UDK 657.6:007
DOI: 10.7251/FIN1703024S

PREGLEDNI RAD

Vladimir Stanimirović*
Mladen Gajić**

Revizija informacionih sistema

Information systems audit

Rezime

Revizija informacionih sistema predstavlja proces prikupljanja i nezavisne procjene revizorskih dokaza na osnovu kojih se vrši kontrola efikasnosti funkcionisanja informacionih sistema, te njegova primjena i kvalitet. Revizija obuhvata kontrolu pravne, informacione i ekonomske komponente informacionih sistema.

Cilj ove revizije je ispitivanje i ocjena dijelova integrisanog informacionog sistema u subjektu revizije, te postizanje razumnog uvjerenja da oni pri svom radu proizvode pravovremene, tačne, potpune i pouzdane informacije, uz obezbjeđenje povjerljivosti, integriteta, raspoloživosti i pouzdanosti informacija.

Na kraju, na osnovu prikupljenih i nezavisno procijenjenih revizorskih dokaza sačinjava se izvještaj revizije, kao osnovni proizvodi revizijskog procesa. Ovaj izvještaj predstavlja adekvatnu osnovu za promjene u načinu organizovanja i funkcionisanja informacionog sistema, promjene u načinu upravljanja (javnim) sredstvima, pružanje kvalitetnijih i korisnički orijentisanih usluga, podizanje (javne) odgovornosti zaposlenih na viši nivo, kao i promovisanje pravilnog upravljanja i javnosti rada zaposlenih u subjektu revizije.

Ključne riječi: *interna revizija, informacioni sistem, revizija IT sistema, informacioni rizik, bezbjednost IT sistema, računovodstveni informacioni sistem, informacione tehnologije u računovodstvu.*

Abstract

The information systems audit represents the process of collecting and independent evaluation of audit evidence on the basis of which the control of the efficiency of the functioning of information systems is carried out, as well as its application and quality. The audit includes the control of the legal, information and economic components of information systems.

The aim of this audit is to examine and evaluate the parts of the integrated information system in the subject of audit, and to achieve a reasonable belief that they produce prompt, accurate, complete and reliable information in their work, while ensuring the confidentiality, integrity, availability and reliability of information.

Finally, based on the collected and independently evaluated audit evidence, the audit report as the main product of the audit process is made. This report represents the adequate basis for changes in the way of organizing and functioning of the information system, the changes in the way of management of (public) funds, better quality and user-oriented services, raising (public) responsibility of employees to a higher level, and promoting proper management and transparent work of employees in the subject of the audit.

Keywords: *internal audit, information system, IT system audit, information risk, IT system security, accounting information system, information technology in accounting.*

UVOD

Revizorske aktivnosti u reviziji informacionog sistema (u daljem tekstu: IT sistem), posmatrane s aspekta interne i/ili eksterne revizije, usmjerene su prema internim kontrolama i internim kontrolnim postupcima subjekta revizije, a obuhvataju testiranje opštih kontrola, kontrola pojedinačnih aplikacija i programa i kontrolu korisnika koji su u interaktivnoj vezi sa IT sistemom.

Pravni osnov za realizaciju (interne) revizije IT sistema sadržan je u Zakonu o sistemu internih finansijskih kontrola u javnom sektoru Republike Srpske (Zakon o sistemu internih finansijskih kontrola u javnom sektoru, 91/16), prema kojem interne revizije mogu biti:

* Javna zdravstvena ustanova Bolnica „Sveti apostol Luka“ Doboj, e-mail: vladimir@stanimirovic.com
** Javna zdravstvena ustanova Bolnica „Sveti apostol Luka“ Doboj, e-mail: mladen.gajic@bolnicadoboj.com

1) revizija sistema,
2) revizija usklađenosti,
3) revizija učinka,
4) finansijska revizija,
5) revizija informacionih sistema.

Pored zakonskog (pravnog) osnova, ta revizija treba da bude planirana i u godišnjem planu revizije, kreiranog na osnovu strateškog plana i izvršene procjene rizika. Izuzetno, kada su pripreme strateških i godišnjih planova u toku i kada rukovodilac subjekta revizije zahtijeva vanrednu reviziju, revizija počinje nalogom. Na osnovu godišnjeg plana ili naloga rukovodioca subjekta pristupa se izradi pojedinačnog plana revizije, u kojem se identifikuju kontrolne aktivnosti, metode i tehnike koje su relevantne za reviziju IT sistema.

Da bismo ukazali šta predstavlja revizija IT sistema, u nastavku rada obrazloženi su pojmovi predmeta revizije, obima revizije, ciljeva revizije i drugi elementi adekvatni za reviziju, posmatrani s aspekta interne revizije u javnom sektoru Republike Srpske. Iako je u radu revizija IT sistema posmatrana s aspekta interne revizije u javnom sektoru Republike Srpske, a imajući u vidu prirodu revizije i specifičnost revizorskih postupaka, revizorske aktivnosti navedene u nastavku moguće je primijeniti i u eksternoj reviziji.

1. PREDMET, RIZIK I CILJEVI REVIZIJE

Informacioni sistem je sistem koji prikuplja, pohranjuje, obrađuje i isporučuje informacije važne za organizaciju i društvo, tako da budu dostupne i upotrebljive za svakog ko se želi njima koristiti, uključujući poslovodstvo, klijente, zaposlene i ostale (Aleksić-Marić i Stojanović, 2005). Posmatrano s aspekta sistemskog pristupa, IT sistem predstavlja uređen skup aktivnosti neophodnih za prikupljanje, čuvanje, obradu, prenošenje i distribuciju podataka u okviru subjekta revizije, uključujući opremu i zaposlene koji se bave tim aktivnostima. Stoga IT sistem ne treba posmatrati kao odvojen dio jer on djeluje unutar poslovnog sistema subjekta revizije, omogućavajući mu komunikaciju unutar organizacije, kao i komunikaciju sa poslovnim okruženjem. Budući da u poslovni sistem ulaze i izlaze materijalni i informacioni tokovi iz različitih izvora, zadatak IT sistema je njihovo preuzimanje, obrada i prezentacija zaposlenima, menadžmentu i stejkholderima. S obzirom na to da se preuzimanje informacija vrši iz različitih izvora, eksternih i internih, pored definisanog zadatka, treba istaći da je cilj IT sistema snabdijevanje poslovnog sistema potrebnim informacijama pri izvođenju poslovnog procesa i pri upravljanju poslovnim sistemom.

Stoga se potreba za izgradnjom i održavanjem efikasnog i efektivnog IT sistema (koji omogućava prikupljanje, prenos, memorisanje i distribuciju informacija) nameće kao imperativ, pogotovo ako se uzmu u obzir rizici od zloupotrebe IT sistema, koji karakterišu savremeno poslovanje. Generalno, rizik se može posmatrati kao potencijalna opasnost da preduzeta aktivnost dovede do neželjenih posljedica. U skladu s tim, informacioni rizik predstavlja opasnost da primjena informacione tehnologije dovede do neželjenih posljedica, tj. štete u poslovnom sistemu i njegovom okruženju (Aleksić-Marić, 2008). U zavisnosti od uzroka i vrste rizika manifestuju se različiti načini zloupotrebe informacione tehnologije, a to je detaljno prikazano u narednoj tabeli:

Tabela 1. *Uzroci i manifestacije rizika od zloupotrebe informacione tehnologije*

TIP UZROKA	UZROK	MANIFESTACIJA
Unutrašnji	Menadžment	Nedostupnost resursa, neodgovarajuće planiranje i kontrola
	Zaposleni	Greške, krađa, utaja, sabotaže, korupcija, neadekvatno korišćenje ovlašćenja
	Informacioni sistem	Kvarovi hardvera i pomoćne opreme, greške u softveru
Spoljni	Prirodne nepogode, viša sila	Potres, poplava, požar, eksplozija, ekstremna temperatura
	Isporučioci opreme	Nepouzdana ili nekompatibilna oprema, loše održavanje, reklamacije
	Isporučioci softvera	Nekorektan softver, loše održavanje, neblagovremeno pružanje usluga, odavanje poslovne tajne
	Dobavljači usluga	Nestanak napajanja, prekid komunikacionih veza, neblagovremeno pružanje usluga
	Konkurencija	Sabotaže, špijunaža, sudske tužbe, finansijske špekulacije
	Kreditori i investitori	Nelikvidnost, insolventnost
	Sindikati	Štrajkovi, sabotaže, opstrukcije
	Državna uprava	Nepovoljne promjene u fiskalnoj i monetarnoj politici
	Borci za zaštitu okoline	Protesti, opstrukcije, neželjeni i negativni publicitet
	Teroristi, kriminalci i hakeri	Uništenje, oštećenje i krađa imovine, pljačka, kompjuterski virusi, sabotaže i špijunaža

Izvor: Aleksić-Marić, V. (2008). Elektronsko poslovanje. Banja Luka: Ekonomski fakultet, str. 226.

