REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

2019

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi

Direktorat za informacijsko družbo in informatiko

20.12.2019

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi

Različica: 1.0

Datum: 20. 12. 2019

Kazalo vsebine

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi

1 Uvod

1.1 Namen

Sistematični pristop k obvladovanju tveganj informacijske varnosti je nujen za ugotavljanje potreb organa glede zahtev za informacijsko varnost in njihovo uskladitev s potrebami informacijske varnosti v centralnem informacijsko-komunikacijskem sistemu in celotni državni upravi. V sistemu upravljanja informacijske varnosti v državni upravi morajo biti tveganja informacijske varnosti obravnavana pravočasno in učinkovito, v skladu s to metodologijo in v tem dokumentu opisanimi postopki.

Obvladovanje tveganj informacijske varnosti mora biti stalen, neprekinjen proces, v okviru katerega prepoznavamo, ocenjujemo, obravnavamo in spremljamo tveganja informacijske varnosti in o njih poročamo vsem deležnikom. V procesu obvladovanja tveganj ugotavljamo, kaj bi se lahko zgodilo in kakšne bi bile lahko posledice uresničitve groženj, preden se odločimo, kaj moramo storiti in kdaj, da zmanjšamo tveganje na sprejemljivo raven.

Ta navodila opisujejo korake za aktivnosti, ki jih moramo izvesti v procesu obvladovanja tveganj informacijske varnosti. Določajo splošni okvir in smernice, ki niso značilne za določeno organizacijo, organ ali gospodarsko dejavnost. Organi in druge organizacije lahko te smernice prilagodijo glede na lastne potrebe, njihov odnos do informacijske varnosti in glede na svoje posebne poslovne zahteve.

1.2 Občinstvo

Navodila so namenjena vodjem informacijske varnosti in organizacijskih enot, pristojnih za informacijsko tehnologijo, upravljavcem/ocenjevalcem tveganja in notranjim revizorjem. Čeprav obstajajo razlike med javnim in zasebnim sektorjem, zlasti glede prednostnih nalog in zakonskih zahtev, so temeljna načela informacijske varnosti (IV) enaka. Navodila lahko koristno uporabi vsak posameznik, ki potrebuje celovit opis praks in postopkov obvladovanja tveganj informacijske varnosti.

1.3 Uporaba

Ta navodila določajo okvire, ki omogočajo usklajeno obvladovanje tveganj informacijske varnosti v organih državne uprave, povezanih subjektih in drugih organizacijah. Čeprav je terminologija v tem dokumentu prilagojena javnemu sektorju, se ta navodila lahko uporabljajo tudi za obvladovanje tveganj informacijske varnosti na drugih področjih.

Da bi opredelili ustrezne ravni in merila, ki najbolj ustrezajo poslovnim potrebam organa, morajo uporabniki predhodno ovrednotiti svoje poslovne procese in informacijsko infrastrukturo.

1.4 Pravne podlage

Deveti člen Uredbe o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 z dne 26.4.2018) (v nadaljnjem besedilu: uredba) predpisuje, da morajo organi na podlagi ocenitve tveganj informacijske varnosti uvesti ustrezne ukrepe za preprečitev ali omilitev neželenih učinkov in zagotoviti nenehno izboljševanje. Organi morajo izvajati ocenitve tveganj informacijske varnosti najmanj enkrat letno in v primeru bistvenih sprememb v informacijskih sistemih in pri delovnih procesih, pri čemer morajo upoštevati merila za sprejetje tveganj in izvajanje ocenitve tveganj informacijske varnosti. Na podlagi ugotovitev ocenitve tveganja morajo organi vzpostaviti nova ali prilagoditi obstoječa upravljavska, fizična in tehnična nadzorstva. Ocenitev tveganja se izvaja v skladu z Enotno metodologijo upravljanja

(obvladovanja) tveganj informacijske varnosti v državni upravi in se objavi na spletni strani ministrstva, pristojnega za javno upravo. Ta navodila opisujejo enotno metodologijo obvladovanja tveganj informacijske varnosti v državni upravi.

1.5 Obseg dokumenta

Ta navodila vključujejo pojasnila v zvezi z obvladovanjem tveganj informacijske varnosti, ocenitvijo tveganja informacijske varnosti in minimalnimi zahtevami zanjo. Navodila temeljijo na standardu ISO/IEC 27005: 2011 in so v skladu z veljavnimi predpisi. Procesi, navedeni v teh navodilih, se uporabljajo pri izvajanju ocene tveganja informacijske varnosti za vse organe in povezane subjekte. Obravnavana so vsa ključna informacijska sredstva: informacijska premoženja, informacijski sistemi in informacijsko okolje, ki vključuje tudi poslovne prostore in človeške vire.

1.6 Pomen uporabljenih izrazov[1]

	izraz	pomen
1.	analiza tveganja	je proces ugotavljanja vrste tveganja in določitve **ravni tveganja** (15)
2.	deležnik	je oseba ali organizacija, ki lahko prizadene, je lahko prizadeta ali meni, da je prizadeta, zaradi določene odločitve ali dejavnosti
3.	dogodek	je nastanek ali sprememba posameznega niza okoliščin
4.	Inherentno tveganje	je **tveganje** (17), ki bi mu bilo izpostavljeno informacijsko sredstvo, če ne bi bilo vzpostavljeno nobeno nadzorstvo
5.	merilo tveganja	je področje delovanja, na podlagi katerega se vrednoti pomen **tveganja** (17)
6.	nadzorstvo	je ukrep, ki zmanjšuje **tveganje** (17); vključuje postopke, usmeritve, naprave, prakse ali druge aktivnosti, ki zmanjšujejo tveganje
7.	notranji kontekst	je notranje okolje, v katerem organizacija skuša doseči svoje cilje
8.	obravnavanje tveganja	je proces za spremembo tveganja
9.	obveščanje o tveganju in posvetovanje	so stalni in ponovljivi procesi, ki jih organizacija vodi, da zagotavlja, deli ali pridobiva informacije ter vodi dialog z **deležniki** (2) v zvezi z obvladovanjem **tveganja** (17)
10.	obvladovanje tveganja	so usklajene aktivnosti za usmerjanje in nadzorovanje organizacije v zvezi s tveganjem

[1] Večina opredelitev je povzetih po standardu ISO/IEC 27005:2011

	izraz	pomen
11.	ocenjevanje tveganja	je celotni proces **prepoznavanja tveganja** (14), **analize tveganja** (1) in **vrednotenja tveganja** (19)
12.	posledica	je izid **dogodka** (3), ki vpliva na cilje
13.	preostalo tveganje	je **tveganje** (17), ki ostane po **obravnavanju tveganja** (8)
14.	prepoznavanje tveganj	je proces iskanja, spoznavanja in opisovanja tveganj
15.	raven tveganja	je velikost **tveganja** (17), izražena kot kombinacija **posledic** (12) in njihove **verjetnosti** (18)
16.	informacijsko sredstvo	je karkoli, kar ima vrednost za organizacijo in potrebuje zaščito ter lahko vpliva na informacijsko varnost
17.	tveganje	je učinek negotovosti na cilje
18.	verjetnost	je možnost, da se nekaj dogaja
19.	vrednotenje tveganja	je proces primerjanja rezultatov **analize tveganja** (1) z **merili tveganja** (5), da se ugotovi, ali sta tveganje in/ali njegova velikost sprejemljiva ali znosna
20.	zunanji kontekst	je zunanje okolje, v katerem organizacija skuša doseči svoje cilje

2 Upravljanje tveganj

Upravljanje tveganj vzpostavlja zunanji in notranji okvir za obvladovanje tveganj informacijske varnosti, z določitvijo temeljnih meril, ki so potrebna za obvladovanje tveganj informacijske varnosti, opredelitev obsega in meja ter vzpostavitev ustrezne organizacijske strukture za obvladovanje tveganj informacijske varnosti. Upoštevajo se vse informacije o organu, ki se nanašajo na upravljanje obvladovanja tveganj informacijske varnosti: cilje organa, strategijo, politiko obvladovanja tveganj informacijske varnosti, skladnost, predpise in pogodbene zahteve.

2.1 Vloge in odgovornosti

2.1.1 Odbor za upravljanje informacijske varnosti

Za usklajevanje aktivnosti na področju informacijske varnosti v državni upravi, ki vključuje tudi obvladovanje tveganj informacijske varnosti, je pristojen Odbor za upravljanje informacijske varnosti.

2.1.2 Predstojnik organa

Za informacijsko varnost v organu je odgovoren predstojnik posameznega organa.

2.1.3 Vodja informacijske varnosti

Za usklajevanje obvladovanja tveganj informacijske varnosti v posameznem organu je odgovoren vodja informacijske varnosti.

2.1.4 Lastnik tveganja

Tveganja se dodelijo lastnikom tveganj, ki so odgovorni za spremljanje, nadzor in periodično poročanje o stanju in učinkovitosti vseh aktivnosti za obravnavo posameznih tveganj vodji informacijske varnosti.

Lastnik tveganja mora:

- sodelovati pri oblikovanju meril za odzivanje na tveganja in za prepoznavanje tveganja ter se odzvati na nastalo tveganje,
- sodelovati pri periodičnem pregledu, vnovičnem vrednotenju ter spreminjanju verjetnosti in učinka za vsako posamezno tveganje,
- sodelovati pri ugotavljanju in analizi novo nastalih tveganj in
- obveščati o problemih, povezanih s tveganji vodjo informacijske varnosti.

2.2 Določitev obsega in mej

a) Vodja informacijske varnosti določi obseg in meje obvladovanja tveganja informacijske varnosti.

b) V obseg obvladovanja tveganj informacijske varnosti se vključijo vsa informacijska premoženja in druga informacijska sredstva, ki hranijo, obdelujejo in prenašajo ta informacijska premoženja, ali so kako drugače vključena v proces obvladovanja tveganj informacijske varnosti.

c) Pri določanju obsega in meja organ upošteva naslednje:

- strateške poslovne cilje, strategije in politike organa,
- informacijska premoženja, ki jih obravnava,

- pomembne poslovne procese,
- poslovne funkcije in organizacijsko strukturo organa,
- zakonske in pogodbene zahteve, ki veljajo za organ,
- specifične politike informacijske varnosti organa oziroma akte, s katerim organ določi prilagoditve varnostnih zahtev, določenih v uredbi, svojim posebnim potrebam.,
- splošni pristop državne uprave k obvladovanju tveganj,
- informacijske vire,
- ključne notranje in zunanje storitve, ki jih nudi organizacijska enota za IT / IS,
- lokacijo organa in njene geografske značilnosti,
- omejitve, ki vplivajo na organ,
- pričakovanja posameznih deležnikov,
- socialno-kulturno okolje,
- vmesnike, prek katerih je sistem v okviru obsega v interakciji z zunanjim okoljem.

d) Predstojnik organa pregleda in odobri obseg in meje obvladovanja tveganj informacijske varnosti.

2.3 Vloge pri obvladovanju tveganj informacijske varnosti

VLOGA	ODGOVORNOST
OCENJEVALEC TVEGANJ	Ocenjevalec tveganj je oseba, ki dobro pozna proces ocenjevanja tveganj na posameznem poslovnem področju. Določi se za vsako organizacijsko enoto, da usklajuje obvladovanje tveganja informacijske varnosti z vodjem informacijske varnosti.
STROKOVNJAK ZA POSAMEZNO PODROČJE (SPP)	Strokovnjaki za posamezno področje so osebe, ki dobro poznajo posamezna poslovna področja oziroma poslovne enote. Pomagajo ocenjevalcem tveganja in skrbnikom informacijskih sistemov v procesu obvladovanja tveganj.
VODJA INFORMACIJSKE VARNOSTI	Vodja informacijske varnosti je koordinator in odgovorna oseba za izvedbo ocene tveganja. Po potrebi lahko vodja informacijske varnosti deluje tudi kot ocenjevalec tveganja.
SKRBNIK INFORMACIJSKEGA SISTEMA	Naloge skrbnika informacijskega sistema, ki je praviloma poslovni uporabnik tega sistema, so: – informacijski sistem in informacijsko premoženje, ki ga ta informacijski sistem

	obravnava, uvršča v varnostne razrede z vidika zaupnosti, celovitosti in razpoložljivosti, – določa stopnjo zaščite informacijskega sistema, – odloča o spremembah in dopolnitvah informacijskega sistema, – odloča, kdo in kako sme uporabljati storitve in informacije informacijskega sistema, – odloča o uvedbi, upravljanju in vzdrževanju priporočenih varnostnih nadzorstev ter – odobri prenos programske oziroma strojne opreme v obratovalno okolje.
ZUNANJI OCENJEVALEC	Organu lahko pri izvedbi ocene tveganja pomagajo zunanji ocenjevalci tveganja, vendar pa mora skrbnik informacijskega sistema uradno potrditi dejavnosti, informacije in rezultate, ki jih predloži zunanji izvajalec.

2.4 Merila za obvladovanje tveganja informacijske varnosti

2.4.1 Vidiki tveganja informacijske varnosti

Tveganja informacijske varnosti se nanašajo na tveganja izgube:

- zaupnosti, to je lastnosti, da informacije niso razpoložljive ali razkrite nepooblaščenim posameznikom, entitetam ali procesom;
- celovitosti, to je lastnosti, da so informacije in informacijski sistemi pravilni in popolni ter
- razpoložljivosti, to je lastnosti, da so informacije in informacijski sistem dostopni in uporabni na zahtevo pooblaščene osebe ali procesa.

2.4.2 Poslovna vrednost informacijskih sredstev

Poslovna vrednost informacijskih sredstev (informacijskih premoženj in z njimi povezanih informacijskih sistemov in drugih podpornih sredstev) se določi na podlagi ocene vpliva na poslovanje organa, oziroma možnega učinka, ki bi ga imel na organ dogodek, ki bi ogrozil informacijsko premoženje in informacijske sisteme (njihovo zaupnost, celovitost in razpoložljivost), ki jih organ potrebuje za uresničevanje svojega poslanstva, varovanje svojega premoženja, izpolnjevanje zakonskih in pogodbenih obveznosti, vzdrževanje rednega poslovanja in zaščito posameznikov.

Vpliv na poslovanje (možni učinek), kot je opredeljen v prilogi uredbe (Razvrstitvena shema s poimenovanjem varnostnih razredov, merila za uvrščanje informacijskega premoženja in sistemov v posamezni varnostni razred ter postopki razvrščanja in označevanja), je lahko:

- MAJHEN,
- ZMEREN ali
- VELIK.

Vpliv je MAJHEN, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela omejene negativne posledice za poslovanje ali premoženje organa ali posameznike. Izraz omejene negativne posledice pomeni, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij zmanjšana,
- povzročila manjšo škodo premoženju organa (manj kot 100.000 eurov),
- povzročila manjšo finančno izgubo (manj kot 100.000 eurov),
- povzročila manjšo škodo posameznikom (ni potrebna zdravniška oskrba, manj kot dva dni izgube delovnega časa),
- povzročila manjšo škodo ugledu organa (posamične omembe v nekaterih tiskanih, elektronskih in spletnih medijih).

Vpliv je ZMEREN, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela resne negativne posledice za poslovanje ali premoženje organa ali posameznike. Izraz resne negativne posledice pomeni, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- pomembno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij znatno zmanjšana,
- povzročila znatno škodo premoženju organa (od 100.000 eurov do 500.000 eurov),
- povzročila znatno finančno izgubo (od 100.000 eurov do 500.000 eurov),
- povzročila znatno škodo posameznikom, ki pa ne vključuje izgube življenj ali resnih, smrtno nevarnih poškodb (potrebna zdravniška oskrba, do 30 dni izgube delovnega časa),
- povzročila znatno škodo ugledu organa (poročanje v medijih več dni zapored in/ali razprava v Državnem zboru).

Vpliv je VELIK, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela zelo resne ali katastrofalne negativne posledice za poslovanje ali premoženje organa ali posameznike. Izraz zelo resne ali katastrofalne negativne posledice pomeni, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

- močno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da organ ne bi mogel izvajati ene svoje primarne funkcije ali več svojih primarnih funkcij,
- povzročila veliko škodo premoženju organa (nad 500.000 eurov),
- povzročila veliko finančno izgubo (nad 500.000 eurov),
- povzročila zelo resno ali katastrofalno škodo posameznikom, ki zajema resne, smrtno nevarne poškodbe, množične poškodbe in smrtne žrtve,
- povzročila veliko škodo ugledu organa (večtedensko poročanje v medijih in/ali razprava o ukrepih v Državnem zboru).

