HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

COBIT metodologija

CCERT-PUBDOC-2006-04-155

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

COBIT (eng. ***C**ontrol **OB**jectives for **I**nformation and related **T**echnology*) definira radni okvir koji određuje način implementacije upravljanja informacijskim i komunikacijskim sustavima i tehnologijom (eng. ICT - *Information and Communication Technology*). U današnje vrijeme poslovni procesi mnogih organizacija uvelike ovise o pouzdanoj i dobroj funkciji njihovih informatičkih sustava pa je s tim razlogom osnovana neprofitna institucija ITGI (*IT Governance Institute*) sa ciljem unapređenja i donošenja novih standarda i publikacija koje se odnose na problematiku upravljanja ICT sustavima. ITGI je osnovan od neprofitne organizacije ISACA (*Information System Audit and Control Association*), osnovane 1963. godine čiji su članovi stručnjaci iz svijeta koji se bave upravljanjem, kontrolom, revizijom i sigurnošću informatičkih sustava.

Kritični elementi važni za opstanak i uspjeh organizacije je efikasno upravljanje informacijskom i komunikacijskom tehnologijom (ICT), a ono se ogleda u:povećanju zavisnosti o informacijama i njima pridruženim sustavima, povećanju ranjivosti i širokom spektru prijetnji ICT tehnologiji, obujmu i troškovima postojećih i budućih investicija u ICT sustave, potencijalu tehnologija za promjenom rada organizacije i poslovne prakse, stvaranju novih prilika i reduciranju troškova.

COBIT je bio izdan 1996., 1998., i 2000. godine u inačicama 1, 2 i 3, a zadnja je aktualna inačica 3.2 zamijenjena nadopunjenom novom inačicom COBIT 4.0. koja ni u kojem slučaju ne isključuje prakse navedene u prijašnjoj inačici. Naprotiv, COBIT 4.0 daje mogućnost daljnjeg unapređenja procesa upravljanja informatičkim sustavima, što je opisano u publikaciji COBIT4.0 u slijedećim poglavljima:

- pregled namijenjen menadžmentu (eng. *The Executive Overview*),
- COBIT radni okvir (eng. *Framework*) i
- glavni dio koji opisuje ciljeve kontrola, upute za upravljanje i model zrelosti informatičkih procesa

COBIT definira radni okvir upravljanja informatičkim sustavom tako da je zadovoljeno slijedeće:

- poslovni procesi organizacije su u skladu s arhitekturom i funkcijom informatičkog sustava,
- rizici koji nastaju neispravnim ili nepotpunim funkcioniranjem informatičkim sustavom su smanjeni,
- omogućeno je upravljanje rizicima funkcioniranja informatičkog sustava na zadovoljavajući način i
- omogućeno je korištenje informatičkih resursa na racionalan način.

Između ostalog, COBIT sadrži i publikaciju „*Skup alata za implementaciju*“ koja objašnjava kako su neke organizacije primijenile COBIT u svojim radnim okolinama. Publikacija sadrži dva alata: „Dijagnostika svjesnosti menadžmentu“ i „Dijagnostika IT kontrole“.

COBIT je metodologija koja omogućava integraciju poslova vezanih za zahtjeve kontrole, tehničku problematiku i poslovni rizik, i komuniciranje te postignute razine kontrole prema vlasnicima tvrtke. Omogućava i razvoj politika i dobrih praksi ICT kontrole u organizacijama. Implementacija COBIT-a očituje se na različite načine:

- upravama kompanija pomaže razumjeti koncept upravljanja informatičkim sustavima,
- definira odgovornosti koje su potrebne za normalno funkcioniranje sustava,
- usklađuje sustav s regulatornim obvezama i
- organizira aktivnosti unutar ICT sustava na prihvatljiv način.

COBIT spaja poslovne i informatičke ciljeve, pružajući mogućnost da se metrikama prati zrelost informatičkog sustava (eng. *Maturity Model*). COBIT daje menadžmentu mogućnost optimizacije informatičkih resursa kao što su aplikacije, informacije, infrastruktura i ljudi. Praksa koju preporučuje COBIT je produkt konsenzusa znanja mnogih stručnjaka i proizvod je dobre prakse, primjenjive u bilo kojoj organizaciji.

2. COBIT

2.1. Osnovna terminologija

Radi boljeg razumijevanja ovog dokumenta potrebno je definirati značenje pojedinih termina koji se u dokumentu i u COBIT publikacijama često upotrebljavaju:

- kontrola (eng. *control*) – sigurnosna politika, procedure i prakse koje osiguravaju da će poslovni ciljevi biti ostvareni te da će neželjeni događaji biti detektirani i njihov učinak smanjen ili eliminiran;
- cilj primjene kontrole (eng. *control objective*) – očekivani rezultat ili svrha primjene određene kontrole;
- proces – cilj kontrole višeg nivoa (eng. *high level control objective*).

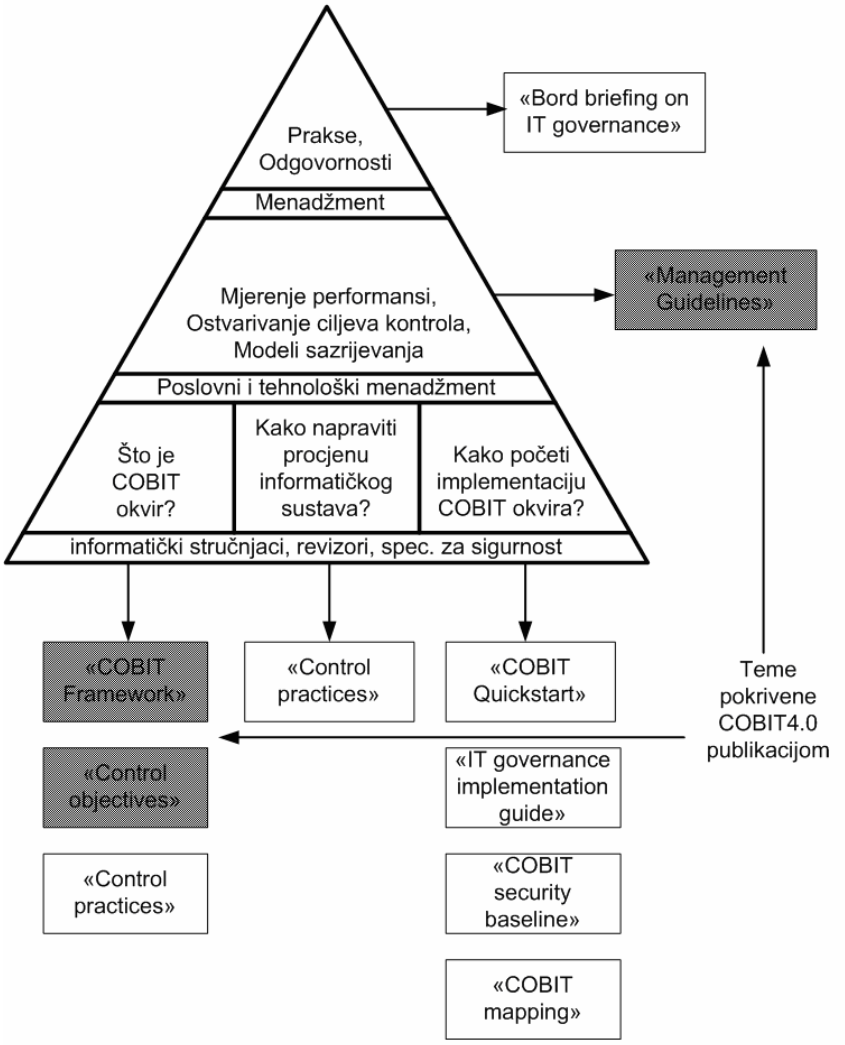
COBIT definira generički model informatičkih procesa koji se mogu pojaviti u jednom informatičkom sustavu i na taj način opisuje model funkcioniranja informatičkog sustava poslovnom i informatičkom menadžmentu. Da bi se uspostavilo uspješno upravljanje njime, nužno je da informatički menadžment implementira potrebne kontrole koje su definirane za sve COBIT-om definirane informatičke procese. Budući da su ciljevi primjene kontrola unutar COBIT-a organizirani po IT procesima, tada okvir zapravo daje stvarnu vezu između primijenjenih kontrola, procesa i upravljanja informatičkim sustavima.

