UDC: 657.6:007:004 Info M str. 4-10

IT REVIZIJA U SAVREMENIM ORGANIZACIJAMA
IT AUDIT IN MODERN ORGANIZATIONS

Kristijan Lazić, Dragan Jovičić, Vladan Pantović

REZIME: IT revizija predstavlja ispitivanje (proveru) i procenu informacionih tehnologija organizacije, koju sprovode lica sa adekvatnim stručnim znanjima – IT revizori. Sprovođenje IT revizije predstavlja uređen, definisan proces, koji prolazi kroz tri ključne faze: 1) planiranje revizorskog angažmana, 2) sprovođenje angažmana IT revizije i 3) izveštavanje i praćenje rezultata IT revizije. Sertifikacija IT revizora predstavlja važan korak u potvrdi znanja i veština koje revizor treba da poseduje, a izbor između osnovnih i naprednijih sertifikata pruža priliku IT revizorima na svim nivoima znanja da se konstantno unapređuju. Prednosti IT revizije su višestruke, prvenstveno u savremenim organizacijama koje svoje poslovanje temelje na naprednom i zrelom informacionom sistemu.

KLJUČNE REČI: IT revizija, IT revizor, sprovođenje IT revizije, sertifikati za IT revizore, budućnost IT revizije

ABSTRACT: An IT audit is an examination (verification) and assessment of an organization's information technologies, carried out by personnel with adequate professional knowledge - IT auditors. Conducting an IT audit is a structured, defined process that goes through three key phases: 1) planning the audit engagement, 2) conducting the IT audit engagement, and 3) reporting and monitoring the results of the IT audit. IT auditor certification is an important step in confirming the knowledge and skills that an auditor should possess, and the choice between basic and more advanced certificates provides an opportunity for IT auditors at all levels of knowledge to constantly improve themselves. The advantages of an IT audit are multiple, primarily in modern organizations that base their operations on the advanced and mature information system.

KEY WORDS: IT audit, IT Auditor, IT audit engagement, IT audit certificates, future of IT audit

UVOD

Informacione tehnologije predstavljaju osnov modernog poslovanja u skoro svim oblastima i industrijama – navedena činjenica u praksi je zamenila višegodišnju premisu da je IT „samo" servis čija je osnovna (i često jedina) funkcija bila da podrži sve ostale poslovne procese. Danas su servisi poput mobilnog bankarstva, usluga državne administracije (npr. *on-line* izdavanje dokumenata), različitih vidova *on-line* kupovine i dostave, samo neki od primera koji su trajno izmenili i modele poslovanja i uobičajene navike korisnika i klijenata. Nije pogrešno reći da je „IT je samo servis" zamenilo pravilo da „nema biznisa ako nema IT-ja". To potvrđuje i činjenica da organizacije, koje bar u nekom svom segmentu (npr. oglašavanje i marketing), nisu krenule put digitalne transformacije, drastično umanjuju priliku za opstanak na tržištu.

Poslovanje koje se u potpunosti oslanja na digitalne tehnologije, u značajnoj meri povećava izloženost rizicima informacionih sistema. Uređen IT sistem u kome su procesi definisani, kontrole implementirane a rizici adekvatno procenjeni, više se ne smatra „skupim i komplikovanim" već neophodnom potrebom i kapitalnim ulaganjem. Vesti o kompanijama i organizacijama na svim meridijanima, koje su pretrpele značajnu finansijsku i reputacionu štetu usled narušene poverljivosti, integriteta i dostupnosti informacionog sistema, predstavljaju opomenu i podsetnik da je upravljanje IT rizicima kroz revizije informacionih sistema, neophodna aktivnost „digitalne higijene" i mali trošak koji donosi mnogo benefita.

REVIZIJA I INTERNA REVIZIJA

Pojam revizije (engl. *audit*) je višeznačan i podrazumeva različite tipove metodoloških pregleda i provera, obično od strane nezavisnog tela [1] [2] [3]. Prvobitno se pojam revizije odnosio na finansijske provere, da bi se tokom 20. veka postepeno formirale profesionalne prakse revizije poslovnih procesa, proizvodnje, novih tehnologija, kao i specijalizovanih provera poput istraga.

Uvidevši važnost i korist funkcije revizije, organizacije su vremenom formirale timove unutrašnje revizije, kako bi pravovremeno identifikovali rizike poslovanja i primenili adekvatne korektivne mere za njihovo smanjenje, ali i postigli zahtevani nivo usklađenosti sa zakonskom regulativom i sprečili potencijalne finansijske i druge implikacije koje bi mogle da proisteknu iz zaključaka (nalaza) eksternih provera. Međunarodni okvir profesionalnih praksi (MOPP), publikacija međunarodnog instituta internih revizora [4], definiše internu reviziju kao „*nezavisnu i objektivnu uslugu uveravanja i savetovanja osmišljenu s ciljem dodavanja vrednosti i unapređenja poslovanja organizacije. Ona pomaže organizaciji u ostvarivanju njenih ciljeva putem sistematičnog i disciplinovanog pristupa za vrednovanje i poboljšanje efektivnosti upravljanja organizacijom, upravljanja rizicima i kontrolnih procesa.*" [5].

Interna revizija, i interna IT revizija kao deo organizacione jedinice revizije, u modernim organizacijama predstavlja poslednju „liniju odbrane", kako u oblasti analize rizika, praćenja implementacije korektivnih mera, tako i savetodavnoj ulozi u svim važnim projektima i značajnijim promena poslovnog okruženja.

IT REVIZIJA I INTERNA IT REVIZIJA

Revizija informacionih sistema i tehnologija (skraćeno IT revizija), prestavlja ispitivanje (proveru) i procenu informacionih tehnologija organizacije [6]. Koncept IT revizije formiran je sredinom 1960-ih, nakon čega je IT revizija je prošla kroz brojne promene, uglavnom zbog napretka tehnologije i sve veće zavisnosti modernog poslovanja od informacionih

tehnologija. Moderna IT revizija predstavlja definisan sistem procesa, metodologija i postupaka, kako bi se na adekvatan način osiguralo upravljanje kompleksnim IT rizicima.