Poslovna vrednost informacijskega premoženja se glede na posamezni vidik informacijske varnosti (zaupnost, celovitost, razpoložljivost) določi, kot je prikazano v spodnji preglednici:

Vpliv na poslovanje	Poslovna vrednost (opisna)	Poslovna vrednost (številčna)

Brez	Brez	0
Majhen	Nizka	1
Zmeren	Srednja	2
Velik	Visoka	3

Poslovno vrednost (V) informacijskega premoženja lahko torej zapišemo tako:

$$V = \{V_Z, V_C, V_R\},$$

kjer je V_Z poslovna vrednost iz vidika zaupnosti, V_C poslovna vrednost z vidika celovitosti in V_R poslovna vrednost z vidika razpoložljivosti.

Poslovna vrednost informacijskih premoženj in informacijskih sistemov se določi v postopku popisa informacijskega premoženja in informacijskih sistemov v skladu z enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.

Za določitev poslovne vrednosti sestavnih delov informacijskih sistemov in drugih podpornih sredstev se upoštevajo vse poslovne vrednosti informacijskih premoženj, ki se obravnavajo s temi informacijskimi sredstvi. Poslovne vrednosti, dodeljene tem informacijskim sredstvom glede na vse tri varnostne vidike (zaupnost, celovitost, razpoložljivost), so najvišje poslovne vrednosti posameznih informacijskih premoženj, ki se obravnavajo s temi informacijskimi sredstvi. Sestavni deli informacijskih sistemov in druga podporna sredstva torej dedujejo najvišje poslovne vrednosti informacijskih premoženj, ki se s temi sredstvi obravnavajo (pri drugih podpornih sredstvih se upoštevajo samo smiselni varnostni vidiki).

Poslovno vrednost podpornega sredstva (V_p) lahko torej zapišemo tako:

$$V_p = \{V_{Z,max}, V_{C,max}, V_{R,max}\},$$

kjer je $V_{Z,max}$ največja poslovna vrednost iz vidika zaupnosti, $V_{C,max}$ največja poslovna vrednost z vidika celovitosti in $V_{R,max}$ največja poslovna vrednost z vidika razpoložljivosti vseh informacijskih premoženj, ki se s tem sredstvom obravnavajo.

2.4.3 Vrednost učinka grožnje na poslovanje

Učinek grožnje na poslovanje (v nadaljnjem besedilu: poslovni učinek) je odvisen od vrste grožnje in poslovne vrednosti informacijskega sredstva, na katero se grožnja nanaša. Grožnja lahko ogrozi ene vidik ali več vidikov informacijske varnosti (zaupnost, celovitost, razpoložljivost). Poslovni učinek na posamezni vidik informacijske varnosti je enak poslovni vrednosti informacijskega sredstva, na katerega se grožnja nanaša, glede na ta vidik informacijske varnosti, pomnožen z dejavnikom te grožnje glede tega vidika informacijske varnosti, kjer je dejavnik grožnje lahko 1 (grožnja vpliva na ta vidik) ali 0 (grožnja ne vpliva na ta vidik).

Poslovni učinek (U), ki ga povzroči določena grožnja na določeno informacijsko sredstvo, lahko torej zapišemo tako:

$$\mathbf{U = \{V_Z\, d_Z, V_C\, d_C, V_R\, d_R\},}$$

kjer je V_Z poslovna vrednost iz vidika zaupnosti, V_C poslovna vrednost z vidika celovitosti in V_R poslovna vrednost z vidika razpoložljivosti tega informacijskega sredstva, $d_{z,c,r}$ pa dejavniki grožnje na posamezne vidike informacijske varnosti, ki imajo lahko vrednost 1 ali 0.

2.4.4 Verjetnost grožnje

Pri določanju verjetnosti uresničitve grožnje oziroma nastanka dogodka informacijske varnosti se lahko uporabijo informacije, kot so:

- zgodovina pojavljanja dogodka informacijske varnosti,
- obvestila obveščevalnih in raziskovalnih organizacij, statistika incidentov informacijske varnosti, predhodne ocene tveganja in geopolitična poročila o nevarnostih in tveganjih ipd.

Za določitev vrednosti verjetnosti uresničitve grožnje uporabimo spodnjo tabelo:

Verjetnost uresničitve grožnje	Vrednost	Pogostnost (povprečna)	Premislek
Zelo malo verjetno (ZMV)	1	Enkrat v sto letih	Grožnja je omejena. Uvedena so nadzorstva, ki učinkovito zmanjšujejo verjetnost izkoriščanja ranljivosti.
Malo verjetno (MV)	2	Enkrat letno	Grožnja je srednja. Uvedena so nadzorstva, ki zmanjšujejo verjetnost izkoriščanja ranljivosti.
Verjetno (V)	3	Enkrat mesečno	Grožnja je velika. Uvedena nadzorstva za zmanjševanje verjetnost izkoriščanja ranljivosti niso zadostna.
Zelo verjetno (ZV)	4	Vsak dan	Grožnja je zelo velika. Nadzorstva za zmanjševanje verjetnost izkoriščanja ranljivosti niso uvedena ali so neučinkovita.

2.4.5 Učinkovitost in raven izvedbe nadzorstev

Merila za ocenjevanje učinkovitosti nadzorstev oziroma protiukrepov, ki se izvajajo za zmanjšanje tveganja na sprejemljivo raven oziroma za zaščito informacijskih sredstev, so navedena v spodnji preglednici:

Učinkovitost nadzorstva	Vrednost (%)	Opis učinkovitosti	Premislek
Nezadostna – neučinkovito nadzorstvo	0	Ne zmanjšuje pogostnosti ali resnosti grožnje (groženj)	Nadzorstvo ni učinkovito v nobenem primeru
Nizka – slabo učinkovito nadzorstvo	25	Pogostnost ali resnost grožnje (groženj) zmanjšuje neučinkovito	Nadzorstvo je učinkovito v posameznih primerih
Srednja – zmerno učinkovito nadzorstvo	50	Pogostnost ali resnost grožnje (groženj) zmanjšuje zmerno učinkovito	Nadzorstvo je učinkovito v polovici primerov

Visoka– učinkovito nadzorstvo	75	Pogostnost ali resnost grožnje (groženj) učinkovito zmanjšuje	Nadzorstvo je učinkovito v večini primerov
Zelo visoka – zelo učinkovito nadzorstvo	95	Pogostnost ali resnost grožnje (groženj) zmanjšuje zelo učinkovito	Nadzorstvo je učinkovito v skoraj vseh primerih

Merila za oceno **ravni izvedbe** nadzorstva so navedena v spodnji preglednici:

Opis	**Vrednost (%)**
Ni izvedeno	0
Delno izvedeno	25
Polovično izvedeno	50
Skoraj v celoti izvedeno	75
V celoti izvedeno	100

2.4.6 Tveganje in raven tveganja

Tveganje je odvisno od verjetnosti, da se uresniči grožnja, ki ogroža posamezno informacijsko sredstvo in povzroči negativni poslovni učinek. Posamezno tveganje se ugotavlja s parom informacijsko sredstvo – grožnja, ki se nanaša na to sredstvo. **Raven tveganja** (R) je enaka poslovnemu učinku grožnje, ki je povezan s poslovno vrednostjo informacijskega sredstva (glede na posamezni vidik IV), pomnoženega z verjetnostjo, da se grožnja uresniči (G).

$$\mathbf{R = \{U_Z, U_C, U_R\}\ G,}$$

kjer je U_Z poslovni učinek iz vidika zaupnosti, U_C poslovni učinek z vidika celovitosti in U_R poslovni učinek z vidika razpoložljivosti, G pa verjetnost uresničitve grožnje.

Celotna raven tveganja (R_s) je seštevek ravni tveganj glede na posamezne vidike IV:

$$\mathbf{R_s = (U_Z + U_C + U_R)\ \ G = U_s\ G,}$$

kjer je z U_s je označen celotni poslovni učinek.

Celotna raven tveganja upošteva vse vidike IV in jo uporabljamo pri odločanju o obravnavi tveganja. Vendar pa moramo biti vedno pozorni na ravni tveganja po posameznih vidikih IV. Kadar so te (posamezne) ravni visoke, je njihova obravnava, neglede na celotno raven tveganja, potrebna ali celo nujna, kar je pojasnjeno v naslednjem poglavju.

2.4.7 Obravnava tveganj

Za odločanje glede obravnave tveganj se uporablja spodnja matrika:

Verjetnost uresničitve grožnje		ZMV (1)	MV (2)	V (3)	ZV (4)
Celotni poslovni učinek	Zanemarljiv (1)	1	2	3	4
	Zelo majhen (2)	2	4	6	8
	Majhen (3)	3	6	9	12
	Zmeren (4)	4	8	12	16
	Večji (5)	5	10	15	20
	Velik (6)	6	12	18	24
	Zelo velik (7)	7	14	21	28
	Izjemno velik (8)	8	16	24	32
	Ogromen (9)	9	18	27	36

Razvrstitev tveganj v povezavi s potrebo po obravnavi tveganja je prikazana v spodnji preglednici:

Celotna raven tveganja	Potreba po obravnavi tveganja
Nizka (1 – 6)	Tveganje je sprejemljivo; nadaljnji ukrepi niso potrebni.
Srednja* (7 – 17)	Obravnava tveganja je potrebna. Nadzorstva se uvedejo v razumnem času (glede na poslovne okoliščine).
Visoka* (18 – 36)	Obravnava tveganja je nujna. Nadzorstva za zmanjševanje tveganja se uvedejo nemudoma.

* Če je zmanjšanje (ublažitev) tveganja nemogoče ali nerealno glede na analizo stroškov, izvedljivosti ali koristi, mora lastnik informacijskega sredstva sprejeti preostalo tveganje.

Obravnava tveganja je nujna tudi v primerih, ko je raven tveganja za posamezni vidik IV večja od 10. Primer: vpliv grožnje na poslovanje je različen od 0 samo z vidika zaupnosti, kjer je poslovni vpliv s tega vidika $U_z = 3$ (velik), verjetnost uresničitve grožnje G = 4 (zelo verjetno) {$R_z = U_z$ G = 12, $R_c = U_c$ G = 0, $R_r = U_r$ G = 0}.

2.4.8 Ocenitev učinkovitosti nadzorstev

Nadzorstvo je ukrep, ki zmanjšuje tveganje. Nadzorstva so pri zmanjševanju posameznih tveganj različno učinkovita in imajo različne učinke na posamezne vidike informacijske varnosti (zaupnost, celovitost in razpoložljivost).

Za oceno učinkovitosti nadzorstva uporabljamo spodnjo matriko:

Opis	Zmanjšanje tveganja (%) (zaupnost – z)	Zmanjšanje tveganja (%) (celovitost – c)	Zmanjšanje tveganja (%) (razpoložljivost – r)
Brez vpliva	0	0	0
Zelo majhen	10	10	10
Majhen	25	25	25
Srednji	50	50	50
Velik	75	75	75
Zelo velik	90	90	90

2.4.9 Izvajanje ocenitev tveganja

Tveganja informacijske varnosti se ocenijo:

- vsako leto,
- po vsaki pomembni spremembi v notranjem oziroma zunanjem IT okolju, na podlagi ocene vodje informacijske varnosti in odobritve vodstva organa in
- po vsaki pomembni spremembi v notranjem oziroma zunanjem poslovnem okolju, na podlagi ocene vodje informacijske varnosti in odobritve vodstva organa.

2.4.10 Matrika vlog in odgovornosti

Pri izvajanju nalog v procesu obvladovanja tveganj je pomembna jasna dodelitev vlog in odgovornosti. Večje organizacije posamezne vloge dodelijo različnim osebam in s tem zagotovijo učinkovito upravljanje in izvajanje tega procesa. V manjših organizacijah, kjer ni mogoče zagotoviti dovolj oseb, lahko več vlog opravlja tudi ena oseba, vendar je pri tem treba zagotoviti ločevanje vlog oziroma nalog, ki so iz upravljavskega in varnostnega vidika nezdružljive.

V matrikah vlog in odgovornosti v nadaljevanju dokumenta so uporabljene naslednje oznake:

ZOPPI

Z	Zadolžen – oseba, ki izvaja nalogo
O	Odgovoren – lastnik naloge in končni odločevalec; samo ena oseba (vloga) lahko prevzame odgovornost za izvedbo nalog pri posameznem koraku
PD	Podpira – oseba, dodeljena za podporo/pomoč pri izvedbi naloge
PS	Posvetovan – oseba, ki jo je treba zaprositi za nasvet/mnenje o nalogi (ali odločitvi)
I	Informiran – oseba, ki mora biti obveščena o nalogi

3 Register tveganj informacijske varnosti

3.1 Vsebina registra

Za dokumentirano spremljanje in obvladovanje tveganj informacijske varnosti se vzpostavi register tveganj informacijske varnosti (register), ki vsebuje vsaj naslednje podatke:

- referenčna oznaka tveganja,
- lastnik tveganja,
- opis grožnje,
- informacijsko sredstvo, ki je ogroženo,
- poslovni učinek z vidika zaupnosti, celovitosti in razpoložljivosti,
- verjetnost uresničitve grožnje,
- raven inherentnega tveganja,
- izhodiščna raven preostalega tveganja,
- raven preostalega tveganja in
- uvedena nadzorstva in njihova učinkovitost.

3.2 Organizacija registra

Register na ravni celotnega organa je lahko, kadar je to primerno, sestavljen iz več posameznih registrov, na primer za posamezne organizacijske enote, procese ali projekte. Za vzdrževanje posameznih registrov so odgovorne osebe, ki so odgovorne za področja, na katera se ti registri nanašajo. Omogočen mora biti celovit pogled na vsa tveganja v organu.

4 Postopek obvladovanja tveganj informacijske varnosti

V tem poglavju je podrobno opisan postopek obvladovanja tveganja informacijske varnosti, ki je razdeljen v 5 faz.

1. faza:

ANALIZA TVEGANJA

2. faza:

VREDNOTENJE TVEGANJA

3. faza:

OBRAVNAVA TVEGANJA

4. faza:

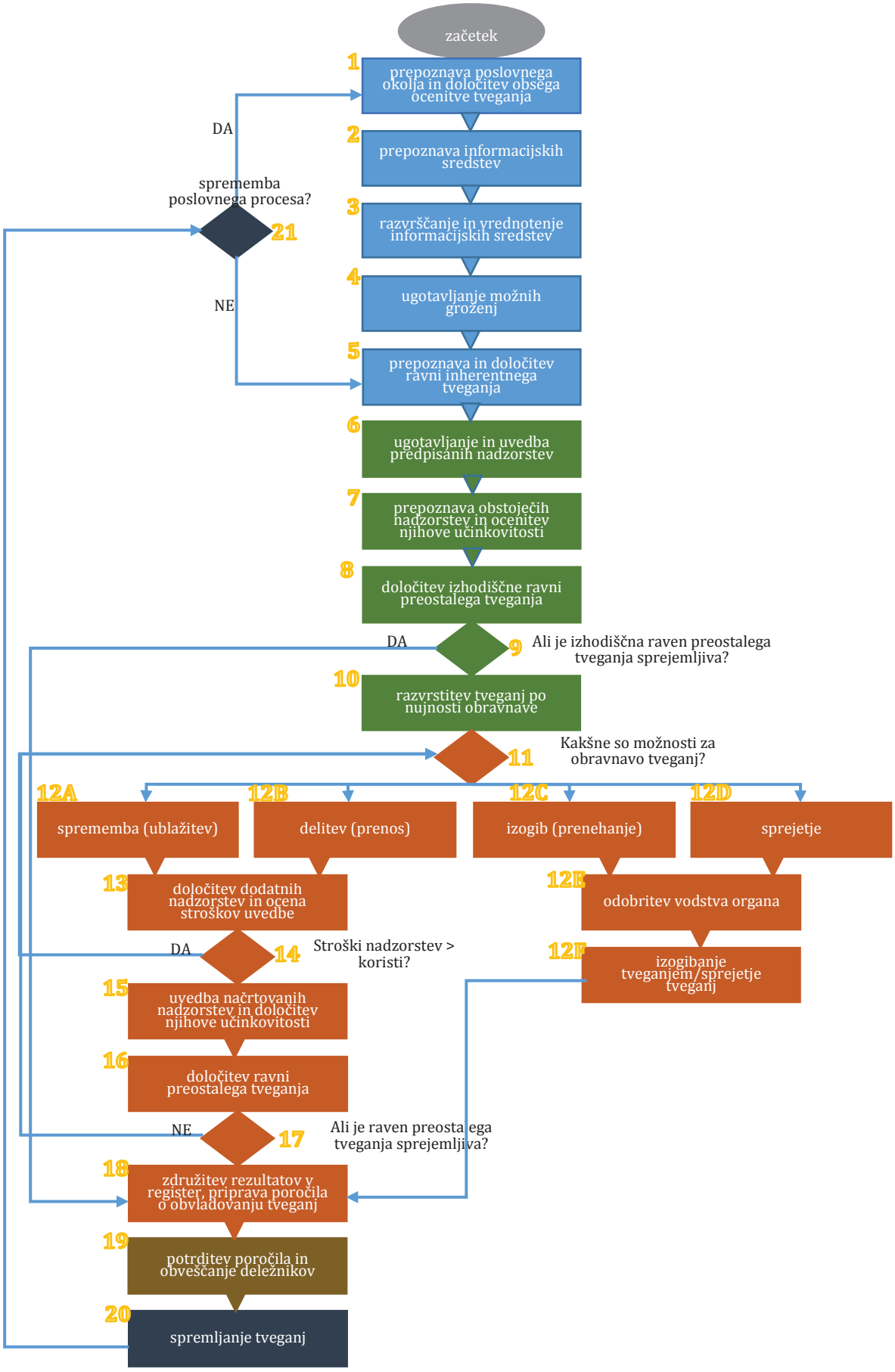
OBVEŠČANJE O TVEGANJU

5. faza:

