključak o efikasnosti odgovarajućih kontrola u entitetu na nivou entiteta, sistema i aplikacija. Ukoliko određeni značajan element nije postignut odgovarajuća kategorija kontrola verovatno neće biti postignuta. Revizor treba da koristi profesionalno rasuđivanje za donošenje takvih odluka.

A. Testovi opštih kontrola na nivou entiteta i sistema

Revizor može da testira opšte kontrole kombinovanjem procedura uključujući posmatranje, ispitivanja, inspekciju (koja uključuje pregled dokumentacije na sistemima i procedurama), i ponovnog izvođenja korišćenjem odgovarajućih softvera. Mada se uzorkovanje obično ne koristi za testiranje opštih kontrola revizor može da koristi uzorkovanje da bi testirao izvesne kontrole kao što su one koje obuhvataju odobrenja.

Ukoliko opšte kontrole na nivou entiteta i sistema nisu planirane i ne funkcionišu na efikasan način kako je planirano, revizor će uglavnom biti u nemogućnosti da bude zadovoljan da su kontrole na nivou aplikacija poslovnih procesa efikasne. U takvim slučajevima revizor treba (1) da utvrdi i dokumentuje prirodu i nivo rizika koji je rezultat neefikasnih opštih kontrola, i (2) da utvrdi i testira sve manuelne kontrole koje postižu kontrolne ciljeve koje je trebalo da postignu.

Međutim, ukoliko manuelne kontrole ne postižu kontrolne ciljeve revizor treba da utvrdi da li su specifične IS kontrole planirane da postignu ciljeve. Ukoliko nisu, revizor treba da pripremi odgovarajuće nalaze uglavnom da bi obezbedio preporuke za unapređenje internih kontrola. Ukoliko su specifične kontrole planirane da postignu ciljeve, ali su u stvari neefikasne zbog slabih opštih kontrola, testiranje po pravilu ne bi bilo potrebno sem da bude podrška nalazima.

B. Testovi opštih kontrola na nivou aplikacija poslovnih procesa

Ukoliko revizor dođe do povoljnog zaključka o opštim kontrolama na nivou entiteta i sistema on treba da oceni i testira efikasnost opštih kontrola za one aplikacije u okviru kojih kontrole aplikacija poslovnih procesa ili kontrole korisnika treba da budu testirane. Ukoliko opšte kontrole ne funkcionišu na efikasan način u okviru aplikacije poslovnih procesa, kontrole aplikacija poslovnih procesa i kontrole korisnika će biti neefikasne. Ukoliko revizija IS kontrola predstavlja deo finansijske revizije ili revizije poslovanja specijalista (specijalni stručnjak) za IS kontrole treba da prodiskutuje o prirodi i nivou rizika koji su rezultat neefikasnih opštih kontrola, sa timom za reviziju. Revizor treba da odluči da li će da nastavi sa ocenjivanjem kontrola aplikacija poslovnih procesa i kontrola korisnika.

C. Testovi kontrola aplikacija poslovnih procesa

Revizor obično treba da obavi testove onih kontrola aplikacija poslovnih procesa (poslovni proces, interfejs, upravljanje podacima), i kontrola korisnika potrebnih da se postignu kontrolni ciljevi gde je utvrđeno da su opšte kontrole na nivou entiteta, sistema i aplikacija efikasne.

Ukoliko nije verovatno da su IS kontrole efikasne revizor treba da se dovoljno upozna sa kontrolnim rizicima koji su rezultat informacionih sistema:

- da bi utvrdio uticaj na ciljeve revizije,
- planirao procedure revizije,
- pripremio odgovarajuće nalaze.

Takođe, u takvim okolnostima, revizor razmatra da li manuelne kontrole postižu kontrolne ciljeve uključujući manuelne kontrole koje mogu ublažiti slabosti u IS kontrolama. Ukoliko nije verovatno da su IS kontrole efikasne i ukoliko manuelne kontrole ne postižu kontrolne ciljeve revizor treba da utvrdi i oceni specifične IS kontrole koje su planirane da se postignu kontrolni ciljevi da bi se dale preporuke za unapređenje internih kontrola.

IS kontrole koje nisu efikasno planirane nije potrebno testirati. Ukoliko je revizor utvrdio u prethodnoj godini da kontrole u nekoj posebnoj računovodstvenoj aplikaciji nisu bile efikasne i ukoliko menadžment ukaže da kontrole nisu značajno unapređene revizor ne treba da ih testira.

6. IZVEŠTAJ O REZULTATIMA REVIZIJE

Kao konačnu etapu revizije kontrola revizor treba da donese zaključak o pojedinačnom zbirnom efektu utvrđenih slabosti u opštim IT kontrolama i postizanju utvrđenih kontrolnih ciljeva. Pre sastavljanja izveštaja o reviziji obično je prikladno obavestiti o utvrđenim slabostima menadžment da bi se dobila njihova saglasnost sa činjenicama i da se sazna da li postoje dodatni faktori koji su relevantni za revizorovo ocenjivanje efekta slabosti. Informisanje menadžmenta o utvrđenim slabostima po pravilu uključuje sledeće informacije: prirodu i nivo rizika; kontrolne ciljeve, kontrolnu aktivnost, nalaze i preporuke.

7. ZAKLJUČAK

Opšte kontrole su primenjuju na nivou entiteta, sistema i aplikacija, i stoga revizor treba da uzme u obzir opšte kontrole na svakom od ovih nivoa. Kontrolne tehnike i odgovarajući revizijski testovi se razlikuju prema nivou na koji se primenjuju. Prilikom planiranja ocenjivanja IT kontrola revizor utvrđuje oblasti od interesa za reviziju i kritične kontrolne tačke. Prilikom utvrđivanja ovih oblasti revizor razmatra aplikacije poslovnih procesa koje su relevantne za ciljeve revizije. Prilikom planiranja ocenjivanja opštih kontrola revizor razmatra najefektivniji i najefikasniji način da skupi dokaze da bi utvrdio efikasnost opštih IT kontrola kritičnih kontrolnih tačaka.

LITERATURA

[1] Stanišić, M., Stanojević, LJ., Revizija i primena kompjutera, Univerzitet Singidunum, Beograd, 2010, str. 14-15

[2] Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, Paul J. Sobel, Internal Auditing: Assurance & Advisory Services, Internal Audit Foundation, USA, 2017, p. 7-14.

[3] COSO Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, COSO, September 2012, p. 94.

[4] David A. Richards, Alan S. Oliphant, Charles H. Le Grand, Global Technology Audit Guide (GTAG) 1, Information Technology Risk and Controls, The Institute of Internal Auditors, 2012, pp. 16-17.

[5] *COSO Internal Control-Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, 1992, pp. 52-53.

[6] COSO Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, COSO, September 2012, p. 97.

[7] Chris Davis, Mike Schiller, IT Auditing: Using Controls to Protect Information Assets, Second Edition, The McGraw-Hill Companies, 2011, pp. 35-60.

[8] The Institute of Internal Auditors (IIA), GAIT Methodology, A risk-based approach to assessing the scope of IT general controls, The Institute of Internal Auditors, 2007. pp. 18.

[9] Global Technology Audit Guide (GTAG) 1, Information Technology Risk and Controls, The Institute of Internal Auditors, 2012, pp. 10-12.

[10] Robert r. Moeller Brink's Modern Internal Auditing, John Wiley & Sons, Inc., Hoboken, New Jersey, 2016, pp. 642-643.