Iz prethodnog tabelarnog pregleda uočavaju se razlike između internih i eksternih uzroka rizika, koji imaju različite posljedice po poslovni sistem. U cilju upravljanja potencijalnim rizicima, rukovodstvo subjekta revizije treba da kreira metodologiju upravljanja informacionim rizicima, koja treba da se zasniva na: identifikaciji rizika, ispitivanju vjerovatnoće i kvantifikaciji rizika, utvrđivanju prioriteta rizika, identifikaciji protivmjera, utvrđivanju odnosa troškova i koristi od primjene protivmjera, izboru najprihvatljivijih protivmjera, implementaciji protivmjera, definisanju mjera otklanjanja potencijalnih šteta, kontroli, reviziji i modifikaciji postupka (Aleksić-Marić, 2008). Iz ovoga proizlazi da upravljanje rizikom nije jednosmjeran proces, već naprotiv, proces koji se zasniva na informacijama unaprijed (feedforward) i unazad (feedback), čineći na taj način cjelinu koja ima pravce svog razvoja, ali i učenja iz sopstvenih postupaka.

S obzirom na to da se tema rada, kao i sam revizorski proces, zasniva na informacijama unazad (feedback), u nastavku su navedene i obrazložene aktivnosti koje se odnose na kontrolu IT sistema, a koje u suštini čine predmet revizije. Ciljevi kontrole informacione i slične tehnologije suštinski se ne razlikuju od kontrola u drugim procesima ili postupcima. Naime, funkcija kontrole je usmjerena na kontrolu procesa gdje je težište na odstupanjima od pravila i odgovornosti za nepoštovanje određenih pravila ili zadanih veličina (Malešević i Vranković, 2007). Ako se na prethodni način posmatra kontrola, onda kontrole IT sistema obuhvataju opšte kontrole, kontrole aplikacija i programa i kontrole zaposlenih koji su u interaktivnom odnosu sa ovim sistemom. Opšte kontrole i kontrole aplikacija su uvijek kontrole IT sistema. Za razliku od navedenih kontrola, kontrola korisnika predstavlja kontrolu IT sistema ukoliko njihova efikasnost zavisi od obrade ili pouzdanosti, tačnosti, potpunosti, valjanosti i usaglašenosti informacija koje je ovaj sistem obradio.

Da bi se izvršila provjera postojanja i funkcionisanja opštih i aplikativnih kontrola i kvaliteta IT sistema, a u skladu s navedenom metodologijom upravljanja rizicima, rukovodstvo subjekta revizije treba da uspostavi kontinuirane kontrolne aktivnosti: kontrolu upravljanja zaštitom IT sistema, kontrolu logičkog i fizičkog pristupa programima i aplikacijama, kontrolu upravljanja konfiguracijama i izmjenama programa i kontrolu podjele dužnosti i odgovornosti korisnika. Pravilno definisanim (programiranim) kontrolnim postupcima u okviru aplikacija, baza podataka i operativnih sistema moguće je ostvariti efektivno razdvajanje dužnosti i odgovornosti zaposlenih u svakodnevnim poslovnim aktivnostima. U ovom slučaju, kontrolne aktivnosti predstavljaju kombinaciju manuelnih i automatskih (programskih) kontrolnih postupaka, s tim da vrsta kontrolnih postupaka zavisi od prirode, složenosti i kvaliteta IT sistema.

Iz prethodnog se može zaključiti da se kvalitet IT sistema, posmatran s aspekta interne revizije, osigurava internom kontrolom i internim kontrolnim postupcima, a stepen kvaliteta utvrđuje se internom revizijom. S druge strane, za konačnu ocjenu dotičnog sistema treba da se angažuje nezavisna kontrola, koju sprovode eksterna revizorskog društva. Bez obzira na to da li se predmetna revizija posmatra iz ugla internog ili eksternog revizora, u cilju sprovođenja adekvatnih revizorskih postupaka, potrebno je izvršiti kontrolu pravne, informacione i ekonomske komponente ukupnog (ili dijela) IT sistema subjekta revizije. Ovako utvrđena revizija IT sistema, u slučaju utvrđenih nepravilnosti i slabosti internih kontrolnih postupaka, treba imati preporuke rukovodstvu subjekta revizije koje za cilj imaju poboljšanje kvaliteta IT sistema.

Ukoliko znamo da treba izvršiti prethodno navedene kontrole (pravnu, informacionu i ekonomsku), utvrdili smo i okvir za definisanje glavnog cilja i potciljeva revizije. Glavni cilj revizije IT sistema treba da se odnosi na ispitivanje i ocjenu komponenti sistema radi uvjeravanja da taj sistem proizvodi pravovremene, tačne, potpune i pouzdane informacije neophodne za poslovno odlučivanje. U svrhu realizacije glavnog cilja revizije, prilikom izvođenja revizorskih postupaka revizor treba tražiti odgovor na glavno revizorsko pitanje: Da li IT sistem subjekta revizije funkcioniše na odgovarajući način, uz održavanje integriteta podataka neophodnih za poslovno odlučivanje?

Nakon utvrđivanja glavnog cilja i revizorskog pitanja, mogu se definisati njegovi potciljevi. Glavni revizorski cilj se može razraditi kroz sljedeće potciljeve:

- ocjena povjerljivosti, integriteta, raspoloživosti i pouzdanosti informacija i ocjena usklađenosti IT sistema s relevantnim zakonskim i regulatornim zahtjevima;
- upoznavanje sa sveobuhvatnim uticajem informacionih tehnologija na značajne poslovne procese subjekta revizije, uključujući pripremu finansijskih izvještaja i druge aktivnosti u vezi sa osnovnom djelatnošću;
- upoznavanje s okolnostima koje utiču na: korišćenje informacionih tehnologija u obradi, čuvanju i dostavljanju finansijskih i nefinansijskih informacija; sisteme internih kontrola, kao i razmatranje inherentnog i kontrolnog rizika;
- upoznavanje sa internim postupcima koje rukovodstvo subjekta revizije primjenjuje u ocjeni, upravljanju i kontrolisanju IT sistema;
- donošenje zaključaka o efikasnosti kontrola IT sistema koje imaju neposredan uticaj na obradu i prezentaciju finansijskih i nefinansijskih informacija;
- uvjeravanje da se svi aspekti IT sistema, uključujući interne kontrole, primenjuju na efikasan i efektivan način.

U svrhu dobijanja razumnog uvjerenja za prethodno utvrđene potciljeve, revizor treba tražiti odgovore i na sljedeća pitanja:

Tabela 2. *Primjeri revizorskih pitanja*

Revizorsko pitanje 1	Na koji način informacije, kao proizvodi ukupnog IT sistema, utiču na poslovanje subjekta revizije?
Revizorsko pitanje 2	U kojoj mjeri IT sistem odgovara potrebama subjekta revizije?
Revizorsko pitanje 3	Kako IT sistem utiče na očuvanje imovine subjekta revizije i zaštitu prava kupaca (klijenata) subjekta revizije?
Revizorsko pitanje 4	Da li IT sistem i informacione tehnologije utiču na efikasnost rada zaposlenih u subjektu revizije?
Revizorsko pitanje 5	Na koji način interno generisane informacije utiču na poslovanje subjekta revizije i prezentaciju subjekta revizije u poslovnom okruženju?

