

Kontrolni okvir i okruženja u informacionoj bezbednosti



Jovan Bogićević – Cybersecurity Consultant

Jovan.bogicevic@rs.ey.com



The better the question. The better the answer.
The better the world works.



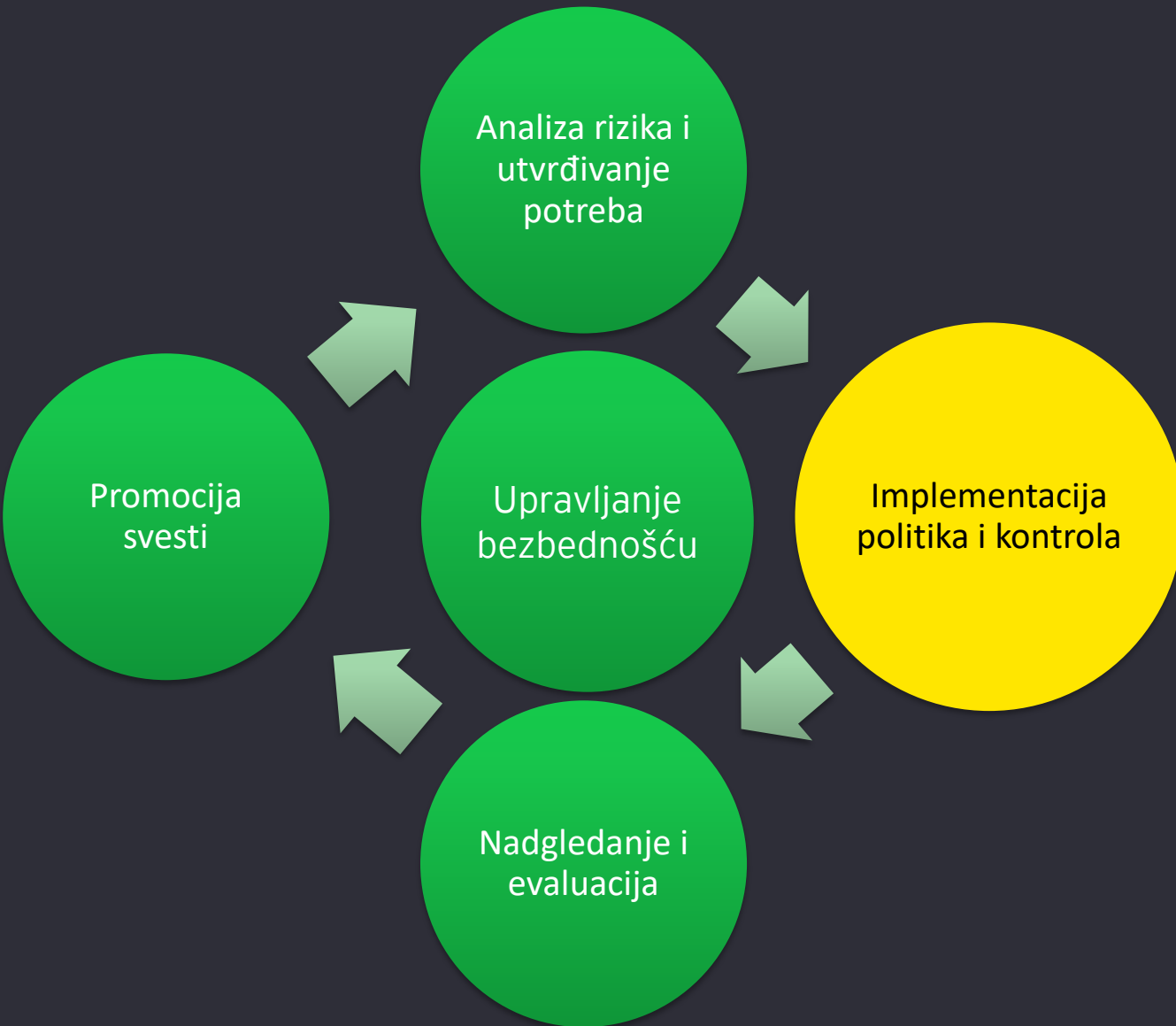
Agenda predavanja

- **Kontrolni okviri**
 - Osnovni elementi kontrolnog okvira
 - Ključne komponente
 - Kontrole
 - Kontrolni okviri
 - Korišćenje kontrolnog okvira za ispunjenje zahteva regulative
- **COBIT i ISO27001**
 - Pregled okvira
 - Oblasti i kontrole
- **Zadatak za vežbe**

Kontrolni okviri



Upravljanje informacionom bezbednošću (eng. Security governance)



Upravljanje bezbednošću osigurava da su rizici identifikovani i da je adekvatno kontrolno okruženje uspostavljeno radi ublažavanja rizika.

Upravljanje bezbednošću obezbeđuje međusobne odnose između:

- procene rizika
- sprovođenje politika i kontrola kao odgovor na identifikovane rizike
- praćenje efikasnosti kontrola
- promovisanje svesti o očekivanjima

Kontrolni okviri i kontrole

Kontrola, u širem smislu, predstavlja postupke, pravila, standarde i aktivnosti usmerene ka osiguranju da se određeni ciljevi ostvare na način koji je u skladu sa očekivanjima i standardima.

Kontrolni ciljevi: Specifični ciljevi koji se postavljaju kako bi se osiguralo da su procesi u skladu sa poslovnim ciljevima i strategijama upravljanja rizicima.

Kontrolne aktivnosti: Konkretno akcije koje se preduzimaju radi sprovođenja kontrolnih politika, procedura i standarda. Ove aktivnosti osiguravaju da se zadane direktive efektivno sprovode.

IT procesi: COBIT definiše IT procese kao skup aktivnosti i praksi koje se sprovode unutar organizacije kako bi se postigli određeni ciljevi upravljanja i kontrole. IT procesi po COBIT-u su strukturirani u domene i podržavaju sve aspekte IT upravljanja.

