UČINKOVITA IMPLEMENTACIJA CJELOVITIH SUSTAVA INFORMACIJSKE SIGURNOSTI

ZIH d.o.o.
Silvana Tomić Rotim, Lead Auditor, CISA

Agenda

- Motivi uvođenja ISMS-a
- Proces uvođenja ISMS-a
- Upravljanje informacijskom imovinom
- Upravljanje sigurnosnim rizicima
- Implementacija i mjerenje učinkovitosti ISMS-a
- Nešto za kraj

MOTIVI UVOĐENJA ISMS-a

- Zaštita imovine
- Nesmetano odvijanje poslovnih procesa
- Zahtjev poslovne okoline
- Smanjenje ili uklanjanje rizika
- Smanjenje broja incidenata
- Usklađenost sa zakonskom regulativom
- Konkurentnost
- Imidž

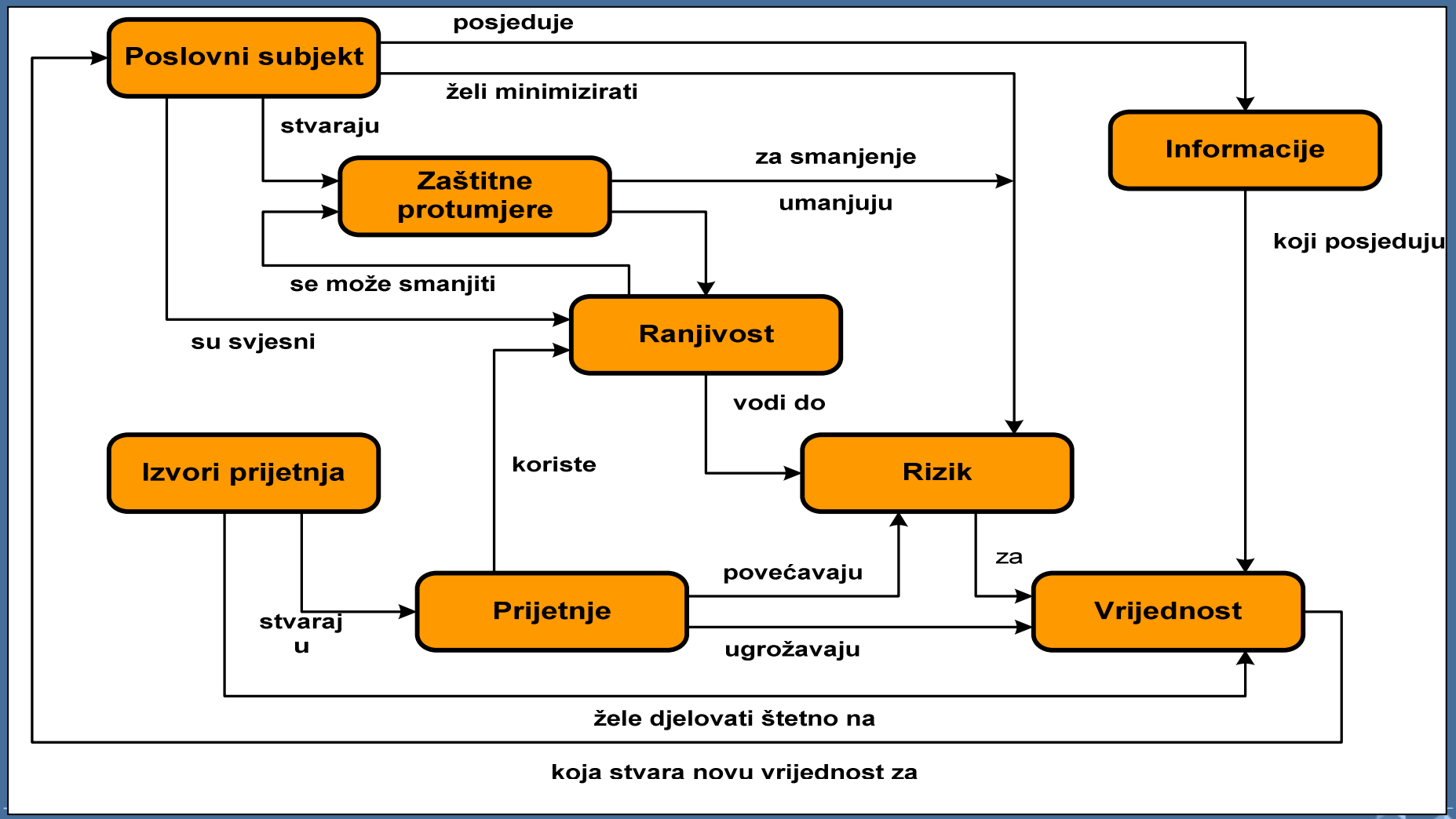
Prednosti koje se postižu ISMS-om

- Sigurnost i povjerenje u IS
- Prikladna zaštita informacijske imovine
- Tržišna prednost
- Sukladnost sa zakonom
- Imidž
- Pruža se izvrsna check lista raspoloživih kontrola
- Predstavljanje vlastite prakse s dokazima
  - Krajnjim korisnicima
  - Poslovnim partnerima
  - Auditorima

