ISSN 1864-6168

USPOREDBA REZULTATA REVIZIJE INFORMACIJSKIH SUSTAVA PROVEDENIH PREMA COBIT OKVIRU I UVOD U COBIT 5 OKVIR

[1]Varga M., [2]Varga V.
[1]Tehnička škola Čakovec, Čakovec, Hrvatska
[2]Mursko Središće, Hrvatska

Sažetak: *Ovim radom prikazana je revizija informacijskih sustava odabrane tvrtke, te okvir za korporativno upravljanje informatikom CobiT. U radu su nabrojane aplikacije, tj. moduli koji se koriste u promatranoj tvrtki. Spomenute su aktivnosti obavljene revizije, te je opisano značenje revizije informacijskih sustava i interne revizije. Prikazan je program stručnog usavršavanja za zvanje interni revizor informacijskih sustava i primjeri pripreme i provedbe revizije informacijskih sustava promatrane tvrtke. Revizijski dokazi su prikupljeni intervjuiranjem, vođenjem neformalnih razgovora, tehničkim ispitivanjem i testiranjem sustava. Rad pokazuje način funkcioniranja informacijskog sustava i kako djelovati na njegovo poboljšanje.*

Ključne riječi: *proces, potproces, modul glavna knjiga, aktivnosti, CobiT 4.1, CobiT 5, revizija informacijskih sustava.*

Summary: *This paper presents a review of information systems of the selected company and corporate governance framework for information technology. The paper lists the application modules that are used in the company. The aforementioned activities are audits which are conducted in the referred company. This paper describes the meaning of information systems auditing and internal auditing. It also depicts a training program for the profession of internal information systems auditor and examples of the preparation and implementation of information systems audit of the observed companies. Audit evidence was gathered by interviewing, conducting informal interviews, technical testing and system testing. The paper shows how the information system operates and how to work on improving information systems.*

Key words: *process, sub-process, general ledger module, activity, CobiT 4.1, CobiT 5, IT systems auditing* **.**

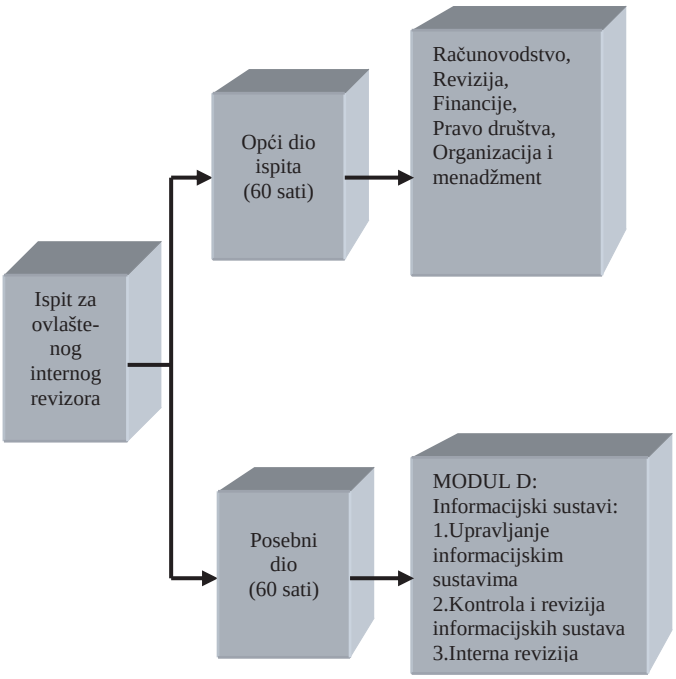
1. UVOD

Kako se kod revizije informacijskih sustava provode različite metode, slično je i ovdje gdje je riječ o reviziji informacijskog sustava u tvrtki Y. Potrebno je naglasiti da je kod revizije informacijskih sustava kao podrška financijskoj reviziji najčešći izbor CobiT okvir. Taj okvir pruža cjelokupnu metodološku potporu. U radu je prikupljeno nešto više podataka o reviziji informacijskih sustava promatrane tvrtke, kao i podataka o metodi kojom se provodi revizija IS-a (informacijskih sustava). Revizija informacijskih sustava je vrlo osjetljiva tema. Brojne tvrtke ne žele ju provoditi. Ona omogućava revizoru i upravi tvrtke da donese adekvatne odluke koje će u krajnjem slučaju poboljšati postojeći informacijski sustav tvrtke. Danas se o temi koja se odnosi na IT reviziju raspravlja i na internetskim servisima (npr. na Facebooku [8]), gdje je IT revizija otvorila svoj profil koji se odnosi na određenu regiju.