Kontrolni okvir pruža sveobuhvatni pristup za razvoj, implementaciju, praćenje i unapređenje praksi upravljanja i kontrole IT-a. Kontrole unutar okvira pomažu u osiguravanju da IT procesi i resursi budu usklađeni sa poslovnim ciljevima, da su rizici adekvatno upravljani, i da se vrednost koju IT pruža optimizuje.

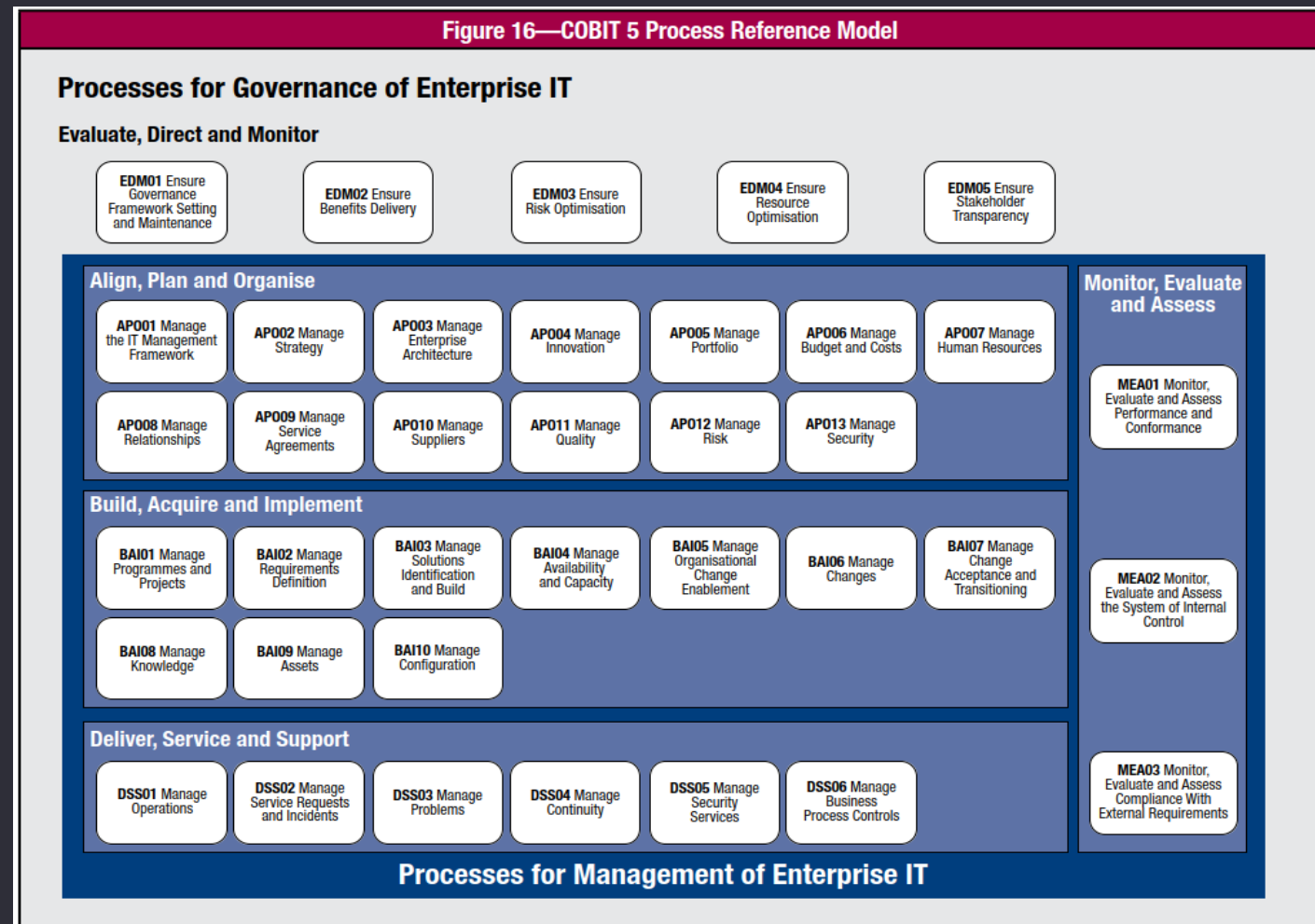
Primer kontrola i CIA trougao

Dostupnost	Integritet	Poverljivost
Dovoljan niz diskova (RAID)	Heširanje (integritet podataka)	Enkripcija za podatke u mirovanju (ceo disk, enkripcija baze podataka)
Klasterovanje	Konfiguracioni menadžment (integritet sistema)	Enkripcija za podatke u pokretu (IPSec, SSL, SSH)
Balansiranje opterećenja (Load balancing)	Kontrola promena u sistemu(integritet procesa)	Kontrole pristupa (Fizičke i tehničke)
Suvišni podaci i linije podataka	Kontrola pristupa (fizički i tehnički)	Autentikacija
Softverski i podatkovni bekap	Digitalno potpisivanje	Klasifikacija podataka
Kolokacija i udaljene lokacije	Aktivno logovanje aktivnosti	Trening podizanja svesti
Uspostavljanje „roll back“ funkcija	IDS/SIEM	
Konfiguracija „fail-over“	Princip „4 oka“	

Kontrolni okviri i kontrole

Kontrolni okviri: Kako bi se postigli ciljevi i zahtevi nivoa bezbednosti organizacije ili usklađenosti sa određenim standardnima, organizacije usvajaju kontrolne okvire kako bi omogućili:

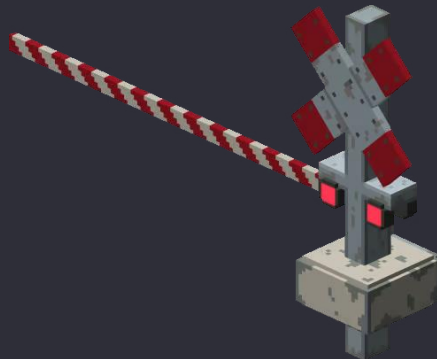
- Konzistentnost
- Merljivost
- Standardizaciju
- Sveobuhvatnost
- Modularnost



Tipovi kontrola

1. Preventivne kontrole (Preventive Controls)

1. **Cilj:** Sprečavanje incidenata ili problema pre nego što se dogode.
2. **Primeri:**
 1. Pravila i procedure za kontrolu pristupa.
 2. Sigurnosni trening za zaposlene.
 3. Sistemi za detekciju i prevenciju upada (IDS/IPS).
 4. Enkripcija podataka.
 5. Autorizacija procedure za pristup sistemima i podacima.



