ZAŠTITA OSOBNIH PODATAKA KAO DIO CJELOVITOG SUSTAVA SIGURNOSTI INFORMACIJA

Silvana Tomić Rotim, Lead Auditor, CISA
ZIH d.o.o.
www.zih.hr

© ZIH

Zaštita osobnih podataka dio cjelovitog sustava sigurnosti ili u suprotnosti s njim?

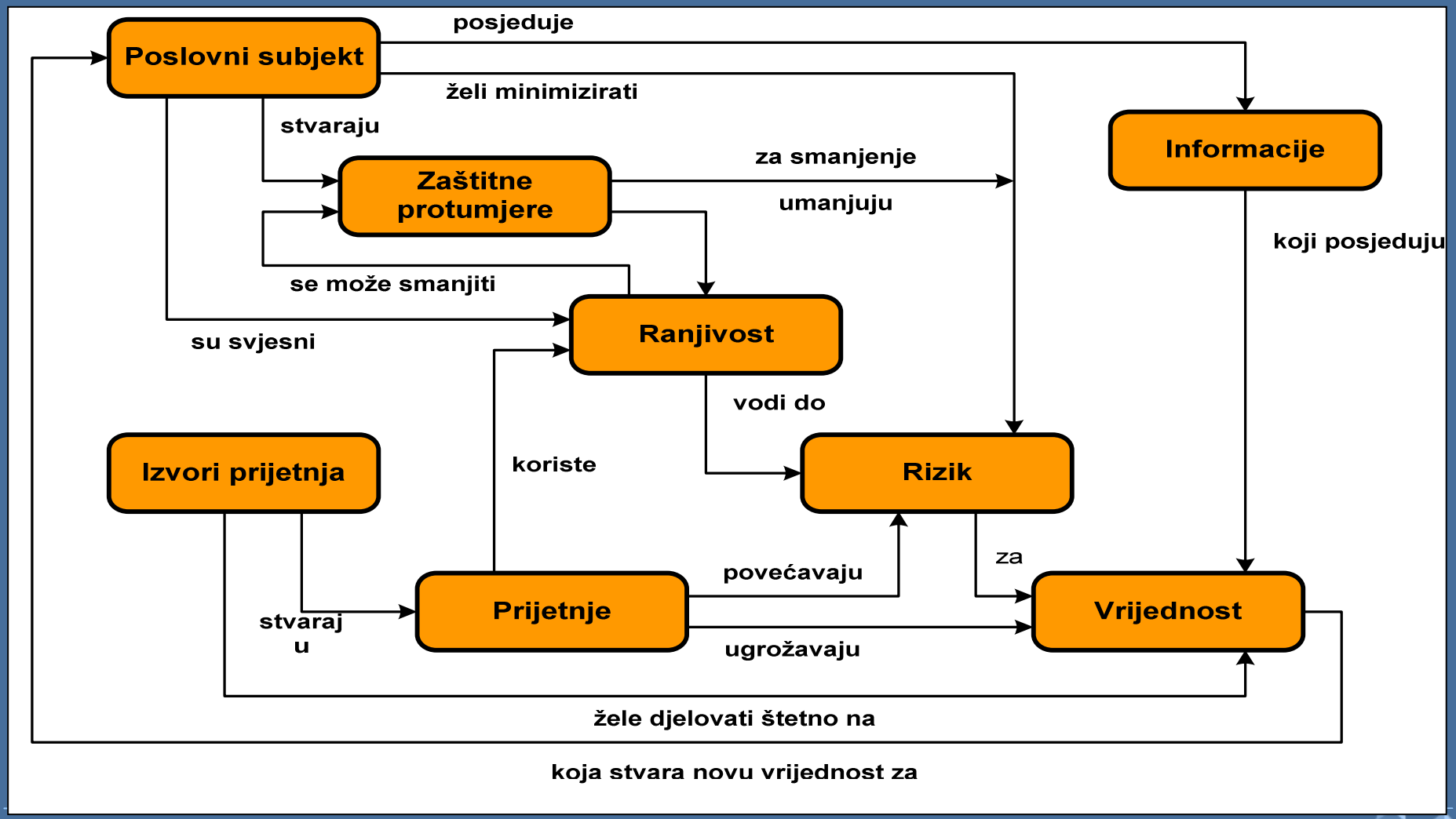
© ZIH

ZAŠTO SUSTAVI SIGURNOSTI INFORMACIJA ?

