

Управљање безбедношћу и ризицима

Принципи и кључни концепти управљања Информационом безбедношћу



Бранко Суботић, Консултант
Контакт: branko.subotic@rs.ey.com



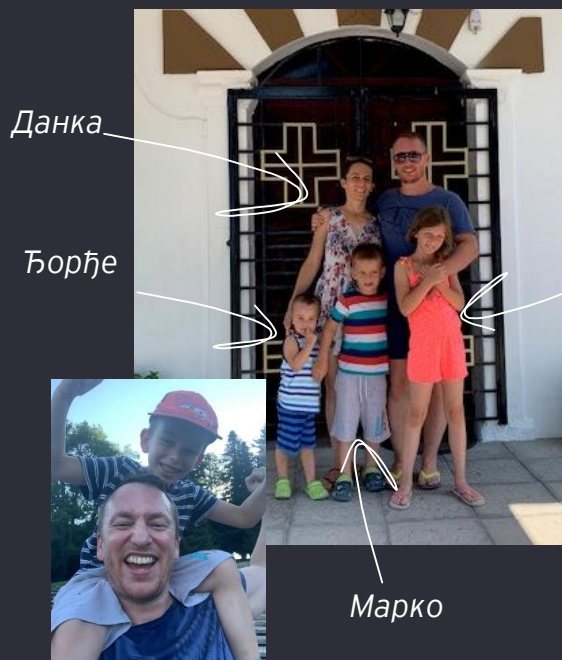
Бранко Суботић
Косултант, ЕУ

О мени

Моја породица:

Шта волим да радим:

Шта би још волео да радим:



