Centar Informacijske Sigurnosti

COBIT Framework 5

lipanj 2012.

CIS-DOC-2012-06-051

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

U današnjim tržišnim okolnostima neprijeporna je činjenica kako se sve veći dio poslovanja odvija uz potporu informacijskih sustava. Informacijski sustavi često menadžmentu predstavljaju tzv. 'crnu kutiju' o kojoj vrlo malo znaju, a još je teže nadziru i upravljaju. Zbog toga se tema nadzora i revizije informacijskih sustava u današnje 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 pogrešnim strategijama. Često smo također svjedoci pogrešno postavljene ili slabo učinkovite informacijske infrastrukture koja nije prilagođena potrebama poslovanja i strateškim ciljevima. Upravo zbog toga iziskuju se dodatni nepotrebni troškovi te se stvaraju nepremostivi problemi. Dileme oko upravljanja informacijskim sustavima nikako se ne mogu smatrati samo tehničkim već i poslovnim pitanjima, pri čemu koncept revizije i upravljanja informacijskim sustavima predstavlja kariku koja spaja menadžment i informatiku.

COBIT metodologija donosi novi koncept upravljanja i revizije informacijskih i komunikacijskih sustava koja prati njegovu evoluciju i razvoj od podrške reviziji financijskih izvještaja do samostalne upravljačke i savjetodavne funkcije. Ova metodologija se koristi u cijelom svijetu pri oblikovanju i provedbi poslovnih i informacijskih procesa. Ovim radnim okvirom definira se pojam korporativnog upravljanja informacijskim i komunikacijskim sustavima.

U prvom poglavlju dokumenta opisan je radni okvir COBIT 5 te su navedene najvažnije publikacije vezane uz taj radni okvir. U drugom poglavlju opisan je opseg metodologije COBIT te poslovna orijentacija ovog radnog okvira. Nakon toga opisana je organizacija radnog okvira COBIT. U četvrtom poglavlju opisani su procesi te je objašnjen način opisivanja procesa. U zadnjem, petom, poglavlju navedeni su dodatni paketi koji čine zaokruženi skup radnog okvira zajedno s COBIT-om.

2. COBIT Framework 5

Radni okvir COBIT (eng. Control *Objectives for Information and related Technology, COBIT*) Framework 5 opisuje način provedbe upravljanja informacijskim i komunikacijskim tehnologijama (eng. *Information and Communication Technology, ICT).* Poslovni procesi mnogih organizacija uvelike ovise o pouzdanoj i dobroj funkcionalnosti njihovih informacijskih sustava. Zbog toga je osnovana neprofitna institucija ITGI (eng. *Information Technology Governance Institute, ITGI*) s ciljem donošenja i poboljšanja standarda te izdavanje publikacija koje se odnose na problematiku upravljanja ICT sustavima. Sljedeća slika prikazuje logo organizacije ITGI.

Slika 1. *Logo organizacije ITGI*
Izvor: *ITGI*

Institucija ITGI osnovala je neprofitnu organizaciju ISACA (eng. *Information System Audit and Control Association, ISACA*), koja je započela s radom 1963. godine. Članovi te organizacije su stručnjaci iz područja upravljanja, ispitivanja, revizije i sigurnosti informacijskih tehnologija. Slika 2 prikazuje logo organizacije ISACA.[8]

Slika 2. *Logo organizacije ISACA*
Izvor: *ISACA*

Elementi važni za opstanak i uspjeh organizacije su učinkovito upravljanje informacijskim i komunikacijskom tehnologijama, a oni se očituju u:

- povećanju zavisnosti o informacijama te informacijskim i komunikacijskim tehnologijama,
- povećanju ranjivosti i širokom spektru prijetnji takvim tehnologijama,
- povećanim troškovima u postojeće sustave i porast investicija u nove ICT sustave,
- promjeni rada i poslovne prakse organizacije,
- stvaranju novih poslovnih prilika te
- reduciranju troškova.

Izvorno je prva inačica COBIT-a iz 1996. godine nastala kao alat za podršku provedbe revizije financijskih izvještaja. Radni okvir CobiT se vrlo brzo razvijao i pratio razvoj uloge informacijskih sustava u poslovanju te je druga inačica (iz 2000. godine) već u svjetskim razmjerima postala najkorišteniji okvir ispitivanja i provjere informacijskih sustava. Treća inačica, iz 2004. godine, je predstavljala integralni okvir upravljanja informatikom. Inačica COBIT 4 predstavljala je najvažniji okvir provedbe koncepta korporativnog upravljanja informatikom, a izdana je 2005. godine. Najnovija inačica - COBIT 5, izdana je 2012. godine. COBIT sadrži 5 područja, 37 ključna informatička procesa (cilja provjere), preko 300 detaljnih informacijskih provjera, 18 aplikacijskih i 6 procesnih provjera.[5]

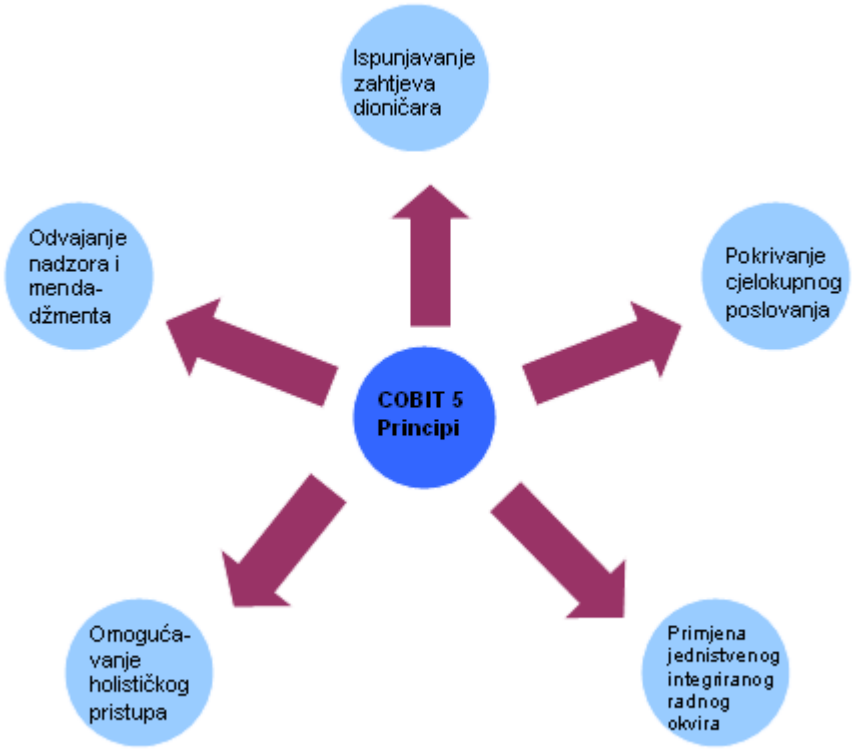
COBIT 5 objedinjuje i integrira COBIT 4.1, Val IT 2.0 i Risk IT okvir i izvodi se iz ISACA IT sigurnosnog okvira (eng. *ISACA IT Assurance Framework, ITAF*) i Poslovnog modela za

informacijsku sigurnost (eng. *Business Model for Information Security, BMIS*). Uključuje okvire i standarde kao što su Biblioteka za IT infrastrukturu (eng. *Information Technology Infrastructure Library, ITIL*), Međunarodna organizacija za normizaciju (eng. *International Standardization Organization, ISO*), Projekt menadžmenta za znanje (eng. *Project Management Body of Knowledge, PMBOK*), PRINCE2 i Radni okvir skupine za arhitekturu (eng. *Open Group Architecture Framework, TOGAF*).[8]

COBIT definira radni okvir upravljanja informacijskim i komunikacijskim tehnologijama tako da je zadovoljeno sljedeće:

- Poslovni procesi organizacije su u skladu s arhitekturom i funkcijom ICT sustava.
- Smanjeni su rizici koji nastaju neispravnim ili nepotpunim postavkama ICT sustava.
- Omogućeno je upravljanje rizicima ICT sustava na zadovoljavajući način.
- Omogućeno je korištenje informacijskih resursa na racionalan i učinkovit način.