Osnovni zadaci IT revizije je utvrđivanje da li IT kontrole štite imovinu organizacije, obezbeđuju integritet podataka, kao i da li su usklađene sa opštim ciljevima poslovanja. IT revizori ispituju ne samo logičke i fizičke (bezbednosne) kontrole, već često i opšte poslovne i finansijske kontrole koje uključuju IT sisteme. IT revizija treba da pruži uverenje da kontrole i procesi vezani za IT ispravno funkcionišu, odnosno da preporuči mere i isprati njihovu implementaciju kako bi se ukupni identifikovan IT rizik smanjio na prihvatljiv nivo [7]. Primarni ciljevi IT revizije uključuju:

- Procenu rizika IT sistema, IT procesa, podataka u elektronskom formatu i ostale tipove informacione / digitalne imovine organizacije, kao i predlaganje preporuka i mera za smanjenje ukupnog IT rizika.
- Proveru da li su IT kontrole implementirane, da li su efektivne i da li se redovno održavaju na adekvatnom nivou.
- Pružanje uveravanja da su procesi upravljanja informacijama u skladu sa Zakonima, politikama i standardima specifičnim za oblasti informacionih tehnologija i informacione bezbednosti.
- Utvrđivanje uticaja uočenih neefikasnosti kontrola u IT sistemima na ostale poslovne procese (najčešće finansijsko izveštavanje).

IT revizije mogu biti revizije opštih IT kontrola (ITGC[1]) ili revizije posebnih oblasti informacionog sistema, poput:

- Revizija IT sistema i aplikacija: provere koje imaju za cilj da utvrde da li su sistemi i aplikacije odgovarajući, efikasni i adekvatno kontrolisani. Posebne revizije koje se fokusiraju se na poslovne IT sisteme usmerene na (ključne) poslovne procese, često se sprovode u sklopu finansijskih revizija.
- Revizije razvoja (aplikativnih) sistema utvrđuju da li kontrole u razvoju softvera ispunjavaju ciljeve organizacije sa poslovnog, tehnološkog i bezbednosnog aspekta.
- Revizije upravljanja IT organizacijom (Odeljenjem, Sektorom, Službom itd.) i poslovnom arhitekturom proveravaju da li je IT rukovodstvo IT razvilo organizacionu strukturu i procedure kako bi se osiguralo kontrolisano i efikasno okruženje za obradu informacija.
- Revizije sistema za skladištenje podataka (npr. baze podataka i repozitorijuma za izveštavanje), utvrđuju da li su kontrole kojima se osiguravaju blagovremena, tačna i efikasna obrada podataka od strane aplikativnih sistema implementirane i adekvatne.
- Revizije mrežne arhitekture i protoka podataka, čiji cilj je provera adekvatnosti telekomunikacionih kontrola, poput garantovanog nivoa brzine protoka podataka ili dostupnosti *on-line* servisa.

Takođe, u praksi se često sprovode i revizije IT projekata i tehnoloških inovacija (evaluacija rizika postojećih i novih projekata), revizije informacione bezbednosti i druge.

[1] ITGC – *Information Technology General Controls*.

Zadaci, ciljevi i postupci sprovođenja IT revizije, u najvećoj meri su isti za eksternu (spoljnu) IT reviziju i za internu IT reviziju. Interna IT revizija deo je sektora interne revizije organizacije, i sprovode je zaposleni interni IT revizori organizacije. Interni IT revizori, u zavisnosti od tipa angažmana, detaljno testiraju sistem internih IT kontrola. Eksterni IT revizori angažovani su od strane organizacije kao treća lica, što im obezbeđuje viši stepen nezavisnosti, ali i ograničeno vreme za sprovođenje detaljnije analize IT sistema, usled nižeg nivoa poznavanja poslovnih procesa organizacije. U praksi, eksterni IT revizori se oslanjaju na izveštaje (nalaze i preporuke) internih IT revizora, i fokusiraju se na identifikovane rizike najvišeg nivoa kao i na IT kontrole koje obezbeđuju ključne IT procese.

BENEFITI IT REVIZIJE

Svaka organizacija može imati koristi od redovnih ili periodičnih IT revizija. IT Revizori se smatraju nezavisnim od IT organizacije i od njih se očekuje da pažljivo i nepristrasno ispitaju IT kontrole, identifikujući šta funkcioniše, a šta ne, izveštavajući objektivno o svojim nalazima i izdajući preporuke za smanjenje izloženosti rizicima. Iskusni (IT) lideri prepoznaju značaj IT revizija kao važnog pokazatelja stanja informacionog sistema, prvenstveno oblasti i procesa za koje postoji osnovana sumnja da ne ispunjavaju očekivanja. Redovne IT revizije, koje se sprovode u skladu sa standardima struke i planu zasnovanom na rizicima, obezbeđuju IT organizaciji „alat“ kojim se minimizuju pretnje i osigurava adekvatno upravlja IT sistemom.

S obzirom na to koliko su moderni informacioni sistemi vreme složeni i sve više zavisni od on-line servisa i trećih strana pružaoca usluga (npr. oslanjanje na *cloud* tehnologije), organizacije sprovode IT revizije, između ostalog, kako bi dokazali rukovodstvu da njihovi IT sistemi funkcionišu usaglašeni sa poslovnim procesima, očekivanjima klijenata i u skladu sa zakonskom regulativom i standardima (dobrom stručnom praksom) industrije u kojoj organizacija posluje. Takođe, IT revizije pružaju važan dokaz o usklađenosti klijentima ali i regulatornim telima i nadležnim državnim agencijama.

IT REVIZOR

IT reviziju sprovodi revizor specijalizovan za informacione sisteme – IT revizor. IT revizor je odgovoran za procenu rizika opštih IT kontrola (ITGC), kao i uticaja IT rizika na druge rizike, prvenstveno na finansijske i regulatorne. IT revizor sprovodi IT revizije sam, ili kao deo tima IT revizora kod kompleksnih i IT revizija gde su potrebna specifična znanja. Takođe, IT revizor često je deo tima drugih revizora, najčešće finansijskih, kome pomaže u sprovođenju revizije kontrola u aplikacijama koje podržavaju finansijsko izveštavanje ili ključne poslovne procese preduzeća. IT revizori mogu biti interni (deo su organizacije) ili eksterni, i mogu biti opšti IT revizori ili se specijalizovati za određene oblasti kao što su veštačka inteligencija, usklađenost sa IT regulativom ili sajber bezbednost. Interni i eksterni IT revizori u praksi obavljaju slične zadatke.