Izvor: Prikaz revizorskih pitanja koje su definisali autori

Prethodno navedena revizorska pitanja kreirana su na osnovu subjektivnih procjena rizika, a suštinski zavise od procjene i analize rizika. Pored definisanja revizorskih ciljeva, pitanja, rizika i manifestacija rizika navedenih u tabeli 1, sa stanovišta revizije IT sistema, revizori treba da izvrše analizu ukupnog rizika revizije. Ukupan rizik revizije IT sistema je proizvod:

1) inherentnog rizika, koji se odnosi na informacione resurse ili resurse koji se koriste u kontroli IT sistema i informacionih tehnologija (krađa opreme, destrukcija, objavljivanje povjerljivih informacija, neautorizovana modifikacija ili drugi način ugrožavanja IT sistema);
2) kontrolnog rizika, koji predstavlja rizik od materijalnih grešaka u podacima koji neće biti pravovremeno detektovani i korigovani provođenjem internih kontrolnih postupaka;
3) rizika detekcije, koji predstavlja mogućnost da interni revizor tokom revizije IT sistema neće uočiti materijalno značajnu grešku ili nepravilnost.

Iz ovoga proizlazi da specifičnost rizika predstavljaju potencijalne opasnosti da IT sistem netačno obrađuje i prezentuje informacije, dozvoljava neovlašćeni pristup informacijama, daje zaposlenima privilegovan pristup, omogućava neovlašćene promjene informacija i slično.

2. REGULATORNI I METODOLOŠKI OKVIR IT REVIZIJE

Interna revizija u Republici Srpskoj vrši se na osnovu Zakona o sistemu internih finansijskih kontrola u javnom sektoru Republike Srpske, koji je usaglašen s Međunarodnim standardima za profesionalnu praksu interne revizije, utvrđenim od Instituta međunarodnih revizora (IIA – The Institute of Internal Auditors). Pored Zakona i Međunarodnih standarda, ova oblast uređena je i podzakonskim propisima, koji zajedno sa Zakonom čine procesne propise na osnovu kojih se vrši revizija. Ovdje izdvajamo:

1) Uputstvo za interne revizore javnog sektora – akt kojim se uređuju procedure čija je primjena obavezna tokom rada interne revizije, a propisane su u svrhu ostvarivanja plana rada interne revizije;
2) (Okvirna) povelja interne revizije – interni akt kojim se uređuju cilj, ovlašćenja i odgovornosti interne revizije i rukovodioca subjekata u odnosu na internu reviziju;
3) Kodeks profesionalne etike za internu reviziju kojim se uređuju principi profesije i prakse interne revizije (integritet, nezavisnost, objektivnost, povjerljivosti i stručnost), te pravila ponašanja internih revizora u obavljanju svojih funkcija, a koji se primjenjuje i na pojedince i na subjekt kod koga se vrši interna revizija.

Međunarodnim standardima, zakonskim i podzakonskim propisima, propisano je da se revizija IT sistema, kao vrsta interne revizije, vrši na osnovu:

1) strateškog plana,
2) godišnjeg plana i
3) plana pojedinačne revizije.

Iz ovoga se može zaključiti da aktivnost interne revizije u Republici Srpskoj ne predstavlja jednokratan posao, već aktivnost kojoj se treba pristupiti na strateškoj osnovi, strateškim planiranjem i procjenom rizika, a koje za posljedicu ima adekvatne godišnje i operativne (pojedinačne) planove. Rezultat navedenih (planskih) aktivnosti su konkretni revizorski postupci na koje, pored planiranja, utiče i izabrana (definisana) metodologija u svakoj vrsti revizije. Za pravilno definisanje metodologije neophodno je poznavati opšte principe, kao i specifičnost svakog predmeta revizije. Međutim, ako se uopšteno posmatra svaka revizija, pa i revizija IT sistema, mogu se kao zasebne cjeline posmatrati tri faze revizije: faza planiranja, faza testiranja i faza izvještavanja.

U fazi planiranja revizor treba da se upozna sa IT sistemom subjekta revizije i njegovim komponentama, elektronskim poslovanjem, kontrolama i inherentnim rizicima. Tokom upoznavanja sa IT sistemom neophodno je prikupiti informacije opšteg karaktera, kao što su: vrsta programa i aplikacija koji su u primjeni, način primjene, broj programa u primjeni, broj programa koji nisu u primjeni, broj, vrsta i vrijednost ugovora za nabavku, razvoj i održavanje programa i aplikacija i druge informacije relevantne za reviziju.

Nakon završetka faze planiranja, vrši se faza testiranja. U ovom dijelu revizije potrebno je izvršiti testiranje, poznato pod nazivom 3E, tj. potrebno je testirati ekonomičnost, efikasnost i efektivnost IT sistema i kontrola koje su relevantne za ciljeve revizije. Na osnovu testiranja revizor prikuplja dovoljne i adekvatne revizorske dokaze o internim kontrolnim politikama, procedurama i kontrolnim aktivnostima rukovodstva i zaposlenih u subjektu revizije.

Na kraju, kao posljednja, vrši se faza izvještavanja. U ovom dijelu revizor prezentuje rukovodstvu subjekta revizije značajne nalaze, zaključke i preporuke. Uz pretpostavku da su, na osnovu izvršenih revizorskih postupaka, utvrđene slabosti i nepravilnosti u funkcionisanju internih kontrolnih postupaka, revizor treba da navede značajne zaključke o uticaju utvrđenih slabosti u kontroli IT sistema, te informiše rukovodstvo subjekta revizije o rezultatima revizije, uključujući navođenje materijalno značajnih slabosti i drugih značajnih nedostataka.

Prethodno navedene faze revizije ne treba posmatrati kao odvojene dijelove jer one sinergetski djeluju jedna na drugu, čineći kompaktnu cjelinu postupka revizije. Iako je postupak revizije IT sistema moguće izvršiti na više načina, predložena metodologija je u skladu sa Zakonom i podzakonskim aktima kojima se uređuje ova oblast. Metodologija se zasniva na analizi i procjeni rizika – od analize na višem hijerarhijskom nivou ka analizi na nižem nivou organizovanja. Značaj izbora metodologije proizlazi i iz toga što ona ima značajnu ulogu prilikom prikupljanja revizorskih dokaza. Naime, u zavisnosti od izabrane metodologije, mogu se odabrati neki od načina prikupljanja dokaza:

- proučavanje zakonskih i podzakonskih propisa;
- proučavanje planova, programa rada i izvještaja o poslovanju;
- posmatranje organizacije i načina funkcionisanja;
- pregledi dokumentacije o nabavci, razvoju i održavanju IT sistema;
- pregledi finansijskih i analitičkih kartica;
- razgovori s angažovanima na IT poslovima (unutar i izvan subjekta revizije);
- razgovori sa zaposlenima koji koriste IT sistem.

Revizorske dokaze, prikupljene na navedene načine i drugi materijal prikupljen tokom izvođenja revizije potrebno je dokumentovati i čuvati. Za razliku od prikupljenih dokaza u drugim revizijama, dokazi prikupljeni u reviziji IT sistema, koji se odnose na kontrolu informacione komponente IT sistema, imaju nematerijalnu ili neopipljivu osobinu, te se postavlja pitanje kako takve dokaze dokumentovati. Pored navedenog, problem u dokumentovanju ogleda se i u činjenici da programeri sa „udaljenih lokacija“ mogu vršiti izmjene u programima i tako uticati na adekvatnost revizorskih dokaza, te se s razlogom postavljaju pitanja kako dokumentovati tehničke probleme u radu računovodstvenog programa, kako dokumentovati spor i nefunkcionalan rad aplikacije i kako evidentirati smetnje i nepravilnosti u radu baze podataka.