Sljedeća slika prikazuje 5 principa po kojima funkcionira COBIT.

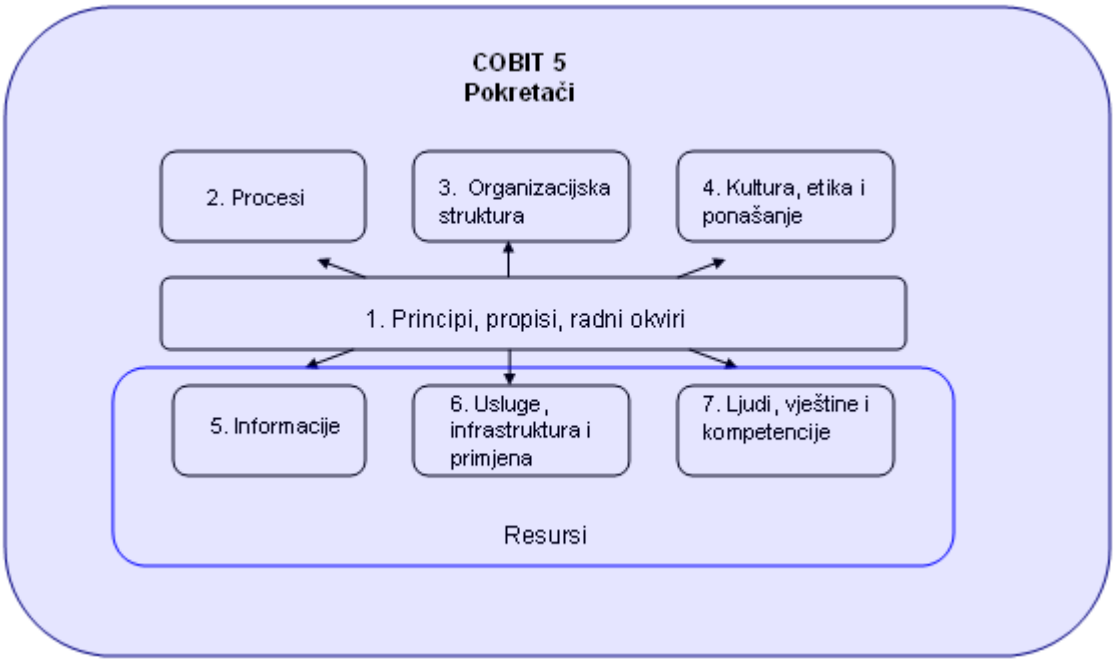


Slika 3. *Principi COBIT-a*
Izvor: *CIS*

Novi radni okvir veću pažnju pridaje pokretačima (eng. *enablers*). Oni su podijeljeni u 7 kategorija:

1. principi i politike upravljanja u radnom okviru (eng. *principles, policies, frameworks*),
2. procesi (eng. *processes*),
3. organizacijska struktura (eng. *organizational structures*),
4. kultura, etička pripadnost i ponašanje(eng. *culture, ethics, behavior*),
5. informacije (eng. *information*),
6. usluge, infrastruktura i primjena (eng. *services, infrastructure, application*) i
7. ljudi, vještine, kompetencije (eng. *people, skills, competencies*).

Na sljedećoj slici prikazani su pokretači u radnom okviru COBIT 5.



Slika 4. *Pokretači prema radnom okviru COBIT*
Izvor: *CIS*

Radni okvir COBIT omogućuje integraciju poslova vezanih za nadzor poslovnih procesa, problematiku poslovnog rizika, oblikovanje komunikacijskih kanala te razinu nadzora prema potrebama vlasnika tvrtke. Moguć je razvoj dobrih politika i poslovnih praksi ispitivanja sustava ICT u organizacijama. COBIT upravama i vlasnicima tvrtki omogućuje:

- lakše razumijevanje koncepta upravljanja ICT sustavima,
- definiranje odgovornosti koje su potrebne za kvalitetnu integraciju ICT sustava,
- usklađivanje sustav s regulatornim obvezama i
- organiziranje aktivnosti unutar ICT sustava na prihvatljiv način.

COBIT Framework 5 omogućuje optimizaciju informacijskih resursa kao što su programski paketi, informacije, infrastruktura i ljudi. COBIT preporuča praksu koja je proizvod rada mnogih stručnjaka i proizvod je dobre prakse, primjenjive u bilo kojoj organizaciji.

Ovaj radni okvir definira generički model informacijskih i komunikacijskih procesa koji se mogu pojaviti u jednom ICT sustavu. Na taj način opisuje model rada informacijskog sustava poslovnom i informacijskom menadžmentu. Kako bi se uspostavilo uspješno upravljanje njime, menadžment mora primjeniti potrebne provjere koje su propisane za sve COBIT-om definirane informacijske procese. Budući da su ciljevi primjene nadzora unutar COBIT-a organizirani po IT procesima, tada okvir zapravo daje stvarnu vezu između primijenjenih provjera, procesa i upravljanja ICT sustavima.[2]

Potrebno je definirati značenje pojedinih termina koji se u COBIT publikacijama često upotrebljavaju:

- **nadzor i provjera** (eng. *control*) – sigurnosna politika, procedure i prakse koje osiguravaju ostvarivanje poslovnih ciljeva te smanjeno ili uklonjeno pojavljivanje neželjenih događaja;
- **kontrolni cilj** (eng. *control objective*) – očekivani rezultat ili svrha primjene određene provjere;
- **proces** – kontrolni cilj više razine (eng. *high level control objective*).

2.1. COBIT publikacije

Najvažnije publikacije vezane uz radni okvir COBIT 5 su:

- COBIT 5 Framework,
- COBIT 5 Implementation,

- COBIT 5: Enabling Processes.

Ove publikacije opisuju COBIT 5 te način primjene ovog alata u poslovnom okruženju.

COBIT donosi niz publikacija namijenjenih sljedećim sudionicima u upravljanju ICT sustavima:

- za upravu i visoki menadžment: publikaciju „*Broad Briefing on IT Governance*“ koja objašnjava problematiku upravljanja ICT sustavima i odgovornosti koje oni imaju,
- za informacijski i operativni menadžment: publikaciju „*Management guidelines*“ koja pomaže pri određivanju opsega nadzora informacijskih procesa, pri mjerenju performansi i određivanju dobrih poslovnih praksi,
- za ICT stručnjake koji se brinu o izravnoj primjeni provjera, informacijske revizore i sigurnosne stručnjake:
    - publikacija „*COBIT Framework*“ objašnjava kako COBIT organizira ciljeve upravljanja i dobru praksu upravljanja podijeljenu u domene i njima pripadajuće procese,
    - publikacija „*Control objectives*“ opisuje 5 domena, 37 procesa i više od 300 ciljeva provjera te dobru praksu u upravljanju svim aktivnostima kod ICT sustava,
    - publikacija „*Control Practices*“ opisuje dobre prakse primjenom kojih se može doći do ciljeva primjenjivanjem zadanih provjera,
    - publikacija „*IT Assurance guide*“ opisuje generički pristup reviziji ICT sustava,
    - publikacija „*COBIT Quickstart*“ definira reducirani skup provjera i procesa, a namijenjena je manjim organizacijama,
    - publikacija „*COBIT Security Baseline*“ opisuje osnovne korake pri provedbi sigurnosti informacijskih sustava, a namijenjena je prvenstveno menadžmentu,
    - publikacija „COBIT Mappings“ opisuje područja preklapanja COBIT standarda i ostalih standarda s područja upravljanja i sigurnosti ICT sustava.