2. ZNAČENJE REVIZIJE INFORMACIJSKIH SUSTAVA I INTERNE REVIZIJE

U engleskom govornom području riječ revizija potječe od latinske riječi revidere, što znači ponovno gledanje ili ponovno viđenje, te je u skladu s tim revizija naknadni pregled i preispitivanje poslovnih procesa i stanja.[1] Revizija informacijskih sustava je sustavni proces koji se sastoji od aktivnosti koje se odvijaju po određenom logičkom slijedu radi ostvarenja postavljenih ciljeva. Revizija informacijskih sustava obuhvaća procjenu sigurnosti, pouzdanosti, zaštitu informacijskih sustava i analizu usklađenosti poslovnih planova s planovima uvođenja novih informacijskih tehnologija.[5] Revizor mora znati da će se u tom procesu susresti s uzrocima materijalnih i nematerijalnih gubitaka informacijskog sustava. Program osposobljavanja internog revizora za zvanje ovlašteni interni revizor u Republici Hrvatskoj prikazan je slikom 1.[6] Interna revizija je ispitivanje organizacijskih dijelova subjekata, načina rada i zadataka. Korisnici interne revizije su službe, sektori, odjeli, uprava, poslovodstvo, a u krajnjem slučaju mogu biti i zaposlenici na nižim razinama rukovođenja.[3] Internu reviziju provode osobe zaposlene u tvrtki čije se poslovanje ocjenjuje i riječ je o neovisnoj funkciji ispitivanja, prosuđivanja i ocjenjivanja bez ikakvih ograničenja i pritiska na programiranu prosudbu

internog revizora tvrtke. Sve aktivnosti tvrtke pripadaju krugu rada internog revidiranja.



Slika 1. Program stručnog usavršavanja za zvanje interni revizor informacijskih sustava

Slika 1.[6] prikazuje program stručnog usavršavanja za zvanje interni revizor informacijskih sustava. Uvjeti za pristupanje stručnom usavršavanju i ispitu za ovlaštenog internog revizora su odgovarajuća visoka stručna sprema, tri godine radnog iskustva u računovodstvu, financijama, reviziji, internoj reviziji ili u kontroli i kontrolingu. Certifikat s odgovarajućim zvanjem koji se stječe nakon položenih ispita i određenih modula je ovlašteni interni revizor za područje informacijskih sustava. Prije pristupa usavršavanju treba napomenuti koje sve certifikate kandidat posjeduje jer postoji mogućnost priznavanja drugih položenih certifikata što rezultira manjim obavezama, te bržim završetkom i stjecanjem naziva ovlašteni revizor informacijskih sustava. Položeni certifikati koji se priznaju, a spomenuti su na stranicama Hrvatske zajednice računovođa i financijskih djelatnika[6] su: ovlašteni revizor, ovlašteni državni revizor, ovlašteni unutarnji revizor u javnom sektoru, ovlašteni računovođa. Osim tih certifikata priznaje se završen poslijediplomski studij, ali kandidat opet mora polagati razlikovne ispite, tj. dokazati svoje znanje za određene nastavne cjeline i jedinice.

3. REVIZIJA INFORMACIJSKIH SUSTAVA

Revizija se još naziva kontrolom. Revizija ili kontrola informacijskih sustava je proces prikupljanja i vrednovanja (evaluacije) dokaza na temelju kojih se može utvrditi čuva li se imovina informacijskog sustava tvrtke na odgovarajući način, održava li se integritet podataka, omogućuje li se djelotvorno ostvarivanje postavljenih ciljeva i da li se učinkovito koriste dostupna sredstva.[3] Uz ostale kontrole koje se provode u informacijskim sustavima, povremeno je potrebno podsustave podvrgnuti reviziji, bilo unutarnjoj ili vanjskoj. Svrha revizije informacijskih sustava je ostvariti tradicionalne revizijske ciljeve, dokazne i upravljačke. Dokazni ciljevi ili vanjski revizijski ciljevi su oni koji se odnose na očuvanje imovine i integriteta podataka, dok se upravljački, odnosno unutarnji revizijski ciljevi usmjeravaju na provjeru učinkovitosti dokaznih ciljeva. Uz dva spomenuta cilja, postoji još jedan, a to je utvrđivanje udovoljava li organizacija odgovarajućim propisima, pravilima ili uvjetima, odnosno provjera zakonske sukladnosti poslovanja tvrtke. Nakon svega dolazimo do zaključka da se revizija informacijskih sustava može smatrati sredstvom što boljeg ostvarivanja glavnih ciljeva, a to su: bolje čuvanje imovine informacijskog sustava tvrtke, što viši stupanj integriteta podataka i promicanje učinkovitosti sustava.[3] Prilikom revizije informacijskih sustava u užem smislu može se nabrojati pet osnovnih koraka: analiza dokumentacije, prikupljanje revizijskih dokaza, analiza i vrednovanje revizijskih dokaza, priprema i predstavljanje revizijskog izvještaja. Tablica 1.[2] pokazuje postotak ukupnog trajanja revizije informacijskih sustava po pojedinim fazama. Za uspješno obavljenu reviziju potrebno je više vremena. Vrijeme koje se utroši po pojedinim fazama ovisi o veličini informacijskog sustava, tj. o softveru, hardveru, livewareu i orgwareu.