OKVIR SPROVOĐENJA IT REVIZIJE

Smernice za sprovođenje interne IT revizije definisane su različitim okvirima, poput Međunarodnog okvira profesionalne prakse[2] Instituta internih revizora [8] (Globalnih standarda interne revizije [9] i posebno Smernica za tehnološke revizije[3] [10], Okvira IT revizije[4] [11] instituta ISACA, kao i drugom relevantnom stručnom praksom [12]. Većina organizacija uređuje procese IT revizije usklađujući ih prvenstveno sa MOPP i ITAF standardima, prilagođavajući radne programe korišćenjem GTAG smernica. Iako usklađivanje sa navedenim okvirima ne predstavlja formalnu obavezu IT revizora, uređen i definisan proces sprovođenja aktivnosti u IT reviziji, obezbeđuje transparentnost i efikasnost u radu, kao i konzistentnost sa aktivnostima interne revizije drugih organizacija, omogućavajući optimalno iskorišćenje revizorskih resursa.

IT revizija u praksi se najčešće sprovodi u skladu sa smernicama provođenja opšte revizije, poštujući sve faze / korake revizorskog angažmana. MOPP pruža strukturni plan i sveobuhvatni sistem koji olakšava dosledan razvoj, tumačenje i primenu korpusa znanja korisnog za profesiju [5], i sastoji se od Globalnih standarda interne revizije, Tematskih zahteva i Globalnih smernica. Faze revizorskog angažmana, definisane su Globalnim standardima interne revizije, i to domenom „V: Pružanje usluga interne revizije“, odnosno sledećim principima:

- Princip 13 Planirajte angažmane efektivno.
- Princip 14 Sprovedite angažman.
- Princip 15 Saopštite rezultate angažmana i nadzirite planove aktivnosti[5].

Svaki od navedenih principa sadrži više faza i aktivnosti, koje su detaljno opisane okvirom i čije dosledno poštovanje obezbeđuje visok kvalitet celokupnog revizorskog angažmana.

FAZA 1: PLANIRANJE REVIZORSKOG ANGAŽMANA

Planiranje revizorskog angažmana predstavlja „*proces tokom kojeg interni revizori prikupljaju informacije, ocenjuju i utvrđuju prioritet rizika u vezi sa aktivnošću koja se pregleda, utvrđuju ciljeve i obuhvat angažmana, identifikuju kriterijume za vrednovanje i izrađuju program rada angažmana.*“ [5].

Fazu planiranja neophodno je sveobuhvatno sprovesti na sistematičan, disciplinovan način. Aktivnosti faze planiranja revizorskog angažmana, detaljno se opisuju internim aktima odeljenja revizije u formi metodološkog pristupa koji se sprovodi u praksi. Neadekvatna, površna priprema revizorskog angažmana, može u značajnom meri negativno uticati na ostale faze revizije, prvenstveno u pogrešnoj identifikaciji oblasti sa najvećim rizicima. Fazu planiranja uspostavlja i odobrava izvršni rukovodilac revizije.

Prvi korak faze planiranja predstavlja razumevanje i dokumentovanje početnih očekivanja od angažmana, i priprema za naredne korake koji očekivanja treba da potvrde ili u određenim aspektima dopune. U tu svrhu, prikupljaju se najvažnije informacije koje treba da omoguće razumevanje revidirane organizacije, relevantnih procesa za predmet revizije i preliminarnih ciljeva revizije. Najčešći tipovi dokumenata koji se u fazi planiranja prikupljaju su dokumenti interne regulative (politike, standardi, smernice, standardne operativne procedure, uputstva i sl.) koji su dostupni većini zaposlenih u organizaciji ili zaposlenima u revidiranim organizacionim jedinicama.

Za skladištenje prikupljenih informacija u elektronskom formatu, koje uključuju i kreirane inicijalne, preliminarne beleške i zapažanja, IT revizori najčešće koriste namenske repozitorijume (deljene lokacije / foldere za smeštaj fajlova, DMS[6] softvere poput SharePoint portala i dr.). Takođe, u fazi planiranja često se mogu prikupiti i kopije štampanih važećih verzija raznih dokumenata (npr. potpisani ugovori), iako u praksi informacije u „*hard copy*“ formatu sve više predstavljaju izuzetak[7].

Važno je naglasiti da u fazi planiranja IT revizori mogu sprovesti i određene operativne aktivnosti prikupljanja informacija iz produkcionog tehničkih elemenata informacionog sistema (npr. jednostavni upiti nad bazama podataka), ali navedene aktivnosti u ranoj fazi revizorskog angažmana predstavljaju izuzetak i neophodno je da budu pažljivo planirane, obrazložene, odobrene i izvedene uz maksimalne mere opreza i podršku stručnih lica. Iako se opisani pristup različitim segmentima produkcionog sistema „očekuje“ u fazi sprovođenja angažmana („terenskog rada“), u fazi planiranja (redovnih) IT revizija to nije uobičajena praksa i najčešće se sprovodi u specijalnim IT revizijama (npr. istrage pronevera, sajber napada, kao i posebni angažmani drugih specijalnih revizija, najčešće finansijskih i regulatornih itd.).

U fazi planiranja, IT revizori obavljaju i prve, preliminarne analize rizika, čiji se rezultati u daljem toku angažmana mogu izmeniti u odnosu na nove dostupne i dodatno prikupljene informacije. Preliminarna analiza rizika ima za cilj da usmeri i prioritizuje aktivnosti na angažmanu u oblastima gde je identifikovan najviši rizik, ali i u cilju pripreme plana angažovanja resursa, preciznijeg i detaljnijeg određivanja obima (obuhvata) i ciljeva revizije.