1. Detektivne kontrole (Detective Controls)

1. **Cilj:** Otkrivanje incidenata ili problema nakon što su se dogodili.
2. **Primeri:**
 1. Sistemi za nadgledanje i praćenje mrežnih aktivnosti.
 2. Revizija i analiza logova.
 3. Alarmi za sigurnosne događaje.
 4. Periodični sigurnosni testovi i skeniranja.
 5. Revizorski tragovi i praćenje transakcija.



Tipovi kontrola

1. Korektivne kontrole (Corrective Controls)

1. **Cilj:** Ispravljanje incidenata ili problema nakon što su otkriveni.
2. **Primeri:**
 1. Planovi za oporavak od katastrofa (DRP).
 2. Procedure za oporavak od sigurnosnih incidenata.
 3. Patch management i ispravljanje ranjivosti.
 4. Aktivnosti za povratak sistema u normalno stanje nakon incidenta.
 5. Izveštaji i analize nakon incidenata (post-mortem).



1. Direktivne kontrole (Directive Controls)

1. **Cilj:** Obezbeđivanje pravilnog ponašanja putem politike, procedura i uputstava.
2. **Primeri:**
 1. Sigurnosne politike i procedure.
 2. Priručnici i uputstva za zaposlenike.
 3. Standardi i smernice za razvoj i upravljanje IT resursima.
 4. Edukacija i trening za podizanje svesti o bezbednosti.
 5. Izvršna podrška i sponzorstvo za sigurnosne inicijative.



Tipovi kontrola

1. Kompensatorne kontrole (Compensatory Controls)

1. **Cilj:** Nadoknađivanje nedostataka u drugim kontrolama, obično kada nije moguće implementirati primarnu kontrolu.
2. **Primeri:**
 1. Dodatne kontrole za pristup kada multifaktorska autentifikacija nije moguća.
 2. Ručne procedure za proveru kada automatizovana rešenja nisu dostupna.
 3. Alternativne mere bezbednosti koje nadoknađuju slabosti u postojećim kontrolama.



1. Deterrentne kontrole (Deterrent Controls)

1. **Cilj:** Ograđivanje od potencijalnih pretnji ili napada putem zastrašivanja ili stvaranja barijera.
2. **Primeri:**
 1. Upozorenja o sigurnosnim politikama i pravnim posledicama.
 2. Fizičko obezbeđenje i vidljive sigurnosne mere.
 3. Pravne i regulativne sankcije.
 4. Interni kodeksi ponašanja i etički standardi.



Komponente interne kontrolne matrice

Način označavanja pregleda i revizije kontrola

Kontrola	Kontrolna aktivnost	Odgovoran za kontrolu	Tip kontrole	Frekvencija sprovođenja kontrole	Evaluacija kontrole	Dizajn kontrole	Operativna efikasnost
Kontrola udaljenog pristupa	Omogućavanje dvofaktorske autentifikacije putem VPN-a.	Mrežni inženjer	Preventivna	Po potrebi	Uspostavljena (nivo XY)	Uspostavljen	Uspostavljen

Za svaku kontrolu je potrebno definisati interno zaposlenog koji je zadužen za sprovođenje kontrole. Potrebno je definisati RACI matricu za svaku uspostavljenu kontrolu.

Definisati frekvenciju sprovođenja kontrole:

- Mesečno
- Po potrebi
- Nedeljno
- Godišnje

Korišćenje kontrolnog okvira za ispunjenje zahteva regulative

Korišćenje kontrolnog okvira za ispunjenje zahteva regulativa je ključno za obezbeđivanje usklađenosti sa propisima i standardima iz oblasti informacione bezbednosti. Evo kako možete koristiti kontrolni okvir za ispunjenje zahteva regulativa:



Važnost usklađivanja sa regulativama i standardima



COBIT

Control Objectives for Information
and Related Technologies
ISACA

■ ■ ■
The better the question. The better the answer.
The better the world works.