2.2. COBIT publikacije

COBIT kao produkt predstavlja niz publikacija namijenjenih slijedećim sudionicima u upravljanju informatičkim sustavima:

- Upravi i visokom menadžmentu - "*Bord Briefing on IT Governance*" publikacija je pisana za osobe u upravi organizacija te objašnjava problematiku koja se odnosi na upravljanje informatičkim sustavima i odgovornosti koje oni imaju.
- Informatičkom i operativnom menadžmentu - "*Management guideliness*" publikacija koja pomaže pri pronalaženju odgovora na pitanje kako daleko treba ići u kontroli informatičkih procesa, kako mjeriti performanse, koje prakse primijeniti te kako i što uspoređivati i mjeriti.
- Informatičkim stručnjacima koji se brinu o direktnoj primjeni kontrola, informatičkim revizorima i sigurnosnim stručnjacima. Literatura koja je namijenjena njima je slijedeća:
  - "*COBIT Framework*" - objašnjava kako COBIT organizira ciljeve upravljanja i dobru praksu upravljanja u četiri domene i njima pripadajuće procese.
  - "*Control objectives*" - opisuje 4 domene, 34 procesa i 318 ciljeva kontrola te dobru praksu u upravljanju svim aktivnostima u informatičkim sustavima. Ova se problematika je isto tako sada uključena u COBIT 4.0 publikaciju.
  - "*Control Practices*" - publikacija nije sastavni dio COBIT 4.0 publikacije, ali je nadopunjuje s detaljima koji su potrebni u praksi upravljanja i revizije te opisuje 1549 dobrih praksi primjenom kojih se može doći do ciljeva primjenjenih kontrola.
  - "*IT Assurance guide*" - publikacija nije u sastavu COBIT 4.0 publikacije, a opisuje generički pristup reviziji informatičkih sustava.
  - "*IT Governance Implementation Guide*" - publikacija opisuje metodologiju za implementaciju COBIT standarda i bazira se na inačici 3 COBIT-a i još nije usklađena s inačicom 4.
  - "*COBIT Quickstart*" - publikacija definira reducirani skup (oko 20%) kontrola i procesa specificiranih COBIT 4.0 publikacijom, a namijenjena je manjim organizacijama.
  - "*COBIT Security Baseline*" - opisuje osnovne korake pri implementaciji sigurnosti informatičkih sustava i namijenjena je prvenstveno menadžmentu.
  - "*COBIT mapping*" - opisuje područja preklapanja COBIT standarda i ostalih standarda s područja upravljanja i sigurnosti informatičkih sustava.

Skup COBIT publikacija je prikazana piramidom na slici Slika 1, a sadržaj slijedećih poglavlja ovog rada će se većinom odnositi na sadržaj publikacije COBIT 4.0.



Slika 1: COBIT publikacije

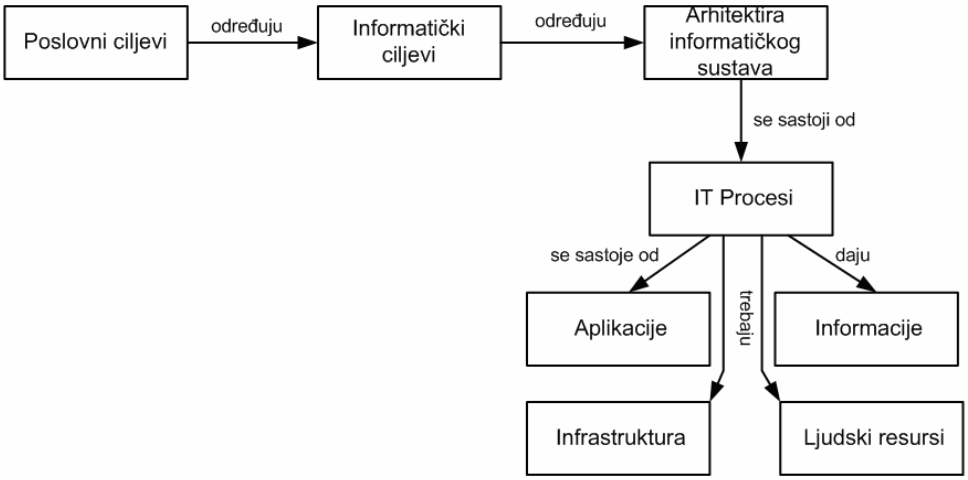
3. Karakteristike i organizacija COBIT-a

3.1. Poslovna orijentacija

Budući da je COBIT poslovno orijentiran, on pomaže harmonizirati informatički sustav s poslovnim zahtjevima u svrhu postizanja poslovnih ciljeva. U tom smislu COBIT definira skup generičkih, uobičajenih, poslovnih i s druge strane informatičkih ciljeva, te definira matricu korelacije koja prikazuje odnos poslovnih ciljeva i potrebnih informatičkih ciljeva koji vode u smjeru njihove realizacije. Tako je na primjer jedan od definiranih poslovnih ciljeva u dijelu publikacije „povrat investicije“, a njegova implementacija ovisi o funkcionalnom i cjenovno primjerenom (eng. *Cost effective*) informatičkom rješenju čija implementacija se odnosi na 4 definirana informatička procesa. Obzirom na činjenicu da je tabela korelacija poslovnih i informatičkih ciljeva velika, ovaj rad se dalje neće baviti njenim drugim tumačenjima.

COBIT pomaže pri procesu definiranja informatičkih ciljeva koji moraju biti usklađeni s poslovnim ciljevima pošto primjenom COBIT-a poslovni ciljevi imaju direktni utjecaj na arhitekturu informatičkog sustava. Zahtjevi poslovanja određuju implementaciju informatičkih usluga, koje imaju utjecaj na neke od informatičkih kriterija kao što su pouzdanost, integritet, učinkovitost,... Stoga COBIT pomaže pri definiranju informatičkih rješenja koja mogu podržati zahtijevane poslovne ciljeve definirajući informatičke procese koji se oslanjaju na ljudske potencijale, informatičku infrastrukturu i

aplikacije. Na slici Slika 2 prikazani su osnovni odnosi između poslovnih i informatičkih ciljeva pri primjeni COBIT alata.