Iako problemi postoje, dokumentovanje je moguće izvršiti pomoću određenih fotografskih i video-funkcija računara i drugih uređaja. Tako, recimo, primjenom funkcije Print Screen, zajedno sa prikazanim podatkom o datumu i vremenu, obezbijediće se dokaz da je u određenom vremenu evidentirana nepravilnost u IT sistemu. Navedena funkcija može se primijeniti i za dokumentovanje dokaza čiji su izvori programi i aplikacije koje nemaju opciju štampanja. U slučaju potrebe za dokumentovanjem dokaza koji traju određeni period (spor rad i drugi tehnički problemi) može se koristi videofunkcija Screen recorder kojom se u kontinuitetu može evidentirati nepravilnost u radu IT sistema.

Na kraju, da bi se pravilno definisala metodologija revizije IT sistema, a uzimajući u obzir specifičnost ovog procesa, revizor treba da predvidi kontrolu primjene zakona, podzakonskih akata, kao i međunarodnih standarda koji nisu u uskoj vezi s procesom revizije, već upravo s predmetom. Da bi se sveobuhvatno izvršila

revizija IT sistema, neophodno je uzeti u obzir i materijalne propise kojima je uređena oblast nabavke, razvoja, primjene IT sistema, od kojih izdvajamo:

- Zakon o računovodstvu i reviziji Republike Srpske („Službeni glasnik Republike Srpske“ broj 94/15);
- Međunarodni računovodstveni standard 38 – Nematerijalna imovina;
- Međunarodni računovodstveni standard 36 – Umanjenje vrijednosti imovine;
- Pravilnik o kontnom okviru i sadržini računa u kontnom okviru za privredna društva, zadruge, druga pravna lica i preduzetnike („Službeni glasnik Republike Srpske“ broj 106/15);

Pored navedenih zakonskih, podzakonskih propisa i međunarodnih računovodstvenih standarda, revizori treba da prouče i interne akte subjekta revizije (pravilnike, procedure i odluke) kojima se reguliše oblast IT sistema. Pri tome ne treba zanemariti ni interne akte kojima je definisana oblast računovodstava i računovodstvenih politika (pravilnik o računovodstvu i računovodstvenim politikama), ili internih kontrola i kontrolnih postupaka (pravilnik o internim kontrolama i internim kontrolnim postupcima), ali i niz drugih materijalnih propisa u kojima je neposredno ili posredno regulisana predmetna oblast revizije.

3. NALAZI, ZAKLJUČCI I PREPORUKE REVIZIJE – SMJERNICE ZA PRAVILNO SPROVOĐENJE REVIZIJE

U skladu s revizorskim pitanjima i ciljevima revizije IT sistema, te definisanom metodologijom, nalaze revizije moguće je prikupiti, organizovati i prezentovati u nekoliko odvojenih, ali međusobno zavisnih cjelina:

1) kontrola planiranja i organizovanja IT sistema;
2) kontrola pravnog osnova za nabavku, izradu i održavanje IT sistema;
3) kontrola internih akata koji definišu funkcionisanje IT sistema;
4) kontrola bezbjednosti IT sistema;
5) kontrola računovodstvenog IT sistema i primjene informacionih tehnologija u računovodstvu;
6) računovodstveno evidentiranje IT sistema.

Sumirajući navedene cjeline, dolazi se do zaključka da se revizorskim postupcima vrši kontrola pravne, informacione i ekonomske komponente IT sistema. Međutim, za potrebe rada i obrazloženja revizorskih postupaka treba razmotriti svaku od pomenutih cjelina pojedinačno, uzimajući u obzir da se one prožimaju i dopunjavaju čineći cjelinu revizorskog izvještaja.

3.1. Kontrola planiranja i organizovanja IT sistema

Prve revizorske aktivnosti u fazi ispitivanja i testiranja treba da budu usmjerene na planiranje i način organizovanja integrisanog IT sistema. Prilikom kontrole planiranja i organizovanja IT sistema revizor treba da utvrdi da li je rukovodstvo subjekta revizije:

- definisalo IT strategiju, rizike, ciljeve i tehnološki pravac razvoja i upravljanja IT investicijama;
- kreiralo i usvojilo strateški IT plan;
- kreiralo i usvojilo godišnji IT plan;
- uskladilo plan nabavke, razvoja, izmjene i implementacije IT sistema sa stvarnim potrebama subjekta revizije;
- normativno definisalo kontrolu kvaliteta IT sistema;
- definisalo način upravljanja ljudskim resursima i korisnicima informacionih tehnologija;
- definisalo način upravljanja IT projektima i slično.

Ukoliko subjekt revizije, u okviru planiranja i organizovanja poslovanja, nije definisao ranije navedene strateške i godišnje planove, kao i operativne aktivnosti, revizor treba da, u vidu preporuka, ukaže rukovodstvu subjekta revizije da je neophodno kreirati interne (planske) dokumente kojima će ova oblast biti definisana, na način da se uspostave IT strategija, planovi i ciljevi, upravljanje IT rizicima, kontrola kvaliteta IT sistema i usklađenost s poslovnim potrebama, te strateški IT plan, tehnološki pravac razvoja, upravljanje IT investicijama i ljudskim resursima. U suprotnom, ukoliko ne postoje jasni pravci razvoja, može doći do kreiranja ili nabavke nepotrebnih IT sistema, koji ne odgovaraju stvarnim potrebama poslovnog sistema, čime dolazi do neopravdanog trošenja sredstava.

3.2. Kontrola pravnog osnova za nabavku, izradu i održavanje IT sistema

Prije kontrole ugovora, tehničkih sporazuma i drugih akata na osnovu kojih su izvršeni nabavka, razvoj i održavanje, potrebno je jasno utvrditi koliko je programa, aplikacija i drugih vidova IT sistema (interne i eksterne baze podataka) u funkciji u revidiranom periodu. Imajući u vidu specifičnost predmeta revizije, revizor treba u ovom koraku, ali i u svim drugim aktivnostima kada procijeni da je potrebno, koristiti usluge zaposlenih na IT poslovima (u funkciji eksperta) i drugih odgovornih za funkcionisanje IT sistema u subjektu revizije.

Nakon utvrđivanja broja i funkcije programa, aplikacija i drugih vidova IT sistema koji su u primjeni, može se pristupiti kontroli njihove pravne osnove. Prilikom kontrole pravnog osnova za nabavku, izradu i održavanje IT sistema (kontrola ugovora, tehničkih sporazuma, odluka), revizor treba da utvrdi:

- namjenu svakog pojedinačnog programa;
- neposredne i posredne korisnike programa i aplikacija (kako interne, tako i eksterne);
- usklađenost ugovora i tehničkih sporazuma sa stvarnim potrebama subjekta revizije;
- vrijednost pojedinačnih ugovora i tehničkih sporazuma;
- vrijednost ugovora iz prethodnog perioda;
- vrijednost nabavke drugih programa koji se koriste u okruženju (za potrebe komparativne analize i kontrole);
- usklađenost ugovora i tehničkih sporazuma sa zakonskim i podzakonskim aktima;
- da li su svi ugovoreni poslovi (nabavka i razvoj IT sistema) realizovani i plaćeni;
- da li subjekat revizije ima potpisane ugovore, tehničke sporazume ili druge akte za sve programe i aplikacije, posebno za programe i aplikacije čije informacije koriste eksterni korisnici i slično.

Prilikom kontrolisanja pravnog osnova za nabavku, izradu i održavanje IT sistema potrebno je imati u vidu regulatorni okvir kojim je definisano poslovanje subjekta revizije. Tako, recimo, prilikom revidiranja programa i aplikacija koje se koriste za obradu medicinske dokumentacije u zdravstvenim ustanovama, revizori treba da ispitaju da li je rukovodstvo subjekta revizije preduzelo mjere za zaštitu prava pacijenata, a posebno prava na tajnost podataka o zdravstvenom stanju pacijenta (Pravilnik o zaštiti prava osiguranih lica, br. 26/11, 21/14).