EY

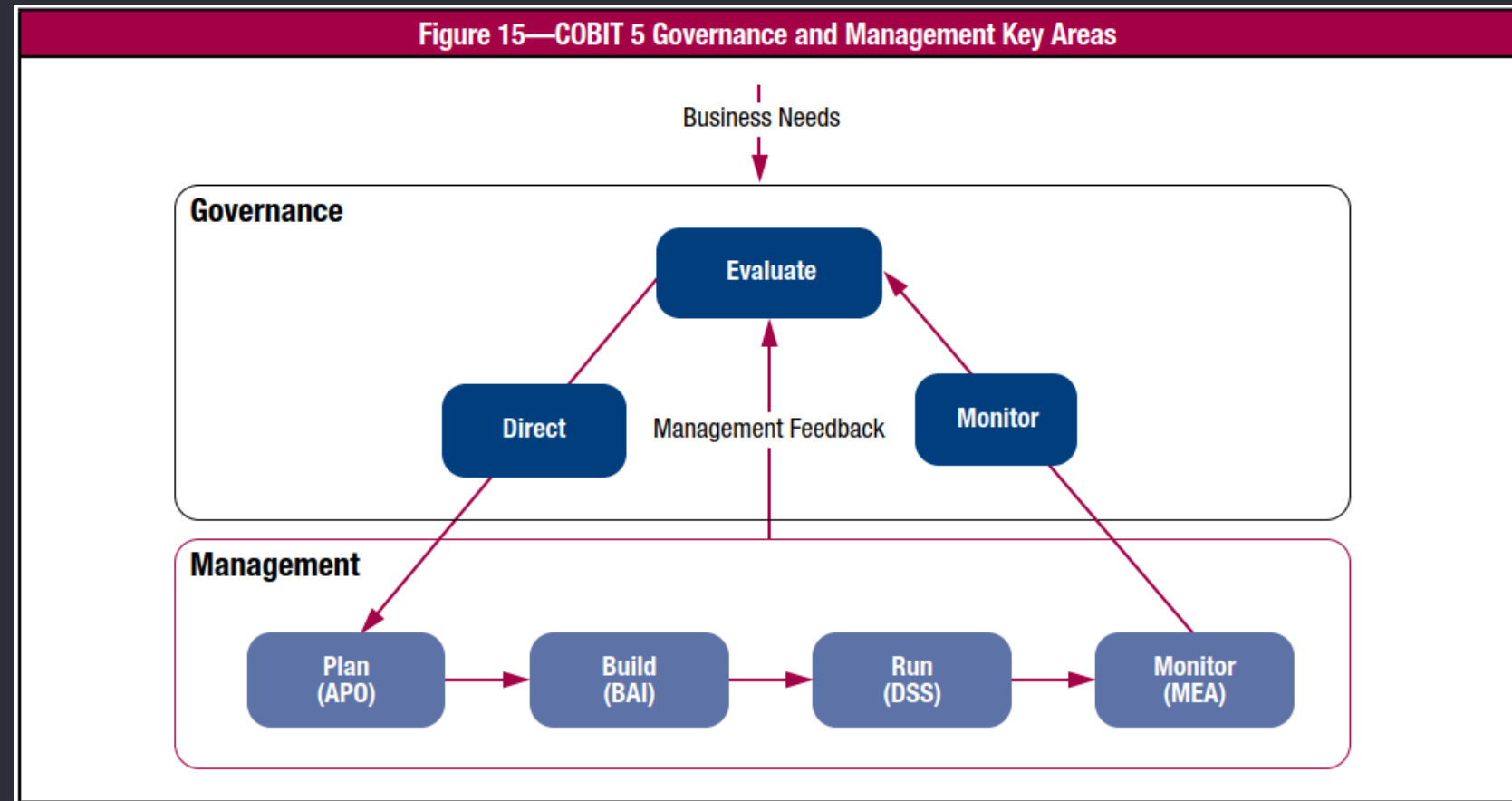
Building a better
working world

COBIT – ključne oblasti i upravljanje

Organizacija može da organizuje svoje procese kako smatra da je prikladno, sve dok su svi neophodni ciljevi upravljanja pokriveni.

Trenutno aktuelna verzija COBIT 5.0. <<https://isaca.org>>

COBIT 5 uključuje referentni model procesa, koji definiše i detaljno opisuje niz procesa upravljanja. Predstavlja sve procese koji se obično nalaze u organizaciji u vezi sa IT aktivnostima, obezbeđivanjem zajedničkog referentnog modela razumljivog operativnim IT i poslovnim menadžerima. Svaka organizacija mora da definiše sopstveni model, uzimajući u obzir specifičnu situaciju.