- Zaštita informacijske imovine – ***i ljudskih resursa***
- Nesmetano odvijanje poslovnih procesa
- Zahtjev poslovne okoline
- Smanjenje ili uklanjanje rizika
- Smanjenje broja incidenata
- Usklađenost sa zakonskom regulativom
- Konkurentnost
- Imidž

© ZIH

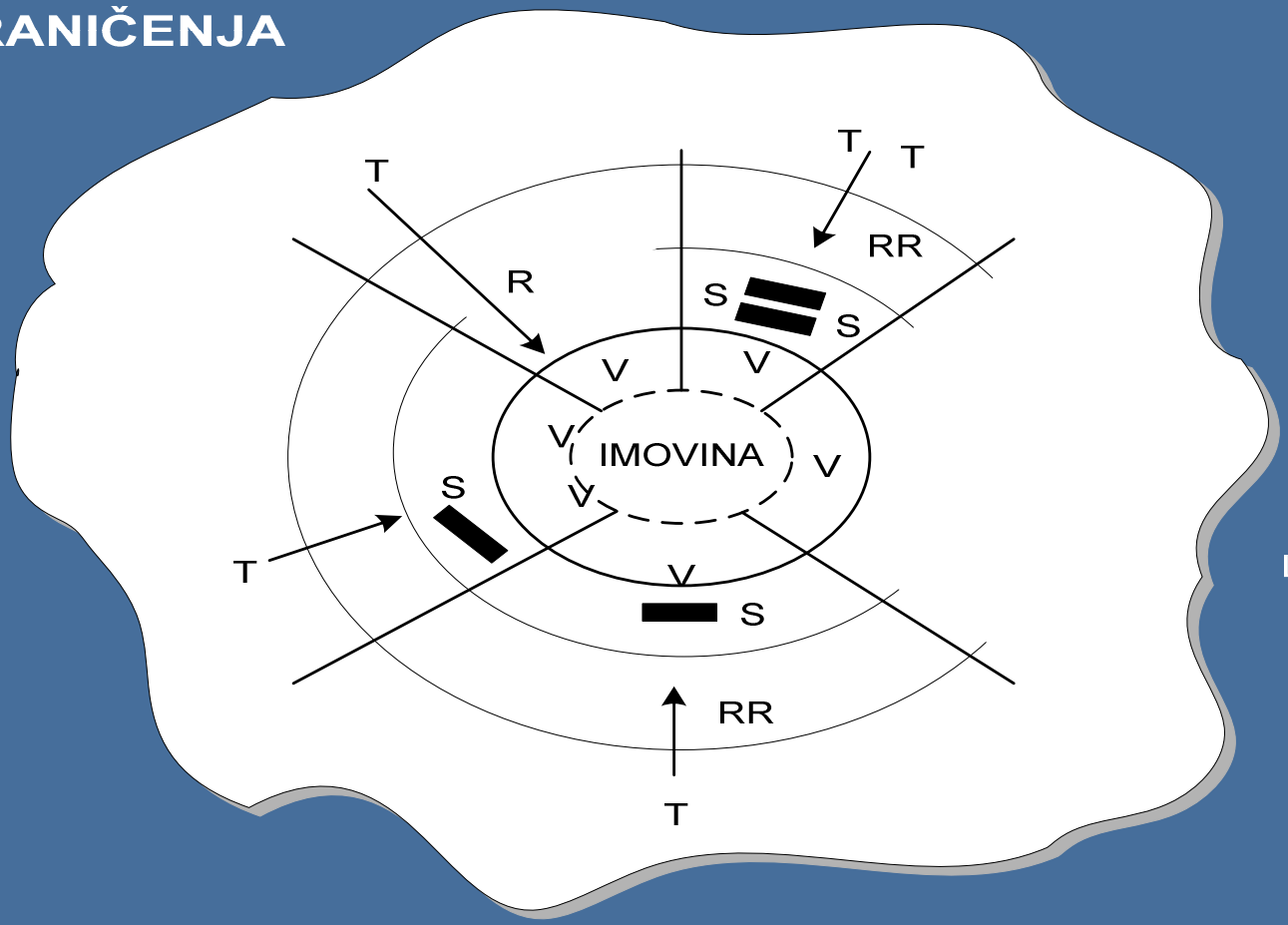
Pogled u informacijsku sigurnost



© ZIH

ODNOSI MEĐU ELEMENTIMA SIGURNOSTI

OGRANIČENJA



Legenda:

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

© ZIH

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.

