PRETHODNO PRIOPĆENJE
UDK 007:65.012.16

Prof. dr. sc. Mario Spremić

METODE PROVEDBE REVIZIJE INFORMACIJSKIH SUSTAVA

METHODS OF AUDITING INFORMATION SYSTEMS

SAŽETAK: U današnjim tržišnim okolnostima neprijeporna je činjenica da se sve veći dio poslovanja odvija uz potporu informacijskih sustava. S obzirom na činjenicu da informacijski sustavi često menadžmentu predstavljaju tzv. 'crnu kutiju' o kojoj vrlo malo znaju, a još je teže kontroliraju i upravljaju, tema kontrole i revizije informacijskih sustava u današnje se doba nameće kao imperativ uspješnog poslovanja. Naime, svjedoci smo sve veće razine ulaganja u informacijsku tehnologiju i informacijske sustave s često vrlo neizvjesnim ishodom ili pogrješnim strategijama. Često smo također svjedoci pogrješno postavljene ili slabo učinkovite informacijske infrastrukture koja nije prilagođena potrebama poslovanja i strateškim ciljevima, pa iziskuje dodatne nepotrebne troškove ili stvara nepremostive probleme. Dileme oko upravljanja informacijskim sustavima nikako se stoga ne mogu smatrati 'tehničkim' nego 'poslovnim' pitanjima, pri čemu koncept revizije informacijskih sustava menadžmentu predstavlja onu često nedostajuću kariku – 'most' između menadžmenta i informatike. U ovom se radu objašnjava koncept revizije informacijskih sustava, evolucija njegova razvoja (od podrške reviziji financijskih izvještaja do samostalne upravljačke i savjetodavne funkcije) i metode koje se na svjetskom razini koriste pri provedbi. Definira se i pojam korporativnog upravljanja informatikom, čije je jedno od područja upravo revizija informacijskih sustava. Prikazani su i obrađeni preliminarni rezultati istraživanja provedbe revizije informacijskih sustava u hrvatskim poduzećima i metode koje su se pri tome koristile.

KLJUČNE RIJEČI: revizija informacijskih sustava, korporativno upravljanje informatikom, CobiT, ITIL, ISO 27001, istraživanje.

ABSTRACT: In the circumstances of today's market the number of businesses that work with the help of information systems is constantly growing. IT systems are often, black box' to managers, i.e. it is something they know very little about, something they have difficulties controlling and managing, control and auditing of IT systems is an imperative for a successful business. Investing in IT and IT systems is constantly increasing but the results are often difficult to predict and wrong strategies have been often been used. IT infrastructure is often not very efficient or inaccurately installed. They are often not adjusted to needs and strategic goals of a business – therefore it demands additional unnecessary costs and creates insurmountable problems. So the dilemmas around management of IT systems cannot be considered ‚technical' but are ‚business' issues. In this context, the concept of auditing IT systems is a missing link for the management – a ‚bridge' between the

management and IT. This paper explains the concept of IT systems auditing, evolution of ist development (from supporting auditing of financial reports to independent managerial and advisory role) and methods that are globally used for its implementation. Corporate management of IT systems has also been defined – one of ist fields is auditing of IT systems. Preliminary research results of implementing IT systems auditing in Croatian enterprises and methods have been displayed and processed.

KEY WORDS: IT systems auditing, corporate management of IT, CobiT, ITIL, ISO 27001, research

1. ŠTO JE REVIZIJA INFORMACIJSKIH SUSTAVA?

Primjeri koji su doveli do propasti i pogrješne procjene financijskog stanja kompanija, kao što su Barrings Bank i Riječka banka, pokazuju da iako su postupci revizije poslovanja i revizije financijskih izvještaja formalno bili uredno provedeni, nisu rezultirali prikazom stvarnog stanja (u slučaju Riječke banke, koja je tada imala i ISO 9001 certifikat, svake su se godine tijekom 3-4 godine uredno provodile revizije financijskih izvještaja koje nisu otkrile nikakve nepravilnosti, a banka je već pri kraju treće godine bila u potpunom financijskom kolapsu). Zbog takvih i velikog broja sličnih primjera pokazalo se da i sami informacijski sustavi i njihovi ciljani dijelovi trebaju postati predmetom revizije. Informacijski sustavi i informatičko okruženje više se ne može smatrati odvojenim niti 'izoliranim' kontrolnim okruženjem i posve je logično da se regulatorni zahtjevi korporativnog upravljanja (Sarbanes-Oxley, Basel II) počnu primjenjivati i na taj dio poslovanja.

Revizija informacijskih sustava (engl. information system audit) predstavlja proces prikupljanja i procjene dokaza na temelju kojih se može procijeniti uspješnost informacijskog sustava, odnosno odrediti djeluje li informacijski sustav u funkciji očuvanja imovine, održava li se cjelovitost (integritet) podataka, omogućuje li se djelotvorno ostvarivanje ciljeva poslovanja i koriste li se resursi sustava na učinkovit način (Panian, 2001.)[1]. Na mnogim tržištima vrlo mlada struka, nastala isprva kao potpora reviziji financijskih izvještaja, revizija informacijskih sustava, osim egzaktne, analitičke, danas predstavlja i modernu savjetodavnu funkciju, desnu ruku koja menadžmentu pomaže pri (korporativnom) upravljanju informatikom. **Revizija informacijskih sustava** predstavlja stoga sustavan postupak kojim se ocjenjuje djeluje li informatika u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama.

Objekt revizije informacijskih sustava jest sustavno, temeljito i pažljivo pregledati kontrole unutar svih dijelova informacijskog sustava, a **osnovni zadatak** procijeniti njegovo trenutno stanje (zrelost, razinu uspješnosti), otkriti rizična područja i razinu rizika i dati preporuke menadžmentu za poboljšanje prakse njegova upravljanja (Spremić, 2005.).

Revizija informacijskih sustava je dakle *upravljačka* organizacijska funkcija koja omogućuje njegovu neovisnu i objektivnu *provjeru uspješnosti (zrelosti)*, odnosno analizu i provjeru funkcija, ciljeva i dijelova informacijskog sustava kako bi se prikupili dokazi koji se mogu neovisno razmatrati ili biti dobrom podlogom za ostale vrste revizije. Konačan rezultat tih postupaka jest *izvještaj revizora informacijskog sustava* koji se, prema područ-

[1] Prema: Panian, Ž., Kontrola i revizija informacijskih sustava, Sinergija, Zagreb, 2001.

jima analize (temeljene na CobiT ili ITIL okviru ili ISO 27001 normi), sastoji od sljedećih koraka:

- analiza stanja (zrelosti) primjene informacijskih sustava u poslovanju prema promatranim područjima
- procjena poslovnih rizika koji proizlazi iz zatečenog stanja i
- preporuke menadžmentu za poboljšanjem toga stanja.

Najčešći 'povod' primjeni revizije informacijskih sustava jesu regulatorni zahtjevi (primjerice, Sarbanes-Oxley zakon, Basel II norme, smjernice Hrvatske narodne banke o upravljanju rizicima, pojedine odredbe Zakona o bankama i obveze provedbe revizije financijskih izvještaja). Porastom važnosti primjene informatike u poslovanju sve je prisutnija savjetodavna funkcija revizije informacijskih sustava prema kojoj se ona koristi da bi neovisno tijelo 'snimilo' stanje, uočilo kritične točke, procijenilo rizike primjene informatike u poslovanju i dalo preporuke kako tim rizicima učinkovito upravljati. Time se, osim u mnogim zemljama obvezne regulatorne funkcije, revizija informacijskih sustava sve češće koristi i kao analitička i savjetodavna aktivnosti kojom se želi poboljšati postojeća poslovna praksa.