Istina

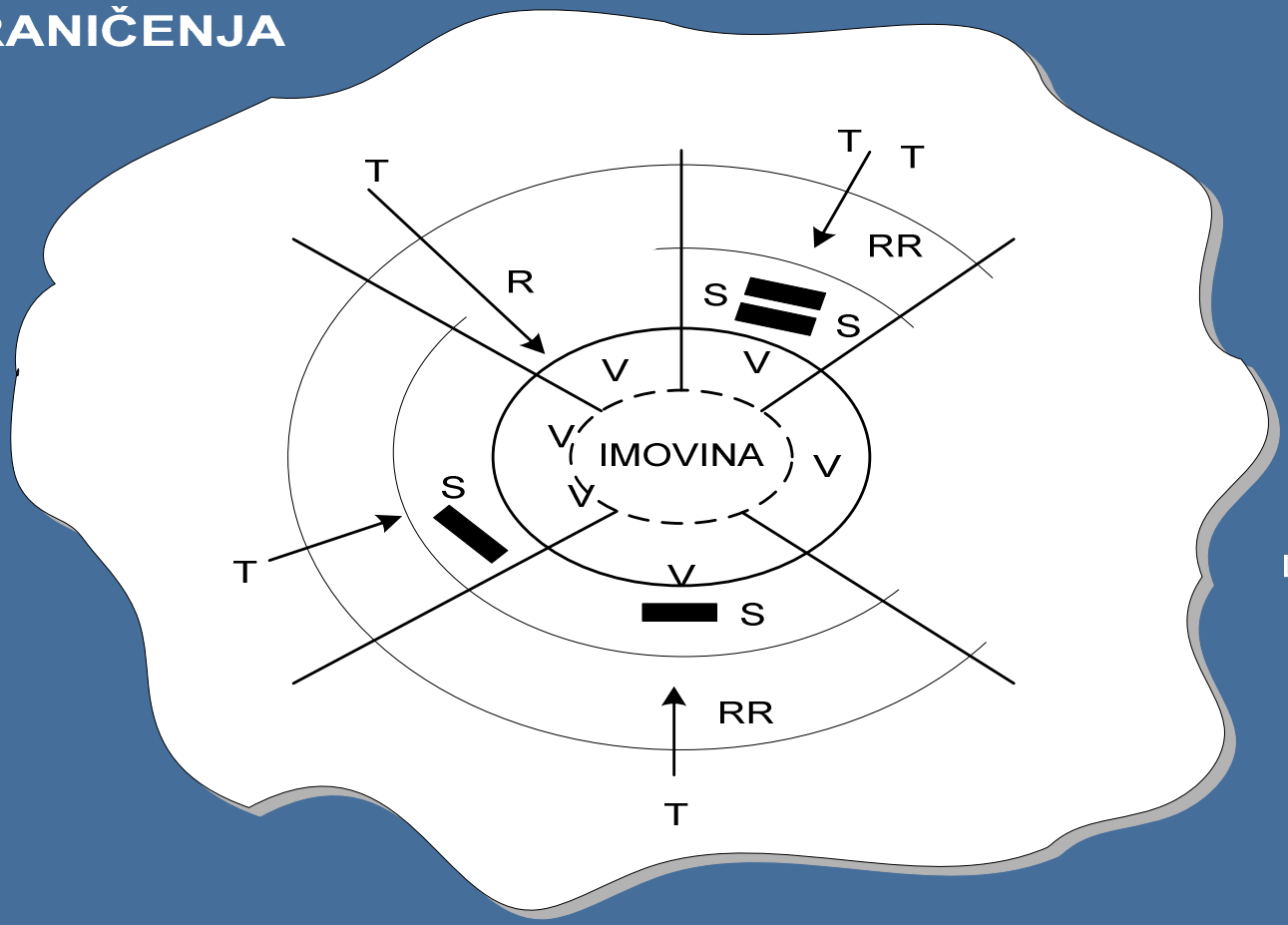
- Ne postoji 100% sigurnost
- Sigurnost se ne može kupiti - nema gotovih rješenja!!!
- **Sigurnost je trajan proces, ne stanje**
- Podrška poslovodstva te organizirana i trajna izobrazba uvjet je za kvalitetan sustav sigurnosti

Pogled u informacijsku sigurnost



ODNOSI MEĐU ELEMENTIMA SIGURNOSTI

OGRANIČENJA



Legenda:

R – Rizik
RR Rezidualni rizici
S - Zaštita
T – Opasnosti
V – (Ranjivosti)

Što je ISMS?

ISMS (Information Security Management System) je dio cjelokupnog sustava upravljanja, a odnosi se na pristup rukovanju sigurnosnim rizicima, te uspostavu, uvođenje, provođenje, nadzor, procjenu, održavanje i kontinuirano poboljšavanje informacijske sigurnosti.

PDCA MODEL

Metodologija Plan-Do-Check-Act može se primijeniti na sve procese ISMS-a.

PLAN: definiranje ciljeva i procesa ISMS-a koji su potrebni da bi se zadovoljili zahtjevi korisnika

DO: provođenje procesa i rukovanje ISMS-om

CHECK: nadziranje i mjerenje rezultata procesa prema definiranim politikama, ciljevima i zahtjevima