Данка

Ђорђе

Јована

Марко

Моје
колеге



Код клијента -
после поноћи



Београдски
маратон

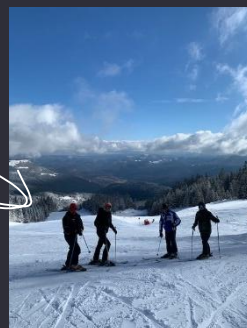


Зелена фарма, РС



Моја гитара

Јахорина, РС



Принципи и кључни концепти управљања Информационом безбедношћу

- ▶ Увод: Основни појмови

- ▶ Организациона и управљачка структура Информационе безбедности

 - Организациона поставка

 - Улоге и одговорности

 - Управљачки стандарди и контролни оквири

 - Значај запослених

- ▶ Основни концепти Информационе безбедности

 - Нивои Информационе безбедности

 - СИА концепт

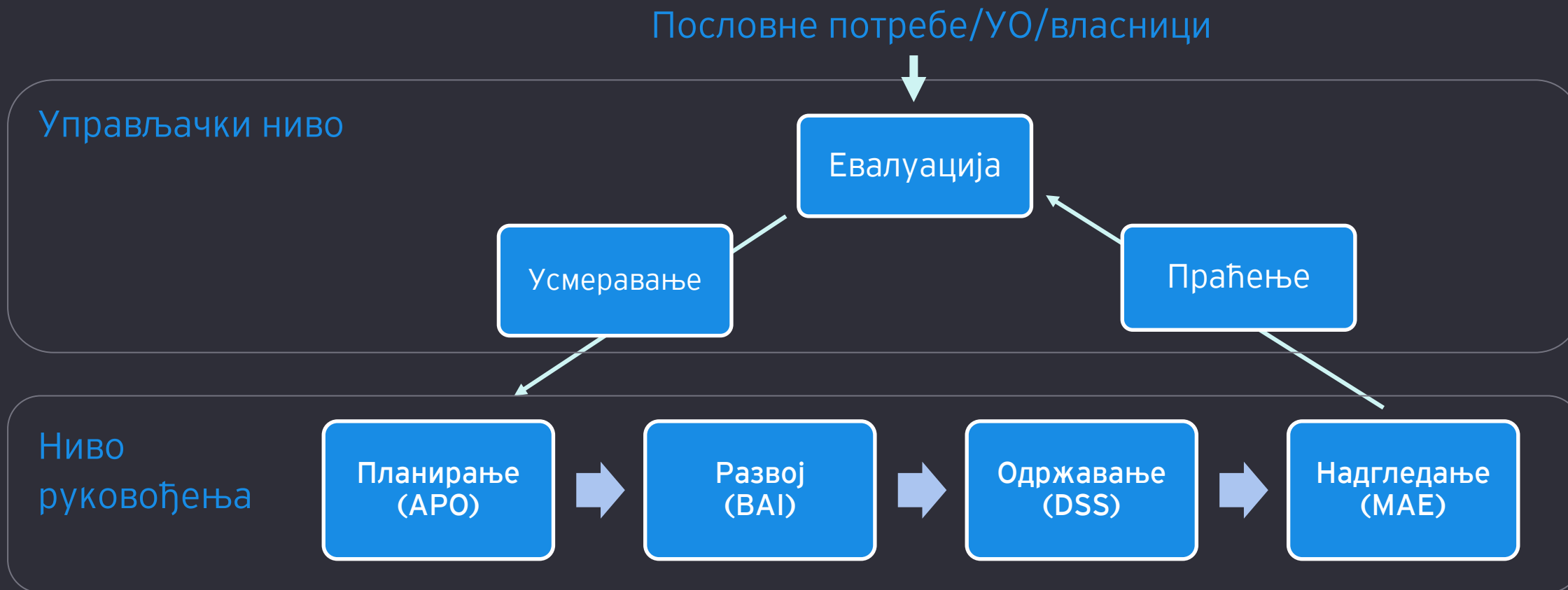
 - Концепт управљања ризицима

 - Концепт идентификације, аутентификације и ауторизације

- ▶ Студија случаја

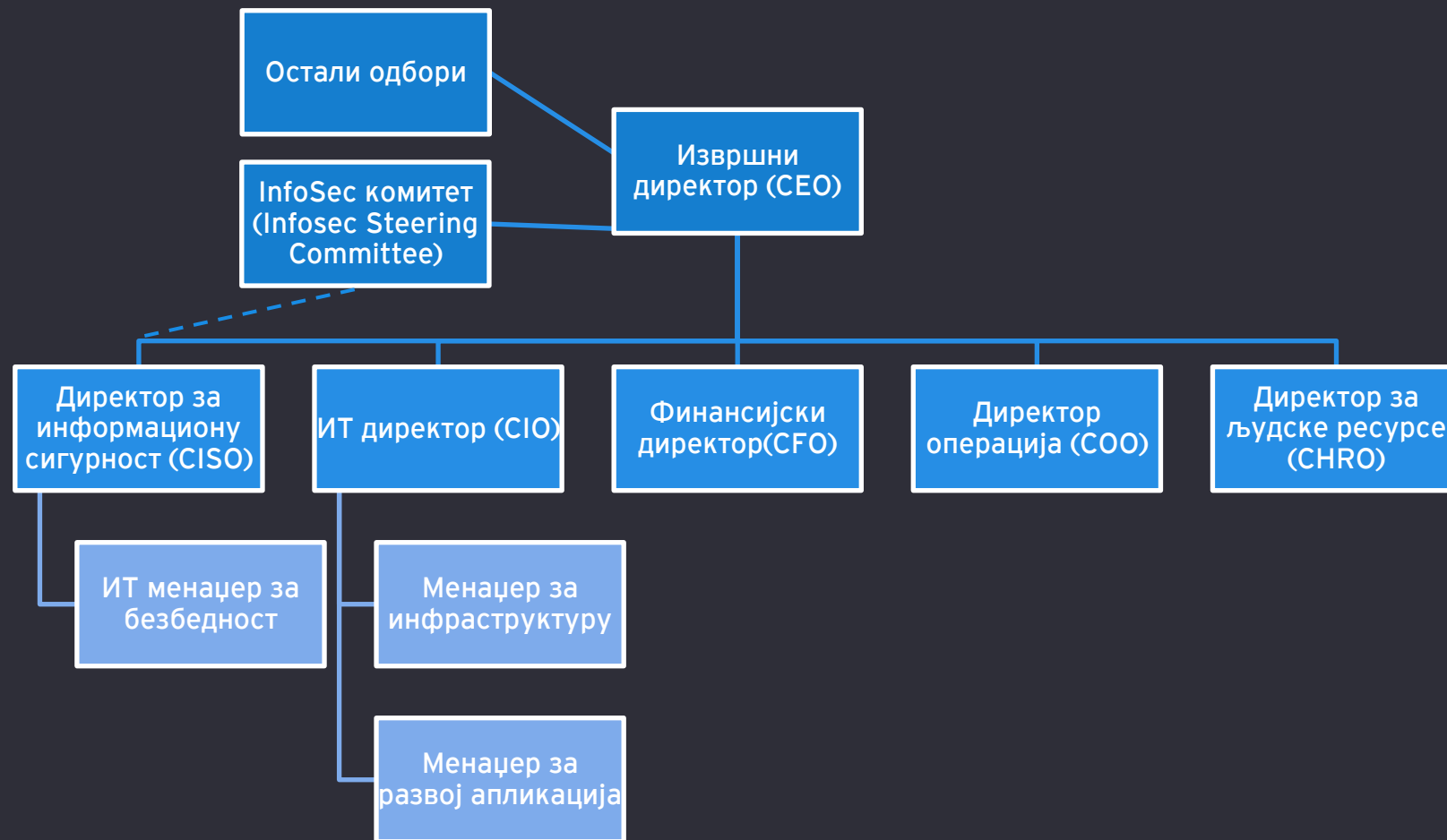
Увод: Основни појмови

- ▶ Информациона безбедност и сајбер безбедност
- ▶ Управљање (Governance) и руковођење (Management)



Организациона и управљачка структура информационе безбедности

- Управљачка структура у корпорацијама и место Информационе безбедности



Организациона и управљачка структура информационе безбедности

► Улоге и одговорности у систему управљања информационом безбедношћу

Управљачко тело	Учесници	Одговорност
