**\* 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](#_Toc216132335)

[2. Referentni dokumenti 3](#_Toc216132336)

[3. Metodologija procjene i obrade rizika 3](#_Toc216132337)

[3.1. Procjena rizika 3](#_Toc216132338)

[3.1.1. Proces 3](#_Toc216132339)

[3.1.2. Resursi, ranjivosti i prijetnje 3](#_Toc216132340)

[3.1.3. Utvrđivanje vlasnika rizika 3](#_Toc216132341)

[3.1.4. Posljedice i vjerojatnost 4](#_Toc216132342)

[3.2. Kriteriji prihvatljivosti rizika 4](#_Toc216132343)

[3.3. Obrada rizika 4](#_Toc216132344)

[3.4. Redoviti pregledi procjene i obrade rizika 5](#_Toc216132345)

[3.5. Izvještavanje 5](#_Toc216132346)

[4. Upravljanje zapisima koji se vode temeljem ovog dokumenta 5](#_Toc216132347)

[5. Valjanost i upravljanje dokumentom 6](#_Toc216132348)

[6. Prilozi 6](#_Toc216132349)

# 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 22301.

Procjena i obrada rizika primjenjuju se na cjelokupni opseg Sustava upravljanja kontinuitetom poslovanja (engl. *Business Continuity Management System – BCMS*), odnosno na sve resurse koji se koriste unutar organizacije ili koji mogu imati utjecaj na informacijsku sigurnost unutar BCMS-a.

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

# Referentni dokumenti

* Norma ISO 22301, točke 8.2.1 i 8.2.3
* Popis pravnih, regulatornih , ugovornih i drugih zahtjeva
* Politika sigurnosti dobavljača

# 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.

### Resursi, ranjivosti i prijetnje

Prvi je korak u procjeni rizika utvrditi sve resurse u opsegu BCMS-a – tj. sve resurse koji mogu izazvati poremećaje u poslovanju. 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 utvrditi 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 dostupnosti ne utječe na financije organizacije, pravne ili ugovorne obveze, ili njen ugled. |
| Srednje posljedice | 1 | Gubitak dostupnosti uzrokuje troškove te ima manji ili srednji utjecaj na pravne ili ugovorne obveze, ili ugled organizacije. |
| Velike posljedice | 2 | Gubitak dostupnosti ima značajan i/ili neposredan utjecaj na financije organizacije, poslovanje, pravne ili ugovorne obveze, ili ugled organizacije. |

Nakon procjene posljedica, potrebno je procijeniti vjerojatnost nastanka takvog rizika, odnosno vjerojatnost da će prijetnja iskoristiti ranjivost predmetnog resursa:

…

**\* ZAVRŠETAK OGLEDNOG PREDLOŠKA \***

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