Mile Stanišić, Nataša Spahić, Milena Tomin

PREGLEDNI RAD
UDK: 657.6:004.4
004.42
doi: 10.5937/Rev1986007S

REVIZIJA KONTROLA APLIKATIVNOG SOFTVERA

UVOD

Tokom poslednjih nekoliko godina, kompanije širom sveta potrošile su milijarde dolara za nadogradnju ili instalaciju novih poslovnih aplikativnih sistema iz različitih razloga, od taktičkih ciljeva, kao što su usklađivanje sa SOX-om, do strateških aktivnosti, kao što je korišćenje tehnologije radi ostvarivanja prednosti kompanije na tržištu. Kompanije se danas više oslanjaju na kontrole aplikacija nego u prošlosti prilikom upravljanja rizikom, zbog njihove inherentne efikasne prirode, ekonomičnosti i pouzdanosti.

IT aplikacije imaju uticaja na mnoge procese u preduzeću. Ove aplikacije se kreću od relativno jednostavnih, koje se tiču samo jednog segmenta procesa, do veoma složenih, koje predstavljaju set međusobno povezanih aplikacija i ogromne baze podataka za kontrolu praktično svih procesa u preduzeću. Iako procedure za opštu IT kontrolu obuhvataju najbolje prakse za celokupno IT poslovanje, specifični kontrolni procesi treba takođe da budu povezani sa svakom instaliranom IT aplikacijom. Da bi obavili preglede internih kontrola u specifičnim oblastima, interni revizori moraju da poseduju sposobnosti da razumeju, ocene i testiraju kontrole IT aplikacija. Pregledi specifičnih aplikativnih kontrola često mogu biti značajniji za ukupne ciljeve revizije od opštih IT kontrola. Cilj ovog rada je da se pruže smernice za razvoj i izvršenje periodičnih revizija kontrola aplikacija kako bi se utvrdilo da li su kontrole aplikacija adekvatno dizajnirane i da li efikasno funkcionišu.

DEFINICIJA KONTROLA APLIKATIVNOG SOFTVERA

Kontrole aplikativnog softvera predstavljaju strukturu, politike i procedure koje se primenjuju kod posebnih pojedinač-

REZIME

Ključne reči: kontrole aplikativnog softvera, revizija, IT kontrole, IT rizici, CAATT

Danas se svi poslovni procesi obavljaju sa savremenim aplikativnim softverom. Svaka aplikacija mora da ima adekvatno dizajnirane interne kontrole, čija je uloga da smanji rizike poslovnog procesa na prihvatljiv nivo. Interne kontrole aplikativnog softvera odnose se na kontrole ulaza, kontrole za obradu i kontrole izlaza. Uveravanje o njihovoj adekvatnosti i efikasnosti funkcionisanja treba da daje interna revizija. Interni revizori, da bi izvršili reviziju kontrola aplikacija, moraju posedovati dovoljno znanja i veština o ključnim informaciono-tehnološkim rizicima i revizorskim tehnikama zasnovanim na tehnologiji i primeni softvera za reviziju. Metodologija obavljanja revizije kontrola aplikativnog softvera je bazirana na značajnim rizicima i ključnim kontrolama. Proizvod revizije je izveštaj revizije koji se upućuje višem rukovodstvu. Rezultati izveštaja su od suštinskog značaja u procesu upravljanja rizicima i donošenju budućih poslovnih odluka o adekvatnom stepenu oslanjanja na revidirane kontrole aplikacija.

Dr Mile Stanišić, vanredni profesor, Univerzitet Singidunum, Beograd, mailto:mile.stanisic@hotmail.com
dr Nataša Spahić, interni revizor, Erste banka, Novi Sad, e-mail: natasa.spahic@dmi.uns.ac.rs
Milena Tomin, Vojvođanska banka, Novi Sad, stariji savetnik za bezbednost, e-mail: milenaa.tomin@gmail.com

nih aplikativnih sistema i direktno su povezane sa pojedinačnim kompjuterskim aplikacijama. Ove kontrole su uglavnom planirane da spreče, otkriju i koriguju greške i nepravilnosti za vreme toka informacija kroz informacione sisteme.

Aplikacije poslovnih procesa predstavljaju softvere koji se koriste za obradu poslovnih informacija kao podrška određenim poslovnim procesima. Kontrole aplikacija odnose se na specifične kompjuterske aplikacije. Cilj internih kontrola nad aplikacionim sistemima je da se obezbedi:

- da svi podaci ulaza budu tačni, kompletni, odobreni i korektni;
- da svi podaci budu obrađeni prema planu;
- da svi memorisani podaci budu tačni i kompletni;
- da izlaz bude tačan i kompletan;
- da se vodi evidencija, kako bi se pratio proces podataka od ulaza do memorije, i eventualnog izlaza.