Sljedeća slika prikazuje naslovnu stranicu kao i logo COBIT 5 publikacija.[5]

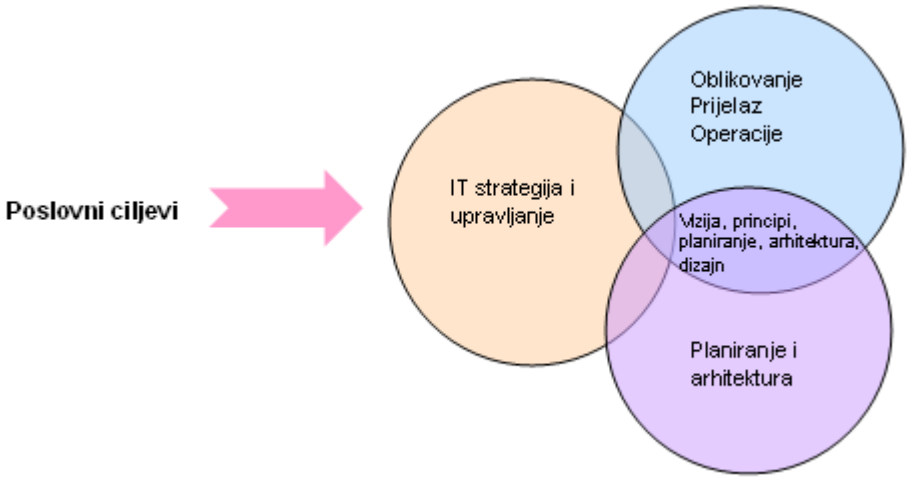
Slika 5. *Logo COBIT 5*
Izvor: *ISACA*

3. Opseg metodologije COBIT

3.1. Poslovna orijentacija

COBIT Framework 5 je poslovno orijentirana metodologija koja usklađuje informacijski sustav s poslovnim zahtjevima u svrhu postizanja poslovnih ciljeva. Kako bi se oni postigli definiran je skup generičkih, uobičajenih, poslovnih te informacijskih ciljeva. Također se definira matrica korelacije koja prikazuje odnos poslovnih ciljeva i potrebnih informacijskih alata koji vode u smjeru ostvarivanja zadanog. Jedan od mogućih poslovnih ciljeva je povrat investiranog, a provođenje ovog cilja ovisi o funkcionalnom i cjenovno primjerenom (eng. c*ost effective*) informacijskom rješenju.

Radni okvir COBIT pomaže pri procesu definiranja informacijskih ciljeva koji moraju biti usklađeni s poslovnim ciljevima kako ostarivanje i uslađivanje poslovnih ciljeva ima izravan utjecaj na arhitekturu informacijskog sustava. Zahtjevi poslovanja određuju arhitekturu informacijskog sustava i njegove mogućnosti koje imaju utjecaj na neke od kriterija kao što su pouzdanost, integritet, učinkovitost, stabilnost, cjenovni rang itd. Stoga COBIT pomaže pri definiranju rješenja koja mogu podržati zahtijevane poslovne ciljeve definirajući informatičke procese koji se oslanjaju na ljudske potencijale, informacijsku infrastrukturu i dostupne programske pakete. Na slici 6 je prikazan utjecaj poslovnih ciljeva na IT strategiju i planiranje.



Slika 6. *Utjecaj poslovnih ciljeva*
Izvor: *CIS*

3.1.1. Potreba za nadzorom

U svim organizacijama postoji potreba za radnim okvirom koji će omogućiti postizanje sigurnosti i uspješnu provjeru informacijskih i komunikacijskih sustava. Kako bi se mogući rizici mogli predvidjeti i nadzirati menadžment mora ulagati u tehnologije koje će poboljšati sigurnost i nadzor u ICT okruženju. Sigurnost i nadzor informacijskih sustava pomažu upravljanju rizicima, međutim ne uklanjaju ih. Važno je nadzirati moguće rizike, ali i donijeti odluku o prihvatljivoj razini rizika koja se može tolerirati u odnosu na troškove. Revizori stalno ulažu napore u standardizaciju kako bi mogli provoditi interne provjere u organizaciji te argumentirati svoje zaključke o razini postignutih informacijskih ciljeva. Menadžeri i revizori zajedno surađuju u donošenju odluka o ICT sustavima i postignutim razinama sigurnosti.

3.1.2. Odnosi u poslovnoj okolini

Kako bi poboljšale poslovanje i simultano iskoristile napretke na području ICT tehnologija za poboljšavanje konkurentske pozicije te postizanje svojih ciljeva organizacije se međusobno udružuju. Neki od načina poboljšanja poslovnih procesa uključuju reinženjering poslovnih procesa i načina organizacije, korištenje vanjskih organizacija (eng. *outsourcing*), distribuiranu obradu, itd. Ove promjene utječu na način odvijanja poslovnih procesa privatnih i javih organizacija. Zbog uključivanja u radni okvir i donošenja brzih promjena menadžeri, specijalisti informacijskih tehnologija i revizori nastoje se razvijati kako bi mogli pratiti novo okruženje u kojem rade. Automatiziranje funkcija u organizaciji diktira uključivanje sve jačih mehanizama provjere u informacijskom okruženju.

3.1.3. Upravljanje ICT-om

Upravljanje poslovnom tvrtkom i ICT-om nisu različite domene. Kako bi se kvalitetno upravljalo ICT-om važno je osigurati povezivanje ICT resursa i informacija sa strategijom tvrtke i pripadajućim ciljevima. Ovo se postiže integrirajući i institucionalizirajući optimalne načine planiranja i organiziranja, primjene, isporuke i podrške te nadziranjem učinaka ICT sustava. Uspješno upravljanje informacijskim i komunikacijskim sustavima dio je uspjeha prilikom upravljanja tvrtkom. Aktivnosti tvrtke zahtijevaju povratne informacije iz IT aktivnosti kako bi se ostvarili poslovni ciljevi. Uspješne organizacije osiguravaju međuzavisnost između svog strateškog planiranja i njihovih IT aktivnosti. Tvrtkama se obično vlada općenito prihvaćenim dobrim praksama kako bi se osiguralo da tvrtka ostvaruje svoje ciljeve. Osiguranje ovih ciljeva omogućeno je određenim ispitivanjima. Iz ovih ciljeva proizlazi usmjerenje organizacije, koje diktira određene aktivnosti korištenjem svojih resursa. Rezultati aktivnosti organizacije se mjere i koriste prilikom stalne revizije i održavanja nadzora, stvarajući na taj način novi ciklus.