Pri tome, naravno, prednjače uspješne kompanije kojima su osnovni ciljevi provedbe revizije informacijskih sustava:

- provjeriti trenutno stanje informatike, odnosno utvrditi razinu zrelosti upravljanja informacijskim sustavom
- provjeriti učinkovitost kontrola informacijskih sustava, osobito kod ključnih poslovnih procesa
- otkriti potencijalno rizična područja i procijeniti razinu rizika kojim je poslovanje izloženo temeljem intenzivne primjene informacijskih sustava
- dati preporuke menadžmentu koje mjere poduzeti da se učinak uočenih rizika smanji ili ukloni i unaprijediti poslovnu praksu o tom pitanju.

Ernst & Young, jedna od 4 vodeće svjetske konzultantske i revizorske kompanije, u 2006. je godini na 1200 organizacija u 48 zemalja provela istraživanje[2] o tome koja su tri najčešća pokretača ili 'motiva' provedbe revizije informacijskih sustava. Rezultati su bili sljedeći:

- 56% posto svih ispitanih je u 2006. godini iz regulatornih razloga provodilo reviziju informacijskih sustava, dok procjenjuju da će u 2007. godini taj postotak biti 50%
- u 2006. godini 47% organizacija je moralo provesti reviziji u skladu s regulativom vezanom uz privatnosti podataka, dok će u 2007 to morati njih 42%
- 38% organizacija je provodilo reviziju u 2006. godini u vidu postizanja poslovnog cilja, dok će to u 2007. godini učiniti 41% ispitanih.

2. PODRUČJA PRIMJENE REVIZIJE INFORMACIJSKIH SUSTAVA

Revizija informacijskih sustava najčešće obuhvaća sljedeće važne aktivnosti:

[2] Ernst & Young (2006.): Achieving Success in a Globalized World – Is Your Way Secure?, 2006 Global Information Security Survey.

- procjena razine rizika djelovanja informacijskih sustava (informacijske funkcije)
- procjena poslovne vrijednosti informacijskog sustava (procjena djelotvornosti i učinkovitosti informacijskog sustava)
- analiza usklađenosti poslovnih planova s planovima informatike (strateško planiranje informacijskih sustava)
- detaljna analiza isplativosti ulaganja u informatiku (dijelovi studije izvedivosti, metode financijske analize informatičkih projekata, preporuke za poboljšanje prakse vođenja informatičkih projekata)
- analiza, pregled i ocjena kvalitete cjelovitog informacijskog sustava ili njegovih pojedinih dijelova
- provjera (revizija) provedbe pravilnika o sigurnosnoj politici informacijskog sustava
- revizija provedbe ostalih korporativnih pravilnika koji se tiču informacijskih sustava
- procjena kvalitete usluge informacijskih sustava ili njegovih dijelova
- primjena kontrolnih mehanizama pri radu i upravljanju informacijskim sustavom (upravljačke, procesne, opće ili aplikacijske kontrole rada informacijskog sustava, a time i kontrola kvalitete rada poslovnog sustava)
- analiza i nadzor informatičkih projekata
- analiza performansi poslovnih procesa koji se odvijaju uz pomoć informacijskih sustava
- analiza rizika ključnih automatiziranih poslovnih procesa
- procjena sigurnosti, pouzdanosti i zaštite informacijskog sustava
- provedba specifičnih kontrolnih mehanizama (primjerice, kontrola neprekidnosti poslovanja, kontrola oporavka nakon neželjenih događaja, kontrola neprekidnosti poslovanja, razne sigurnosne kontrole, kontrole provedbe poslovnih procesa, kontrole obrade, podataka itd.).

Mnoge od tih aktivnosti su ključne sa stajališta upravljanja korporativnim rizicima. Pogrješne procjene menadžmenta o utjecaju informacijske tehnologije i informacijskih sustava mogu imati prilično ozbiljne posljedice na funkcioniranje, pa čak i opstanak poslovanja. Primjerice, prema istraživanju koje je proveo časopis CFO u 2005., samo 40% direktora financija (CFO, engl. Chief Financial Officer) smatra da ulaganja u informatiku daju očekivane rezultate[3], što znatno povećava rizik neisplativih ulaganja u informatiku. Također, prema istraživanjima Disaster Recovery Instituta, 93% kompanija koje dožive katastrofu i prekid odvijanja poslovnih procesa, a nemaju plan kontinuiteta poslovanja, prestanu postojati nakon pet godina. 50% kompanija koje izgube ključne poslovne funkcije na više od deset dana nikada se ne oporave. Za kompanije iz Fortune 500 liste vrijeme zastoja poslovanja stoji u prosjeku 96.000 USD po minuti[4]. Sličnim se procjenama barata i u pojedinim djelatnostima, pa tako u slučaju prekida odvijanja poslovnih procesa na samo jedan sat, prosječan gubitak u investicijskom posredništvu na globalnoj razini iznosi oko 6,5 milijuna USD, u kartičarskom poslovanju (autorizacija kreditnih kartica) oko 2,6 mili-

[3] CFO Research Services (2005.): Risk Denial from the Top?, CFO Publishing Corp. i PriceWaterhouseCoopers.

[4] Kenneth L. Fulmer: 'Business Continuity Planning - A Step-by-Step Guide with Planning Forms, Third Edition, The Rothstein Catalog On Disaster Recovery, Brookfield, Connecticut, 2005., str. 7

juna USD, u logistici i paketnoj distribuciji oko 150.000 USD, a u rezervacijskim sustavima za zrakoplove oko 90.000 USD[5].

Čini se stoga logičnim i posve opravdanim 'braniti', odnosno sustavnim mjerama pokušati štititi vrijednu korporacijsku imovinu. U takvim se okolnostima provedba revizije informacijskih sustava, odnosno prije svega procjena razina rizika kojim je poslovanje izloženo korištenjem informacijske tehnologije i informacijskih sustava čini neminovnim i nužnim koracima koje menadžment treba poduzeti.

3. INFORMACIJSKI SUSTAVI I KONTROLNO OKRUŽENJE

Nezaobilazni dio provedbe revizije informacijskih sustava jest **procjena učinkovitosti kontrola informacijskog sustava**. Pri tome se najčešće radi o procjeni učinkovitosti internih kontrola informacijskog sustava kao sastavnog dijela cjelovitog sustava internih kontrola poslovanja. **Interne kontrole sa stajališta revizije informacijskih sustava** predstavljaju sustav kojim se sprječavaju, otkrivaju i ispravljaju neželjeni događaji i procesi u informacijskom sustavu i njegovom okruženju, stoga su interne kontrole skup međusobno povezanih komponenata koje usklađenim djelovanjem potpomažu ostvarivanju utvrđenih ciljeva informacijskih sustava. To se najčešće postiže na način da se specifične upravljačke, opće i aplikativne kontrole ugrađuju u sve dijelove i na svim razinama funkcioniranja informacijskog sustava, a koncentriraju se na moguće neželjene događaje ili procese unutar sustava. Menadžment kompanije u suradnji s menadžmentom informacijskog sustava izravno je odgovoran za oblikovanje, provedbu i ocjenu efikasnosti sustava internih kontrola unutar informacijskog sustava. **Česta je pogrješka** da se informacijski sustavi smatraju posebnim, 'izoliranim' kontrolnim okruženjem koje je odvojeno od kompanijskog sustava unutarnjih (internih) kontrola. Povod takvom stavu obično je nerazumijevanje kojim poslovnim rizicima kompanija može biti izložena temeljem pogrješnog, neovlaštenog ili nepouzdanog korištenja informacijskog sustava. Iz tih je razloga izrazito važno periodički provoditi reviziju informacijskih sustava, jer ona u modernom poslovanju predstavlja 'sponu' između poslovanja i informatike.

3.1 Osnovne vrste kontrola informacijskog sustava

Kontrole informacijskog sustava možemo razvrstati prema razinama upravljanja kojima su namijenjene i načinu na koji djeluju.