© ZIH

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

© ZIH

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***

© ZIH

Popis imovine (A.7.1.1)

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

	A	B	C	D	E	F	G
1							
2	**ID**	**Naziv imovine**	**Funkcija**	**Povjerljivost**	**Integritet**	**Raspoloživost**	**Klasifikacijska oznaka**
3	**1**	**OSOBLJE**					
4		*Management*					
5		Pero Perić	direktor	Povjerljivo	Srednje važan	Visoka	Visoka
6		Ivan Ivančić	direktor razvoja	Povjerljivo	Srednje važan	Visoka	Visoka
7		Ana Anić	direktor operative	Povjerljivo	Srednje važan	Visoka	Visoka
8		*Projektanti*					
9		Ante Antić	projektant I	Ograničeno	Uobičajen	Umjerena	Srednja
10		Mario Marić	projektant II	Ograničeno	Uobičajen	Umjerena	Srednja
11		Dinko Dinković	projektant II	Ograničeno	Uobičajen	Umjerena	Srednja
12		*Programeri*					
13		Zoran Zorić	programer I	Ograničeno	Uobičajen	Niska	Srednja
14		Tea Tenić	programer II	Povjerljivo	Srednje važan	Niska	Srednja
15		Nina Ninić	programer II	Povjerljivo	Srednje važan	Niska	Srednja
16		*Sistem administratori*					
17		Slaven Slavić					
18		Neven Nević					