Tablica 1. Utrošak vremena po pojedinim fazama revizije

Faza revizije informacijskih sustava	**Postotak ukupnog vremena trajanja revizije**
Priprema i planiranje	10
Analiza i dokumentacija	10
Prikupljanje revizijskih dokaza	25
Analiza i vrednovanje revizijskih dokaza	20
Priprema revizijskog izvještaja	20
Predstavljanje revizijskog izvještaja	5
Aktivnosti nakon revizije	10

4. CobiT 5 UMJESTO CobiT-a 4.1

CobiT (eng. Control Objectives for Information and Related Technology) je okvir za korporativno upravljanje informatikom. Procesno je orijentiran i obuhvaća sve četiri komponente (područja) korporativnog upravljanja informatikom. Osnovna mu

je funkcija dati preporuke za usklađenje ciljeva poslovanja s ciljevima rada informatike. Prema CobiT-u, odgovornosti za provedbu informatičkih procesa nemaju isključivo profesionalni informatičari (CIO – glavni informacijski menedžer), nego i izvršni menedžment tvrtke. Njihov je temeljni zadatak upravljati cijelom informacijskom infrastrukturom, omogućiti da informatika podržava i dopunjuje strateške poslovne ciljeve, brinuti se o odgovornom korištenju informatičkih resursa i upravljati rizicima koji proizlaze iz intenzivne upotrebe informatike u poslovanju. CobiT je stvorio 1992. godine IT Governance Institute (ITGI) i Information System Audit and Control Association (ISACA – svjetska udruga za kontrolu i reviziju informacijskih sustava). CobiT je u samom početku bio orijentiran na poslovne ciljeve i aktivnosti, kako bi ih informatički dio poslovanja uspio podržati jer se jasno pozicionirao kao poslovni, a ne kao tehnički standard. Namijenjen je širokom krugu korisnika (informatičari, menedžment, interni i eksterni revizori, konzultanti...) i primjenjiv je u svim djelatnostima i okruženjima. Inzistira na korištenju jasnog poslovnog rječnika pri primjeni informatike i na uobičajenim poslovnim alatima pri upravljanju.

CobiT menedžmentu predočava funkcioniranje informacijskog sustava tako da određuje i detaljno opisuje ključne informatičke procese (34 procesa svrstana u 4 područja), određuje obaveze i područja odgovornosti (tko je odgovoran, tko kontrolira, te koga treba konzultirati prije same odluke), određuje nadzor i kontrolu (CobiT kontrolni ciljevi kojima se provjerava jesu li poslovni ciljevi ostvareni) te uspješnost informatičkih procesa (modeli zrelosti) i pojedinih aktivnosti.[3] Od 1998. CobiT verzija 2 postaje svjetski priznata kontrola informacijskih sustava i popratnih poslovnih procesa. Kako je vrijeme prolazilo tako je i opseg informacijskih sustava postao znatno širi. Opsežan informacijski sustav podrška je reviziji financijskih izvještaja i danas ima savjetodavnu (upravljačku) ulogu, gdje je opseg revizije cjelokupni informacijski sustav. Trenutačno važeća verzija CobiTa još je 4.1, koja sadrži četiri područja, 34 ključna informatička procesa, više od 300 detaljnih informatičkih kontrola, 18 aplikacijskih i 6 procesnih kontrola. Danas se sve više govori o okviru CobiT 5 umjesto o okviru CobiT 4.1. CobiT 5 će konsolidirati CobiT 4.1. Novost za CobiT 5 okvir je da će se razvijati još tijekom 2011. godine. CobiT 5 obuhvaća najnovija dostignuća upravljanja, a dobiveni rezultati potiču upravu na razmišljanje. Projekt pokretanja dokumentacije za općeniti razvoj CobiT 5 okvira odobrila je uprava svjetske udruge za kontrolu i reviziju informacijskih sustava ISACA. CobiT 5 je izgrađen i proširen na temelju CobiT 4.1 okvira.[7] CobiT 5 pomaže IT profesionalcima upravljati operativnim rizicima i držati ih na vrhu operativne usklađenosti. CobiT 5 pruža vodstvu tvrtke i izvršnom menedžmentu temelj za procjenu, usmjeravanje i praćenje IT-a tvrtke. CobiT 5 pomaže tvrtki da postigne svoje poslovne ciljeve, te predstavlja praktičan pristup za kontrolu i održavanje učinkovitosti upravljanja informatičkom tehnologijom s pratećim smjernicama i alatima. CobiT 5 okvir se temelji na zvučnim načelima i konceptima upravljanja tvrtkom. Osmišljeni CobiT 5 indirektno ojačava područje odlučivanja i organizacijsku strukturu.

5. PRIMJER PRIPREME REVIZIJE U TVRTKI Y

Za pripremu revizije potrebno je prikupiti podatke, odabrati revizijske metode i obaviti podjelu rada. Korištena su standardna revizijska pitanja i provjere. Cilj ove revizije je provjeriti učinkovitost informacijskih procesa, njihovu povezanost, vrijednost informacije, te mogućnost izvještaja i planiranja na temelju podataka. Budući da tvrtka nema implementiran CobiT, trebalo je prilagoditi metodologiju rada, što je pomalo otežavalo reviziju. To se primjenjuje tako da pojedine procese spajamo po sličnosti s CobiT procesima. Sve bi to bili inputi za određivanje rizika ciljeva kontrola i samih kontrola radi provjere učinkovitosti. Mora se naglasiti da većina aplikacija olakšava rad zaposlenicima i korisnicima informacijskih sustava i da je prije njenog provođenja bitno shvatiti strukturu informacijskog sustava i njegove elemente. Iz toga je vrlo lako zaključiti da je struktura složena budući da ne postoji određena dokumentacija o strukturi koja bi olakšala reviziju i omogućila bolji uvid u problematiku. Prema izjavama anketiranih i intervjuiranih zaposlenika, moglo se čuti da ne koriste mogućnosti koje im nude aplikacije. To je još jedan dokaz da je programiranje rutinski posao, tj. mijenjanje kodova u određenim linijama u ovom slučaju.