S obzirom na *razine upravljanja* razlikujemo sljedeće vrste informatičkih kontrola:

- **Upravljačke kontrole** – informatičke kontrole na najvišoj razini upravljanja koje čine sastavni dio sustava internih kontrola poslovanja, a odnose se na kontrole provedbe strategije informacijskog sustava, kontrole upravljanja informatikom, kontrole prekida ili otežanog odvijanja kritičnih poslovnih procesa, kontrole procesa financijskog izvještavanja, kontrole provedbe sigurnosne politike informacijskih sustava, kontrole vođenja informatičkih projekata, kontrole procesa upravljanja rizicima intenzivne primjene informacijskih

[5] Ibidem.

sustava, kontrole planova ulaganja u informatiku, ustrojavanje i funkcioniranje ključnih tijela zaduženih za upravljanje informatikom (Odbor za informatiku, engl. IT Steering Committee), kontrole kvalitete informacijskih sustava i aktivnosti sustavnog provođenja interne kontrole i revizije informacijskih sustava, kontrole poštivanja zakonskih obveza iz područja informatike itd.

- **Procesne i opće kontrole** – kontrole koje se odnose na razvoj i kupnju poslovnih aplikacija, kontrole instalacije aplikacija, kontrole nad podatcima koje te aplikacije i pripadajući poslovni procesi koriste, kontrole promjena softvera, kontrole pristupa programima i podatcima, sigurnosne kontrole, kontrole kontinuiteta poslovanja (BC - engl. business continuity), kontrole oporavka nakon prekida rada (DR - engl. disaster recovery), automatske ili ručne kontrole koje su 'ugrađene' u poslovne procese i koje omogućuju njihovu točnu, pouzdanu i neometanu provedbu, kontrole koje omogućuju učinkovito i korektno funkcioniranje poslovanja u informatičkom okruženju, kontrole ispravnosti transakcija, kontrole prijenosa podataka, kontrole kvalitete podataka, kontrole ključne opreme i sve ostale kontrole koje podržavaju učinkovite kontrole nad aplikacijama koje su temelj odvijanja poslovnih procesa.
- **Aplikacijske kontrole i kontrole informatičkih servisa** (usluga) – odnose se na razne kontrole rada poslovnih aplikacija, kontrole provedbe informatičkih aktivnosti i operacija (jesu li transakcije točne, potpune, cjelovite, podjela dužnosti i kontrola, autorizacija itd.) i kontrole informatičkih servisa (dostupnost i funkcionalnost mreže, infrastrukture, podataka, opreme itd.). U ovu kategoriju spadaju i brojne kontrole samog poslovnog softvera, poput kontrole operacijskog sustava, kontrole instalacije i održavanja softvera, kontrole softvera za prijenos podataka, kontrole sigurnosnog softvera, kontrole opreme nad kojom sustav radi, kontrole funkcioniranja sustava otkrivanja pogrješaka, kontrole otkrivanja uzroka informatičkih incidenata, kontrole konfiguracije opreme, kontrole praćenja rada sistemskog softvera i cjelokupnog informatičkog okruženja, kontrole neovlaštenog 'upada' u sustav, kontrole isporuke informatičke usluge, kontrole funkcionalnosti aplikacija i informatičkih usluga (to se posebno odnosi na ugovor o razini kvalitete usluge, engl. Service level agreement, SLA), kontrole dostupnosti sustava (mreže, opreme itd.), kontrole nad uslugama koje pružaju druge kompanije ('outsourcing' kontrole) i sve ostale operativne, dnevne aktivnosti kojima se kontrolira funkcioniranje cjelokupne informacijske infrastrukture poslovanja.

Prema načinu djelovanja razlikujemo sljedeće vrste informatičkih kontrola:

- **preventivne kontrole (prethodne i procesne)** čiji je osnovni zadatak otkriti probleme ili neželjene događaje prije nego što se pojave, predvidjeti ih, prevencijom pokušati spriječiti propuste i, konačno, stalno pratiti aktivnosti informacijskog sustava, najvažnije operacije, procese, ulaze, izlaze i uočavati anomalije. Tipični primjeri preventivnih kontrola su zapošljavanje obrazovanih, kvalificiranih zaposlenika, određivanje organizacijskih tijela kojima se nadzire rad informacijskog sustava (upravljački odbor za informatiku), ustrojavanje odjela za unutarnju reviziju informacijskog sustava, podizanje razine svijesti o potrebi provedbe kontrole i revizije informacijskih sustava, podjela dužnosti i odgovornosti, logičke i fizičke kontrole pristupa informacijskom sustavu, donošenje pravilnika o sigurnosnoj politici informacijskog sustava itd.
- **detektivne kontrole** predstavljaju kontrole koje otkrivaju pogrješku, propust ili ugrozu bilo kojeg dijela informacijskih sustava, a tipični primjeri su razne opće informatičke kontrole, kontrole unosa podataka, autorizacijske kontrole, fizičke i logičke kontrole pristupa sustavu i podatcima, provjera ovlasti za rad na sustavu, kontrole točnosti rada aplikacija, procesne kontrole, kontrole nad podatcima, itd.

- **korektivne kontrole** koje imaju za cilj minimizirati učinak prijetnje ili ugroze informacijskom sustavu, pri čemu one utvrđuju uzrok problema te automatski izvršavaju posebne instrukcije kako bi se uočene pogrješke ispravile (procedure kopiranja i arhiviranja podataka, kontrole prijenosa podataka, procedure ponovnog uspostavljanja funkcija sustava, kontrole nad ključnom opremom itd.

Osim toga, informatičke se kontrole mogu razvrstati i prema specifičnim područjima koje 'pokrivaju' (**sigurnosne kontrole, informacijske (podatkovne) kontrole**, **kontrole kontinuiteta poslovanja itd.)**

Informatičke kontrole možemo također razvrstati i prema okvirima ili normama koje se koriste pri procjeni njihove učinkovitosti i efikasnosti. Tu se već radi o specifičnim pogledima na kontrolne mehanizme informacijskih sustava, a okviri i norme koje se u svjetskim razmjerima najčešće pri tome koriste su CobiT, ITIL i ISO 17799 i ISO 27001 norme. Njihov je detaljniji opis prikazan u nastavku rada, a u ovoj prilici obratimo pozornost na razradu procesnih i aplikacijskih kontrola koje propisuje CobiT okvir.

Prema CobiT okviru postoji 6 procesnih i 18 aplikacijskih informatičkih kontrola koje se u velikoj mjeri mogu koristiti i pri provjeri (reviziji) efikasnosti kontrola financijskog izvještavanja. Procesne kontrole (kontrole CobiT procesa) su prikazane na slici 1, a CobiT aplikacijske kontrole na slici 2.

