Mile Stanišić

PREGLEDNI RAD
UDK: 005.334:657.633
657.6:004.4

DOI: 10.5937/Rev2090061S

IMPLIKACIJE IT RIZIKA I KONTROLA NA INTERNU REVIZIJU

UVOD

Informacione tehnologije (IT) menjaju način na koji organizacije formulišu svoje strategije, obavljaju svakodnevne aktivnosti i donose odluke. Ove promene izazivaju nove rizike i teraju organizacije da modifikuju svoje upravljanje, upravljanje rizicima i kontrolišu procese. Sve širi uticaj IT na organizacije naizmenično primorava interne revizore da unaprede svoja znanja i sposobnosti iz oblasti IT i prilagode obavljanje svog posla njima.

IT se menjaju rapidnim tempom i predstavljaju nove izazove sa kojima se sve organizacije moraju suočiti, čak i ukoliko one odluče da ne prihvate takve izmene i način razvijanja IT u svojoj organizacionoj strukturi. Bez obzira na to koliko brzo organizacije usvajaju nove tehnologije tempom kako one nastaju, sve one investiraju jako mnogo u IT. One to rade iz više razloga, od kojih se neki odnose direktno na postizanje poslovnih ciljeva organizacija. Na primer, IT omogućavaju poslovne strategije, poboljšanje obavljanja poslovnih procesa, olakšavanje procesa donošenja odluka. U stvari, IT su dostigle tačku gde su tako isprepletene sa poslovnim ciljevima organizacija, strategijama i aktivnostima u kojima IT inicijative moraju biti uzete u obzir zajedno sa poslovnim inicijativama da bi se osigurala veza između to dvoje.

Funkcija interne revizije ima mogućnost da se vrlo rano uključi u proces IT kod pojave novonastalih problema i da obezbedi uvid unutar organizacije u vezi sa optimiziranjem mogućnosti i smanjenjem rizika. Sve raširenij uticaj IT na poslovne strategije i svakodnevno poslovanje organizacija značajno je uticao i na profesiju interne revizije. IT je promenio kompetencije koje funkcije interne revizije moraju da poseduju i način na koji obavljaju usluge uveravanja i konsultacija. U današnjem poslovnom svetu je praktično nemo-

REZIME

Ključne reči: interna IT revizija, IT rizici, IT kontrole, GTAG vodič, standardi interne revizije

Informacione tehnologije su značajno promenile kompetencije koje interni revizori moraju da poseduju i način na koji obavljaju svoj posao. Sposobnost funkcije interne revizije da pruža usluge uveravanja i konsultantske usluge u smislu dodavanja vrednosti u velikoj meri zavisi od njene IT stručnosti. Svi interni revizori moraju imati osnovno tehnološko znanje i veštine utvrđene standardima interne revizije.
Funkcije interne revizije moraju razumeti informacione sisteme svojih organizacija i IT rizike koji prete postizanju poslovnih ciljeva organizacija. Takođe moraju da znaju da procenjuju procese upravljanja informacijama u IT, upravljanje rizikom i kontrolu svojih organizacija i da budu u mogućnosti da efikasno primene tehnike revizije zasnovane na tehnologiji.

Prof. dr Mile Stanišić, vanredni profesor, Univerzitet Singidunum, Beograd, mailto: mile.stanisic@hotmail.com

guće da bilo koja funkcija interne revizije pruži usluge dodavanja vrednosti svojoj organizaciji, osim ako ta funkcija nema veliku stručnost u poznavanju IT rizika i kontrola i nema sposobnost da efikasno primenjuje metodologiju revizije zasnovanu na tehnologiji. Ovo uključuje veliko iskustvo i usvajanje analitike podataka u procesima revizije. Vrhunske IT veštine koje bi trebali imati svi interni revizori uključuju:

- Analizu podataka – kako analizirati podatke i koristiti softverske alate za reviziju.
- Ključne komponente sajber bezbednosti – to su informacije o bezbednosti, uključujući terminologiju i ključne rizike.
- Kontinuitet poslovanja i oporavak od katastrofe – razumevanje najznačajnijih poslovnih oblasti i praksi za oporavak.
- Sposobnost da Istaknete znanje menadžmenta o upravljanju projektima i promenama procesa i da izvrše odgovarajući uticaj na organizaciju.
- Novije tehnologije – praćenje pametnih tehnologija, kao i aktuelnih pitanja novih tehnologija i njihovog potencijalnog uticaj na poslovanje.