Kontrole aplikacija i način na koji informacije prolaze kroz informacione sisteme mogu se klasifikovati u tri faze, ciklusa, obrade:

- Input: podaci su autorizovani, konvertovani u automatizovani oblik, i uneseni u aplikaciju tačno, potpuno i pravovremeno;
- Obrada: podaci su pravilno kompjuterski obrađeni i datoteke su korektno ažurirane; i
- Autput: datoteke i izveštaji proizvedeni ovom aplikacijom odražavaju transakcije ili događaje koji su se stvarno dogodili i tačno odražavaju rezultate obrade, a izveštaji se kontrolišu i šalju ovlašćenim korisnicima.

Kontrole aplikacija se mogu klasifikovati po vrstama ciljeva kontrole, uključujući i to da li su transakcije i informacije autorizovane, potpune, tačne i valjane. Kontrole autorizacije odnose se na valjanost transakcija i pomažu da se osigura da transakcije predstavljaju događaje koji su se stvarno dogodili u datom periodu. Kontrole potpunosti odnose se na to da li su sve valjane transakcije evidentirane i pravilno klasifikovane. Kontrole tačnosti se bave time da li su transakcije tačno evidentirane i da li su svi elementi podataka tačni. Kontrole integriteta obrade i datoteka, ukoliko imaju nedostatke mogu poništiti svaku pomenutu aplikativnu kontrolu i omogućiti da dođe do neovlašćene transakcije, kao i da doprinesu tome da podaci budu nekompletni i netačni.

Takođe je važno da viši rukovodioci revizije i njihovo osoblje razumeju razliku između aplikativnih kontrola i IT opštih kontrola. Opšte IT kontrole se primenjuju na sve komponente sistema, procese i podatke [3,3], dok su aplikativne kontrole specifične za program ili sistem koji podržava određeni poslovni proces. Opšte IT kontrole uključuju između ostalog i kon-

trole politike bezbednosti informacija, nabavke i održavanje sistemskog softvera, zaštitu pristupa i razvoj i održavanje aplikacionih sistema. One stvaraju okruženje u kojem funkcionišu aplikacioni sistemi zajedno sa usklađenim kontrolama.

Primeri kontrola aplikacija za testiranje dati su u dokumentu *Auditing Aplication Controls* [1,18–20]. Opšte IT kontrole se primenjuju na sve sistemske komponente, procese i podatke prisutne u organizacionom ili sistemskom okruženju [3,3]. Ciljevi ovih kontrola su da osiguraju odgovarajući razvoj i implementaciju aplikacija, kao i integritet programa i datoteka podataka i računarskih operacija [2, 3]. S obzirom na vrlo širok dijapazon kontrola kompjuterskih programa, u ovom napisu akcenat je na softverskim aplikacijama iz domena finansijskog poslovanja sa stanovišta interne revizije.

IZBOR APLIKACIJA ZA PREGLEDE INTERNE REVIZIJE

Da bi dodali vrednost organizacijama procenjujući rizik kontrole, interni revizori treba da definišu univerzum aplikacija, bazu podataka i podržavajuće tehnologije koje koriste kontrole aplikacija. Nadalje, za izbor aplikacije treba definisati faktore rizika koji su povezani sa svakom kontrolom aplikacije, uključujući ključne kontrole aplikacija i njihovu efikasnost. Treba uzeti u obzir koliko kritičnih poslovnih procesa podržava aplikacija, učestalost promena u aplikacijama ili bazama podataka, kao i finansijski uticaj kontrole aplikacije. Dakle, kao i kod bilo koje revizije, izbor treba da je baziran na najrizičnijim kontrolama aplikacija.

Mada sve značajne IT operacije i ključne aplikacije treba da budu predmet redovnih pregleda, interna revizija po pravilu nema resurse ili vremena da redovno obavlja pregled kontrola za sve IT aplikacije. Pored toga, mnoge IT aplikacije predstavljaju minimalni deo kontrolnog rizika. Kao deo specifičnog operativnog pregleda ili pregleda opštih IT kontrola, interna revizija treba da odabere samo značajnije aplikacije za pregled. Proces revizije za selekciju ovih aplikacija treba da se bazira na diskusiji o planiranju revizije na bazi rizika. Pošto su IT aplikacije toliko značajne za poslovanje preduzeća, interni revizori često dobijaju posebne zahteve od odbora za reviziju ili menadžmenta da obave pregled kontrola specifičnih aplikacija. Mnogi od faktora koji mogu uticati na odluku interne revizije da odabere jednu specifičnu aplikaciju u odnosu na drugu mogu obuhvatati: zahteve menadžmenta, preglede novih aplikacija pre primene, preglede aplikacija posle primene. Postoje mnogi razlozi zašto interni revizori odaberu jednu aplikaciju između ostalih

za detaljan pregled internih kontrola. Selekcija može biti bazirana na sledećim razmatranjima:

