

ANALIZA KONCEPTA REVIZIJE INFORMACIONIH SISTEMA PREMA COBIT METODOLOGIJI

Milovan Stanišić

Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: mstanisic@singidunum.ac.rs

Dalibor Radovanović

Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: dradovanovic@singidunum.ac.rs

Dubravka Lučić

Ernst & Young Beograd d.o.o.
Bulevar Mihajla Pupina 115d, Beograd, Srbija
E-mail: dubravka.lucic@yu.ey.com

Sažetak

U ovom radu se objašnjava koncept revizije informacionih sistema, koji predstavlja proces prikupljanja i procene dokaza na osnovu kojih se može proceniti uspešnost informacionog sistema. Potrebno je odrediti da li je funkcionisanje informacionog sistema u funkciji očuvanja imovine i održavanja integriteta podataka. Revizija informacionih sistema se nameće kao imperativ uspešnog poslovanja. Jedna od metodologija za reviziju informacionih sistema je COBIT, koji daje uputstva o tome šta može biti urađeno u jednoj organizaciji u pogledu kontrole, aktivnosti, merenja i dokumentacije procesa i poslovanja.

Ključne reči: IT revizija, korporativno upravljanje informacionim tehnologijama, Cobit.

Abstract

This paper explains the concept of information systems audit, which is the process of gathering and evaluating evidence based on which one can evaluate the performance of IT systems. It is necessary to determine whether the operation of information systems in the function of preserving the property and maintain data integrity. Revision information system is imposed as an imperative for successful business. One of the methodologies for auditing information systems is COBIT, which provides guidelines on what can be done in an organization in terms of control activities, measurement and documentation of processes and operations.

Key words: IT audit, IT governance, Cobit.

1. UVOD

Kritičan element važan za opstanak i uspeh organizacije je efikasno upravljanje informaciono komunikacionom tehnologijom (IKT), koji se ogleda u povećanju zavisnosti od informacija i njima pridruženih sistema, odnosno povećanju ranjivosti i širokom spektru pretnji IKT tehnologiji.

Revizija informacionih sistema (*engl. Information system audit*) predstavlja proces prikupljanja i procene dokaza na osnovu kojih se može proceniti uspešnost informacionog

sistema, odnosno odrediti da li je funkcionisanje informacionog sistema u funkciji očuvanja imovine i održavanja integriteta podataka. Takođe je potrebno odrediti da li informacioni sistem omogućuje delotvorno ostvarivanje ciljeva poslovanja i koriste li se resursi sistema na efektivan i efikasan način. Revizija informacionih sistema, osim egzaktne i analitičke funkcije, danas predstavlja i modernu savetodavnu funkciju, "desnu ruku" koja menadžmentu pomaže pri korporativnom upravljanju informacionom tehnologijom (*engl. IT Governance*) [1.]. Takođe, predstavlja postupak kojim se ocenjuje da li informatika deluje u skladu sa poslovnim ciljevima, u kojoj meri delotvorno i efikasno podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacionih sistema na raznim hijerarhijskim nivoima. Postoji više metodologija i standarda koji se bave ovom problematikom: Cobit, ITIL, COSO, ISO 17799, ISO 9000.

2. COBIT

Cobit je svetski prihvaćen standard u kojem se propisuju područja i pojedinačne kontrole za korporativno upravljanje informatikom i pripadajućim informatičkim procesima. Autori Cobit okvira su neprofitne organizacije ISACA i ITGI. On spaja poslovne i informatičke ciljeve, pružajući mogućnost da se metrički prati zrelost informacionog sistema. Cobit daje menadžmentu mogućnost optimizacije informatičkih resursa kao što su aplikacije, informacije, infrastruktura i ljudi. Uputstva koja pruža Cobit su produkt konsenzusa znanja mnogih stručnjaka i proizvod je dobre prakse, primenjive u bilo kojoj organizaciji.

