

UPRAVLJAJMO standardizirano

Svakih par godina ISACA/ITGI izdaje novu inačicu svjetski priznatog standarda CobiT. Na redu je peta iteracija. Zaslužuje li ova iteracija nositi oznaku nove inačice ili je tek manja evolucija dosad vrlo uspješnog CobiT-a 4.1?

■ DALIBOR UREMOVIC

U svjetu upravljanja informacijskim sustavima i tehnologijama postoji čitavo more smjernica i standarda. Jedan je od njih CobiT i nalazi se u onoj skupini za koju su svi čuli (drugi su poznati standardi ITIL, ISO 27002, NIST i sl.). Od tehnološki odnosno vendorski specifičnih razlikuje se time da je neovisan o korištenim IT platformama pa je samim tim primjenjiv na sve informacijske sustave, bilo da se radi o finansijskim institucijama, proizvodnim tvrtkama ili državnim neprofitnim organizacijama. Svoju reputaciju poznatog i općeprihvaćenog standarda može zahvaliti jakim institucijama koje stoje iza njega (ISACA i ITGI), sveobuhvatnosti i dugom nizu godina postojanja, a ipak uz redovito osvježavanje u skladu s novim trendovima i stanjem na tržištu.

Ove godine izašla je nova inačica standarda, CobiT 5. Na nju smo čekali punih pet godina te se s pravom pitamo ispunjava li ona naša očekivanja te je li zaslужila da nosi naziv potpuno nove inačice. Kako ćemo pročitati u članku, čini se da je to ipak slučaj. No prije nego što kreнемo na značajke nove inačice, kratak uvod u povijest nastanka i razvoja CobiT-a.

Prva inačica izašla je davne 1996. godine te je bila usmjereni uglavnom na pitanja metodologije revizije informacijskog sustava. Ovo ne čudi jer je ISACA prije svega udruga profesionalaca revizora informacijskih sustava. Kako

je, međutim, revizija morala obuhvatiti cijelovito upravljanje informacijskim sustavom, tako su se i nove inačice usmjeravale prema područjima IT upravljanja, a reviziju promatrale kao jedno od uobičajenih područja efikasnog upravljanja informacijskim sustavom. Ugrubo možemo reći da su se sljedeće inačice fokusirale na područje sustava upravljanja unutarnjim kontrolama (CobiT 2), organizacijskim strukturama i vođenju IT jedinice (CobiT 3), upravljanja informacijskim sustavom u užem smislu (CobiT 4/4.1) te upravljanja organizacijom uz jaku potporu IT-a (CobiT 5). Iako je možda teško primijetiti razliku u posljednje tri verzije, radi se o tome da je ISACA shvatila da je praktički nemoguće (i neefikasno) odvojiti upravljanje IT-om od upravljanja cjelo-