- Da li se ovom aplikacijom kontrolišu značajna sredstva?
- Da li obavljanje aplikacije predstavlja značajnu izloženost preduzeća riziku?
- Da li aplikacija predstavlja strateški sistem za odlučivanje u preduzeću?
- Da li se ovom aplikacijom podržava funkcija koja će biti kasnije predmet pregleda kao planirani pregled interne revizije?
- Da li su izvršene značajne promene aplikacije?
- Da li je bilo značajnih promena kadrova u odeljenjima ili funkcijama koji koriste ovu aplikaciju?

Kao i sa bilo kojom drugom tehnologijom koja se koristi za podršku poslovnih procesa, aplikacije za transakcije i podršku poslovanju mogu predstavljati rizike za organizaciju, koji potiču od inherentne prirode tehnologije i načina konfigurisanja, upravljanja i korišćenja sistema od strane zaposlenih. Stepen uspešnog upravljanja rizicima direktno zavisi od od [1,1]:

- Apetita rizika (sklonosti riziku) organizacije ili tolerancije.
- Temeljitosti procene rizika u vezi sa aplikacijom.
- Ugroženosti poslovnih procesa.
- Efikasnosti opštih kontrola informacione tehnologije.
- Dizajna i kontinuiranog stepena operativne delotvornosti kontrolnih aktivnosti.

Prilikom planiranja angažmana, interni revizori moraju da razmotre značajne rizike koji utiču na poslovne ciljeve, kao i sredstva pomoću kojih će se potencijalni efekat rizika održavati na prihvatljivom nivou. Takođe, interni revizori treba da razmotre adekvatnost i efektivnost procesa upravljanja rizicima, kontrolnih procesa i upravljanja aktivnostima u odnosu na relevantni okvir upravljanja rizicima i kontrolama [4,14].

Izvesni indikatori mogu da upozore na visok nivo rizika u IT procesima. Njih treba razmotriti prilikom ocenjivanja rizika [5,17–18]:

- Koliko i koje ključne kontrole su imale propuste u testiranju prethodnog perioda ili za vreme internih revizija?
- Koja je starost aplikacije i koliko često se ona modifikuje?
- Da li postoje poznati problemi kod obrade ili podataka?
- Da li ima poznatih problema kod funkcionalnosti važnih aplikacija?
- Koliko široko je menjana kupljena aplikacija, prilagođena klijentima, ili menjana njena konfiguracija?
- Koji su bili zahtevi promena visokog prioriteta?
- Koliko se često dešavaju problemi u obradi?
- Koliko često se vrše hitne promene?
- Koji je nivo fluktuacije osoblja na ključnim pozicijama?

- Koliko je osoblje iskusno i da li je prošlo kroz dovoljnu obuku?

Dobro poznavanje infrastrukture aplikacije je bitno za efikasnu reviziju. Sledeće stavke su tipične stavke koje treba dobiti da bi se shvatili i ocenili rizici na svakom nivou seta aplikacija [5,18]:

- Elementi infrastrukture koji podržavaju aplikacije (na primer: baze podataka, operativni sistemi, mreže i centri podataka).
- Stepen do kojeg automatizovane kontrole predstavljaju rezultat postavljene konfiguracije pre nego aplikacionog koda.
- Tehnologija baze podataka u upotrebi. Upoznati se sa prirodom i dinamikom promena kod elemenata baze podataka, kao što su šematski prikazi, koje promene su bitne za ključne automatizovane kontrole.
- Operativni sistem (na primer: koji se koristi za koju aplikaciju i koliko često se vrše promene).
- Značajni interfejsi i njihove manualne kontrole. Možda je potrebno da se ove kontrole dodaju listi ključnih automatizovanih kontrola ukoliko nisu uključene kao ključne kontrole, jer njihovi propusti ne bi bili otkriveni uobičajenom primenom utvrđenih ključnih kontrola i one bi mogle dovesti do materijalne greške.
- Infrastruktura mreže i njene potencijalne tačke propusta (na primer: aplikacija i njene ključne automatizovane kontrole se možda oslanjaju na prenos kroz mrežu, gde bi propusti u mreži ili kršenje zaštite mreže mogli da imaju za posledicu neotkrivene materijalne greške u finansijskim izveštajima).
- Da li je aplikacija kreirana interno, ili je kupljena?
- Da li se aplikacija održava interno, ili se održava uslugama iz spoljnih izvora?
- Kako su aplikacije i infrastruktura podržavane: centralizovano, kroz zajedničke usluge, geografski, ili pojedinačno, po poslovnim jedinicama?
- Da li centri podataka funkcionišu interno, ili uz pomoć usluga iz spoljnih izvora?
- Koje primene mreže i tehničke infrastrukture se obavljaju interno, a koje uz pomoć trećih lica?
- Kako je IT organizovan? Da li postoji podela važnih funkcija?