Tablica 2. Vrste transakcija i odgovarajuće aplikacije (moduli)

Važni procesi – razredi transakcije	**Odgovornost (tko)**	**Koriste li elektroničke revizijske dokaze? (da** ili **ne)**	**Aplikacije koje podupiru važne poslovne procese - transakcije**
Rezerviranje (ispravak vrijednosti)	Rukovoditelj računovodstva	Ne	Aplikacija za glavnu knjigu

za sumnjiva i sporna potraživanja			
Obračun poreza na dobit	Rukovoditelj računovodstva	Ne	Aplikacija za glavnu knjigu
Rezerviranja spravci vrijednosti za zalihe)	Rukovoditelj računovodstva	Ne	Aplikacija za glavnu knjigu
Nabava	Rukovoditelj komercijale i financija	Ne	Modul za nabavu
Prodaja	Rukovoditelj komercijale i financija	Ne	Modul za prodaju
Isplate	Rukovoditelj komercijale i financija	Ne	Aplikacija za blagajničko poslovanje
Uplate	Rukovoditelj komercijale i financija	Ne	Aplikacija za blagajničko poslovanje
Plaće	Rukovoditelj komercijale i financija	Ne	Aplikacija glavna knjiga
Zaključivanje financijskih izvještaja	Rukovoditelj računovodstva	Ne	Aplikacija glavna knjiga

Zbog povezanosti s bitnim revizijskim procesima trebalo je revidirati sljedeće aplikacijske module: modul glavne knjige, modul za nabavu, modul za prodaju, modul za blagajničko poslovanje. Treba obratiti pozornost na ostale komponente, prije svega tehničke i sigurnosne, te je potrebno iste kontrolirati. Kod tehničkih uvjeta, osim čvrstih dijelova (računala, mreža itd.), mislimo i na one programske komponente tipa operacijski sustavi i baze podataka koji se koriste, te na bilo koji način mogu utjecati na poslovanje tvrtke. Tablica 2.[3] prikazuje važne procese, odnosno vrste transakcija i odgovarajuće module aplikacija. Vidimo da je za spomenute procese najčešće odgovoran rukovoditelj komercijale i financija.

6. PRIMJER PROVEDBE REVIZIJE U TVRTKI Y

Kada se kreće s revizijom informacijskog sustava tvrtke prvo se gleda dokumentacija izrađena na temelju prethodne revizije informacijskih sustava. Ovaj rad ima određenu vrijednost i djelomično ukazuje na neke probleme koji nisu bili primijećeni, a bili su ili jesu potencijalno opasni, te mogu utjecati na poslovanje tvrtke Y. Nakon pregleda prijašnje dokumentacije, određuju se osobe koje će provoditi reviziju. Nakon toga može se planirati detaljni plan revizije koji se sastoji od sljedećih koraka: određivanje ciljeva i opsega revizije, identifikacija IT procesa, određivanje rizika za informatičke procese, odabir ciljeva i kontrole, priprema revizijskog programa, procedura i područja provjere, provedba revizije, identifikacija nedosljednosti kontrola, priprema izvještaja, diskusija o nalazima i rezultatima revizije s naručiteljem, priprema finalnog izvještaja[3]. Kod kontrole računalnih procesa riječ je o tome da je to vrlo bitna stavka kako bi revizijski nalaz bio vredniji i kako bi se mogli osloniti na revizijske dokaze. Nakon kontrole određujemo IT procese koji će biti predmet revizije. Procesi se odabiru i usklađuju s CobiT okvirom, ali se prilagođavaju metodologiji kojom provodimo reviziju. Naravno, prije same revizije važno je potpuno savladati korištenje informacijske infrastrukture i uočiti sve njene dijelove, što se lako postiže pregledavanjem dokumentacije IT odjela.[3]

6.2. Analiza IT okruženja u promatranoj tvrtki Y

Podatke o osnovnoj strukturi informacijskog sustava tvrtke prikupili smo iz anketa koje su ispunili odgovorni zaposlenici iz tvrtke Y. Osnovna struktura informacijskog sustava prikazana je u tablici 3.[3] Programska oprema promatrane tvrtke se koristi već izvjesno vrijeme i ne testira se. Vide se rješenja u slučaju incidenta na sustavima, kakva je povezanost glavnog i backup sustava, veza na internet i zaštita informacijskog sustava, ADSL veza u lokalnoj mreži, brzina od 100 Mbps, NOD ESET Smart Security 4 antivirusni program, tvrtka koristi antivirusnu zaštitu koja je instalirana na svim osobnim i prijenosnim računalima i na poslužiteljima, nadogradnja antivirusnog programa je ažurna, triput u tjednu skenira se cijeli sustav, te postoji kontrola u slučaju prestanka rada mreže ili pojedinih dijelova IS-a.