Cobit se sastoji od 34 ključna poslovna kontrolna procesa i za svaki proces opisuje model zrelosti. Sadrži preko 300 detaljnih informatičkih kontrola. Primarni kontrolni ciljevi podeljeni su u četiri domena:

- **Planiranje i organizacija** (*engl. Planning and Organization, PO*), uključuje procese za planiranje i dizajn organizacije namenjene postizanju poslovnih ciljeva organizacije. Ovaj domen obuhvata i procenu rizika.
- **Nabavka i implementacija** (*engl. Acquisition and Implementation, AI*), uključuje procese koji se odnose na nabavku i razvoj IT rešenja i upravljanje promenama tih rešenja tokom vremena.
- **Isporučka i podrška** (*engl. Delivery and Support, DS*), uključuje procese koji se odnose na aktuelne isporuke IT usluga organizaciji. Ovaj domen uključuje procese za upravljanje problemima i incidentima, upravljanje sigurnošću, i druge procese koji se odnose na izvršavanje IT.
- **Nadzor i procena uspešnosti** (*engl. Monitoring and Evaluation, ME*), uključuje procese za regularnu proveru IT procesa i njihove uspešnosti u postizanju relativnih ciljeva IT kontrola.

Za svaki od ključnih poslovnih i IT procesa Cobit definiše i nudi [7.]:

- modele zrelosti (*engl. maturity models*),
- kritične faktore uspeha (*CSF, engl. Critical Success Factors*),
- ključne indikatore ostvarenja cilja (*KGI, engl. Key Goal Indicators*),
- smernice menadžmentu za praćenje performansi i ključne indikatore performansi (*KPI, engl. Key Performance Indicators*),
- smernice menadžmentu za upravljanje rizicima (tzv. RACI Chart),
- ciljeve kontrole i kontrolne testove.

RACI matrica predstavljaju matricu kojom se za svaki od procesa i aktivnosti određuju odgovornosti i ovlašćenja, i služe kao smernice menadžmentu za upravljanje rizicima. Na slici 1 prikazana je RACI matrica za poslovni proces PO4, iz domena planiranja i organizacije, koji definiše IT procese, uloge i odgovornosti u okviru organizacije. Za svaku aktivnost u okviru ove matrice definisano ko je u organizaciji odgovoran (engl. **Responsible**), ovlašćen (engl. **Accountable**), a koga treba samo konsultovati (engl. **Consulted**) i informisati (engl. **Informed**) za posmatrane aktivnosti.

Aktivnosti	Funkcije										
	Generalni direktor (CEO)	Finansijski direktor (CFO)	Izvršni direktor	Šef informatike	Vlasnik poslovnog procesa	Glavni rukovodilac	Glavni arhitekta IS	Rukovodilac razvoja	Rukovodilac IT administracije	Usklađenost, revizija, rizik i bezbednost	
Uspostaviti IT organizacionu strukturu.	C	C	C	A		C	C	C	R	C	I
Dizajn okvira IT procesa	C	C	C	A		C	C	C	R	C	C
Identifikovanje vlasnika sistema.		C	C	A	C	R	I	I	I	I	I
Identifikovanje vlasnika podataka.		I	A	C	C	I	R	I	I	I	C
Uspostaviti i implementirati IT uloge i odgovornosti, uključujući nadzor i segregaciju dužnosti.		I	I	A	I	C	C	C	R	C	C

Slika 1. RACI matrica P04 – Definisane IT procesa, organizacije i odnosa

Upućenom menadžmentu i korporativnim strukturama lako je pomoću Cobit metode utvrditi koji su od tih procesa i u kojoj meri važni. Sa stanovišta kontrole i revizije informacionih sistema Cobit određuje i 18 aplikativnih i 6 procesnih kontrola.