Pregled pokrivenosti izmedju COBIT-a I drugih kontrolnih okvira

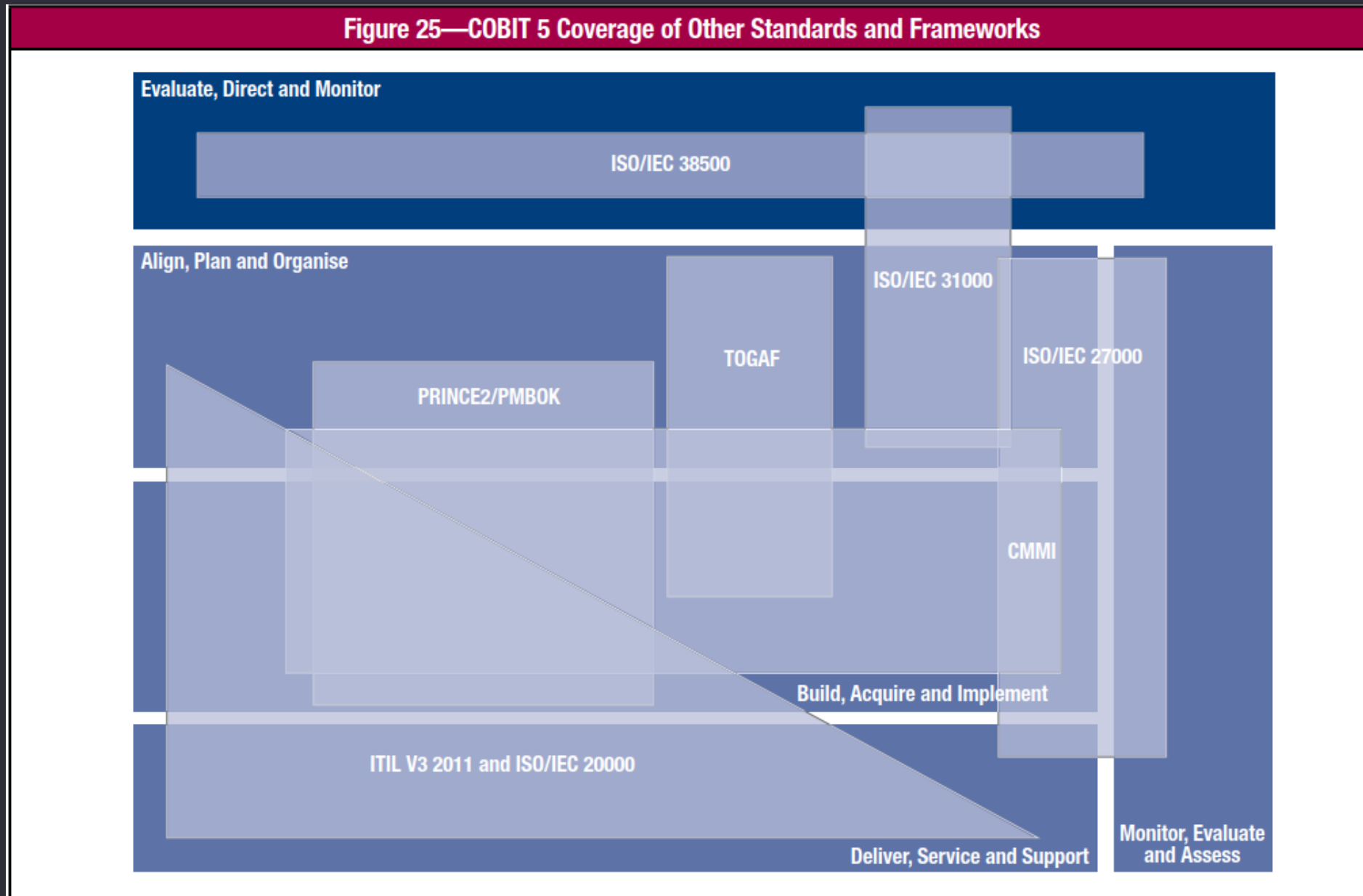


Figure 16—COBIT 5 Process Reference Model

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

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

MEA02 Monitor, Evaluate and Assess the System of Internal Control

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

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

COBIT – procesni referentni model (1/3)

1. Evaluate, Direct, and Monitor (EDM)

Ovaj domen se bavi procenom, usmeravanjem i nadzorom IT upravljanja kako bi se osigurala usklađenost sa strategijama i ciljevima organizacije.

•EDM01: Osiguravanje upravljanja IT-jem

- **Cilj:** Osigurati da IT usklađuje sa poslovnim ciljevima.
- **Aktivnosti:** Postavljanje IT strategije, definisanje IT politika.

•EDM02: Osiguravanje ostvarivanja koristi od IT-a

- **Cilj:** Maksimiziranje vrednosti IT ulaganja.
- **Aktivnosti:** Upravljanje portfolijom IT projekata.

2. Align, Plan, and Organize (APO)

Ovaj domen se fokusira na planiranje i organizovanje IT strategija i resursa.

•APO01: Upravljanje okvirom IT upravljanja

- **Cilj:** Definisanje i održavanje okvira IT upravljanja.
- **Aktivnosti:** Razvoj IT governance modela, implementacija okvira upravljanja.

•APO02: Upravljanje strategijom

- **Cilj:** Osigurati da IT strategija usklađuje sa poslovnom strategijom.
- **Aktivnosti:** Izrada IT strateškog plana, komunikacija strategije.

COBIT – procesni referentni model (2/3)

3. **Build, Acquire, and Implement (BAI)**

Ovaj domen se odnosi na razvoj, nabavku i implementaciju IT rešenja i sistema.

•**BAI01:** Upravljanje programima i projektima

- Cilj: Upravljanje IT projektima radi postizanja ciljeva u rokovima i budžetu.
- Aktivnosti: Upravljanje projektnim portfolijom, praćenje i kontrola projekata.

•**BAI02:** Definisanje zahteva za rešenja

- Cilj: Osigurati da rešenja odgovaraju poslovnim potrebama.
- Aktivnosti: Prikupljanje i analiza zahteva, specifikacija rešenja.

4. **Deliver, Service, and Support (DSS)**

Ovaj domen pokriva pružanje IT usluga, podršku korisnicima i operativne aktivnosti.

•**DSS01:** Upravljanje operacijama

- Cilj: Osigurati pouzdano i efikasno operisanje IT resursima.
- Aktivnosti: Upravljanje IT operacijama, monitoring performansi sistema.

•**DSS02:** Upravljanje incidentima i servisnim zahtevima

- Cilj: Efikasno rešavanje IT incidenata i servisnih zahteva.
- Aktivnosti: Implementacija ITIL procesa za upravljanje incidentima, korisnička podrška.

COBIT – procesni referentni model (3/3)

5. **Monitor, Evaluate, and Assess (MEA)**

Ovaj domen obuhvata praćenje performansi IT-a, evaluaciju usklađenosti i ocenu rezultata.

- **MEA01**: Praćenje, evaluacija i ocena performansi i usaglašenosti sa spoljnim zahtevima
 - Cilj: Osigurati da IT performanse zadovoljavaju poslovne potrebe i regulatorne zahteve.
 - Aktivnosti: Redovna revizija performansi IT-a, sprovođenje revizija usklađenosti.
- **MEA02**: Praćenje, evaluacija i ocena internog upravljanja
 - Cilj: Procena efikasnosti internog upravljanja IT-jem.
 - Aktivnosti: Interna kontrola, procena rizika.



ISO27001:2013

■ ■ ■
The better the question. The better the answer.
The better the world works.

EY

Building a better
working world

ISO 27001 standard I okvir

ISO/IEC 27001 je međunarodni standard koji specificira zahteve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sistema upravljanja sigurnošću informacija (ISMS). Standard je razvijen kako bi organizacije svih veličina i industrija mogle da zaštite svoje informacione resurse na sistematičan i proaktivan način.

Osnovni ciljevi ISO/IEC 27001:

- **Zaštita poverljivosti:** Osigurava da su informacije dostupne samo ovlašćenim osobama.
- **Zaštita integriteta:** Osigurava tačnost i potpunost informacija i metoda obrade.
- **Zaštita dostupnosti:** Osigurava da su informacije i povezani resursi dostupni kada su potrebni.

