**\* OVO JE BESPLATNI OGLEDNI PREDLOŽAK DOKUMENTA \***

[logo organizacije]

[naziv organizacije]

**METODOLOGIJA ZA PROCJENU I OBRADU RIZIKA**

|  |  |
| --- | --- |
| Oznaka: |  |
| Verzija: |  |
| Datum verzije: |  |
| Izradio/la: |  |
| Odobrio/la: |  |
| Stupanj povjerljivosti: |  |

**Povijest promjena**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Verzija** | **Izradio/la** | **Opis promjena** |
|  | 0.1 | Advisera | Osnovni nacrt dokumenta |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sadržaj**

[1. Svrha, područje primjene i korisnici 3](#_Toc216131009)

[2. Referentni dokumenti 3](#_Toc216131010)

[3. Metodologija procjene i obrade rizika 3](#_Toc216131011)

[3.1. Procjena rizika 3](#_Toc216131012)

[3.1.1. Proces 3](#_Toc216131013)

[3.1.2. Resursi, ranjivosti i prijetnje 3](#_Toc216131014)

[3.1.3. Utvrđivanje vlasnika rizika 4](#_Toc216131015)

[3.1.4. Posljedice i vjerojatnost 4](#_Toc216131016)

[3.2. Kriteriji prihvatljivosti rizika 4](#_Toc216131017)

[3.3. Obrada rizika 5](#_Toc216131018)

[3.4. Redoviti pregledi procjene i obrade rizika 5](#_Toc216131019)

[3.5. Izvješće o primjenjivosti i Plan obrade rizika 5](#_Toc216131020)

[3.6. Izvještavanje 5](#_Toc216131021)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 6](#_Toc216131022)

[5. Valjanost i upravljanje dokumentom 7](#_Toc216131023)

[6. Prilozi 7](#_Toc216131024)

# Svrha, područje primjene i korisnici

Svrha je ovog dokumenta propisati metodologiju procjene i obrade informacijskih rizika u [naziv organizacije], kao i određivanje prihvatljivog nivoa rizika, sukladno s normom ISO/IEC 27001.

Procjena i obrada rizika primjenjuju se na cjelokupni opseg Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*), odnosno na sve informacijske resurse koji se koriste unutar organizacije ili koji mogu imati utjecaj na informacijsku sigurnost u ISMS-u.

Korisnici su ovog dokumenta svi zaposlenici [naziv organizacije] koji sudjeluju u procjeni i obradi rizika.

# Referentni dokumenti

* Norma ISO/IEC 27001, točke 6.1.2, 6.1.3, 8.2 i 8.3
* Norma ISO 22301, točke 8.2.1 i 8.2.3
* Politika informacijske sigurnosti
* Popis pravnih, regulatornih , ugovornih i drugih zahtjeva
* Politika sigurnosti dobavljača
* Izvješće o primjenjivosti

# Metodologija procjene i obrade rizika

## Procjena rizika

### Proces

Procjena rizika provodi se kroz Tablicu procjene rizika. Proces procjene rizika koordinira [naziv radnog mjesta], utvrđivanje prijetnji i ranjivosti provode vlasnici resursa, a procjenu posljedica i vjerojatnosti provodi vlasnik rizika. [Naziv radnog mjesta] je odgovoran za uključivanje podataka o prijetnjama, ranjivostima, posljedicama i vjerojatnosti u Tablicu procjene rizika.

### Resursi, ranjivosti i prijetnje

Prvi je korak u procjeni rizika utvrditi sve informacijske resurse u opsegu ISMS-a od strane predstavnika svakog područja u opsegu ISMS-a – tj. utvrditi sve resurse koji mogu utjecati na povjerljivost, cjelovitost i dostupnost informacija u organizaciji. Resursi mogu uključivati dokumente u papirnatom i elektroničkom obliku, aplikacije i baze podataka, ljude, IT opremu, infrastrukturu i vanjske usluge/vanjske procese. Prilikom utvrđivanja resursa potrebno je odrediti i njihove vlasnike – osobu ili organizacijsku jedinicu odgovornu za svaki od resursa.

Sljedeći je korak da vlasnici resursa utvrde sve prijetnje i ranjivosti vezane za pojedini resurs. Prijetnje i ranjivosti određuju se putem kataloga uključenih u Tablicu procjene rizika. Svaki resurs može biti povezan s nekoliko prijetnji, a svaka prijetnja može biti povezana s nekoliko ranjivosti.

### Utvrđivanje vlasnika rizika

Za svaki rizik potrebno je utvrditi i vlasnika rizika – osobu ili organizacijsku jedinicu odgovornu za pojedini rizik. Ta osoba može, ali ne mora, biti ista kao i vlasnik resursa.

### Posljedice i vjerojatnost

Nakon određivanja vlasnika rizika, potrebno je procijeniti posljedice za svaku kombinaciju prijetnji i ranjivosti za pojedini resurs, ukoliko se takav rizik ostvari:

|  |  |  |
| --- | --- | --- |
| Slabe posljedice | 0 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti ne utječe na financije organizacije, pravne ili ugovorne obveze, ili njen ugled. |
| Srednje posljedice | 1 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti uzrokuje troškove te ima manji ili srednji utjecaj na pravne ili ugovorne obveze, ili ugled organizacije. |
| Velike posljedice | 2 | Gubitak povjerljivosti, dostupnosti ili cjelovitosti ima značajan i/ili trenutni utjecaj na financije organizacije, poslovanje, pravne ili ugovorne obveze, ili ugled organizacije. |

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

(Kako biste pristupili potpunoj verziji dokumenta molimo Vas da kupite ISO 27001 i ISO 22301 Premium paket dokumentacije   
<https://advisera.com/27001academy/hr/iso-27001-iso-22301-premium-paket-dokumentacije/>)