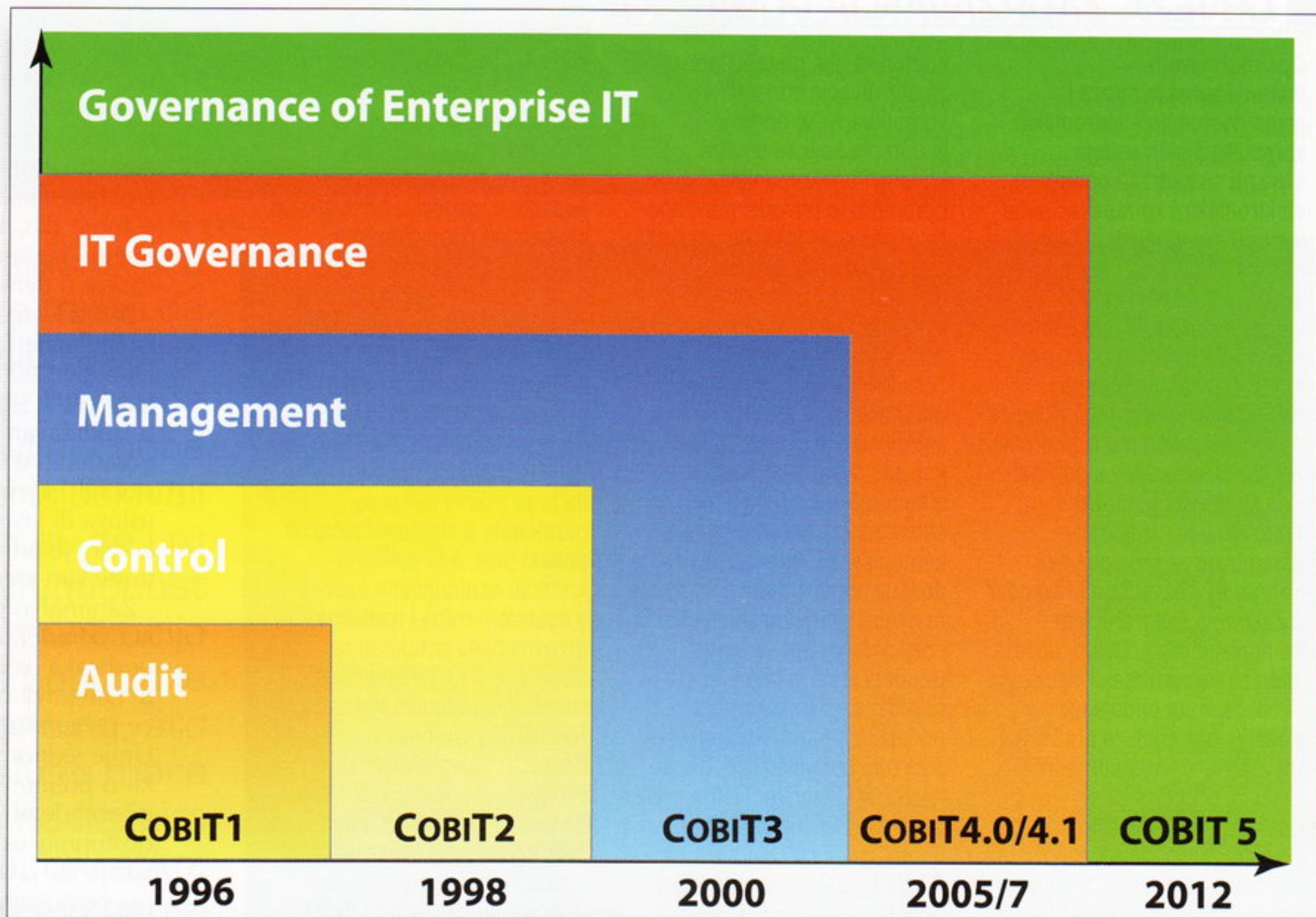
kupnom organizacijom i da je u današnje vrijeme upravo informacijska tehnologija ta koja usmjerava razvoj cijele organizacije i daje joj najveću konkurenčku prednost.

Privlačnost CobiT-a

Voditelji informatike obično se pitaju koji standard upotrijebiti kao osnovu za strateški razvoj IT jedinice u svojoj organizaciji. Razlog zbog kojeg je CobiT toliko privlačan uglavnom leži u činjenici da je on jedan od rijetkih koji stavlja jak naglasak na povezanost poslovnih ciljeva i IT ciljeva, što je još izraženije u ovoj novoj inačici.

Ova se povezanost očituje putem kašadnog modela uskladivanja ciljeva organizacije s ciljevima IT-a te obraćanjem pažnje na sve bitne sudionike (*stakeholders*) koji bitno utječu na ovu povezanost. ISACA je već davno shvatila da bez ovoga primjena novih tehnologija postaje skupa igračka, a poštivanje raznih zakonskih i regulatornih zahtjeva postaje vrlo neefikasno te se tada često čini kako je informatika sama sebi svrha i troškovni centar koji ne opravdava cilj.

CobiT polazi od koristi koje informacijska tehnologija donosi organizaciji s nekoliko ključnih ciljeva: stvoriti kvalitetne informacije koje će omogućiti pozitivne poslovne odluke, kreirati dodanu vrijednost i nove proizvode putem implementacije novih tehnologija, postići operacijsku izvrsnost putem primjene standardnih IT procesa i aktivnosti, održati prihvatljivu razinu IT rizika te optimizirati IT troškove. Kako bi se ostvarili ovi ciljevi, ISA-