InfoSec комитет	CEO, CFO, COO, CIO, председава CISO	Успоставља и промовише програме информационе безбедности
Извршни менаџмент	С-ниво менаџмента (Топ менаџмент)	Спроводи управљачке контроле и евалуацију InfoSec програма
Директор за информациону сигурност (CISO)	CISO и тим	Усмерава, прати и координише имплементацију програма информационе безбедности
Пословна одељења (јединице)	Менаџери одељења и тимови	Власници података и процеса. Дефинишу и приоритизирају захтеве за заштитом информационих добара

► Подршка топ менаџмента

Организациона и управљачка структура информационе безбедности

- ▶ **Управљачи стандарди и контролни оквири**
- ▶ PCI-DSS - Payment Card Industry Data Security Standard
- ▶ COBIT - Control Objectives for Information and related Technology. Дефинисање циљева са ИТ сегмент, на основу пословних циљева - потребе стјекхолдера су мапирани на релевантне ИТ циљеве
- ▶ COSO - Committee of Sponsoring Organizations. Циљеви за целу организацију
- ▶ ITIL - Information Technology Infrastructure Library. IT Service Management (ITSM).
- ▶ FRAP - Facilitated Risk Analysis Process.
- ▶ ISO 27000 серија (ISO 27001: Успостављање, имплементација, контрола и унапређење ИСМС-а)