Interni revizor koji radi intenzivno u oblasti kompjuterizovanih informacionih sistema mora da poseduje visoku stručnost o IT rizicima, kontroli i reviziji. Takvi revizori se obično nazivaju revizorima informacionih tehnologija ili revizorima informacionih sistema (IS). Iako svi interni revizori ne moraju imati stručnost specijaliste za IT reviziju, svaki interni revizor mora imati makar dobro razumevanje određenih osnovnih IT koncepata. Na primer, svi interni revizori treba da razumeju osnovne komponente informacionih sistema svojih organizacija, IT rizike koji prete postizanju poslovnih ciljeva organizacija, kao i IT upravljanje, upravljanje rizicima i kontrolne procese organizacija. Pored toga, oni moraju p aplikacija i tehnologije koju poslovne jedinice koriste za reviziju.

Interni revizor mora da ima visoko poznavanje IT rizika.

Rastući i šireći uticaj IT na poslovne strategije i svakodnevne aktivnosti organizacija značajno utiču na profesiju interne revizije. IT menjaju nadležnosti koje funkcije interne revizije moraju posedovati, kao i način na koji obavljaju kontrolne i konsultantske usluge.

ZAHTEVI STANDARDA INTERNE REVIZIJE

Dva značajna implementacijska standarda interne revizije posebno naglašavaju IT znanja koja interni revizori moraju imati i pažnju koju oni moraju posvetiti korišćenju revizijskih tehnika zasnovanih na tehnologijama (1, 11).

Standard 1210.A3 – Interni revizori moraju imati dovoljno znanja o ključnim rizicima i kontrolama, kao i raspoložive revizijske tehnike zasnovane na tehnologiji, kako bi obavljali određene poslove. Ipak, ne traži se od svih internih revizora da imaju znanja kao interni revozor koji ima primarnu odgovornost za IT reviziju.

Standard 1210.A2 – U primeni dužne profesionalne pažnje, interni revizori moraju razmotriti korišćenje tehnološki zasnovane revizije i drugih tehnika analize podataka.

Standardi 1210.A3. i 1210.A2 jasno pokazuju da svi interni revizori koji pružaju usluge treba da imaju barem osnovni nivo znanja iz oblasti IT rizika, kontrole i revizije.

Najveći broj funkcija interne revizije ima istu vrstu automatizovanog rada sa dokumentima, kao što je TeamMate, čime dokumentuje, organizuje i povezuje posao interne revizije. Automatizovani sistemi rada sa dokumentima značajno poboljšavaju dokumentacione aspekte interne revizije putem poboljšanja efektivnosti i efikasnosti obavljenog posla.

Automatizovani sistemi rada sa dokumentima značajno doprinose poboljšavaju efektivnosti i efikasnosti obavljenog posla.

Standard 1210.A3 takođe pokazuje da interni revizor ne treba da poseduje onaj nivo znanja koji se očekuje od revizora specijaliste za IT. Ipak, pošto potražnja za visokoobučenim IT revizorima povećava ponudu, može se govoriti da su zainteresovani za ovu oblast ohrabreni da istražuju dalje kompetencije i licence potrebne da se uspe kao IT specijalista. Te osobe mogu želeti da steknu sertifikate iz oblasti IT kontrole u cilju kompletiranja svoje licence internog revizora. Takve licence-serifikati uključuju npr. Ovlašćeni revizor informacionih sistema, kao i Ovlašćeni revizor iz oblasti bezbednosti informaconih sistema.

Kao što je to slučaj sa drugim oblastima relevantnog znanja, izvršni rukovodilac revizije je odgovoran za obezbeđenje uslova da funkcija interne revizije ima dovoljno stručnosti da ispuni odgovornosti angažmana uveravanja. Neke od funkcija interne revizije imaju dovoljno IT internih revizora među svojim osobljem. Oni koji nemaju takve stručnjake među osobljem, takvo znanje traže izvan funkcije interne revizije. U nekim slučajevima može se tražiti od kvalifikovanih osoba iz drugih oblasti unutar organizacije da pomognu u aktivnostima interne revizije, na primer kada se traži znanje iz oblasti IT koje funkcija interne revizije ne poseduje. U drugim slušajevima, šef interne revizije unajmljuje vanjske davaoce usluga sa traženim IT znanjem i sposobnostima (tzv. *outsourcing servises*).

Tri implementaciona standarda koja se odnose na informacione sisteme i tehnologiju posebno se odnose na interne revizore u oblasti njihovih odgovornosti za angažmane uveravanja (1, 19-21):

2110.A2 – Aktivnost interne revizije mora oceniti da li IT upravljanje organizacije podržava organizacione strategije i ciljeve.

2120.A1 – Aktivnost interne revizije mora oceniti koliko su informacioni sistemi organizacije izloženi riziku.

2130.A1 – Aktivnost interne revizije mora oceniti adekvatnost i efikasnost kontrola u vezi sa rizicima informacionih sistema unutar organizacije.