Slika 2: Poslovni ciljevi i arhitektura

3.1.1. Potreba za kontrolom

Potreba za referencijskim radnim okvirom za sigurnost i kontrolu ICT-om postoji u svim organizacijama. Uloga menadžmenta je odlučivanje o razumnim investicijama za sigurnost i kontrolu u ICT-u te kako balansirati rizike i kontrolirati okolinu u ICT okruženju. Sigurnost i kontrola informacijskih sustava pomažu upravljanju rizicima, ali ih ne eliminiraju. Menadžment mora odlučiti o prihvatljivoj razini rizika koja se može tolerirati, u odnosu na troškove dok revizori ulažu napore u standardizaciju jer su oni kontinuirano suprotstavljeni s potrebom argumentiranja svog mišljenja o internim kontrolama u izvješćima menadžmentu. Bez radnog okvira to je izuzetno teški zadatak. Menadžeri često pozivaju revizore na konzultacije i savjete u vezi ICT sigurnosti i kontroli.

3.1.2. Odnosi u poslovnoj okolini

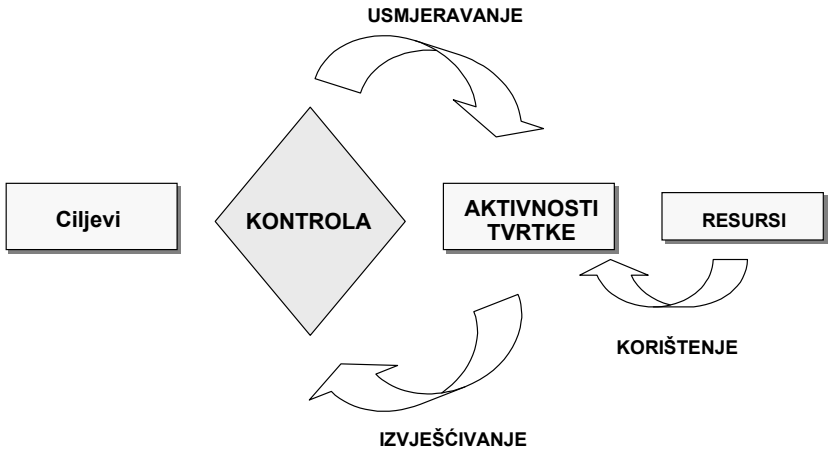
Organizacije se udružuju da bi poboljšale poslovanje i simultano iskoristile napretke u ICT-u za poboljšavanje konkurentske pozicije. Reinženjering poslovnih procesa, načina organizacije, korištenje vanjskih organizacija (eng. *outsourcing*), "plitka" organizacija i distribuirana obrada su sve promjene koje utječu na način odvijanja operacija poslovnih i vladinih organizacija.
Automatiziranje funkcija organizacije diktira uključivanje sve moćnijih mehanizama kontrole u ICT okruženje. U radnom okviru ubrzane promjene čine da se menadžeri, specijalisti informacijskih tehnologija i revizori nastoje razvijati jednako brzo kao i tehnologije i okolina.

3.1.3. Vladanje ICT-om

Vladanje poduzećem i ICT-om nisu različite discipline. Vladanje ICT-om osigurava povezivanje ICT resursa i informacija sa strategijom tvrtke i pripadajućim ciljevima integrirajući i institucionalizirajući optimalne načine planiranja i organiziranja, akvizicije i implementiranja, isporuke i podrške te nadgledanja ICT učinaka. Vladanje ICT-om je integralni dio uspjeha vladanjem tvrtke. Aktivnosti tvrtke zahtijevaju informacije iz IT aktivnosti kako bi se realizirali poslovni ciljevi. Uspješne organizacije osiguravaju međuzavisnost između svog strateškog planiranja i njihovih IT aktivnosti.

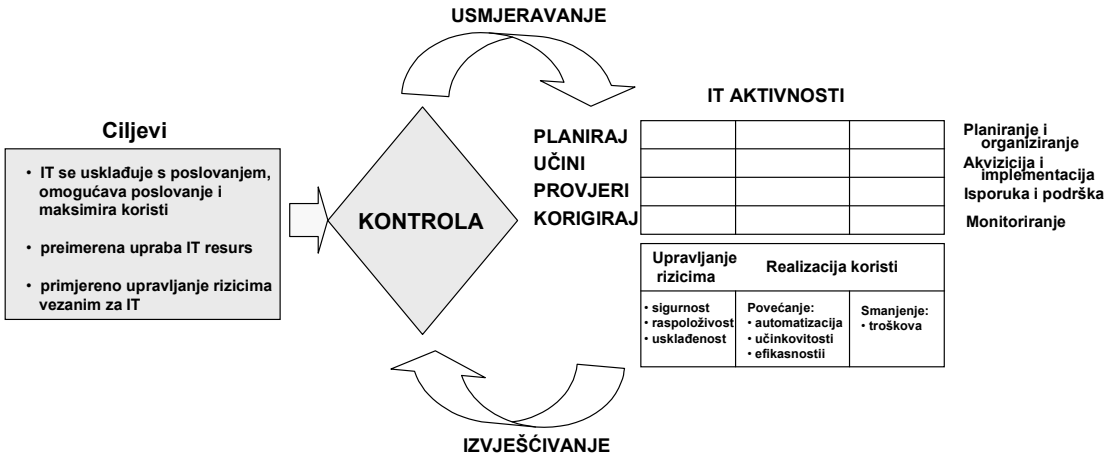
Slika 3: Međuzavisnost strateškog planiranja i IT aktivnosti

Tvrtkama se obično vlada općenito prihvaćenim dobrim (najboljim) praksama, kako bi se osiguralo da tvrtka ostvaruje svoje ciljeve – čije osiguranje je garantirano određenim kontrolama. Iz ovih ciljeva proizlazi usmjerenje organizacije, koje diktira određene aktivnosti tvrtke, korištenjem resursa tvrtke. Rezultati aktivnosti tvrtke se mjere i koriste kao ulaz u konstantnu reviziju i održavanje kontrola, stvarajući opet na taj način novi ciklus.



Slika 4: Usmjeravanje aktivnosti tvrtke prema ciljevima

ICT-om se također vlada dobrim (ili najboljim) praksama, kako bi se osiguralo da informacije tvrtke i pridružene tehnologije podržavaju ciljeve poslovanja. Resursi se moraju primjereno koristiti te primjereno upravljati s rizicima. Ove prakse čine temelj usmjeravanja aktivnosti ICT-a, koje se mogu karakterizirati kao planiranje i organiziranje, akvizicija i implementacija, isporuka i podrška i nadgledanje s dvostrukom svrhom - upravljanja rizicima i ostvarivanja koristi (učinkovitost i efikasnost). Izvještava se o izlazima aktivnosti IT-a, koji se uspoređuju s različitim praksama i kontrolama, pa tako opet ponovno u novom ciklusu.



