ANALIZA VPLIVOV NA POSLOVANJE – vzorčna dokumentacija

Različica:	**1.0**
Datum veljavnosti:	
Avtor:	
Odobril:	

November 2025

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Analiza vplivov na poslovanje« iz 4. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1) in je skladen s Politiko neprekinjenega poslovanja. 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].

Metodologija za izvedbo analize vplivov na poslovanje (ang. *Business Impact Analysis – BIA*) predstavlja osrednji korak pri vzpostavljanju in vzdrževanju sistema upravljanja neprekinjenega poslovanja (SUNP) v organizaciji. Glavni namen analize je sistematično prepoznati poslovne procese in storitve, katerih motnja ali izpad bi imela najhujše posledice za delovanje organizacije, jih povezati z (informacijskimi) sredstvi ter na podlagi tega določiti potrebne korake oziroma prioritete za preventivo, odzivanje in obnovo procesov.

Dokument predstavlja poenostavljeno, a v celoti skladno metodologijo za izvedbo analize vplivov na poslovanje, ki je prilagojena malim in srednje velikim organizacijam. Metodologija je zasnovana tako, da je enostavna za razumevanje in izvedbo, hkrati pa zagotavlja zanesljive in pričakovane rezultate – jasno razvrstitev procesov po stopnji kritičnosti, določitev realnih ciljnih časov obnove (RTO) in ciljnih točk obnove podatkov (RPO) ter pregledno identifikacijo ključnih odvisnosti in tveganj.

V dokumentu navedeni podatki so vzorčni in dokument ni univerzalna rešitev, temveč izhodiščni okvir, ki ga mora vsaka organizacija obvezno prilagoditi, zato mora organizacija pri izvedbi analize vplivov na poslovanje upoštevati lastno veljavno Politiko neprekinjenega poslovanja, trenutno stanje in značilnosti lastne informacijsko-komunikacijske infrastrukture, posebnosti sektorja, v katerem deluje (npr. javna uprava, finance, zdravstvo, energetika), specifične grožnje, ki so značilne za njeno delovno področje, »*all-hazards*« pristop (upoštevanje vseh vrst nevarnosti – naravnih, tehničnih, človeških, kibernetskih, ipd.), obseg in kompleksnost poslovanja ter zahteve veljavnih standardov in dobrih praks, predvsem standarda ISO/IEC 22301 ter določb ZInfV-1. Dokument podpiše oziroma potrdi vodstvo organizacije in ga pregleda najmanj letno.

<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;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *Standard ISO/IEC 22301:2019;Technical Implementation Guidance on Cybersecurity Risk Management Measures, ENISA, junij 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/2025-06/ENISA_Technical_implementation_guidance _on_ cybersecurity_risk _management_measures_version_1.0.pdf

KAZALO

1. Namen dokumenta

Ocena vplivov na poslovanje (ang. *Business Impact Analysis - BIA*) določa okvir in metodologijo za ocenjevanje posledic morebitnih motenj na ključne poslovne funkcije, procese, vire in storitve [IME ORGANIZACIJE]. Namen dokumenta je prepoznati (kritične) procese, katerih prekinitev bi imela največji vpliv na poslovanje, ter določiti prioritete za zagotavljanje neprekinjenega delovanja.

2. Obseg in cilji

Ocena vplivov na poslovanje se uporablja za vse organizacijske enote, funkcije in procese, ki so vključeni v opredeljen obseg sistema upravljanja neprekinjenega poslovanja in obsega:

- prepoznavanje ključnih oziroma kritičnih poslovnih procesov ter njihovih odvisnosti;
- določitev lastništva posameznim poslovnim procesom in enoznačne oznake procesa;
- ocenjevanje možnih posledic motenj;
- določitev ciljne časovne točke za obnovo procesa (RTO) in ciljne točke obnove podatkov (RPO) za kritične procese oziroma funkcije;
- upoštevanje odvisnosti od notranjih virov, ključnega osebja, tehnologije, objektov, dobaviteljev in zunanjih izvajalcev;
- zagotavljanje vhodnih podatkov za razvoj in stalno izboljševanje sistema upravljanja neprekinjenega poslovanja in
- seznam poslovnih procesov in seznam informacijskih sistemov, ki podpirajo oziroma zagotavljajo delovanje poslovnih procesov oziroma storitev, sta prilogi Politike neprekinjenega poslovanja.