Ova tri standarda odražavaju činjenicu da funkcija interne revizije ne može efikasno oceniti upravljanje, upravljanje rizicima i kontrolne procese bez uzimanja u obzir informacionionih sistema i tehnologija. Da bi ispunila svoje IT obaveze i odgovornosti, funkcija interne revizije mora:

- Uključiti informacioni sistem organizacije u svoj godišnji plan revizije.
- Identifikovati i oceniti IT rizike organizacije.
- Osigurati dovoljan nivo stručnog znanja iz oblasti IT revizije.
- Oceniti IT upravljanje, rukovođenje, i tehničke kontrole.
- Rasporediti revizore sa odgovarajućim nivoom stručnosti u oblasti IT na svaki dodeljeni posao.
- Koristiti odgovarajuće tehnološki zasnovane revizijske tehnike.

IT RIZICI

Revizor treba preliminarno da oceni i dokumentuje prirodu i nivo IT 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 (2, 18). IT 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 IT rizika obuhvata ocenu verovatnoće da se takav gubitak poverljivosti, integriteta ili raspoloživosti 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 IT rizika i njihov potencijalni uticaj na efikasnost IT kontrola. Globalni vodič za reviziju tehnologija (GTAG) je u svom dokumentu „Rizici i kontrole informacionih tehnologija" dao analizu rizika informacionih sistema (3, 10-12).

Savremeni IS značajno se razlikuju od organizacije do organizacije i nećemo se ovde baviti širokim spektrom različitosti sistemskih konfiguracija koje postoje danas u poslovnom svetu. Ipak, postoje zajedničke ključne komponente IS koje interni revizori treba da razumeju. Ove komponente uključuju kom-

pjuterski hardver, mreže, kompjuterski softver, bazu podataka, informacije i ljude (4, 11-21). Svaka od ključnih komponenti informacionog sistema predstavlja potencijalni izvor rizika. Na primer:

- Kompjuterski hardver je osetljiv na nestanak struje, što prekida obavljanje transakcija.
- Informacije koje se prenose putem mreže mogu biti presretnute, ukradene ili zloupotrebljene.
- Kompjuterski softver koji je netačno programiran može proizvesti informacije koje nisu valjane, nekompletne i/ili netačne informacije.
- Baza podataka može biti infiltrirana u svrhu protivpravnog prisvajanja ili zloupotrebe informacija.
- Informacija koja nije valjana, koja je nekompletna i/ili netačna, može rezultirati lošim odlukama. (Ovaj rizik da loša informacija rezultira lošom odlukom se generalno smatra informacionim rizikom).
- Osoba može obavljati nespojive IT dužnosti i tako biti u poziciji da načini i prikrije greške ili prevaru.

Upotreba IT u informacionim sistemima otvara vrata za IT rizike. Posebni IT rizici sa kojima se jedna organizacija suočava će zavisiti od prirode njenog posla i aktivnosti, delatnosti u okviru koje organizacija posluje, konfiguracije njenog IS, kao i od drugih internih i eksternih faktora. Štaviše, rizici se menjaju kao rezultat promena u internom i eksternom okruženju organizacija i ništa se ne menja brže od IT u današnjem poslovnom svetu. U skladu s tim, organizacije moraju stalno pratiti napredovanje IT i kontinuirano razmatrati grananje rizika tih napredovanja.

Upotreba IT u informacionim sistemima otvara vrata za IT rizike.

Ipak, postoje određene vrste IT rizika koji imaju tendenciju da su zajednički za sve organizacije i delatnosti.

- **Rizik odabira**. Odabir IT rešenja koje odstupa od strateških ciljeva može onemogućiti izvršenje strategija koje zavise od IT. Takođe, odabir određenog IT rešenja koje je nedovoljno fleksibilno i/ili podesivo može rezultirati nekompatibilnošću između IT rešenja i postojećeg sistema organizacija i/ili može ometati buduće organizacione promene i rast. Razlozi nastanka rizika odabira uključuju, na primer, nekvalifikovane donosioce odluka i neadekvatne informacije na kojima se zasniva proces donošenja odluka. *GTAG 4: Upravljanje IT revizijom* (5, 8-9) *i GTAG 11: Razvijanje plana IT revizije* (6, 12-15) (*deo IIA iz Priručnika za reviziju globalne tehnologije – GTAG*) pružaju više detalja o riziku odabira i smernicama o tome kako funkcija interne revizije treba da rasporedi svoje resurse u cilju obezbeđenja sigurnosti da se rizik odabira adekvatno ublaži.