ULOGA INTERNE REVIZIJE

Svi interni revizori treba da budu u stanju da evaluiraju sve kontrole poslovnog procesa od početka do kraja, uključujući i evaluaciju ključnih kontrola aplikacija. U skladu sa Međunarodnim standardima IIA za profesionalnu praksu interne revi-

zije (Standardi) – posebno standardima 1220 i 1210.A3 – interni revizori moraju primeniti opažanja i veštine razumnog i pouzdanog revizora [4,6]. Takođe, oni moraju posedovati dovoljno znanja o ključnim informaciono-tehnološkim rizicima i raspoloživim revizorskim tehnikama zasnovanim na tehnologiji, kako bi izvršili poslove koji su im dodeljeni. Ipak, ne očekuje se od svih internih revizora da imaju isti nivo stručnosti kao interni revizor, čija je primarna dužnost revizija informacione tehnologije [4,6]. Drugim rečima, svaki interni revizor mora biti svestan IT rizika i kontrola i dovoljno znati da može da utvrdi da li su primenjene kontrole adekvatno dizajnirane i da li delotvorno upravljaju rizicima u finansijskoj, operativnoj i regulatornoj oblasti.

Interni revizori treba da stave akcenat na obavljanje pregleda odgovarajućih IT aplikacija kada obavljaju preglede u drugim oblastima preduzeća. Da bi pravilno ocenila kontrole IT aplikacija interna revizija treba da se dobro upozna sa IT procedurama i specifičnim kontrolnim i proceduralnim karakteristikama svake oblasti aplikacija, odnosno treba obezbediti pun pristup svim konfiguracionim fajlovima, dokumentaciji i informacijama, kako bi se postigao cilj interne revizije: da se višem rukovodstvu obezbedi nezavisno uveravanje o postojanju kontrola aplikacija i njihovom efektivnom funkcionisanju, kao i unapređenje internih kontrola aplikacija pomoću identifikovanja nedostataka sistema kontrola i davanjem predloga za otklanjanje istih. Uveravanje o kontrolama koje interna revizija pruža višem rukovodstvu je od suštinskog značaja u procesu upravljanja rizicima.

INTERNA REVIZIJA KONTROLA APLIKACIJA

Pri reviziji kontrola aplikacija interni revizor treba da se pridržava adekvatne *metodologije revizije*. To podrazumeva da interni revizor mora da stekne opšte razumevanje o aplikaciji koja će biti predmet pregleda: njene glavne poslovne ciljeve, inpute i autpute i tehnološko okruženje. Na bazi ovih opštih saznanja o aplikaciji, on treba da izradi dijagram toka opšteg procesa kojim se utvrđuju ključne tačke odlučivanja u procesu, i interne kontrole. Zatim, treba da se upozna sa opštim kontrolnim okruženjem, samom aplikacijom i njenom obradom. Opšte kontrole obuhvataju pristup i kontrole revidiranja programa uključujući informacione sisteme u koje je smeštena aplikacija. Loše opšte kontrole mogu da negiraju sve druge detaljne kontrole aplikacija.

Interni revizor treba da prodiskutuje o aplikaciji sa korisnicima sistema odgovornim za rad sistema, kao i sa članovima organizacije informacionih sistema, kako bi se oni upoznali sa

problemima ili planiranim aspektima koji se tiču aplikacije. Zatim je potrebno da izradi plan testiranja za aplikaciju, sa naglaskom na:

- identifikaciji značajnih kontrola koje se odnose na transakcije i poslovanje u okviru aplikacije;
- utvrđivanju ciljeva koji uključuju sve te značajne kontrole, tj. na koje će se oblasti revizor fokusirati kako bi mogao da utvrdi da li je ključna kontrola efikasna;
- razvoju pristupa testiranja i uzorkovanja za svaku ključnu kontrolu aplikacije.