Na osnovu prikupljenih inicijalnih informacija i preliminarne analize rizika, određuju se potrebni resursi za sprovođenje revizorskog angažmana, i utvrđuju kriterijumi u odnosu na koje će „izmeren“ sistem internih kontrola. Resursi podrazumevaju broj izvršilaca, neophodna (stručna) znanja i veštine, tehničke resurse (npr. softverska rešenja za analizu većeg broja podataka) i sl. Rezultat faze planiranja, predstavlja program rada interne revizije, koji definiše korake, obim / okvir (engl. *scope*) revizije i precizan vremenski plan izvršenja aktivnosti. [5] Program rada predstavlja osnov za aktivnosti faze „Princip 14 – sprovođenje angažmana“ i odobrava se od strane rukovodioca interne IT revizije.

---

2 *International Professional Practices Framework (IPPF)*.

3 *Global Technology Audit Guides (GTAG).*

4 *IT Audit Framework (ITAF).*

5 U praksi, princip 15 često se razdvaja na fazu izveštavanja i fazu praćenja, radi efikasnijeg sprovođenja i grupisanja (podele) aktivnosti.

6 *Document Management System*, sistemi / softveri za upravljanje dokumentima.

7 Čest razlog za prikupljanje kopija u papirnom formatu je dokaz da su dokumenti formalno važeći jer sadrže potpise nadležnih na naslovnoj strani. Sa napretkom multifunkcionalnih uređaja, revizori danas češće koriste opciju “skeniraj I pošalji na mejl” umesto nekadašnjeg fotokopiranja dokumenata.

FAZA 2: SPROVOĐENJE ANGAŽMANA IT REVIZIJE

Nakon faze planiranja, revizorski angažman prelazi u fazu sprovođenja programa rada. Program rada sprovodi se disciplinovano, na način da se svaka planirana aktivnost realizuje sa jasnom namerom da se ispuni neki od manjih ciljeva revizije, koji zbirno doprinose ukupnim ciljevima revizije.

U fazi sprovođenja revizije (u praksi se često koristi i termin „terenski rad“), IT revizori prikupljaju dodatne informacije relevantne za reviziju, vrše dodatne analize tih informacija i vrednuju ih u cilju izvođenja adekvatnih i relevantnih dokaza. Aktivnosti sprovedene u okviru terenskog rada, omogućavaju IT revizorima da:

a) identifikuju potencijalne nalaze i utvrde njihov ukupni uticaj / značaj,
b) utvrde uzroke, posledice i ocene rizike nalaza, i
c) sačine zaključke, koji uključuju formulisane mere / preporuke, usklađene sa rukovodstvom i revidiranim entitetima / vlasnicima procesa, u cilju otklanjanja identifikovanih nedostataka i izradi planova koji imaju cilj smanjenja rizika na prihvatljiv nivo.

Blok nalaza interne IT revizije najčešće se sastoji od više logičkih, međusobno povezanih celina. Česta praksa je da pre teksta nalaza, postoji formulisano kratko objašnjenje koje treba da pomogne razumevanje kontrolnog okruženja (korišćenih tehnologija, procesa, ključnih aktivnosti i zaduženja zaposlenih i sl.), u meri u kojoj je to neophodno da se rukovodstvo uputi u stanje koje je IT revizor identifikovao (često se koristi odrednica „*as-is* stanje“). U okviru kratkog objašnjenja, navode se i korišćeni kriterijumi u odnosu na koje je *as-is* stanje vrednovano, tj. obrazlažu se razlozi njihovog korišćenja i relevantnost navođenja. U zavisnosti od stila pisanja izveštaja IT revizije, objašnjenje može sadržati i metode korišćene u pribavljanju dokaza, postupak izvođenja dokaza i druge elemente, što predstavlja uobičajenu praksu u detaljnim izveštajima IT revizije.

Nakon kratkog objašnjenja, formuliše se sam nalaz IT revizije, koji treba da bude jasan, precizan i da na dovoljno jednostavan način iskaže uočeno odstupanje u odnosu na korišćene kriterijume. Nalazi se uobičajeno formulišu u jednoj, najviše par jasnih rečenica. U izuzetnim situacijama, kada nalaz sadrži više odstupanja koja je potrebno posebno naglasiti, preporučeno je da se koristi stil nabrajanja, odnosno da se formuliše više „manjih“ nalaza, ukoliko pripadaju istoj revidiranoj oblasti. Nalazi IT revizije treba da uzmu u obzir da su korisnici izveštaja revizije visoko rukovodstvo, ali i operativni menadžment, te da nalaz ne treba da sadrži složene stručne odrednice, ali da ne sme ni da ostavi prostor proizvoljnom razumevanju (usled nepreciznosti pisanja) od strane lica koje će biti odgovorno da implementaciju preporuka i mera.

Nalaz IT revizije obavezno prati i objašnjenje rizika, i to procenu inherentnog rizika (rizik koji je prisutan pre primene bilo kakvih mera interne kontrole odnosno uz neadekvatne i neefikasne mere interne kontrole), kao i procenu rezidualnog rizika tj. rizika nakon primene preporučenih (ili drugih, adekvatnih) mera. Procena rizika vrši se u odnosu na uspostavljene kriterijume, i radi jednostavnijeg razumevanja, najčešće se primenjuje kvalitativna metodologija. Ukupan rizik, kao kombinacija izmerenog uticaja i verovatnoće pojave štetnog događaja, predstavlja važnu informaciju u odnosu na koju rukovodstvo treba da odredi prioritete rešavanja identifikovanih problema.

Zaključci nalaza predstavljaju preporuke koje IT revizija izdaje u cilju efikasne implementacije kontrola, a čija svrha i cilj su smanjenje rizika na prihvatljiv nivo. Preporuke treba da budu jasne, efikasne, finansijski prihvatljive, da (po mogućstvu) utiču pozitivno i na posledice i na uzroke identifikovanih rizika, kao i da budu usaglašene sa revidiranim entitetima i rukovodstvom. U situaciji identifikovanja nalaza viših nivoa rizika, kao i nalaza koji opisuju sistemske rizike koji zahtevaju značajnije angažovanje ljudskih resursa, materijalnih i finansijskih sredstava, IT revizor može izdati više preporuka, kako bi pomogao revidiranima da postepeno, uz pristup baziran na riziku, rešavaju kompleksnije situacije. Takođe, na ovaj nečim se olakšava praćenje implementacije internih kontrola, i omogućava, da se u slučaju potrebe, izvrši vanredna revizija ograničenog obima, uz ažuriranje nalaza novim informacijama (najčešće uz smanjenje inherentnog rizika).