Važno je osigurati da informacije tvrtke i tehnologije koje ona koristi podržavaju ciljeve poslovanja. Resursi se moraju primjereno koristiti te je potrebno primjereno upravljati s rizicima. Ove prakse čine temelj usmjeravanja aktivnosti ICT-a, koje se mogu karakterizirati kao planiranje i organiziranje, provedba, isporuka, podrška i nadgledanje s dvostrukom svrhom - upravljanja rizicima i ostvarivanja koristi (učinkovitost). Izvještava se o izlazima aktivnosti IT-a, koji se uspoređuju s različitim praksama i provjerama, ponavljajući ovaj proces u svakom novom ciklusu.

Kako bi menadžment mogao postići svoje ciljeve mora usmjeravati i upravljati ICT aktivnostima na način da se postigne ravnoteža između upravljanja rizicima i ostvarivanja koristi. Menadžment treba identificirati najvažnije aktivnosti, mjeriti napredak prema postizanju ciljeva i utvrditi kvalitetu obavljanja ICT procesa. Dodatno tomu, menadžment treba posjedovati sposobnost procjenjivanja stupnja zrelosti organizacije prema najboljim praksama industrije i međunarodnim standardima. Kako bi pružile podršku ovim potrebama upravljanja, COBIT smjernice za menadžment su identificirale kritične faktore uspjeha, ključne indikatore ostvarivanja cilja i učinka te pridružene modele zrelosti za vladanje IT-om.

3.1.4. Korisnici radnog okvira

COBIT Framework je dizajniran i namijenjen za:

- menadžment: radni okvir se koristi kao pomoć prilikom stvaranja ravnoteže između poslovnog rizika i investiranja u nove provjere u često nepredvidljivoj IT okolini,
- korisnici: radni okvir koriste kako bi preispitali i stekli mišljenje te pružali savjet menadžmentu o sigurnosti i provjerama IT sustava pružanih interno ili od treće strane,
- revizori: radni okvir koriste kako bi donijeli mišljenje o kvaliteti postojećeg ICT sustava te kako bi savjetovali menadžment glede internog nadzora.

3.1.5. Orijentacija na poslovne ciljeve

Radni okvir COBIT se koristi prilikom stvaranja poslovnih ciljeva. Ciljevi provjere jasno su i razdvojeno povezani s ciljevima poslovanja. Ciljevi provjere su definirani na procesno orijentiran način slijedeći principe ponovnog stvaranja i optimiziranja poslovnih procesa. Kod identificiranja domena i procesa, također je potrebno identificirati ciljeve nadzora visoke razine i razjasniti dane principe u dokumentiranju veze s ciljevima poslovanja. Potrebno je dati razmatranja i smjernice za definiranje i provođenje ciljeva provjere ICT-a. Klasifikacija područja gdje se primjenjuju ciljevi provjere visoke razine (domene i procesi), indikacija zahtjeva poslovanja s informacijama u domenama, kao i IT resursi, na koje primarno djeluju ciljevi provjera zajedno čine COBIT-ov radni okvir. Radni okvir je temeljen na aktivnostima istraživanja, koje su identificirale 37 ciljeva provjere visoke razine i 318 detaljnijih ciljeva provjere.

4. Organizacija COBIT-a

Publikacije COBIT u svom glavnom djelu govore o 37 procesa (eng. *high level control objective*) koji spadaju u pet logičkih domena. Nadalje, svaki od tih procesa je razrađen u ciljeve detaljnije provjere (eng. *detailed control objectives*) kojih ima sveukupno 318. Daljnja podjela, odnosno razrada problema odnosi se na načine primjene nadzora (eng. *control practices*) kojih ima ukupno 1547 i one su opisane u publikaciji „*Control Practices*“.

4.1. Domene i pripadni procesi

Domene i procesi predstavljaju ispravan put životnog ciklusa informacijskog rješenja, odnosno faze koje svako rješenje mora proći prilikom uvođenja u sustav i uporabu. Domene i procesi predstavljaju okvir unutar kojeg se moraju provesti sva informatička rješenja i dobar su alat onima koji se bave planiranjem, uvođenjem i korištenjem informacijskih sustava, a posao ICT revizora treba biti utvrđivanje dosljednosti primjene okvira definiranog COBIT-om.

Procesi radnog okvira COBIT 5 podijeljeni su u dva područja:

a) vladanje poslovnim IT procesima:
   - procjena, smjer, nadzor (eng. *Evaluating, Direction, Monitoring, EDM*),

b) menadžment poslovnim IT procesima:
   - planiranje i organiziranje (eng. *Align, Plan and Organize, APO*),
   - nadgledanje i evaluacija (eng. *Monitor, Evaluate and Assess, MEA*),
   - isporuka, usluga i podrška (eng. *Delivery, Service and Support*),
   - izgradnja, stjecanje i primjenjivanje (eng. *Build, Acquire and Implement*).

Domena upravljanja osigurava da se ciljevi poduzeća postižu procjenom potreba sudionika poslovnog procesa, uvjeta i mogućnosti, postavljanjem smjera tako da se oblikuju prioriteti, pravilno donose odluka, prate performanse sustava, usklađenost i napredak prema dogovorenom smjeru i ciljevima (eng. *Evaluating, Direction, Monitoring, EDM*). Procesi koji to osiguravaju su:

- EDM 1: osiguravanje postavki i održavanja okvira za upravljanje,
- EDM 2: osiguravanje beneficija,
- EDM 3: osiguravanje optimizacije rizika,
- EDM 4: osiguravanje optimizacije resursa,
- EDM 5: osiguravanje transparentnosti

Unutar domene svrstavanja, planiranja i organiziranja (eng. *Align, Plan and Organize, APO*) razrađuje se poslovna tehnologija koja je osnova za definiranje potreba ICT-a korištenjem sljedećih procesa:

- APO 1: upravljanje radnim okvirom IT menadžmenta,
- APO 2: definiranje strateškog IT plana,

- APO 3: definiranje informacijske arhitekture,
- APO 4: upravljanje inovacijama
- APO 5: upravljanje portfolijom,
- APO 6: upravljanje budžetom i troškovima,
- APO 7: upravljanje ljudskim resursima,
- APO 8: upravljanje odnosima,
- APO 9: upravljanje uslugama,
- APO 10: upravljanje dobavljačima,
- APO 11: upravljanje kvalitetom,
- APO 12: upravljanje rizikom i
- APO 13 upravljanje sigurnošću.

Unutar domene nadgledanja i evaluacije (eng. *Monitor, Evaluate and Assess, MEA*) prate se performanse i smjerovi rada sustava i poduzimaju određeni ispravci, a procesi su sljedeći:

- MEA 1: nadziranje, procjena i ocjena performansi i sukladnosti,
- MEA 2: nadziranje, procjena i ocjena sustava internog nadzora,
- MEA 3: nadziranje, procjena i ocjena vanjskih zahtjeva.

Kroz domenu isporuke, usluge i podrške (eng. *Delivery, Service and Support*) definiraju se postupci za rad programa unutar IT sustava te se pruža podrška procesima koji omogućuju učinkovit rad IT sustava. Navedeni procesi su:

- DSS 1: upravljanje operacijama,
- DSS 2: upravljanje zahtjevima usluga i incidentima,
- DSS 3: upravljanje problemima
- DSS 4: upravljanje kontinuitetom,
- DSS 5: upravljanje uslugama sigurnosti i
- DSS 6: upravljanje provjerama poslovnog procesa.