Interni revizor utvrđuje plan i program testiranja. Utvrđuje raspored vremena i obavlja testiranja ključnih kontrola aplikacije korišćenjem sakupljenog materijala za testiranje. Nakon testiranja revizor ocenjuje sve rezultate testova u kontekstu da li su kontrole efikasne ili neefikasne i obaveštava o rezultatima ovog testiranja ključne korisnike sistema i organizaciju informacionih sistema. Potrebno je imati na raspolaganju kopije svih dokaza testiranja i dokumentovati rezultate testiranja na radnim papirima interne revizije. I na kraju, potrebno je izraditi plan korektivnih aktivnosti sa informacionim sistemima, drugim entitetima koji dostavljaju podatke aplikaciji ili korisnicima koji treba da reše probleme koji su utvrđeni kao deo pregleda aplikacije.

RADNI PROGRAM REVIZIJE KONTROLA APLIKACIJA

Program interne revizije treba da obezbedi reviziju izloženosti riziku ključnih kontrola aplikcije. Prema IIA standardu, interni revizori moraju da razviju i dokumentuju radne programe kojima se ostvaruju ciljevi angažmana. Uzorak programa revizije dat je u dokumentu *Auditing Aplication Controls* u prilogu B [1,21–25]. Ovde dajemo pregled samo nekih procedura za reviziju kontrola ulaza, obrade, izlaza i datoteka čuvanja podataka, a koje treba da bude sastavni deo programa revizije.

Kod revizije ulaznih kontrola revizor treba da oceni:

- Da li je ulaz svih najvažniji podataka, uključujući promene stalnih podataka, odobren na odgovarajući način.
- Za onlajn sisteme, da li je mogućnost unosa podataka iz terminala adekvatno ograničena i kontrolisana.
- Da li postoji metod za sprečavanje i otkrivanje duplirane obrade izvornog dokumenta.
- Da li je sav odobreni ulaz dostavljen ili, u onlajn sistemu, prenesen i da li postoje procedure za obezbeđenje tačnosti i ponovno dostavljanje odbačenih podataka.

Revizor treba da obezbedi da postoje kontrole za otkrivanje nepotpune i netačne obrade podataka ulaza. Aplikacioni procesi mogu da obavljaju dalje potvrđivanje transakcija provera-

vanjem podataka zbog dupliranja i konzistentnosti, sa drugim informacija koje vode drugi delovi sistema. Kompjuterizovani sistemi treba da vode dnevnik obrađenih transakcija. Dnevnik transakcija treba da sadrži dovoljno informacija za identifikovanje izvora svake transakcije.

Potpunost i integritet izveštaja o izlazu zavisi od ograničavanja mogućnosti da se izvrše promene i dopune izlaza i uključivanjem provera o potpunosti, kao što su brojevi stranica i provere iznosa. Kompjuterski izlaz treba da bude redovan i vremenski planiran. Korisnici će verovatno otkriti da izlaz nedostaje ukoliko očekuju da ga redovno primaju. Izlazi treba da budu zaštićeni da bi se smanjio rizik od neovlašćenih izmena i dopuna.

Revizori treba da zapaze sledeće dok vrše ispitivanje sistema stalnih datoteka:

- Da li su izmene i dopune stalnih podataka pravilno odobrene i kontrolisane.
- Da li je integritet centralnih i stalnih datoteka verifikovan proverom, kontrolnim zbirovima i periodičnim usaglašavanjem sa nezavisno vođenim evidencijama.
- Da li su procedure koje se odnose na izmene i dopune pravilno dokumentovane i kontrolisane potvrđivanjem od strane menadžmenta i naknadnim pregledom.
- Da li je ograničen i kontrolisan fizički i logički pristup datotekama aplikacije.

OBAVLJANJE TESTOVA KONTROLA APLIKACIJA

Testiranje kontrola aplikacije je regulisano IIA standardom 2300, u kom se od internih revizora zahteva da identifikuju, analiziraju, procene i dokumentuju informacije dovoljne za ostvarenje ciljeva angažmana. Procedure se razlikuju u zavisnosti od toga (1) da li aplikacija prvenstveno koristi kupljene ili interne komponente softvera; (2) da li je aplikacija integrisana sa drugim ili predstavlja poseban proces; (3) da li koristi provajdere veb usluga, klijent–server model, ili metode starih nasleđenih kompjuterskih sistema; i (4) da li su njene kontrole uglavnom automatizovane, ili zahtevaju ekstenzivne aktivnosti ljudskog intervenisanja. Tačna priroda aplikacija može takođe da se razlikuje u znatnoj meri. Mada je akcenat internih revizija nekada prvenstveno bio stavljan na kontrole u računovodstvenim aplikacijama, današnji interni revizori treba da obavljaju pregled aplikacija i drugih oblasti, kao što je planiranje proizvodnih resursa ili analiza kreditnog portfolija. Svaka ova oblast zahteva poznavanje specifičnih osobina aplikacije i odgovarajućih tehnologija. To znači da interni revizor treba da upozna ka-