Razvoj standarda kroz vrijeme i stavljanje fokusa na određene segmente

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

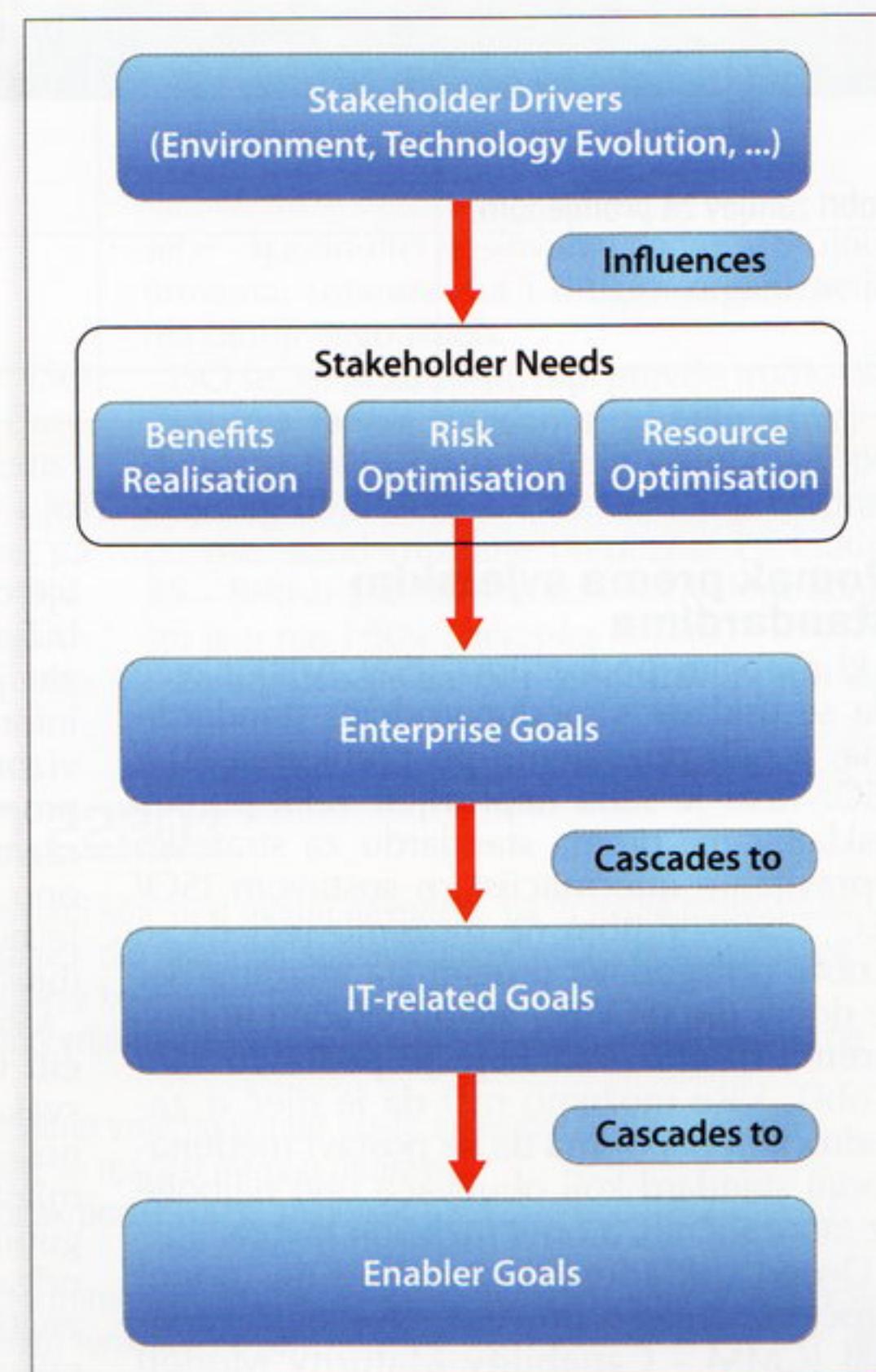
Processes for Management of Enterprise IT

Nova shema IT procesa kako je vidi CobiT

CA kaže: primijenite sveobuhvatni okvir koji pomaže organizacijama da ostvare dodanu vrijednost putem efikasnog usmjeravanja i upravljanja informacijskim sustavom, što je ništa drugo nego novi CobiT.

Što donosi nova inačica?