Slika 1. CobiT procesne kontrole

COBIT PROCESNE KONTROLE (PROCESS CONTROL - PC)
PC1 Određivanje vlasnika poslovnog procesa
PC2 Određivanje repetitivnih (ponavljajućih) procesa
PC3 Određivanje jasnih ciljeva svakog procesa
PC4 Uloge i odgovornosti
PC5 Performanse procesa
PC6 Politike, planovi i procedure

Slika 2. Aplikacijske kontrole prema CobiT metodi kontrole i revizije informacijskih sustava

COBIT APLIKACIJSKE KONTROLE (APPLICATIONS CONTROL – AC)

KONTROLE AUTORIZACIJE PODATAKA
AC1 Procedure pripreme podataka
AC2 Autorizacija izvornih dokumenata
AC3 Prikupljanje podataka
AC4 Upravljanje pogrješkama
AC5 Pohrana podataka

KONTROLE ULAZA PODATAKA
AC6 Autorizacijski postupci
AC7 Točnost, potpunost i autorizacija
AC8 Upravljanje pogrješkama pri unosu

KONTROLE OBRADE PODATAKA
AC9 Cjelovitost obrade podataka
AC10 Provjera ispravnosti obrade
AC11 Upravljanje pogrješkama

KONTROLE IZLAZA PODATAKA
AC12 Prikaz i pohrana izl. pod.
AC13 Distribucija izl.pod.
AC14 Usklađenje izl.podataka
AC15 Pregled ispravnosti izl. pod.
AC16 Sigurnost izlaznih podataka

KONTROLE PRI PRIJENOSU PODATAKA
AC17 Autentifikacija, autorizacija i provjera cjelovitosti
AC18 Zaštita osjetljivih podataka pri prijenosu na daljinu

4. METODE PROVEDBE KONTROLE I REVIZIJE INFORMACIJSKIH SUSTAVA

Važan zadatak revizije informacijskih sustava jest i procijeniti udovoljava li sustav minimalnim zahtjevima uspješnosti, odnosno procijeniti razinu usklađenosti kontrola u sustavu sa svjetski priznatim normama i okvirima prema kojima se takva provjera (revizija) provodi. Primjeri norma i okvira kojima se određuje najbolja svjetska praksa pri upravljanju informatikom i provedbi revizije informacijskih sustava su CobiT, ITIL i ISO/IEC 17799:2005 i ISO/IEC 27001 norma.

4.1. CobiT

CobiT[6] (engl. **CobiT – Control Objectives for Information and Related Technologies**) je svjetski prihvaćen okvir unutar kojega se propisuju područja i pojedinačne kontrole za upravljanje informatikom i pripadajućim informatičkim procesima. Autor CobiT okvira je ISACA (Information System Audit and Control Association, www.isaca.org) i ITGI (IT Governance Institute, www.itgi.org).

Izvorno (CobiT v1 iz 1996.) nastao kao alat za podršku provedbe revizije financijskih izvještaja, CobiT se vrlo brzo razvijao i pratio razvoj uloge informatike u poslovanju (CobiT v2 iz 2000. već je u svjetskim razmjerima postao najkorišteniji okvir kontrole informacijskih sustava, verzija 3 iz 2004. godine je predstavljala integralni okvir upravljanja informatikom, a trenutno važeća verzija – CobiT 4.1 predstavlja najvažniji okvir provedbe koncepta korporativnog upravljanja informatikom). CobiT sadrži 4 područja, 34 ključna informatička procesa (cilja kontrole), preko 300 detaljnih informatičkih kontrola, 18 aplikacijskih i 6 procesnih kontrola. Za svaki od 34 IT procesa CobiT 'nudi':

- modele zrelosti (engl. maturity models, ocjene od 0 do 5)
- kritične čimbenike uspjeha (CSF, engl. critical success factors)
- ključne indikatore ostvarenja cilja (KGI, engl. key goal indicators)
- smjernice menadžmentu za praćenje performansi i ključne indikatore performansi (KPI, engl. key performance indicators)
- smjernice menadžmentu za upravljanje rizicima (tzv. RACI matrica, prema akronimu engleskih riječi Responsible, Accountable, Consulted, Informed, što predstavlja matricu kojom se za svaki od 34 procesa određuje tko je odgovoran i ovlašten provoditi pojedine kontrolne aktivnosti, a koga samo treba izvijestiti i konzultirati.)
- ciljeve kontrole i kontrolne testove.

Temelj CobiT okvira su 34 ključna informatička procesa, odnosno cilja kontrole funkcioniranja informacijskih sustava podijeljenih u ove četiri kategorije:

- **Planiranje i organizacija informatike** (engl. planning and organization, PO)
- **Akvizija (nabava) i implementacija** (engl. aquisition and implementation, AI)
- **Isporuka i potpora radu (uporaba)** (engl. delivery and support, DS)
- **Nadzor i procjena uspješnosti** (engl. monitoring and evaluation, ME).

[6] ITGI (2007), CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, IT Governance Institute, Rolling Meadows, SAD.

Slika 3. 34 ključna IT procesa (ili cilja kontrole) prema CobiT metodologiji (napomena: crvenom bojom su istaknuti procesi najvišeg prioriteta)

PLANIRANJE I ORGANIZACIJA (PO)
PO1 Strateško planiranje IS
PO2 Definiranje informacijske arhitekture
PO3 Određivanje tehnoloških smjernica
PO4 Definiranje IT procesa, organizacije i odnosa
PO5 Upravljanje IT investicijama i troškovima
PO6 Komuniciranje prema menadžmentu
PO7 Upravljanje ljudskim resursima
PO8 Upravljanje kvalitetom
PO9 Upravljanje i procjena rizika
PO10 Upravljanje projektima

AKVIZICIJA I IMPLEMENTACIJA (AI)
AI1 Određivanje mogućih rješenja
AI2 Nabava i održavanje aplikacijskih programa
AI3 Nabava i održavanje tehnološke arhitekture
AI4 Korištenje i funkcionalnost rada (obrade)
AI5 Nabava IT resursa
AI6 Upravljanje promjenama
AI7 Instalacija i odobravanje rješenja i promjena

ISPORUKA I POTPORA (DS)
DS1 Definiranje i upravljanje razinama usluga
DS2 Upravljanje vanjskim uslugama
DS3 Upravljanje performansama i kapacitetom
DS4 Osiguranje kontinuiteta usluga
DS5 Sigurnost sustava
DS6 Određivanje i dodjela troškova
DS7 Izobrazba i trening korisnika
DS8 Podrška korisnicima
DS9 Upravljanje konfiguracijom
DS10 Upravljanje problemima i incidentima
DS11 Upravljanje podatcima
DS12 Upravljanje pomoćnom opremom
DS13 Upravljanje operacijama (obradom)

NADZOR I PROCJENA (ME)
ME1 Nadzor i procjena IT performansi
ME2 Nadzor i procjena internih kontrola
ME3 Sukladnost s zakonskim i drugim normama
ME4 Korporativno upravljanjem IT-om

CobiT poslovnu informatiku 'dijeli' u 4 područja, 34 ključna poslovna procesa (cilja kontrole) i za svaki opisuje model zrelosti. Upućenom menadžmentu i korporativnim strukturama lako je pomoću CobiT metode utvrditi koji su od tih procesa i u kojoj mjeri važni. Sa stajališta kontrole i revizije informacijskih sustava CobiT određuje i 18 aplikacijskih i 6 procesnih kontrola.

4.2. ITIL (engl. IT Infrastructure Library)

Iako je nastao prije gotovo 20 godina (potkraj 1980-ih), ovaj se okvir tek u novije vrijeme nametnuo kao koristan, praktičan i u svjetskim razmjerima gotovo neizostavan skup preporuka i najbolje prakse pri upravljanju informatičkim uslugama (engl. IT Service Management). Autor ITIL metodologije je britanska Central Computer and Telecommunications Agency (mogli bismo je slobodno prevesti kao Agenciju za telekomunikacije i informatiku, koja više ne djeluje pod tim imenom nego kao Office of Government Commerce (UK)) koja je potkraj 80-ih godina prošlog stoljeća napravila prvi popis uputa za korištenje informatičkih usluga kojih su se sva tijela u britanskoj javnoj administraciji trebala pridržavati (između ostalog i poznati MI 5 špijunski odjel u kojemu su tajni agenti koristili najnovije tehnologije koje su im pomagale u poslu). Od tada su se ITIL upute stalno nadograđivale i unaprjeđivale, a danas su, u svjetskim razmjerima općeprihvaćeni standardi upravljanja informatičkim uslugama razvijeni do te mjere da čak i dobavljači nude svoju opremu i usluge koja je u skladu s ITIL metodologijom. IT Service Management Forum (ITSMF) je neprofitna organizacija koja vodi brigu o unaprjeđenju prakse korištenja i upravljanja informatičkim uslugama i napretku ITIL metodologije.