ACT: kontinuirano poduzimanje akcija da bi se poboljšalo izvođenje ISMS procesa

NORME SERIJE ISO 27000

Smjernice za ISMS auditore

Smjernice za ISMS audit

ISO 27007

ISO 27008

ISMS- načela i rječnik

ISO 27000

ISMS- zahtjevi

ISMS- smjernice za uvođenje

ISO 27003

Zahtjevi za tijela koja pružaju certifikaciju ISMS-a

ISO 27006

ISO 27001

ISMS- upravljanje rizikom

ISO 27005

ISO 27002

ISMS u zdravstvu

ISO 27799

ISMS- sigurnosne tehnike

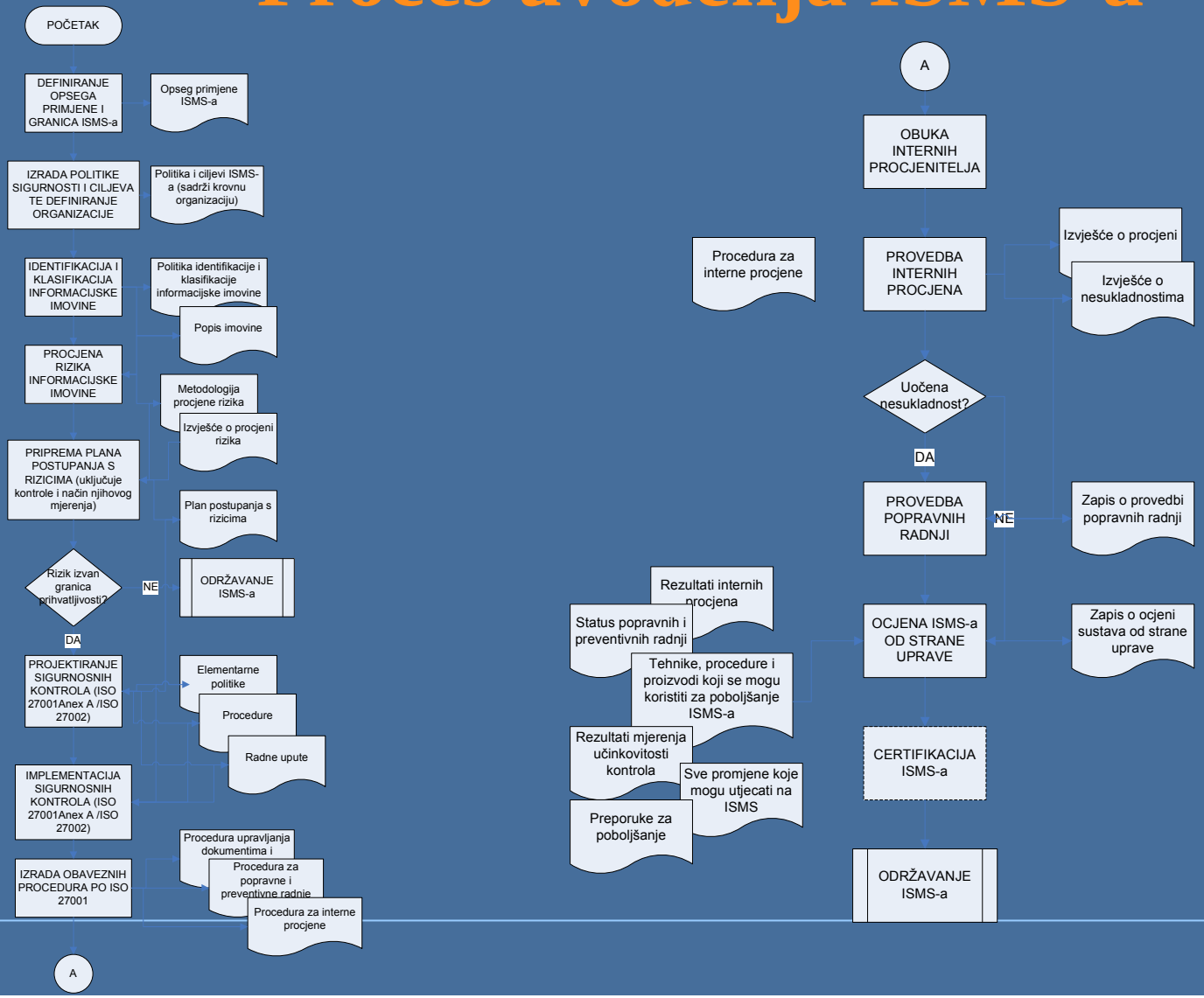
ISO 27011

ISMS- metrike i mjerenja

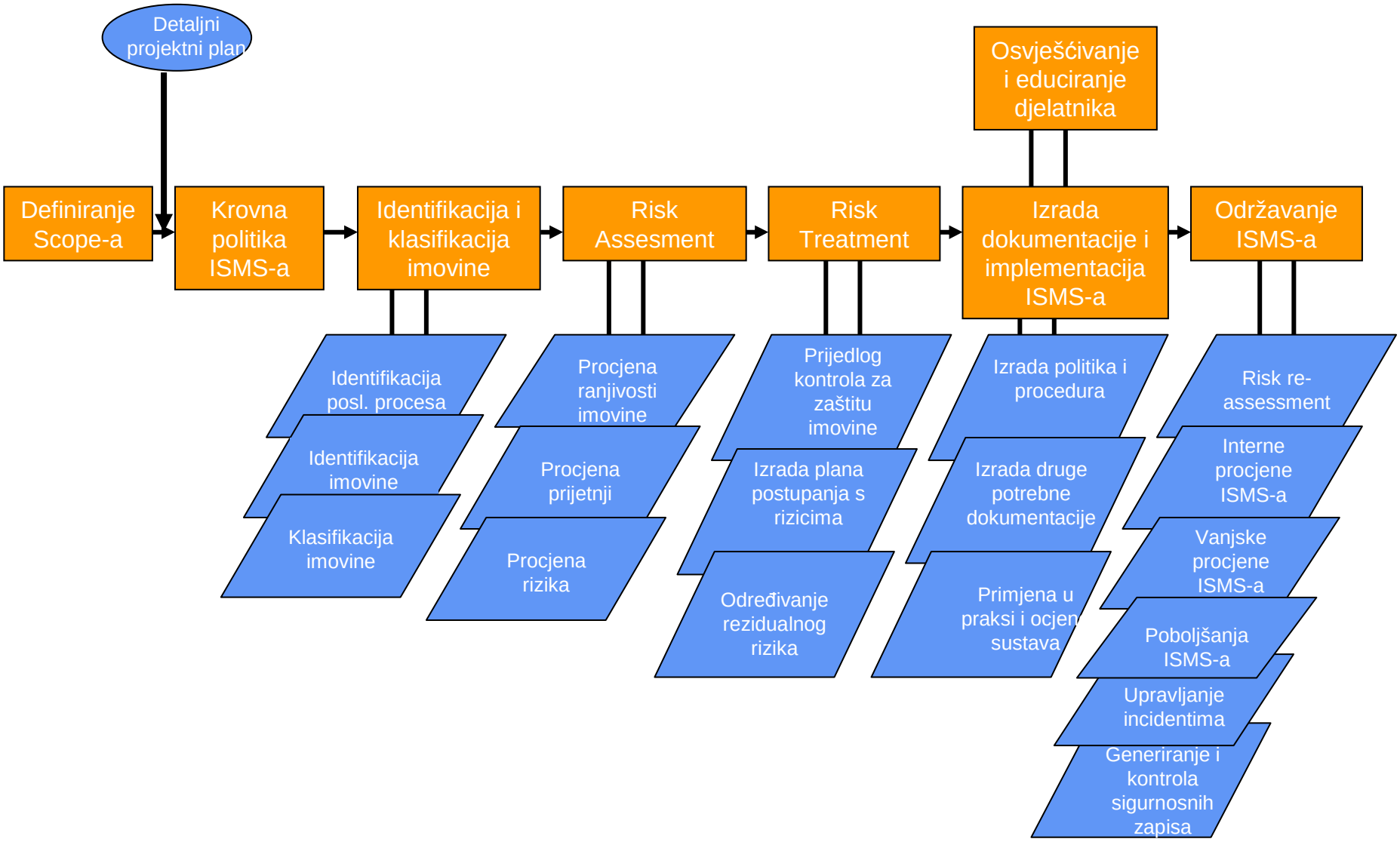
ISO 27004

ISMS u telekomunikacijama

Proces uvođenja ISMS-a



Plan projekta



Upravljanje informacijskom imovinom