Tablica 3. Programi i popratna oprema koju koristi tvrtka

Aplikacija	Odjeli gdje se koristi	BR. Koris-nika	Opera-cijski sustav	Strojna oprema server	DBMS – sustav za upravljanje bazom podataka	Vlasnik aplikacije	Učestalost promjene na aplikaciji	Mogućnost udaljenog pristupa (da /ne)	Zajednička upotreba s poslovnim partnerima
Glavna knjiga	Računovodstvo	2	Linux	Server1	X – base	Tvrtka X i Y	Mjesečno	Da	Da
Potpora nabavi	Nabava	3	Linux	Server2	X – base	Tvrtka X i Y	Mjesečno	Da	Da
Potpora baždarnici	Baždarenje	6	Linux	Server3	X – base	Tvrtka X i Y	Mjesečno	Da	Da
Potpora distribucijskoj službi	Održavanje vodova za distribuciju	22	Linux	Server4	X – base	Tvrtka X i Y	Mjesečno	Da	Da
Potpora prodaji	Prodaja	7	Linux	Server5	X – base	Tvrtka X i Y	Mjesečno	Da	Da

6.1. Pregled poslovanja

Pregledom poslovanja, a koji se najčešće zbog netransparentnosti programa obavlja provjerom dostupne dokumentacije, dobivamo na uvid kako funkcioniraju poslovni procesi i jesu li oni povezani kontrolama. Ako je aplikacija vrlo složena, ti procesi su često odvojeni u posebne module koji predstavljaju zasebne procese. Prvo se provode tzv. walktrough testovi[3] promjena u aplikaciji. Osim prikupljanja dokumentacije nužno je u programu provesti pojedini postupak. U tablici 3. je opisan generički proces i osobe koje kontroliraju pojedine procese.

U tablici 4.[3] vide se procesi koje smo usporedili s procesima u tvrtki Y d.o.o. Iz tablice zaključujemo da je svaku promjenu u aplikaciji potaknuo korisnik i da su one u skladu sa zakonom. Ista osoba koja je zaprimila zahtjev odlučuje o tome je li za promjenu nužna treća strana (programer tvrtke X) ili se ona može provesti kroz opcije programa (bez dodatnog programiranja). U slučaju većih izmjena o tome odlučuju pomoćnik direktora tvrtke Y i IT menedžer tvrtke X. Kod dogovaranja uvjeta programer koji održava aplikaciju pomaže kod određivanja istih. Kod same izvedbe, aplikaciju testiraju u tvrtki X, ali isto tako i testni korisnici tvrtke Y (najčešće je to rukovoditelj komercijale i financija). Prelazak na novu verziju programa provode programeri tvrtke X, ali uz uvjet da se može prijeći na staru verziju programa. Ovdje je nužno da se pomoćnik direktora tvrtke konzultira s rukovoditeljem tehničke ili informatičke službe. Ako ga nema u tvrtki potrebno je “uzeti“ konzultantske usluge radi dodatne kontrole procesa.

Kod prelaska na novu verziju programa, osim programera tvrtke X u proces bi trebalo uključiti i osobu koja bi bila najbliža zvanju administratora informacijskog sustava tvrtke. Iz tablice 4. i 5. vidi se uredno provođenje kontrole u tvrtki Y.

6.2. Provjera pristupa programima

Tablica 5.[3] opisuje provjeru pristupa programima i povezane kontrole u tvrtki Y. Nakon što se novi zaposlenik zaposli u tvrtki, definira mu se radno mjesto te se piše molba za otvaranjem korisničkog računa ako mu je potreban. Razine pristupa ovise o radnom mjestu. Molbu potvrđuje pomoćni direktor tvrtke, a zahtjev za dodjelom prava pristupa šalje se administratoru tvrtke X koji održava cijelu informatičku infrastrukturu tvrtke. Upravo se tamo zaposleniku otvara korisnički račun, te mu se dodjeljuju prava pristupa. Ista molba šalje se na provjeru ostalim programerima koji održavaju aplikaciju tvrtke Y. U molbi se definiraju ovlasti i prava pristupa zaposlenika. O eventualnim promjenama prava pristupa ili pak o odlasku zaposlenika iz tvrtke kadrovska služba tvrtke Y obavještava tvrtku X. U slučaju odlaska iz tvrtke korisnički račun bivšeg zaposlenika se trajno briše. Osim pisanja i potvrđivanja molbe za otvaranjem korisničkog računa i određivanja prava pristupa sve se ostalo obavlja u tvrtki X. Od rukovoditelja odjela i pomoćnika direktora očekuje se dobro poznavanje informacijskog sustava kako bi točno odredili razinu pristupa novog zaposlenika. Ostalo obavlja tvrtka X i smatra se da su oni odgovorni za moguću štetu nastalu uslijed neovlaštenog pristupa pojedinim razinama sustava.