- **Rizik razvoja/preuzimanja i primene**. Problemi koji nastaju nakon razvoja, preuzimanja i primene IT rešenja mogu uzrokovati nepredviđena odlaganja, rast troškova, ili čak i odustajanje od projekta. Razlozi nastanka rizika razvoja/preuzimanja i primene, na primer, uključuju nedovoljnu internu stručnost, neadekvatnu podršku dobavljača i otpor prema promenama. *GTAG 12: Revizija IT projekata* (7, 3-7, 14, 16-17) *i GTAG 14: revizija korisnički razvijenih aplikacija* (8, 6-11), identifikuju mnoge dodatne primere rizika IT projekata koji se javljaju u organizaciji.
- **Rizik dostupnosti**. Nedostupnost sistema kada je potreban može uzrokovati odlaganja u procesu donošenja odluka, prekide poslovanja, gubitak prihoda, kao i nezadovoljstvo potrošača. Razlozi za rizik dostupnosti uključuju na primer: kvar na hardveru ili softveru, neplanirano održavanje, viruse i ostale zlonamerne akte. *GTAG 10: Poslovno i trajno upravljanje* pruža smernice za obavljanje najboljih praksi u vezi sa poslovnim oporavkom (9, 8-11).
- **Rizik hardvera/softvera**. Kvar na hardveru ili softveru može uzrokovati prekide poslovanja, privremenu ili stalnu štetu na podacima ili njihovo uništenje, kao i troškove popravke ili zamene hardvera ili softvera. Razlozi za ovaj rizik uključuju, na primer, prirodno habanje, štetu nastalu pod uticajem okruženja, kao npr. usled preterane vlage, nesreće kao što su požari i poplave, kao i viruse i ostale zlonamerne akte (10, 2-22).
- **Rizik pristupa**. Neovlašćen fizički ili logički pristup sistemu može rezultirati krađom ili zloupotrebom hardvera, zlonamernim modifikacijama softvera, kao i krađom, zloupotrebom ili uništenjem podataka. Razlozi za rizik pristupa uključuju, na primer, pristup putem pametnih telefona, modifikovanje i pohranjivanje korporativnih podataka i slobodnu upotrebu bežičnih mreža za gostujući pristup poslovnim podacima. *GTAG 9: Upravljanje identitetom i pristupom*, naglašava brojna pitanja u vezi sa kontrolama pristupa, skupa sa rešenjima (11, 1-2, 4, 12-16).
- **Rizik pouzdanosti sistema i ispravnosti informacija**. Sistemske greške ili nedoslednosti u obradi mogu uzrokovati nerelevantne, nepotpune, netačne i/ili nepravovremene informacije. Naizmenično, loše informacije koje sistem proizvede mogu nepovoljno uticati na odluke koje se donose na osnovu tih informacija. Razlozi za ovaj rizik uključuju, na primer, greške u programiranju softvera i neovlašćene izmene softvera. *GTAG 8: Revizija kontrola*

aplikacije daje smernice revizorima, koje traba da prate dok ocenjuju kontrole ugrađene u aplikacije (12, 4-10).

- **Rizik poverljivosti i privatnosti**. Neovlašćeno otkrivanje poverljivih informacija poslovnih partnera ili privatnih informacija osoba, mogu rezultirati gubitkom poslovanja, tužbama, negativnim javnim mnjenjem i gubitkom reputacije. Razlozi za ovaj rizik uključuju, na primer, slobodan pristup sistemskim mrežama, softveru i bazi podataka. IIA Praktični vodič, *Revizijski rizici privatnosti*, obrađuje rizike kontrola i privatnosti, uključujući i one koji su direktno povezani sa IT, i pružaju smernice kako da se efikasno revidira privatnost (13, 2, 5-6, 9-10, 13-21).
- **Rizik prevare i zlonamernih dela**. Krađa IT resursa, namerna zloupotreba IT resursa, ili namerna deformacija ili uništenje informacija, mogu rezultirati finansijskim gubicima i/ili pogrešnim informacijama na osnovu kojih se donose odluke. Razlozi za ovaj rizik uključuju, na primer, namere nezadovoljnih zaposlenika ili hakera da naude organizaciji iz lične koristi. *GTAG 13: Prevencije krađe i otkrivanje u svetu automatike* naglašava rizike od krađe povezane sa IT i daje smernice internim revizorima kako da koriste tehnologiju kako bi efikasno otkrili krađu (14, 2-8, 11-13, 16-17).

Svi globalni vodiči za reviziju tehnologija (*Global Technology Audit Guide* – GTAG) dostupni su na sajtu Instituta internih revizora: https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx pod naslovom „Dodatne smernice (Vodiči za praksu)". Vodiči pružaju detaljne smernice za sprovođenje aktivnosti interne revizije. To uključuje aktuelne oblasti, sektorska pitanja, kao i procese i postupke, alate i tehnike, programe, postupne pristupe i primere rezultata.