ko aplikacija funkcioniše, prvo dokumentovanjem IT aplikacija, a zatim definisanjem specifičnih ciljeva revizijskog testiranja, i najzad obavljanjem serije revizijskih testiranja da bi se verifikovalo da li postoje kontrole aplikacija i da li funkcionišu kako se očekuje.

Interni revizor može da koristi više procedura prilikom ocenjivanja internih kontrola IT aplikacija. Zbog prirode i ciljeva aplikacije, ove procedure se ne mogu primeniti na sve aplikacije. Neka od revizorskih testiranja koja se preporučuju internom revizoru su sledeća:

- **Testiranje ključnih obračuna.** Korišćenjem uzoraka transakcija potrebno je uvrditi da li su rezultati i ukupne vrednosti (totali) tačni.
- **Razmotranje potrebe obavljanja specijalne revizije samo test transakcija.** Priprema se set transakcija koje obuhvataju sve ključne aspekte aplikacije i organizuje specijalna revizija samo test transakcija. Pregledaju se rezultati test transakcija zbog preciznosti kontrola i obrade, i eliminišu test transakcije koje su bile predmet revizije iz proizvodnog ciklusa.
- **Obavljanje saldiranja transakcija.** Korišćenjem ukupnih vrednosti transakcija iz proizvodnog procesa obračunavaju se pojedinačni iznosi i usaglašavaju ukupne vrednosti revizijske kontrole sa prikazanim ukupnim vrednostima aplikacije iz istog ciklusa.
- **Obavljanje pregleda logičke sigurnosti (zaštite) aplikacije.** Vrši se pregled nivoa sigurnosti (zaštite) aplikacije da bi se utvrdilo da li svi korisnici imaju odgovarajuće nivoe pristupa za čitanje, pisanje i izmenu.
- **Dokumentovanje interne kontrole.** Testiraju se kontrole ključnih dokumenata (ID brojeva, itd.) da bi se utvrdilo da li se ažurirane transakcije mogu pratiti unazad do svoje tačke porekla (izvora).
- **Obavljanje pregleda neovlašćenih promena.** Obavlja se pregled logova ažuriranih datoteka programa i utvrđuje se da li su verzije programa tj. aplikacija u proizvodnim datotekama iste kao one u fajlovima dokumentacije.
- **Ocenjivanje odredbe planiranja nepredviđenih događaja.** U zavisnosti od revizijskog rizika, ispituju se odredbe planiranja, kontinuiteta i nepredviđenih događaja.

Testiranja aplikativnih inputa i autputa. Na samom početku IT revizije mnogi revizijski testovi predstavljaju nešto više od provera kojima se potvrđuje da su svi inputi programa pravilno obuhvaćeni i da je korektan broj transakcija proizveden na bazi inputa. Na primer, razmatra se revizorov pregled automatizovanog platnog sistema (platnog spiska). Interni revizor obavlja testiranje da utvrdi da li su vremenske kartice (kartice

vremena provedenog na poslu) prihvaćene ili odbačene i da li se broj provera autputa platnog spiska koji je proizveden može usaglasiti sa vremenskim karticama inputa sistema. Ovo je testiranje inputa i autputa sistema.

Mada automatizovane aplikacije postaju sve složenije, mnoge procedure revizijskog testiranja danas predstavljaju nešto više od ovih istih testiranja inputa i autputa. Interni revizor treba da obavi pregled autputa koje generiše aplikacija, kao što su fakture koje proizvodi sistem za fakturisanje, da bi utvrdio da li su podaci inputa i kompjuterski obračuni tačni. Ova vrsta revizijskog testiranja je ograničene prirode i neće obuhvatati sve transakcije ili funkcije u okviru aplikacije.