Unutar domene izgradnje, stjecanja i primjenjivanja (eng. *Build, Acquire and Implement*) identificiraju se i alociraju potrebne tehnologije za poslovne procese i definiraju se načini upravljanja kroz naredne procese:

- BAI 1: upravljanje programima i projektima
- BAI 2: upravljanje definiranim zahtjevima,
- BAI 3: upravljanje pronalaženjem rješenja i izgradnjom,
- BAI 4: upravljanje dostupnošću i kapacitetom,
- BAI 5 :upravljanje mogućnostima mijenjanja organizacije,
- BAI 6: upravljanje promjenama,
- BAI 7: upravljanje prijelazima i prihvaćanjem promjena,
- BAI 8: upravljanje znanjem,
- BAI 9: upravljanje imovinom i
- BAI 10: upravljanje konfiguracijom.[4]

4.1.1. Detaljne provjere

COBIT Framework definira generički model niza procesa koji u stvarnosti predstavljaju pojedine funkcije unutar informacijskog sustava. Na taj način pomaže stručnjacima i menadžmentu u razumijevanju i upravljanju informacijskim i komunikacijskim sustavima. Kako bi se omogućilo upravljanje ICT sustavima potrebno je uvesti provjere za sve procese unutar pojedinog sustava. U tu svrhu COBIT definira za svaki proces više detaljnih provjera koje se moraju provesti kako bi upravljanje procesom bilo moguće. Detaljne provjere (eng. *detailed controls*) se u specifikacijama označavaju s oznakom procesa i brojem provjere.

Kao primjer može se uzeti generički proces “Procjena i upravljanje rizicima ICT sustava“ i označiti ga oznakom PO9. Za provedbu ovog procesa potrebno je sljedećih šest detaljnih provjera:

- PO9.1: uključivanje procjene rizika informacijskog sustava u sustav upravljanja rizicima cijele organizacije,
- PO9.2: uspostavljanje konteksta procjene rizika,
- PO9.3: definiranje ciljeva procjene i kriterija po kojima se obavlja procjena rizika,
- PO9.4: identificiranje prijetnje,
- PO9.5: procjena utjecaja nekog događaja na ciljeve i poslovanje kompanije,
- PO9.6: procjena rizika pomoću kvalitativnih i kvantitativnih metoda.

4.1.2. Upute za upravljanje

Uz popis detaljnih provjera za svaki proces su opisani generički ulazi i izlazi, te je dana matrica potrebnih aktivnosti i odgovornosti. Definirani su ciljevi aktivnosti i metrika koja prikazuje način procjene prilikom ostvarivanja ciljeva.

Svi procesi u COBIT-u su opisani na isti način, što ce detaljnije biti objašnjeno u sljedećim poglavljima.

4.1.3. Mjerenje performansi

Radni okvir COBIT definira ciljeve i metriku kojom se mjeri razina postignuća tih ciljeva u tri razine:

1. metrika informacijskih procesa koja pokazuje u kojoj mjeri ICT sustav zadovoljava potrebe poslovanja,
2. metrika informacijskih procesa kojom se mjeri u kolikoj mjeri neki proces zadovoljava ispunjenje svoje funkcije ili cilja,
3. metrika za mjerenje performansi informacijskog procesa kojom se mjeri učinkovitost 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. *Key Goal Indicators, KGI*) postaju neki od indikatora mjerenja performansi (eng. *Key Performance Indicators, KPI*). U specifikacijama se za svaki proces definiraju tri cilja:

- cilj aktivnosti,
- cilj procesa,
- cilj ICT sustava.

Kroz ključne indikatore cilja definiraju se zahtjevi koji se trebaju nadzirati tijekom izvođenja projekta. U nastavku su navedeni glavni i izvedeni zahtjevi te načini ostvarivanja koji dovode do ispunjenja zadanih ciljeva:

- prošireni učinci i upravljanje troškovima,
- poboljšana dobit na ICT investicijama,
- skraćeno vrijeme izlaska proizvoda na tržište,
- povećana kvaliteta i inovacije
- poboljšano upravljanje rizikom,
- primjerno integrirani i standardizirani procesi poslovanja,
- dohvat novih klijenata i veće zadovoljstvo postojećih klijenata,
- raspoloživost odgovarajuće širine pojasa (eng. *bandwidth*),
- ostvarivanje zahtjeva i očekivanja proračuna vremena za proces,

- usklađenost sa zakonima, regulacijama, industrijskim standardima i ugovornim obvezama,
- transparentnost preuzetih rizika i usklađenost s ugovorenim,
- stvaranje novih kanala za isporuku usluga, itd.

Ključni indikatori performansi koji vode učinkovitijem poslovanju, a time i čestim provjerama obavljanja posla:

- poboljšani omjer troškova i učinkovitosti ICT procesa,
- povećani broj planova akcija i inicijativa za poboljšavanje procesa u IT-u,
- povećana iskoristivost IT infrastrukture,
- povećano zadovoljstvo vlasnika,
- poboljšana produktivnost osoblja (broj pruženih usluga i izdanih proizvoda),
- povećana raspoloživost znanja i informacija za menadžment tvrtke,
- povećana povezanost upravljanja tvrtkom i odijelom IT,
- poboljšana učinkovitost, itd.

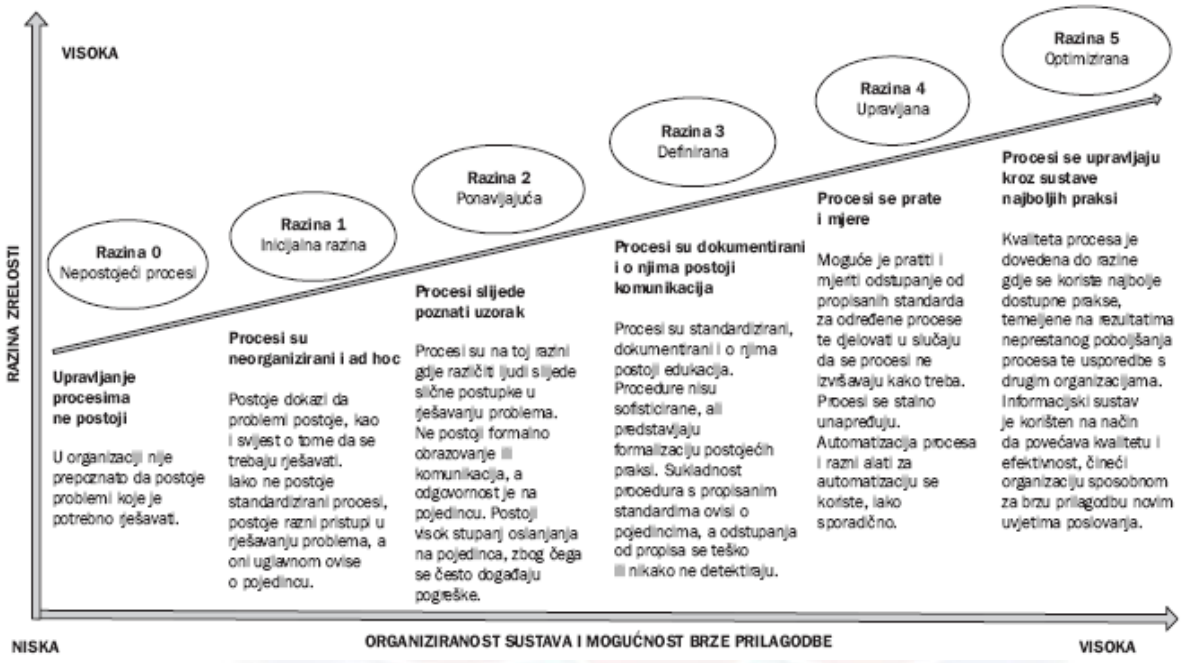
Ciljevi se po COBIT-u, definiraju po modelu odozgo prema dolje (eng. *top-down*), odnosno poslovni ciljevi definiraju broj i vrstu informacijskih procesa. Svaki informacijski proces tada definira potrebne aktivnosti za njegovo ostvarenje. Grafički prikaz metrike ide u obrnutom smjeru od najnižih aktivnosti prema ciljevima procesa te na kraju informacijskog sustava. Na primjeru metrike procesa oznake PO2: Definiranje arhitekture informacije prikazan je takav pristup:

1. Aktivnosti:
    - osiguravanje točnosti podatkovnog modela,
    - pridruživanje vlasništva pojedinim podacima,
    - klasifikacija informacija,
    - održavanje integriteta podataka,
    - održavanje konzistencije komponenti informacijske infrastrukture,
2. Aktivnosti se mjere s KGI najniže razine:
    - frekvencija ažuriranja informacijskog modela kompanije,
    - postotak podataka bez vlasnika,
    - frekvencija aktivnosti ispitivanja valjanosti podataka,
    - razina sudjelovanja korisnika u oblikovanju podataka,
3. KGI najniže razine postaje KPI kojim se mjere performanse sljedećeg višeg cilja:
    - uspostava podatkovnog modela kompanije,
    - reduciranje redundantnosti podataka,
    - uspostava učinkovitog upravljanja informacijama,
4. ispunjenje cilja mjeri sa 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 zamišljene van arhitekture ICT sustava,
5. gornji KGI postaje dio KPI kojim se mjere performanse najvišeg cilja:
    - optimiziranje korištenja informacija,
    - osiguravanje integracije aplikacija u poslovni model,
    - odgovori na poslovne zahtjeve i poslovnu strategiju,
6. ostvarenje najvišeg cilja se mjeri s KGI:
    - postotak korisnika koji su zadovoljni s ICT sustavom,
    - postotak redundantnih ili višestrukih podatkovnih elemenata.

4.1.4. Modeli zrelosti

Implementacija COBIT-a započinje procjenom cjelokupne zrelosti informacijskih procesa u organizaciji. To je početna faza koja daje prikaz trenutačnog stanja zrelosti informacijskog sustava. Na menadžmentu organizacije je da na osnovi dobivene analize odabere procese koje će dodatno promatrati i poboljšati. Vrlo poželjno svojstvo COBIT-a je mogućnost njegove selektivne primjene samo na one procese koji su u središtu interesa menadžmenta. Ako menadžment smatra da je potrebno poboljšati cjelokupni sustav na način da se uvede bolji način predlaganja informacijskih projekata, tada se može ciljano uložiti napor u unapređenje procesa PO10 Upravljanje projektima.

Sljedeća slika prikazuje moguće razine zrelosti.



Slika 7. *Prikaz određivanja razine zrelosti*
Izvor: *Hrcak.hr*

Modelom zrelosti (eng. *Maturity Model*) i njegovom primjenom se može doći do određenih poboljšanja stabilnosti prilikom nadziranja informacijskih procesa i sustava. Model definira metriku i ciljeve do kojih se dolazi mjerenjem performansi informacijskih 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 sve procese sa sljedećim ocjenama:

- 0 – **Nepostojeći** (eng. *non-existant*): upravljanje procesom nije primijenjeno. Potpun nedostatak bilo kakvih raspoznatljivih procesa vladanja IT-om. Nisu prepoznati problemi koje je potrebno rješavati,
- 1 – **Početni** (eng. *initial*): organizacija je prepoznala postojanje problema vezanih uz vladanja IT-om i potrebu rješavanja takvih problema. Nema standardiziranih procesa, već umjesto njih postoje nedefinirani pristupi primjenjivani od pojedinaca,
- 2 – **Ponavljajući** (eng. *repeatable*): Procesi su standardizirani i dokumentirani te se ponašaju na očekivani način. Definirane procedure ponavljaju različiti zaposlenici, međutim one nisu dokumentirane. Izvođenje procedura je prepušteno znanju pojedinaca. Razvija se svijest o problematici upravljanja ICT sustavima. Nema formalnog treninga i standarda upravljanja, a odgovornost je ostavljena pojedincima,

- 3 – **Definiran** (eng. *defined*): procedure su standardizirane i dokumentirane, a njihova učinkovitost izvođenja se periodično mjeri. Prihvaća se potreba za upravljanjem ICT sustavom. Menadžment komunicira standardiziranim procedurama, a uspostavljen je i neformalni trening. Indikatori učinkovitosti svih aktivnosti vladanja ICT-om se analiziraju te vode poboljšanjima širom tvrtke. Alati su standardizirani korištenjem trenutno raspoloživih tehnika,
- 4 – **Upravljan** (eng. *managed*): nadgledaju se i mjere parametri izvođenja procedura, a procesi su u stanju stalnog poboljšavanja. Većina provjera je automatizirana i redovito preispitivana. Upotreba alata za automatizaciju provjere je djelomična. Postoji potpuno razumijevanje problematike na svim razinama, podržano s formalnim treningom. 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 mogu ponuditi. Aktivnosti vladanja ICT-om postaju integrirane s procesima vladanja tvrtkom.
- 5 - **Optimiziran** (eng. *optimised*): utvrđen je cjeloviti program rizika i primjenjenih provjera, a upravljanje rizicima je integrirano u cjelokupni program organizacije gdje su provjere automatizirane pri čemu su zaposlenici aktivno uključeni u program poboljšanja nadzora. Postoji razumijevanje problematike i rješenja vladanja IT-om. ICT tehnologije se koriste na ekstenzivan, integriran i optimiziran način za automatiziranje tijeka rada te pružaju alate za poboljšavanje kvalitete i učinkovitosti. Vladanje tvrtkom i IT-om je strateški povezano, iskorištavajući tehnologije te ljudske i financijske resurse za povećavanje konkurentske prednosti tvrtke.

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

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

Pozitivni su aspekti povećanja zrelosti informacijskog sustava:

- smanjenje cijene proizvoda ili usluga,
- povećanje zadovoljstva kupaca,
- povećanje odgovornosti zaposlenih za procese,
- povećanje nadzora nad procesima,
- ukupno povećanje poslovnih rezultata poslovanja.

COBIT model za određivanje razine zrelosti informatike ima i nekoliko nedostataka. Svako povećanje razine zrelosti procesa znači i težnju za sve snažnijom provjerom i dokumentacijom. To ponekad vodi do dokumentiranja potrebnih, ali i nepotrebnih aktivnosti.

5. Opis procesa u COBIT-u

5.1. Informacijski sustav u kojem je primijenjen COBIT

Radni okvir definiran COBIT-om može se predstaviti trodimenzionalnim prostorom koji zbraja sve što je njime definirano. Ovakva kocka upravo predstavlja integralni prostor koji međusobno povezuje ciljeve, resurse i aktivnosti, tako da se tri dimenzije kocke odnose na međusobno povezane poslovne zahtjeve, informacijske resurse i procese. Tri dimenzije kocke odnose se na:

1. ostvarenje poslovnih ciljeva koji oblikuju poslovne zahtjeve:
    - učinkovitost,
    - tajnost,
    - integritet,
    - dostupnost,
    - pouzdanost,
    - usklađenost,
2. ciljevi se mogu ostvariti ICT procesima:
    - koji su podijeljeni u domene,
    - za čiju provedbu su potrebne određene aktivnosti,
3. pri čemu se informacijski procesi odnose na:
    - programske pakete,
    - informacije,
    - tehnološku infrastrukturu,
    - ljudske resurse.

