REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

METODOLOGIJA UPRAVLJANJA TVEGANJ NA PODROČJU INFORMACIJSKE VARNOSTI – vzorčna dokumentacija

Različica:	1.0
Datum veljavnosti:	
Avtor:	
Odobril:	

November 2025

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Analiza obvladovanja tveganj (vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije)« iz 3. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1). Dokument je generičen in je namenjen kot pomoč pri doseganju skladnosti predvsem malim in srednje velikim organizacijam v Republiki Sloveniji (do približno 200 uporabnikov oziroma naprav), ki morajo izpolnjevati zahteve iz ZInfV-1[1].

Dokument je namenjen temu, da organizaciji na pregleden in praktičen način pomaga pri obravnavi tveganj na področju informacijske varnosti. Organizacija mora pri tem upoštevati dejansko stanje svoje informacijsko-komunikacijske infrastrukture, posebnosti svojega sektorja in delovnega področja, sektorsko specifične grožnje in ranljivosti, obseg poslovanja ter relevantne standarde in dobre prakse. Dokument tako predstavlja poenostavljeno, vendar skladno metodologijo, ki je razumljiva tudi uporabnikom brez poglobljenih strokovnih znanj in omogoča doseganje ponovljivih ter primerljivih rezultatov. Dokument podpiše oziroma potrdi vodstvo organizacije, pregleda pa ga najmanj enkrat letno.

Metodologija temelji na zahtevah Zakona o informacijski varnosti (ZInfV-1) ter standardih ISO/IEC 27001:2022 in ISO/IEC 27005:2022. Upravljanje tveganj se izvaja sistematično in strukturirano na ravni (ključnih) informacijskih sredstev (npr. strežniki, končne naprave, aplikacije, omrežje, baze podatkov), pri čemer se za vsako sredstvo ocenjuje vpliv na zaupnost, celovitost, razpoložljivost in avtentičnost (ZCRA), verjetnost uresničitve grožnje ter posledice za poslovanje. Rezultat je kvantitativna ocena tveganj po modelu 5×5.

Dokument ni mišljen kot končni, nespremenljivi dokument, temveč kot praktičen, poenostavljen in takoj uporaben okvir, ki ga je možno prilagoditi specifičnim potrebam vsake posamezne organizacije.

Prilogi dokumenta sta register tveganj in seznam izjem (datoteki .xls), kjer so navedeni vzorčni primeri sredstev, groženj in ranljivosti.

Za bolj sistematično, sledljivo in učinkovito/uspešno izvajanje procesa analize obvladovanja tveganj je priporočljivo označevanje informacijskih sredstev in varnostnih ukrepov z unikatnimi identifikatorji, ki jih je potem možno povezati tako s procesi (analiza vpliva na poslovanje) kot s tveganji (ranljivosti).

<u>Uporabljeni viri</u>:

- *Zakon o informacijski varnosti (Uradni list RS, št. 40/25);*
- *Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024, o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022;*
- *Standard ISO/IEC 27005:2022;*
- *Standard ISO 31000:2018;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *Ocena kibernetskih tveganj, verzija 1.0, URSIV, oktober 2018;*
- *ENISA Threat Landscape 2025, oktober 2025.*[2]

[1] Zavezanci iz ZInfV-1, ki so ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnega centra, ponudniki omrežij za dostavo vsebin, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja, morajo pri pripravi tega dokumenta upoštevati določbe Izvedbene uredbe Komisije (EU) št. 2024/2690, z dne 17. oktobra 2024.
2 https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf.

KAZALO

1. Uvod

Postopek upravljanja tveganj na področju informacijske varnosti omogoča prepoznavanje in vrednotenje pomembnosti tveganj, ki ogrožajo poslovanje organizacije. Na podlagi rezultatov analize tveganj se določijo primerne strategije obravnave, prioritete ter ukrepi za obvladovanje ali popolno odpravo tveganj. Organizacija lahko tudi sprejme posamezna tveganja, kadar ugotovi, da bi bila pričakovana škoda manjša od stroškov, potrebnih za njihovo odpravo.