- Informacijska imovina tvrtke je sve ono što za tu tvrtku predstavlja određenu vrijednost i samim time se treba zaštititi.
- Informacijska imovina se može klasificirati na:
  - Informacije (baze podataka, datoteke, dokumenti …)
  - Programsku podršku (aplikacije, sistemski SW …)
  - Fizičku imovinu (računalna i komunikacijska oprema, mediji …)
  - Usluge (računalne, opće – napajanje, klima …)
  - Ljudske resurse

Popis imovine (A.7.1.1)

- identifikacija imovine (vrijednost i važnost)
- popis imovine s dogovorenim i dokumentiranim vlasništvom, klasifikacijom i razinom zaštite

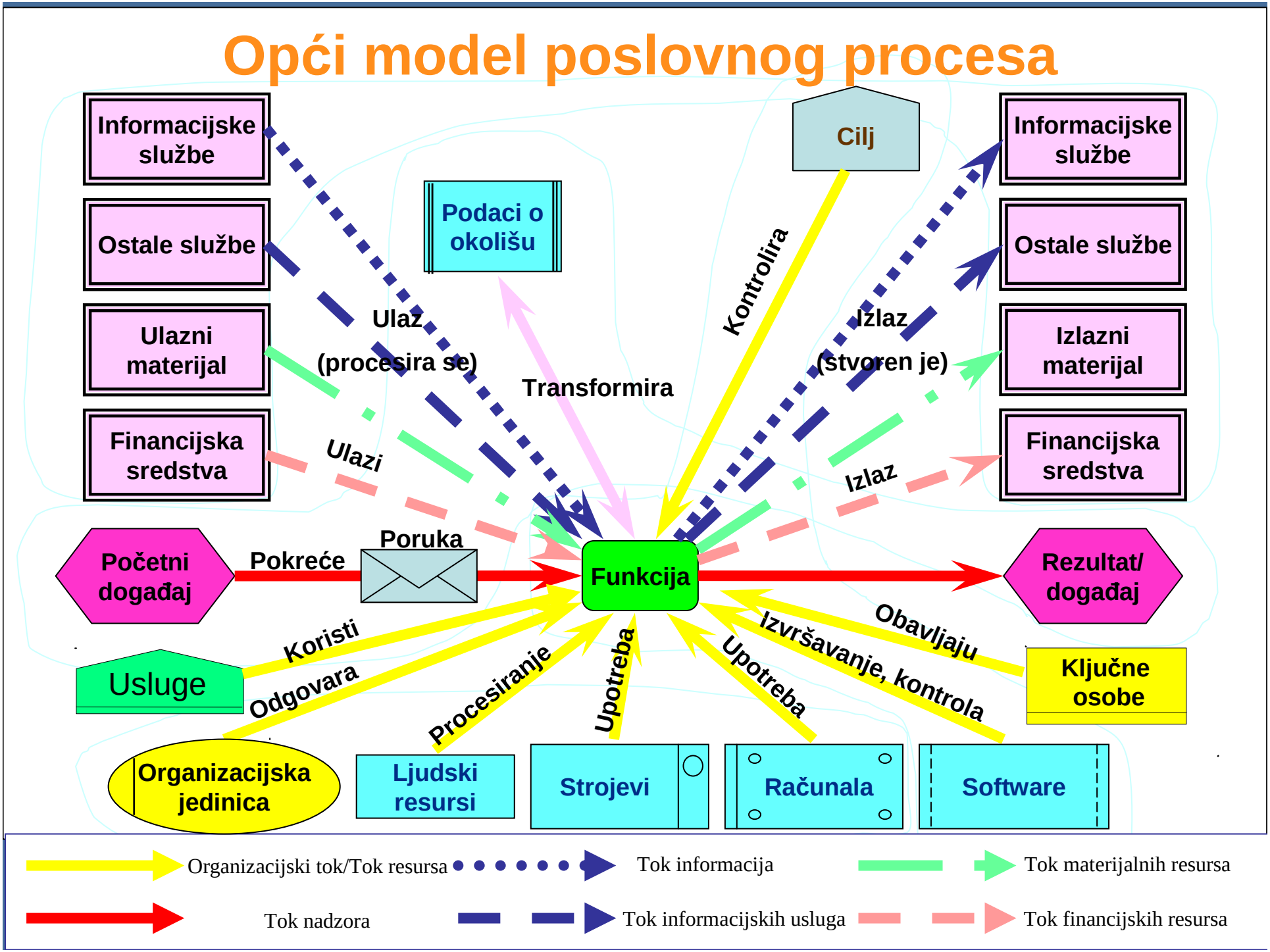
Vlasništvo nad imovinom (A.7.1.2)