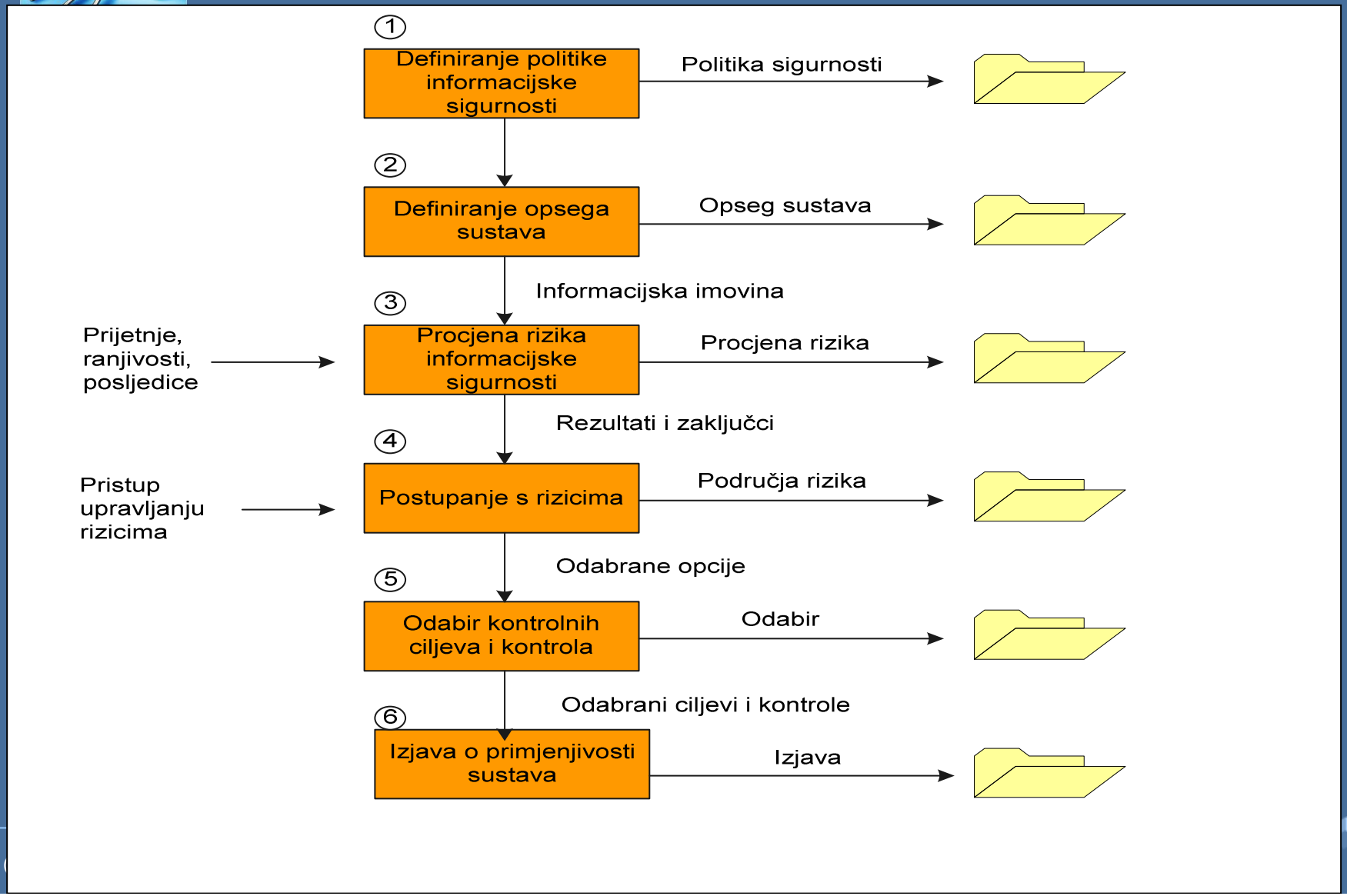
© ZIH

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

© ZIH

Upravljanje sigurnosnim rizicima



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

© ZIH

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:
  - Manipulacija osobnim podacima zaposlenika
  - 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 …)

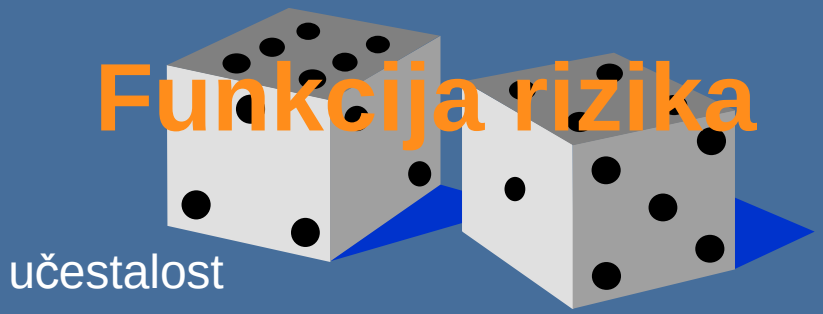
© ZIH

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:
  - Nepostojanje pravila zaštite i privatnosti osobnih podataka
  - Nezaštićen fizički pristup osjetljivim prostorima
  - Nepostojanje UPS-a
  - Nekorištenje antivirusnih programa
  - Nedefinirana pravila logičkog pristupa aplikacijama

© ZIH

Funkcija rizika



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

© ZIH

Procjena rizika – primjer metodologije

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

© ZIH

Procjena rizika – primjer za osoblje

	A	B	C	D	E	F	G	I
1	Grupe imovine	Vrijednost grupe imovine	Prijetnja	Vjerojatnost ostvarivanja prijetnje	Ranjivost	Razina ranjivosti informacijske imovine	Razina rizika	Prijedlog dodatnih kontrola
456	*OSOBLJE*	3	Neplanirano odsustvovanje ili iznenadan odlazak zaposlenika iz firme	1	Nepostojanje plana zamjena	1	3	-
457								-
458								Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
459					Nepostojanje postupaka rada	2	4	Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
460			Pogreška osoblja	1	Nejasno definiran posao	2	4	Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
461					Nepostojanje postupaka rada	2	4	Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
462					Nedostatak izobrazbi	2	4	Postupak za odabir kandidata, ugovornih suradnika i treće strane te obuku za rad s aspekta informacijske sigurnosti
463								Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
464					Nedostatak informiranosti o sigurnosti	2	4	Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
465					Nedostatak kontrolnih mehanizama	3	5	Politika informacijske sigurnosti
466								Dorada Pravilnika o radu (s disciplinskim mjerama)
467								Obuka osoblja i periodička komunikacija sigurnosnih zahtjeva ISMSa
468								-
469					Nedostatak politike / standarda / postupka	3	5	ISMS politike i procedure
470			Manipulacija osobnim podacima zaposlenika	1	Nedostatak politike / standarda / postupka	2	4	Politika zaštite i privatnosti osobnih podataka
471			Zlouporaba ovlasti	1	Neadekvatne kontrole kod zapošljavanja	1	3	Postupak za odabir kandidata, ugovornih suradnika i treće strane te obuku za rad s aspekta informacijske sigurnosti
472								-
473					Zlouporaba ovlasti od strane djelatnika tvrtke	2	4	Izjava o prihvaćanju administratorskih odgovornosti
474								Stimuliranje zaposlenika (vrijeme za samoučenje, bonusi, etc.)