Analiza tveganj temelji na strukturiranem pristopu k ocenjevanju stopnje tveganja in primerjavi z vnaprej določenimi kriteriji za sprejemljivost tveganja.

Analiza tveganj se izvede v skladu z določeno metodologijo vsaj enkrat letno ali ob organizacijskih spremembah, incidentih ali ob pojavu novih groženj ter posledično tveganj, povezanih s katero koli komponento informacijskega sistema.

2. Obseg in proces obvladovanja tveganj

Analiza informacijskih tveganj se izvaja sistematično, strukturirano, primerljivo in ponovljivo, v skladu z zahtevami 21. in 22. člena Zakona o informacijski varnosti (ZInfV-1) ter smiselno uporabo standarda ISO/IEC 27001:2022 in ISO/IEC 27005:2022. Namen analize je prepoznati, oceniti in obvladovati tveganja, ki bi lahko vplivala na izgubo zaupnosti, celovitosti, razpoložljivosti in avtentičnosti informacijskih sredstev organizacije. Priporočljivo je, da obseg izvedbe ocene in analize tveganj zajema celotno organizacijo.

Analiza tveganj se izvaja v okviru sistema upravljanja informacijske varnosti organizacije in je usklajena s Politiko informacijske varnosti. Vključuje notranji in zunanji kontekst: zakonodajo, pogodbene zahteve, organizacijsko strukturo, posebnosti področja, tehnološko okolje ter zunanje deležnike in dobavitelje.

Analiza tveganj se izvaja v okviru poslovnih procesov na ravni posameznih pomembnih informacijskih sredstev (npr. poštni strežnik, končne delovne postaje, omrežni sistemi, aplikacijski strežniki, podatkovne zbirke ipd.), kar omogoča podrobno identifikacijo in vrednotenje tveganj, povezanih z vsakim sredstvom ali skupino sredstev ter njegovim lastnikom.

Za vsako sredstvo ali skupino (enakih) sredstev se ugotavljajo:

- grožnje in ranljivosti;
- vpliv na izgubo zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA);
- verjetnost uresničenja grožnje ter posledice za poslovanje in
- ocena (faktor) tveganja in ustrezni ukrepi za njegovo zmanjšanje ali sprejem.

Tveganja so nato agregirana na ravni poslovnih procesov organizacije, da se zagotovi celovit pregled nad izpostavljenostjo informacijskih sredstev.

Obseg analize zajema vsa informacijska sredstva, procese, aplikacije, storitve in infrastrukturo, ki podpirajo poslovne cilje organizacije.

Proces upravljanja tveganj vključuje pet ključnih faz, in sicer:

1. identifikacijo oziroma ugotavljanje tveganj (prepoznavanje informacijskih sredstev, groženj, ranljivosti in možnih posledic njihovega uresničenja);

2. merjenje oziroma ocenjevanje tveganj (določita se verjetnost uresničitve posamezne grožnje in posledično tveganja ter vpliv na poslovanje);
3. obvladovanje tveganj (za vsako tveganje se določi ustrezna strategija: zmanjšanje, prenos, sprejem ali izogib; izvedejo se ukrepi in določijo se odgovorne osebe ter roki);
4. spremljanje tveganj (redno se preverjajo uspešnost izvedenih ukrepov, stanje tveganj in spremembe v poslovnem, tehničnem ali zakonodajnem okolju) in
5. poročanje vodstvu o tveganjih (o stanju tveganj in uspešnosti ukrepov se redno poroča vodstvu in odgovorni osebi za informacijsko varnost).

3. Metodologija za izvedbo ocene tveganj

Postopek ocene tveganj temelji na poenostavljenem modelu kvantitativne ocene tveganj, ki upošteva ocenjevanje konteksta organizacije, vrednosti sredstev, ocenjuje verjetnost realizacije grožnje in s tem pojava tveganja in vpliv na poslovanje.