- Sve informacije i sva imovina vezana uz opremu za obradu informacija trebala bi biti vlasništvo određenog dijela organizacije
- Vlasnik imovine treba biti odgovoran za:
  - klasifikaciju informacija i imovine
  - određivanje i periodičko provjeravanje ograničenja i klasifikacije pristupa u skladu s politikama kontrole pristupa

Kako načiniti popis imovine? - Polazište

- **Polazište:** poslovni procesi Vaše organizacije
- Kategorizirati procese i donijeti odluku o kritičnosti svakog od njih za poslovanje
- Za odabrane kritične procese radi se klasifikacija imovine i analiza rizika
- Osigurati da je količina promatrane imovine takva da je upravljiva u analizi rizika
- Imovina nasljeđuje kritičnost od procesa kojima pripada
- "Kritičnost" je kombinacija "raspoloživosti", "integriteta" i "povjerljivosti"

Opći model poslovnog procesa

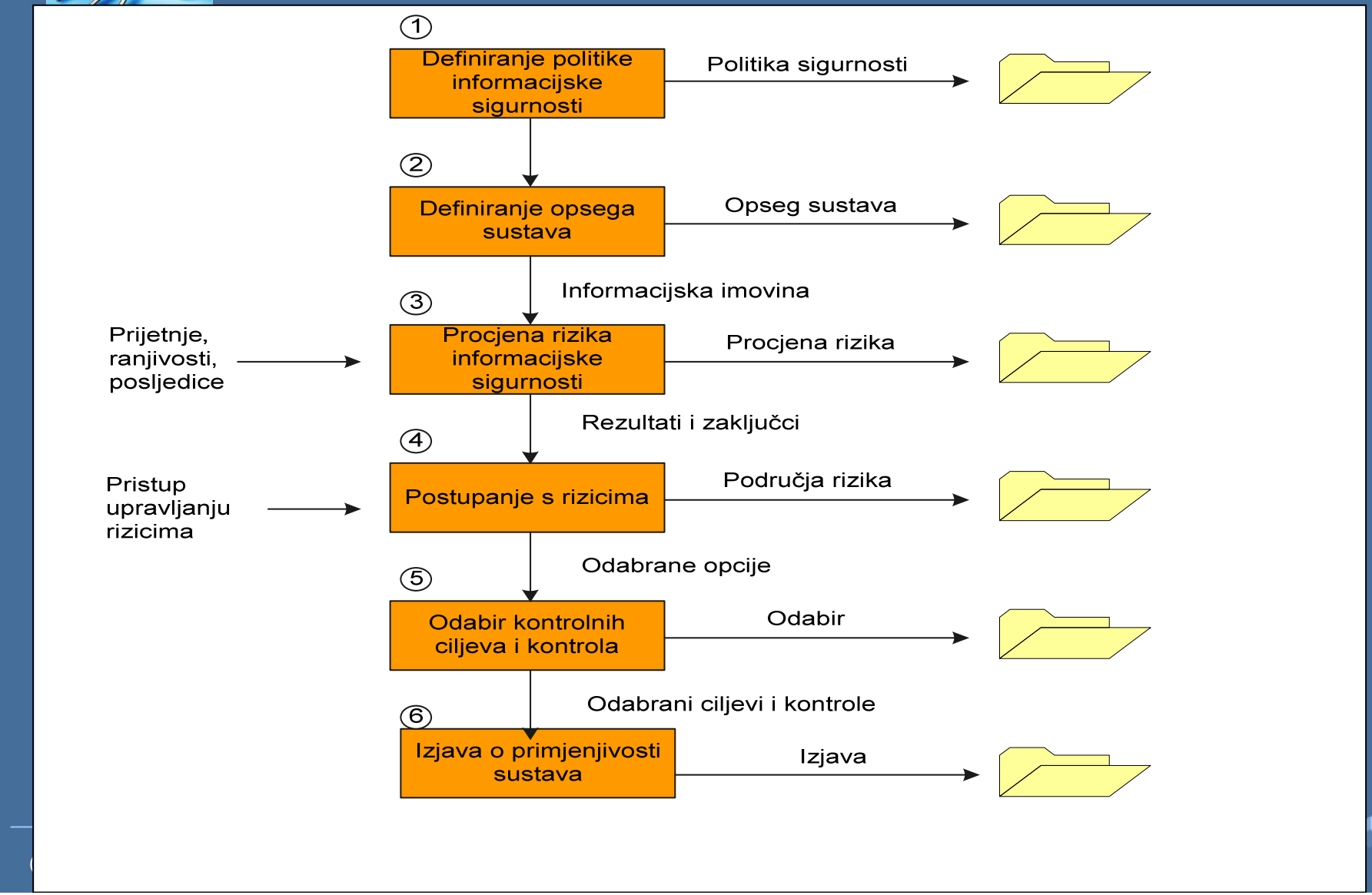


Klasifikacija informacijske imovine (A.7.2)

Povjerljivost	*Integritet*	*Raspoloživost*	*Klasifikacijska oznaka*
Vrlo tajno ili Tajno	Nužan, Važan ili Uobičajen	Kritična, Visoka, Standardna, Umjerena, Niska ili Bez utjecaja	**VRLO VISOKA**
Povjerljivo, Ograničeno ili Neklasificirano	Nužan	Kritična, Visoka, Standardna, Umjerena, Niska ili Bez utjecaja	**VRLO VISOKA**
Povjerljivo, Ograničeno ili Neklasificirano	Važan ili Uobičajen	Kritična ili Visoka	**VRLO VISOKA**
Povjerljivo ili Ograničeno	Važan ili Uobičajen	Standardna, Umjerena, Niska ili Bez utjecaja	**VISOKA**
Neklasificirano	Važan	Standardna, Umjerena, Niska ili Bez utjecaja	**VISOKA**
Neklasificirano	Uobičajen	Standardna	**VISOKA**
Neklasificirano	Uobičajen	Umjerena, Niska, Bez utjecaja	**NORMALNA**

UPRAVLJANJE SIGURNOSNIM RIZICIMA

Položaj rizika u ISMS-u



Što je sigurnosni rizik?