Standard

Prilog A
Kontrole
bezbednosti

Kontinuirano
unapređenje
PDCA

Pregled ISO 27001 standarda

ISO/IEC 27001 koristi visoku strukturu nivoa (High-Level Structure - HLS) koju koriste svi ISO standardi upravljanja, što olakšava integraciju sa drugim ISO standardima, kao što su ISO 9001 (upravljanje kvalitetom) i ISO 14001 (upravljanje životnom sredinom). HLS osigurava doslednost i kompatibilnost između različitih standarda.



Pregled ISO 27001 standarda

4. Kontekst organizacije (Context of the Organization)

1. **Razumevanje organizacije i njenog konteksta:** Identifikacija unutrašnjih i spoljašnjih faktora koji mogu uticati na sposobnost organizacije da postigne ciljeve informacione bezbednosti.
2. **Razumevanje potreba i očekivanja zainteresovanih strana:** Identifikacija zainteresovanih strana (stakeholders) i njihovih zahteva vezanih za informacionu bezbednost.
3. **Određivanje obima ISMS-a:** Definisanje granica i primenljivosti ISMS-a unutar organizacije.
4. **ISMS i njegov kontekst:** Definisanje internih i eksternih faktora koji utiču na ISMS.

5. Liderstvo (Leadership)

1. **Liderstvo i posvećenost:** Viši menadžment mora pokazati posvećenost informacijskoj bezbednosti, pružiti potrebne resurse i podršku.
2. **Politika informacione bezbednosti:** Izrada, implementacija i održavanje politike informacione bezbednosti koja je usklađena sa ciljevima organizacije.
3. **Uloge, odgovornosti i ovlašćenja:** Jasno definisanje i dodeljivanje uloga i odgovornosti vezanih za ISMS.

6. Planiranje (Planning)

1. **Akcije za rešavanje rizika i prilika:** Identifikacija rizika i prilika koje mogu uticati na ISMS i planiranje akcija za njihovo rešavanje.
2. **Ciljevi informacione bezbednosti i planiranje za njihovo postizanje:** Postavljanje merljivih ciljeva informacione bezbednosti i definisanje planova za njihovo ostvarivanje.
3. **Planiranje promena:** Osiguravanje da se promene u ISMS-u planiraju na kontrolisan način.

7. Podrška (Support)

1. **Resursi:** Osiguravanje potrebnih resursa za uspostavljanje, implementaciju, održavanje i poboljšanje ISMS-a.
2. **Kompetencija:** Osiguravanje da osoblje ima potrebne kompetencije za izvršavanje svojih zadataka u vezi sa informacijskom sigurnošću.
3. **Svest:** Podizanje svesti među zaposlenima o važnosti informacione bezbednosti i njihovoj ulozi u ISMS-u.
4. **Komunikacija:** Uspostavljanje internih i eksternih komunikacionih procesa vezanih za ISMS.
5. **Dokumentovane informacije:** Upravljanje dokumentovanim informacijama potrebnim za ISMS, uključujući kreiranje, ažuriranje i kontrolu.

8. Operacije (Operation)

1. **Operativno planiranje i kontrola:** Planiranje, implementacija i kontrola procesa potrebnih za postizanje ciljeva informacione bezbednosti.
2. **Procena rizika:** Kontinuirano procenjivanje rizika za informacionu bezbednost.
3. **Tretman rizika:** Definisanje i implementacija planova za tretman rizika.

9. Evaluacija performansi (Performance Evaluation)

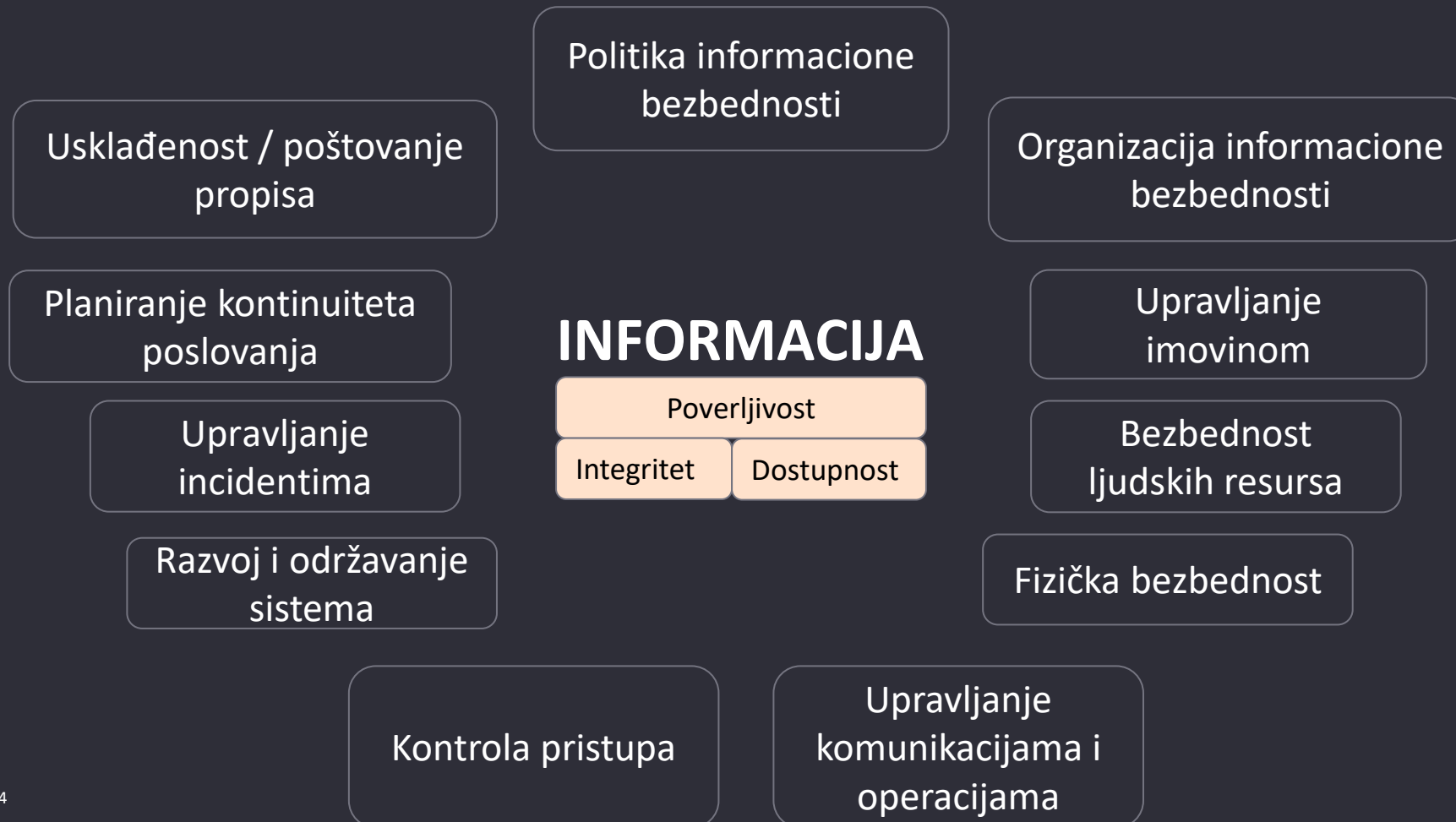
1. **Praćenje, merenje, analiza i evaluacija:** Uspostavljanje procesa za praćenje i merenje performansi ISMS-a.
2. **Interna revizija:** Sprovođenje redovnih internih audita kako bi se procenila usklađenost sa zahtevima ISO/IEC 27001 i efikasnost ISMS-a.
3. **Preispitivanje menadžmenta:** Redovno preispitivanje ISMS-a od strane višeg menadžmenta kako bi se osigurala njegova adekvatnost, efektivnost i usklađenost sa poslovnim ciljevima.