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

5.2. Način opisa procesa

Radni okvir COBIT specificira procese po domenama, a za svaki je proces definirano sljedeće:

- opći opis procesa u kaskadnom obliku,
- detaljne provjere,
- upute za procjenu i mjerenje te
- 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.

5.2.1. 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 sljedeći izgled:

- nadzor procesa - ime procesa,
- poslovni ciljevi koje proces mora zadovoljiti – nabrojeni poslovni ciljevi,
- najvažniji ciljevi s područja ICT,
- način ostvarivanja ciljeva - glavne točke nadzora,

- opis evaluacije ciljeva - nabrojena metrika.

Prikazani su informacijski kriteriji na koje taj proces ima utjecaj te kakav utjecaj proces ima na učinkovitost, tajnost, integritet, dostupnost 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,
- mjerenje performansi.

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

5.2.2. Druga sekcija publikacije

U drugoj sekciji su opisani detaljni ciljevi provjera (eng. *detailed control objective*) za drugu skupinu procesa. U ovom dijelu publikacije su točno definirani načini nadzora koje je potrebno primijeniti u praksi kako bi se procesi što lakše nadzirali.

5.2.3. 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. Tablično su prikazane oznake pojedinih procesa i njihovi rezultati koji se koriste kao ulazi za opisivani proces, a isto tako su tablično prikazani rezultati opisivanog procesa koji mogu bili ulazi drugim procesima. U jednoj tablici za proces PO1 – Definiranje strateškog IT plana navedeno je da je jedan od njegovih ulaza procjena rizika koja je izlaz iz procesa PO9.

U drugoj podsekciji je prikazana tablica aktivnosti i funkcija, tzv. RACI (eng. *Responsible, Accountable, Consulted and Informed*) tablica kojom su opisane odgovornosti delegirane pojedinim osobama u procesu izvođenja akcija. Budući da tablica vrlo jasno prikazuje odgovornosti pojedinih ljudi na pojedinim pozicijama primjenom RACI tablica definiranih COBIT-om se može osigurati potpuno izvođenje definiranih akcija. Također je moguće njihovo uklapanje u cijeli sustav s obzirom na činjenicu da su RACI tablicom definirane i poslovne funkcije s kojima je potrebno obaviti savjetovanje prilikom planiranja sustava.

Sljedeće funkcije mogu se pojaviti u RACI tablici :

- generalni direktor (eng. *Chief Executive Officer, CEO*),
- direktor financija (eng. *Chief Financial Officer, CFO*),
- poslovni direktori,
- direktor IT odjela (eng. *Chief Information Officer, CIO*),
- vlasnici poslovnih procesa,
- voditelji proizvodnje,
- glavni arhitekt informacijskog sustava,
- voditelji projekata (eng. *Project Management Officer, PMO*),
- revizori, stručnjaci za sigurnost i svi oni koji se ne bave operativnim radom.

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

- R: nadležan za izvođenje (eng. *Responsible*),
- A: glavni odgovoran (eng. *Accountable*),
- C: priupitan (eng. *Consulted*),
- I: informiran (eng. *Informed*).

Treća podsekcija se odnosi na metriku, te su za svaki proces definirani ciljevi akcija, procesa i općeniti informacijski 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.

Četvrta sekcija se odnosi na model zrelosti i u njoj se opisuju uvjeti koji moraju biti ispunjeni da bi neki proces dobio ocjenu od 0 do 5.[3]

6. Dodatni paketi

Radni okvir COBIT 5 objedinjuje i integrira radne okvire COBIT 4.1, Val IT 2.0 i Risk IT za procjenu rizika i dodatne vrijednosti, a također sadrži značajke Poslovnog modela za informacijsku sigurnost i ITAF-a.

Okvir za upravljanje Val IT koristi se za stvaranje poslovne vrijednosti od ulaganja u ICT. Sastoji se od niza ideja vodilja, velikog broja procesa i najbolje prakse koja je dodatno definirana kao skup ključnih praksi upravljanja za podršku i pomoć izvršnom i upravljačkom tijelu na razini poduzeća. Najnoviju inačicu ovog okvira objavio je ITGI na temelju iskustva globalnih praktičara i akademika, te poznate prakse i metodologije. Obuhvaća procese ključne za upravljanje i prakse za tri specifična područja te uključuje IT usluge, sredstva, resurse, principe i procese za upravljanje IT portfeljem.

Val IT omogućuje poslovnim menadžerima mogućnost dobivanja veće vrijednost od ulaganja u IT, pružajući okvir upravljanja koji se sastoji od

- skupa načela,
- broj procesa skladu s tim načelima koji su dodatno definirani kao skup ključnih praksi upravljanja.

Glavna područja na koja se odnosi su:

- upravljanje vrijednosti (eng. *Value Governance*, VG prefix),
- menadžment portfolija (eng. *Portfolio Management*, PM prefix),
- investicijski menadžment (eng. *Investment Management*, IM prefix).[7]

Radni okvir Risk IT pruža sveobuhvatan prikaz s kraja na kraj (eng. *end-to-end*) svih rizika koji se odnose na korištenje ICT-a i sličnih tehnologija te temeljitu obradu upravljanja rizicima.

Radni okvir Risk IT je dio poslovanja s rizicima. Naime, poslovni rizik povezan je s primjenom, vlasništvom, poslovnim operacijama, sudjelovanjem, utjecajem i usvajanje ICT tehnologija unutar kompanije. Sastoji se od aktivnosti povezanima s informacijskim i komunikacijskim tehnologijama koji bi mogli utjecati na poslovanje. Ovo može stvoriti izazove u ispunjavanju strateških ciljeva. Upravljanje poslovnim rizicima je bitna komponenta odgovorne uprave bilo koje organizacije. Zbog njegove važnosti za cjelokupno poslovanje rizik povezan s IT tehnologijama rizika treba procijeniti i stvoriti plan predviđanja mogućih neželjenih događaja.

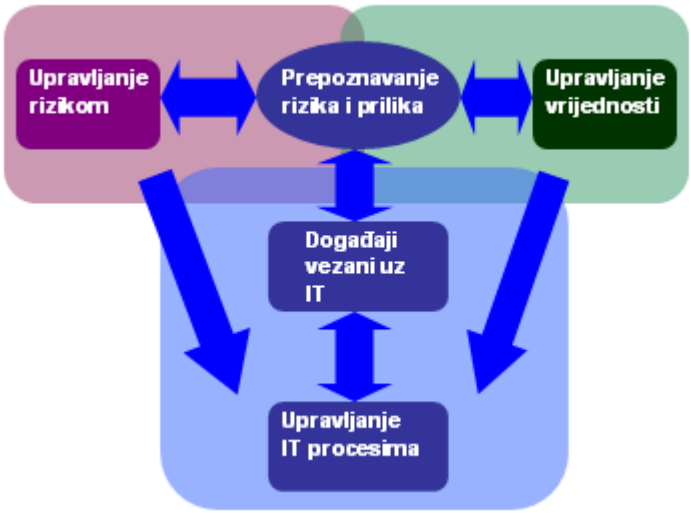
Ovaj okvir objašnjava rizik i omogućuje korisnicima:

- integraciju upravljanja IT rizikom s ukupnim menadžmentom poslovnog rizika (eng. *Enterprise Risk Management, ERM*)[1],
- usporedba procijenjenog IT rizika s razinom tolerancije rizika koju je donio menadžment organizacije,
- razumijevanje upravljanja rizikom,

Rizikom ICT sustava moraju upravljati i razumjeti svi ključni poslovnim čimbenici unutar organizacije jer on nije samo tehničko pitanje IT odjela.[6]

Sljedeća slika prikazuje međusobni odnos funkcija radnih okvira COBIT-a, Val IT i Risk IT-a.