Počev od IPPF-a koji je donet u julu 2015, svi vodiči za praksu, vodiči za globalnu reviziju tehnologije (GTAGs) i uputstva za procenu IT rizika (GAIT) automatski postaju deo preporučenog dodatnog sloja uputstva.

IT KONTROLE

Kontrola se definiše kao proces uključen u upravljanje rizicima i obavljan od strane uprave u cilju ublažavanja rizika i njegovog spuštanja na prihvatljiv nivo. IT kontrole se obično klasifikuju kao opšte ili aplikativne kontrole, opisane kao:

- *Opšte kontrole,* koje se primjenjuju na sve sistemske komponente, procese i podatke za datu organizaciju ili sistemsko okruženje (15, 16).

- *Aplikativne kontrole*, odnose se na područje individualnih poslovnih procesa ili aplikativnih sistema i uključuju kontrole unutar aplikacije u vezi sa ulaznim podacima, obradom podataka i izlaznim rezultatima (15, 16).

Drugi vid klasifikacije kontrola je „prema grupi odgovornoj za obezbeđenje da li su one implementirane i održavane na odgovarajući način" (15, 17). Na primer, kao što je predstavljeno na slici 1, kontrole se mogu kategorisati na način od vrha na dole u tri kategorije, i to kontrole upravljanja, kontrole rukovođenja i tehničke kontrole. Prema slici 1, prvu kategoriju „kontrole upravljanja" čine Politike. Druga kategorija kontrola „kontrole rukovođenja" obuhvataju Standarde, Organizaciju i menadžment i Fizičke i kontrole okruženja. Treću kategoriju „Tehničke kontrole" čine Kontrole sistemskog softvera, Kontrole razvoja sistema i Kontrole bazirane na aplikacijama.

Gornjih šest slojeva IT kontrola prikazanih na slici 1. predstavljaju opšte IT kontrole, a donji sloj predstavlja kontrole aplikacija. Važno je, međutim, razumeti da „različiti elementi hijerarhije nisu međusobno isključivi, svi su povezani i mogu se mešati" (15, 18).

Slika 1. IT okvir kontrole

Izvor: GTAG: Information Technology Risk and Controls, 2nd Edition, The Institute of Internal Auditors, 2012, 18.

Pojedinačne kontrole unutar organizacije mogu se svrstati po hijerarhiji IT kontrola, od politika na visokom nivou, izdatih od strane menadžmenta i odobrenih od strane Odbora, do konkretnih mehanizama kontrole ugrađenih u aplikacije. Sledi opis sedam grupa kontrola za koje su odgovorne određene grupe.

IT kontrole upravljanja

IT upravljanje je sastavni deo celokupnog upravljanja. Isto tako, IT kontrole na upravljačkom nivou su važan podskup celokupnog sistema internih kontrola unutar organizacije. IT kontrole

na upravljačkom nivou potpadaju pod nadležnost uprave i višeg rukovodećeg osoblja. Ipak, odgovornost uprave je da nadgleda sistem internih kontrola organizacije, a ne da vrši kontrole. Poslovi obavljanja svakodnevnih kontrolnih procesa su zadatak višeg rukovodećeg osoblja.

Kao što je predstavljeno na slici, IT kontrole upravljanja uključuju IT politike. Ove politike određuju prirodu kontrola koje treba obaviti i one se ,na primer, odnose na:

- Opštu politiku na nivou sigurnosti i privatnosti u celoj organizaciji.
- Izjavu o klasifikaciji informacija i pravu pristupa na svakom od nivoa.
- Definiciju koncepta podataka i vlasništva nad sistemom, kao i ovlašćenje potrebno za proizvodnju, modifikovanje ili brisanje informacija.
- Personalne politike koje definišu i nameću uslove za osoblje u osetljivim područjima.
- Definicije zahteva planiranja kontinuiteta celokupnog poslovanja. (15, 18)

IT kontrola rukovođenja

Odgovornost rukovodstva je da obezbedi adekvatan dizajn IT kontrola i njihovo efikasno obavljanje, uzimajući u obzir ciljeve organizacije, rizike koji prete postizanju tih ciljeva, kao i njene poslovne procese i resurse. Kao što je prikazano na slici, IT kontrole na nivou rukovođenja obuhvataju standarde, organizaciju i rukovođenje, i fizičke kontrole i kontrole okruženja.