Metodologija temelji na modelu 5×5, kjer je bistveni faktor vpliva pomembnost sredstva (ocena 1 do 5). Tak pristop zagotavlja objektivno in primerljivo oceno tveganj v organizaciji, skladno z zahtevami ISO/IEC 27005:2022 in vključuje opredelitev meril sprejemljivosti tveganj, razlikovanje med inherentnim in rezidualnim tveganjem ter določitev vlog in odgovornosti.

Vsako tveganje ima določene: lastnika sredstva, lastnika tveganja, izvajalca ukrepov in osebo, ki odobri sprejemljivo raven tveganja.

Za vsako tveganje se najprej oceni inherentno tveganje (brez kontrol), nato se pri oceni upoštevajo že uvedene kontrole ter se tako oceni oziroma določi rezidualno (preostalo) tveganje, ki je osnova za odločitev o sprejemu, zmanjšanju ali prenosu tveganja.

Tveganja se razvrstijo po prioritetah in določijo ukrepi za njihovo obvladovanje.

3.1 Koraki postopka

1. Identifikacija sredstev – določijo se informacijska sredstva, njihove lastnosti in lastniki.

2. Ocena vpliva na sredstvo - določi se vpliv na poslovanje oziroma pričakovane posledice v primeru uresničitve grožnje na sredstvo, zapiše se ocena ZCRA, ki je določena v seznamu informacijskih virov (vpliv na zaupnost, celovitost, razpoložljivost in avtentičnost). Ocena ZCRA določa lestvico vpliva - lestvica od 1 do 5.

3. Prepoznava groženj in ranljivosti - za vsako sredstvo se določi grožnja in ranljivost (uporaba relevantnih obveščevalnih podatkov, obvestil CSIRT in URSIV, ocen ali samoocen skladnosti in podatkov dobaviteljev) - lestvica od 1 do 5.

4. Ocena verjetnosti – določi se pogostost oziroma verjetnost uresničitve grožnje (brez uvedenih ukrepov in kontrol) - lestvica od 1 do 5.

5. Izračun inherentnega tveganja – **Faktor (inherentnega) tveganja = Vpliv × Verjetnost** (brez uvedenih ukrepov in kontrol) - lestvica od 1 do 25.

6. Določitev sprejemljive stopnje tveganj – vodstvo organizacije določi sprejemljivo stopnjo tveganj.

7. Navedba ukrepov in kontrol, ki so že uvedene.

8. Ocena verjetnosti uresničitve grožnje po izvedenih ukrepih oziroma kontrolah.

9. Izračun preostalega tveganja – **Faktor (rezidualnega) tveganja** = **Vpliv × Verjetnost (**po izvedenih ukrepih oziroma kontrolah) - lestvica od 1 do 25.

10. Določitev ukrepov in kontrol, ki jih je treba izvesti za znižanje faktorja (preostalega) tveganja (obvezno, če je faktor tveganja nad sprejemljivo ravnijo tveganja).

11. Določitev prioritet ukrepov – na podlagi faktorja preostalega (rezidualnega) tveganja se določi strategija obravnave posameznega tveganja.

3.2 Lestvica vpliva (1–5)

Ocena	Opis	Primer posledic
1	Zanemarljiv	Vpliv na sredstvo ne povzroči poslovne motnje (najvišja ocena ZCRA je 1). Brez opaznega vpliva na poslovanje.
2	Majhen	Vpliv na sredstvo vpliva le na posameznika ali del organizacijske enote (najvišja ocena ZCRA je 2). Manjše motnje ali zelo omejen vpliv.
3	Srednji	Vpliv na sredstvo privede do motenj delovanja, a poslovanje ostane vzdržno (najvišja ocena ZCRA je 3). Kratkotrajne motnje, manjši vpliv na posamezno organizacijsko enoto.
4	Visok	Vpliv na sredstvo vpliva na ključne procese, verjetne so zakonske neskladnosti ali negativen vpliv na ugled (najvišja ocena ZCRA je 4). Motnje ključnih procesov, finančni vpliv, izguba podatkov v manjšem obsegu.
5	Kritičen	Vpliv na sredstvo ima resne posledice, poslovanje je onemogočeno, pravne in finančne posledice (najvišja ocena ZCRA je 5). Prekinitev poslovanja, velik finančni vpliv, izguba podatkov, izguba ugleda.