Budući da je za nabavku, razvoj i održavanje IT sistema neophodna konsultacija sa zaposlenima na IT poslovima, revizor treba da utvrdi da li je pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mjesta ili drugim internim aktom definisana njihova uloga i zadatak u tim poslovima. Ukoliko je definisana, potrebno ih je intervjuisati, a nakon toga utvrditi da li uistinu obavljaju definisane zadatke.

3.3. Kontrola internih akata koji definišu funkcionisanje IT sistema

U okviru revizije potrebno je izvršiti ispitivanje postojanja internih akata u kojima su definisane politike, procedure i prakse koje se odnose na uspostavljanje, funkcionisanje i održavanje IT sistema.

Na prvom mjestu potrebno je izvršiti uvid u pravilnik o računovodstvu i računovodstvenim politikama subjekta revizije, kojim se treba urediti organizacija računovodstvenog sistema, interni računovodstveni kontrolni postupci i računovodstvene politike. Naime, računovodstveni IT sistem predstavlja sastavni dio ukupnog IT sistema poslovnog subjekta, te je neophodno konstatovati da li je pravilnikom o računovodstvu i računovodstvenim politikama to i definisano, jer računovodstveni informacioni sistem treba da obezbijedi podatke i informacije o finansijskom položaju, uspješnosti poslovanja i promjenama u finansijskom položaju subjekta revizije, kako za interne, tako i za eksterne korisnike. Neophodno je utvrditi i da li je ovim pravilnikom definisano koje su to mjere koje se primjenjuju pri radu računovodstvenog IT sistema, a koje imaju za cilj obezbjeđenje funkcionisanja internih računovodstvenih kontrola, tj. mjera koje se odnose na kontrole pouzdanosti i vjerodostojnosti računovodstvenih podataka i informacija, kao i mjera interne revizije. Pored navedenih, ovim pravilnikom trebalo bi definisati i mjere kojima se onemogućava brisanje proknjiženih poslovnih promjena, a to je i definisano Zakonom o računovodstvu i reviziji Republike Srpske (Zakon o računovodstvu i reviziji, 94/15).

Drugo, potrebno je izvršiti provjeru pravilnika o internim kontrolama i internim kontrolnim postupcima (ukoliko postoji), kojim se uređuje sistem interne kontrole rada i poslovanja u domenu upravljačkih, administrativnih, računovodstvenih postupaka, postupaka informisanja radi obezbjeđivanja zakonitosti u radu i slično. Prilikom kontrole potrebno je utvrditi da li su u pravilniku navedene interne računovodstvene kontrole koje se odnose i na kontrole pouzdanosti i vjerodostojnosti računovodstvenih podataka i informacija, tj. potrebno je utvrditi da li su uspostavljene preventivne kontrole (da li se, recimo, vrši pristup programima pomoću korisničkog imena i šifre) i korektivne kontrole (kontrola načina rada i izvještavanja) IT sistema. U slučaju da se pristup programima vrši pomoću korisničkog imena i šifre, uspostavljen je preventivni kontrolni mehanizam (provjera identiteta korisnika) i zaštita od neovlašćenog pristupa i neovlašćene obrade podataka. Za razliku od preventivnih, korektivnim kontrolnim postupcima, poput kontrole usklađenosti dvaju različitih izvještaja o istim pokazateljima, moguće je utvrditi eventualna odstupanja i nepravilnosti u radu sistema, te preduzeti mjere da bi se uočene nepravilnosti korigovale.

Treće, potrebno je utvrditi da li su internim aktom definisane opšte i aplikativne kontrole. Internim aktom treba da budu definisane opšte kontrole integrisanog IT sistema, kao što su kontrole upravljanja bezbjednošću, pristupa, upravljanja konfiguracijom, razdvajanja dužnosti i planiranja za nepredviđene događaje.

Pored opštih kontrola, ukoliko subjekt revizije u svojoj organizaciji ima više različitih IT sistema (različiti programi za kadar, računovodstvo, upravljanje dokumentacijom, digitalno arhiviranje i sl.), internim aktom treba da budu definisane kontrole na nivou pojedinačnih aplikacija (posebna kontrola za svaku aplikaciju ili program), kao što su:

- Opšte kontrole na nivou pojedinačnih aplikacija. Za primjer se može navesti oblast zdravstva, u kojoj su jasno definisana prava i obaveze ljekara i medicinskih sestara prilikom pružanja zdravstvenih usluga. U pojedinim zdravstvenim institucijama kreirani su programi za upravljanje medicinskom dokumentacijom, koji zaposlenima omogućavaju brži i efikasniji rad. U ovom slučaju, rukovodstvo subjekta odgovorno je za jasno definisanje ovlašćenja i pristupa programu, kako ljekara, tako i medicinskih sestara/tehničara. Razdvajanje pristupa i ovlašćenja vrši se pomoću korisničkog imena i šifre. Tako, recimo, program treba da obezbijedi medicinskim sestrama/tehničarima mogućnost unosa i obrade ličnih podataka o pacijentima, dok ljekari imaju mogućnost unosa podataka o anamnezi, dijagnozi i slično;
- Kontrole povezanosti sa poslovnim procesom. Ovdje treba da se utvrdi da li su definisane kontrole provjere pojedinih dijelova (modula) računovodstvenog IT sistema, poput modula koji se odnosi na evidentiranje zaliha i usklađenosti modula sa stvarnim potrebama.

Pored navedenih opštih i aplikativnih kontrola neophodno je utvrditi da li su u internim aktima definisane i druge kontrole, koje su specifične za svaki program ili aplikaciju koju koristi subjekt revizije.

Četvrto, potrebno je utvrditi ko obavlja IT poslove u subjektu revizije, te da li broj zaposlenih odgovara stvarnim potrebama subjekta revizije. Ukoliko subjekt revizije nema organizovane i sistematizovane IT poslove, potrebno je utvrditi ko, kako i na koji način obavlja informatičke poslove u subjektu revizije. Naime, značaj ovog utvrđivanja proizlazi iz toga što se u poslovnom sistemu moraju znati prava i odgovornosti zaposlenih i rukovodstava u vezi s nabavkom, razvojem i održavanjem IT sistema.

Peto, potrebno je utvrditi da li subjekt revizije ima interne akte kojima je definisano planiranje i organizovanje, pribavljanje i implementacija, isporuka, podrška i nadzor IT sistema. Uspostavljanje ovog internog akta je od velike važnosti za poslovni sistem, jer ako rukovodstvo subjekta nema jasan plan i način njegove realizacije, može doći do nabavke neodgovarajućih IT sistema, tehničkog prijema neadekvatnog IT sistema, plaćanja troškova održavanja koji su iznad tržišne vrijednosti i tome slično.

Šesto, potrebno je utvrditi da li subjekt revizije ima interne akte u kojima su definisani:

- Change Management proces – proces vršenja programskih izmjena, od postupka slanja zahtjeva za izmjenu dijela ili ukupnog programa, do realizacije izmjene dijela ili ukupnog programa;
- User Administration process – proces otvaranja korisničkih naloga, izmjena i njihovo brisanje.

Prethodna dva procesa neophodno je uspostaviti iz dva razloga. Prvi se odnosi na upravljanje troškovima, kada se radi o izmjenama na programu, dok je značaj drugog u tome što utiče na upravljanje sigurnošću sistema.

Sedmo, potrebno je utvrditi da li subjekt revizije ima registar (evidenciju) programa i aplikacija koje se koriste za kreiranje, obradu i izvoz podataka, a u kojem treba da budu navedeni svi programi i aplikacije, vlasništvo, vrijednosti (nabavna, sadašnja i tržišna), način i vrijednost održavanja, podaci o ugovoru (osnovni elementi ugovora), garancije i drugi elementi bitni za primjenu informacionih tehnologija u subjektu revizije.