IT standardi podržavaju IT politike tako što posebno definišu šta se zahteva za postizanje ciljeva organizacije. Ovi standardi treba, na primer, da obuhvate:

- **Proces razvoja sistema**. Kada organizacija razvija vlastite aplikacije, standardi se primenjuju u procesu dizajniranja, razvoja, testiranja, implementacije i održavanja sistema i programa.
- **Konfiguraciju sistemskog softvera**. Zbog toga što sistemski softver obezbeđuje brojne elemente za kontrolu u IT okruženju, standardi koji se odnose na obezbeđenje konfiguracije sistema počinju da dobijaju velik stepen prihvatanja i primene od strane vodećih organizacija i snabdevača iz oblasti IT.
- **Kontrole aplikacija**. Sve aplikacije koje podržavaju poslovne aktivnosti treba da se kontrolišu.
- **Struktura podataka**. Postojanje konzistentnog određivaja podataka u celom sistemu niza aplikacija, osigurava da posve različiti sistemi mogu pristupiti podacima s lakoćom, i sigurnosne kontrole za privatne i druge osetljive podatke mogu biti primenjene na jedinstven način.

- **Dokumentacija**. Standardi treba da odrede minimalni nivo potrebne dokumentacije za svaki aplikativni sistem ili IT instalaciju, kao i za različite klase aplikacija, procesa i procesnih centara (15, 18-19).

IT kontrole organizacije i rukovođenja pružaju osiguranje da je organizacija strukturirana sa jasno definisanim linijama izveštavanja i odgovornostima i implementiraju efikasne kontrolne procese. Tri važna aspekta ovih kontrola su: razdvajanje dužnosti, finansijske kontrole i kontrola promena rukovodstva.

- Razdvajanje dužnosti je vitalni element svih kontrola. Struktura organizacije ne treba dozvoliti da se sva odgovornost za sve procese obrade podataka zadrži na jednoj osobi. Funkcije nastanka, odobravanja, unosa, obrade i provere podataka treba da budu razdvojene, da bi se osiguralo da niko ne može da napravi grešku, propust, ili da odobri neku drugu neregularnost i/ili prikrije dokaze o tome. Kontrole razdvajanja dužnosti za aplikativne sisteme implementiraju se odobravanjem pristupnih privilegija u skladu sa poslovnim zahtevima za procesnim funkcijama i pristupnim informacijama (15, 22).
- Budući da organizacije ulažu značajna ulaganja u IT, budžetske i druge finansijske kontrole su neophodne da bi se osiguralo da tehnologija donosi predviđeni povrat investicije ili predloženu uštedu. Procesi rukovođenja treba da budu takvi da prikupljaju, analiziraju i izveštavaju o tim pitanjima. Nažalost, novi razvoj IT često nosi sa sobom ogromno prekoračenje troškova i propuštanje ostvarenja očekivanih ušteda u troškovima ili ostvarenja prihoda zbog pogrešnih ocena ili nedovoljnog planiranja (15, 22).
- Procesi promene rukovodstva obezbeđuju da promene u IT okruženju, sistemskom softveru, aplikativnim sistemima, i podacima koji se primenjuju, na način koji nameće razdvajanje dužnosti, osigurava da se promene obavljaju i implementiraju kako treba i preventiraju eksploataciju promena u svrhe prevara. Nedostatak promena u rukovodstvu može ozbiljno uticati na korisnost sistema i usluge (15, 22).

Fizičke kontrole i kontrole okruženja štite resurse informacionog sistema (hardver, softver, dokumentaciju i informacije) od slučajnog ili namernog oštećenja, pogrešne upotrebe ili gubitka. Ove kontrole uključuju, na primer:

- Smeštaj servera u zaključanim prostorijama sa ograničenim pristupom.
- Ograničen pristup serveru samo za određene osobe.
- Obezbeđenje detektora požara i sredstva za gašenje požara.

- Smeštaj osetljive opreme, aplikacija i podataka na udaljenosti od opasnosti okoline, kao što su plavna područja, vazdušne linije ili skladišta zapaljivih tvari. (15, 19-20)

IT tehničke kontrole

„Tehničke kontrole često čine okosnicu kontrolnog okvira rukovodstva. Ove kontrole su specifične za tehnologije u upotrebi unutar IT infrastrukture organizacije (15, 17).“ Kao što je prikazano na slici 1, tehničke kontrole uključuju kontrole sistemskog softvera, kontrole razvoja sistema i kontrole bazirane na aplikacijama.