** Vpliv se ocenjuje celostno glede na izgubo v primeru zaupnosti, celovitosti, razpoložljivosti in avtentičnosti ter se lahko nanaša na skladnost z zakonodajo/pogodbami; finančni učinek; vpliv na ugled; ter na poslabšanje varnosti in zdravja pri delu (kjer je relevantno).*

** V evidenci popisa informacijskih sredstev je vsako sredstvo (ali skupina sredstev) ocenjeno z vidika zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA). Končna ocena vpliva upošteva najvišjo izmed ocenjenih vrednosti ZCRA.*

3.3 Lestvica verjetnosti (1-5)

Ocena	Opis	Primer
1	Zelo nizka	Dogodek je malo verjeten (1× v 10 letih).
2	Nizka	Redko, vendar možno (1× v 5 letih).
3	Srednja	Občasno (1× na 2 do 3 leta).
4	Visoka	Pogosto (vsaj 1× na leto).
5	Zelo visoka	Pričakovano večkrat letno.

** Pri oceni verjetnosti realizacije grožnje se, kjer je to možno, uporabijo empirični viri (SIEM/MDR statistike, ENISA objave, CSIRT/obvestila URSIV, opozorila in objave, zgodovina incidentov, poročila dobaviteljev).*

3.4 Lestvica razvrstitve tveganj (1-25)

Faktor tveganja	Stopnja	Opis
1 – 5	Nizko	Sprejemljivo, spremlja se le ob spremembah okolja ali sistema.
6 - 10	Zmerno	Potrebno spremljanje in izvajanje osnovnih ukrepov.
11 – 15	Povišano	Zahteva načrt za zmanjšanje tveganja in določitev odgovorne osebe.
16 – 20	Visoko	Nujna izvedba ukrepov v kratkem roku in poročanje vodstvu.
21 – 25	Kritično	Tveganje nesprejemljivo, potrebno je takojšnje ukrepanje.

4. Merila sprejemljivosti tveganj

Sprejemljivost tveganj je določena z matriko od 1 do 25. Določene meje so: nizko (ukrepi niso potrebni), zmerno (potrebno spremljanje in izvajanje osnovnih ukrepov), povišano (zahteva se izdelava načrta za zmanjšanje tveganja in določitev odgovorne osebe), visoko (nujna uvedba ukrepov in poročanje vodstvu) in kritično (potrebni so takojšnji ukrepi).

Prage sprejemljivosti potrjuje vodstvo ob letnem pregledu. Vodstvo lahko izrecno določi izjeme - katera visoka ali kritična tveganja bo sprejelo kot sprejemljiva.[3] Določene izjeme (sprejem visokega/kritičnega tveganja) se dokumentirajo z utemeljitvijo, časovno omejitvijo in datumom naslednjega pregleda.

[3] Primer: »Vodstvo organizacije je na seji dne 10. 11. 2025: 1. pregledalo register tveganj (Priloga 1), 2. potrdilo prag sprejemljivosti rezidualnega tveganja na največ 12/25, 3. za sredstva z ZCRA = 4 ali 5 določilo strožji prag 8/25, 4. odobrilo vse ukrepe z roki 30/90 dni, 5. sprejelo vsa tveganja, ki so v registru označena kot 'sprejeto' z utemeljitvijo.«.