Prethodno navedeni interni akti i registar (evidencija) programa i aplikacija neophodni su za poslovno odlučivanje rukovodstva subjekta revizije koje se odnosi na nabavku, razvoj i održavanje IT sistema. lako se u ovom dijelu rada navodi više internih akata, koji treba da budu uspostavljeni kod subjekta revizije, moguće je uspostavljanje jednog kojim bi se obuhvatila cjelokupna problematika. Pored pomenutih zahtjeva za definisanje internih kontrolnih postupaka, internim aktima treba jasno klasifikovati šta predstavlja razvoj, a šta održavanje IT sistema. Jasna klasifikacija jedna je od pretpostavki za pravilno knjiženje u skladu sa Međunarodnim računovodstvenim standardom 38 – Nematerijalna imovina.

3.4. Kontrola bezbjednosti IT sistema

Generalno posmatrano, bezbjednost IT sistema najčešće je ugrožena od neovlašćenih korisnika čija je namjera činjenje određene zloupotrebe (Aleksić-Marić, 2008). Prilikom kontrole bezbjednosti IT sistema, s ciljem prikupljanja revizorskih dokaza, revizorskim postupcima potrebno je utvrditi da li:

- korisnici programa i aplikacija imaju pojedinačne (odvojene) pristupne podatke (username) i generisani (password);
- u skladu sa opisom posla, te utvrđenim odgovornostima, zaposleni imaju različite pristupe programskim nivoima (šef računovodstva, recimo, treba da ima pristup svim podacima, dok blagajnik treba da ima pristup samo dijelu programa koji se odnosi na rad blagajne);
- postoji mogućnost brisanja unesenih podataka;
- za svaki unos i izmjenu podataka postoje podaci o licu koje je izvršilo unos ili izmjenu;
- postoje tehnički problemi u radu programa i aplikacija.

Naime, ukoliko korisnici programa i aplikacija imaju različite pristupne podatke, ukoliko je obezbijeđena transparentnost i funkcionalnost IT sistema, revizor može zaključiti da je rukovodstvo subjekta preduzelo sve neophodne aktivnosti na očuvanju bezbjednosti IT sistema, a samim tim i pouzdanost informacija neophodnih za svakodnevno poslovno odlučivanje.

Kada se vrši kontrola bezbjednosti IT sistema, ne treba zanemariti činjenicu da je najznačajniji napredak u primjeni savremenih informacionih tehnologija identifikovan kao pronalazak interneta i World Wide Web-a. Primjenom internet tehnologija u svakodnevnim poslovnim aktivnostima zahtijeva se pristup podacima dvadeset četiri sata dnevno. S druge strane, paralelno s novom tendencijom povećava se rizik od nezakonitih radnji i rizik od sistemskog oštećenja i pogrešne prezentacije subjekta revizije u javnosti. Jedna od posljedica svakodnevne primjene interneta je razvoj društvenih (socijalnih) mreža. Društvena mreža je vrsta internet servisa, koji se najčešće javlja u obliku platforme ili internet stranice i služi za međusobno povezivanje korisnika. Danas postoje stotine ovakvih servisa, a među najpoznatijima su: Facebook, Instagram i Twitter. Pored navedenih društvenih mreža YouTube je popularni internet servis za razmjenu video-sadržaja u kojem korisnici mogu postavljati, pregledati i ocjenjivati video-sadržaje.

Stoga prilikom kontrolisanja bezbjednosti informacija kao proizvoda IT sistema i prezentacije informacija o subjektu revizije u javnosti, revizor treba da ispita ima li subjekt revizije zvaničnu internet prezentaciju na internetu i društvenim mrežama i da li je njihovo kreiranje i održavanje definisano internim aktom. Ukoliko se utvrdi da postoji zvanična prezentacija, potrebno je ispitati kojim internim aktom je definisano ko, kako i na koji način vrši prezentaciju informacija na njima.

Važno je napomenuti da revizori prikupljanje dokaza o internet stranicama i nalozima na društvenim mrežama treba dvojako da posmatraju (zvanični nalozi subjekta revizije i nezvanični nalozi zaposlenih) i da vrše različita ispitivanja i procjene s obzirom na način rada ovih platformi.

U skladu s navedenim rizicima u vezi s prezentacijom subjekta revizije na internetu, prilikom kontrolisanja revizor treba da utvrdi:

- da li subjekt revizije ima zvaničnu internet stranicu;
- ko je odgovoran za prezentovani sadržaj na zvaničnoj internet stranici;
- da li se na internet stranici nalaze osnovni podaci o subjektu revizije (istorijski i sadašnji podaci, mapa, lokacija, kontakt podaci), podaci o svim organizacionim jedinicama, podaci namijenjeni korisnicima (savjeti, ciljani sadržaji koji povećavaju posjećenost internet stranice), dio za javne nabavke (subjekt iz javnog sektora) i drugo;
- da li se informacije koje se prezentuju na internet stranici kreiraju u subjektu revizije, tj. da li eksterni korisnici mogu mijenjati sadržaj na stranici.

Ukoliko zvanična internet stranica postoji, ali informacije na njoj nisu ažurne, tačne i pouzdane, postavlja se pitanje svrhe i opravdanosti troškova kreiranja internet stranice.

S druge strane, prilikom kontrolisanja prezentacije informacija o subjektu revizije na društvenim mrežama revizor treba da utvrdi:

- da li subjekt revizije ima zvanične naloge na društvenim mrežama;
- jesu li informacije koje se prezentuju na društvenim mrežama kreirane u subjektu revizije, tj. da li eksterni korisnici mogu mijenjati sadržaj na stranici;
- nalaze li se na društvenim mrežama neprimjerene fotografije i drugi neprimjereni sadržaji, nastali u toku radnog vremena i u prostorijama subjekta revizije;
- da li zaposleni subjekta revizije svojim neadekvatnim „objavama“ na društvenim mrežama narušavaju ugled subjekta revizije;
- jesu li preduzete određene aktivnosti kako bi se zaposlenima ukazalo na dozvoljene i nedozvoljene objave na društvenim mrežama u toku radnog vremena, a sve u cilju obavljanja radnih zadataka u skladu s principima i pravilima etičkog kodeksa i profesionalnog ponašanja;
- postoji li procedura ili interni akt u kojem je navedeno ko može, kako i na koji način kreirati, objavljivati i održavati zvanične naloge na društvenim mrežama.

Iako na sadržaj pojedinih objava na internetu nije moguće uticati (na primjer: objave na ličnim profilima korisnika društvenih mreža koji nisu zaposleni u subjektu revizije), rukovodstvo subjekta treba da utiče na objave zaposlenih čije neprimjereno objavljivanje sadržaja na društvenim mrežama u toku radnog vremena daje povod drugima za negativne komentare i objave koje se odnose na poslovanje subjekta revizije.

3.5. Kontrola računovodstvenog IT sistema i primjene informacionih tehnologija u računovodstvu

Sve vrste podsistema integrisanog IT sistema subjekta revizije za cilj treba da imaju kvalitetno izvještavanje korisnika – eksternih i internih, a posebno rukovodstva subjekta revizije. Posmatrajući pojedinačno, informacioni podsistemi (programi, aplikacije) imaju svoje mjesto, ulogu i značaj u okviru ukupnog (integrisanog) IT sistema subjekta revizije. Ipak, računovodstvo subjekta revizije, odnosno računovodstveni IT sistem, kao strogo formalizovan i institucionalizovan sistem (podsistem), treba biti najpouzdaniji i najvažniji dio ukupnog IT sistema subjekta revizije.

Prema svojoj prirodi, karakteristikama i ciljevima, računovodstveni IT sistem, koji čini sastavni dio integrisanog IT sistema, može se shvatiti kao uređena organizaciona cjelina sa međusobno povezanim činiocima. Stoga, s aspekta sistemskog pristupa, strukturu informacionog sistema čine sljedeće komponente (Aleksić-Marić i Stojanović, 2005):

- zaposleni (lifeware),
- oprema (hardware),
- programi (software),
- organizacija i čuvanje podataka (dataware),
- mrežne veze (netware),
- organizacioni postupci (orgware) koji omogućavaju prikupljanje, razvrstavanje, evidentiranje, sumiranje i čuvanje računovodstvenih

i finansijskih informacija neophodnih za sastavljanje i publikovanje računovodstvenih izvještaja.