Ocene zrelosti su zasnovane na poznatom CMM modelu (*SEI Software Engineering Institute je izradio model zrelosti i kvalitete softvera kojega je nazvao CMM - Capability Maturity Model*), samo što su u Cobit modelu ocene vrlo detaljno opisane i objašnjene za svaki proces. Ocene zrelosti procesa upravljanja informatikom na korporativnom nivou su u rasponu od 0 do 5 [2.]:

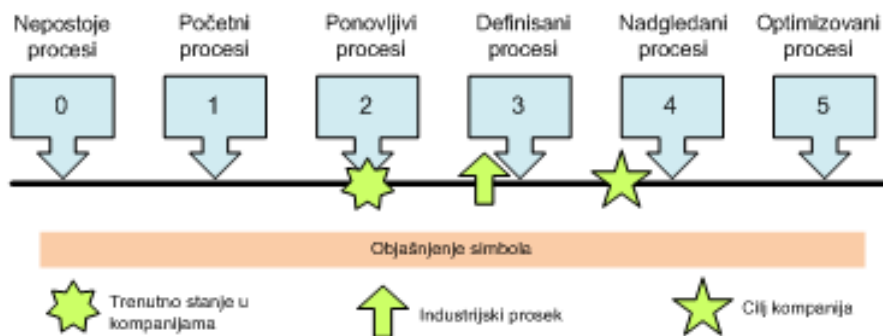
- **0 – Ne postoje procesi;** Proces upravljanja informatikom na korporativnom nivou ne postoji. Menadžment nije prepoznao važnost tog koncepta, odluke o ulaganjima u informatiku su stihijske, od slučaja do slučaja ('ad-hoc'), van sistemskog nadzora i procene rizika i potpuno su u rukama pojedinaca.
- **1 – Početni procesi;** Menadžment nije svestan važnosti upravljanja informatikom, iako nema nikakvih formalnih procedura, upravljanje i nadzor informatike se uglavnom zasniva na pojedinačnoj, stihijskoj bazi, a postupanje u tim prilikama je od slučaja do slučaja. Ne postoje standardi, niti korporativna pravila, nikakve obaveze i odgovornosti po tom pitanju, ne koriste se nikakva uputstva. Menadžment uglavnom

uopšte nije svestan važnosti informatičkih rizika. Upravljanje informatikom i merenje njene uspešnosti su procesi koji se sprovode samo unutar odeljenja informatike, a menadžment je po tim pitanjima pasivan i uglavnom neupućen i neobrazovan.

- **2 – Ponovljivi procesi;** Procesi upravljanja informatikom postoje, ali su nekoordinisani i pokrenuti uglavnom od odeljenja informatike ili nekog drugog operativnog nivoa. Često se događa da veći broj ljudi obavlja iste zadatke, nema sistemskog nadzora, koordinacije, niti standardizovane procedure. Odgovornost je prepuštena pojedincima, politike na korporativnom nivou ne postoje ili nisu predstavljene zaposlenima.
- **3 – Definisani procesi;** Procedure upravljanja informatikom su propisane i dokumentovane i stalno se usavršavaju formalnim treninzima i edukacijom. Procedure i korporativna pravila, iako formalno postoje, nisu sofisticirane, zrele niti prilagođene poslovanju organizacije, nego uglavnom predstavljaju formalizovanje postojećih procedura. Iako procedure postoje, odgovornost za njeno izvršenje je na pojedincima, a obzirom da nema sistemskog nadzora, malo je verovatno da neko može otkriti anomalije po tom pitanju.
- **4 - Nadgledani procesi;** Osim što korporativne politike i procedure postoje, moguće je i stalno nadzirati njihovo izvršenje i meriti uspešnost, pa prema potrebi i preduzimati potrebne korekcije. Proces i aktivnosti se stalno unapređuju. Postavljaju se vrlo sofisticirani ciljevi upravljanja informatikom koji su usko usklađeni sa poslovnim U merenju uspešnosti i reviziji obavezno se koriste moderne metode i okviri (Cobit, IT BSC, ITIL).
- **5 – Optimizovani procesi;** Proces upravljanja informatikom su dovedeni na optimalan nivo, a kompanija je lider u tom području . Stalno se meri uspešnost i efikasnost informatike kao poslovne funkcije, a rezultati se upoređuju sa najboljom praksom i drugim organizacijama. Vlada potpuna transparentnost u upravljanju informatikom, korporativna tela imaju putem niza formalnih mehanizama stvarni nadzor nad informatikom. Informatika se koristi u strateške svrhe, kao ključan poslovni resurs, a informatičke aktivnosti (ulaganja, projekti, rizici,..) na optimalan se način odvijaju prema stvarnim poslovnim prioritetima.