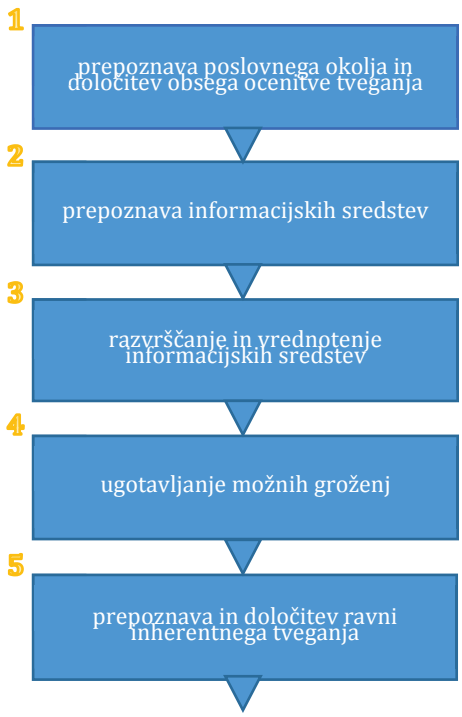
SPREMLJANJE TVEGANJ

Postopek opredeljuje različne dejavnosti oziroma korake v vsaki fazi procesa obvladovanja tveganj informacijske varnosti, ki vključujejo zajem vhodnih podatkov, navodila in smernice, izhodne rezultate ter vloge in odgovornosti.

Delovni tok celotnega procesa obvladovanja tveganj informacijske varnosti je prikazan na spodnji sliki.



4.1 1. faza: analiza tveganja



Tveganje lahko opišemo tudi kot verjetnost nastanka (negativnih) posledic zaradi prihodnjih dogodkov. Tveganje informacijske varnosti je torej verjetnost, da se bo obstoječa grožnja uresničila in negativno vplivala na posamezno informacijsko sredstvo in posredno poslovanje organa. Za obstoj tveganja mora obstajati verjetnost, da se grožnja in negativne posledice (poslovni učinki), kot rezultat njene uresničitve, uresničijo. Tveganje prepoznamo po grožnji, s katero je povezano in po informacijskem sredstvu, na katero se grožnja nanaša.

Analiza tveganja je proces razumevanja narave tveganja in določitve ravni tveganja. Je podlaga za vrednotenje tveganja in odločitve o obravnavanju tveganja. Vključuje oceno tveganja.

Analiza tveganja predstavlja izhodišče upravljanja tveganj informacijske varnosti. Namen analize tveganja je ugotoviti, kaj bi lahko povzročilo potencialno izgubo (katere grožnje), in pridobiti vpogled v to, kako, kje in zakaj se to lahko zgodi. Analiza tveganja se običajno izvaja z vprašalniki in skupnimi delavnicami, ki vključujejo ljudi z različnih področij v organu (strokovnjake za informacijsko varnost, skrbnike (lastnike) informacijskih sistemov in sredstev ter uporabnike, upravljavce informacijskih sistemov, osebje in višje vodstvo).

Proces analize tveganja se lahko sproži na kateri koli organizacijski ravni v organu: na podlagi določenega razporeda (vsaj enkrat letno), ob uvedbi večjih sprememb obstoječih informacijskih sistemov, med pridobivanjem ali uvedbo novega postopka ali sistema, ali na podlagi prijavljenih incidentov, ki lahko povzročijo ali nakazujejo potencialno izpostavljenost tveganju informacijske varnosti.

4.1.1 Vložki

- Najpomembnejše informacije, ki so potrebne za določitev obsega ocenjevanja tveganj:
    - katere organizacijske enote (poslovne funkcije oziroma procesi) so vključene v ocenjevanje tveganj (organigram),
    - seznam informacijskih premoženj in drugih informacijskih sredstev (po organizacijskih enotah),
    - lokacije, vključene v oceno tveganja,
    - odgovorne osebe (vodje organizacijskih enot, lastniki procesov, skrbniki informacijskih sistemov ipd.),
    - pregled razvrstitve informacijskih sredstev iz priloge A tega navodila.
- Merila za oceno tveganja informacijske varnosti, opredeljena v poglavju 2.4 tega navodila.
- Informacije o grožnjah (in ranljivostih), pridobljene z analizo incidentov, od skrbnikov informacijskih sistemov, uporabnikov in iz drugih virov, vključno iz javno objavljenih seznamov groženj.
- Seznam skupin in vrst groženj iz priloge B tega navodila.

4.1.2 Postopkovna navodila

1. korak – prepoznava poslovnega okolja in določitev obsega ocenitve tveganja

a. Tveganja informacijske varnosti so povezana s poslovnimi tveganji organa, zato je treba ugotoviti oziroma poznati notranji kontekst, to je glavne poslovne procese in poslovne cilje organa ter z njimi povezane poslovne informacije oziroma informacijska premoženja. Določi se obseg, v katerem se ocenjujejo in obvladujejo tveganja informacijske varnosti in opiše zunanji kontekst, ki vpliva nanj.

b. Izdela se organizacijska shema oziroma organigram organa oziroma dela organa v obsegu, v katerem se ocenjujejo in obvladujejo tveganja informacijske varnosti.

c. Prepoznajo se odgovorne osebe organizacijskih enot ali glavnih poslovnih procesov oziroma skrbniki informacijskih sistemov, s katerimi se obravnavajo glavna informacijska premoženja in podpirajo izvajanje teh poslovnih procesov. Osebe, odgovorne za posamezna poslovna področja, lahko zagotovijo temeljne informacije o poslovnih procesih in poslovnih informacijah (informacijskih premoženjih), potrebne za izvajanje teh dejavnosti (procesov).

2. korak – prepoznava informacijskih sredstev

a. Sredstvo je karkoli, kar ima vrednost za organizacijo in ga je zato treba zaščititi. Informacijska sredstva kot del sistema upravljanja informacijske varnosti, so lahko ogrožena in jih lahko varujemo z nadzorstvi za zmanjševanje tveganj informacijske varnosti, ki so jim izpostavljena. Informacijska sredstva imajo poslovno vrednost, ki se lahko izrazi z nabavno vrednostjo sredstva, za potrebe te analize pa predvsem z velikostjo vpliva na poslovanje, če bi prišlo do uničenja, okvare, nedostopnosti ali nepooblaščenega razkritja tega sredstva.

Vsakemu informacijskemu sredstvu se določi njegov skrbnik, ki je odgovoren in pristojen za njegovo upravljanje. Skrbnik sredstva nima nujno lastninskih pravic, vendar je odgovoren za njegovo pridobitev, razvoj, vzdrževanje, uporabo in primerno varovanje. **Skrbnik sredstva je najprimernejša oseba za določitev vrednosti sredstva za organizacijo.** Vrednotenje informacijskih sredstev je opisano v naslednjem koraku.

b. Temeljne skupine informacijskih sredstev so: informacijska premoženja (primarna sredstva), informacijski sistemi (podporna sredstva) in podporni viri (druga podporna sredstva).

- **Informacijska premoženja (primarna sredstva)** so skupine ključnih poslovnih informacij oziroma podatkov, ki jih organ uporablja v svojih delovnih procesih oziroma pri poslovanju v okviru upravljanja informacijske varnosti.

- **Informacijski sistemi (glavna podporna sredstva)** so med seboj povezani elementi računalniške strojne, programske in komunikacijske opreme, s katerimi se obravnavajo informacijska premoženja (primarna sredstva).

- **Informacijsko okolje (druga podporna sredstva)** je skupina informacijskih sredstev, v katero uvrščamo osebje, ki obravnava informacijska premoženja in delovno okolje, v katerem so nameščena podporna sredstva in kjer se obravnavajo informacijska premoženja.

c. Informacijska premoženja, ki spadajo v obseg obvladovanja tveganj informacijske varnosti, prepoznamo iz popisa informacijskega premoženja in informacijskih sistemov, pripravljenega v skladu z

Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi[2].

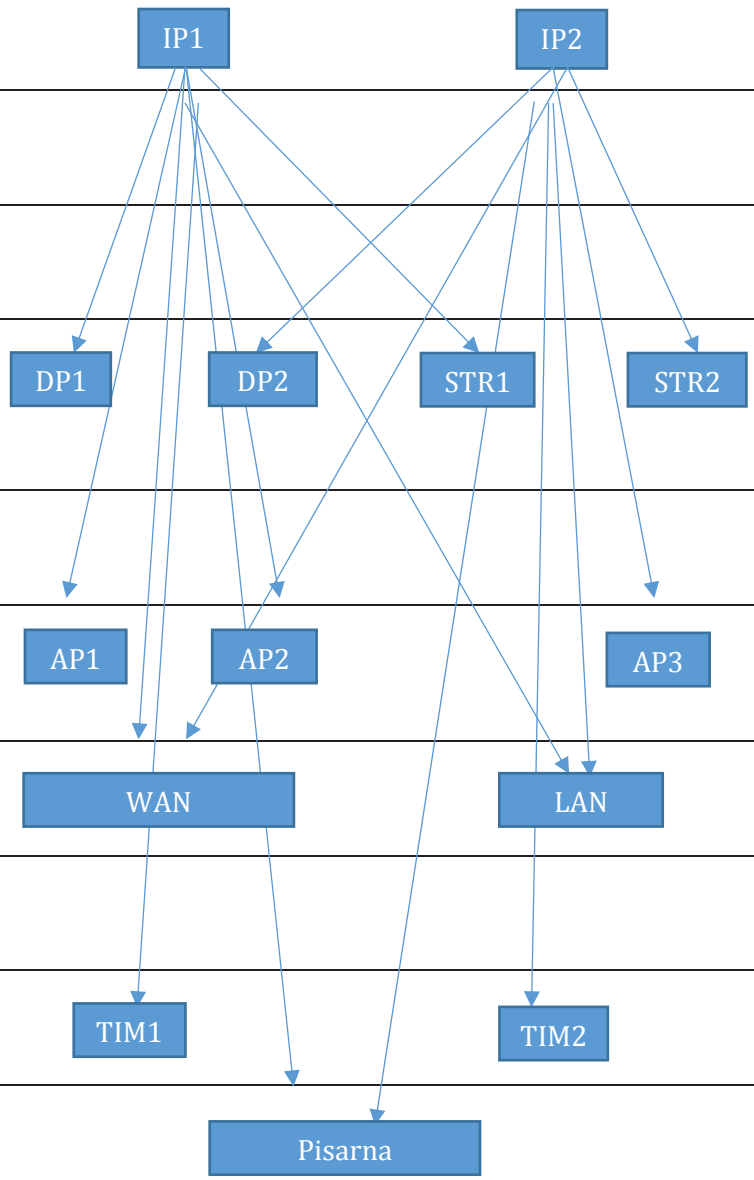
d. Informacijske sisteme, ki spadajo v obseg obvladovanja tveganj informacijske varnosti, ugotovimo iz popisa informacijskega premoženja in informacijskih sistemov, pripravljenega v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi. Podrobnejše informacije o delih informacijskih sistemov pridobimo od skrbnikov posameznih informacijskih sistemov.

e. Prepoznavo delov informacijskih sistemov in drugih informacijskih sredstev opravimo na primerni ravni podrobnosti, ki zagotavlja dovolj informacij za ocenjevanje tveganj. Raven podrobnosti, uporabljena za prepoznavo informacijskih sredstev, vpliva na celotno količino informacij, zbranih med ocenjevanjem tveganj. Podrobnejšo analizo, če je potrebna, lahko izvedemo v ponovitvah ocenjevanja tveganj.

f. Okvir za razvrstitev informacijskih sredstev je opisan v prilogi A tega navodila. Raven podrobnost razvrščanja informacijskih sredstev je odvisna od pristopa k obravnavi tveganja in posebnosti poslovnega okolja. Preveč podrobnosti povečuje kompleksnost obravnave tveganja in ne prispeva k njeni večji učinkovitosti. Premalo podrobnosti sicer poenostavlja obravnavo tveganja, vendar lahko vodi do neoptimalnih rešitev. Za uspešno in učinkovito obvladovanje tveganj informacijske varnosti je priporočljiva izdelava poenostavljenega modela sistema informacijskih sredstev, ki je predmet obvladovanja tveganj. Model naj vsebuje samo bistvena informacijska premoženja in podporna informacijska sredstva (skupine sredstev). Iz modela naj bodo razvidne povezave podpornih sredstev z informacijskimi premoženji, ki jih ta sredstva podpirajo.

[2] https://www.gov.si/assets/ministrstva/MJU/DI/Enotna_metodologija_popisovanja_inf_premozenja_in_sistemov_v_DU.pdf

Primer modela:

Skupine / razredi informacijskih sredstev	Posplošen model informacijskih sredstev
IP (informacijsko premoženje)	
IS (informacijski sistemi)	
HW (strojna oprema)	
HWF (nepremične računalniške naprave)	
SW (programska oprema)	
SWAP (poslovne aplikacije)	
NW (omrežje)	
IO (informacijsko okolje)	
LJU (osebje)	
DO (delovno okolje)	

g. Določimo ocenjevalca (ali več ocenjevalcev) tveganja, ki vodi in usklajuje celotni proces ocene tveganja na svojem področju.

h. Ocenjevalec tveganja in vodja informacijske varnosti prepoznata in dokumentirata informacijska sredstva, ugotovita njihove skrbnike (lastnike) in jih uvrstita v skupine in podskupine, ugotovita medsebojne povezave in jih povežeta z organizacijskimi enotami in lokacijami organa.

i. Ugotovljena informacijska sredstva posodabljamo v popisu informacijskega premoženja in informacijskih sistemov v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi, in jih vključimo v register.

3. korak – razvrščanje in vrednotenje informacijskih sredstev

a. Vsako informacijsko premoženje in informacijski sistem razvrstimo v varnostne razrede glede na zaupnost, celovitost in razpoložljivost v skladu s prilogo uredbe oziroma navodili iz poglavja 2.4.2 te metodologije. Varnostni razredi informacijskih premoženj in informacijskih sistemov so razvidni iz popisa informacijskega premoženja in informacijskih sistemov v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.

b. Razvrstitev informacijskih sredstev odraža njihovo **poslovno vrednost** glede na posamezne vidike informacijske varnosti (zaupnost, celovitost ali razpoložljivost). Za potrebe ocenitve tveganja uporabljamo oznake za stopnje vpliva.

c. Za določitev poslovne vrednosti drugih informacijskih sredstev (delov informacijskih sistemov in drugih podpornih sredstev) upoštevamo vse poslovne vrednosti informacijskih premoženj, ki se obravnavajo s temi informacijskimi sredstvi. Poslovne vrednosti, dodeljene tem informacijskim sredstvom glede na vse tri varnostne vidike (zaupnost, celovitost, razpoložljivost), so najvišje poslovne vrednosti posameznih informacijskih premoženj, ki se obravnavajo s temi informacijskimi sredstvi. Deli informacijskih sistemov in druga podporna sredstva torej dedujejo najvišje poslovne vrednosti informacijskih premoženj, ki jih obravnavajo.