Skinete li s Interneta novi CobiT, čeka vas set dokumenata koje ISACA/ITGI nazivaju "obitelj proizvoda". Ukratko, radi se o glavnoj knjizi okvira CobiT 5 te o dodatnim dokumentima zvanim CobiT 5 profesionalnim vodičima (vodič za implementaciju, vodič za upravljanje rizikom, reviziju te upravljanje informacijskom sigurnošću, razni drugi vodiči) i CobiT 5 detaljnim vodičima (*enablers guides*, što je vrlo teško prevesti te dajem slobodan prijevod s obzirom na sadržaj tih vodiča). Osim ova tri seta dokumenata, dobije se i niz drugih pomoćnih alata za implementaciju CobiT-a u vidu raznih MS Excel tablica, PowerPoint prezentacija i sl. pod zajedničkim nazivom CobiT 5 Toolkit. Da biste sve ovo skinuli, trebate se registrirati na ISACA-inoj stranici. Nakon uvida u sve ove dokumente možemo s pravom zaključiti da je



CobiT potpuno nova inačica standarda, a glavne značajke, odnosno razlike u odnosu na prethodni standard (CobiT 4.1, op. a.) navedene su u nastavku članka.

Vjerojatno najbitnija razlika odnosi se na činjenicu da je puno veći prostor sada posvećen procesima upravljanja odnosno usmjeravanja razvoja IT-a i poravnjana s poslovnim ciljevima organizacije. Tako sada imamo još jednu potpuno novu domenu uz već postojeće četiri - Vrednuj, usmjeruj i nadziri (*Evaluate, Direct and Monitor*). Ova domena sadrži nekoliko strateških procesa koji su dosad bili razbacani po ostalim domenama, prije svega prvoj i četvrtoj (PO - Plan and Organize, ME - Monitor and Evaluate). Osim već postojećih procesa iz prethodne inačice, uklopljeni su procesi koji pojašnjavanju ostvarivanje dodane vrijednosti i upravljanje IT rizicima. Ovi su procesi dosad bili izdvojeni u posebne knjige nazvane Val IT i Risk IT. Više ne govorimo o 34 procesu, već o njih 37, ali redizajniranih tako da daju puno više nego što se to čini pro-

Povezivanje poslovnih i IT ciljeva osnova je primjene ovog standarda

■ INFORMACIJE KOJE PRUŽA NOVI COBIT (detaljni vodič za procese)

Dokumentacija koju dobijete kad skinete novi CobiT prilično je opširna te vrlo detaljna. Dolje prikazani primjer odnosi se samo na jednu aktivnost od njih više stotina koje su raspoređene na 37 IT procesa. Riječ je o izvatu koji je skraćen kako bi se pokazala obrađena poglavija. U stvarnosti je ova tablica puno detaljnija.

IZGRADI, NABAVI I IMPLEMENTIRAJ (BAI06 UPRAVLJANJE PROMJENAMA)																									
PODRUČJE																									
Opis procesa i cilj	Upravlja svim promjenama na kontrolirani način, uključujući standardne i hitne promjene vezane uz poslovne procese, aplikacije i infrastrukturu. Ovo uključuje standardne aktivnosti bilježenja promjena, procjenu utjecaja, rangiranje i odobrenje promjena, praćenje i izvješćivanje o promjenama te dokumentiranje. Omogući brzu i pouzdanu isporuku promjena uz izbjegavanje negativnog rizika na stabilnost informacijskog sustava u cijelini.																								
Ciljevi i metrike	1. Odobrene promjene napravljene su na vrijeme i uz minimalne pogreške 2. Procjena utjecaja promjene pokazuje na sva mesta na koja je potrebno pripaziti prilikom implementacije promjene 3. Sve su hitne promjene pregledane, naknadno odobrene i dokumentirane 4. korisnici obuhvaćeni promjenom informirani su o promjeni		<ul style="list-style-type: none"> • Količina bugova zbog primjene promjene • Smanjenje vremena obrade zahtjeva za promjenom • Broj i količina zapisa o promjenama • Postotak neuspjelih implementacija promjena • Postotak hitnih promjena u ukupnom broju promjena • Broj neodobrenih hitnih promjena • Zadovoljstvo korisnika IT podrškom za područje upravljanja poslovnim promjenama 																						
Detaljni opis aktivnosti	BAI06.01 Vrednuj, odredi prioritete i odobri zahtjev za promjenom. Vrednuj sve zahtjeve za promjenom kako bi odredio utjecaj na poslovne procese, IT servise i prepoznao rizike. Uvjeri se da su promjene zabilježene, rangirane, kategorizirane, procijenjene i planirane za implementaciju. BAI06.02 itd.	BAI03.05 DSS02.03 itd.	Konfiguracija komponenata Zahtjev za promjenom itd.	Procjena utjecaja Odobren zahtjev za promjenom itd.	BAI06.02 BAI07.01 itd.																				
Aktivnosti	1. Uvjeri se da vlasnici poslovnih procesa i IT servisa mogu podnosi formalne zahtjeve za promjenom. Svi zahtjevi za promjenom moraju proći formalnu proceduru bilježenja. 2. Kategoriziraj sve zahtjeve za promjenom (npr. poslovni proces, aplikacija, operacijski sustav, mrežne promjene i sl.) te poveži s konfiguracijskim postavkama. 3. Rangiraj sve zahtjeve prema poslovnoj važnosti, traženim resursima i zakonskim i drugim obavezama. 4. Itd.																								
RACI matrica	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Aktivnost</th><th>Vlasnik poslovnog procesa</th><th>Ured vođenja projekata</th><th>Risk manager</th><th>CIO</th></tr> </thead> <tbody> <tr> <td>BAI06.01 Vrednuj, odredi prioritete i odobri zahtjev za promjenom.</td><td>R</td><td>C</td><td>C</td><td>R</td></tr> <tr> <td>BAI06.02 Upravlja hitnim promjenama.</td><td>I</td><td></td><td>C</td><td>R</td></tr> <tr> <td>Itd.</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>	Aktivnost	Vlasnik poslovnog procesa	Ured vođenja projekata	Risk manager	CIO	BAI06.01 Vrednuj, odredi prioritete i odobri zahtjev za promjenom.	R	C	C	R	BAI06.02 Upravlja hitnim promjenama.	I		C	R	Itd.								
Aktivnost	Vlasnik poslovnog procesa	Ured vođenja projekata	Risk manager	CIO																					
BAI06.01 Vrednuj, odredi prioritete i odobri zahtjev za promjenom.	R	C	C	R																					
BAI06.02 Upravlja hitnim promjenama.	I		C	R																					
Itd.																									