Cilj ocenjivanja kontrolnog rizika ili testiranja usaglašavanja jeste da se utvrdi da li kontrole aplikacija funkcionišu. Ukoliko treba pregledati sve transakcije ili sve podatke, potrebno je koristiti procedure suštinskog testiranja ili testiranje salda finansijskih izveštaja. Obim ovog testiranja zavisi od ciljeva revizije. Na primer, eksterni revizor će obavljati testiranja usaglašenosti sa propisima onih aspekata aplikacije koji obuhvataju interne računovodstvene kontrole koje se odnose na finansijske izveštaje. Interni revizor može takođe poželeti da obavi testiranja usaglašenosti sa propisima nekih drugih oblasti, kao što je efikasnost administrativnih kontrola. Da nije ograničenja prostora, moglo bi da se razmotri još mnogo primera testiranja različitih transakcija.

Ne treba zaboraviti da se pri pregledu mogu koristiti softveri za reviziju – CAATTs (*Computer-assisted audit tools and techniques* – kompjuterski revizijski alati i tehnike), zatim pregledi izvornog koda programa, pristupi stalnog monitoringa revizije, ponovno obavljanje funkcija aplikacije ili obračuna, itd. S obzirom da CAATT-ovi pružaju mogućnost da analiziraju velike količine podataka, dobro dizajnirana revizija podržana CAATT testom može izvršiti kompletan pregled svih transakcija i otkriti abnormalnosti (npr. duplikate dobavljača ili transakcija) ili skup unapred utvrđenih problema kontrole (npr. segregaciju konfliktnih dužnosti).

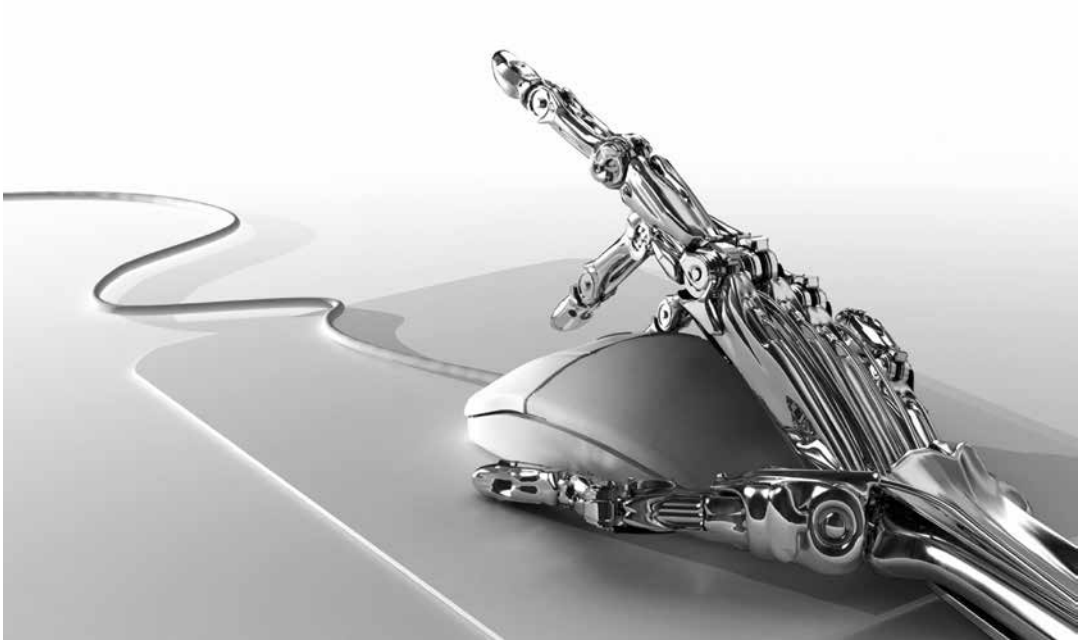
Tehnike revizije uz pomoć računara koriste računarske aplikacije kao što su ACL, IDEA, VIRSA, SAS, SKL, Excel, Cristal Reports, Business Objects, Access i Word, kako bi se automatizovao i olakšao proces revizije. Upotreba CAATT-a pomaže da se obezbedi odgovarajuća pokrivenost za pregled kontrola aplikacija, naročito kada postoje hiljade ili možda milioni transakcija koje se javljaju tokom perioda testiranja. U ovim situacijama bilo bi nemoguće dobiti odgovarajuće informacije u formatu koji se može pregledati bez upotrebe automatskog alata.