Ako posmatramo poslovne sisteme koji obavljaju djelatnost u Republici Srpskoj, oni moraju poštovati odredbe Zakona o računovodstvu i reviziji Republike Srpske (Zakon o računovodstvu i reviziji, 94/15), kojim je određeno da se organizovanje, prikupljanje i sačinjavanje knjigovodstvenih isprava, vođenje poslovnih knjiga, sačinjavanje godišnjih finansijskih izvještaja vrši u skladu sa ovim zakonom i odgovarajućim podzakonskim propisima, poštujući pri tome usvojene računovodstvene standarde, računovodstvena načela i principe urednog knjigovodstva. Naime, pravno lice koje vrši obradu podataka na računaru dužno je koristiti računovodstveni softver koji omogućava funkcionisanje sistema internih računovodstvenih kontrola i onemogućava brisanje proknjiženih poslovnih događaja. Imajući u vidu ranije navedene odredbe Zakona, revizor na prvome mjestu treba da utvrdi da li je subjekat revizije usvojio novi pravilnik o računovodstvu i računovodstvenim politikama ili je izvršeno usklađivanje postojećeg pravilnika sa novim Zakonom koji je stupio na snagu krajem 2015. godine. Pored toga, revizorskim postupcima treba provjeriti usklađenost funkcionisanja računovodstvenog IT sistema sa zakonskom i podzakonskom regulativom. Provjera zakonske i podzakonske regulative odnosi se na kontrolu usklađenosti funkcionisanja računovodstvenog IT sistema sa Zakonom o računovodstvu i reviziji, te internim pravilnikom o računovodstvu i računovodstvenim politikama. Naime, krajem 2015. godine usvojen je Zakon o računovodstvu i reviziji, na osnovu kojeg je subjekt revizije izložen riziku plaćanja novčane kazne ukoliko ne uredi organizaciju računovodstva na propisan način.[1] Propisno organizovanje računovodstva podrazumijeva donošenje opštih akata kojima se uređuju pitanja od značaja za uspostavljanje i funkcionisanje sistema knjigovodstva i računovodstva u tim pravnim licima. Pod opštim aktima podrazumijevaju se Pravilnik o računovodstvu i računovodstvenim politikama i sva druga akta kojima uprava pravnog lica, u skladu sa zakonskim i profesionalnim pravilima uređuje pitanja od značaja za uspostavljanje i funkcionisanje sistema knjigovodstva i računovodstva. U skladu s navedenim, rukovodstvo subjekta revizije treba da kreira novi pravilnik o računovodstvu i računovodstvenim politikama ili uskladi postojeći, kojima će se definisati pitanja od značaja za uspostavljanje i funkcionisanje sistema knjigovodstva i računovodstva, a samim tim i računovodstvenog IT sistema.

U drugom koraku, revizor može izvršiti uvid u računovodstveni softver, te izvršiti komparativnu analizu sa sličnim programima koji se koriste u okruženju kako bi se dobilo uvjerenje o svrsishodnosti programa u upotrebi i cijeni licence koja se plaća za program u subjektu revizije. Pored ove analize, a s ciljem sticanja uvida u rad računovodstvenog softvera, revizor treba da dobije odgovore na pitanja:

- Da li se računovodstveni program zasniva na zastarjelim programskim rješenjima i primjeni zastarjelih funkcija?
- Da li je u programu navedeno uputstvo za korišćenje programa (help desk) za pojedine funkcije i operacije i lakše „kretanje“ zaposlenih kroz program?
- Da li je omogućen eksport podataka u excel i e-mail?
- Postoji li mogućnost izvještavanja i sortiranja po različitim kriterijumima neophodnim rukovodstvu subjekta revizije za donošenje poslovnih odluka.

Dobijanjem odgovora na navedena pitanja, revizor utvrđuje zadovoljstvo korisnika i ispunjenje njihovih potreba na postojećem programskom rješenju.

3.6. Računovodstveno evidentiranje nabavke i razvoja IT sistema

Nabavka IT sistema ili njegovog dijela podrazumijeva kupovinu licenci (nabavka programa za upravljanje kadrom, na primjer), a to se u poslovnim knjigama subjekta revizije treba knjižiti na bilansnoj poziciji „licence” jer se kupuje samo licenca, a ne kompletan softver. U specifičnim slučajevima nabavku je moguće iskazati i na bilansnoj poziciji „oprema” (recimo, nabavka softvera i licenci koje su sastavni dio hardvera i bez koga hardver ne može funkcionisati). S druge strane, razvoj IT sistema ili njegovog dijela zahtijeva definisanje određenih faza i postupaka razvoja, a u računovodstvenom smislu potrebno je razlikovati:

- održavanje poslovnih programa,
- nadogradnju i razvoj poslovnih programa.

Održavanje poslovnih programa, po pravilu, uvijek predstavlja trošak poslovanja, a nadogradnja i razvoj programa se, ako su ispunjeni uslovi predviđeni MRS 38, može kapitalizovati (ukoliko se nadogradnjom obezbijede nove funkcionalnosti programa). Iz ovoga se može konstatovati da kod računovodstvenog tretmana navedenih postupaka primarnu ulogu u primjeni ima Međunarodni računovodstveni standard 38 – Nematerijalna imovina, kojim je definisano da nematerijalnu imovinu čini imovina koja je bez fizičke suštine i koja se može identifikovati.

Međunarodnim računovodstvenim standardom 38 – Nematerijalna imovina određeno je da priznavanje neke stavke kao nematerijalne imovine zahtijeva da entitet pokaže da stavka zadovoljava definiciju nematerijalne imovine i kriterijume priznavanja. Nematerijalnu imovinu treba priznati ako su, i samo ako su, zadovoljeni sljedeći kriterijumi:

- ako je vjerovatno da će se buduće ekonomske koristi koje su pripisive imovini uliti u entitet,
- ako se nabavna vrijednost imovine može pouzdano odmjeriti.

Imajući u vidu brze promjene u tehnologiji, kompjuterski softver i mnoga druga nematerijalna imovina su podložni tehnološkoj zastarjelosti. Zbog toga postoji vjerovatnoća da će njihov korisni vijek biti kratak. Međutim, korisni vijek trajanja nematerijalne imovine može biti i veoma dug ili čak neograničen. Korisni vijek nematerijalne imovine, koja nastaje na osnovu ugovornih ili drugih zakonskih prava, ne treba da prevazilazi period važenja tih ugovornih ili drugih zakonskih prava, ali može biti kraći u zavisnosti od perioda tokom kojeg entitet očekuje da će koristiti imovinu.

Nakon izvršene kontrole primjene MRS 38, potrebno je izvršiti kontrolu primjene MRS 36 – Umanjenje vrijednosti imovine, kojim su definisani postupci koje entitet primjenjuje radi obezbjeđenja da se imovina ne knjiži po vrijednosti koja je veća od nadoknadivog iznosa. Sredstvo se knjiži po vrijednosti koja je veća od nadoknadivog iznosa, ako njegova knjigovodstvena vrijednost premašuje iznos koji će biti nadoknađen korišćenjem ili prodajom tog sredstva. U tom slučaju smatra se da je vrijednost sredstva umanjena i Standard zahtijeva da entitet izvrši priznavanje gubitka od umanjenja vrijednosti. Standard određuje i kada entitet treba da stornira gubitak od umanjenja vrijednosti i propisuje objelodanjivanja. U cilju primjene Standarda, entitet treba da na kraju svakog izvještajnog perioda procijeni da li postoje bilo kakve naznake da je vrijednost nekog sredstva umanjena, te ako postoje takve naznake, entitet treba da izvrši procjenu nadoknadivog iznosa za takvo sredstvo.