Slika 5*:* Vladanje ICT-om

Da bi menadžment postigao svoje ciljeve, on mora usmjeravati i upravljati ICT aktivnostima u svrhu postizanja učinkovite ravnoteže između upravljanja rizicima i ostvarivanja koristi. Management treba identificirati najvažnije aktivnosti, mjeriti progres prema postizanju ciljeva i utvrditi, koliko se dobro ICT procesi izvode. Dodatno tomu, menadžment treba posjedovati sposobnost evaluacije stupnja zrelosti organizacije prema najboljim praksama industrije i međunarodnim standardima. Za podršku ovih potreba upravljanja, COBIT *Management smjernice* su identificirale kritične faktore uspjeha, ključne indikatore cilja, ključne indikatore učinka te pridružene modele zrelosti za vladanje IT-om koji su objašnjeni u nastavku ovog dokumenta.

3.1.4. Auditorij: management, korisnici i revizori

COBIT je dizajniran za sva tri auditorija:

- menadžment - kao pomoć u balansiranju rizika i investiranja u kontrolu u često nepredvidljivoj IT okolini,
- korisnici - za dobivanje mišljenja i/ili pružanja savjeta menadžmentu o sigurnosti i kontrolama IT servisa pružanih interno ili od treće strane i
- revizori - za materijaliziranje njihova mišljenja i/ili savjetovanja menadžmenta glede interne kontrole.

3.1.5. Orijentacija na poslovne ciljeve

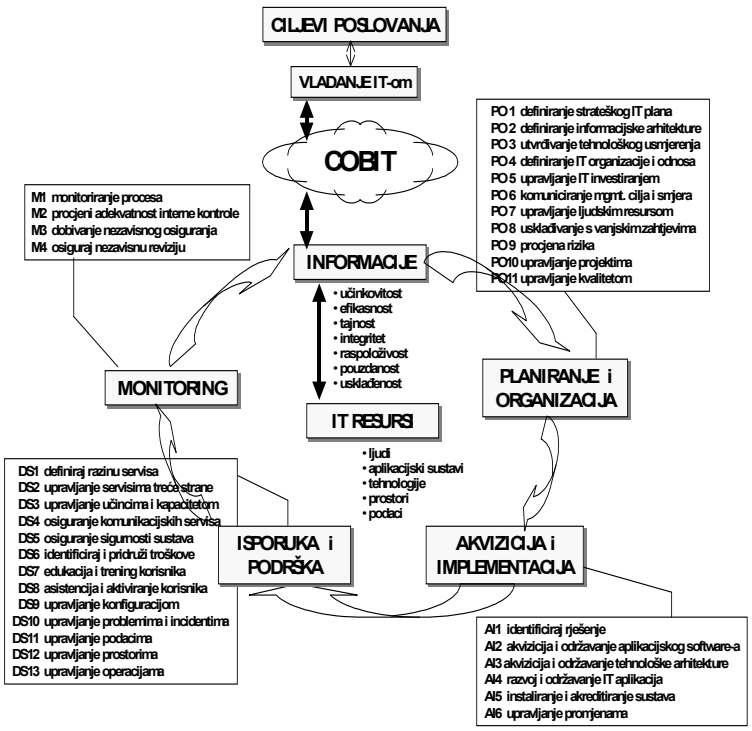
Cilj COBIT-a je adresiranje ciljeva poslovanja. Ciljevi kontrole jasno su i razdvojeno povezani sa ciljevima poslovanja s namjerom podržavanja značajnu uporabu izvan revizorske zajednice. Ciljevi kontrole su definirani na procesno orijentiran način slijedeći principe reinženjeringa poslovnih procesa. Kod identificiranih domena i procesa, također su identificirani ciljevi kontrole visoke razine i ekspliciranje danih principa u dokumentiranju veze sa ciljevima poslovanja. Dodatno tomu, dana su razmatranja i smjernice za definiranje i implementiranje ciljeva kontrole ICT-a. Klasifikacija područja gdje se primjenjuju ciljevi kontrole visoke razine (domene i procesi), indikacija zahtjeva poslovanja za informacijama u domenama, kao i IT resursi, na koje primarno djeluju ciljevi kontrole zajedno čine COBIT-ov radni okvir. Radni okvir je temeljen na aktivnostima istraživanja, koje su identificirale 34 cilja kontrole visoke razine i 318 detaljna cilja kontrole.

3.2. Organizacija COBIT-a

COBIT publikacija u svom glavnom djelu govori o 34 procesa (*high level control objective*) koji spadaju u četiri logičke domene. Nadalje, svaki od procesa je detaljnije razrađen u detaljnije kontrole (*detailed control objectives)* kojih ima sveukupno 318. Daljnja podjela, odnosno razrada problema nije specificirana u publikaciji COBIT 4.0, a odnosi se na načine implementacije kontrola (*control practices*) kojih ima ukupno 1547 i one su opisane u publikaciji "*Control Practices*".

3.2.1. Četiri domene i procesi

Na sljedećoj slici prikazani su COBIT ICT procesi podijeljeni u 4 domene:



Slika 6: COBIT ICT procesi definirani unutar 4 domene

3.2.1.1. Planiranje i organiziranje (eng. *Plan and Organize*)

Domena planiranja i organiziranja definira procese čija primjena daje odgovor na planiranje informatičkih sustava koji moraju biti u skladu sa strateškom vizijom poslovanja. Ovom domenom su također adresirani problemi upravljanja rizicima IT sustava, kvalitetom informatičkog sustava i usluga te optimalnog korištenja informatičkih resursa.

3.2.1.2. Nabava i implementacija (eng. *Acquire and Implement*)

Nabava i implementacija je domena koja definira procese koji se odnose na implementaciju informatičkih rješenja koja odgovaraju strateškoj viziji informatičkog sustava. Ova domena se odnosi na rješavanje problematike ispravnog funkcioniranja novih sustava, vrijeme njihovog izvođenja i resursa, novih informatičkih usluga i njihovom ispunjavanju strateškog cilja.

3.2.1.3. Isporuka i podrška (eng. *Deliver and Support*)

Ova domena se odnosi na problematiku isporuke pojedinih informatičkih usluga (eng. *service delivery*), upravljanjem sigurnosti, podrške korisnicima i operativnim upravljanjem sustava. Problematika ove domene se odnosi i na pitanje cijena usluga koje moraju biti optimizirane, na optimalno korištenje ljudskih resursa te na pitanje tajnosti, integriteta i dostupnosti informacija i usluga.

3.2.1.4. Nadgledanje i evaluacija (eng. *Monitor and Evaluate*)

Kvaliteta i usklađenost svih IT procesa mora biti redovito procjenjivana, te se tako problematika ove domene odnosi na upravljanje performansama, procjeni usklađenosti sa zakonskom regulativom, internoj kontroli, procjeni rizika i slično.