ITIL pruža tzv. *top-down*, odnosno poslovno orijentiran pristup menadžmentu informatike koji stavlja poseban naglasak na stratešku poslovnu vrijednost informatike i potrebu da se isporuči njezina visokokvalitetna usluga (informatička usluga, IT usluga). Osim toga, ITIL pruža smjernice i preporuke koje su usmjerene radu ljudi, funkcioniranju procesa i korištenju tehnologije pri korištenju informatike i pružanju kvalitetne usluge.

ITIL se sastoji od uputa temeljenih na najboljoj praksi upravljanja informatičkim uslugama u javnim i privatnim organizacijama širom svijeta. ITIL se formalno sastoji od skupa knjiga kojima su propisane upute za pružanje kvalitetnih informatičkih usluga i procedurama, opremi i aktivnostima koje omogućuju kvalitetnu informatičku podršku. Organiziran kao skup knjiga, ITIL predstavlja repozitorij najbolje prakse u pružanju, podršci, isporuci i upravljanju informatičkim uslugama. Osim toga, ITIL pruža vrlo precizne upute i smjernice kako procijeniti kvalitetu usluge, kako kontrolirati isporuku usluge i, u konačnici, kako upravljati cjelokupnom informatičkom uslugom. Vrlo je korisna mogućnost što se za svaki proces, odnosno uslugu može procijeniti usklađenost s ITIL preporukama, čime se ocjenama od 0 do 5 (kao u CobiT-u) procjenjuje zrelost načina njezina korištenja, što, u konačnici, omogućuje da se procjenjuje kvaliteta cjelokupne informatičke usluge, podrške i upravljanja.

ITIL je osobito korišten u Europi, najčešće u javnom sektoru (za čije je potrebe i nastao). Jedini trenutno važeći 'standard' za upravljanje informatičkim uslugama jest ISO 20000 (ili njegov ekvivalent BS 15000) koji je gotovo u potpunosti preuzeo svu ITIL terminologiju i djelokrug, stoga se sam ITIL ne može smatrati standardom, no, budući da je ISO 20000, jedini važeći standard za upravljanje informatičkim uslugama, potpuno preuzeo svu ITIL terminologiju, ITIL smatramo 'de facto' standardom.

Prva verzija ITIL-a nastala je 1986., sadržavala je ukupno 40 knjiga u kojima su se opisivale razne prakse i preporuke korištenja informatike i vrijedila je sve do 1999. godine. Druga verzija ITIL-a se sastojala od 8 knjiga od kojih su dvije bile najčešće korištene: **Podrška uslugama** (engl. *Service Support*) i **Isporuka usluge** (engl. *Service Delivery*).

Trenutno važeća, treća verzija ITIL-a koja je izašla sredinom 2007. sadrži 5 knjiga, odnosno 5 ključnih procesa: strategija usluga (engl. service strategy), oblikovanje usluga (engl. service design), isporuka usluge (engl. service transition), korištenje usluge (engl. service operation) i stalno unaprjeđenje usluge (engl. continual service improvement).

ITIL v3 je procesno orijentirani okvir koji je dodatno usklađen s ostalim okvirima (npr. CobiT), normama (ISO/IEC 20000) i regulatornim zahtjevima (Sarbanes-Oxley, Basel II).

4.3. ISO 17799 i ISO 27001 norma

ISO/IEC 17799:2005 i ISO/IEC 27001:2005 norma predstavlja minimalne zahtjeve i mjere koje organizacija treba poduzeti da bi se uspostavio sustav upravljanja sigurnošću informacija (engl. information security management system - ISMS). Radi se o normi koja je usko fokusirana na sigurnost informacija, a njezina je primjena u području revizije informacijskih sustava česta. To su jedine službene informatičke norme koje unutar 10 područja sadrže preko 100 preporučenih kontrola kojima bi se informacijski sustav i informacije koje nastaju njegovim funkcioniranjem trebale smatrati sigurnima i pouzdanima, no nisu određene i upute kako ih primijeniti u praksi. One propisuju minimalne kontrolne zahtjeve, odnosno minimalni skup kontrola koje je unutar informacijskog sustava potrebno implementirati kako bi se smanjio sigurnosni rizik njihove primjene. ISO 17799 i ISO 27001 predstavljaju

preporuke, odnosno nabraja koje je sve kontrole potrebno (moguće) implementirati kako bi se prije svega sigurnosni rizik sveo na primjerenu razinu. Te su norme vrlo popularne i često korištene, a njihova implementacija omogućuje ostvarenje najvažnijih ciljeva procesa internih kontrola informacijskih sustava (sigurnosni ciljevi, informacijski ciljevi, ciljevi kontinuiteta poslovanja itd.). S obzirom na uočene nedostatke prošlih normi i porast važnosti upravljanja informatikom, ISO je najavio i, već djelomice proveo temeljitu reorganizaciju ovih normi i postupno uvođenje cijelog niza novih iz tzv. ISO 27000 obitelji. Neke od njih već su aktualne i popularne (ISO 27001:2005), a druge, kao što su ISO 27002, ISO 27003, ISO 27004, ISO 27005, su nove norme koje bi, osim sigurnosti, temeljito trebale pokriti i područja upravljanja informatičkim rizicima i provedbe mehanizama kontrole nad informacijskim sustavima u svrhu ostvarivanja sigurnosnih i drugih rizika i time biti primjerenije konceptu upravljanja informatikom na korporativnoj razini.

4.4. Izvještaj revizora informacijskih sustava

Rezultat analize i revizije informacijskog sustava jest **mišljenje (procjena) o zrelosti (kvalitete) ključnih poslovnih ili informatičkih procesa** uz **obvezne preporuke** menadžmentu kako poboljšati poslovnu praksu u promatranom području (primjerice, kako bolje iskoristiti informacijsku infrastrukturu, gdje i u koja područja ulagati, kako poboljšati kontrole unutar informacijskog sustava itd.).

Mišljenje se iskazuje izvještajem revizora informacijskih sustava. Taj se izvještaj temelji na provjerama i pregledima (testovima) koje revizor informacijskog sustava treba provesti kako bi ispunio cilj revizije i obuhvatio njezin djelokrug. Revizor je dužan naručitelja upoznati s metodologijom provedbe revizije (CobiT, ISO 27001, ITIL) i prema svojoj stručnoj prosudbi odabrati one ciljeve kontrola koji omogućuju ostvarenje cilja revizije. Izvještaj revizora informacijskog sustava sastoji se od sljedećih dijelova:

- pismo namjere upravi i izvršnom menadžmentu naručitelja
- objašnjenje metodologije, njihovih ograničenja i djelokruga revizije
- klasifikacija rizika prema važnosti i utjecaju na poslovanje, objašnjenje što koja kategorija znači i kakve su obveze menadžmenta po tom pitanju
- nalazi, objašnjenje rizika, mišljenje o zrelosti informatičkih procesa i preporuke za poboljšanje prema područjima revizije (odabrane kontrole unutar nekih od već objašnjenih metodologija provedbe revizije informacijskih sustava). Primjer strukture ovog dijela izvještaja revizora informacijskog sustava prikazan je u tablici 1.

Ovisno o cilju i predmetu revizije, revizor informacijskog sustava odabire metode ili okvire prema kojima se provode aktivnosti testiranja i provjere. Nakon odabira područja revizije, za svako od njih revizor je dužan procijeniti trenutno stanje (i, naravno, temeljiti ga na dokazima, rezultatima testova i provjera), procijeniti razinu rizika, opisati na koji je način cjelokupno poslovanje izloženo rizicima i dati preporuke menadžmentu za poboljšanje zatečenog stanja.