Prilično je važno i bitno što najvažnije metode upravljanja i revizije informacionih sistema kao što su ITIL, Cobit i Sarbanes-Oxley koriste taj isti jednak raspon ocena zrelosti IT procesa i uspešnosti kontrola nad njima (od 0 do 5 uz ista objašnjenja), što proces revizije čini lakšim i transparentnijim.

Da bi rezultati ocene zrelosti procesa bili upotrebljivi menadžmentu na razumljiv način potrebno da prilikom prikazivanja upravljačkim strukturama organizacije budu grafički prikazani kao na slici 2. Na tako prikazan način menadžment u okviru kompanije, može lako uočiti stanje na kome se nalaze procesi u njihovoj kompaniji. Najbitnije je da mogu uočiti prosek ocena zrelosti u industrijskoj grani u kojoj se oni nalaze, i uporediti ga sa vlastitim. Menadžment kompanija može na takvom grafičkom prikazu videti u kom pravcu treba da nastavi sa unapređenjem procesa, tj. vidi cilj kome mora težiti.



Slika 2. Grafički prikaz ocena zrelosti procesa

Da bi zadovoljila poslovne ciljeve, informacija treba da bude u skladu sa određenim kontrolnim kriterijumima koji su u skladu sa Cobit okvirom i poslovnim potrebama za informacijama. Cobit okvir ističe sedam različitih kriterijuma informacije u odnosu na poslovne zahteve, i međusobno se preklapaju [2.]:

- **Delotvornost** – Informacija treba da bude relevantna i bitna za poslovni proces. Potrebno je da se isporučuju na vreme, tačno, konzistentno i na upotrebljiv način.
- **Efikasnost** – Informacija mora biti pružena putem optimalnog korišćenja resursa.
- **Poverljivost** – Osetljive informacije moraju biti zaštićene od neovlašćenog otkrivanja.
- **Integritet** – Informacija mora biti tačna, potpuna, i ispravna u skladu sa poslovnim vrednostima i očekivanjima.
- **Dostupnost** – Informacije moraju biti dostupne kada se to zahteva od poslovnih procesa, kako u sadašnjosti, tako i u budućnosti. Moraju se očuvati neophodni resursi.
- **Usklađenost** – Informacija mora biti u skladu sa zakonima, propisima i ugovornim aranžmanima koji su predmet poslovnih procesa, kao i sa unutrašnjim politikama.
- **Pouzdanost** – Odgovarajuće informacije moraju biti pružene menadžmentu za potrebe upravljanja i radi ostvarivanja poslovnih ciljeva.

Resursi informacione tehnologije koji su predmet kontrolnih aktivnosti su definisani kao ljudi, aplikacije, infrastruktura i informacije. Sumarno, IT resursima se upravlja preko IT procesa radi postizanja ciljeva koji odgovaraju poslovnim zahtevima organizacije.

3. COBIT KONTROLNI CILJEVI

Cobit metodologija je dosta korišćena u poslednjih nekoliko godina od strane velikog broja organizacija, odobrena je i testirana od strane stručnjaka širom sveta. U tabeli 1 su prikazani kontrolni ciljevi Cobit metodologije i informacioni kriterijumi koji podržavaju te kontrolne ciljeve. Cobit kontrolni ciljevi su namenjeni revizorima informacionih tehnologija, a za svaki kontrolni cilj definisana je važnost njegove primene, koja može biti velika, srednja ili mala [7.].