1. Poboljšanja (Improvement)

1. **Neusklađenosti i korektivne mere:** Identifikacija neusklađenosti, sprovođenje korektivnih mera i njihova efektivnost.
2. **Kontinuirano poboljšanje:** Kontinuirano unapređivanje ISMS-a kako bi se poboljšala efikasnost informacione bezbednosti.

ISO 27001 - Kontrolne klauzule Priloga A.

Prilog A u ISO/IEC 27001 standardu pruža detaljan skup kontrola bezbednosti informacija koje organizacije mogu koristiti za zaštitu svojih informacija. Organizacije mogu koristiti ovaj skup kontrola za izradu svog sistema upravljanja sigurnošću informacija, prilagođavajući ih svojim specifičnim potrebama i rizicima. Prilog A sadrži 114 kontrola, podeljenih u 14 domena (ISO 27001:2013).

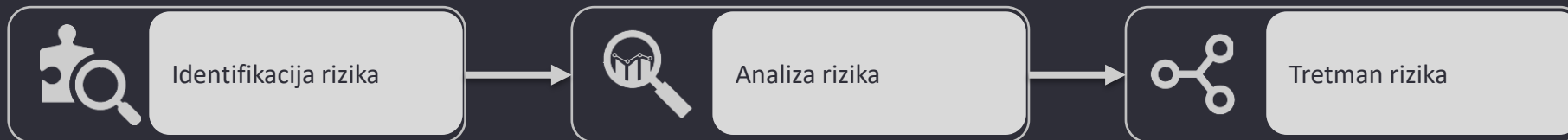


Prilog A – Kontrolni okvir sigurnosnih kontrola

Kontrolna oblast	Kontrolni ciljevi
A.5 Informacione sigurnosne politike	Osiguravanje da su informacione sigurnosne politike uspostavljene u skladu sa ciljevima organizacije.
A.6 Organizacija informacione bezbednosti	Upravljanje informacijskom sigurnošću unutar organizacije.
A.7 bezbednost ljudskih resursa	Osiguravanje da zaposleni razumeju svoje odgovornosti i da su prikladno obučeni za svoje sigurnosne uloge.
A.8 Upravljanje imovinom	Identifikacija, klasifikacija i zaštita informacione imovine.
A.9 Kontrola pristupa	Ograničavanje pristupa informacijama samo ovlašćenim osobama.
A.10 Kriptografija	Osiguravanje efikasne primene kriptografskih rešenja za zaštitu informacija.
A.11 Fizička i ekološka bezbednost	Zaštita informacija putem fizičkih i ekoloških mera zaštite.
A.12 Bezbednost operacija	Osiguravanje bezbednog i efikasnog upravljanja IT operacijama.
A.13 Komunikaciona bezbednost	Zaštita informacija u mrežama i njihovih usluga.
A.14 Nabavka, razvoj i održavanje sistema	Osiguravanje bezbednosti informacijskih sistema tokom celog životnog ciklusa.
A.15 Odnosi sa dobavljačima	Upravljanje rizicima vezanim za dobavljače.
A.16 Upravljanje incidentima informacione bezbednosti	Osiguravanje efikasnog odgovora na bezbednosne incidente.
A.17 Upravljanje kontinuitetom poslovanja	Održavanje kontinuiteta poslovanja i oporavak od katastrofa.
A.18 Usklađenost	Osiguravanje usklađenosti sa pravnim i regulatornim zahtevima.