Menadžment je dužan promotriti izvješće revizora informacijskih sustava i dati odgovarajuće objašnjenje u vezi s uočenim nedostatcima. Preporuke koje je revizor informacijskoj sustava istaknuo u svojemu izvješću nisu obvezne, ali svakako su dobrodošle, pa će ih savjesni menadžeri uzeti u obzir i, u razgovoru s revizorima i ostalim članovima menadžerskog tima, provesti određene aktivnosti kojima će se razina rizika svesti na prihvatljivu razinu.

Tablica 1. Primjer strukture izvještaja revizora informacijskog sustava:

Područje revizije: Strateški plan informatike

Razina rizika: Visok (kritičan utjecaj na poslovanje, nema korektivnih kontrola, menadžment treba hitno poduzeti određene aktivnosti)

Nalazi:

Provedbom razgovora s višim razinama menadžmenta i uvidom u poslovnu dokumentaciju ustanovljeno je da strateški plan informatike formalno ne postoji. Postoje određene neformalne i ad hoc procedure planiranja resursa koje informatika kao poslovna funkcija koristi, ali te su aktivnosti stihijske i neusklađene s potrebama poslovanja.

Ocjena rizika:

Informatika se ne razvija u skladu s potrebama poslovanja i potrebama ostvarenja poslovnih ciljeva. Ne postoji poveznica između poslovanja i informatike, nisu određeni ključni ciljevi i zadatci funkcioniranja informatike kao poslovne funkcije.

Preporuke menadžmentu:

Uprava treba dokumentirati kratkoročne i dugoročne razvojne planove informatike kao poslovne funkcije. Ti se planovi donose procesom strateškog planiranja informacijskih sustava kojim se iz poslovnih ciljeva određuje strategija informacijskog sustava, njegova uloga, ciljevi korištenja u poslovanju i poželjna arhitektura. Potrebno je ustrojiti posebno korporativno tijelo (odbor za korporativno upravljanje informatikom), kao savjetodavno tijelo menadžmenta, koje bi na najvišoj hijerarhijskoj razini donosilo ključne (strateške) informatičke odluke i nadziralo njihovu provedbu.

5. REZULTATI ISTRAŽIVANJA O KORIŠTENJU METODA REVIZIJE INFORMACIJSKIH SUSTAVA

Anketni je upitnik sadržavao 15 pitanja iz područja provedbe kontrole i revizije informacijskih sustava. Upitnik se distribuirao elektroničkom poštom, a uzorak istraživanja bio je popis informacijama o 500 najvećih tvrtki u Republici Hrvatskoj iz 2005. koju je ustupila Hrvatska udruga menadžera CROMA. Anketa je poslana na oko 250 adresa elektroničke pošte direktora informatike s popisa najvećih tvrtki, a vratila su se (samo) 32 korektno ispunjena upitnika. Time je stopa odgovora iznosila oko 13%, što je na granici statističke prihvatljivosti, pa se i rezultati mogu smatrati preliminarnima. Svi vraćeni upitnici bili su korektno ispunjeni što se može smatrati prilično zadovoljavajućim s obzirom na osjetljivost teme (izloženost rizicima radi primjene informacijske tehnologije i kontrolni mehanizmi, odnosno mehanizmi provedbe revizije informacijskih sustava).

Naime, istraživanja u ovom području su prilično rijetka i teška za provedbu, ne samo iz razloga što se radi o osjetljivim temama o kojima menadžment ne voli previše razgovarati niti iznositi bilo kakve podatke u javnost nego i poradi činjenice da se radi o prilično

'svježim' i novim konceptima koji možda još uvijek nisu u potpunosti 'zaživjeli' u menadžerskoj praksi. Neka pitanja su u nekim upitnicima ostala neispunjena, što se može opravdati osjetljivošću teme, eventualnom slučajnom pogrješkom ili ostalim razlozima (primjerice, nedostupnošću informacija ili nedovoljnim poznavanjem teme da bi se dao primjeren odgovor).

Revizija informacijskih sustava kao organizacijska funkcija provodi se preko posebne organizacijske jedinice, najčešće pod izravnim nadzorom najvišeg menadžmenta. Najčešće se radi o odjelu ili službi kontrole i revizije informacijskih sustava. Preliminarni rezultati istraživanja pokazuju da u 36,67% kompanija takva posebna organizacijska jedinica postoji, dok u 60% slučajeva izostaju sustavni organizacijski napori o tom pitanju.

U kompanijama u kojima postoji posebna organizacijska jedinica zadužena za kontrolu i reviziju informacijskih sustava, ona se najčešće nalazi unutar odjela/sektora revizije (u 45% slučajeva), a u 36% slučajeva u odjelu/sektoru informatike. Organizacijska pozicija službe revizije informacijskih sustava može imati veliki utjecaj na njezinu efikasnost i učinkovitost. Ako se služba revizije informacijskih sustava nalazi unutar odjela/sektora informatike, to većinom znači niži položaj u organizacijskoj hijerarhiji, ali i dostupnost često oskudnih znanja iz toga područja. Ako se služba revizije informacijskih sustava nalazi unutar odjela/sektora revizije, njen organizacijski položaj je uglavnom bolji, ali s obzirom na nedostatak informatičkih znanja, njena je efikasnost dvojbena. Naime, obavljanje revizije informacijskih sustava često zahtijeva usko specijalizirana informatička znanja kakva revizori uglavnom nemaju, stoga se i među revizorima treba očekivati uža specijalizacija, odnosno stalno stjecanje informatičkih znanja, vještina, tehnika kako bi se revizija informacijskih sustava mogla obavljati učinkovito.

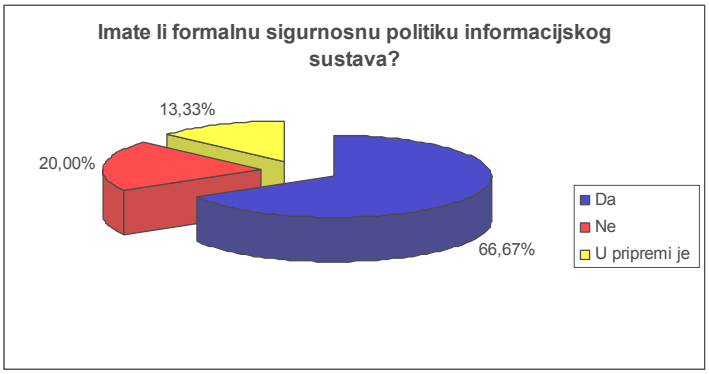
Anketirane hrvatske kompanije i dalje **nedovoljan dio ukupnog godišnjeg prihoda izdvajaju za informatiku** (37 % poduzeća izdvaja manje od 2 % ukupnog godišnjeg prihoda, 30 % do 5 %, a preostalih 33 % izdvaja više od 5% ukupnog godišnjeg prihoda za informatiku), pri čemu se ipak uočavaju pozitivni trendovi u odnosu na ranija usporediva istraživanja. Struktura ulaganja i dalje je nepovoljna, jer se najveći iznosi troše na opremu (hardver). Isplativost ulaganja u informatiku najčešće procjenjuje najviši menadžment (49%), no nisu zanemarive pojave u kojoj to ne obavlja **nitko** (16% slučajeva). Metode koje se koriste pri procjeni ulaganja u informatiku najčešće su analiza troškova i koristi, studija izvedivosti, stopa povrata na ulaganje (ROI).

Slika 4 prikazuje stanje o pitanju formalne sigurnosne politike informacijskog sustava na uzorku anketiranih kompanija. Vidljivo je da gotovo dvije trećine kompanija ima taj gotovo ključni formalni dokument sa stajališta sigurnosti informacijskog sustava, što je svakako ohrabrujući podatak koji oslikava, pretpostavljamo, raširenu svijest o potrebi sustavne kontrole i zaštite vitalnih dijelova i funkcija informacijskog sustava.