IZVEŠTAJ O REZULTATIMA REVIZIJE

Prema IIA standardu 2400, interni revizori moraju da saopšte rezultate angažmana. Kao konačnu etapu revizije kontrola na nivou aplikacija, revizor treba da donese zaključak o pojedinačnom i zbirnom efektu utvrđenih slabosti u kontrolama aplikacija na ciljeve revizije i da prikaže rezultat revizije, uključujući pored zaključaka i primenljive preporuke i/ili planove aktivnosti. Takvi zaključci uglavnom uključuju efekat slabosti na sposobnost poslovnog procesa i aplikacije da postigne kontrolne ciljeve. Revizorovi zaključci treba da budu bazirani na potencijalnoj međuzavisnosti kontrola aplikacija (tj. kontrola čija efikasnost zavisi od drugih kontrola).

Pre sastavljanja izveštaja o reviziji potrebno je sa menadžmentom prodiskutovati o utvrđenim slabostima, da bi se dobila njihova saglasnost na iznete nalaze, ali i da bi se saznalo 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 (uključujući stanje, kriterijume i, gde je to moguće, uzrok i efekat), i
- Preporuke



ZAKLJUČAK

Kontrole na nivou aplikacija poslovnih procesa, koje se još nazivaju „kontrolama aplikacija", jesu kontrole koje se odnose na kompletnost, tačnost, valjanost i raspoloživost transakcija i podataka za vreme obrade. Kontrole aplikacija su specifične za jednu aplikaciju i mogu imati direktan uticaj na obradu pojedinačnih transakcija. Ove kontrole se koriste da bi se obezbedilo uveravanje da su sve transakcije validne, odobrene, evidentirane i potpune.

Za obavljanje efikasne revizije kontrola aplikacija interna revizija treba da prođe sve etape procesa revizije, počevši od planiranja revizije, procene rizika, dokumentovanja aplikacije i kontrola, utvrđivanja kontrolnih ciljeva, sačinjavanja programa revizije, obavljanja testiranja kontrola aplikacija i sačinjavanja izveštaja o obavljenoj reviziji sa akcionim planom za poboljšanje i jačanje kontrola aplikacija. U tom cilju, interni revizor treba da se upozna sa aplikacijom, njenim inputima, autputima i procedurama koje zahtevaju manuelne ili druge sistemske interakcije. Kada je god to izvodljivo, revizor treba da koristi softverske alate da bi pratio obradu svake faze modula ili radne stanice i da bi pratio transakcije kako bi utvrdio da li aplikacije funkcionišu sa odgovarajućim kontrolama i onako kako se očekuje. Na kraju praćenja revizor treba sa revidiranom stavom da prodiskutuje o svim neuobičajenim ili neočekivanim problemima i dokumentuje status internih kontrola. Na samom kraju procesa, nakon izveštaja interne revizije o sprovednoj reviziji kontrola aplikacija, potrebno je doneti odluku o preduzimanju daljih aktivnosti i prihvatljivom stepenu oslanjanja na kontrole aplikacija. Odgovornost revizora jeste da predstavi sve prednosti i nedostatke koje je identifikovao tokom revizije kontrola aplikacija, kao i koristi i gubitke koji mogu biti posledica izabrane alternative. Za razliku od revizora, donosilac odluke je odgovoran za buduće postupanje tj. prihvaćeni stepen rizika (ne)oslanjanja na revidirane kontrole aplikacija.

LITERATURA

1. Bellino, C., J. Wells, S. Hunt, Global Technology Audit Guide (GTAG) 8, Auditing Application Controls, The Institute of Internal Auditors, 2007.
2. Information Systems Audit and Control Association (ISACA), IS Auditing Guideline – Application Systems Review, Document G14, 2001.
3. Richards, D. A., Alan S. Oliphant, Charles H. Le Grand, Global Technology Audit Guide (GTAG) 1, Information Technology Controls, The Institute of Internal Auditors, 2005.
4. The Institute of Internal Auditors (IIA), GAIT Methodology - A risk-based approach to assessing the scope of IT general controls, 2007.
5. The Institute of Internal Auditors (IIA), INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS), IIA, USA, 2017.

AUDITING OF APPLICATION CONTROLS

SUMMARY

Key words: application controls, audit, IT controls, IT risks, CAATT.

All business processes are performed today with modern applicative software. Each application must have an adequately designed internal control whose role is to reduce the risks of the business process to an acceptable level. Internal application controls relate to input controls, processing controls, and output controls. The assurance of their adequacy and efficiency of the functioning should be given by an internal audit. Internal auditors, in order to carry out the audit of application control, must possess sufficient knowledge and skills on critical information and technology risks and technology-based audit techniques and application of audit software. The methodology for performing the audit of application control is based on significant risks and key controls. An audit product is an audit report sent to senior management. The results of the reports are essential in the process of risk management and the adoption of future business decisions on an adequate degree of reliance on audited application controls.