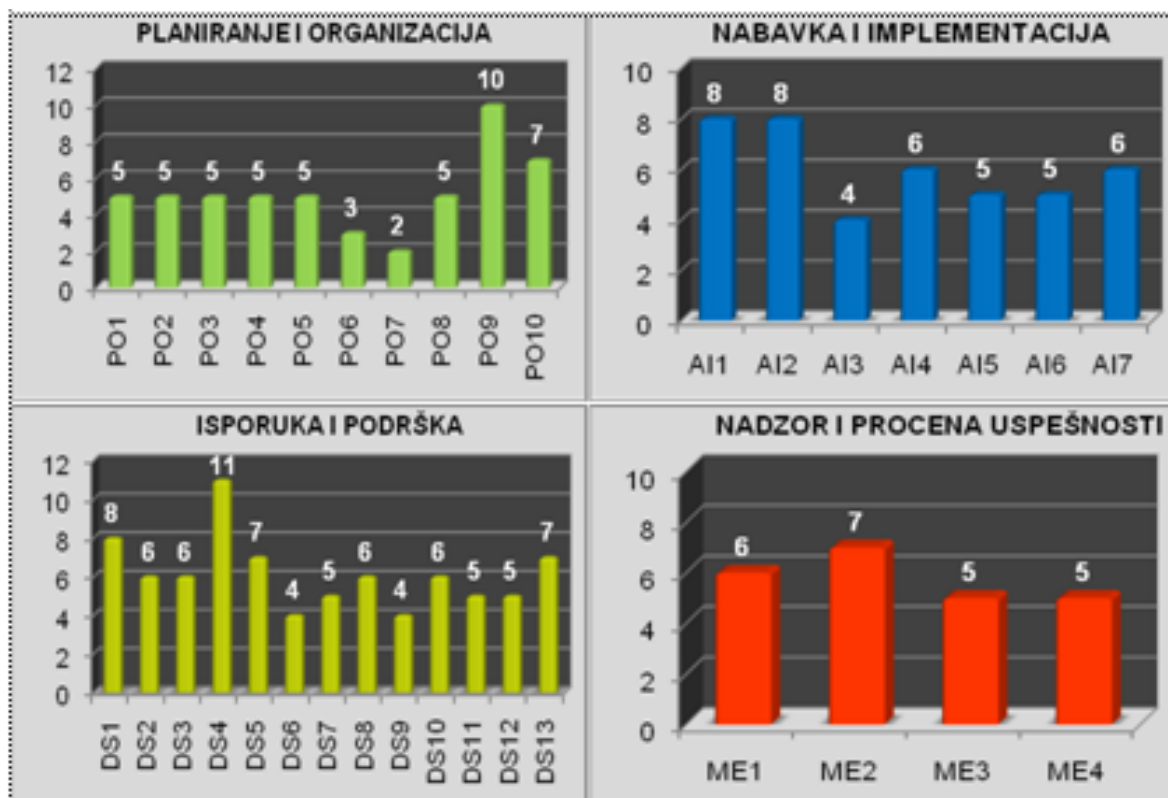
U tabeli 1 važnost svakog cilja je obeležena početnim slovom važnosti; velikim slovom M, S ili M. Za informacione kriterijume svakog cilja definiše se uloga, koja može biti primerna ili sekundarna, u zavisnosti koji je informacioni kriterijum najbitniji, a koji je manje bitan. Kontrolni ciljevi mogu imati više primarnih ili sekundarnih informacionih kriterijuma u okviru jednog cilja, a u tabeli su obeleženi početnim slovima uloge (važnosti), P ili S. Takođe, za svaki cilj su definisani i IT resursi potrebni za određeni cilj. Resursi mogu biti aplikacije, informacije, infrastruktura i ljudi. Ciljevima mogu biti dodeljeni svi resursi, kao što je slučaj

sa kontrolnim ciljem PO9, koji definiše upravljanje i procenu rizika, ili može biti dodeljen samo jedan resurs, kontrolni cilj PO7.