Prilikom kontrole računovodstvenog evidentiranja, pored navedenog zakona i standarda, obavezno se moraju uzeti u obzir i odredbe Pravilnika o kontnom okviru i sadržini računa u kontnom okviru za

[1] Zakon o računovodstvu i reviziji Republike Srpske, „Službeni glasnik Republike Srpske“ broj 94/15, član 64, navodi da će se novčanom kaznom od 3.000 KM do 15.000 KM kazniti za prekršaj pravno lice ako ne uredi organizaciju računovodstva na propisan način, ukoliko vrši obradu podataka na računaru, a ne obezbijedi da računovodstveni softver omogućava funkcionisanje sistema internih računovodstvenih kontrola, ukoliko ne sačinjava, ne kontroliše i ne čuva knjigovodstvene isprave, odnosno ne vodi i ne čuva poslovne knjige i druge izvještaje saglasno odredbama Zakona.

privredna društva, zadruge, druga pravna lica i preduzetnike, kojim je definisano da se:

- na računima grupe 01 – Nematerijalna sredstva, iskazuju ulaganja u određeno nematerijalno sredstvo bez fizičkog sadržaja, koje služi za proizvodnju ili isporuku robe ili usluga, za iznajmljivanje drugim licima ili se koristi u administrativne svrhe;
- nematerijalna sredstva priznaju se i vrednuju u skladu sa MRS 38, MRS 36, MSFI 6 i drugim relevantnim MRS, odnosno MSFI;
- na računu 011 – Koncesije, patenti, licence i ostala prava iskazuju se ulaganja u nematerijalna prava koja se priznaju u skladu sa MRS 38;
- na računu 014 – Ostala nematerijalna sredstva, iskazuju se izdaci za sticanje ostalih nematerijalnih sredstava koja se priznaju u skladu sa MRS 38;
- na računu 015 – Nematerijalna sredstva u pripremi, iskazuju se svi oblici nematerijalnih sredstava koji se priznaju u skladu sa MRS, odnosno MSFI od dana ulaganja do dana početka korišćenja;
- na računu 016 – Avansi za nematerijalna sredstva iskazuju se za sticanje svih oblika nematerijalnih sredstava;
- na računu 019 – Ispravka vrijednosti nematerijalnih sredstava, iskazuje se obračunata amortizacija, troškovi iscrpljivanja prirodnih bogatstava koji se knjiže na teret računa 540 – Troškovi amortizacije, kao i razlika između niže fer i knjigovodstvene vrijednosti, koja se knjiži na teret računa 580 – Obezvređenje nematerijalnih sredstava.

Stoga, prilikom kontrole računovodstvenog tretmana IT sistema subjekta revizije i komponenti IT sistema, revizor treba da:

- utvrdi evidentirani iznos u finansijskim izvještajima subjekta revizije, u aktivi bilansa stanja na dan 31. 12. 20XX. godine, na poziciji Nematerijalna sredstva;
- utvrdi strukturu nematerijalnih sredstava na poziciji Nematerijalna sredstva;
- utvrdi da li su nabavka i razvoj IT sistema (licenci) evidentirani na pozicijama Koncesije, patenti, licence i ostala prava;
- izvrši logičku, formalnu i računsku kontrolu analitičkih (finansijskih) kartica na kojima je izvršena evidencija nabavke, razvoja i održavanja programa i aplikacija;
- na osnovu slučajno odabranog uzorka izvrši kontrolu likvidiranja i knjiženja računa (da li računi sadrže sve neophodne priloge, na primjer, zapisnik o prijemu programa);
- da li se pravilno knjiži nabavka, razvoj i održavanje IT sistema, tj. da li se nabavka i razvoj IT sistema evidentira u okviru nematerijalnih sredstava, u skladu sa Međunarodnim računovodstvenim standardom 38 – Nematerijalna imovina, te da li finansijski izvještaji subjekta revizije u posmatranom periodu daju istinit i objektivan prikaz finansijskog stanja i rezultata poslovanja u posmatranom periodu;
- da li se razvoj IT sistema knjiži u skladu sa Međunarodnim računovodstvenim standardom 38 – Nematerijalna imovina, a ne u okviru, na primjer, nematerijalnih troškova – Troškova neproizvodnih usluga.

Međutim, pored navedenih revizorskih postupaka, koji se neposredno odnose na provjeru knjiženja nabavke i razvoja IT sistema, revizori treba da izvrše i dodatne provjere i kontrole koje su u posrednoj vezi s nabavkom i razvojem IT sistema. Primjer dodatnih postupaka može biti provjera da li je u slučaju postojanja neusklađenosti nematerijalne imovine redovnim godišnjim popisom utvrđena razlika i neusklađenost imovine subjekta revizije na dan popisa.

ZAKLJUČAK

Sprovođenje revizije informacionih sistema zahtijeva mnogo šire sagledavanje od uobičajenih procedura revizije, jer se za sveobuhvatan pregled moraju prikupiti (ne)materijalni dokazi koji su definisani različitim zakonima, podzakonskim aktima, ali i internim dokumentima.

Stoga rad kao cjelina ne predstavlja samo sagledavanje planova, nabavki i knjiženja, već i pojmovno obrazloženje i značaj informacionog sistema koji poslovnom sistemu pruža tačne i pouzdane informacije na osnovu kojih se donose upravljačke odluke. Osnova za donošenje upravljačkih odluka ogleda se u pripremi i kreiranju strateškog plana, evidencija i procedura upravljanja informacionim sistemom kako bi se izbjeglo neracionalno trošenje sredstava i ispravno evidentirale investicije i troškovi razvoja i održavanja. Samo uspostavljanje prethodnog nije dovoljno ako se ne definišu kontrolni mehanizmi, koji će davati signale da li ovaj sistem daje pouzdane i tačne informacije, te da li se njegov razvoj odvija prema određenim ciljevima.

Pored navedenog neophodno je obratiti pažnju na bezbjednost i dostupnost podataka, kako prilikom ulaza, tako i prilikom izlaza informacija iz poslovnog (informacionog) sistema. Naime, svi podaci u poslovnom sistemu ne treba da budu dostupni svim zaposlenima, kao ni javnosti. Iz tog razloga neophodno je kroz interna akta definisati nivoe dostupnosti, te koje informacije mogu i treba da se dostavljaju na uvid javnosti. Nepravilno rukovođenje informacijama može dovesti do materijalnih, ali i nematerijalnih troškova, koji u nekim slučajevima uveliko utiču na poslovanje i imidž poslovnog sistema, izazivajući daleko veće posljedice od materijalnih troškova.

IZVORI

1. Aleksić-Marić, V. (2008). *Elektronsko poslovanje*. Banja Luka: Ekonomski fakultet.
2. Aleksić-Marić, V., Stojanović, D. (2005). *Informacioni sistemi.* Banja Luka: Ekonomski fakultet.
3. Malešević, Đ., Vranković, M. (2007). *Poslovna analiza*. Subotica: Ekonomski fakultet.
4. Međunarodni računovodstveni standard (MRS) 36 – Umanjenje vrijednosti imovine. Preuzeto 18. 8. 2017. sa http://www.mfin.gov.rs/UserFiles/File/MRS/2014/IAS/IAS%2036.pdf.
5. Međunarodni računovodstveni standard (MRS) 38 – Nematerijalna imovina, paragraf 8. Preuzeto 18. 8. 2017. sa http://www.mfin.gov.rs/UserFiles/ File/MRS/2014/IAS/IAS%2038.pdf.
6. Pravilnik o kontnom okviru i sadržini računa u kontnom okviru za privredna društva, zadruge, druga pravna lica i preduzetnike. "Službeni glasnik Republike Srpske" br. 106/15.
7. Pravilnik o zaštiti prava osiguranih lica. "Službeni glasnik Republike Srpske" br. 26/11, 21/14.
8. Zakon o računovodstvu i reviziji Republike Srpske. "Službeni glasnik Republike Srpske" br. 94/15.
9. Zakon o sistemu internih finansijskih kontrola u javnom sektoru Republike Srpske. "Službeni glasnik Republike Srpske" br. 91/16.