- Rizik predstavlja kombinaciju vjerojatnosti ostvarenja određene prijetnje i njezinih posljedica na imovinu.
- Upravljanje rizikom obuhvaća:
  - Procjenu rizika
  - Obradu rizika
  - Prihvaćanje rizika i
  - Priopćenje

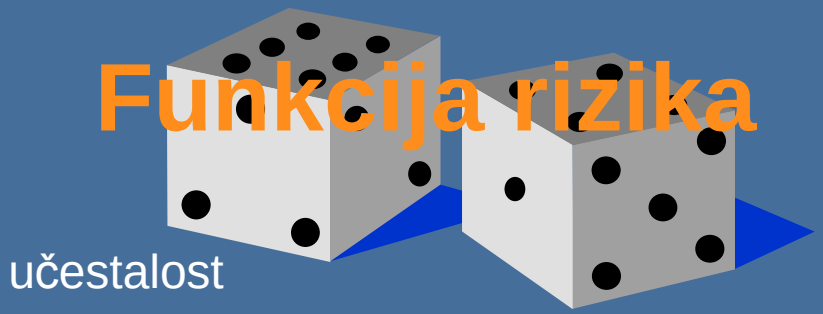
Prijetnja

- Predstavljaju potencijalni uzrok neželjenog incidenta koji može rezultirati ugrožavanjem sustava ili organizacije i njezine imovine. Može biti slučajna ili namjerna. Predmet prijetnji je uvijek imovina tvrtke.
- Neke od prijetnji jesu:
  - Prirodne katastrofe (potres, poplava, grom …)
  - Prijetnje uzrokovane ljudskim djelovanjem (slučajne i namjerne)
  - Tehnologija (kvar opreme, nesukladna oprema …)
  - Prijetnje uzrokovane organizacijskim propustima (nedostatak kontrolnih mehanizama, pravila …)

Ranjivost

- Ranjivost je slabost imovine koju jedna ili više prijetnji mogu iskoristiti. Ranjivost sama po sebi ne uzrokuje štetu, ali ako dođe do incidenta i njome se ne upravlja na pravilan način, tada šteta nastaje.
- Neke od ranjivosti su:
  - Nezaštićen fizički pristup osjetljivim prostorima
  - Nepostojanje UPS-a
  - Nekorištenje antivirusnih programa
  - Nedefinirana pravila logičkog pristupa aplikacijama

Funkcija rizika



- Rizik = f(
  - » vjerojatnosti prijetnje
  - » vrijednosti imovine
  - » razine ranjivosti imovine
  - » utjecaja prijetnje na imovinu
  - » itd....
  - »)

Izvori i oblici prijetnji informacijskoj imovini

PRIJETNJE			
IZVOR	**OBLIK**	**IZVOR**	**OBLIK**
LJUDI S ATRIBUCIJOM NAMJERE	Neautorizirani pristup	OPREMA	Tehnička pogreška opreme
	Krađa		Prestanak napajanje
	Prisluškivanje		Ispadi opreme
	Virusi i drugo		Prekidi komunikacije
	Sabotaža		Zračenja
	Uništenje	PRIRODA	Onečišćenja
LJUDI- NENAMJERNI UTJECAJ	Nepažnja		Požar
	Nedisciplina		Incidentne situacije
	Nemar		Oluja
	Neznanje		Potres
	Neodgovarajuća organizacija		Poplava

Procjena rizika - primjer

Rizik se izračunava kao:

$$R = P_T * I_T$$

	Vjerojatnost ostvarenja prijetnje (P_T)		
Utjecaj štete (I_T)	**Visoka(3)**	**Srednja(2)**	**Niska (1)**
Visok (3)	**9**	**6**	**3**
Srednji (2)	**6**	**4**	**2**
Nizak (1)	**3**	**2**	**1**
Bez utjecaja (0)	**0**	**0**	**0**

Tabela razina rizika

Obrada rizika

Postoje 4 mogućnosti obrade rizika:

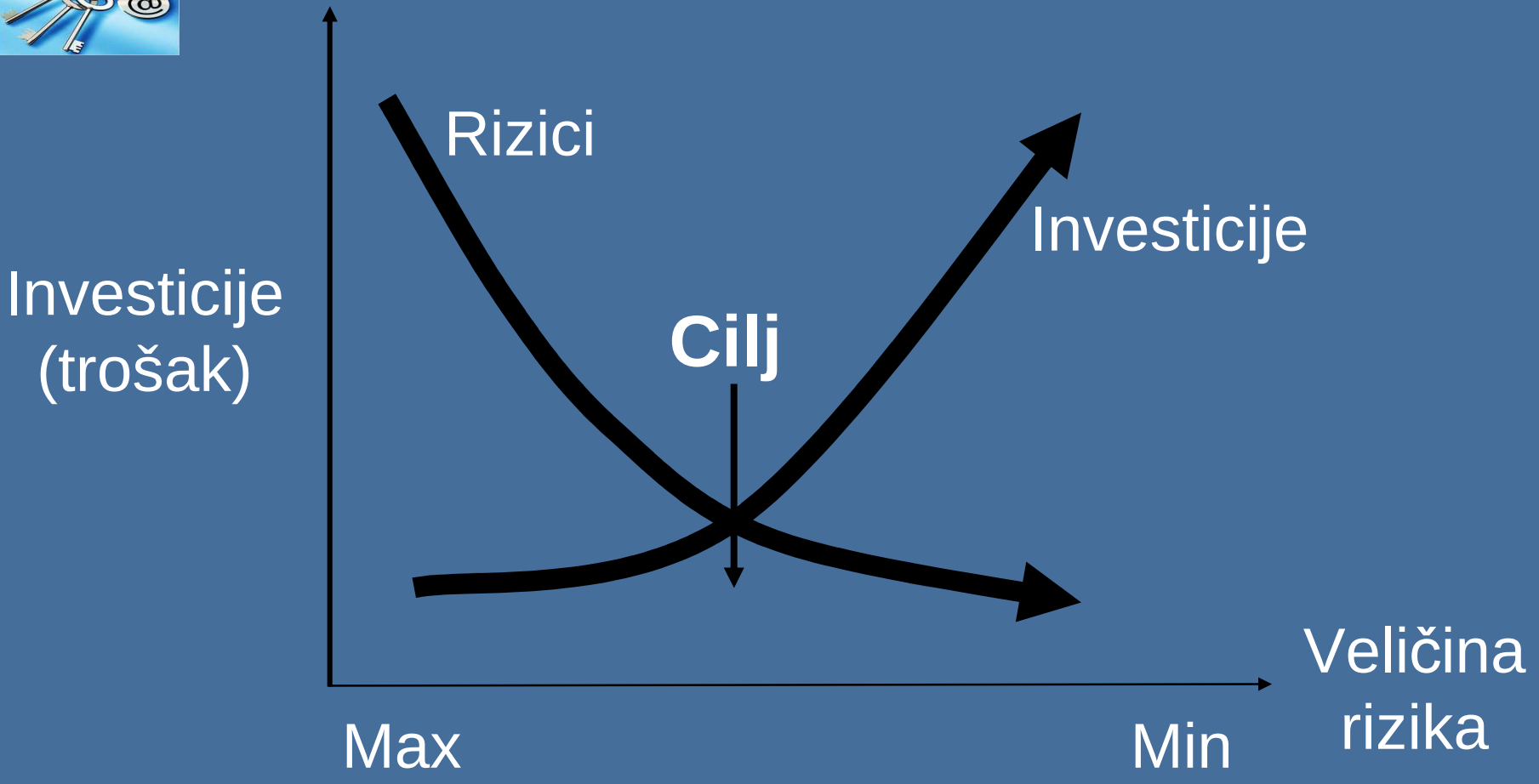
1. Primjenjivanje odgovarajućih kontrola za smanjenje rizika
2. Svjesno i objektivno prihvaćanje rizika (ako on zadovoljava politiku organizacije i kriterije za prihvaćanje rizika)
3. Izbjegavanje rizika
4. Prijenos rizika na druge strane, npr. osiguravatelje ili dobavljače

Koje kontrole odabrati?

Kontrole mogu uključivati:

- Kontrole iz ISO/IEC 27001:2005 Anex A
- Kontrole iz zakona i ostalih regulativa
- Zahtjeve korisnika
- Zahtjeve organizacije
- Ostale važeće kontrole

ODNOS RIZIKA I TROŠKA SIGURNOSTI



SVRHA - Odrediti prihvatljiv rizik

Obavezni dokumenti vezani za rizike po ISO 27001

- Metodologija procjene i postupanja s rizicima
- Izvješće o procjeni rizika
- Plan postupanja s rizicima
- Izjava o primjenjivosti - SOA

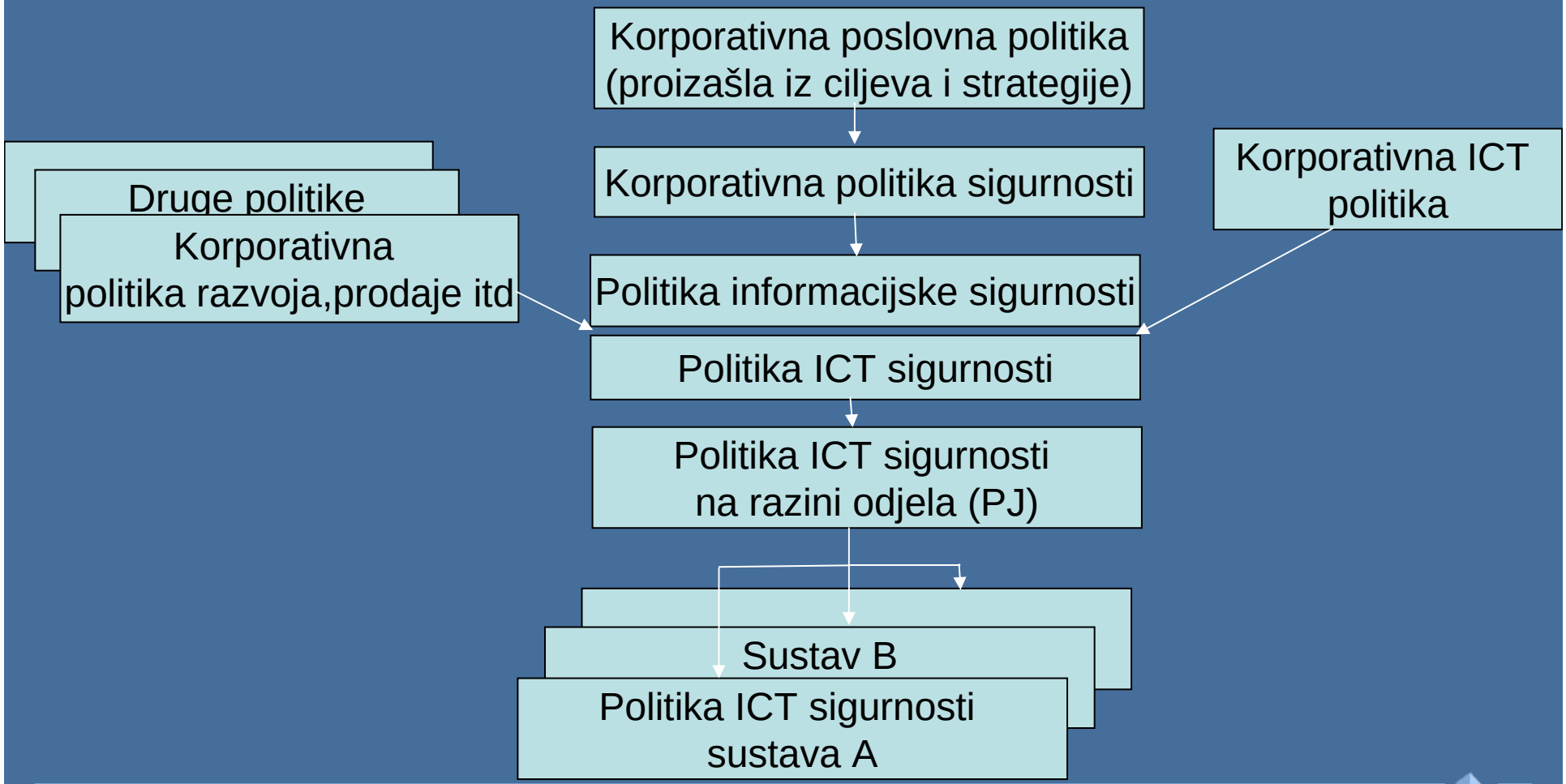
Izjava o primjenjivosti (SOA)