4. korak – ugotavljanje možnih groženj

a. Ocenjevalec tveganja ugotavlja možne grožnje, ki lahko škodijo posameznim informacijskim sredstvom (informacijskim premoženjem, informacijskim sistemom in informacijskemu okolju), in posledično organu oziroma njegovemu poslovanju.

b. Te informacije lahko pridobimo iz procesov upravljanja groženj in ranljivosti ter upravljanja incidentov informacijske varnosti, od obveščevalnih in raziskovalnih organov in ustanov, iz analiz incidentov, predhodnih ocen tveganja in geopolitičnih poročil o nastajajočih tveganjih.

c. Ugotovljene možne grožnje lahko razvrstimo glede na vrste groženj v naslednje skupine:

1. Fizični napad – grožnje, povezane z namernimi, sovražnimi človeškimi aktivnostmi;
2. Nenamerno povzročanje škode – Grožnje, povezane z nenamernimi človeškimi dejanji ali napakami;
3. Dogodki, ki povzročijo škodo večjih razsežnosti – Grožnje, povezane s poškodbami informacijskih sredstev, ki jih povzročajo naravni ali okoljski dejavniki;
4. Okvare / slabo delovanje – Grožnje, povezane z okvarami ali slabm delovanjem informacijske infrastrukture (na primer poslabšanje kakovosti, neustrezni delovni parametri, motenje). Vzrok za napako je večinoma notranja težava (na primer preobremenitev električnega omrežja v stavbi);
5. Izpadi – Grožnja popolne odsotnosti ali izgube virov, potrebnih za računalniško infrastrukturo. Vzrok za izpad je predvsem zunanja težava (npr. izpad električne energije v celotnem mestu);
6. Prisluškovanje / prestrezanje / ugrabitev – Grožnje, ki posegajo v komunikacijo med dvema stranema. Za te napade ni potrebna namestitev dodatnih orodij ali programske opreme na mestu žrtve.
7. Zlonamerne aktivnosti / zlorabe – Grožnje, povezane z zlonamernimi aktivnostmi, ki zahtevajo uporabo orodij s strani napadalca. Ti napadi zahtevajo namestitev dodatnih orodij oziroma programske opreme ali izvajanje dodatnih korakov na računalniški infrastrukturi oziroma programski opremi žrtve.

Kot pomoč pri ugotavljanju značilnih groženj za informacijsko varnost se uporablja seznam skupin in vrst groženj iz priloge B tega navodila;

Grožnje, ki lahko škodijo posameznim informacijskim sredstvom in označujejo tveganja informacijske varnosti, vpišemo v register.

d. Posamezne vrste groženj lahko vnaprej povežemo s posameznimi vrstami/razredi informacijskih sredstev ter vidiki IV in te povezave uporabimo pri ugotavljanju tveganj (glej prilogo B tega navodila).

e. Ocenimo verjetnost uresničitve groženj. Na verjetnost uresničitve določene grožnje vplivajo:

- privlačnost sredstva ali možni učinek, do katerega bi prišlo, kadar gre za namerno grožnjo,
- enostavnost pretvorbe izkoriščanja ranljivosti sredstva v želeni izid, kadar gre za namerno grožnjo,
- tehnične zmožnosti agenta grožnje, kadar gre za namerne grožnje.

Ocenjevalec tveganja določi stopnjo verjetnosti (uresničitve) grožnje (G) za vsako informacijsko sredstvo v skladu z merili za verjetnost grožnje in posodobi register (glej 2.4.4).

5. korak – prepoznava in določitev ravni inherentnega tveganja

a. **Inherentno tveganje** je tveganje, ki bi mu bilo izpostavljeno informacijsko sredstvo, če ne bi bila vzpostavljena nadzorstva. Pri prepoznavanju inherentnih tveganj torej ne upoštevamo morebitnih že obstoječih nadzorstev.

b. Tveganja se prepoznajo tako, da se ugotovijo grožnje, ki lahko ogrozijo informacijska sredstva. **Tveganje določata grožnja in informacijsko sredstvo, na katero se grožnja nanaša.**

Primeri:

Oznaka tveganja (ID)	Grožnja	Informacijsko sredstvo
T-001	1.10 Nepooblaščeni fizični dostop/ nepooblaščeni vstop v prostore	3.2.3 Varovana območja
T-002	6.4 Industrijsko vohunjenje	3.1 Osebje org. enote za razvoj
T-003	3.1 Požar	3.2.2 Poslovna zgradba
T-004	1.1 Goljufija	1 Informacijsko premoženje (glavna knjiga)
T-005	1.1 Goljufija	2.2.4 Poslovna aplikacija za knjigovodenje

c. Vodja informacijske varnosti mora opredeliti celotno območje tveganj informacijske varnosti, ki mora vključevati vse skupine groženj, ki bi lahko ogrozile organ;

d. Za ugotavljanje različnih skupin groženj, ki se nanašajo na organ oziroma njegova informacijska sredstva, vodja informacijske varnosti upošteva naloge, ki se opravljajo na poslovnih področjih in na področju IT v organu ter zunanje in notranje dejavnike tveganja. Pri tem upošteva:

- Okoljske pogoje: okoljska tveganja – na primer letne temperaturne razpone, vremenske razmere itd.

- Premisleke o lokaciji: tveganja, povezana z lokacijo oziroma prostori organa – kakor so na primer bližina glavnih avtocest, možni teroristični cilji, skladišča za shranjevanje tekočih goriv in plina itd.

- Veljavno zakonodajo in druge predpise: vso veljavno zakonodajo in druge predpise z morebitnim učinkom na informacijsko varnost, vključno s predpisi o upravljanju podjetij, varstvu osebnih podatkov, tajnih podatkih, zdravju in varnosti, delovnem pravu, informacijski varnosti itd.

- Poslovne partnerje in tretje osebe: vse tretje osebe, ki lahko vplivajo na varnost informacij.

f. **Raven inherentnega tveganja R_{iv}** glede na posamezni vidik informacijske varnosti (v = z, c ali r) izračunamo po naslednji enačbi:

$$R_{iv} = U_v G,$$

kjer je U_v poslovni učinek grožnje glede na posamezen vidik informacijske varnosti (v = z, c ali r), G pa verjetnost uresničitve grožnje.

Celotna raven inherentnega tveganja R_s je vsota ravni inherentnih tveganj za posamezne vidike informacijske varnosti:

$$R_s = (U_Z + U_C + U_R) G = U_s G,$$

kjer je U_s celotni poslovni učinek.

g. Vsakemu prepoznanemu tveganju v registru pripišemo ravni inherentnih tveganj za posamezne vidike informacijske varnosti in raven celotnega inherentnega tveganja.

h. Register lahko sestavlja več registrov, ki se nanašajo na posamezne organizacijske enote oziroma lokacije, vendar mora omogočiti celovit pregled vseh tveganj organa.

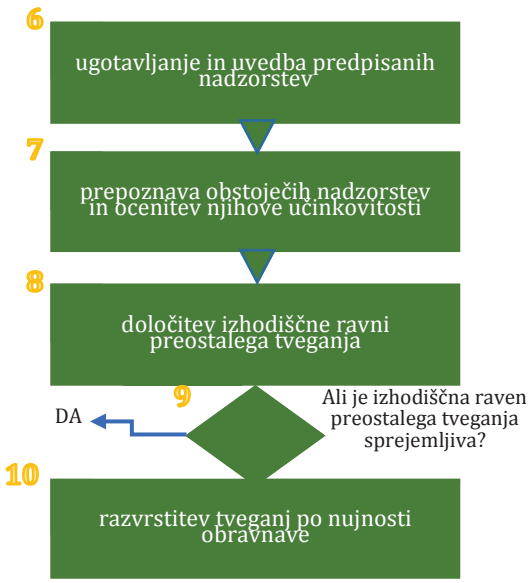
4.1.3 Izložki

Seznam inherentnih tveganj z dodeljenimi ravnmi tveganja

4.1.4 Vloge in odgovornosti

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	STROKOVNJAK ZA PODROČJE	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV
1		Ps	Pd	O		Z
2	Z	Ps	Pd		Ps	O
3	Z		Pd			O
4	Z	Ps	Z	O	Z	Z
5	Z		Z	O		Z

4.2 2. faza – vrednotenje tveganja



Vrednotenje tveganja je proces primerjanja rezultatov analize tveganja z merili tveganja, da ugotovimo, ali je tveganje oziroma njegova raven sprejemljiva. Vrednotenje tveganja nam je v pomoč pri odločitvi o obravnavanju tveganja.

Vrednotenje tveganja izhaja iz razumevanja tveganja, ki ga pridobimo z analizo tveganja, da sprejmemo odločitve o prihodnjih ukrepih. Odločamo predvsem o tem, ali moramo opraviti določene aktivnosti in katere so prednostne naloge pri obravnavi tveganja ob upoštevanju ocenjenih ravni tveganja.

4.2.1 Vložki

– Seznam ugotovljenih informacijskih premoženj in sistemov ter drugih informacijskih sredstev z razvrstitvijo v varnostne razrede in z njimi povezana tveganja z določitvijo ravni tveganj.

4.2.2 Postopkovna navodila

6. korak – ugotavljanje in uvedba predpisanih nadzorstev

a. Iz popisa informacijskega premoženja in informacijskih sistemov, ki smo ga pripravili v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi, prepoznamo varnostne razrede, v katere so sistemi razvrščeni v skladu s predpisi o informacijski varnosti, tajnih podatkih, osebnih podatkih in drugimi predpisi.

b. Določimo nadzorstvene zahteve iz predpisov o informacijski varnosti, tajnih podatkih, osebnih podatkih in drugih predpisov, glede na razvrstitev v varnostne razrede.

c. Ugotovljena predpisana nadzorstva povežemo s prepoznanimi tveganji.

d. Uvedemo še neuvedena predpisana nadzorstva.

7. korak – prepoznava obstoječih nadzorstev in ocenitev njihove učinkovitosti

a. Obstoječa nadzorstva so zaščite oziroma protiukrepi, ki jih organ že izvaja za zaščito informacijskih sredstev.

b. S prepoznavo obstoječih nadzorstev, ki vplivajo na posamezna tveganja, se izognemo nepotrebnemu delu ali stroškom, na primer zaradi podvajanja nadzorstev.

c. Informacije o obstoječih nadzorstvih pridobimo od skrbnikov informacijskih sistemov in vodij organizacijskih enot.

d. Skrbniki informacijskih sistemov in vodje organizacijskih enot za prepoznavanje obstoječih nadzorstev izvedejo naslednje dejavnosti:

- pregled dokumentov, ki vsebujejo informacije o nadzorstvih, če so procesi dobro dokumentirani z vsemi obstoječimi nadzorstvi in podatki o njihovi uvedbi oziroma izvajanju,
- preveritev pri odgovornih osebah in uporabnikih, ki izvajajo nadzorstva,
- pregleda fizičnih nadzorstev na kraju samem, ali delujejo pravilno in učinkovito,
- pregled izidov notranjih presoj ali drugih pregledov skladnosti.

e. Skrbnik informacijskega sistema ali vodja organizacijske enote oceni učinkovitost obstoječih nadzorstev v skladu z matriko iz poglavja 2.4.8.

8. korak – določitev izhodiščne ravni preostalega tveganja

a. Izhodiščna raven preostalega tveganja upošteva (predpisana, obstoječa) nadzorstva in jo določimo tako, da se vsak posamezni vidik (inherentnega) tveganja zmanjša za faktor učinkovitosti, ki ga ocenimo za posamezno nadzorstvo glede na ta vidik in raven izvajanja tega nadzorstva (glej poglavje 2.4.5).

b) **Izhodiščna raven preostalega tveganja** $\boldsymbol{R_{ip,v}}$ za posamezni vidik informacijske varnosti (v = z, c ali r) z upoštevanjem posameznega nadzorstva, izračunamo z enačbo:

$$\boldsymbol{R_{ip,v} = R_{i,v}\left(1 - \frac{N_{u,v}}{100}\right) = R_{i,v}\,F_v}$$

kjer je $R_{i,v}$ raven inherentnega tveganja glede na posamezen vidik informacijske varnosti (v = z, c ali r), $N_{u,v}$ učinkovitost[3] (v %) tega nadzorstva glede na posamezni vidik informacijske varnosti (v = z, c ali r). F je faktor zmanjšanja tveganja.

Tveganje lahko zmanjšujemo z uvedbo več nadzorstev.

Izhodiščna raven preostalega tveganja ($R_{ip,v,n}$) za posamezen vidik (v) informacijske varnosti (v = zaupnost (z), celovitost (c) ali razpoložljivost (r), **z upoštevanjem n nadzorstev**, izračunamo torej po enačbi:

$$\boldsymbol{R_{ip,v,n} = R_{i,v}\ F_1\,F_2 \ldots F_n}$$

Celotna izhodiščna raven preostalega tveganja $\boldsymbol{R_{ip}}$ je vsota vrednosti preostalih tveganj za posamezne vidike informacijske varnosti.

$$\boldsymbol{R_{ip} = \sum_{v=z,c,r} R_{ip,v}}$$

h. Vsakemu ugotovljenemu tveganju v registru pripišemo nadzorstva, ki se nanašajo na to tveganje in celotno izhodiščno raven preostalega tveganja.

9. korak – vprašamo se, ali je izhodiščna raven preostalega tveganja sprejemljiva

a. Ocenjevalec tveganja v sodelovanju z vodjem informacijske varnosti oceni, ali je izhodiščna raven preostalega tveganja sprejemljiva. Pri tem upošteva merila iz poglavja 2.4.7.

[3] Takšno učinkovitost nadzorstva upoštevamo v primeru, ko je nadzorstvo v celoti izvedeno. Če je izvedba delna, učinkovitost ustrezno zmanjšamo.

b. Če je raven izhodiščnega preostalega tveganja sprejemljiva, nadaljujemo s korakom 18, sicer nadaljujmo s korakom 10, da določimo prednostne naloge pri obravnavi tveganj.

10. korak – razvrstitev tveganj po nujnosti obravnave

a. Ocenjevalec tveganja oziroma vodja informacijske varnosti določi vrstni red obravnave ocenjenim tveganjem v skladu z merili iz poglavja 2.4.7.

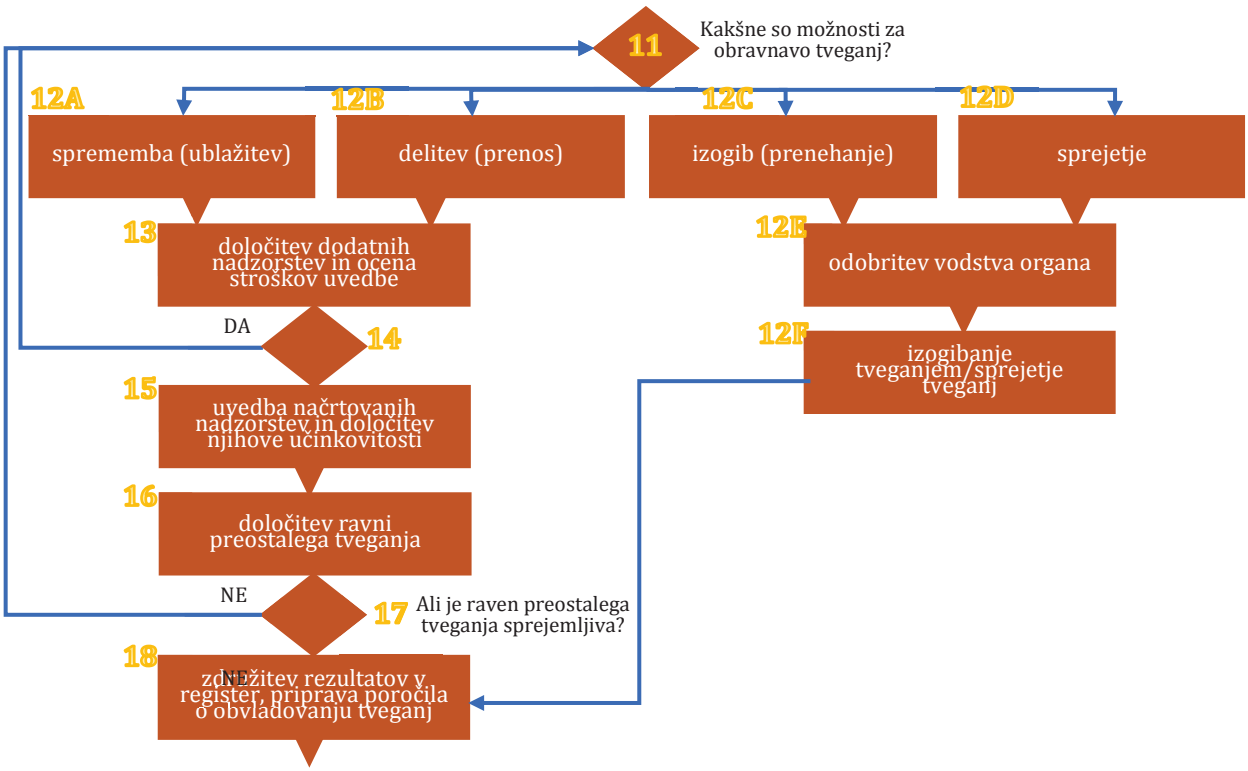
4.2.3 Izložek

Seznam tveganj z ocenami izhodiščnih ravni preostalih tveganj, razvrščenih po vrstnem redu njihove obravnave.

