ANALIZA METODA ZA KONTROLU I REVIZIJU INFORMACIONIH SISTEMA
ANALYSIS OF METHODS FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS

Dalibor Radovanović, Marko Šarac, *Univerzitet Singidunum, Beograd, Srbija*
Dubravka Lučić, *Ernst & Young Beograd d.o.o., Srbija*
Saša Adamović, *Univerzitet Singidunum, Beograd, Srbija*

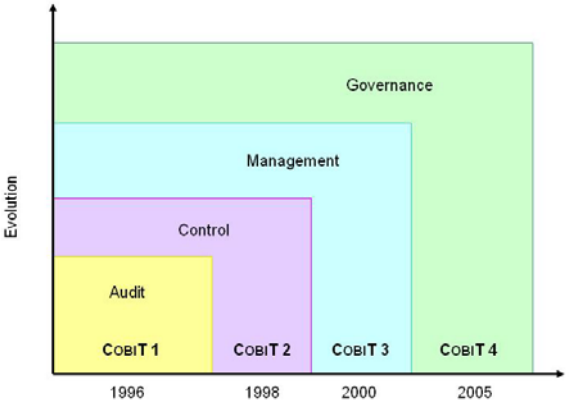
Sadržaj - *U ovom radu se objašnjava koncept kontrole i revizije informacionih sistema, koji se nameće kao imperativ uspešnog poslovanja. Jedna od metodologija koje se koristi je Cobit. On daje uputstva o tome šta može biti urađeno u jednoj organizaciji u pogledu kontrole, aktivnosti, merenja i dokumentacije procesa i poslovanja. U završnom delu rada prikazani su rezultati istraživanja i dato je poređenje najčešće korišćenih metodologija.*
Abstract - *This paper explains the concept of control and IT audit, which imposes an imperative of successful business. One of the methodologies used is COBIT. It gives instructions on what can be done in an organization in terms of control activities, measurement and documentation of processes and operations. The results of research and comparison of the most commonly used methodologies are presented in the final part of the paper.*

1. UVOD

Revizija informacionih sistema 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].

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.



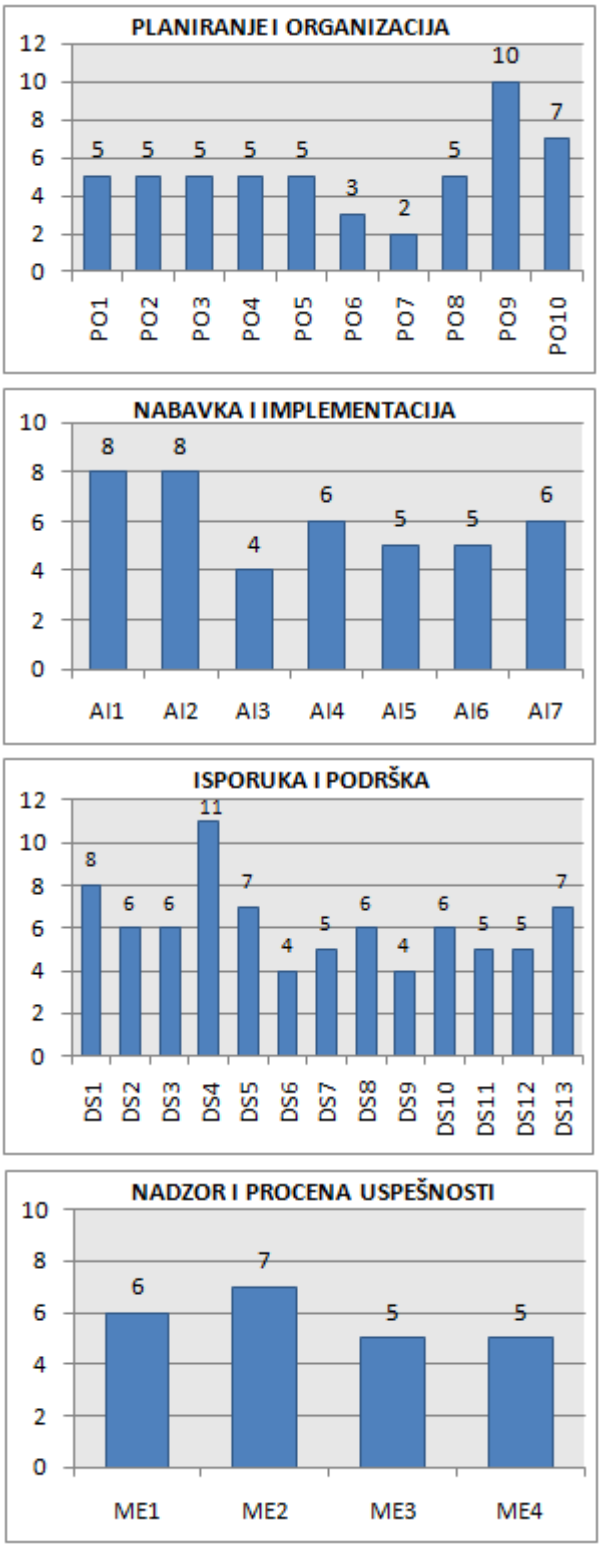
Sl.1. Razvoj Cobit okvira

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 i to su [2]:

- **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.
- **Isporuka 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.