Организациона и управљачка структура информационе безбедности

- Значај запослених као најважније карике у ланцу информационе безбедности

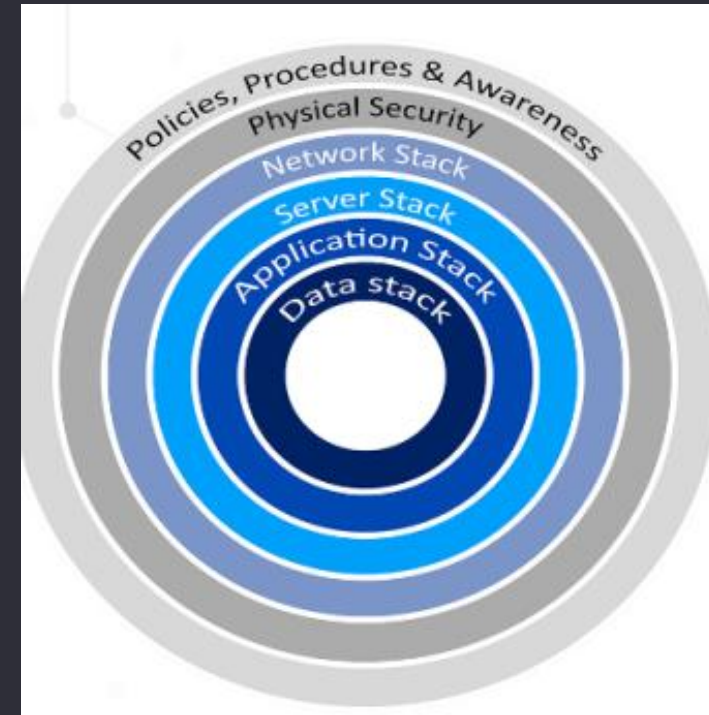


Организациона и управљачка структура информационе безбедности

► Кратка питања

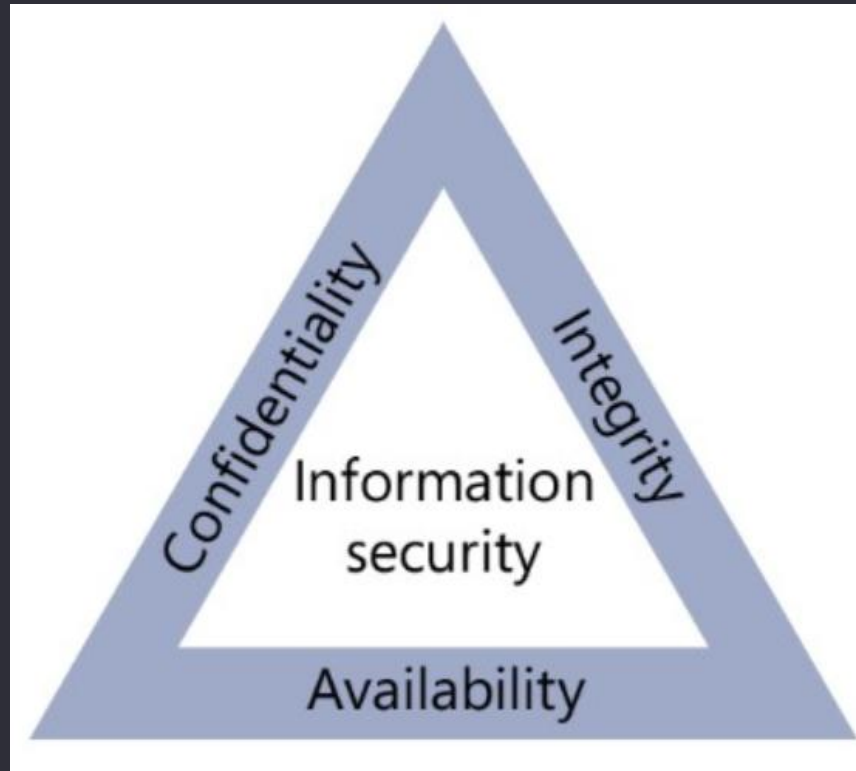
Основни концепти Информационе безбедности

- ▶ **Нивои информационе безбедности**
- ▶ Органски ниво - ниво запослених (политике, процедуре и свест)
- ▶ Физичка безбедност
- ▶ Ниво мреже
- ▶ Ниво сервера
- ▶ Ниво апликација
- ▶ Ниво података (базе података)



Основни концепти Информационе безбедности

- Основни циљеви информационе безбедности: Поверљивост, интегритет и доступност



Основни концепти Информационе безбедности

- ▶ Поверљивост, интегритет и доступност

Претње:

Одговори (контроле):

Основни концепти Информационе безбедности

► Поверљивост, интегритет и доступност

Претње:

- Кriptoанализа (напади на механизме енкрипције)
- Социјални инжењеринг
- Keyloggers, камере
- IoT - потенцијални back-door до ваших уређаја и система

Одговори (контроле):

- Енкрипција за податке у мировању (нпп. AES256), енкрипција целог диска
- Сигурне транспортне протоколе за податке у покрету (SSL, TLS, IPSEC)
- Најбоље праксе за податке у употреби - политика чистог стола, превенција гледања преко рамена - заштите екрана, аутоматско закључавање уређаја
- Јаке лозинке, вишефакторска аутентификација