3. Kriteriji za oceno kritičnosti procesov

Lastnik procesa oceni kritičnost procesa z vidika vpliva izpada procesa na poslovanje oziroma zagotavljanje storitev. Pri določanju kritičnosti posameznega procesa se praviloma upoštevajo naslednji vidiki:

- Finančni vpliv – izguba dohodkov, povečani stroški, pogodbene kazni.
- Ugled organizacije – izguba zaupanja strank, negativna medijska izpostavljenost.
- Varnost in zdravje – ali proces neposredno vpliva na varnost zaposlenih, strank ali okolja.
- Operativne odvisnosti – ali drugi procesi ne morejo delovati brez tega procesa.
- Pravni/regulatorni vpliv – ali obstajajo zakonske zahteve za delovanje procesa (izvajanje zakonskih nalog, izvajanje javnega pooblastila, poročanje davčni upravi, izplačevanje plač zaposlenim).

Vsak proces se oceni glede na to, koliko časa lahko organizacija preživi brez njega oziroma ne da bi nastale škodljive posledice za poslovanje organizacije.

- RTO (ang. *Recovery Time Objective*) – ciljni čas, v katerem mora biti proces obnovljen.
- RPO (ang. *Recovery Point Objective*) – maksimalen čas sprejemljive izgube podatkov.

Krajša kot sta RTO in RPO, bolj je proces kritičen.

4. Metoda ocenjevanja kritičnosti procesov

Procesi se razvrstijo v tri kategorije: **Kritični procesi**[3] (obnovitev procesov v nekaj minutah ali urah), **pomembni procesi**[4] (obnovitev v nekaj dneh) in **podporni procesi**[5] (obnovitev v dveh tednih). Za opis kritičnosti procesa se uporablja naslednja opisna matrika ocenjevanja:

Vpliv izpada	Opis	Primer
Visok (**kritičen proces**)	Izpad lahko povzroči zelo veliko finančno škodo. Izpad ima velik negativni vpliv na ugled. Izpad ima težke pravne (zakonske) posledice ali za dlje časa ali popolnoma onemogoči nadaljevanje poslovanja.	Glavni proizvodni procesi, obdelava naročil, izvajanje plačil, opravljane pomembnih zakonskih nalog.
Srednji (**pomemben proces**)	Izpad lahko povzroči veliko finančno škodo. Izpad ima pravne (zakonske) posledice. Izpad za krajši čas onemogoči nadaljevanje poslovanja.	Upravljanje s kadri, priprava analiz in poročil.
Nizek (**podporni proces**)	Izpad lahko povzroči manjši vpliv, ki ga je mogoče prenesti dalj časa.	Interne raziskave, poročila, podporne naloge.

Za ocenjevanje oziroma določanje kritičnosti procesov se vsak poslovni proces oceni glede na **štiri glavne kriterije**, kjer se vsak kriterij oceni s točkami od 1 do 3 (**1 = nizek vpliv, 2 = srednji vpliv, 3 = zelo visok vpliv**):

- Finančni vpliv: kolikšna bi bila izguba dohodkov ali koliko bi bilo povzročenih stroškov (odvisno od letnega prometa organizacije).
- Pravni/regulatorni vpliv: kakšno je tveganje kršitve izvajanja zakonskih ali regulatornih obveznosti (visoke globe, izguba licence/koncesije/javnega pooblastila).
- Ugled organizacije: kakšen je vpliv na zaupanje strank, partnerjev in širše javnosti (posledice zaradi izgube zaupanja in ugleda).
- Časovna občutljivost: kako hitro mora biti proces obnovljen (RTO/RPO).