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



Sl. 2. Ukupan broj aktivnosti u okviru kontrolnih ciljeva Cobit metodologije

Postoji ukupno 197 definisanih aktivnosti u okviru četiri domena. Slike 2 prikazuje pojedinačan broj aktivnosti za svaki kontrolni cilj u okviru Cobit metodologije. Ukupan broj aktivnosti po domenima je:

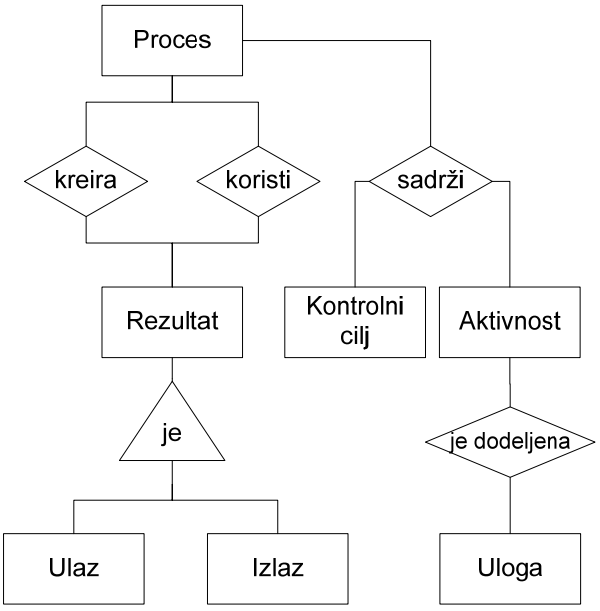
- planiranje i organizacije – definisano 52 aktivnosti;
- nabavka i implementacija – definisano 42 aktivnosti;
- isporuka i podrška – definisano 80 aktivnosti;
- nadzor i procena uspešnosti – definisano 23 aktivnosti.

Za svaki od ključnih poslovnih i IT procesa COBIT definiše i nudi [3]:

- 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.

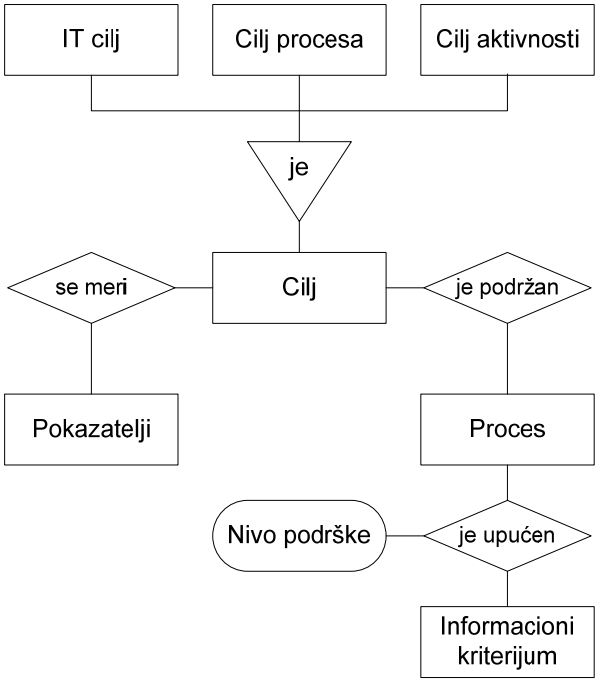
3. COBIT KOMPONENTE

Procesi sadrže kontrolne ciljeve koji predstavljaju željene rezultate koji treba da se postignu primenom kontrolnih procedura u određenom procesu. Za svaki kontrolni cilj definisana je važnost njegove primene, koja može biti velika, srednja ili mala. Aktivnosti su sastavni deo procesa i dodeljena im je uloga. Procesi kreiraju ili koristi rezultate koji se dobijaju na osnovu ulaznih ili izlaznih informacija (slika 3.).



Sl. 3. Kontrolni ciljevi, aktivnost i rezultat

Svi procesi u okviru COBIT metodologije imaju kontrolne ciljeve koji se mogu podeli na ciljeve procesa, ciljeve aktivnosti i IT ciljeve (slika 4.).