Osim činjenice da kompanija posjeduje formalnu sigurnosnu politiku informacijskog sustava, od velike je važnosti i njezina praktična provedba u svakodnevnom poslovanju. Slijedi niz rezultata koji prikazuju određene poteškoće pri praktičnoj provedbi pojedinih dijelova sigurnosne politike informacijskog sustava. Primjerice, 55.17% anketiranih tvrtki ima interni pravilnik o uporabi informacijskog sustava, ali samo trećina njih redovito provodi postupke interne kontrole i revizije informacijskog sustava, što je gotovo u izravnoj koliziji.

S obzirom da više od tri četvrtine anketiranih kompanija koristi vlastitu metodologiju kontrole i revizije informacijskih sustava, postavlja se pitanje njene usklađenosti sa svjetski prihvaćenim metodologijama u ovoj djelatnosti, pri čemu se samo može pretpostavljati na čemu se vlastita metodologija temelji i kakve praktične rezultate daje u svojoj provedbi.

Slika 4. Postoji li formalna sigurnosna politika informacijskog sustava?

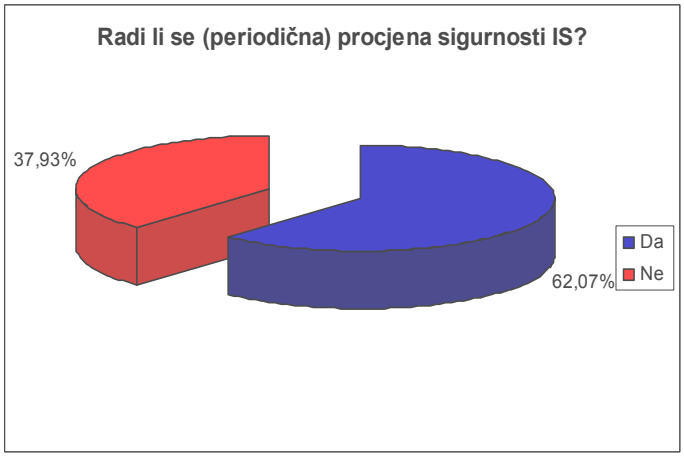


Tablica 2. Koju metodologiju koristite pri aktivnostima kontrole i revizije IS?

Koju metodologiju koristite pri aktivnostima kontrole i revizije IS?	%
Vlastita metodologija	76.47%
COBIT metodologija	11.76%
ISO 17799 / BS 7799	5.88%
ostale (metodologija revizorske kuće)	5.88%

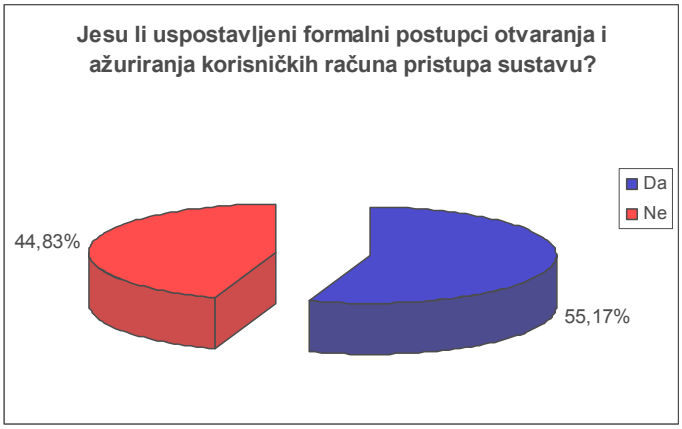
Slika 5 prikazuje da oko 62% anketiranih kompanija periodično procjenjuje razinu sigurnosti informacijskog sustava, dok u oko 48% anketiranih kompanija postoje (periodična) izvješća višim razinama menadžmenta o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim nedopuštenim (neželjenim) aktivnostima koja je prepoznao kontrolni sustav.

Slika 5. Postoje li periodična izvješća o slučajevima povrede sigurnosti, nedopuštenim pokušajima pristupa sustavu i ostalim nedopuštenim (neželjenim) aktivnostima?



Slika 6 prikazuje da su u 55% slučajeva anketirane kompanije svjesne važnosti i sustavne brige oko uspostavljanja formalnih postupaka za otvaranje, ukidanje i održavanje korisničkih računa čime se znatno poboljšavaju kontrole pristupa sustavu i utječe na povećanu sigurnost njegova rada. Dobra poslovna praksa o tom pitanju uključuje formalno potpisivanje ugovora pri otvaranju korisničkih računa pristupa sustavu s točno određenim ovlastima pristupa, popisom funkcija koje su korisniku dozvoljene pri radu sa sustavom (primjerice, koje podatke smije pregledavati, a koje mijenjati ili brisati, odnosno kojim dijelovima transakcijskog sustava korisnik može pristupati i s kojim ovlastima itd.) i precizno propisanom procedurom pri zatvaranju računa (u situacijama kada korisnik odlazi iz kompanije, mijenja svoje radno mjesto ili slično).

Slika 6. Formalni postupci otvaranja i održavanja korisničkih računa

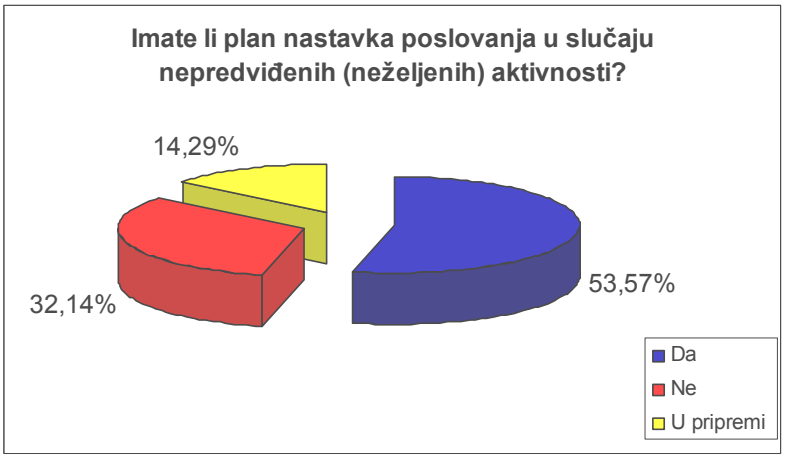


U svakodnevnom poslovanju relativno je česta potreba promjene nekih dijelova transakcijskog informacijskog sustava, odnosno njegova aplikacijskog softvera. U poslovnoj praksi anketiranih kompanija primjećujemo da u oko 45% slučajeva postoji razrađena i formalnim procedurama propisana aktivnost promjene aplikacijskog softvera, pri čemu tablica 3 prikazuje tko je nakon provedenih promjena odgovoran za testiranje njihove djelotvornosti, točnosti i funkcionalnosti. Iz navedene tablice je vidljivo da ključni korisnici nisu u najvećoj mjeri uključeni u aktivnosti kontrole promjena programskog koda dijela informacijskog sustava koji upravlja poslovnim procesima za koje su ti ključni korisnici odgovorni, što, svakako, nije dobra poslovna praksa.

Tablica 3. Tko je odgovoran za testiranje promjena programskog koda?

Tko odobrava (provjerava) kontrole ugrađene u aplikacijski softver i tko je odgovoran za testiranje promjena programskog koda?	**%**
Projektanti / programeri	41%
Ključni korisnici (neposredno odgovorni za odvijanje poslovnih procesa koji su se informatizirali)	26%
Tim / radna skupina sastavljen(a) od informatičara i ključnih korisnika	19%
(Interna) revizija i kontrola	10%
Netko drugi (programer, voditelj projekta i ključni korisnik, a u drugom slučaju: ovisno o situaciji – programer, ali ponekad i help-desk?!)	10%

Slika 7. Imate li plan nastavka poslovanja i ponovnog podizanja informacijskog sustava u slučaju nepredviđenih (neželjenih)aktivnosti (engl. disaster recovery plan i business continuity plan)?