ISSN 1864-6168

Tablica 4. Opis procesa i ključnih osoba

Program i popratna oprema	Opis kontrole	Kontrolor
Informacijski sustav ERP-Enterprise Resource Planning	Promjenu programa najčešće potiče korisnik. Zahtjeve treba poslati na mail osobama koje brinu o aplikaciji, odnosno o informacijskom sustavu.	Programer koji održava aplikaciju - zaposlenik tvrtke X
Informacijski sustav ERP-Enterprise Resource Planning	Osoba koja održava aplikaciju određuje može li se promjena provesti u samoj tvrtki ili je potrebno angažirati zaposlenika tvrtke koji održava informacijski sustav.	Programer koji održava aplikaciju
Informacijski sustav ERP-Enterprise Resource Planning	U slučaju većih promjena koji zahtijevaju više resursa i imaju utjecaj na poslovanje, odluku treba potvrditi? (Tko?) Obrazloži(CIO, CEO)	IT menadžer tvrtke X i pomoćnik direktora tvrtke Y
Informacijski sustav ERP-Enterprise Resource Planning	Dobavljač, odnosno provoditelj promjena pomaže kod procjene i izvedivosti utjecaja na sustav. Precizno se određuju resursi.	Programer koji održava aplikaciju. Tvrtka X.
Informacijski sustav ERP-Enterprise Resource Planning	Ako nema važnijih prepreka, dogovori o primjeni se potvrđuju, definiraju se na relevantnoj razini (društvo i dobavljač) i dokumentiraju se na odgovarajućoj razini.	Pomoćnik direktora i IT menadžer tvrtke X.
Informacijski sustav ERP-Enterprise Resource Planning	Implementacija se provodi u testnom okruženju, osiguranje kvalitete (eng. Quality assurance). Sve završene aktivnosti trebaju potvrditi osobe koje brinu o aplikaciji.	Testni korisnici i osobe koje održavaju aplikacije
Informacijski sustav ERP-Enterprise Resource Planning	Transfer iz testnog u produkcijsko okruženje provode programeri tvrtke X. Pri tome se uzima u obzir da je moguć povratak na staro.	Programeri tvrtke X

Tablica 5. Opis provjere pristupa programima i povezane kontrole u tvrtki Y

Programska oprema	Opis kontrole	Kontrolor
Informacijski sustav ERP	Rukovoditelj odjela u koji dolazi novi zaposlenik šalje molbu za otvaranjem korisničkog računa s podacima o razini i pravima pristupa. Pored ostalih osnovnih podataka, molba treba sadržavati i naziv radnog mjesta, opis rada i potrebna prava pristupa.	**Rukovoditelj odjela**
Informacijski sustav ERP	Molba se šalje kod pomoćnika direktora tvrtke Y koji je potvrđuje.	**Pomoćnik direktora**
Informacijski sustav ERP	Pomoćnik direktora tvrtke Y priprema drugu molbu (zahtjev) za dodjelom prava pristupa novom zaposleniku koja se šalje u tvrtku X. Tu Tu se novom zaposleniku dodjeljuje korisničko ime i lozinka i izvještava se pomoćnik direktora tvrtke Y da je postupak uspješno dovršen.	**Pomoćnik direktora** **i tvrtka X.**

Informacijski sustav ERP	Zahtjev se šalje tvrtki X koja otvara novi korisnički račun, dodaje novog zaposlenika u domenu i dodjeljuje mu prava pristupa. Administrator sustava prema specifikaciji iz zahtjeva priprema hardver i softver koji je određen novom zaposleniku. Oprema i softver se uručuju nakon što je zaposlenik potpisao izjavu da je upoznat s pravilima njihova korištenja i s pravilima pristupa domeni.	**Sustavski administrator tvrtke X**
Informacijski sustav ERP	Molba (zahtjev) se dostavlja svim osobama koje održavaju ostale povezane aplikacije. Svaka osoba odgovorna za održavanje aplikacije treba provjeriti odgovaraju li dodijeljena prava pristupa opisu radnog mjesta. U molbi trebaju biti popisane sve aktivnosti novog zaposlenika, koje se prema potrebi detaljnije objasne.	**Programeri koji održavaju aplikaciju.**
Informacijski sustav ERP	O svakoj promjeni podataka za bilo kojeg zaposlenika kadrovska služba treba obavijestiti administratore sustava i programere koji održavaju aplikaciju. Zajedno s voditeljem odjela oni utječu na razinu prava pristupa. Kada zaposleniku prestane radni odnos, kadrovska služba o tome obavještava administratore sustava i programere koji održavaju aplikaciju. Zaposlenik koji napušta tvrtku treba od administratora sustava (osobe koja održava aplikaciju) i svih ostalih odgovornih zaposlenika dobiti potvrdu da više nema pristup podacima i sustavu, te da je vratio svu zaduženu opremu. Svojim potpisom te osobe jamče da korisniku više nije omogućen pristup sustavu i podacima. Nakon dva mjeseca korisnički račun se trajno briše.	**Kadrovska služba, administrator sustava, programeri koji održavaju aplikaciju.**
Informacijski sustav ERP	Važnije aktivnosti korisnika se bilježe (prijavljuju) u domeni i u aplikacijama. Bilješke („logovi“) na domeni administratora sustava se kontroliraju svaki dan, a aplikacijske samo po potrebi.	**Administratori sustava, programeri koji održavaju aplikaciju.**