Tabela 1. Cobit kontrolni ciljevi

Cilj	COBIT KONTROLNICEVI	VAŽNOST	Informacioni i tehnološki							IT resursi			
			Deljivost	Ekivnost	Povjerenost	Integritet	Dostupnost	Usklađenost	Pouzdanost	Aplikacije	Informacije	Infrastruktura	Ljudi
PO - PLANIRANJE I ORGANIZACIJA													
PO1	Strateško planiranje IS	V	P	S						✓	✓	✓	✓
PO2	Definisanje informacione arhitekture	M	S	P	S	P				✓	✓		
PO3	Određivanje tehnoloških merica	S	P	P						✓		✓	
PO4	Definisanje IT procesa, organizacije i odnosa	M	P	P									✓
PO5	Upravljanje IT investicijama i troškovima	S	P	P					S	✓		✓	
PO6	Komuniciranje prema menadžmentu	S	P					S			✓		
PO7	Upravljanje ljudskim resursima	M	P	P									✓
PO8	Upravljanje kvalitetom	S	P	P		S			S	✓	✓	✓	✓
PO9	Upravljanje i procena rizika	V	S	S	P	P	P	S	S	✓	✓	✓	✓
PO10	Upravljanje projektima	V	P	P						✓		✓	
AI - NABAVKA I IMPLEMENTACIJA													
AI1	Određivanje mogućih rešenja	S	P	S						✓		✓	
AI2	Nabavka i održavanje aplikativnih programa	S	P	P		S			S	✓			
AI3	Nabavka i održavanje tehnološke arhitekture	M	S	P		S	S					✓	
AI4	Korišćenje i funkcionalnost rada (obrade)	M	P	P		S	S	S	S	✓		✓	✓
AI5	Nabavka IT resursa	S	S	P				S		✓	✓	✓	✓
AI6	Upravljanje promenama	V	P	P		P	P		S	✓	✓	✓	✓
AI7	Instalacija i odobranje rešenja i promena	S	P	S		S	S			✓	✓	✓	✓
DS - ISPORUKA I PODRŠKA													
DS1	Definisanje i upravljanje servisnim uslugama	S	P	P	S	S	S	S	S	✓	✓	✓	✓
DS2	Upravljanje spoljnim uslugama	M	P	P	S	S	S	S	S	✓	✓	✓	✓
DS3	Upravljanje performansama i kapacitetom	M	P	P			S			✓		✓	
DS4	Osiguranje kontinuiteta usluga	S	P	S			P			✓	✓	✓	✓
DS5	Sigurnost sistema	V			P	P	S	S	S	✓	✓	✓	✓
DS6	Određivanje i dodela troškova	M		P					P	✓	✓	✓	
DS7	Edukacija i obuka korisnika	M	P	S									✓
DS8	Podrška korisnicima	M	P	P						✓			
DS9	Upravljanje konfiguracijom	S	P	S			S		S	✓	✓	✓	✓
DS10	Upravljanje problemima i incidentima	S	P	P			S			✓	✓	✓	✓
DS11	Upravljanje podacima	V				P			P		✓		
DS12	Upravljanje pomoćnom opremom	M				P	P					✓	
DS13	Upravljanje operacijama (obradom)	M	P	P		S	S			✓	✓	✓	✓
ME - NADZOR I PROCENA USPEŠNOSTI													
ME1	Nadzor i procena IT performansi	V	P	P	S	S	S	S	S	✓	✓	✓	✓
ME2	Nadzor i procena internih kontrola	S	P	P	S	S	S	S	S	✓	✓	✓	✓
ME3	Usklađenost sa zakonskim i drugim normama	V						P	S	✓	✓	✓	✓
ME4	Korporativno upravljanje m IT-om	V	P	P	S	S	S	S	S	✓	✓	✓	✓

Svaki kontrolni cilj u okviru Cobit metodologije sastoji se iz više definisanih aktivnosti. Broj aktivnosti u okviru kontrolnih ciljeva nije konstantan.