© ZIH

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

© ZIH

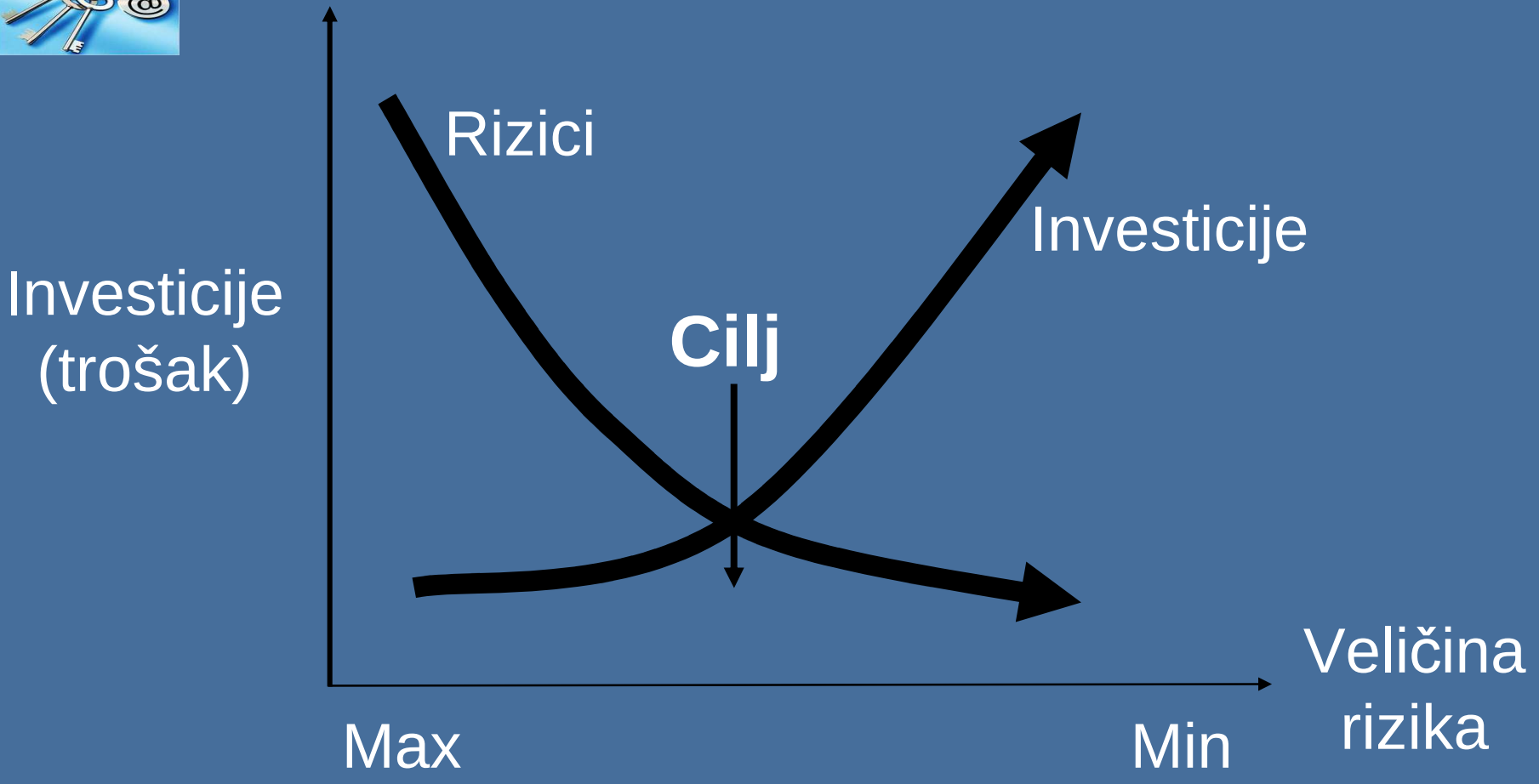
Koje kontrole odabrati?

Kontrole mogu uključivati:

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

© ZIH

ODNOS RIZIKA I TROŠKA SIGURNOSTI



SVRHA - Odrediti prihvatljiv rizik

© ZIH

Koje kontrole odabrati za zaštitu osobnih podataka?