matrajući samo broj procesa u standardu. U detaljnim je vodičima ovaj novi procesni model uskladen s filozofijom kaskade ciljeva pa je tako moguće naći detaljne opise svih procesa (i aktivnosti svakog od procesa, što do ove inačice nije bio slučaj), mapiranja poslovnih i IT ciljeva, ulaze i izlaze procesa i aktivnosti, RACI matrice za svaku od aktivnosti, prijedlog metrika za praćenje efikasnosti i sl. Pravo bogatstvo informacija za voditelje informatike. Sve što treba napraviti jest iskoristiti te informacije kao besplatno znanje koje se nudi nadohvat ruke. Osim gore navedenih informacija, dane su tablice mapiranja na Val IT, Risk IT i stari CobiT kako bi organizacija lako migrirala aktivnosti s već odradenim naporima uskladijanja s CobiT-om.

Pomak prema svjetskim standardima

U mnogim područjima, ISACA/ITGI teže da se usklade s međunarodnim standardima, a njih poznajemo po prefiksima ISO/IEC. Tako je sada napravljen velik pomak uskladijanja prema standardu za strateško upravljanje informacijskim sustavom ISO/IEC 38500. Pritom ne možemo reći da se CobiT prilagođava drugim standardima jer je dobar dio ISO/IEC 38500 izrađen upravo prema trendovima koje je postavio sâm CobiT. Više možemo reći da je riječ o zajedničkim naporima da se postavi međunarodni standard koji obuhvaća ono najbolje iz mora sličnih, a opet različitih izvora.

Drugo usklajenje odnosi se na model procjene zrelosti procesa. Dosadašnji model (CMM - Capability Maturity Model)

vjerojatno je najprihvaćeniji dio bivšeg CobiT-a koji su koristile mnoge naše organizacije, prvenstveno pri obavljanju revizije informacijskog sustava i ocjeni koju su rezizori davali za svaki od procesa, odnosno promatranih područja. Sada je ovaj model razrađen po više atributa, a upravo je to ono što je nedostajalo bivšem modelu te je uskladen sa standardom ISO/IEC 15504 (bivši SPICE).

Možemo li za kraj reći isplati li se proučiti CobiT 5 i primjeniti ga? Odgovor je: svakako i bez ustezanja. Ovaj standard donosi toliko korisnih informacija na jednom mjestu da je vrlo neodgovorno i neefikasno gubiti vrijeme na otkrivanje tople vode i odgadanjem primjene ovakvih svjetski priznatih praksi. Skinite još danas svoj primjerak novog CobiT-a.