Nalazi IT revizije treba da budu utemeljeni na čvrstim dokazima, na način da ponovljena revizija od strane drugog tima, a na osnovu prikupljenih informacija i dokaza, može da izvede iste zaključke. Postupak izvođenja dokaza neophodno je urediti internim aktima odeljenja revizije, uz kontinuirane obuke IT revizora [13] [14] koje će osigurati visok nivo stručnih veština. U posebnim slučajevima (npr. u okviru istraga), dokazima je neophodno obezbediti atribut neporecivosti, odnosno nemogućnost revidiranih da osporavaju način, vreme pribavljanja i suštinu dokaza.

FAZA 3: IZVEŠTAVANJE I PRAĆENJE REZULTATA IT REVIZIJE

Izveštaj interne revizije predstavlja finalni proizvod rada revizorskog tima, i u sebi sadrži niz elemenata i struktura, poput obima revizije, informacija o revizorskom timu, korišćenim tehnikama revizije, pozicije i imena intervjuisanih lica itd. Najvažniji deo izveštaja IT revizije predstavljaju blokovi nalaza koji su formirani u okviru faze terenskog rada. Izveštaji se uobičajeno razlikuju među organizacijama, ali dobra praksa podrazumeva sledeće smernice prilikom njihovog sastavljanja:

a) Srodni nalazi (iz iste revidirane oblasti) se grupišu u okviru poglavlja.
b) Nalazi sa identifikovanim višim nivoom rizika se nalaze prvi u okviru svojih poglavlja, ukoliko to ne utiče u značajnoj meri na praćenje toka izveštaja.
c) Tabela koja sadrži nalaze, preporuke, procenjene rizike i druge elemente od značaja (zadužene osobe, rok za implementaciju mera, odgovore revidiranih i sl.) predstavlja sastavni deo izveštaja i osnovu za pod fazu praćenja.

Izveštaju IT revizije se dostavljaju svim zainteresovani stranama, i uobičajeno su označeni višim nivoom poverljivosti u odnosu na druge dokumente organizacije.

Pod faza praćenja ispunjenja nalaza, počinje nakon izdavanja finalnog izveštaja IT revizije, i sprovodi se kao zasebna, periodična aktivnost, opisana radnim procedurama, ili kroz namenske revizije praćenja. Ukoliko se organizacija odluči za prvi pristup, praćenje može da se automatizuje korišćenjem nekog od softverskih alata, koji će u definisanim vremenskim intervalima obaveštavati zadužena / odgovorna lica za implementaciju internih kontrola (vlasnike nalaza i preporuka) kroz sistem notifikacija (najčešće e-mail porukom). Nakon toga, zadužena lica dostavljaju svoje odgovore (i eventualno, adekvatne dokaze) što inicira procenu situacije od strane IT revizora, nakon čega se o rezultatima procene obaveštavaju zadužena lica i periodično, visoko rukovodstvo. U određenim situacijama, ukoliko je tehnički moguće i razumno, provera ispunjenja odgovarajućih preporuka može se automatizovati (npr. automatska detekcija prekida rada sistema dostavlja notifikaciju; po prijemu notifikacije, sistem zatvara nalaz revizije), čime se optimizuje vreme i smanjuje angažovanje IT revizora.

Namenske revizije praćenja (tzv. „*follow-up* revizije"), koje se koriste kao drugi način za praćenje nalaza, u obimu revizije opredeljuju proveru stanja nalaza ocenjenih nekih od visokih rizika, srodnih po tipu (npr. baze podataka ili nalazi iz oblasti upravljanja korisničkim identitetima), sprovode se na sličan način kao i druge IT revizije. Ipak, treba naglasiti da se u ovoj situaciji, u praksi često dešava da se IT revizor identifikuje i nove nalaze, koji u trenutku vršenja prvobitne IT revizije nisu postojali (npr. usled promena koje su dovele do degradacije kontrolnog okruženja u određenoj oblasti). Izveštaji *follow-up* revizije koriste se za ažuriranje stanja postojećih nalaza, odnosno za zatvaranja nalaza čije su preporuke ispunjene, kao i za ažuriranje stanja rizika kod nalaza koji još uvek nisu zatvoreni.

PREPORUČENA STRUČNA ZNANJA I VEŠTINE IT REVIZORA

Za uspešno sprovođenje IT revizije, neophodno je da revizorski tim ima adekvatan nivo tehničkih i „mekih"[8] znanja i veština, kako bi efikasno obavili delegirane zadatke.

Generalna (opšta) znanja, neophodna su kako bi IT revizor mogao da sagleda sve aspekte IT revizije, podjednako sa poslovnog i tehničkog aspekta. Opšta znanja smatraju se preporučljivim za većinu radnih pozicija u modernim organizacijama, ali u IT reviziji su neke od specifičnih znanja i veština neophodne (obavezne) kako se revizorski angažman uspešno realizovao. Generalna znanja koja se očekuju od IT revizora su sledeća:

1. Analitičke veštine, sposobnost analize kompleksnih IT sistema, njihovih ključnih elemenata i međuzavisnosti, kao i identifikacija tehničkih slabosti.
2. Kritičko razmišljanje, sposobnost donošenja objektivnih zaključaka na osnovu podataka, činjenica i ispravne procene dokaza.
3. Komunikacione veštine, sposobnost da se jasno prenesu sve činjenice (nalazi, preporuke, rizici itd.) tehničkim i „ne tehničkim" kolegama. Važno je naglasiti da su komunikacione veštine usko povezane sa prezentacionim veštinama, odnosno sposobnosti da se rukovodstvu prenesu najvažnije poruke na efikasan način, često putem prezentacija.
4. Visok nivo pismenog izražavanja, kako u cilju izrade jasnih i konciznih izveštaja (dokumentovanje nalaza), tako i u ostalim vidovima komunikacije na angažmanu (najava angažmana, zahtevi za dostavom dokaza i dodatnih informacija email porukama i sl.)
5. Sposobnost rešavanja problema – brzo pronalaženje efikasnih rešenja za otkrivene slabosti.
6. Upravljanje vremenom, sposobnost izvršenja više zadataka pod pritiskom i u zadatom roku, veština prioritizacije zadataka i fokus na kritične aktivnosti.
7. Interpersonalne veštine, timski rad i stav, saradnja sa različitim organizacionim delovima, stručnjacima i eksternim partnerima. Saradnja sa drugim revizorima, IT osobljem i menadžmentom.
8. Liderstvo, vođenje i motivisanje drugih, delegiranje zadataka i preuzimanje odgovornosti za rezultate.
9. Kontinuirano usavršavanje i učenje. Kako se IT tehnologije brzo menjaju, neophodno je da IT revizor permanentno prati novosti, trendove i usvaja nova znanja, prvenstveno ona koja su relevantna za organizaciju i industriju u kojoj organizacija pripada.
10. Etika i profesionalnost predstavljaju jedan od „kamena temeljaca" za uspešnog IT revizora. Poverljivost, objektivnost i visok integritet neophodni su za dugogodišnju karijeru, prvenstveno ako se ima na umu da su u modernim organizacijama najvažnije informacije u najvećoj meri u elektronskoj formi i da predstavljaju jedan od najvažnijih i najvrednijih resursa organizacije.
11. Prilagodljivost, fleksibilnost u radu sa različitim organizacionim strukturama i tehnologijama, kao i spremnost na improvizaciju u meri u kojoj to ne ugrožava principe profesionalne prakse, etiku i integritet.
12. Kreativnost, formulisanje novih ideja i pronalaženje inovativnih rešenja.

Generalna znanja i „meke veštine" dovode do značajno boljih performansi na poslu, što utiče na viši kvalitet revizije ili mogućnost sprovođenja više revizija u toku jednog revizorskog ciklusa. Takođe, razvijene interpersonalne veštine kreiraju i unapređuju pozitivne odnose sa kolegama, klijentima i trećim stranama, stvarajući poverenje i omogućavajući revizoru da identifikovanim rizicima i preporukama doprinese unapređenju kontrolnog okruženja. Na ličnom planu, visok nivo opštiv veština često daje znatnu prednost kandidatima koji pokazuju ove osobine, omogućavajući i lični rast IT revizora i sposobnost snalaženja u različitim životnim situacijama.

Tehnička znanja podrazumevaju poznavanje i razumevanje najmanje sledećih IT oblasti:

1. Poznavanje osnova računarstva i osnovnih IT koncepata, poput osnovnih elemenata računara, IT veličina i teorijskih principa (binarni i heksadecimalni sistemi, osnovne jedinice za smeštaj i brzine prenosa podataka, kapacitete i brzine hardverskih komponenti, osnovne formate podataka i sl.).
2. Poznavanje operativnih sistema (*Windows*, *Linux*) na nivou korisnika (preporučljivo je i poznavanje naprednijeg korišćenja, poput instalacije i podešavanja aplikacija i komponenata operativnog sistema i sl.).

[8] „Meke" veštine (engl. *soft skills*) predstavljaju lične osobine koje ljudi koriste za interakciju sa okolinom. Često se nazivaju i međuljudskim veštinama i ključne su za uspeh u sprovođenju revizije.

3. Poznavanje sistema za upravljanje bazama podataka (SQL, NoSQL) i mogućnost efikasnog korišćenja jednostavnih upita za pribavljanje podataka (IT revizija podataka često zahteva rad sa bazama podataka).
4. Razumevanje računarskih mreža, tipova računarskih mreža i osnovnih elemenata prenosa informacija.
5. Poznavanje generalne informacione bezbednosti na nivou računarskih mreža, zaštite podataka, operativnih sistema i fizičke zaštite.
6. Razumevanje procesa upravljanja IT projektima, poznavanje *Agile*, *Scrum* i *Waterfall* metodologija vođenja projekata.
7. Adekvatno poznavanje zakonske regulative iz oblasti informacionih tehnologija i informacione bezbednosti (npr. Zakon o informacionoj bezbednosti, Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije Narodne Banke Srbije), kao i relevantnih IT okvira, standardi i dobre stručne prakse poput ISO 27001, CobiT, ITIL, NIST *Special Publications* itd.)

Napredna tehnička znanja, u IT reviziji najčešće se obezbeđuje privremenim angažovanjem trećih strana – eksperata[9]. Njihov se rad usmerava na oblasti koje zahtevaju viši nivo specijalizacije, u cilju boljeg razumevanja rizika koji mogu biti posledica neadekvatnog korišćenja naprednih tehnologija. Ne očekuje se da IT revizor poznaje napredni nivo znanja iz informacionih tehnologija za koje je neophodno formalno visoko obrazovanje ili specijalistički kursevi, ali je neophodno razumevanje na osnovnom nivou tehnoloških koncepata i stepena uticaja na poslovne procese organizacije. Ovoj grupi najčešće pripadaju sledeće tehnologije i veštine:

1. Veštine programiranja i skriptovanja[10] (npr. *Python*, *PowerShell*, *Bash*) – automatizacija revizorskih procesa ubrzava rad i smanjuje mogućnost nenamerne ljudske greške.
2. Napredno znanje iz računarskih mreža, rutiranja, mrežnih protokola i pripadajućih tehnologija i procesa, u cilju razumevanja kompleksnih rizika koji mogu negativno uticati na poverljivost, integritet i dostupnost podataka i sistema.
3. Razumevanje *cloud* tehnologija („računarstva u oblaku“) i virtualizacije, i razlike u rizicima u odnosu na tradicionalne tehnologije data centara i održavanja IT sistema na fizičkoj lokaciji organizacije.
4. Razumevanje koncepata veštačke inteligencije, prvenstveno u podržavanju ključnih i kritičnih poslovnih procesa, kao i osnovno razumevanje korišćenja aktuelnih dostupnih servisa u ovoj oblasti.

Iako formalno ne pripada korpusu znanja iz informacionih tehnologija, poznavanje koncepata privatnosti sve više predstavlja obavezan deo revizorskog angažmana. Osim regulative iz ove oblasti (Zakon o zaštiti podataka o ličnosti i GDPR kao osnovni okviri), IT revizori upoznati sa tehnologijama koje implementiraju principe privatnosti u IT sistemima (npr. *Microsoft Purview Information Protection* [15]) mogu u značajnoj meri doprineti kvalitetu revizije i identifikovati rizike sa potencijalno visokim negativnim regulatornim i finansijskim uticajem na organizaciju.