4.2.4 Vloge in odgovornosti

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	STROKOVNJAK ZA PODROČJE	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV
6	Pd	Ps	O		Z	Z
7	Z	Ps	Pd		Z	O
8	Z	Pd		O		
9	Z		Z			O
10	Z	Pd		O		

4.3 3. faza – obravnava tveganja



Obravnava tveganja vključuje ugotavljanje, razvrščanje, vrednotenje in uvedbo oziroma izvajanje ustreznih dodatnih ukrepov za zmanjševanje tveganja. Organ odloči, ali bo tveganje, ki vpliva na posamezno informacijsko sredstvo, spremenil, delil z drugimi subjekti, se mu izognil ali ga sprejel (v primerih, kadar ustrezni ukrepi za zmanjšanje tveganja niso na voljo ali niso uresničljivi).

Ob sprejetju končnega preostalega tveganja (z obstoječimi nadzorstvi ali dodatnimi nadzorstvi) mora obravnavo tveganja odobriti skrbnik informacijskega sistema, na katerega se tveganje nanaša. Nato pripravimo načrt obravnave tveganj in začnemo z izvedbo.

4.3.1 Vložek

Seznam tveganj z ocenami izhodiščnih ravni preostalih tveganj, razvrščenih po prednostnem vrstnem redu njihove obravnave.

4.3.2 Postopkovna navodila

11. korak – vprašamo se, kakšne so možnosti za obravnavo tveganj

a. Če je potrebna obravnava tveganja, upoštevamo eno od naslednjih možnosti:

- **spremembo tveganja** – spremenimo (ublažimo) tveganje,
- **delitev tveganja** – delimo tveganje tako, da ga (delno) prenesemo na drug subjekt,
- **izogib tveganju** – izognemo se tveganju,
- **sprejetje tveganja** – obdržimo (sprejmemo) tveganje.

12.A korak – sprememba (ublažitev)

a. Za spremembo oziroma ublažitev tveganj ugotovimo in izberemo ustrezna nadzorstva.

b. Cilj izbire nadzorstva je zmanjšanje tveganja na sprejemljivo raven.

c. Če je izbrana ta možnost (sprememba tveganja), nadaljujemo s 13. korakom.

12.B korak – delitev (prenos)

a. Delitev tveganja je lahko najboljša možnost v primeru, ko se ni mogoče izogniti tveganju ali pa je zmanjšanje tveganja prezahtevno ali predrago.

b. Prenos tveganja na primer lahko dosežemo z zavarovanjem informacijskih sredstev pri zavarovalnici ali z uporabo tretjih oseb oziroma pogodbenih zunanjih izvajalcev, ki prevzamejo del odgovornosti za poslovno škodo zaradi uresničitve tveganj.

c. Če je izbrana ta možnost (delitev tveganja), nadaljujemo s 13. korakom.

12.C korak – izogibanje (prenehanje)

a. Izogibanje tveganju vključuje vse ukrepe, pri katerih se informacijska sredstva oziroma poslovne aktivnosti prenesejo s tveganih na varna območja ali se kritične aktivnosti opustijo.

b. Pri presoji možnosti za izogib tveganjem je treba upoštevati ravnovesje med poslovnimi in finančnimi potrebami.

c. Če je izbrana ta možnost (izogib tveganju), nadaljujemo z 12.E korakom.

12.D korak – sprejetje

a. Sprejetje tveganja vključuje obveščanje odločevalcev o preostalih tveganjih.

b. Če tveganja ni mogoče zmanjšati z uporabo nadaljnjih nadzorstev, odločimo, kako ravnati z njimi.

c. Če je izbrana ta možnost (sprejetje tveganja), nadaljujemo z 12.E korakom.

12.E korak – odobritev vodstva organa

a. Če je izbrana možnost za izogibanje tveganju ali sprejetje tveganja, ocenjevalec tveganja ali vodja informacijske varnosti analizira ta tveganja ter pripravi in predstavi poročilo o oceni s priporočili in utemeljitvami vodstvu organa.

b. Seznam tveganj, ki se jim je treba izogniti ali jih sprejeti, posebej označimo in mu dodamo ustrezne ocene s priporočili in utemeljitvami ter posodobimo register.

c. Vodstvo organa pregleda ta seznam in ga uradno odobri.

12.F korak – izogibanje tveganjem/sprejetje tveganj

a. Izogibanje tveganjem izvedemo z umikom iz načrtovane ali obstoječe dejavnosti ali področja dejavnosti ali spreminjanjem pogojev, pod katerimi se dejavnost izvaja. Primer: za tveganja, ki jih povzroča narava, je lahko stroškovno najučinkovitejša druga možnost fizična preselitev informacijskih sredstev v kraj, kjer tveganja ni ali je pod nadzorom,

b. Sprejetje tveganj zaključimo z njihovim dokumentiranjem.

c. Ko je ta korak (izogibanje tveganjem/sprejetje tveganja) končan, nadaljujemo s 17. korakom.

13. korak – določitev dodatnih nadzorstev in ocena stroškov uvedbe

a. Če je izbrana možnost spreminjanja ali delitve tveganja, morata skrbnik informacijskega sistema in drugih informacijskih sredstev ter ocenjevalec tveganja določiti dodatna nadzorstva, da za zmanjšanje tveganja na sprejemljivo raven, ali prenesti (del) tveganj na tretje osebe in/ali zunanje ponudnike storitev.

b. Skrbnik informacijskega sistema in drugih informacijskih sredstev ter ocenjevalec tveganja morata določiti različne dodatne možnosti nadzorstev ali prenosa tveganja in ugotoviti, ali ti nadzorni ukrepi lahko prispevajo k zmanjšanju tveganja.

c. Ocenjevalec tveganja po posvetovanju s skrbnikom informacijskega sistema in drugih informacijskih sredstev določi stroškovno učinkovita nadzorstva oziroma možnosti prenosov tveganja, ki se lahko uvedejo za obravnavo (spreminjanje ali prenos) posameznega tveganja. Pri tem je treba preučiti potrebe po virih (vključno z nakupi strojne opreme, programske opreme in vzdrževanjem).

d. Nadzorstvo je ocenjeno kot stroškovno učinkovito, če so stroški njegovega izvajanja in vzdrževanja v danem obdobju manjši od pričakovanih stroškov zaradi posledic tveganja, na katerega se nanaša.

e. Ocenjevalec tveganj ali vodja informacijske varnosti posodobi register z informacijami o izbranih možnostih za spreminjanje oziroma prenos tveganja.

f. Skrbnik informacijskega sistema in drugih informacijskih sredstev ali ocenjevalec tveganja oceni stroške dodatnega nadzorstva (nadzorstev), izbranega (izbranih) za vsako sredstvo.

g. Vodja informacijske varnosti v register za vsako uvedeno nadzorstvo vključi naslednje podatke:

- oseba, odgovorna za uvedbo,
- predvideni datum uvedbe in
- ocena stroškov uvedbe.

14. korak – vprašamo se, ali so stroški načrtovanih nadzorstev večji od koristi

a. Ocenjevalec tveganja oziroma skrbnik informacijskega sistema in drugih informacijskih sredstev opravi analizo stroškov in koristi, da ugotovi, ali sta spreminjanje oziroma prenos tveganja stroškovno učinkovita, tj. ali so stroški načrtovanih nadzorstev večji od dejanskih koristi.

b. Če so stroški načrtovanih nadzorstev večji, nadaljujemo z 11. korakom, kjer izberemo drugo možnost za obravnavo tveganja, sicer nadaljujemo s 15. korakom.

15. korak – uvedba načrtovanih nadzorstev in določitev njihove učinkovitosti

a. Skrbnik informacijskega sistema in drugih informacijskih sredstev oziroma ocenjevalec tveganja uvede načrtovana nadzorstva za vsako sredstvo.

b. Pripravi se načrt izvajanja, uvedbo je treba uskladiti z vodjem informacijske varnostni.

c. Ocenjevalec tveganja oziroma skrbnik informacijskega sistema in drugih informacijskih sredstev oceni učinkovitost načrtovanih nadzorstev za vsako sredstvo v skladu z matriko iz poglavja 2.4.8.

16. korak – določitev ravni preostalega tveganja

a) **Raven preostalega tveganja** $R_{p,v}$ za posamezni vidik informacijske varnosti (v = zaupnost (z), celovitost (c) ali razpoložljivost (r), z upoštevanjem posameznega nadzorstva, izračunamo z enačbo:

$$R_{p,v} = R_{i,v}\left(1 - \frac{N_{u,v}}{100}\right) = R_{i,v}\,F_v$$

kjer je $R_{i,v}$ raven inherentnega tveganja glede na posamezni vidik informacijske varnosti (v = z, c ali r), $N_{u,v}$ učinkovitost[4] (v %) tega nadzorstva glede na posamezni vidik informacijske varnosti (v = z, c ali r). F je faktor zmanjšanja tveganja.

Z upoštevanjem več nadzorstev izračun ponovimo tako, da je nova vrednost preostalega tveganja po upoštevanju naslednjega nadzorstva zmanjšana tako, da na predhodni vrednosti preostalega tveganja, izvedemo enako operacijo.

Raven preostalega tveganja $R_{p,v,n}$ za posamezni vidik (v) informacijske varnosti (v = zaupnost (z), celovitost (c) ali razpoložljivost (r), z upoštevanjem n nadzorstev, izračunamo torej z enačbo:

$$R_{p,v,n} = R_{i,v}\;F_1\,F_2 \ldots F_n$$

Celotna raven preostalega tveganja je vsota ravni preostalih tveganj za posamezne vidike informacijske varnosti.

$$R_p = \sum_{v=z,c,r} R_{p,v}$$

b. Vsakemu ugotovljenemu tveganju v registru pripišemo nadzorstva, ki se nanašajo na ta tveganja, raven preostalega tveganja za posamezni vidik IV in celotno raven preostalega tveganja.

c. Raven preostalega tveganja za vsako tveganje presodimo in razvrstimo z uporabo matrike iz poglavja 2.4.7 in posodobimo v registru.

17. korak – vprašamo se, ali je raven preostalega tveganja spremenljiva

a. Ocenjevalec tveganja v sodelovanju z vodjem informacijske varnosti oceni, ali je raven preostalega tveganja sprejemljiva. Pri tem se upoštevajo merila iz poglavja 2.4.7.

b. Če je raven preostalega tveganja sprejemljiva, nadaljujemo s korakom 18, sicer se vrnemo na 11. korak

c. Ocenjevalec tveganja oziroma skrbnik(-i) informacijskega sistema in drugih informacijskih sredstev razišče(-jo) možnosti nadomestnih ukrepov za zmanjševanje tveganja in znoja oceni(-jo) raven tveganja z izbiro dodatnih nadzorstev, dokler ne presodi(-jo), da je preostalo tveganje sprejemljivo.

d. Ocenjevalec tveganja oziroma skrbnik(-i) informacijskega sistema in drugih informacijskih sredstev določi(-jo) nadomestno možnost obravnave tveganja, ki se izbere za naslednje vrste tveganj:

- preostala tveganja, za katere ne obstajajo dodatna izvedljiva nadzorstva in
- preostala tveganja, katerih ravni niso sprejemljive in za kater nehamo iskati dodatna nadzorstva.

[4] Takšno učinkovitost nadzorstva upoštevamo v primeru, ko je nadzorstvo v celoti izvedeno. Če je izvedba delna, učinkovitost ustrezno zmanjšamo.

18. korak – združitev rezultatov v register in priprava osnutka poročila o obvladovanju tveganj informacijske varnosti

a. Vodja informacijske varnosti oziroma ocenjevalec tveganja združi rezultate obvladovanja tveganj oziroma posamezne registre iz različnih organizacijskih enot v skupni register organa.

b. Vodja informacijske varnosti pripravi osnutek poročila o obvladovanju tveganj informacijske varnosti, ki vključuje;

- združen register tveganj informacijske varnosti,
- seznam tveganj, ki so spremenjena, prenesena, smo se jim izognili ali smo jih sprejeli in
- deset največjih tveganj za organ.

4.3.3 Izložek

Osnutek poročila o obravnavanju tveganj informacijske varnosti in združeni register s seznamom tveganj informacijske varnosti, ki jih je treba spremeniti, prenesti, se jim izogniti ali jih sprejeti, vključuje:

- načrt za spremembo in prenos tveganj ter preostala tveganja in
- seznam tveganj, ki smo se jim izognili oziroma smo jih sprejeli.

4.3.4 Vloge in odgovornosti

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	STROKOVNJAK ZA PODROČJE	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV
11	Z	Ps	Pd	I	Z	O
12A	Ps	-	Pd	I	Ps	O
12B	Ps	-	Pd	I	-	O
12C	Ps	-	Pd	I		
12D	Ps	-	Pd	I	-	O
12E	-	-	Pd	Z,O	-	-
12F	Pd	-	Pd	-	-	Z,O
13	Z	Pd	Z	Ps	Ps	Z,O
14	Z		Pd	I	-	Z,O
15	Z		Pd	-	Z	Z,O
16	Z	Pd	-	O	-	-
17	Z	-	Z	-	-	O

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	STROKOVNJAK ZA PODROČJE	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV
18	Pd	-	Z	O	-	-

4.4 4. faza – obveščanje o tveganju

Obveščanje o tveganjih je opredeljeno kot kakršna koli medsebojna komunikacija med deležniki o obstoju, vrsti, obliki, resnosti ali sprejemljivosti tveganj. Za učinkovito obveščanje o tveganjih je treba doseči dogovor o tem, kako obvladovati tveganja z izmenjavo informacij o tveganjih informacijske varnosti med odločevalci in drugimi deležniki.

Dobra odločitev glede obvladovanja tveganja izhaja iz postopka sprejemanja odločitev, ki izraža stališča tistih, ki jih zadeva odločitev. Pri tem je treba upoštevati različne strokovne ocene, vrednote, znanje in dojemanja.

FAZA OBVLADOVANJA TVEGANJ	VODJA INFORMACIJSKE VARNOSTI:
UPRAVLJANJE TVEGANJ	se posvetuje z deležniki pri določanju obsega obvladovanja tveganj informacijske varnosti in se dogovori o načinih komuniciranja;
IDENTIFIKACIJA TVEGANJA	se pogovori o grožnjah ter virih ranljivosti in izpostavljenosti;
OCENA TVEGANJA	sporoča rezultate deležnikom in zagotovi, kadar je to mogoče, hitro dojemanje deležnikov o tveganjih in koristih ter razlogih za to;
OBRAVNAVA TVEGANJ	se posvetujte z deležniki, da pridobi vhodne informacije, potrebne za prepoznavanje in vrednotenje možnih nadzorstev, obvesti deležnike o izbranih strategijah za nadzor tveganja in financiranja, seznani deležnike o koristih, stroških in morebitnih novih tveganjih, povezanih s predlaganimi možnostmi nadzorstev, oceni sprejemljivost možnih nadzorstev in preostalih tveganj, ugotovi, ali so možni kompromisi in obvešča o odločitvah glede izbranih nadzorstev in njihove uvedbe;
SPREMLJANJE IN POROČANJE O TVEGANJIH	spremlja potrebe po spremembah, probleme in pomisleke obstoječih in novih deležnikov.

4.4.1 Vložki

Osnutek poročila o upravljanju tveganja informacijske varnosti in združeni register tveganj informacijske varnosti s seznamom tveganj za varnost informacij, ki jih je treba spremeniti, prenesti, se jim izogniti ali jih sprejeti.