Rezultati ovoga dijela istraživanja pokazuju stoga da je, kako to obično biva, lako formalno propisati postupke sigurnosne politike informacijskog sustava, no dosta je teže, a i zahtjevnije inzistirati na njihovoj sustavnoj provedbi u svakodnevnom poslovanju. Iz ovih rezultata vidljivo je da, osim postojanja formalne sigurnosne politike, ipak **više pozornosti treba posvetiti njezinoj provedbi** u svakodnevnom poslovanju kako bi se informacijski resursi poslovanja štitili ili koristili na učinkovit način. U tu je svrhu kompanijama koristan i **plan nastavka poslovanja** (engl. business continuity plan) i ponovnog podizanja, odnosno **oporavka informacijskog sustava u slučaju nepredviđenih (neželjenih) aktivnosti** (engl. disaster recovery plan) kojega posjeduje oko 53% anketiranih kompanija.

Proces **upravljanja kontinuitetom poslovanja** (engl. business continuity) predstavlja skup aktivnosti, radnih procedura i pravila prema kojima se preventivnim mjerama sprječava pojava neželjenih štetnih događaja, ali i skup reaktivnih mjera prema kojima se postupa u slučaju njihova nastanka. Tim se procesom angažiraju razni poslovni resursi (ljudski, materijalni) kako bi se omogućila neprekidnost poslovanja i smanjio operativni rizik koji proizlazi iz neočekivanih prekida kritičnih poslovnih funkcija i procesa ili njihova otežanog funkcioniranja. **Osnovna svrha i cilj procesa upravljanja kontinuitetom poslovanja** jest omogućiti neometan nastavak poslovanja u slučaju bilo kakvog štetnog događaja, ispada ili otežanog rada informacijskog sustava. Drugi važan cilj procesa upravljanja kontinuitetom poslovanja jest omogućiti brz i efikasan **oporavak i ponovno pokretanje poslovanja nakon štetnog događaja** (engl. disaster recovery). Osim reaktivnih mjera prema kojima se postupa u slučaju nastanka neželjenog štetnog događaja, osnovni smisao procesa upravljanja kontinuitetom poslovanja jest ustrojiti i preventivne mjere kojima će se spriječiti njihov nastanak ili smanjiti vjerojatnost takvog ishoda.

Rizik prekida kontinuiteta poslovanja spada među vrlo važne poslovne (upravljačke) rizike kojima su izložene gotovo sve kompanije koje za odvijanje poslovnih procesa koriste informacijske sustave. Obveza (iako još uvijek nije formalno prisutna i u hrvatskoj regulativi) je najviših tijela upravljanja kompanijom ustrojiti mehanizme upravljanja kontinuitetom poslovanja, utvrditi potencijalne štetne i neželjene događaje koji mogu uzrokovati

prekide poslovnih procesa ili njihovo otežano odvijanje i odrediti protumjere (kontrole, organizacijske mjere, korporacijska pravila) kako bi se njihov utjecaj smanjio ili ublažio.

6. UMJESTO ZAKLJUČKA - REVIZIJA INFORMACIJSKIH SUSTAVA KAO KOMPONENTA KORPORATIVNOG UPRAVLJANJA INFORMATIKOM

Revizija informacijskih sustava je u vrlo kratkom razdoblju prošla dinamičan razvojni put. Osim svoje izvorne uloge kao nezaobilazne podrške reviziji financijskih izvještaja, revizija informacijskih sustava danas sve češće predstavlja nezaobilaznu 'analitičku' kariku procesa korporativnog upravljanja informatikom i 'most' između menadžmenta i informatike. Ona se, naime, odnosi na sustavan postupak kojim se ocjenjuje djeluje li informatika u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama. Konačan rezultat tih postupaka jest *izvještaj revizora informacijskog sustava* koji se, prema područjima analize (temeljene na CobiT ili ITIL okviru ili ISO 27001 normi), sastoji od sljedećih koraka:

- analiza stanja (zrelosti) primjene informacijskih sustava u poslovanju prema promatranim područjima
- procjena poslovnih rizika koji proizlaze iz zatečenog stanja i
- preporuke menadžmentu za poboljšanjem toga stanja.

U današnje vrijeme revizija informacijskih sustava predstavlja važnu komponentu koncepta korporativnog upravljanja informatikom. **Korporativno upravljanje informatikom (engl. IT Governance)** se odnosi na okvir kojim korporativna razina upravljanja (uprava, nadzorni odbor) 'ovladava' primjenom informatike u poslovanju, odlukama o ulaganjima u informatiku, performansama i rizicima njezina korištenja, ali i preuzima odgovornost za kontrolu provedbe informatičkih procesa i svih aktivnosti. Time se sintagma informatike kao 'tehničke' struke nepovratno gubi, a moderne metode i okviri revizije informacijskih sustava (CobiT, ITIL, ISO norme, i drugi koji nisu obrađeni u ovom radu) menadžerima pružaju nužan 'aparat' za upravljanje informatikom kao bilo kojom drugom poslovnom funkcijom. To se osobito odnosi na CobiT, krovni okvir provedbe revizije informacijskih sustava, ali i korporativnog upravljanja informatikom koji svojim metrikama i upravljačkim alatima (procesni pristup, modeli zrelosti, ključni pokazatelji performansi, ključni pokazatelji ostvarenja ciljeva, RACI matrice obveza i odgovornosti, kontrolni ciljevi itd.) upućenim menadžerima nudi cjelovitu metodu korporativnog upravljanja informatikom.

U hrvatskim kompanijama revizija informacijskih sustava se mahom koristi radi regulatornih obveza, a u rijetkim (redom uspješnim) primjerima radi se o aktivnostima usmjerenima ostvarenju poslovnih ciljeva. Osim toga, iako pojedini ključni dokumenti nužni za učinkovito upravljanje informatičkih rizika postoje (pravilnik o sigurnosti informacijskih sustava), njihova provedba ipak i dalje nije zadovoljavajuća. Međutim, ohrabrujuće je da kod menadžera sve više raste svijest o potrebi učinkovita upravljanja informatičkim rizicima, što reviziju informacijskih sustava čini posebno zanimljivom i traženom samostalnom uslugom.

LITERATURA

1. Champlain, J.J. (2003.): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.
2. Ernst & Young (2006.): Achieving Success in a Globalized World – Is Your Way Secure?, 2006 Global Information Security Survey.
3. Hunton, J.E., Bryant, S.M., Bagranoff, N.A.: (2004.): Core Concepts of Information Technllogy Auditing, John Wiley &Sons Inc., SAD.
4. International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005.
5. ITGI (2007.), CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, IT Governance Institute, Rolling Meadows, SAD.
6. Nolan, R. and McFarlan, F.W., (2005.): Information Technology and Board of Directors, Harvard Business Review, October, 2005.
7. Panian, Ž., Kontrola i revizija informacijskih sustava, Sinergija, Zagreb, 2001.
8. Spremić, M. (2005.): Procjena razine pouzdanosti internih kontrola informacijskog sustava s pomoću CobiT metodologije, Revizija, računovodstvo i financije, br. 12/2005, str. 126-134.
9. Spremić, M., Strugar, I., (2002.): Strategic Information System Planning in Croatia: Organizational and Managerial Challenges, *International Journal of Accounting Information Systems*, Vol. 3, Num. 3, pp. 183-200.
10. Spremić, M. (2005.): Managing IT risks by implementing information system audit function, Proceedings of the 3rd International Workshop in Wireless Security Technologies, Westminster University, London, 04-05.04.2005, pp. 58-64.
11. Srića, V., Spremić, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.
12. Symons, C., (2005.): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.
13. Weill, P., Ross, J.W., IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvards Business School Press, 2004.