3.2.1.5. Procesi po domenama

Ako se domene i procesi malo bolje promotre, može se zaključiti da oni predstavljaju ispravan put životnog ciklusa informatičkih rješenja, odnosno faze koje bi svako rješenje moralo proći pri svojoj implementaciji i uporabi. Domene i procesi predstavljaju okvir unutar kojeg se moraju implementirati

sva informatička rješenja i dobar su alat onima koji se bave planiranjem, implementacijom, eksploatacijom informatičkih sustava, a posao informatičkih revizora treba biti utvrđivanje dosljednosti primjene okvira definiranog COBIT-om.
Unutar domene **planiranja i organiziranja** razrađuje se poslovna tehnologija koja je osnova za definiranje potreba ICT-a korištenjem sljedećih procesa:

- P01 - Definicija strateškog IT plana,
- P02 - Definicija informatičke infrastrukture,
- P03 - Određivanje tehnološkog smjera,
- P04 - Definicija IT procesa, organizacije i povezanosti,
- P05 - Upravljanje IT investicijom,
- P06 - Provođenje uputa menadžmenta,
- P07 - Upravljanje ljudskim resursima za IT,
- P08 - Upravljanje kvalitetom,
- P09 - Procjena i upravljanje IT rizicima,
- P10 - Vođenje projekta.

Kroz domenu **nabave i implementacije** definiraju se postupci nabave rješenja i njihovo korištenje u radu kroz naredne procese:

- AI1 - Identificiraj automatizirana rješenja,
- AI2 - Nabava i održavanje aplikacijskih programa,
- AI3 - Nabava i implementacija tehnološke infrastrukture,
- AI4 - Puštanje u pogon i korištenje,
- AI5 - Nabava informatičkih resursa,
- AI6 - Upravljanje promjenama,
- AI7 - Instalacija i akreditacija rješenja i promjena.

Unutar domene **isporuke i podrške** identificiraju se i alociraju troškovi za procese i definiraju se načini njihovog upravljanja kroz naredne procese:

- DS1 - Definicija i upravljanje uslugama,
- DS2 - Upravljanje trećim (eng. *third-party*) uslugama,
- DS3 - Upravljanje performansama i kapacitetom,
- DS4 - Osiguraj konstantnu uslugu,
- DS5 - Osiguraj sigurnost sustava,
- DS6 - Odredi cijenu usluge,
- DS7 - Educiraj korisnike,
- DS9 - Upravljanje konfiguracijom,
- DS10 - Upravljanje problemima,
- DS11 - Upravljanje podacima,
- DS12 - Upravljanje informatičkom okolinom,
- DS13 - Upravljanje produkcijom.

Unutar domene **nadgledanja i evaluacije** prate se performanse i smjerovi rada sustava i poduzimaju određene korekcije, a procesi su sljedeći:

- ME1 - Nadgledanje i evaluacija performanse IT sustava,
- ME2 - Nadgledanje i evaluacija internih kontrola,
- ME3 - Osiguraj skladnost s regulatornom stranom,
- ME4 - Osigura upravljanje s informatičkim sustavom.

3.2.2. Detaljne kontrole

COBIT definira generički model niza procesa koji u stvarnosti predstavljaju pojedine funkcije unutar informatičkog sustava te time pomaže stručnjacima i menadžmentu u razumijevanju i upravljanju informatičkim sustavima. Da bi se omogućilo upravljanje informatičkim sustavom, moraju biti implementirane kontrole za sve procese unutar pojedinog informatičkog sustava. U tu svrhu COBIT definira za svaki proces više detaljnih kontrola koje moraju biti implementirane da bi upravljanje procesom bilo moguće. Detaljne kontrole (eng. *Detailed Controls*) se u specifikacijama označavanju s oznakom procesa i brojem kontrole.
U sljedećem primjeru oznakom PO9 je označen generički proces “Procjeni i upravljaj rizicima informatičkog sustava“, za čiju implementaciju je potrebno slijedećih šest detaljnih kontrola:

- PO9.1 - uključi procjenu rizika informatičkog sustava u sustav upravljanja rizicima cijele kompanije,
- PO9.2 - uspostavi kontekst procjene rizika,
- PO9.3 - definiraj ciljeve procjene i kriterije po kojima se radi evaluacija rizika,
- PO9.4 - identificiraj prijetnju,
- PO9.5 - procjena utjecaj nekog događaja toga na ciljeve i poslovanje kompanije i
- PO9.6 - procjeni rizik pomoću kvalitativnih i kvantitativnih metoda.

3.2.3. Upute za upravljanje

Pored popisa detaljnih kontrola, za svaki proces su opisani generički ulazi i izlazi, dana je matrica potrebnih aktivnosti i odgovornosti, definirani su ciljevi aktivnosti i metrika koja prezentira način mjerenja pri postizanju ciljeva.
Svi procesi u COBIT-u su opisani na isti način, što će detaljnije biti objašnjeno u slijedećim poglavljima.

3.2.4. Mjerenje performansi

COBIT definira ciljeve i metriku kojom se mjeri nivo postignuća tih ciljeva u slijedeća tri nivoa:

- metrika informatičkih procesa koja pokazuje u kojoj mjeri informatički sustav zadovoljava potrebe poslovanja,
- metrika informatičkih procesa kojom se mjeri u kolikoj mjeri neki informatički proces zadovoljava ispunjenje svoje funkcije ili cilja i
- metrika za mjerenje performansi informatičkog procesa kojom se mjeri efikasnost funkcioniranja procesa.

U specifikacijama COBIT-a je za svaki informatički proces opisan sustav metrike na način da prikazuje ciljeve po hijerarhiji i metriku kojom se mjeri postignuće istih ciljeva. Odnos između metrike i ciljeva je takav da indikatori postignuća ciljeva (eng. KGI – *key goal indicators*) postaju neki od indikatora mjerenja performansi (eng. KPI – *key performance indicators*). U specifikacijama se za svaki proces definiraju tri cilja: cilj aktivnosti, procesa i informatičkog sustava.
Kroz ključne indikatore cilja (KGI) definiraju se zahtjevi koji se trebaju kontrolirati tijekom izvođenja projekta. U nastavku su navedeni glavni i izvedeni zahtjevi te načini realizacije koji dovode do ispunjenja zadanih ciljeva:

- prošireni učinci i upravljanje troškovima,
- poboljšana dobit na glavnim IT investicijama,
- poboljšano vrijeme izlaska na tržište (eng. *time-to-market*),
- povećan kvaliteta i inovacije i upravljanje rizikom,
- primjerno integrirani i standardizirani procesi poslovanja,
- dohvat novih i zadovoljavanje postojećih klijenata,
- raspoloživost odgovarajuće širine pojasa (eng. *bandwith*),
- ostvarivanje zahtjeva i očekivanja proračuna i vremena procesa,
- usklađenost sa zakonima, regulacijama, industrijskim standardima i ugovornim obvezama,
- transparentnost preuzetih rizika i usklađenost s ugovorenim,
- komparativna ispitivanja zrelosti vladanja IT-om,
- kreiranje novih kanala za isporuku servisa, itd…

Ključni indikatori performansi (KPI) koji vode učinkovitijem poslovanju, a time i periodičnim kontrolama obavljanja posla:

- poboljšani omjer troškovi-učinkovitost IT procesa,
- povećani broj planova akcija i inicijativa za poboljšavanje procesa u IT-u,
- povećana iskoristivost IT infrastrukture,
- povećano zadovoljstvo vlasnika (pregled i broj pritužbi/reklamacija),
- poboljšana produktivnost osoblja (broj isporučenog) i poboljšani moral (anketa),
- povećana raspoloživost znanja i informacija za menadžment tvrtke,
- povećana povezanost vladanja tvrtkom i IT-om,
- poboljšana učinkovitost mjerena balansiranim IZ bodovnim karticama, itd…