4.4.2 Postopkovna navodila

19. korak – potrditev poročila in obveščanje deležnikov

a. Vodja informacijske varnosti združeni register in predlog poročila o obvladovanju tveganj informacijske varnosti pošlje vodstvu organa.

b. Vodstvo organa pregleda in potrdi predlog poročila o obvladovanju tveganja informacijske varnosti in združeni register.

c. Vodja informacijske varnosti stalno komunicira s tretjimi osebami, posebnimi interesnimi skupinami in regulatornimi organi, da:

- ugotovi in zagotovi skladnost s pričakovanji tretjih oseb in s predpisi,
- prepozna nove in prihodnje predpisane zahteve, pomembne za obvladovanje tveganja informacijske varnosti in
- prepozna in razume nove ali nastajajoče grožnje oziroma tveganja, pomembna za organ, državno upravo in širše območje.

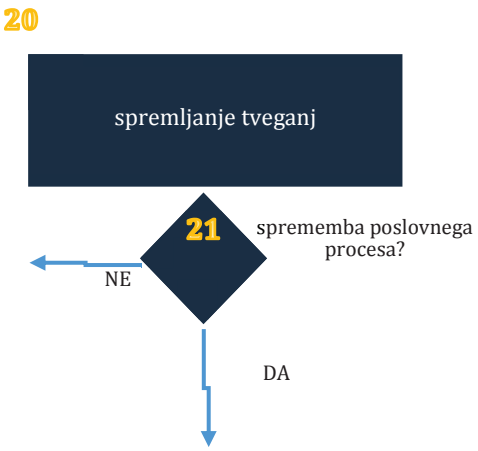
4.4.3 Izložki

- Odobreno poročilo o obvladovanju tveganj informacijske varnosti in združeni register,
- e-poštna sporočila/beležke/brošure.

4.4.4 Vloge in odgovornosti

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV
19	Pd	Z	O	I	I

4.5 5. faza – spremljanje tveganja



Spremljanje tveganja je zadnja faza v procesu obvladovanja tveganj informacijske varnosti. Spremljamo in pregledujemo tveganja in njihove dejavnike (na primer uvrščanje informacijskih sredstev v varnostne razrede oziroma vrednost sredstev, ranljivosti, grožnje, verjetnost nastanka, vpliv in preostalo tveganje), da bi čim prej prepoznali morebitne spremembe organizacijskega okolja in ohranili celovit pogled nad vsemi značilnostmi tveganja.

4.5.1 Vložki

– Vse informacije o tveganjih informacijske varnosti, pridobljene v procesu obvladovanja tveganja in pri zunanjih ter notranjih virih.

4.5.2 Postopkovna navodila

20. korak – spremljanje tveganj

a. Lastnik(-i) tveganja, opredeljen(-i) v registru tveganj informacijske varnosti, mora(-jo) redno spremljati, nadzirati in poročati o stanju in učinkovitosti vsakega ukrepa za obravnavo tveganja.

b. Vodja informacijske varnosti redno spremlja načrt za spreminjanje in prenos tveganj ter doseganje ciljev oziroma odstopanja od načrta.

c. Vodja informacijske varnosti poročilo o spremljanju tveganj v rednih časovnih presledkih pošlje vodstvu organa.

č. Vodstvo organa pregleda poročilo o spremljanju tveganj in priporoči nadaljnje ukrepe, ki jih je treba sprejeti (kadar oceni, da je to potrebno).

d. Vodja informacijske varnosti določi postopke obvladovanja tveganj informacijske varnosti, ki jih je treba sprožiti za vnovično ocenitev vrednosti končnih preostalih tveganj (enkrat letno ali po potrebi).

e. Vodja informacijske varnosti redno zbira informacije, povezane s tveganji informacijske varnosti, iz različnih virov in procesov.

f. Informacije zbiramo iz procesa upravljanja incidentov in problemov, ki vključuje tudi naslednje vire:

- poročila in obvestila SI-CERT-a, nacionalnega odzivnega centra za kibernetsko varnost, SI.GOV-CERT-a, odzivnega centra za kibernetsko varnost v državni upravi, operativnega središča informacijske varnosti v državni upravi itd.,
- poročila notranjih revizij,
- poročila o oceni ranljivosti,
- svetovna raziskovalna poročila,
- revizijska poročila tretjih oseb,
- druge javne informacije.

g. Vodja informacijske varnosti oceni zbrane informacije in presodi, ali obstajajo dejavniki, ki vplivajo na tveganje, in ali vplivajo na organ.

h. Najpomembnejši dejavniki, ki vplivajo na razmere na področju obvladovanja tveganj, so povezani:

- z izjemami pri vzdrževanju nadzorstev,
- z napredkom pri izvajanju načrta za uvedbo sprememb in prenos tveganja,
- s spremembami v značilnostih tveganj in
- s prepoznavo novih informacijskih sredstev.

21. Korak – vprašamo se, ali je prišlo do spremembe poslovnega procesa

a. Vodja informacijske varnosti presodi, ali je prišlo do sprememb v obstoječih ključnih poslovnih procesih, ali so uvedeni novi ključni poslovni procesi, ki lahko vplivajo na cikel obvladovanja tveganj informacijske varnosti, in jih prepozna.

b. Kadar so bile ugotovljene spremembe v obstoječih kritičnih poslovnih procesih ali so bili uvedeni novi ključni poslovni procesi, nadaljujemo s 1. korakom, sicer nadaljujemo s 5. korakom.

c. Vodja informacijske varnosti organa sporoči spremembe v organizaciji vodstvu organa in začne z vnovično oceno tveganja informacijske varnosti.

4.5.3 Izložki

- Nenehno usklajevanje obvladovanja tveganj informacijske varnosti s poslovnimi cilji organa in merili sprejemljivosti tveganja in
- dejavniki/informacije za začetek procesa obvladovanja tveganj.

4.5.4 Vloge in odgovornosti

ŠT. KORAKA V PROCESU	OCENJEVALEC TVEGANJA	STROKOVNJAK ZA PODROČJE	VODJA INFORMACIJSKE VARNOSTI	VODSTVO ORGANA	VODJA IT	SKRBNIK (LASTNIK) INFORMACIJSKEGA SISTEMA, PREMOŽENJA, SREDSTEV	LASTNIK TVEGANJA
20	Pd	-	O	Z	Pd	Pd	Z
21	Z	Ps	Pd	I	Ps	O	-

5 PRILOGA A: Razvrstitev informacijskih sredstev

Informacijska sredstva so kateri koli objekti sistema informacijske varnosti, ki so lahko ogroženi in varovani z nadzorstvi. Za potrebe ocenitve tveganj jih razvrščamo v tri glavne skupine:

1. informacijska premoženja (primarna sredstva),

2. informacijski sistemi (glavna podporna sredstva) in

3. informacijsko okolje (druga podporna sredstva).

Informacijska sredstva lahko nadalje uvrščamo v podskupine itd., jih med seboj povezujemo in tako ustvarimo model sistema upravljanja informacijske varnosti.

Informacijska sredstva v posameznih skupinah oziroma podskupinah so lahko izpostavljena enakim značilnim grožnjam in jih lahko varujemo z enakimi nadzorstvi.

5.1 Informacijska premoženja (primarna sredstva) (IP)

Informacijska premoženja so skupine ključnih informacij, ki se uporabljajo v procesih oziroma pri poslovanju v okviru obsega upravljanja informacijske varnosti. So podatki in informacije, ki jih je glede na poslovna in varnostna merila smiselno obravnavati kot celoto.

Informacije o informacijskih premoženjih so navedene v popisu informacijskega premoženja in informacijskih sistemov, ki je pripravljen v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.

Informacijska premoženja se lahko povezujejo z drugimi informacijskimi sredstvi z namenom, da se zahteve informacijske varnosti, ki veljajo za informacijska premoženja, prenesejo tudi na z njimi povezana druga informacijska sredstva.

Primeri informacijskih premoženj: Centralni register prebivalstva (CRP), Register davčnih zavezancev (RDZ), Kadrovska evidenca organa (KDO) itd.

5.2 Informacijski sistemi (glavna podporna sredstva) (IS)

Informacijski sistemi so soodvisni sestavni deli računalniške strojne, programske in komunikacijske opreme, namenjene za obravnavo (zajemanje, procesiranje, predstavitev, hrambo, prenos ipd.) informacijskega premoženja; so soodvisne storitve, ki zagotavljajo strežniške in omrežne vire, vire za hrambo podatkov, vire uporabniške programske opreme ipd.

So sredstva, s katerimi se obravnavajo informacijska premoženja. Ranljivosti teh sredstev se lahko izkoriščajo za ogrožanje informacijskih premoženj.

Informacije o informacijskih sistemih so v popisu informacijskega premoženja in informacijskih sistemov, ki je pripravljen v skladu z Enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.

Sestavne dele informacijskih sistemov lahko podrobneje razvrstimo v razrede, kot je opisano v nadaljevanju.

5.2.1 Strojna oprema (HW)

5.2.1.1 Nepremične informacijske naprave (HWF)

So računalniške naprave, ki se uporabljajo v prostorih organa, kot so podatkovni, aplikativni, spletni in drugi strežniki, delovne postaje ipd.

5.2.1.2 Prenosne informacijske naprave (HWM)

So prenosni računalniki, dlančniki, osebni organizatorji, pametni telefoni ali podobne prenosne elektronske naprave, ki lahko hranijo, obdelujejo, prikazujejo ali elektronsko prenašajo podatke.

5.2.1.3 Periferne naprave (HWP)

So naprave, priključene na računalnik preko komunikacijskih vrat, za zajem, prikaz ali prenos podatkov, kot so tiskalniki, izmenljivi diskovni pogoni, monitorji ipd.;

5.2.1.4 Izmenljivi (digitalni) nosilci podatkov (INP)

So nosilci podatkov, ki jih je mogoče preprosto povezati z informacijsko napravo ali ločiti od nje (na primer ključ USB, polprevodniški disk, CD, DVD, trdi disk, disketa, magnetni trak ipd.);

5.2.1.5 Drugi nosilci podatkov (DNP)

Na primer papir, fotografski film ipd.

5.2.2 Programska oprema (SW)

5.2.2.1 Operacijski sistem (SWOS)

Je računalniško programje, ki tvori operativne temelje, na katerih se izvajajo vsi drugi programi.

5.2.2.2 Servisna, vzdrževalna in upravljavska programska oprema (SWU)

je računalniška oprema, ki dopolnjuje storitve operacijskega sistema in ni neposredno razpoložljiva končnim uporabnikom in aplikacijam;

5.2.2.3 Standardna predpripravljena programska oprema (SWS)

So celoviti produkti, ki se tržijo in zagotavljajo storitve za uporabnike in aplikacije; primeri: programje za upravljanje podatkovnih baz, programje za elektronsko sporočanje, spletne strežnike, upravljanje imenikov ipd.

5.2.2.4 Poslovne aplikacije (SWAP)

5.2.2.4.1 Standardne poslovne aplikacije (SWSAP)

So komercialni programski paketi, namenjeni neposrednemu dostopu uporabnikov do storitev in funkcij, ki jih potrebujejo pri svojem delu; primeri: računovodske aplikacije, aplikacije za upravljanje odjemalcev in dobaviteljev, aplikacije za upravljanje projektov itd.

5.2.2.4.2 Posebne poslovne aplikacije (SWXAP)

So aplikacije, razvite posebej za uporabnika, ki mu omogočajo dostop do storitev in funkcij, ki jih potrebuje pri svojem delu.

5.2.3 Omrežje (NW)

5.2.3.1 Nosilci in podpora komunikacij (NWN)

5.2.3.2 Pasivni in aktivni releji (NWR)

5.2.3.3 Komunikacijski vmesniki (NWI)

5.2.4 Storitve računalništva v oblaku (SRO)

5.2.4.1 Infrastruktura kot storitev (SRO-IaaS)

5.2.4.2 Platforma kot storitev (SRO-PaaS)

5.2.4.3 Programska oprema kot storitev (SRO-SaaS)

5.3 Informacijsko okolje (druga podporna sredstva) (IO)

So človeški viri in druga materialna sredstva, ki omogočajo delovanje informacijskega sistema ter vplivajo na njegovo varnost in varnost informacijskega premoženja.

5.3.1 Osebje (LJ)

Sestavljajo ga vse skupine oseb, ki so vključene v delovanje informacijskega sistema in obravnavo informacijskega premoženja.

5.3.1.1 Odločevalci (LJO)

so skrbniki (lastniki) informacijskih sistemov in informacijskega premoženja (primarnih sredstev) oziroma organizacijski in projektni vodje;

5.3.1.2 Uporabniki (LJU)

Je osebje, ki pri delu na svojih poslovnih področjih odgovorno ravna s primarnimi in podpornimi sredstvi.

5.3.1.3 Operativno in vzdrževalno osebje (LJOp)

Je osebje, ki zagotavlja obratovanje in vzdrževanje informacijskih sistemov; za izvajanje svojih nalog imajo posebne dostopne pravice.

5.3.1.4 Razvijalci (LJR)

So zadolženi za razvoj aplikacij organa; dostopajo do delov informacijskih sistemov s posebnimi pravicami, vendar niso vključeni v obravnavo produkcijskih podatkov.

5.3.2 Delovno okolje (DO)

Vključuje vse kraje, lokacije in prostore, kjer so sredstva in viri, ki spadajo v obseg upravljanja informacijske varnosti, ter fizična sredstva, potrebna za njihovo obratovanje.

5.3.2.1 Zunanje okolje (ZO)

So vse lokacije, na katerih ni mogoče uporabiti varnostnih nadzorstev organizacije.

5.3.2.2 Poslovne zgradbe (PZ)

So območja zgradb organa, ki so ločena od zunanjega okolja s fizičnimi preprekami in/ali z nadzorom.

5.3.2.3 Varovana območja (VO)

So območja v zgradbah organa, ki so fizično razmejena in se razlikujejo po režimih dostopov.

5.3.2.4 Storitve in sredstva za dobavo storitev (UT)

So viri in sredstva za zagotavljanje električne energije, telekomunikacijske storitve, internet, vodovod, kanalizacija, gretje, hlajenje.

6 PRILOGA B: Skupine in vrste groženj

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIV NA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
1. FIZIČNI NAPAD	Grožnje, ki se nanašajo na namerne, sovražne človeške aktivnosti		
1.1. GOLJUFIJA	Goljufija, ki jo stori človek	z, c	1-IP, 2.2-SW, 2.3-NW
1.2. GOLJUFIJA, KI JO IZVRŠI ZAPOSLENEC	Goljufije, ki jih storijo zaposlenci ali drugi, ki so v razmerju s subjekti, ki imajo dostop do informacijskih premoženj in drugih informacijskih sredstev subjektov.	z, c	1-IP, 2.2-SW, 2.3-NW, 3.1-LJ
1.3. SABOTAŽA	Namerne dejavnosti (neizpolnitev ali pomanjkljivo izpolnjevanje osebnih dolžnosti), katerih cilj je povzročiti motnje ali poškodbe informacijskih sredstev.	c, r	1-IP, 2.1-HW, 2.2-SW, 2.3-NW, 3-IO
1.4. VANDALIZEM	Dejanje fizičnega poškodovanja informacijskih sredstev.	c, r	2.1-HW, 2.3-NW, 3-IO
1.5. KRAJA (NAPRAV, MEDIJEV ZA HRAMBO IN DOKUMENTOV)	Kraja informacij ali drugih informacijskih sredstev.	z, c, r	1-IP, 2.1-HW, 2.2-SW
1.6. KRAJA NEPREMIČNE STROJNE OPREME	Odtujitev strojne opreme druge osebe (razen prenosnih naprav), ki pogosto vsebuje poslovno občutljive podatke.	z, c, r	2.1.1-HWF
1.7. KRAJA DOKUMENTOV	Kraja dokumentov iz zasebnih arhivov ali arhivov podjetij, pogosto zaradi preprodaje ali osebne koristi.	z, r	2.1.4-INP, 2.1.5-DNP
1.8. KRAJA VARNOSTNIH KOPIJ	Kraja naprav z mediji, na katerih se hranijo kopije pomembnih informacij.	z, r	2.1.4-INP, 2.1.5-DNP
1.9. UHAJANJE/NEPOOBLAŠČENA IZMENJAVA INFORMACIJ	Izmenjava podatkov z nepooblaščenimi osebami. Izguba zaupnosti informacij zaradi namernih človeških dejanj (na primer lahko pride do uhajanja informacij zaradi izgube papirnih izvodov zaupnih informacij).	z	1-IP-3.1-LJ
1.10. NEPOOBLAŠČENI FIZIČNI DOSTOP/NEPOOBLAŠČENI VSTOP V PROSTORE	Neodobreni dostop do objekta.	z	3.2-DO