[9] Često se koristi termin *Subject Matter Expert*, SME.

[10] Termin „skriptovanje“ odnosi se na pisanje programskog koda (skripte) koja automatizuje neke ponavljajuće zadatke u okviru aplikacije ili specifičnog softverskog okruženja. U praksi se skriptovanje često koristi za proširenje funkcionalnosti postojećeg softvera.

SERTIFIKATI ZA IT REVIZORE

Visok nivo opštih i stručnih znanja i veština, IT revizori mogu formalno dokazati sticanjem nekog od međunarodno priznatih sertifikata. Sertifikovan IT revizor, osim što potvrđuje posedovanje širokog spektra kompetencija na visokom nivou, dokazuje i da je posvećen daljem konstantnom usavršavanju, što u praksi utiče na vođenje kreativnijih i složenijih angažmana, dinamičniju radnu atmosferu ali i (značajnije) uvećanje ličnih primanja i bolje pozicioniranje na tržištu rada.

Najvažniji i međunarodno najpriznatiji sertifikat za (interne) IT revizore predstavlja sertifikovani revizor informacionih sistema – CISA[11] [16]. CISA je širom sveta priznat kao „zlatni standard“ za IT revizore. Sticanje CISA sertifikata dokazuje visoku stručnost kandidata (neophodnih znanja i veštine za IT revizije i procene IT sistema) i potvrđuje sposobnost primene pristupa zasnovanim na proceni i prioritizaciji rizika u revizorskim angažmanima. Poslednja verzija ispita za sticanje sertifikata unapređena je neophodnim znanjima koje se odnose na nove tehnologije poput veštačke inteligencije, računarstva u oblaku (*cloud*) i *block chain* tehnologija, osiguravajući da IT revizori budu u toku sa najnovijim tehnološkim trendovima i napretkom. Neophodni uslovi za sticanje CISA sertifikata predstavlja dokaz o pet ili više godina iskustva u reviziji, kontroli, osiguranju ili bezbednosti IS/IT sistema (precizno definisana izuzeća od iskustva su moguća za najviše tri godine) i uspešno položen ispit za sertifikovanog revizora informacionih sistema – CISA ispit. Ispit se sastoji od 150 pitanja koja pokrivaju 5 oblasti radne prakse, a sva pitanja testiraju znanje i sposobnosti kandidata u stvarnim radnim iskustvima koje u realnom radu koriste stručni profesionalci.

Prihvatajući realnost da značajan broj organizacija daje prednost kandidatima sa čvrstom osnovom znanja o informacionim tehnologijama i IT reviziji, ISACA je 2022. godine predstavila sertifikat o osnovama IT revizije – *IT Audit Fundamentals Certificate* [17]. Sertifikat je namenjen prvenstveno mladim profesionalcima i onima koji žele da usmere tok karijere na IT reviziju, pružajući uvid u principe IT revizije i priliku da kandidat izgradi i potvrdi temelje znanja i veština kako bi bili uspešni IT revizori. Iako u osnovi zahteva niži nivo znanja u odnosu na CISA sertifikat (demonstriranjem znanja na osnovnom nivou), najvažnija prednost sertifikata o osnovama IT revizije je da ne zahteva nikakvo prethodno iskustvo. Na ovaj način, poslodavcima je omogućena nezavisna potvrda da je kandidat posvećen budućoj karijeri, a kandidatima pružena šansa da postanu sertifikovani u oblasti IT revizije bez prethodnog revizorskog iskustva.

Brzi napredak tehnologije, uz konstantno unapređenje CISA ispita i usavršavanja sertifikovanih profesionalaca kroz godišnje programe kontinuiranih profesionalnih obuka (CPE) [18], omogućio je da se IT revizori dodatno usmere u revizije novih tehnologija, prvenstveno veštačke inteligencije. Novi program ISACA sertifikacije naziva napredna revizija veštačke inteligencije (*Advanced in AI Audit – AAIA* [19]) prevazilazi standardne revizorske akreditive i podrazumeva najsavremenije veštine za procenu rizika, identifikovanje mogućnosti i obezbeđivanje usklađenosti u tri ključna domena veštačke inteligencije: upravljanje rizicima veštačke inteligencije, operacije veštačke inteligencije i alati i tehnike revizije veštačke inteligencije.

[11] Akronim od *Certified Information Systems Auditor*.

Na kraju, svim zainteresovanim profesionalcima koji žele da steknu neophodna znanja iz oblasti IT revizije, ali bez ambicije za promenu karijere, preporučuje se razmatranje kursa „Osnove IT revizije“ [20] Instituta internih revizora. U dva dana / 16 sati, pripremljena su sva neophodna znanja koja će pomoći da se razumeju procesi, značaj i okvir delovanja IT revizije, ali i da se steknu osnovna, ali razumljiva znanja o IT tehnologijama.

BUDUĆNOST IT REVIZIJE

U objavljenom istraživanju [21] iz 2019, institut ISACA objavio je procene da će IT revizori biti sve više uključeni u velike tehnološke projekte, i to u više od 30% već u početnim fazama projekata. Takođe, kompanijama će biti potrebni IT revizori sa visokim stručnim znanjima (veštačka inteligencija, prediktivna analiza, automatizacija procesa uz korišćenje robota), ali se u isto vreme očekuje i da će nedostatak stručnih revizora omogućiti značajan broj otvorenih radnih mesta. IT i ostale revizije će postati u značajnijoj meri automatizovane, a revizorski timovi agilniji, sa mogućnošću brzog prilagođavanja promenama. Zaključak je da 92% ispitanih optimistično po pitanju budućnosti IT revizije, a 77% da će stručna znanja biti dostupna u adekvatnoj meri i obimu kako bi se postojeći IT revizori konstantno usavršavali.

IT revizija već dugi niz godina predstavlja potvrđenu i priznatu profesiju, sa definisanim pravilima, smernicama i višedecenijskom praksom koja garantuje obezbeđivanje dodatne vrednosti organizacijama svih nivoa i industrija. IT revizori su profesionalci koji žele da praktična IT znanja primene kako bi pomogli organizacijama da IT tehnologiju ispravno primene, koriste, održavaju i zamene naprednijim na kraju životnog ciklusa.