Sistemski softver olakšava upotrebu sistemskog hardvera i uključuje, na primer, operativne sisteme, sisteme upravljanja bazama podataka, zaštitne zidove, i antivirus softvere. Kontrole sistemskog softvera ograničavaju logičan pristup sistemima i aplikacijama organizacije, nadziru upotrebu sistema, i obezbeđuju kontrole knjiženja. *Kontrole sistemskog softvera uključuju*, na primer:

- Prava pristupa dodeljena i kontrolisana u skladu sa navedonom politikom organizacije.
- Podelu dužnosti koja se izvršava pomoću sistemskog softvera i drugih kontrola aplikacije.
- Stalni nadzor nad ocenom nedopuštenog ulaska i ranjivosti, prevencija i otkrivanja na licu mesta.
- Testiranje nedopuštenog ulaska, koje se obavlja se na regularnoj osnovi.
- Usluge šifriranja, koje se primenjuju tamo gde je naveden zahtev za poverljivošću.
- Procese upravljanja promenama (uključujući upravljanje zakrpama), umesto osiguravanja strogo kontrolisanog procesa primene svih promena i zakrpa na softveru, sistemima, mrežnim komponentama i podacima. (15, 20)

Aplikativni sistemi, bez obzira na to da li su razvijeni unutar kuće ili su nabavljeni na tržištu, moraju efektivno i efikasno obrađivati informacije u skladu sa zahtevima korisnika. *Kontrole razvoja i nabavke sistema* uključuju, na primer, sledeće propise:

- Zahtevi korisnika treba da budu dokumentovani, i njihovo ispunjenje treba da bude merljivo.
- Dizajn sistema treba da prati formalni postupak kako bi se osiguralo da su zahtevi i kontrole korisnika ugrađeni u sistem.
- Razvoj sistema treba da se obavlja na koncipiran način, tako da osigura da obeležja zahteva i odobrenog dizajna budu ugrađeni u finalni proizvod.
- Testiranje treba da osigura da pojedinačni elementi sistema funkcionišu kako se zahteva, da vezni sklop (*interfa-*

ce) radi na očekivani način i da vlasnik sistema potvrđuje da je obezbeđena nameravana funkcionalnost.
- Procesi održavanja aplikacija trebalo bi da osiguraju da promene u aplikativnim sistemima prate dosledne (konzistentne) kontrolne modele. Upravljanje promenama mora da bude podložno strukturiranim procesima validacije uveravanja. (15, 20)

Kontrole bazirane na aplikacijama implementirane su da osiguraju da:
- Svi ulazni podaci budu tačni, potpuni, autorizovani i korektni.
- Svi podaci budu obrađeni kako je planirano.
- Svi sačuvani podaci budu tačni i potpuni.
- Svi rezultati budu tačni i potpuni.
- Redovno se vodi evidencija koja prati proces podataka od unosa do skladištenja i eventualnog izlaza. (15, 21)

Kontrole bazirane na aplikacijama uključuju, na primer:
- **Kontrole inputa** (kontrole unosa). Ove kontrole se uglavnom koriste za proveru integriteta podataka unesenih u poslovnu aplikaciju, bilo da se izvor unosi direktno od strane osoblja, na daljinu od strane poslovnog partnera ili putem omogućene veb-aplikacije (mrežne aplikacije).
- **Kontrole procesa** (kontrole za obradu). Ove kontrole pružaju automatizovana sredstva kako bi se osigurala potpuna, tačna i autorizirana obrada.
- **Kontrole autputa** (kontrole izlaza). Ove kontrole se odnose na to šta se radi sa podacima. One treba da porede ostvarene rezultate sa planiranim rezultatom i da ih provere u odnosu na ulazne podatke.
- **Kontrole integriteta**. Ove kontrole mogu nadgledati podatke u procesu obrade i/ili skladištenja, kako bi se osiguralo da podaci ostanu konzistentni (dosledni) i tačni.
- **Upravljanje tragom**. Istorijske kontrole obrade (*processing history controls*), koje se često nazivaju i revizorskim tragom, omogućavaju menadžmentu da prati transakcije od izvora do krajnjeg rezultata i da prati unazad, od rezultata do izvora, kako bi se identifikovale transakcije i događaji koji su knjiženi. (15, 21)

PRIMENA KONTINUIRANE REVIZIJE U IT PROCESIMA

Kao što se primenjuje kontinuirana revizija u svim poslovnim procesima isto tako je treba primenjivati i u informacionim sistemima, kako bi se primenio kontinuirani monitoring nad rizicima i kontrolama. Kontinuirana revizija predstavlja metod koji koriste revizori u obavljanju stalnih revizorskih aktivnosti.

Ove aktivnosti se kreću od stalnog ocenjivanja kontrole do neprekidnog ocenjivanja rizika. Tehnologija igra ključnu ulogu u stvaranju održive opcije kroz automatizaciju (16, 7). Kao što je opisano u GTAG3, kontinuirana revizija uključuje dve glavne aktivnosti:

- Kontinuirane ocene rizika, čija je svrha „označiti procese ili sisteme koji sadrže više nivoe rizika od očekivanih“ i
- Kontinuirane ocene kontrola, čija je svrha „fokusirati revizijsku pažnju na nedostatke kontrole što je moguće ranije“.