[1] Menadžment poslovnog rizika uključuje metode i procese koji koriste organizacije za upravljanje rizicima kako bi iskoristile mogućnosti vezane za ostvarivanje njihovih ciljeva. Osigurava se okvir za upravljanje rizikom koji obično uključuje identificiranje određenih događaja ili okolnosti koje mogu biti važne za organizacije (rizici i prilike). Njihovu važnost se procjenjuje u terminima vjerojatnosti i veličine utjecaja te se utvrđuje odgovor na takav događaj i praćenje napretka.



Slika 8. *Interakcija radnih okvira*
Izvor: *CIS*

7. Zaključak

Korporativno upravljanje informacijskom tehnologijom se odnosi na okvir kojim se upravlja primjenom informatike u poslovanju, odlukama o ulaganjima u ICT sustave, performansama i rizicima korištenja takvog sustava. Također se preuzima odgovornost za provjeru i provedbu informatičkih procesa i svih IT aktivnosti. Ovo se prvenstveno odnosi na korporativnu razinu upravljanja, tj. upravu i nadzorne odbore. Time se uloga informatike kao tehničke struke mijenja, a moderne metode i okviri revizije informacijskih sustava po COBIT metodologiji menadžerima pružaju nužan aparat za upravljanje informatikom kao bilo kojom drugom poslovnom funkcijom.

COBIT Framework 5, predstavlja krovni okvir i za provedbe revizije informacijskih i komunikacijskih sustava, ali i korporativnog upravljanja takvim sustavima 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 mnogim, pa tako i hrvatskim organizacijama, 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, njihova provedba ipak i dalje nije zadovoljavajuća. Međutim, ohrabrujuće je da kod menadžera sve više raste svijest o potrebi učinkovitog upravljanja informacijskim rizicima, što reviziju informacijskih sustava čini posebno traženom samostalnom uslugom.

8. Leksikon pojmova

COBIT (eng. Control Objectives for Information and Related Technologies)

Radni okvir i metodologija rada za upravljanje i reviziju ICT sustava. Alat koji omogućava menadžerima premoćavanje jaza između zahtjeva provjera, tehničkog aspekta sustava i poslovnih rizika.

http://en.wikipedia.org/wiki/COBIT

VAL IT

Radni okvir namijenjen za stvaranje poslovne vrijednosti od IT ulaganja. Sastoji se od niza ideja vodilja i najboljih praksi koje su dodatno definirane kao skup ključnih praksi upravljanja za podršku i pomoć u kompanijama.

http://en.wikipedia.org/wiki/Val_IT

Risk IT

Radni okvir namijenjen procjeni mogućih rizika. Osigurava sveobuhvatan prikaz svih rizika koji se odnose na korištenje IT-a, temeljitu obradu upravljanja rizicima, s naglaskom na operativnim pitanjima.

http://en.wikipedia.org/wiki/Risk_IT

ICT (eng. Information and Communication Technology, ICT)

Informacijska i komunikacijska tehnologija. Obuhvaća područja telekomunikacije, računarstva i elektrotehnike. Podrazumeva tehnologije za prijenos, izmjenu i spremanje informacija te tehologije za omogućavanje komunikacije primjenom najnovijih tehničkih dostignuća.

http://en.wikipedia.org/wiki/Information_and_Communications_Technology

ITGI (eng. Information Technology Governance Institute, ITGI)

Institut za upravljanje informacijskim tehnologijama. Promovira uspješnije upravljanje ICT tehnologijama u kompanijama. Izdaje alate namjenjene upravljanju i nadzoru ICT-a te brojne publikacije.

http://www.itgi.org/

ISACA (eng. Information System Audit and Control Association, ISACA)

Organizacija za reviziju i nadzor informacijskih sustava. Glavna namjena joj je unaprijediti područje revizije i upravljanja ICT tehnologijama.

http://en.wikipedia.org/wiki/Information_Systems_Audit_and_Control_Association

ITAF (eng. ISACA IT Assurance Framework, ITAF)

ISACA IT sigurnosni okvir. Namjenjen je za nadzor i reviziju sigurnosnih aspekata informacijskog okruženja.

http://www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Pages/default.aspx

BMIS (eng. Business Model for Information Security, BMIS)

Poslovni model za informacijsku sigurnost. Ovaj model daje detaljan uvid u cjeloviti poslovni proces koji se bavi sigurnošću iz perspektive sustava.

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Model-for-Information-Security.aspx

ITIL (eng. Information Technology Infrastructure Library, ITIL)

Biblioteka za IT infrastrukturu. Predstavlja skup praksi za upravljanje IT uslugama koje su usredotočene na usklađivanje IT usluga s potrebama poslovanja.

http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

ISO (eng. International Standardization Organization, ISO)

Međunarodna organizacija za normizaciju. Razvija i izdaje međunarodne norme.

http://www.iso.org/iso/home.html

PMBOK (eng. Project Management Body of Knowledge, PMBOK)

Projekt menadžmenta za znanje. Objedinjuje skup procesa i znanja općenito prihvaćenih kao dio najboljih praksi unutar discipline upravljanja projektima.

http://www.projectsmart.co.uk/pmbok.html

PRINCE2 (eng. PRojects IN Controlled Environments 2, PRINCE2)

PRINCE2 je metoda strukturiranog projektnog menadžmenta potvrđena od strane vlade u Velikoj Britaniji kao standard upravljanja projektima namjenjen upravljanju javnim projektima.

http://en.wikipedia.org/wiki/PRINCE2

TOGAF (eng. Open Group Architecture Framework, TOGAF)

Radni okvir skupine za arhitekturu. Predstavlja okvir za arhitekturu poduzeća koji pruža sveobuhvatan pristup za projektiranje, planiranje, implementaciju i upravljanje informacijskim sustavom poduzeća.

http://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework

9. Reference

[1] COBIT:
http://www.itsm.hr/itil-itsm-metodologija/metodologija-cobit.php, lipanj 2012.
[2] COBIT 5 launched and ready:
http://thisiswhatgoodlookslike.com/2012/04/08/cobit-5-launched-and-ready-for-download/, lipanj 2012.
[3] COBIT domene i procesi:
http://www.qualified-audit-partners.be/index.php?cont=463&lgn=3, lipanj 2012.
[4] COBIT 5 – What's New?:
http://www.focus-on-training.co.uk/blog/cobit-5-whats-new, srpanj 2012.
[5] COBIT:
http://en.wikipedia.org/wiki/COBIT, srpanj 2012.
[6] Risk IT:
http://en.wikipedia.org/wiki/Risk_IT, srpanj 2012.
[7] Val IT:
http://en.wikipedia.org/wiki/Val_IT, srpanj 2012.
[8] ISACA:
https://www.isaca.org/Pages/default.aspx, lipanj 2012.