Zaštita osobnih podataka

Zakon o zaštiti osobnih podataka

ISO 27001 Anex A.15 Sukladnost

Izmjene i dopune Zakona o zaštiti osobnih podataka

Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka

Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka

A.15.1.4 Zaštita podataka i privatnosti osobnih informacija

A.8.1.2 Odabir kandidata – zaštita osobnih podataka pri provjeri kandidata

© ZIH

ISO 27001 A.15 Sukladnost

- Sukladnost sa zakonskim propisima
- Sukladnost sa sigurnosnim politikama i standardima i tehnička sukladnost
- Razmatranja revizije informacijskih sustava

© ZIH

Sukladnost sa zakonskim propisima

Cilj:

Sprječavanje kršenja svih pravnih, zakonskih, regulativnih ili ugovornih obveza i sigurnosnih zahtjeva.

A.15.1.1 Određivanje primjenjivih zakona

A.15.1.2 Prava intelektualnog vlasništva

A.15.1.3 Zaštita organizacijskih zapisa

A.15.1.4 Zaštita podataka i privatnosti osobnih informacija

A.15.1.5 Sprječavanje zlouporabe opreme za obradu informacija

A.15.1.6 Odredbe o kriptografskim kontrolama

© ZIH

Zaštita podataka i privatnosti osobnih informacija (A.15.1.4)

Potrebno je osigurati zaštitu podataka i privatnosti u skladu s važećim zakonskim propisima i odredbama i, ako je primjenjivo, ugovornim člancima.

Osobni podataka je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati…

© ZIH

ISO 27001 A.8 Sigurnost ljudskog potencijala

- Prije zaposlenja
- Tijekom zaposlenja
- Prekid ili promjena zaposlenja

© ZIH

Prije zaposlenja

Cilj:

Osigurati da zaposlenici, ugovorni suradnici ili treće strane shvate svoje odgovornosti, osigurati da budu podobni za posao za koji su predviđeni, te na taj način smanjiti rizik od krađa, prijevara i korištenja sredstava u krive svrhe.

A.8.1.1 Funkcije i odgovornosti

A.8.1.2 Odabir kandidata

A.8.1.3 Trajanje i uvjeti zaposlenja

© ZIH

Odabir kandidata (A.8.1.2)

- Kod odabira kandidata za posao, ugovornih suradnika ili korisnika trećih strana potrebno je:
  - Provjeriti dostupnost zadovoljavajućih karakternih referenci
  - Provjeriti točnost životopisa
  - Obaviti nezavisnu provjeru identiteta
  - Akademske i profesionalne kvalifikacije
  - Te ukoliko je to potrebno, provjeriti kreditnu sposobnost ili provjeriti da li je kandidat kažnjavan
    - ***Da li je to u suprotnosti sa zaštitom osobnih podataka?***

© ZIH

Što to konkretno znači?

- Načiniti Politiku zaštite podataka i privatnosti osobnih informacija
- Upoznati sve djelatnike koji sudjeluju u obradi osobnih podataka s tom Politikom
- Voditi pri tome računa da je Politika usklađena s
- Od kandidata dobiti pismenu suglasnost za korištenje njihovih osobnih podataka u svrhu odabira

Zaštita podataka i privatnosti osobnih informacija definirana je Zakonom o zaštiti osobnih podataka, Uredbom o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka i Uredbom o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka.

Osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.

Osobni podaci moraju biti točni, potpuni i ažurni te se unutar tvrtke prikupljaju samo u svrhu s kojom je upoznat davatelj podataka, a obrađuju sukladno zakonskim odredbama i ograničenjima. Tvrtka ne smije davati te podatke trećim stranama, niti ih koristiti u bilo koju drugu svrhu bez pristanka davatelja podataka.

Za upravljanje osobnim podacima unutar tvrtke odgovoran je …

© ZIH

Zaključak

- Obavezni ste uskladiti se sa zakonskom regulativom
- To je moguće učiniti na više načina, ali pristup razvoja cjelovitog sustava sigurnosti informacija vam pruža najviše – i sigurnost vašeg sustava i zaštitu osobnih podataka
- Pripremite vaša pravila ponašanja po pitanju informacijske sigurnosti i zaštite osobnih podataka i svakako…
- … primjenjujte ih u praksi!

© ZIH

Pitanja...

Nedoumice...

Nejasnoće...

Hvala.

© ZIH