5. Rezultat izvedene analize tveganj in izvajanje ukrepov[4]

Rezultat analize tveganj je register tveganj, ki vključuje: naziv sredstva (ali skupine sredstev) na katerega se tveganje nanaša, lastnika sredstva/tveganja, opis tveganja, vpliv izgube sredstva v primeru kršitve oceno verjetnosti zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA), oceno verjetnosti realizacije grožnje, faktor tveganja, predlagane ukrepe za zmanjšanje tveganj, prenos ali sprejem tveganj, faktor (rezidualnega) tveganja, rok za realizacijo ukrepov in uspešnost uvedenih ukrepov (se preverja ali po izvedenem ukrepu ali v določenem intervalu po uvedbi ukrepov).

Register tveganj je Priloga 1 tega dokumenta in njegov sestavni del.

Za vsako nesprejemljivo tveganje je potrebno:

- določiti in izvesti ustrezne ukrepe za zmanjšanje ali odpravo tveganja,
- zavestno sprejeti tveganje, pri čemer je odgovorna oseba organizacije seznanjena z okoliščinami in dokumentirano potrdi sprejem tveganja ali
- določiti prenos tveganja na tretjo osebo (npr. zavarovanje, pogodbeni dogovor, zunanji izvajalec).

Za vsako tveganje se v registru tveganj navede:

- izbrana strategija (zmanjšanje/prenos/sprejem);
- tveganje v dobavni verigi (DA/NE in ime dobavitelja);
- opis ukrepa;
- odgovorna oseba;
- rok izvedbe;
- kriteriji uspešnosti;
- datum preverjanja;
- status realizacije ukrepov in
- opombe.

Tveganja, povezana z dobavitelji in zunanjimi izvajalci, se ocenjujejo posebej. Za vsakega dobavitelja se določi raven zaupanja glede na skladnost z varnostnimi zahtevami, certifikati (npr. ISO 27001, ISO 22301) in pogodbenimi določili. Register tveganj tako vključuje polje 'tveganje v dobavni verigi' z navedbo izvajalca.

Uspešnost izvedenih ukrepov se redno preverja, tveganja pa se ponovno ocenjujejo ob spremembah v poslovnem ali tehnološkem okolju, ob incidentih, oziroma najmanj enkrat letno.

Za izvedbo ukrepov kategorije visokih tveganj je rok izvedbe največ 90 dni; za izvedbo ukrepov kategorije kritičnih tveganj je rok takoj ali v roku 30 dni od odobritve analize.

Spremljanje in pregled tveganj potekata v okviru procesa stalnega izboljševanja, pri čemer se uporabljajo vnaprej določeni kazalniki učinkovitosti oziroma uspešnosti za nadzor tveganj in uspešnost izvedenih ukrepov, kar je pa odvisno od konteksta organizacije.

[4] Ukrepi se izvajajo sorazmerno glede na velikost organizacije, izpostavljenost tveganjem, verjetnost incidentov ter njihov družbeno-gospodarski vpliv. Za male organizacije se lahko namesto namenskih vlog uporabi neposredni nadzor vodstva.

6. Spremljanje, posodabljanje in poročanje

Analiza tveganj se izvaja najmanj enkrat letno ali ob večjih spremembah informacijskega sistema ali prepoznanih incidentih ali spremembah ključnih procesov. Rezultati se beležijo v register tveganj, pregled uspešnost ukrepov pa se izvaja v okviru internih sestankov ali vodstvenih pregledov.

Za spremljanje uspešnosti izvajanja ukrepov se uporabljajo merljivi kazalniki, kot so: delež izvedenih ukrepov v roku, število odprtih visokih tveganj, delež zmanjšanih tveganj in število ponavljajočih se incidentov.

Vsi zapisi v registru tveganj morajo biti dokumentirani v skladu s postopkom obvladovanja dokumentiranih informacij, ki zagotavlja sledljivost sprememb.

Rezultati analize tveganj in trendi se poročajo vodstvu najmanj četrtletno.

PRILOGI:

- register tveganj, verzija 1.0, z dne 31. 10. 2025
- seznam izjem, verzija 1.0, z dne 31. 10. 2025