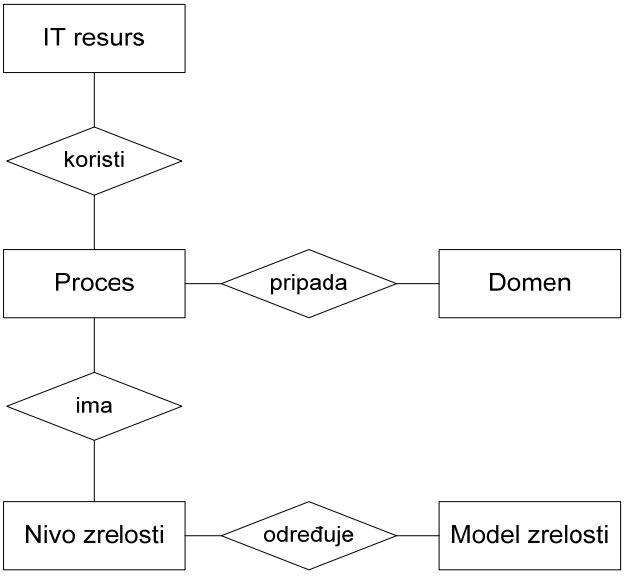


Sl. 4. Ciljevi, pokazatelji i informacioni kriterijumi

Ostvarenje svakog cilja se meri uz pomoć različitih pokazatelja i metrika (ključni indikatori performansi, indikator ostvarenja cilja, itd.). Osim toga, proces sadrži informacije o kriterijumima, koji su apstraktni poslovne ciljeve. COBIT okvir ističe sedam različitih kriterijuma informacije [4]:

- **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.

Svi procesi u COBIT-u pripadaju nekom od četiri domena, podeljeni i organizovani su u skladu sa životnim ciklusom. Za izvršenje aktivnosti procesi koriste IT resurse. Resursi informacione tehnologije su definisani u okviru metodologije i predstavljaju ljude, aplikacije, infrastrukturu i informacije (slika 5.).



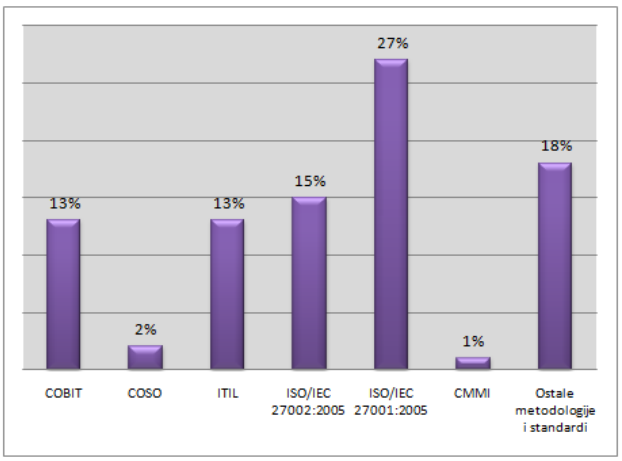
Sl. 5. Model i nivo zrelost, IT resursi

Sumarno, IT resursima se upravlja preko IT procesa radi postizanja ciljeva koji odgovaraju poslovnim zahtevima organizacije.