Za izvedbo točkovne ocene kritičnosti procesov, se uporablja naslednja matrika ocenjevanja vpliva:

Kriterij/Vpliv	1 – Nizek (1 točka)	3 – Srednji (2 točki)	5 – Visok (3 točk)
Finančni vpliv	Izguba manj kot 1.000 EUR.	Izguba od 1.000 do 20.000 EUR.	Izguba več kot 20.000 EUR.

[3] Procesi, ki morajo biti obnovljeni v nekaj minutah ali urah, ker so nujni za neprekinjeno izvajanje ključnih storitev; njihova prekinitev takoj povzroči resne operativne, varnostne, ugledne ali pravne posledice.
[4] Procesi, ki so bistveni za delovanje kritičnih procesov in jih podpirajo; lahko so začasno prekinjeni, vendar morajo biti obnovljeni v določenem času, da se izogne večjim motnjam ali degradaciji storitev.
[5] Procesi, ki niso neposredno vezani na delovanje kritičnih ali pomembnih procesov in lahko začasno stojijo; njihova obnovitev je sprejemljiva v nekoliko daljšem časovnem obdobju, brez večjega vpliva na ključne storitve.

Pravni/regulatorni vpliv	Brez pravnih posledic.	Možna opozorila, opomini ali manjše globe do največ 20.000 EUR.	Visoke globe, izguba licence ali koncesije.
Ugled	Interni vpliv, stranke ali javnost ne opazi.	Negativne pritožbe posameznih strank, omejen negativni odmev na socialnih omrežjih.	Velika škoda ugledu, odmevna negativna medijska izpostavljenost.
Časovna občutljivost	Izpad sprejemljiv več kot en teden.	Izpad sprejemljiv do treh dni.	Izpad nesprejemljiv že več kot 24 ur.

** Vrednosti finančnih vplivov so navedene informativno in izhajajo iz konteksta organizacije in posebnosti področja. Vrednosti ne predstavljajo dejanske lestvice, ki bi bile primerne za vse organizacije. Organizacije si vrednosti predpišejo skladno z lastno nagnjenostjo k tveganjem na področju finančnega vpliva.*

Skupna ocena kritičnosti procesa se določi s seštevkom točk vseh štirih kriterijev, pri čemer pomeni seštevek:

- **10 do 12 točk: kritični proces**;
- 7 do 9 točk: pomembni proces in
- 4 do 6 točk: podporni proces.

Primer izračuna kritičnosti procesov (hipotetični primer za izmišljeno organizacijo):

Proces	*Finančni vpliv*	*Pravni vpliv*	*Ugled*	*Časovna občutljivost*	*Skupaj*	*Kritičnost*
Prodaja/naročila	*3*	*2*	*3*	*3*	*11*	***Kritični***
Računovodstvo	*2*	*3*	*2*	*2*	*9*	*Pomembni*
Kadrovske evidence	*1*	*2*	*2*	*1*	*6*	*Podporni*
Elektronska pošta	*3*	*2*	*3*	*3*	*11*	***Kritični***
Izdaja osebnih dokumentov	*1*	*3*	*3*	*3*	*10*	***Kritični***

5. Metoda za izvedbo analize tveganj in ranljivosti procesov

Za vsak poslovni proces se identificirajo možna tveganja, ocenita se verjetnost njihovega nastopa in vpliv na poslovanje. Na podlagi tega se določi **raven tveganja, ki je lahko nizka, srednja ali visoka**. Analiza vključuje tudi prepoznavo notranjih ranljivosti, ki povečujejo verjetnost uresničitve tveganj. Za ocenjevanje se uporabi spodnja matrika verjetnosti in vpliva:

Lestvica verjetnosti	Opis
Zelo nizka verjetnost (1 točka)	Dogodek je malo verjeten (1× v 10 letih).
Nizka verjetnost (2 točki)	Redko, vendar možno (1× v 5 letih).
Srednja verjetnost (3 točke)	Občasno (1× na 2 do 3 leta).
Visoka verjetnost (4 točke)	Pogosto (vsaj 1× na leto).
Zelo visoka verjetnost (5 točk)	Pričakovano večkrat letno.
Lestvica vpliva	**Opis**
Zanemarljiv vpliv (1 točka)	Dogodek ne povzroči opaznega vpliva na poslovanje.
Majhen vpliv (2 točki)	Dogodek lahko povzroči manjše motnje, obvladljivo brez večjih posledic ali zelo omejen vpliv.
Srednji vpliv (3 točke)	Dogodek lahko povzroči opazne kratkotrajne motnje (finančne izgube in krajše prekinitve,) z manjšim vplivom na posamezno organizacijsko enoto.
Visok vpliv (4 točke)	Dogodek lahko povzroči motnje ključnih procesov, večji finančni vpliv ali izgubo podatkov v manjšem obsegu.
Kritičen vpliv (5 točk)	Dogodek lahko povzroči hude posledice - dolgoročne prekinitve ključnih procesov, velik negativni finančni vpliv, prekinitev poslovanja, izgubo podatkov ali izgubo ugleda.

Za vsak poslovni proces se izvede tudi analiza tveganj, kjer se tveganje določi oziroma izračuna kot **zmnožek števila točk verjetnosti in vpliva**.

Za vsako tveganje se tako določi ocena verjetnosti (1–5) in ocena vpliva (1–5). Skupna raven tveganja (1–25) se določi na podlagi zmnožka teh dveh ocen. Na podlagi dobljene vrednosti se tveganja razvrstijo v tri kategorije:

- visoko (od 16 do 25 točk);

- srednje (od 9 do 15 točk) ali

- nizko (od 1 do 8 točk).

Spodnja preglednica upošteva izračun (zmnožek) verjetnosti in vpliva, ki določa raven tveganja:

Zmnožek (Verjetnost × Vpliv)	Raven tveganja	Opis
1–8 točk	**Nizko tveganje**	Dogodek lahko povzroči manjše posledice, obvladljivo z rednimi ukrepi. Operativno delo je mogoče nadomestiti ali prestaviti.
9–15 točk	**Srednje tveganje**	Dogodek lahko povzroči opazne posledice, potrebni so ukrepi za obvladovanje tveganj. Možne so zamude, povečani stroški ali zmanjšana kakovost storitev.
16–25 točk	**Visoko tveganje**	Dogodek lahko ima resne negativne posledice, zahteva proaktivne ukrepe in ukrepe za pripravljenost. Možno je prenehanje delovanja ali bistveno omejevanje ključnih storitev.

Spodnja preglednica prikazuje (trenutna) ključna (tipična) tveganja, njihovo verjetnost, vpliv in raven tveganja[6].

Tveganje	Verjetnost	Točk	Vpliv	Točk	Raven tveganja	Točk
Kibernetski napad (npr. izsiljevalska programska oprema)	Visoka	4	Visok	4	Visoko	16
Izpad infrastrukture (npr. električni izpad)	Nizka	2	Kritičen	5	Srednje	10
Človeška napaka (npr. napačna konfiguracija)	Srednja	3	Srednji	3	Srednje	9
Tveganje dobavne verige (npr. izpad Microsoft oblaka)	Srednja	3	Visok	4	Srednje	12

[6] Verjetnost pojava tipičnih groženj je različna glede na sektor ali dejavnost subjekta. Prikazane vrednosti predstavljajo povprečje vrednosti iz razpoložljivih virov podatkov.

Ranljivosti, ki povečujejo možnost uresničitve navedenih tveganj, vključujejo predvsem dejansko stanje: zastarelo ali neposodobljeno programsko opremo, šibko avtentikacijo, pomanjkanje nadzora ključnih dobaviteljev in pomanjkanje redundance (podvojenih zmogljivosti).

6. Analiza odvisnosti in verižnih vplivov

Za vsak poslovni proces je treba opisno določiti notranje in zunanje odvisnosti, ki omogočajo njegovo delovanje. Poleg tega se identificirajo in navedejo možni verižni vplivi, kjer izpad enega procesa povzroči posledice na drugih procesih in s tem na celotno poslovanje organizacije.

Vrsta odvisnosti	Opis
Notranje odvisnosti	Odvisnost od infrastrukture, IT sistemov, kadrov in notranjih podpornih procesov.
Zunanje odvisnosti	Odvisnost od dobaviteljev, partnerjev, regulatornih organov in storitev tretjih oseb.
Verižni vplivi	Povezani učinki, kjer izpad enega procesa povzroči zakasnitve, izgube ali neskladnosti v drugih procesih.