- Izjava o primjenjivosti - SOA (Statement of Applicability) je dokument u koji se zapisuju razlozi odabira tj. isključenja pojedinih kontrola.

IMPLEMENTACIJA I MJERENJE UČINKOVITOSTI ISMS-a

- Odabrane sigurnosne kontrole implementiraju se kroz:
  - Organizaciju za sigurnost
  - Dokumentaciju (politike, procedure, upute, …)
  - Fizičku provedbu sigurnosnih mjera
  - Instalaciju i konfiguraciju softvera u skladu sa sigurnosnim zahtjevima
  - Obuku osoblja
  - Procjene itd.

Politika informacijske sigurnosti kao krovni dokument



Zahtjevi norme ISO 27001:2005

- 4. Sutav upravljanja informacijskom sigurnošću
- 5. Odgovornost uprave
- 6. Interne procjene ISMS-a
- 7. Ocjena sustava od strane uprave
- 8. Poboljšanja ISMS-a
- Anex A

Annex A

A.5 Politika sigurnosti
A.6 Organizacija informacijske sigurnosti
A.7 Upravljanje imovinom
A.8 Sigurnost ljudskog potencijala
A.9 Fizička sigurnost i sigurnost okruženja
A.10 Upravljanje komunikacijama i operacijama
A.11 Kontrola pristupa
A.12 Nabava, razvoj i održavanje informacijskih sustava
A.13 Upravljanje sigurnosnim incidentom
A.14 Upravljanje kontinuitetom poslovanja
A.15 Sukladnost

Veza normi ISO 27001:2005 i ISO 27002:2005

ISO 27001 - Anex A:		ISO 27002:
A.5	→	Klauzula 5
A.6	→	Klauzula 6
A.7	→	Klauzula 7
A.8	→	Klauzula 8
A.9	→	Klauzula 9
A.10	→	Klauzula 10
A.11	→	Klauzula 11
A.12	→	Klauzula 12
A.13	→	Klauzula 13
A.14	→	Klauzula 14
A.15	→	Klauzula 15

Zakonska regulativa RH u području informacijske sigurnosti

Zakon o informacijskoj sigurnosti

Uredba o mjerama informacijske sigurnosti

Pravilnici
Standardi informacijske sigurnosti

- Zakon o tajnosti podataka
- Zakon o pravu na pristup informacijama
- Zakon o zaštiti osobnih podataka
- Zakon o autorskom pravu i srodnim pravima

- Pravilnik o standardima sigurnosne provjere
- Pravilnik o standardima fizičke sigurnosti
- Pravilnik o standardima sigurnosti podataka
- Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava
- Pravilnik o standardima sigurnosti poslovne suradnje

Pripreme za implementaciju ISMS-a

Pripremne radnje za implementaciju ISMS-a obuhvaćaju:

- Pregled i ovjeru dokumentacije ISMS-a
- Distribuciju dokumentacije svima na koje se odnosi (djelatnici i treća strana)
- Edukaciju i osvješćivanje djelatnika

Edukacija djelatnika

- Pri implementaciji ISMS-a potrebno je provesti više vidova edukacije:
  - Obuku djelatnika za postupanje u skladu sa zahtjevima norme ISO 27001:2005 i ISMS dokumentacijom koja se na njih odnosi, uz obavezni osvrt na njihove odgovornosti
  - Obuku internih procjenitelja koji će provoditi interne procjene ISMS-a
  - Awareness radionice za podizanje svijesti o informacijskoj sigurnosti - kontinuirano

Implementacija sustava i ono što slijedi

- Nakon provedenih pripremnih radnji, sustav se implementira i kontinuirano nadzire i poboljšava:
  - Provode se interne procjene primjene sustava u praksi
  - Analiziraju se rezultati procjena i otklanjaju nesukladnosti
  - Prate se metrike za mjerenje učinkovitosti implementiranih kontrola
  - Uprava vrši ocjenu sustava na temelju informacija o njegovom funkcioniranju, dobivenih iz različitih izvora

Pitanja...

Nedoumice...

Nejasnoće...

Hvala.