6.3. Ostale i opće IT kontrole u tvrtki

U tablici 6.[3] opisuju se ostale IT kontrole u tvrtki. Lozinke se mijenjaju svakih mjesec dana i za svaki dio aplikacije postoji posebna lozinka. Ovdje se postavlja pitanje koliko je zaposlenicima zahtjevno pamtiti nekoliko lozinki postavljenih kao kombinacija velikih slova, malih slova i brojeva, a koje se mijenjaju svakih mjesec dana. Do nekih aplikacija je vanjski pristup moguć samo zaposlenicima programerske tvrtke X. Iz tablice 6. može se zaključiti da tvrtka X ima monopol kada je posrijedi vanjski pristup nekim modulima aplikacije i bazi podataka. Backup ili sigurnosna kopija se obavlja svaka tri dana, pa se postavlja pitanje kojih bi razmjera bila šteta u slučaju da pad sustava bude dva dana nakon posljednjeg backupa ili izrade sigurnosne kopije. U ovom slučaju u odnosu na prethodnu reviziju, iz revizijskog izvještaja vidi se da se backup obavlja dva dana prije, tj. svaka tri dana. Iz izvještaja za provedenu reviziju na dan 1.4.2010. godine vidljivo je da su se redovito pohranjivali podaci i programi svakih pet dana. Tablica 6. pokazuje da se sastanci predstavnika tvrtke Y i X na kojima se raspravlja o IT pitanjima održavaju najmanje dva puta u tjednu. Postavlja se pitanje koliko je dobra komunikacija među njima. U odnosu na prethodnu reviziju, vidljivo je da se sastanci održavaju u prosjeku jedan dan više u tjednu.

Drugim riječima, iz tablica proizlazi da tvrtka X nadzire informatiku tvrtke Y.
Tablica 6. prikazuje prisutnost više lozinki (s velikim i malim slovima**,** te brojevima od 7 znakova), pa se one e mogu zapisati na papir**.** Kodovima svih programskih modula mogu pristupiti samo programeri tvrtke X. Backup ili sigurnosna provjera radi se prosječno svaka tri dana, pa bi bilo poželjno analizirati što tvrtka gubi ukoliko korisnici određeni broj dana ne mogu pristupiti bazi podataka.

Tablica 6. Opis ostalih IT i općih kontrola u društvu

Kategorija	Opis
Upravljanje Lozinkama	Svaki zaposlenik mora imati lozinku da bi imao pristup određenom dijelu aplikacije, tj. određenom modulu. Lozinka se obično mijenja svakih mjesec dana i ima sedam znakova. Svaka lozinka sadrži velika i mala slova, te brojeve.
Udaljeni pristup (vanjski pristup)	Interna računalna mreža je zaštićena obrambenim zidom (vatrozidom ili firewall-om). Do nekih aplikacija je omogućen vanjski pristup samo programerima tvrtke X.
Antivirusna zaštita	NOD ESET SMART SECURITY 4 antivirusni program. Tvrtka koristi antivirusnu zaštitu koja je instalirana na svim osobnim računalima zaposlenika i na prijenosnim računalima, kao i na poslužiteljima. Nadogradnja antivirusnog programa je ažurna. Tri puta u tjednu pregledava se, odnosno skenira cijeli sustav.
Sigurnosne kopije	Podaci se snimaju svaka tri dana na novi disk. RAID 6 – organizacija sa zaštitom od dvostrukog kvara (P(1 paritetni disk)+Q(drugi paritetni disk) zalihost). Postoje dva zaštitna pojasa za svaku zaštićenu skupinu diskova koji se ravnomjerno raspoređuju po svim diskovima. Za sigurnosne kopije se brinu tvrtka Y i X. Administrator sustava je obaviješten o uspješnosti izrade sigurnosnih kopija. Tvrtke imaju sklopljen ugovor o tajnosti podataka, tako da tvrtka X ne može zlorabiti podatke tvrtke Y, kao ni zaposlenici tvrtke X. Zaposlenici ne mogu zlorabiti podatke tvrtke Y ni nakon prestanka rada u tvrtki X.
Serverska soba (tko nadzire?)	Serversku sob nadziru programeri tvrtke X i zaposlenici tvrtke Y.
Oporavak sustava nakon prekida	Za oporavak IS-a u tvrtki Y potrebno je oko 10 minuta.
Upravljanje problemima, incidentima i monitoring	Procedure u vezi s nadzorom IT procesa jamče adekvatnu kvalitetu izvođenja. Najmanje dvaput u tjednu održavaju se sastanci na kojima informatičari i predstavnici tvrtke Y diskutiraju o IT problemima.
Upravljanje	Tvrtka Y ima sa svim pružateljima usluga ugovore u kojima su regulirana prava, obaveze i odgovornosti.

razinama usluge (SLA-Service Level Agreements)	Tvrtka Y ima sklopljene ugovore s tvrtkom Z i tvrtkom X da podatke o poslovanju nikome ne smiju prosljeđivati niti ih zlorabiti. Od tvrtki Z i X koristi telekomunikacijske usluge i usluge održavanja i dogradnje aplikacija.