Potrebno je napomenuti da se ciljevi, po uputama COBIT-a, definiraju po odozgo prema dolje (eng. *top-down*) modelu, odnosno poslovni ciljevi definiraju broj i vrstu informatičkih procesa, dok će svaki

informatički proces definirati potrebne aktivnosti za njegovo ostvarenje. Grafički prikaz metrike ide u obrnutom smjeru od najnižih aktivnosti prema ciljevima procesa i na kraju informatičkog sustava. Takav odnos je prikazan na slijedećem primjeru metrike procesa oznake PO2 - "Definiraj arhitekturu informacije":

Performanse aktivnosti

- Osiguraj točnost podatkovnog modela
- Pridruži vlasništvo pojedinim podacima
- Klasificiraj informacije
- Održavaj integritet podataka
- Održavaj konzistenciju komponenti informatičke infrastrukture

se mjere s KGI najnižeg nivoa

- Frekvencija ažuriranja informatičkog modela kompanije
- Postotak podataka bez vlasnika
- Frekvencija aktivnosti ispitivanja valjanosti podataka
- Nivo učestvovanja korisnika u kreiranju podataka

koji postaje KPI kojim se mjere performanse slijedećeg višeg cilja

- Uspostava podatkovnog modela kompanije
- Reduciranje redundancije u podacima
- Uspostava učinkovitog upravljanja informacijama

čije se ispunjenje mjeri s KGI kojeg predstavlja

- Postotak podatkovnih elemenata koji se ne uklapaju u model kompanije
- Postotak podataka koji ne poštuju shemu organizacije podataka
- Postotak aplikacija koje su van zamišljene arhitekture informatičkog sustava

koji postaje dio KPI kojim se mjere performanse najvišeg cilja

- Optimiziraj korištenje informacija
- Osiguraj integraciju aplikacija u poslovni model
- Odgovori na poslovne zahtjeve i poslovnu strategiju

Ostvarenje najvišeg cilja se mjeri s KGI

- Postotak korisnika koji su zadovoljni s informatičkim sustavom
- Postotak redundantnih ili duplih podatkovnih elemenata

3.2.5. Model zrelosti

U smislu boljeg upravljanja i kontrole, potrebno je mjeriti performanse postignute primjenom kontrola. COBIT definira za svaki proces metriku koja određuje kako i što mjeriti. U svrhu mjerenja, COBIT definira model zrelosti (eng. *Maturity Model*) čijom primjenom se može doći do određenih poboljšanja u stabilnosti i kontroliranju informatičkih procesa i sustava. Model zrelosti, primijenjen u COBIT specifikacijama je vrlo sličan modelu kojeg je definirao Institut SEI (*Software Engineering Institute*). Model definira metriku i ciljeve do kojih se dolazi mjerenjem performansi informatičkih procesa pri čemu pomaže u upravljanju procesima pridružujući procesima ocjenu od 0 do 5. U tu svrhu su u specifikacijama COBIT-a za svaki proces navedeni kriteriji na koje treba obratiti pažnju pri ocjenjivanju po specificiranim modelu zrelosti.
Model zrelosti je definiran za svaki od 34 procesa sa slijedećim ocjenama:

- **0 – Neimplementiran** (eng. *non-existant*)
  Upravljanje procesom nije implementirano. Potpun nedostatak bilo kakvih raspoznatljivih procesa vladanja IT-om. Organizacija ne prepoznaje postojanje pridružene problematike.
- **1 – Početni** (eng. *initial*)
  Postoji evidencija da je organizacija prepoznala postojanje problema vladanja IT-om i potrebu njihova adresiranja. Međutim nema standardiziranih procesa, već umjesto njih postoje nedefinirani pristupi primjenjivani od pojedinaca ili od slučaja do slučaja. Pristup menadžmenta je kaotičan i samo postoje sporadična, nekonzistentna komunikacija o problemima i pristupima njihovu adresiranju. IT nadzor je implementiran samo reaktivno na incidente koji su prouzrokovali neki gubitak ili nelagodu organizaciji.
- **2 – Ponavljajući** (eng. *repeatable*)-

Proces se ponaša na očekivani način i definirane procedure ponavljaju različiti zaposlenici, ali te procedure nisu dokumentirane. Izvođenje procedura je prepušteno znanju pojedinaca te je time vjerojatnost pogreške povećana. Postoji globalna svijest o problematici aktivnosti vladanja IT-om, a indikatori učinkovitosti su u razvoju, uključujući planiranje IT-a, procese isporuke i nadgledanja. Kao dio tih napora, aktivnosti vladanja IT-om su formalno utemeljene u proces upravljanja promjenama organizacije, s aktivno uključenim višim razinama management-a i odgovarajućim pregledima. Odabrani procesi IT-a su identificirani za poboljšavanje i/ili temeljni procesa tvrtke i efikasno se planiraju i nadziru kao investicije, a izvedeni su unutar konteksta definiranog arhitekturnog radnog okvira IT-a. Menadžment je identificirao temeljne metode i tehnike vladanja IT-om, međutim, proces nije prihvaćen u cijeloj organizaciji. Nema formalnog treninga i komuniciranja standarda vladanja a odgovornost je ostavljena pojedincima..

- **3 – Definiran** (eng. *defined*)
  Procedure su standardizirane i dokumentirane, a njihova učinkovitost izvođenja se periodično mjeri. Potreba za djelovanjem u svezi vladanja IT-om se razumije i prihvaća. Razvijen je temeljni skup indikatora upravljanja IT-om s definiranom vezom između mjerenja rezultata i poticaja učinaka, koji je dokumentiran i integriran u procese strateškog i operativnog planiranja i nadziranja te su time procedure standardizirane, dokumentirane i uvedene. Menadžment komunicira standardiziranim procedurama, a uspostavljen je i neformalni trening. Indikatori učinkovitosti svih aktivnosti vladanja IT-om se memoriraju i analiziraju, vodeći poboljšanjima širom tvrtke. Alati su standardizirani korištenjem trenutno raspoloživih tehnika.
- **4 – Upravljan** (eng. *managed*)
  Moguće je nadgledati i mjeriti parametre izvođenja procedura, procesi su u stanju stalnog poboljšavanja. Mnoge kontrole su automatizirane i redovito preispitivane. Upotreba alata za automatizaciju kontrola je djelomična. Postoji potpuno razumijevanje problematike na svim razinama, podržano s formalnim treningom. Također, postoji jasno razumijevanje tko su klijenti (korisnici), a odgovornosti su definirane i nadzirane. IT procesi su usklađeni s poslovanjem i strategijom IT-a. Poboljšanja procesa u IT-u su temeljena primarno na kvantitativnom razumijevanju i moguće je nadgledati i mjeriti usklađenost s metrikom procedura i procesa. Vlasnici svih procesa su svjesni rizika, važnosti IT-a i prilika koje može ponuditi. Menadžment je definirao tolerancije pod kojima se procesi moraju odvijati. Akcije se poduzimaju u mnogim, ali ne i u svim slučajevima gdje procesi ne rade učinkovito i efikasno. Procesi se povremeno poboljšavaju i ojačavaju se interno najbolje prakse. Izvorna analiza uzroka je u procesu standardiziranja. Postoji uključivanje svih potrebnih internih domenskih eksperata. Vladanje IT-om evoluira u proces širom organizacije. Aktivnosti vladanja IT-om postaju integrirane s procesima vladanja tvrtkom.
- **5 - Optimiziran** (eng. *optimised*)
  Postoji cjeloviti program rizika i implementiranih kontrola, a upravljanje rizicima je integrirano u cjelokupni program organizacije gdje su kontrole automatizirane i nadgledane pri čemu zaposlenici su aktivno uključeni u program poboljšanja kontrola. Također, postoji napredno i unaprijed-orijentirano razumijevanje problematike i rješenja vladanja IT-om. Trening i komuniciranje je podržavano vodećim konceptima i tehnikama. Procesi se rafiniraju do razine vanjskih najboljih praksi, temeljeno na rezultatima kontinuiranog poboljšavanja i modeliranja zrelosti s drugim organizacijama. Implementiranje ovih politika dovelo je do organizacije, u kojoj se ljudi i procesi brzo adaptiraju i u potpunosti podržavaju zahtjeve vladanja IT-om. Svi problemi i devijacije su izvorno uzročno analizirani s brzom identifikacijom i iniciranjem efikasnih akcija. IT se koristi na ekstenzivan, integriran i optimiziran način za automatiziranje tijeka rada i pruža alate za poboljšavanje kvaliteta i učinkovitosti. Vladanje tvrtkom i IT-om je strateški povezano, iskorištavajući tehnologije u ljudske i financijske resurse za povećavanje konkurentske prednosti tvrtke.