Slika 3. Ukupan broj aktivnosti u okviru kontrolnih ciljeva Cobit metodologije

Postoji ukupno 197 definisanih aktivnosti u okviru četiri domena. Slika 3 prikazuje pojedinačan broj aktivnosti za svaki kontrolni cilj u okviru Cobit metodologije. Ukupan broj aktivnosti po domenima je:

- planiranje i organizacije – definisano 52 aktivnosti;
- nabavka i implementacija – definisano 42 aktivnosti;
- isporuka i podrška – definisano 80 aktivnosti;
- nadzor i procena uspešnosti – definisano 23 aktivnosti.

4. ZAKLJUČAK

Revizija informacionih sistema je u kratkom vremenskom periodu prošla kroz dinamičan razvojni put. Izvorna uloge joj je bila podrška reviziji finansijskih izveštaja. Danas, revizija informacionih sistema sve češće predstavlja nezaobilaznu analitičku kariku procesa korporativnog upravljanja informacionom tehnologijom i "most" između menadžmenta i informacione tehnologije. Takođe predstavlja važnu komponentu koncepta korporativnog upravljanja informacionom tehnologijom. Pomoću nje se ocenjuje da li informaciona tehnologija deluju u skladu sa poslovnim ciljevima, u kojoj meri delotvorno i svrsishodno podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacionog sistema na raznim hijerarhijskim nivoima.

Finalni rezultat tih postupaka je izveštaj revizora informacionih sistema, koji se prema područjima analize, zasnovane na Cobit metodologiji, sastoji od sledećih koraka:

- analiza stanja (zrelosti) primene informacionih sistema i tehnologija u poslovanju prema posmatranim područjima;
- procena poslovnih rizika koji proizlaze iz zatečenog stanja;
- preporuke menadžmentu za poboljšanjem tog stanja.

LITERATURA

- [1.] Radovanović D., Radojević T., Lučić D., Šarac M. (2010), *Methods of auditing information systems*, International Conference on Business and Economics, Thessaloniki, Greece.
- [2.] Stanišić M., Radovanović D., Šarac M. (2010), *Revizija informacionih sistema*, Singidunum revija, Beograd.
- [3.] Cannon, D. L. (2008), *CISA Certified Information Systems Auditor Study Guide*. Sybex.
- [4.] Davis, C., Schiller, M., & Wheeler, K. (2007), *IT Auditing: Using Controls to Protect Information Assets*. McGraw-Hill Osborne Media.
- [5.] Grembergen, W. V., & Haes, S. D. (2009), *Enterprise Governance of Information Technology*. New York: Springer Science + Business Media.
- [6.] ITGI. (2007), *CobIT 4.1 – Framework, Control Objectives, Management Guidelines and Maturity Models*, USA: IT Governance Institute.
- [7.] Min, Y. W. (2009), *Understanding and Auditing IT Systems*. Peking: Lulu.
- [8.] Panian, Z., & Spremic, M. (2007), *Korporativno upravljanje i revizija informacijskih sustava*, Zagreb, Zgombić & Partneri.
- [9.] Publishing, V. H. (2008), *IT Governance based on Cobit 4.1 - A Management Guide*. Van Haren Publishing.
- [10.] Spremic, M. (2007), *Methods of auditing information systems*, Zbornik Ekonomskog fakulteta u Zagrebu, 295-312.
- [11.] Schwarz, A., & Hirschheim, R. (2003), An extended platform logic perspective of IT governance. *The Journal of Strategic Information Systems*, 129-166
- [12.] Selig, G. J. (2008), *Implementing IT Governance*. Van Haren Publishing.
- [13.] Senft, S., & Gallegos, F. (2009), *Information Technology Control and Audit* (Third ed.). Boca Raton, USA: Taylor & Francis Group.