7. Analiza vplivov na poslovanje za poslovne procese

Proces zagotavljanja elektronske pošte (hipotetično primer za izmišljen subjekt)

Št. procesa	***IT-001***
Naziv procesa	*Zagotavljanje elektronske pošte (Microsoft Exchange, hibridni model, 200 uporabnikov)*
Lastnik procesa	*Vodja IT oddelka/CISO*
Ključna informacijska sredstva	*- E-poštni strežniki (MS Exchange)* *- strežniki DNS* *- Omrežna oprema (usmerjevalniki, požarne pregrade, stikala)* *- E-poštne baze podatkov* *- Uporabniški računi* *- IT administratorji (3 osebe)* *- 200 uporabnikov*
Kritičnost procesa	***Kritičen*** *(visok vpliv na finance, ugled, pravne obveznosti in operativne procese)*
RTO	*2 uri*
RPO	*15 minut*

Minimalno poslovanje	***DA***

Točkovna ocena kritičnosti procesa:

Kriterij	*Finančni vpliv*	*Pravni/regulatorni vpliv*	*Ugled*	*Časovna občutljivost*
Točke	*4*	*3*	*4*	*5*

Skupaj: ***16 točk*** → ***Kritični proces***

Minimalne operativne zahteve:

Nujno potrebno osebje	*IT administratorji (2 osebi za vzdrževanje sistema), podporno osebje (1 oseba) za komunikacijo v primeru izpada.*
Osnovne informacijske in komunikacijske storitve	*Omrežna povezava (internet), mobilna komunikacija kot rezervni kanal, strežniška in oblačna infrastruktura za e-pošto.*
Nujni dobavitelji, partnerji in dobavne poti	*Microsoft (licence, oblačne storitve), internetni ponudnik, pogodbeni vzdrževalci IT sistemov.*
Potrebni zakonski in varnostni pogoji	*Skladnost z GDPR, veljavne licence za programsko opremo, izvajanje varnostnih ukrepov (avtentikacija, varnostne kopije, požarne pregrade).*

Analiza tveganj in ranljivosti:

Tveganje	*Verjetnost*	Točk	*Vpliv*	Točk	*Raven tveganja*	Točk
Kibernetski napad (npr. Ransomware)	*Visoka*	*4*	*Visok*	*4*	***Visoko***	*16*
Izpad infrastrukture (npr. električni izpad)	*Nizka*	*2*	*Kritičen*	*5*	*Srednje*	*10*
Človeška napaka (npr. napačna konfiguracija)	*Srednja*	*3*	*Srednji*	*3*	*Srednje*	*9*
Dobaviteljsko tveganje (npr. izpad Microsoft oblak)	*Srednja*	*3*	*Visok*	*4*	*Srednje*	*12*

Analiza odvisnosti:

Vrsta odvisnosti	*Opis*
Notranje	*Omrežje, požarne pregrade, uporabniške naprave.*
Zunanje	*Internetni ponudnik (povezave), Microsoft (za Exchange), antivirusni dobavitelj, dobavitelj električne energije.*

Analiza verižnih vplivov:

Dogodek	*Posledica*
Izpad e-pošte	*Zamuda v prodajnih pogodbah (vpliv na finance)*
	Prekinjena podpora strankam (vpliv na ugled)
	Neobdelani osebni podatki (pravni vpliv na GDPR skladnost)

8. Vzdrževanje in izboljševanje

Ta dokument se pregleduje in po potrebi posodablja najmanj enkrat letno ali ob večjih spremembah v organizaciji ali v poslovnih procesih ali ob pojavu pomembnih incidentov, ki vplivajo na neprekinjenost poslovanja.

Za pregled in posodobitev splošnega dela analize vplivov na poslovanje je odgovoren vodja neprekinjenega poslovanja, za pregled in posodobitev posameznih delovnih procesov pa so odgovorni lastniki procesov.