Ocjene dobivene primjenom modela zrelosti pomažu stručnjacima da objasne menadžmentu gdje su slabe točke u upravljanju informatičkim procesima i koje su potrebne akcije da bi se postigli zadovoljavajući nivoi ocjena. Naravno, postoje i kritični procesi kojima se mora upravljati na sigurniji način nego s manje kritičnima, što će opet ovisiti o riziku koji je neka kompanija spremna svjesno preuzeti.

U COBIT specifikacijama je definirana tabela modela zrelosti koja za svaku od pet ocjena definira stanje atribute „zrelosti“, pomoću kojih se određuje ocjena. Ti atributi su slijedeći:

- svijest o potrebi upravljanja procesima i komunikacija (eng. *Awareness and Communication*),
- pravila, standardi i procedure (eng. *Policies,Standars,Procedures*),
- ekspertiza i vještine (eng. *Skills and expertise*),
- nadležnost i glavna odgovornost (eng. *Responsibility and Accountability*) i
- postavljanje cilja i mjerenje (eng. *Goal setting and Measurement*).

U fokusu COBIT-ovog modela zrelosti su pored ostaloga definirane i mogućnosti upravljanja informatičkim procesima gdje ocjenjivanje ocjenama od 0 do 5 nije zamišljeno kao neki formalni proces ocjenjivanja koji koristi određene diskretne vrijednosti i pragove koji trebaju biti zadovoljeni pri dodjeljivanju neke ocjene. Ocjenjivanje se bazira na zadovoljavanju opisanih mogućnosti koje najbolje pristaju uz procese neke kompanije, pri čemu treba u obzir uzimati sva tri aspekta “zrelosti“- mogućnost, performanse i kontrola. Poboljšanje ocjene zrelosti smanjuje rizik, ishod informatičkih procesa je predvidiv, povećava se efikasnost i smanjuje se broj grešaka pri cjenovno uravnoteženoj upotrebi IT resursa.

4. Opis procesa u COBIT-u

4.1. Slika informatičkog sustava u kojem je primijenjen COBIT

Okvir definiran COBIT-om se može predstaviti trodimenzionalnim prostorom odnosno kockom koja sumira sve što je definirano COBIT okvirom. Kocka upravo predstavlja integralni prostor koji međusobno povezuje ciljeve, resurse i aktivnosti, tako da se tri dimenzije kocke odnose na međusobno povezane poslovne zahtjeve, informatičke resurse i informatičke procese. Tako se može kazati da se tri dimenzije kocke odnose na

- ***ostvarenje poslovnih ciljeva koji generiraju poslovne zahtjeve:***
  - učinkovitost,
  - tajnost,
  - integritet,
  - dostupnost,
  - pouzdanost i
  - usklađenost;
- ***koji se mogu ostvariti informatičkim procesima:***
  - koji su podijeljeni u domene i
  - za čiju implementaciju su potrebne određene aktivnosti;
- ***pri čemu se informatički procesi odnose na resurse:***
  - aplikacije,
  - informacije,
  - infrastrukturu i
  - ljudi.

Model definiran COBIT-om koji je podijeljen na domene može također biti prikazan petljom u kojoj se nalaze sve četiri domene sa svojim definiranim procesima.

4.2. Način opisa procesa

COBIT specificira procese po domenama, a za svaki je proces opisano slijedeće:

- opći opis procesa u kaskadnom obliku,
- detaljne kontrole,
- upute za mjerenje i
- model zrelosti.

COBIT specifikacije se sastoje od uvodnog dijela i nakon toga slijede opisi svakog pojedinog procesa što predstavlja glavninu publikacije, pri čemu je svaki opis procesa podijeljen u četiri sekcije.

4.2.1. Prva sekcija publikacije

Opis procesa je dan pomoću kaskadnog prikaza koji slijedi nakon definicije procesa gdje se uglavnom govori o tome zašto je proces potreban odnosno čemu i kome će služiti. Kaskadni prikaz je isti za sve definirane procese i ima slijedeći izgled:

Kontrola procesa
ime procesa
koji zadovoljava poslovne ciljeve
nabrojeni poslovni ciljevi (može ih biti više)
fokusirajući se na
nabrojeni najvažniji informatički ciljevi
koji mogu biti ostvareni pomoću
nabrojene glavne kontrole
i mogu biti mjereni
nabrojena metrika

Na istoj stranici su prikazani informatički kriteriji na koje taj proces ima utjecaj, odnosno kakav utjecaj proces ima na efikasnost, tajnost, integritet, dostupnost, skladnost i pouzdanost. Utjecaj procesa na njih može biti primaran i sekundaran. U opisu procesa je također navedeno na koja područja upravljanja je fokusiran proces pri čemu njegov utjecaj može biti primaran i sekundaran. Područja upravljanja su:

- strateško usklađivanje,
- upravljanje resursima,
- upravljanje rizikom i
- mjerenje performansi.

Isto tako su definirani informatičke resursi (aplikacije, informacije, infrastruktura, ljudi) na koje se odnosi opisivani proces.

4.2.2. Druga sekcija publikacije

U drugoj sekciji su opisani detaljni ciljevi kontrola (eng. *Detailed Control Objective*) za drugu skupinu procesa. U ovom dijelu publikacije su točno definirani načini kontrole koje je potrebno primijeniti u praksi kako bi se procesi što lakše kontrolirali.