Основни концепти Информационе безбедности

- ▶ Поверљивост, **интегритет** и доступност

Претње:

Одговори (контроле):

Основни концепти Информационе безбедности

► Поверљивост, **интегритет** и доступност

Претње:

- Неуторизоване модификације података
- Инјекције кода
- Кriptoанализа

Одговори (контроле):

- Енкрипција података (поново)
- Контролне суме (као што је CRC - Cycling redundancy checks)
- Hashing контроле (MD5, SH1, SHA2)
- Дигитално потписивање
- Контроле приступа

Основни концепти Информационе безбедности

- ▶ Поверљивост, интегритет и **доступност**

Претње:

Одговори (контроле):

Основни концепти Информационе безбедности

► Поверљивост, интегритет и **доступност**

Претње:

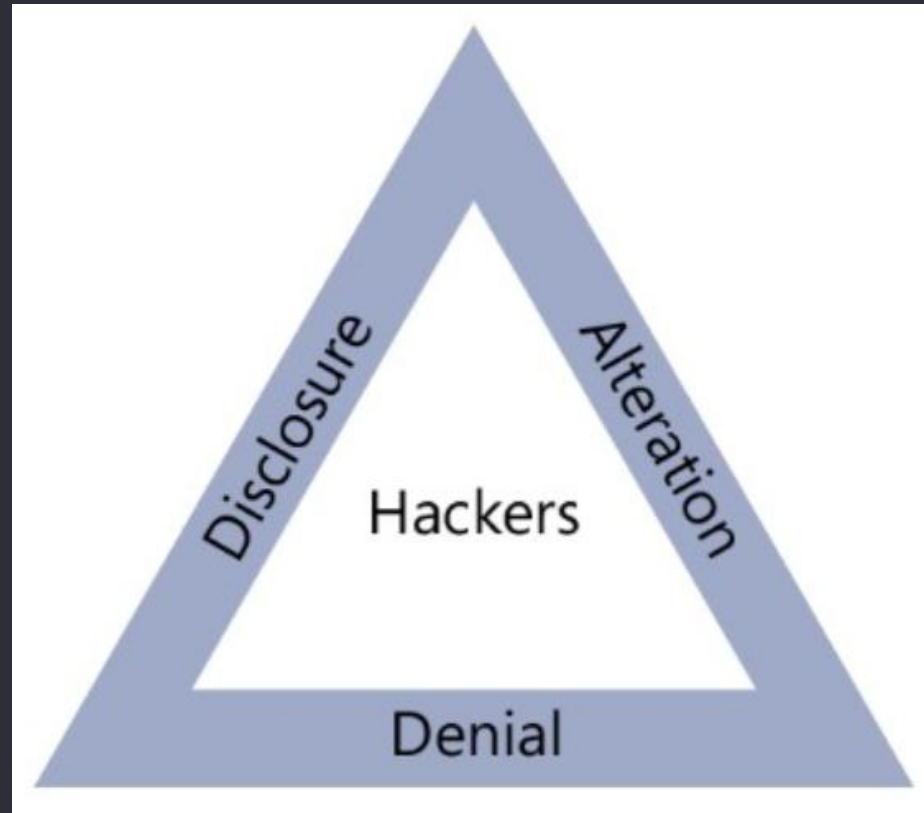
- Малициозни напади (нпр. DDOS, физичко компромитовање сервера)
- Грешке у коду
- Кварови хардверских компоненти

Одговори (контроле):

- IPD/IDS
- Управљање закрпама
- Редуданција хардверских капацитета и енергије
- СЛА уговори

Основни концепти Информационе безбедности

- Основни циљеви нападача: Објављивање, Мењање и Блокирање



Основни концепти Информационе безбедности

- ▶ Концепт управљања ризицима
- ▶ Информационо добро и рањивост информационог добра
- ▶ Претња по информационо добро (по неком од ЦИА циљева)
- ▶ Вероватноћа реализације претње
- ▶ Утицај реализације претње

Основни концепти Информационе безбедности

► Концепти Идентификације, Аутентификације и Ауторизације