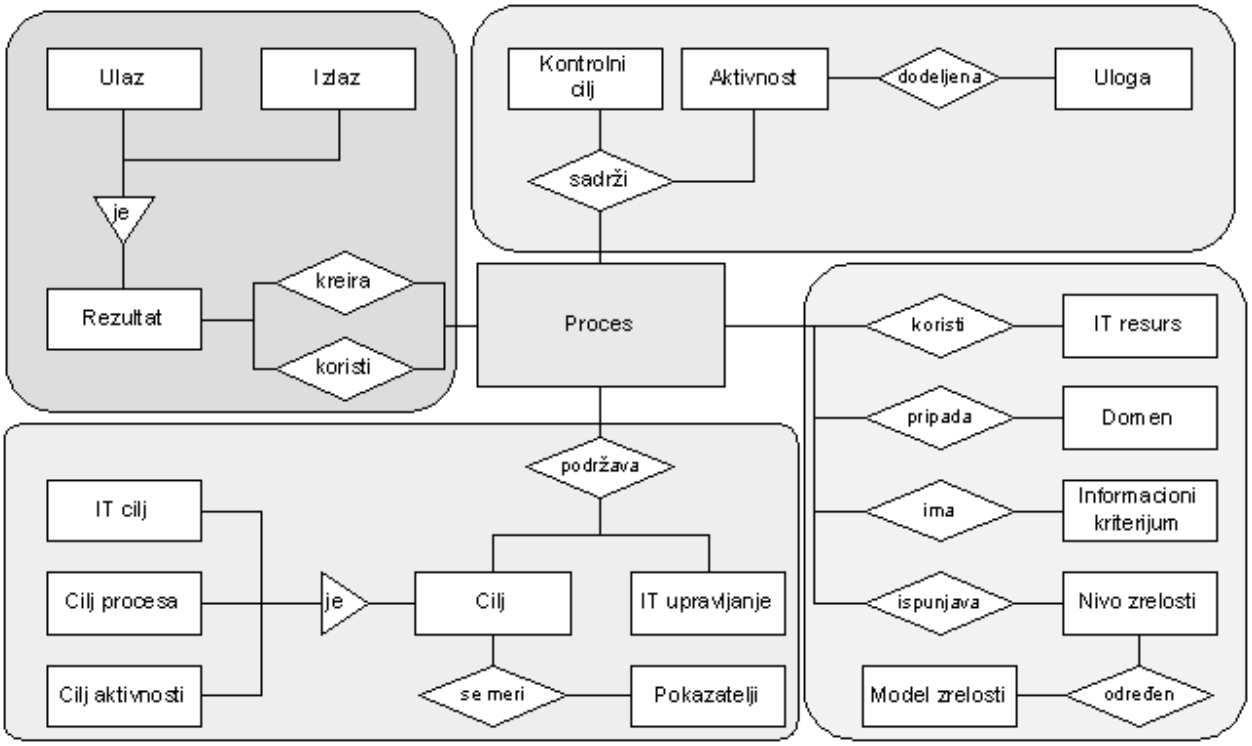
Uz pomoć modela zrelosti za svaki proces se može odrediti nivo zrelosti procesa, što predstavlja početnu tačku u kontinuiranim unapređenju zrelosti procesa. Prema literaturi [5], [6] i [7] ocene zrelosti procesa su definisane u rasponu od 0 do 5:

- 0 – Ne postoje procesi;
- 1 – Početni procesi;
- 2 – Ponovljivi procesi;
- 3 – Definisani procesi;
- 4 – Nadgledani procesi;
- 5 – Optimizovani procesi;

U periodu od 1. juna do 31. jula 2009. godine Ernst & Young je sproveo istraživanje koje je obuhvatilo 1865 kompanija iz 61 zemlje. COBIT spada u grupu najčešće korišćenih metodologija za IT reviziju i informatičku sigurnost. Najčešće se koristi u kombinacija sa ISO27001.



Sl. 6. Najčešće korišćeni standardi za informatičku sigurnost i IT reviziju



Sl. 7. COBIT meta-model

Na slici 7 prikazan je i definisan meta-model COBIT metodologije [9]. On može biti polazna tačka za razumevanje COBIT-a na najnižem nivou, kao i za njegovu primenu u procesu revizije informacionih sistema.

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, posmatrano na raznim hijerarhijskim nivoima.

COBIT spaja poslovne i informatičke ciljeve, pružajući mogućnost da se metrički prati zrelost informacionog sistema. Menadžmentu daje mogućnost optimizacije informatičkih resursa kao što su aplikacije, informacije, infrastruktura i ljudi. Uputstva koja pruža su produkt konsenzusa znanja mnogih stručnjaka i proizvod je dobre prakse, primenjive u bilo kojoj organizaciji.

Pomoću modela koji je prikazan u radu, olakšana je primena COBIT okvira. Na lako razumljiv način je opisana i predstavljena metodologija. Meta-model je polazna tačka za razumevanje COBIT metodologije na najnižem nivou.

LITERATURA

[1] Stanišić M., Radovanović D., Lučić D., *"Revizija informacionih sistema",* Singidunum revija, 2010.

[2] Radovanović D., Radojević T., Lučić D., Šarac M., *"Methods of auditing information systems",* International Conference on Business and Economics, Thessaloniki, Greece, 2010.

[3] ITGI, *COBIT 4.1 – Framework, Control Objectives, Management Guidelines and Maturity Models,* USA: IT Governance Institute, 2007.

[4] Cannon, D. L., *CISA Certified Information Systems Auditor Study Guide,* SYBEX, 2008.

[5] Davis, C., Schiller, M., & Wheeler, K., *IT Auditing: Using Controls to Protect Information Assets.* McGraw-Hill Osborne Media, 2007.

[6] Grembergen, W. V., & Haes, S. D., *Enterprise Governance of Information Technology.* New York: Springer Science + Business Media, 2009.

[7] Panian, Z., & Spremić, M., *Korporativno upravljanje i revizija informacijskih sustava,* Zagreb, Zgombić, 2007.

[8] Senft, S., & Gallegos, F., *Information Technology Control and Audit* (Third Ed.). Boca Raton, USA: Taylor & Francis Group, 2009.

[9] Goeken M., & Alter S., *"Representing IT Governance Frameworks as Meta-models",* Proceedings of the 2008 International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government, Frankfurt, str. 48—54, 2008.