7. PREPORUKE UPRAVI TVRTKE

Kako bi se utvrdila kvaliteta sustava i na temelju toga donijele preporuke, potrebno je definirati idealnu funkciju sustava i mjerenje odstupanja stvarne od idealne funkcije. Informacijski sustav mora biti interno dobar da bi mogao biti sustav eksterno kvalitetan.[4] što se tiče lozinke, promatranoj tvrtki najbolje bi bilo postaviti lozinku koja se lako pamti, koja sadrži kombinaciju brojeva, te velika i mala slova. Nikako se ne preporuča za lozinku koristiti osobna imena, prezimena, imena roditelja, djece, datum rođenja, naziv mjesta boravišta, naziv ulice i sl. Za lozinku nije sigurno koristiti skup istih znakova. Za svaki modul bi bilo najbolje da se promijeni lozinka za određeni modul, a to bi napravili zaposlenici tvrtke Y. Na taj način nastoji se tvrtki X onemogućiti pristup podacima iz baze podataka od velike važnosti.

Preporuke za područje „sve sigurnosne poruke u operacijskom sustavu nisu aktivirane“: Operacijski sustav koji koristi tvrtka Y nudi mogućnost podešavanja automatskog primanja poruka o aktivnostima svih korisnika i pokušaju kršenja sigurnosnih pravila. Sustav ne može otkriti neautorizirane pokušaje pristupa. Nikada se nije dogodilo kršenje sigurnosnih pravila i neovlašteno korištenje podataka. Pokušaji provale uvijek postoje. IT menadžer treba odrediti osobu koja bi promatrala i bilježila poslovne događaje. Odmah nakon implementacije modula u informacijski sustav treba promijeniti pristupnu lozinku.

Kada je posrijedi učestalost pričuvne pohrane podataka, podaci bi se trebali pohranjivati svaki dan na kraju radnog vremena ili dva puta dnevno na novi disk. RAID 6 organizacija sa zaštitom od dvostrukog kvara (P(1 paritetni disk)+Q(drugi paritetni disk) zalihost). Postoje dva zaštitna pojasa za svaku zaštićenu skupinu diskova koji se ravnomjerno raspoređuju po svim diskovima. Za sigurnosne kopije tvrtka bi trebala imati zaposlenika koji bi brinuo o tim kopijama. Kada je riječ o oporavku sustava tvrtke Y, nakon prekida rada pojedinog dijela modula potrebno je oko 15 minuta za oporavak, što je svakako zadovoljavajuće. Vrijeme oporavka uvijek se nastoji smanjiti na što manje vrijeme čekanja.

8. ZAKLJUČAK

Revizija u tvrtki Y provedena je u siječnju 2011. godine. Na temelju poslovnog iskustva zaključujemo da je nužna interna revizija informacijskih sustava u tvrtkama. Svaka velika ili srednja tvrtka bi trebala imati unutarnje revizore informacijskih sustava koji bi trebali biti samostalni, objektivni i profesionalni, te bi tako obavljali internu reviziju. Objektivno i profesionalno provedena interna revizija preduvjet je za kvalitetnu eksternu reviziju. Podaci provedene revizije informacijskih sustava prikupljeni su intervjuom, neformalnim razgovorom, tehničkim ispitivanjem pojedinih softverskih modula, testiranjem informatičke opreme i sustava, te metodom promatranja. Za potpuno promatranje i opisivanje rezultata revizije informacijskog sustava tvrtke Y i CobiT 5 okvira nije dovoljan samo jedan članak, pa će sigurno biti prilike u idućim radovima.

9. LITERATURA

[1] Crnković, L.; Mijoč, I.; Mahaček, D. Osnove revizije. Ekonomski fakultet Osijek, 2010.
[2] Kapp, J. „How to conduct a security audit“. PC Network Advisor, Issue 120, July 2000.
[3] Panian, Ž.; Spremić, M. Korporativno upravljanje i revizija informacijskih sustava. Zagreb : Zgombić i partneri, 2007.
[4] Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb : travanj 2001.
[5] Spremić, M. Metode provedbe revizije informacijskih sustava. Zbornik Ekonomskog fakulteta u Zagrebu 5, 2007. , Hrčak, Članak, Izvor: hrcak.srce.hr/file/41339, (4.2.2011.)
[6] http://www.rif.hr/sekcija-internih-revizora/strucno-usavrsavanje, (27.1.2011.)
[7]http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx, (6.2.2011.)
[8] http://www.facebook.com/itrevizija, (8.2.2011.)

Kontakt:
Matija Varga, mag. inf., univ. spec. oec.
Poslijediplomski doktorski studij “Informacijske i komunikacijske znanosti“
na Filozofskom fakultetu u Zagrebu
Tehnička škola Čakovec, Čakovec, Hrvatska
E-mail: maavarga@gmail.com

Vesna Varga, univ. bacc. oec. i ovl. rač.
Diplomski studij “Financijski menadžment”
na Ekonomskom fakultetu u Osijeku
E-mail: maavarga@gmail.com