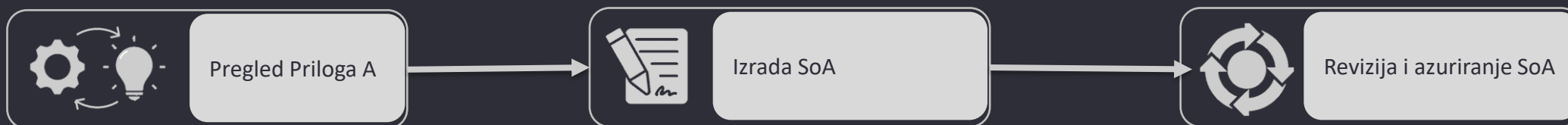
Planiranje i izrada izjave o primenljivosti (eng. Statement of Applicability)

Procena rizika



Planiranje i izrada izjave o primenljivosti (SoA)

Izjava o primenljivosti (SoA) je ključni dokument u okviru ISO/IEC 27001 koji sadrži listu svih kontrola koje su relevantne za organizaciju, zajedno sa objašnjenjem zašto su te kontrole primenljive ili nisu primenljive.



Pregled kontrola iz priloga A.

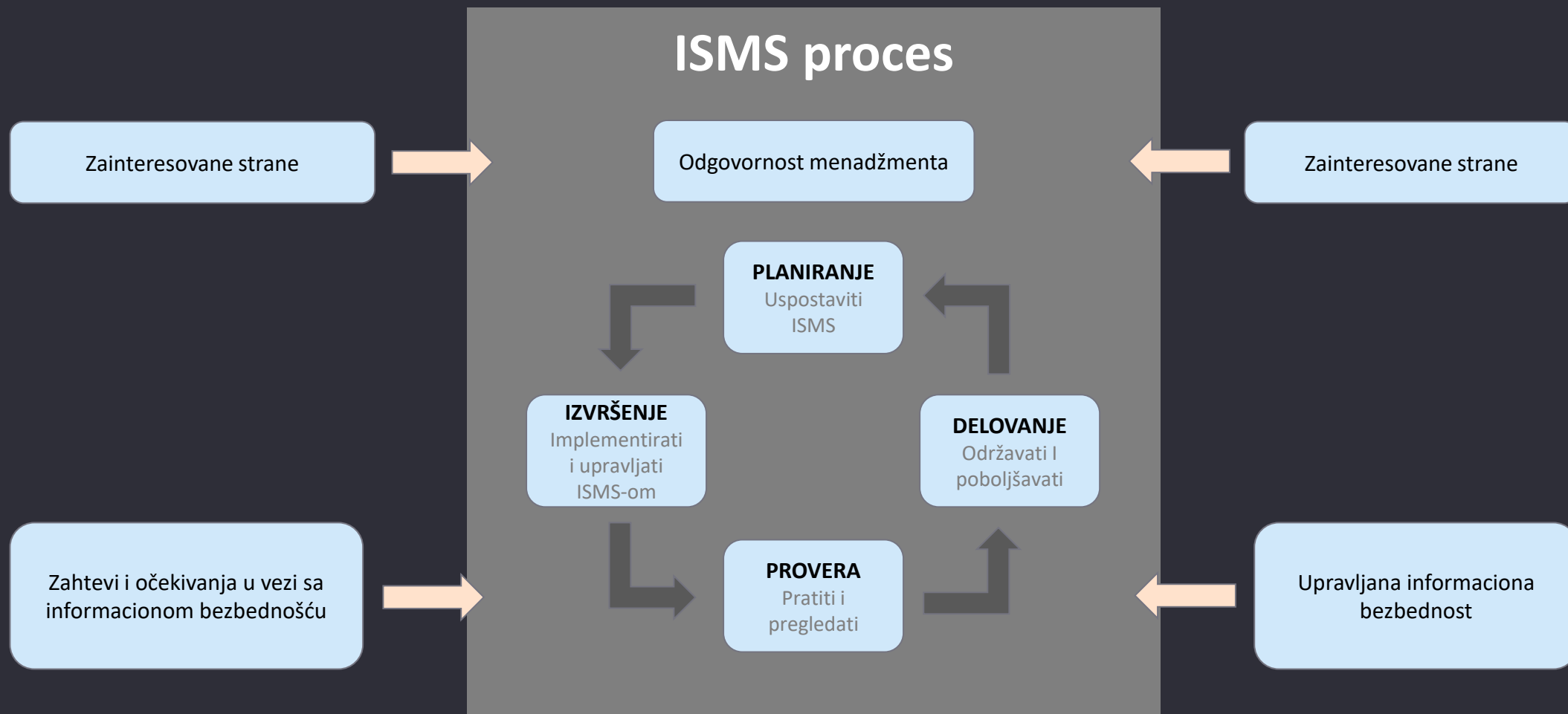
Lista kontrola: Identifikacija svih kontrola iz Priloga A koje su relevantne za organizaciju.

Opis implementacije: Kratak opis kako je svaka kontrola implementirana ili planirana za implementaciju.

Primer izgleda Izjave o primenljivosti

Kontrolna oblast	Kontrola	Status	Primena (Da/Ne)	Justifikacija	Opis implementacije
A.5 Informacione sigurnosne politike	A.5.1.1 Dokumentovana informacijska sigurnosna politika	Primenjena	Da	Organizacija zahteva formalnu politiku za usmeravanje svih aspekata bezbednosti informacija.	Politika je razvijena i odobrena od strane menadžmenta, dostupna svim zaposlenima.
A.6 Organizacija informacione bezbednosti	A.6.1.2 Mobilni uređaji i rad na daljinu	Delimično primenjena	Da	Rad na daljinu je sve češći, što zahteva dodatne sigurnosne mere.	Politike za rad na daljinu su razvijene, ali potpuna implementacija sigurnosnih rešenja je u toku.
A.8 Upravljanje imovinom	A.8.1.1 Inventar imovine	Primenjena	Da	Potrebno je imati popis sve informacione imovine za upravljanje rizicima.	Inventar imovine je uspostavljen i redovno se ažurira.

Planiraj – Izvrši – Proveri – Deluj (eng. Plan-Do-Control-Act)



Zadatak vežba broj 3.