Ocena kontinuiranog monitoringa je treća sastavna komponenta kontinuirane revizije koju obavlja uprava. U oblastima organizacije u kojima uprava implementira efikasno odvijanje procesa monitoringa, interni revizori mogu obavljati manje stroge kontinuirane ocene rizika i kontrola. I obrnuto, ukoliko kontinuirani monitoring ne postoji ili je neefikasan, funkcija interne revizije mora obavljati rigoroznije ocene rizika i kontrola.

ZAKLJUČAK

Prošireni uticaj IT na strategije, informacione sisteme i procese organizacija značajno je uticao na profesiju interne revizije. Interni revizori treba da razumeju komponente modernog informacionog sistema – računarski hardver, mreže, računarski softver, baze podataka, informacije i ljude, i sve rizike i kontrole koje su u vezi sa ovim komponentama. Funkcija interne revizije u svojoj organizaciji treba da omogući sledeće u vezi sa rizicima i kontrolama:

a) da osigura da su IT rizici uključeni u godišnju procenu rizika; b) da daje uvid u razvoj novih sistema i IT infrastrukturne projekte; c) da integriše pregled IT-a u svaku reviziju; d) da shvati kako IT može poboljšati produktivnost interne revizije i kontrolne procese u celoj organizaciji; e) da daje preporuke za kontrolu kada se koristi nova tehnologija; f) da edukuje menadžment o novim informatičkim rizicima i kontrolama koje se mogu primeniti za ublažavanje tih rizika; g) da volontira za pilot IT projekte u cilju pružanja uvida u probleme kontrola pre uvođenja nove tehnologije; h) da zaposli IT stručnjake kao stručnjake za teme revizije koje uključuju veliku složenost IT-a; i) da obaveštava menadžment i upravni odbor o glavnim IT rizicima koji mogu uticati na organizaciju; j) da upozna novu tehnologiju koja utiče na organizaciju bez obzira da li je organizacija trenutno koristi.

IMPLICATIONS OF IT RISKS AND CONTROLS ON INTERNAL AUDITING

SUMMARY

Key words: interal IT audit, IT risks, IT controls, GTAG guides, standards of internal auditing

The implications of IT for internal auditors were addressed. IT has significantly changed the competencies internal auditors must possess and how they conduct their work. An internal audit function's capacity to provide valueadding assurance and consulting services is highly dependent on its IT expertise. All internal auditors need to have a baseline of technology knowledge and skills. This includes automated workpaper systems, data analytics, and IT terminology. The internal audit function can provide insights as to how the organization can best leverage advances in IT.

Internal audit functions need to understand their organizations' information systems and the IT risks that threaten the achievement of their organizations' business objectives. They also must be proficient in assessing their organizations' IT governance, risk management, and control processes and be able to effectively apply technology-based audit techniques.

LITERATURA

1. The Institute of Internal Auditors (IIA), International standards for the professional practice of internal auditing (Standards), IIA, USA, 2017, 11
2. GAIT Methodology, A risk-based approach to assessing the scope of IT general controls, The Institute of Internal Auditors, 2007, 18
3. Global Technology Audit Guide, Information Technology Risk and Controls, The Institute of Internal Auditors, 2012, 10-12
4. Global Technology Audit Guide, IT Essentials for Internal Auditors, The Institute of Internal Auditors, 2020, 11-21
5. Global Technology Audit Guide, Management of IT Auditing, The Institute of Internal Auditors, 2013, 8-9
6. Global Technology Audit Guide, Developing the IT Audit Plan, The Institute of Internal Auditors, 2008, 12-15
7. Global Technology Audit Guide, Auditing IT Projects, The Institute of Internal Auditors, 2009, 3-7, 14, 16-17
8. Global Technology Audit Guide, Auditing User-developed Applications, The Institute of Internal Auditors, 2010, 6-11
9. Global Technology Audit Guide, Business Continuity Management, The Institute of Internal Auditors, 2008, 5, 8-11.
10. Global Technology Audit Guide, Assessing Cybersecurity Risk, The Institute of Internal Auditors, 2008, 2-22
11. Global Technology Audit Guide, Identity and Access Management, The Institute of Internal Auditors, 2007, 1-2, 4, 12-16
12. Global Technology Audit Guide, Auditing Application Controls, The Institute of Internal Auditors, 2007, 4-10
13. The IIA Practice Guide, Auditing Privacy Risks, The Institute of Internal Auditors, 2012, 2, 5-6, 9-10, 13-21
14. Global Technology Audit Guide, Fraud Prevention and Detection in an Automated World, The Institute of Internal Auditors, 2009, 2-8, 11-13, 16-17
15. Global Technology Audit Guide, Information Technology Risk and Controls, The Institute of Internal Auditors, 2012, 16
16. Global Technology Audit Guide, Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment, The Institute of Internal Auditors, 2005, 7