Osim što je u praksi prepoznata i često prisutna kontrola funkcija u organizacijama, IT revizija je podržana i kroz esnafska internacionalna udruženja internih revizora i internih IT revizora, koji broje više desetina hiljada aktivnih članova. U Srbiji, IT revizori su okupljeni kroz beogradski ogranak instituta ISACA (*ISACA Belgrade chapter*) [22].

REFERENCE

[1] „Audit,“ Wikipedia, [Na mreži]. Available: https://en.wikipedia.org/wiki/Audit. [Poslednji pristup 18 7 2025].

[2] „audit (noun),“ Merriam-Webster Dictionary, [Na mreži]. Available: https://www.merriam-webster.com/dictionary/audit. [Poslednji pristup 18 7 2025].

[3] „audit,“ Oxford English Dictionary, [Na mreži]. Available: https://www.oed.com/search/dictionary/?scope=Entries&q=audit. [Poslednji pristup 18 7 2025].

[4] „The Institute of Internal Auditors,“ [Na mreži]. Available: www.theiia.org. [Poslednji pristup 16 7 2025].

[5] „Globalni standardi interne revizije,“ Institut internih revizora, 2024. [Na mreži]. Available: https://uirs.rs/wp-content/uploads/2025/04/global-internal-audit-standards-serbian.pdf. [Poslednji pristup 7 7 2025].

[6] „IT Auditing,“ ISACA, [Na mreži]. Available: https://www.isaca.org/career-center/career-journey/it-auditing. [Poslednji pristup 4 8 2025].

[7] „IT audit (information technology audit),“ TechTarget, [Na mreži]. Available: https://www.techtarget.com/searchcio/definition/IT-audit-information-technology-audit. [Poslednji pristup 4 8 2025].

[8] „Global Internal Audit Standards,“ The Institute of Internal Auditors, [Na mreži]. Available: https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/. [Poslednji pristup 4 8 2025].

[9] „Globalni standardi interne revizije (prevod na srpski),“ The Institute of Internal Auditors, [Na mreži]. Available: https://www.theiia.org/globalassets/site/standards/editable-versions/global-internal-audit-standards-serbian.pdf. [Poslednji pristup 4 8 2025].

[10] „Global Technology Audit Guides (GTAGs),“ The Institute of Internal Auditors, [Na mreži]. Available: https://www.theiia.org/en/standards/2024-standards/global-guidance/#gtags. [Poslednji pristup 4 8 2025].

[11] „IT Audit Framework (ITAF), 4th Edition | Digital | English,“ ISACA, [Na mreži]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko91EAC. [Poslednji pristup 4 8 2025].

[12] „Resources - IT Audit,“ ISACA, [Na mreži]. Available: https://www.isaca.org/resources/it-audit. [Poslednji pristup 4 8 2025].

[13] S. Wurzburger, I. Zlatanović, A. Simonović, V. Popović, K. Lazić i V. Pantović, „Kontinuirana obuka internih revizora u oblasti informacionih tehnologija,“ u *XXIX Skup TRENDOVI RAZVOJA: “UNIVERZITET PRED NOVIM IZAZOVIMA”*, Vrnjačka Banja, 2023.

[14] S. Wurzburger, I. Zlatanović, A. Simonović, V. Popović, K. Lazić i V. Pantović, „Obuka internih revizora u oblasti upravljanja rizicima,“ u *XXX Skup TRENDOVI RAZVOJA: ‘NASTAVNICI I SARADNICI KAO CENTAR PROMENA U VISOKOM OBRAZOVANJU”*, Vrnjačka Banja, 2024.

[15] „Microsoft Purview Information Protection,“ Microsoft, [Na mreži]. Available: https://learn.microsoft.com/en-us/purview/information-protection. [Poslednji pristup 16 7 2025].

[16] „CISA,“ ISACA, [Na mreži]. Available: https://www.isaca.org/credentialing/cisa. [Poslednji pristup 4 8 2025].

[17] „IT Audit Fundamentals Certificate,“ ISACA, [Na mreži]. Available: https://www.isaca.org/credentialing/it-audit-fundamentals-certificate. [Poslednji pristup 4 8 2025].

[18] „CPE IT Continuing Professional Education,“ ISACA, [Na mreži]. Available: https://www.isaca.org/isaca-digital-videos/archive/isaca-cpe-it-continuing-professional-education. [Poslednji pristup 4 8 2025].

[19] „Advanced in AI Audit (AAIA),“ ISACA, [Na mreži]. Available: https://www.isaca.org/credentialing/aaia. [Poslednji pristup 4 8 2025].

[20] „Fundamentals of IT Auditing,“ ISACA, [Na mreži]. Available: https://www.theiia.org/en/products/learning-solutions/course/fundamentals-of-it-auditing/. [Poslednji pristup 4 8 2025].

[21] „THE FUTURE OF IT AUDIT,“ ISACA, 2019. [Na mreži]. Available: https://www.isaca.org/resources/infographics/the-future-of-it-audit. [Poslednji pristup 18 7 2025].

[22] „Belgrade Chapter,“ ISACA, [Na mreži]. Available: https://engage.isaca.org/belgradechapter/home. [Poslednji pristup 4 8 2025].

Kristijan Lazić, konsultant u oblasti IT revizije i upravljanja IT rizicima, Argo Informacione Tehnologije, Beograd
Kontakt: kristijan.lazic@gmail.com
Oblasti interesovanja: IT revizija i usklađenost, Upravljanje rizicima, Informaciona bezbednost, Nivoi zrelosti

Dragan Jovičić, Head of IT Audit, PHOENIX Pharma SE, Corporate Audit, Pfingstweidstraße 10–12, 68199 Mannheim, Germany
Kontakt: dragan.r.jovicic@gmail.com
Oblasti interesovanja: IT revizija, Interna revizija, OT revizija, Informaciona bezbednost, Veštačka inteligencija, Projektni menadžment

Vladan Pantović, vanredni profesor, Fakultet za projektni i inovacioni menadžment prof. dr Petar Jovanović, Beograd
Kontakt: vladan@pantovic.rs
Oblasti interesovanja: Informaciona bezbednost, Projektni menadžment, Veštačka inteligencija, IT revizija