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
1.11. PRISILA, IZSILJEVANJE ALI KORUPCIJA	Aktivnosti, ki so povezane s prisilo, izsiljevanjem ali korupcijo.	z, c	3.1-LJ
1.12. POŠKODBE ZARADI VOJNE	Grožnje neposrednega vpliva vojnih dejavnosti.	c, r	3.1-LJ , 3.2-DO
1.13. TERORISTIČNI NAPAD	Teroristična grožnja	c, r	3.1-LJ , 3.2-DO
2. NENAMERNO POVZROČANJE ŠKODE	Grožnje nenamernih človeških dejanj ali napak.		
2.1. UHAJANJE/IZMENJAVA INFORMACIJ ZARADI ČLOVEŠKE NAPAKE	Uhajanje / izmenjava informacij, ki jo povzročijo ljudje zaradi svojih napak.	z	1-IP
2.2. NENAMERNO UHAJANJE/IZMENJAVA INFORMACIJ ZAPOSLENIH	Nenamerna uslužbenčeva izmenjava zasebnih ali občutljivih informacij uslužbenca z nepooblaščeno osebo.	z	1-IP
2.3. UHAJANJE PODATKOV PREK MOBILNIH APLIKACIJ	Uhajanje zasebnih podatkov (zaradi uporabe aplikacij za mobilne naprave).	z	1-IP, 2.2.3-SWS, 2.2.4-SWAP
2.4. UHAJANJE PODATKOV PREK SPLETNIH APLIKACIJ	Uhajanje pomembnih informacij z uporabo spletnih aplikacij.	z	2.2.3-SWS, 2.2.4-SWAP
2.5. UHAJANJE INFORMACIJ PO OMREŽJU	Prisluškovanje nezavarovanega omrežnega prometa.	z	2.3-NW
2.6. NAPAČNA UPORABA ALI UPRAVLJANJE NAPRAV IN SISTEMOV	Uhajanje informacij izmenjava informacij/povzročitev škode informacijam zaradi zlorabe informacijskih sredstev (pomanjkanje zavedanja o aplikacijskih funkcijah) ali napačna oziroma nepravilna konfiguracija ali upravljanje informacijskih sredstev.	z, c, r	2.1-HW, 2.2-SW
2.7. IZGUBA INFORMACIJ ZARADI NAPAK PRI VZDRŽEVANJU IN NAPAK OPERATERJEV	Izguba podatkov zaradi nepravilno izvedenega vzdrževanja naprav ali sistemov ali drugih dejavnosti upravljavca.	c, r	2.1-HW, 2.2-SW
2.8. IZGUBA INFORMACIJ ZARADI NAPAKE PRI KONFIGURACIJI/NAMESTITVI	Izguba podatkov zaradi napak pri namestitvi ali konfiguraciji sistema.	c, r	2.1-HW, 2.2-SW
2.9. PODALJŠANJE ČASA OKREVANJA	Nerazpoložljivost informacij zaradi napak pri uporabi nosilcev podatkov z varnostnimi kopijami in podaljšanega časa za obnovitev informacij.	r	1-IP, 2.1.4-INP

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
2.10. IZGUBA INFORMACIJ ZARADI NAPAK UPORABNIKA	Nerazpoložljivost informacij ali poškodb informacijskih virov zaradi napak uporabnika (pri uporabi IT infrastrukture) ali trajanja obnovitve programske opreme.	r, c	1-IP, 2-IS
2.11. UPORABA INFORMACIJ IZ NEZANESLJIVEGA VIRA	Slabe odločitve na podlagi nezanesljivih virov informacij ali nepreverjenih informacij.	z, c, r	1-IP
2.12. NENAMERNA SPREMEMBA PODATKOV V INFORMACIJSKEM SISTEMU	Izguba celovitosti informacij zaradi človeške napake (napaka uporabnika informacijskega sistema).	c	1-IP
2.13. NEUSTREZNA ZASNOVA IN NAČRTOVANJE ALI NEUSTREZNA PRILAGODITEV	Neustrezna informacijska sredstva ali zasnova poslovnih procesov (neustrezne specifikacije izdelkov IT, neustrezna uporabnost, nezanesljivi vmesniki, politike / postopkovni tokovi, napake v zasnovi).	z, c, r	2-IS
2.14. POŠKODBA, KI JO POVZROČI TRETJA OSEBA	Poškodbe informacijskih sredstev, ki jih povzroči tretja oseba.	c, r	2-IS
2.15. VARNOSTNE NAPAKE, KI JIH POVZROČI TRETJA OSEBA	Škoda, povzročena informacijskim sredstvom, ki jo povzročijo tretje osebe s kršitvijo varnostnih predpisov.	c, r	2-IS
2.16. POŠKODBE, KI NASTANEJO PRI PENETRACIJSKIH TESTIH	Škoda, povzročena informacijskim sistemom zaradi neustreznega izvajanja penetracijskih testov.	c, r	2-IS
2.17. IZGUBA INFORMACIJ V OBLAKU	Izguba informacij ali podatkov, shranjenih v oblaku.	c, r	2-IS
2.18. IZGUBA (CELOVITOSTI) OBČUTLJIVIH INFORMACIJ	Izguba informacij ali podatkov ali spreminjanje občutljivih informacij.	c. r	1-IP
2.19. IZGUBA CELOVITOSTI CERTIFIKATOV	Izguba celovitosti certifikatov, ki se uporabljajo za storitve avtorizacije.	c	1-IP
2.20. IZGUBA NAPRAV, NOSILCEV PODATKOV IN DOKUMENTOV	Nerazpoložljivost (izguba) informacijskih sredstev in dokumentov.	r	2.1-HW
2.21. IZGUBA NAPRAV/PRENOSNIH NAPRAV	Izguba prenosnih naprav.	z, r	2.1.2-HWM
2.22. IZGUBA MEDIJEV ZA HRAMBO	Izguba medijev za hrambo podatkov (podatkovnih nosilcev).	z, r	2.1.4-INP

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
2.23. IZGUBA DOKUMENTACIJE O IKT INFRASTRUKTURI	Izguba pomembne dokumentacije.	z, r	2.1.5-DNP
2.24. UNIČENJE ZAPISOV	Nerazpoložljivost (uničenje) podatkov in zapisov (informacij), shranjenih v napravah in medijih za hrambo.	r	2.1.4-INP, 2.1.5-DNP
2.25. OKUŽBA IZMENLJIVIH NOSILCEV PODATKOV	Izguba pomembnih podatkov zaradi uporabe izmenljivih nosilcev podatkov, spleta ali okužene pošte.	r	2.1.4-INP, 2.2-SW
2.26. ZLORABA HRAMBE	Izguba zapisov zaradi nepravilne/nepooblaščene uporabe pomnilniških naprav.	r	2.1.3-HWP
3. DOGODKI, KI POVZROČIJO ŠKODO VEČJIH RAZSEŽNOSTI	Poškodbe informacijskih sredstev, ki jih povzročajo naravni ali okoljski dejavniki.		
3.1. POŽAR	Nevarnost požara.	c, r	3.2-DO
3.2. ONESNAŽENJE, PRAH, KOROZIJA	Motenje dela informacijskih sistemov (strojne opreme) zaradi onesnaženja, prahu ali korozije (ki izhajajo iz zraka).	c, r	3.2-DO
3.3. STRELA	Poškodba računalniške strojne opreme, ki jo povzroči udar strele (prenapetost).	c, r	3.2-DO
3.4. VODA	Poškodba računalniške strojne opreme, ki jo povzroča voda.	c, r	3.2-DO
3.5. EKSPLOZIJA	Poškodba računalniške strojne opreme zaradi eksplozije.	c, r	3.2-DO
3.6. UHAJANJE NEVARNEGA SEVANJA	Poškodba računalniške strojne opreme, ki jo povzroči uhajanje sevanja.	c, r	3.2-DO
3.7. NEUGODNE PODNEBNE RAZMERE	Motenje delovanja informacijskih sistemov zaradi podnebnih razmer, ki negativno vplivajo na strojno opremo.	c, r	3.2-DO
3.8. IZGUBA PODATKOV ALI DOSTOPNOSTI IKT INFRASTRUKTURE ZARADI POVEČANE VLAŽNOSTI	Motenje delovanja informacijskih sistemov zaradi velike vlažnosti.	c, r	3.2-DO
3.9. IZGUBA PODATKOV ALI DOSTOPNOSTI INFORMACIJSKE INFRASTRUKTURE ZARADI	Motnje delovanja informacijskih sistemov zaradi visoke ali nizke temperature.	c, r	3.2-DO

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIV NA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
ZELO VISOKE/NIZKE TEMPERATURE			
3.10. GROŽNJE IZ VESOLJA/ELEKTROMAGNETNA NEVIHTA	Nevarnosti zaradi negativnega vpliva sončnega sevanja na satelite in radiovalovne komunikacijske sisteme (elektromagnetna nevihta).	c, r	3.2-DO
3.11. DIVJE ŽIVALI	Uničenje informacijskih sredstev, ki jo povzročijo živali: miši, podgane, ptice itd.	c, r	3.2-DO
4. OKVARE – SLABO DELOVANJE	Okvara/slabo delovanje informacijske infrastrukture (na primer poslabšanje kakovosti, neustrezni delovni parametri, motenje). Vzrok za napako je večinoma notranja težava (na primer preobremenitev električnega omrežja v stavbi).		
4.1. OKVARA NAPRAV ALI SISTEMOV	Okvara računalniške strojne ali programske opreme ali njenih delov.	c, r	2.1-HW, 2.2-SW
4.2. OKVARA NOSILCEV PODATKOV	Okvara nosilcev podatkov.	c, r	2.1.3-HWP, 2.1.4-INP
4.3. OKVARA RAČUNALNIŠKE STROJNE OPREME	Okvara računalniške strojne opreme.	r	2.1-HW
4.4. OKVARA APLIKACIJ IN STORITEV	Okvara aplikativne programske opreme ali storitev.	c, r	2.2.3-SWS, 2.2.4-SWAP
4.5. OKVARA SESTAVNIH DELOV NAPRAV (KONEKTORJI, VTIČNICE)	Okvara računalniške opreme ali njenih delov.	r	2.1-HW
4.6. OKVARA ALI MOTNJA DELOVANJA KOMUNIKACIJSKIH POVEZAV (KOMUNIKACIJSKIH OMREŽIJ)	Okvara ali slabo delovanje komunikacijskih povezav.	c, r	2.3-NW
4.7. OKVARA KABELSKIH OMREŽIJ	Okvara komunikacijskih povezav zaradi težav s kabelskim omrežjem.	c, r	2.3-NW
4.8. OKVARA BREZŽIČNIH OMREŽIJ	Okvara komunikacijskih povezav zaradi težav z brezžičnimi omrežji.	c, r	2.3-NW
4.9. OKVARA MOBILNIH OMREŽIJ	Okvara komunikacijskih povezav zaradi težav z mobilnimi omrežji.	c, r	2.3-NW

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
4.10. OKVARE ALI MOTNJE PRI OSKRBI Z ELEKTRIČNO ENERGIJO	Okvara ali motnje v oskrbi električne energijo, ki je potrebna za informacijske sisteme.	r	3.2.4-UT
4.11. OKVARE ALI MOTNJE ELEKTRIČNEGA NAPAJANJA	Okvara ali motnje električnega napajanja.	r	3.2.4-UT
4.12. OKVARA HLADILNE INFRASTRUKTURE	Okvara informacijskih sredstev zaradi neustreznega delovanja hladilne infrastrukture.	r	3.2.4-UT
4.13. OKVARA ALI MOTNJE PRI PONUDNIKIH STORITEV (OSKRBOVALNA VERIGA)	Okvara ali motnje pri storitvah tretjih oseb, potrebnih za pravilno delovanje informacijskih sistemov.	r	3.2.4-UT
4.14. SLABO DELOVANJE OPREME (NAPRAV ALI SISTEMOV)	Okvara računalniške strojne opreme in/ali programske opreme ali njenih delov (na primer neustrezni delovni parametri, motenje, ponovni zagon).	r	2.1-HW, 2.2-SW
5. IZPADI	Popolna odsotnost ali izguba virov, potrebnih za računalniško infrastrukturo. Vzrok za izpad je predvsem zunanja težava (na primer izpad električne energije v celem mestu).		
5.1. ODSOTNOST OSEBJA	Nerazpoložljivost ključnega osebja in njegovih kompetenc.	r	3.1-LJ
5.2. STAVKA	Nerazpoložljivost osebja zaradi stavke (odsotnost osebja velikih razsežnosti).	r	3.1-LJ
5.3. IZGUBA PODPORNIH STORITEV	Nerazpoložljivost podpornih storitev, potrebnih za pravilno delovanje informacijskega sistema.	r	3.2.4-UT
5.4. IZPAD INTERNETA	Nerazpoložljivost internetnih povezav.	r	3.2.4-UT
5.5. IZPAD OMREŽJA	Nerazpoložljivost komunikacijskih povezav.	r	3.2.4-UT
5.6. IZPAD KABELSKIH OMREŽIJ	Nerazpoložljivost komunikacijskih povezav zaradi težav s kabelskim omrežjem.	r	3.2.4-UT
5.7. IZPAD BREZŽIČNIH OMREŽIJ KRATKEGA DOSEGA	Nerazpoložljivost komunikacijskih povezav zaradi težav z brezžičnimi omrežji (omrežja 802.11, Bluetooth, NFC itd.).	r	3.2.4-UT

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
5.8. IZPADI BREZŽIČNIH OMREŽIJ DOLGEGA DOSEGA	Nerazpoložljivost komunikacijskih povezav zaradi težav z mobilnimi omrežji, kot so omrežja mobilne telefonije (3G, LTE, GSM itd.) ali satelitskih povezav.	r	3.2.4-UT
6. PRISLUŠKOVANJE, PRESTREZANJE, UGRABITEV	Poseganje v komunikacijo med dvema stranema. Za te napade ni potrebna namestitev dodatnih orodij/programske opreme na mestu žrtve.		
6.1. VOJNA VOŽNJA (»WAR DRIVING«)	Iskanje in morebitno izkoriščanje povezave z brezžičnim omrežjem.	z	2.3-NW
6.2. PRESTREZANJE SEVANJA	Razkritje informacij s prestrezanjem in analizo emisij (sevanja), ki vsebuje informacije.	z	2.1.1-HWF, 2.1.2-HWM, 2.1.3-HWP, 2.3-NW
6.3. PRESTREZANJE INFORMACIJ	Prestrezanje informacij, ki so neustrezno zavarovane pri prenosu ali zaradi neustreznih ravnanj osebja.	z	1-IP
6.4. INDUSTRIJSKO VOHUNJENJE	Pridobivanje zaupnih informacij z nepoštenimi sredstvi.	z	3.1-LJ
6.5. DRŽAVNO VOHUNJENJE	Kraje informacij z državnim vohunjenjem (na primer državno vohunjenje na Kitajskem, NSA iz ZDA).	z	3.1-LJ
6.6. UHAJANJE INFORMACIJ ZARADI NEZAVAROVANIH WI-FI, GOLJUFIVIH DOSTOPNIH TOČK	Pridobivanje pomembnih informacij z nezanesljivimi omrežnimi dostopnimi točkami itd.	z	3.2.4-UT
6.7. MOTEČE SEVANJE	Izpad strojne opreme ali komunikacijske povezave zaradi elektromagnetne indukcije ali elektromagnetnega sevanja, ki ga oddaja zunanji vir.	r	2.1-HW, 2.3-NW
6.8. PONOVITEV SPOROČIL	Zlonamerno ali goljufivo ponovljeni ali zapozneli veljavni prenos podatkov.	z	2.3-NW
6.9. IZVIDNIŠTVO OMREŽJA, MANIPULACIJA OMREŽNEGA PROMETA IN ZBIRANJE INFORMACIJ	Prepoznavanje informacij o omrežju pri iskanju varnostnih pomanjkljivosti.	z	2.3-NW