4.2.3. Treća sekcija publikacije

Treća sekcija se odnosi na upute za upravljanje (eng. *Management guidelines*) koje su podijeljene u tri podsekcije.
U prvoj podsekciji_opisani su ulazi i izlazi za neki proces, odnosno tabelarno su prikazane oznake pojedinih procesa i njihovi rezultati koji se koriste kao ulazi za opisivani proces, a isto tako su tabelarno prikazani rezultati (izlazi) opisivanog procesa koji mogu bili ulazi drugim procesima. Tako je na primjer, u jednoj tabeli, za proces PO1 – „Definiraj strateški IT plan“ navedeno da je jedan od njegovih ulaza procjena rizika koja je izlaz iz procesa PO9.
U drugoj podsekciji je prikazana tabela aktivnosti i funkcija, tzv. RACI (eng. *Responsible, Accountable, Consulted and Informed*) tabela kojom su opisane odgovornosti delegirane pojedinim osobama u procesu izvođenja akcija. Budući da tabela vrlo jasno prikazuje odgovornosti pojedinih ljudi (pozicija), primjenom RACI tablica definiranih COBIT-om se može osigurati potpuno izvođenje akcija, a isto tako i njihovo uklapanje u cijeli sustav obzirom na činjenicu da su RACI tablicom definirane i funkcije koje moraju biti konzultirane i informirane.
Funkcije koje se mogu pojaviti u RACI tabeli mogu biti slijedeće:

- generalni direktor - CEO (eng. *Chief Executive Officer*),
- direktor financija - CFO (eng. *Chief Financial Officer*),
- poslovni direktori,
- direktor informatike - CIO (eng. *Chief information Officer*),
- vlasnici poslovnih procesa,
- voditelji produkcije,
- glavni arhitekt informatičkog sustava,

- voditelji projekata - PMO (eng. *Project Management Officer*) i
- revizori, stručnjaci za sigurnost i svi oni koji se ne bave operativnim radom.

Odgovornost pojedine osobe je neku akciju je označena slovom R,A,C ili I, što znači:

- R – nadležan za izvođenje (eng. *responsible*),
- A – glavni odgovoran (eng. *accountable*),
- C – konzultiran (eng. *consulted*),
- I – informiran (eng. *informed*).

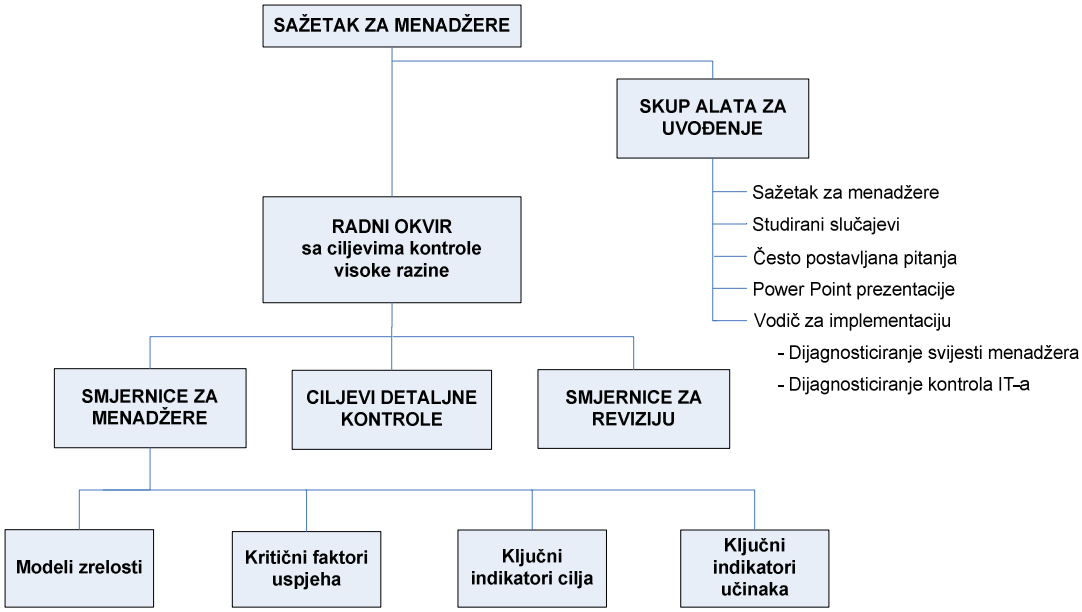
Treća podsekcija se odnosi na metriku, te su za svaki proces definirani ciljevi akcija, procesa i generalni informatički ciljevi na koje se neki proces odnosi. Za svaki od tri cilja definirana je metrika, odnosno indikatori postizanja ciljeva (KGI), koji su ujedno i KPI indikatori performansi višeg cilja.

4.2.4. Četvrta sekcija publikacije

Četvrta sekcija odnosi na model zrelosti i u njoj se na deskriptivan način opisuju uvjeti koji moraju biti ispunjeni da bi neki proces dobio ocjenu od 0 do 5, što je detaljnije analizirano u prijašnjim poglavljima.

5. Evolucija COBIT-a

Očekuje se da će COBIT evoluirati tijekom godina i biti temelj daljnjem istraživanju. Time će se kreirati obitelj COBIT produkata i kada se to dogodi, IT zadaci i aktivnosti koji služe kao struktura za organiziranje ciljeva kontrole bit će poboljšani te tako balansirati između domena i procesa promatranih u svijetlu promjenjivog krajolika industrija.



Slika 7: COBIT obitelj produkata

6. Zaključak

Publikacija „*Control Practices*“ opisuje oko 1600 praksi koje proširuju hijerarhiju COBIT-a tipa „Domena-Proces-Cilj kontrole“. Ako ciljevi kontrola opisuju što treba napraviti, tada skup praksi („Control practice set“) za određeni cilj kontrole opisuje put kojim se dolazi do cilja. Stoga je primjena COBIT radnog okvira moguća u praksi te COBIT ne predstavlja apstraktan model jer su detaljno specificirane prakse za njegovu implementaciju. Isto tako se može kazati da bi bilo nemoguće primijeniti te prakse obzirom na njihov veliki broj, bez da se ima na umu radni okvir definiran COBIT-om koji daje sistemski pogled na cijelu problematiku.

Za COBIT je važno napomenuti da omogućava implementaciju upravljanja informatičkim sustavima i kao takav obuhvaća šire područje informatike, a ne samo područje informatičke sigurnosti. Ako promatramo povijest COBIT-a, moguće je zaključiti da je imao svoj razvojni put na kojem je bio nadopunjavan i usklađivan s ostalim standardima koji se bave sličnom problematikom i rezultat je prakse brojnih stručnjaka. Na kraju, za COBIT se može kazati da je kvalitetan alat jer omogućava primjenu dobre prakse u upravljanju i izgradnji informatičkih sustava.

Ipak, iako primjena COBIT-a može doprinijeti razvoja COBIT-a, važno je istaknuti i nedostatke COBIT-a koji se očituju u kompleksnost i potrebi savladavanja metodologije.

7. Reference

[1] Cobit4.0, ITGI, 2005, ISBN-1-933284-37-4
[2] Cobit4.0 Brochure, ITGI
[3] Cobit security baseline,ITGI, 2004, ISBN-1-83209-89-2
[4] A COBIT Primer, Sandia National Laboratories, 2005
[5] ISACA, http://www.isaca.org