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
6.10. ČLOVEK V SREDINI/UGRABITEV SEJE	Vključevanje v komunikacijo ali spreminjanje komunikacije med dvema stranema.	z	2.3-NW
7. ZLONAMERNE AKTIVNOSTI/ZLORABE	Zlonamerne aktivnostmi, pri katerih napadalci uporabljajo posebna orodja. Ti napadi zahtevajo namestitev dodatnih orodij oziroma programske opreme ali izvajanje dodatnih korakov na računalniški infrastrukturi oziroma programski opremi žrtve.		
7.1. KRAJA IDENTITETE (GOLJUFIJA Z IDENTITETO/RAČUNOM)	Kraja identitete.	z	3.1-LJ
7.2. TROJANCI, KI KRADEJO POVERILNICE	Kraja identitete z zlonamernimi računalniškimi programi.	z	3.1-LJ
7.3. PREJEMANJE NENAROČENE E-POŠTE	Prejemanje neželene e-pošte, kar vpliva na varnost informacij in učinkovitost.	z, r	1-IP, 3.1-LJ
7.4. SPAM (NEZAŽELENA POŠTA)	Prejemanje nenaročenih, nezaželenih ali nezakonitih e-poštnih sporočil.	z	3.1-LJ
7.5. NENAROČENA OKUŽENA E-POŠTNA SPOROČILA	Neželena e-poštna sporočila, ki lahko vsebujejo okužene priloge ali povezave do zlonamernih/okuženih spletnih mest.	z, r, c	3.1-LJ
7.6. ZAVRNITEV (OHROMITEV) STORITVE	Nerazpoložljivost storitve zaradi množičnih zahtev za storitve.	r	2-IS
7.7. PORAZDELJENA ZAVRNITEV (OHROMITEV) OMREŽNE STORITVE (DDOS) (NAPAD NA OMREŽNI SLOJ, NA PRIMER IZKORIŠČANJE PROTOKOLA, SLABO OBLIKOVANI PAKETI, POPLAVLJANJE, PONAREJANJE)	Nerazpoložljivost storitev zaradi velikega števila zahtev za dostop do omrežnih storitev od zlonamernih strank.	r	2.3-NW
7.8. PORAZDELJENA ZAVRNITEV (OHROMITEV) APLIKACIJSKE STORITVE (DDOS) (NAPAD NA APLIKACIJSKI SLOJ, NA PRIMER PING OF DEATH, XDOS, WINNUKE, HTTP POPLAVE)	Nerazpoložljivost storitev zaradi velikega števila zahtev, ki jih pošlje več zlonamernih strank.	r	2.3-NW

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIV NA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
7.9. PORAZDELJENA ZAVRNITEV (OHROMITEV) OMREŽNIH IN APLIKACIJSKIH STORITEV (DDOS) (METODE OJAČITVE/ODBOJA, NA PRIMER NTP, DNS, BITTORRENT)	Ustvarjanje velikega števila zahtev z uporabo metode množenja/ojačevanja.	r	2.2-SW, 2.3-NW
7.10. ZLONAMERNA KODA, PROGRAMSKA OPREMA, DEJAVNOST	Zlonamerna koda, programska oprema ali dejavnost.	z, c, r	2.2-SW
7.11. ZASTRUPITEV ISKALNIKA	Namerna manipulacija indeksov iskalnikov.		
7.12. IZKORIŠČANJE LAŽNEGA ZAUPANJA DRUŽBENIM MEDIJEM	Zlonamerne dejavnosti, ki uporabljajo zaupanja vredne družbene medije.	z	3.1-LJ
7.13. ČRVI/TROJANCI	Zlonamerni računalniški programi (trojanci, črvi)	z, r	2.2-SW
7.14. KORENSKI KOMPLETI (ROOTKITS)	Prikrite vrste zlonamerne programske opreme.	z, c, r	2.2-SW
7.15. MOBILNI ZLONAMERNI PROGRAM	Mobilna zlonamerna programska oprema.	z, c, r	2.2-SW
7.16. OKUŽENE ZAUPANJA VREDNE MOBILNE APLIKACIJE	Uporaba mobilne zlonamerne programske opreme, ki je prepoznana kot zaupanja vredna.	z, c, r	2.2-SW
7.17. POVEČANJE PRIVILEGIJEV	Izkoriščanje hroščev, pomanjkljivosti v zasnovi ali spregledi pri konfiguraciji v operacijskem sistemu ali aplikativni programski opremi za pridobitev višje ravni dostopa do virov.	z, c, r	2.2-SW
7.18. NAPADI NA SPLETNO APLIKACIJO, NAPADI VBRIZGANJA/VRIVANJA (INJICIRANJE KODE: SQL, XSS)	Uporaba po meri narejenih spletnih aplikacij, ki so vgrajene na spletnih mestih družbenih medijev, kar lahko privede do namestitve zlonamerne kode na računalnike, ki se uporablja za pridobitev nepooblaščenega dostopa.	z, c, r	2.2-SW
7.19. VOHUNSKO PROGRAMJE ALI ZAVAJALNO OGLAŠEVALNO PROGRAMJE	Uporaba programske opreme, katere namen je zbiranje informacij o osebi ali organizaciji brez njenega vedenja.	z	1-IP, 3.1-LJ
7.20. VIRUSI	Okužba z virusi.	z, c, r	2.2-SW

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
7.21. ZLONAMERNA VARNOSTNA PROGRAMSKA OPREMA/ZAVAJALNO PROGRAMJE/STRAŠILNO PROGRAMJE	Internetna goljufija ali zlonamerna programska oprema, ki zavede uporabnike, da verjamejo, da je na njihovem računalniku virus, in z njimi manipulira, da kupijo ponarejeno orodje za odstranitev.	z	3.1-LJ
7.22. IZSILJEVALSKO PROGRAMJE	Okužba računalniškega sistema ali naprave z zlonamerno programsko opremo, ki omejuje dostop do nje, in zahteva, da uporabnik plača odkupnino za odstranitev omejitve.	r	3.1-LJ
7.23. IZKORIŠČANJE/IZKORIŠČEVALSKI KOMPLETI	Spletno izkoriščanje ali uporaba izkoriščevalske programske opreme.	z, r	2-IS
7.24. SOCIALNI INŽENIRING	Napadi socialnega inženirstva (cilj: manipulacija ravnanja osebja).	z	3.1-LJ
7.25. NAPADI ZVABLJANJA (RIBARJENJA)	Posebna metoda prevare po e-pošti, v kateri storilec pošilja na videz legitimno e-poštno sporočilo z namenom pridobitve osebnih in finančnih podatkov od prejemnikov. Običajno kaže, da sporočila prihajajo iz dobro znanih in zanesljivih spletnih mest.	z	3.1-LJ
7.26. NAPADI USMERJENEGA ZVABLJANJA	Usmerjeno zvabljanje (spear phishing) je na določene cilje usmerjeno e-poštno sporočilo, ki je pripravljeno tako, da ustvari lažno zaupanje in tako privabi žrtev, da razkrije nekatere poslovne ali osebne skrivnosti, ki jih nasprotnik zlorabi.	z	3.1-LJ
7.27. ZLORABA UHAJANJA INFORMACIJ	Uhajanje pomembnih informacij.	z	1-IP
7.28. UHAJANJE, KI VPLIVA NA MOBILNO ZASEBNOST IN MOBILNE APLIKACIJE	Uhajanje pomembnih podatkov zaradi uporabe zlonamernih mobilnih aplikacij.	z	1-IP
7.29. UHAJANJE, KI VPLIVA NA SPLETNO ZASEBNOST IN SPLETNE APLIKACIJE	Uhajanje pomembnih podatkov zaradi uporabe zlonamerne spletne programske opreme.	z	1-IP
7.30. UHAJANJE, KI VPLIVA NA OMREŽNI PROMET	Uhajanje pomembnih informacij v omrežnem prometu.	z	1-IP, 2.3-NW
7.31. UHAJANJE, KI VPLIVA NA RAČUNALNIŠTVO V OBLAKU	Uhajanje pomembnih informacij v računalništvo v oblaku.	z	1-IP, 2.4-SRO, 3.2.4-UT

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
7.32. USTVARJANJE IN UPORABA PREVARANTSKIH POTRDIL	Uporaba prevarantskih potrdil.	z	1-IP
7.33. IZGUBA (CELOVITOSTI) OBČUTLJIVIH INFORMACIJ	Izguba občutljivih informacij zaradi izgube celovitosti.	r, c	1-IP
7.34. NAPAD S POSREDNIKOM/UGRABITEV SEJE	Napad, ki je sestavljen iz izkoriščanja mehanizma nadzora spletnih sej, ki ga običajno upravlja žeton za sejo.	z	1-IP
7.35. PONAREJENA POTRDILA SSL	Zlonamerna programska oprema, podpisana s certifikatom, ki mu navadno inherentno zaupa končna točka.	z	1-IP
7.36. ZLORABA STROJNE IN PROGRAMSKE OPREME	Neodobren ravnaje s strojno in programsko opremo.	c	2.1-HW, 2.2-SW
7.37. ANONIMNI POSREDNIŠKI STREŽNIKI	Nepooblaščeni posegi anonimnih posredniških strežnikov (proxies).	z	1-IP
7.38. ZLORABA RAČUNALNIŠKIH ZMOGLJIVOSTI V OBLAKU ZA SPROŽITEV NAPADOV (KIBERNETSKA KRIMINALITETA KOT STORITEV)	Uporaba obsežnih računalniških zmogljivosti za sprožanje napadov na zahtevo.	z, c, r	1-IP, 2.4-SRO
7.39. ZLORABA RANLJIVOSTI, RANLJIVOSTI DNEVA 0	Napadi z uporabo ranljivosti dneva 0 ali znanih ranljivosti informacijskih sredstev.	z, c, r	1-IP
7.40. DOSTOP DO SPLETNIH STRANI PREKO VERIG POSREDNIŠKIH STREŽNIKOV HTTP (ZAMEGLITEV)	Zaobidenje varnostnih mehanizmov z uporabo posredniških strežnikov HTTP (mimo črnega seznama spletišč).	z, c, r	1-IP
7.41. DOSTOP DO PROGRAMSKE OPREME NAPRAVE	Nedovoljeno zlonamerno ravnanje z dostopom do programske opreme naprave.	z	2.2-SW
7.42. SPREMENJENA PROGRAMSKA OPREMA	Nepooblaščene spremembe kode ali podatkov, z napadom na njihovo celovitost.	c	1-IP, 2.2-SW
7.43. ZLORABLJENA STROJNA OPREMA	Zloraba zaradi nepooblaščenega dostopa do strojne opreme.	c	2.1-HW
7.44. ZLORABA INFORMACIJ	Namerna zloraba podatkov, da bi zavedli informacijske sisteme ali	c	1-IP

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
	nekoga ali za zakrivanje drugih zlonamernih dejavnosti (izguba celovitosti informacij).		
7.45. ZATAJITEV DEJANJ	Namerne manipulacije s podatki za zatajitev dejanj.	c	1-IP
7.46. UGRABITEV NASLOVNEGA PROSTORA (IP PREDPONE)	Nezakonit prevzem skupin naslovov IP.	c	2.3-NW
7.47. MANIPULACIJA USMERJEVALNE TABELE	Usmerjanje omrežnih paketov do naslovov IP, ki niso tisti, kot je bil namen pošiljatelja, z nepooblaščeno manipulacijo z usmerjevalne tabele.	c	2.3-NW
7.48. DNS ZASTRUPLJANJE/DNS PONAREJANJE/DNS MANIPULACIJE	Ponarejanje podatkov DNS.	c	2.3-NW
7.49. PONAREJANJE ZAPISA	Namerna manipulacija s podatki z namenom ponarejanja zapisov.	c	1-IP
7.50. UGRABITEV AVTONOMNEGA SISTEMA	Napadalčev prevzem lastništva celotnega avtonomnega sistema in njegovih predpon, kljub potrditvi izvora.	c	1-IP
7.51. MANIPULACIJA AVTONOMNEGA SISTEMA	Napadalčeva manipulacija celotnega avtonomnega sistema za izvajanje zlonamernih dejanj.	c	1-IP
7.52. PONAREJANJE KONFIGURACIJ	Namerna manipulacija zaradi ponarejanja konfiguracij.	c	1-IP
7.53. ZLORABA REVIZIJSKIH ORODIJ	Zlonamerna dejanja, izvedena z uporabo revizijskih orodij (odkrivanje varnostnih pomanjkljivosti v informacijskih sistemih)	z, c, r	1-IP
7.54. ZLORABA INFORMACIJ / INFORMACIJSKIH SISTEMOV (VKLJUČNO Z MOBILNIMI APLIKACIJAMI)	Zlonamerna aktivnost zaradi zlorabe informacij/informacijskih sistemov.	z, c, r	1-IP
7.55. NEPOOBLAŠČENE DEJAVNOSTI	Zlonamerno dejanje zaradi nepooblaščenih dejavnosti.	z, c, r	1-IP
7.56. NEPOOBLAŠČENA UPORABA ALI UPRAVLJANJE NAPRAV IN SISTEMOV	Zlonamerno delovanje zaradi nepooblaščene uporabe naprav in sistemov.	z, c, r	2-IS

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIV NA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
7.57. NEPOOBLAŠČENA UPORABA PROGRAMSKE OPREME	Zlonamerno dejanje zaradi nepooblaščene uporabe programske opreme.	z, c, r	2.2-SW
7.58. NEPOOBLAŠČENI DOSTOP DO INFORMACIJSKIH SISTEMOV ALI OMREŽIJ (PROTOKOL IMPI, UGRABITEV REGISTRATORJA DNS)	Nepooblaščeni dostop do informacijskih sistemov/omrežja.	z	2-IS
7.59. VDOR V OMREŽJE	Nepooblaščeni dostop do omrežja.	z	2.3-NW
7.60. NEPOOBLAŠČENE SPREMEMBE ZAPISOV	Nepooblaščene spremembe informacij.	c	1-IP
7.61. NEPOOBLAŠČENA NAMESTITEV PROGRAMSKE OPREME	Nepooblaščena namestitev programske opreme.	c	2.2-SW
7.62. SPLETNI NAPADI (POVEZANI S SNEMANJEM, ZLONAMERNIMI URL-JI, NAPADI NA BRSKALNIK)	Namestitev neželene zlonamerne programske opreme z zlorabo spletnih strani.	z, c, r	2.2-SW
7.63. RAZKRITJE ZAUPNIH PODATKOV	Nepooblaščeno razkritje podatkov.	z	1-IP
7.64. POTEGAVŠČINA	Izguba varnosti informacijskih sredstev zaradi prevare.	z, c, r	2-IS
7.65. LAŽNE GOVORICE IN/ALI LAŽNO OPOZORILO	Motnje dela zaradi govoric in/ali lažnega opozorila.	r	3.1-LJ
7.66. ODDALJENA DEJAVNOST (IZVAJANJE)	Zlonamerno dejanje zaradi oddaljene aktivnosti napadalca.	z, c, r	1-IP
7.67. ODDALJENO IZVAJANJE UKAZOV	Zlonamerno dejanje zaradi oddaljenega izvajanja ukazov.	z, c, r	1-IP
7.68. ORODJE ZA ODDALJENI DOSTOP (RAT)	Okužba programske opreme, ki ima zmogljivosti za oddaljeno upravljanje, ki napadalcu omogoča nadzor nad računalnikom žrtve.	z, c, r	2.2-SW
7.69. BOTNETI/ODDALJENA DEJAVNOST	Vdor s programsko opremo iz distribucije zlonamernega programja.	z, c, r	1-IP, 2.2-SW
7.70. CILJNI NAPADI (APT-JI ITD.)	Celovit, ciljno usmerjen napad, ki združuje številne tehnike napada.	z, c, r	1-IP, 2-IS

IME SKUPINE / VRSTE GROŽNJE	OPIS	VPLIVNA (Z, C, R)	CILJNA INFORMACIJSKA SREDSTVA
7.71. MOBILNA ZLONAMERNA PROGRAMSKA OPREMA (EKSFILTRACIJA)	Mobilna programska oprema, katere namen je zbiranje informacij o osebi ali organizaciji brez njenega vedenja.	z	3.1-LJ
7.72. NAPADI USMERJENEGA ZVABLJANJA	Napad, usmerjen na enega uporabnika ali oddelek v organizaciji, ki prihaja od zaupanja vredne osebe v podjetju in zahteva informacije, kot so prijava, identifikatorji in gesla.	z	3.1-LJ
7.73. NAPAD NAPAJALIŠČA	Škodljivo programje na spletnih mestih, ki jih skupina pogosto uporablja.	z, c, r	3.1-LJ
7.74. NEUSPELI POSLOVNI PROCES	Škoda ali izguba informacijskih sredstev zaradi neustrezno izvedenega poslovnega procesa.	c, r	2-IS
7.75. SUROVA MOČ	Nepooblaščeni dostop s sistematičnim preverjanjem vseh možnih ključev ali gesel, dokler ni najden pravilni.	z	1-IP
7.76. ZLORABA POOBLASTIL	Uporaba pooblaščenega dostopa za izvajanje nezakonitih dejanj.	z, c, r	1-IP, 2-IS