INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

Študija

STROKOVNE PODLAGE ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

DELOVNO GRADIVO

Pripravila projektna skupina:

izr. prof. dr. Denis Čaleta

doc. dr. Milan Vršec

doc. dr. Brane Bertoncelj

mag. Miran Vršec

Aljoša Kandžič

Žiga Podgoršek

Ljubljana, april 2019

S podporo Evropske unije iz Sklada za notranjo varnost

Študija **STROKOVNE PODLAGE ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE**

Naročnik: Ministrstvo za obrambo Republike Slovenije
Direktorat za obrambne zadeve

Avtorji: izr. prof. dr. Denis Čaleta
doc. dr. Milan Vršec
doc. dr. Brane Bertoncelj
mag. Miran Vršec
Aljoša Kandžič
Žiga Podgoršek

Dostopno: www.mo.gov.si

Študija je financirana s podporo Evropske unije iz Sklada za notranjo varnost. Študija je izdelek projekta Priprava strokovnih podlag za ocenjevanje tveganj za delovanje kritične infrastrukture (kratica SPOTKI).

Ljubljana, 2019

Študija

STROKOVNE PODLAGE ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

KAZALO

POVZETEK 7

1 UVOD 19

1.1 METODOLOGIJA IZDELAVE ŠTUDIJE 20
1.2 IZRAZOSLOVJE 21
1.3 OMEJITVE PRI IZDELAVI ŠTUDIJE 22
1.4 PREDSTAVITEV DOSEDANJIH RAZISKAV NA PODROČJU KRITIČNE INFRASTRUKTURE 23

2 PREDSTAVITEV PODROČJA UPRAVLJANJA TVEGANJ (ANG. RISK MANAGEMENT) KOT SPLOŠNEGA TEORETIČNEGA OKVIRJA ZA OCENJEVANJE TVEGANJ 26

2.1 PRAVNA IN DRUGA STROKOVNA PODLAGA 31
2.1.1 Nacionalne resolucije, strategije in programi 32
2.1.2 Standardi 43
2.1.3 Nekatera poslovna orodja in tehnike, ki prispevajo k učinkovitemu upravljanju tveganj 48
2.2 SISTEMATIKA UPRAVLJANJA TVEGANJ 49
2.3 RAZLIČNI POGLEDI NA UPRAVLJANJE TVEGANJ 59
2.4 PREGLED RAZLIČNIH VIDIKOV UPRAVLJANJA TVEGANJ 62
2.4.1 Tehnični vidik upravljanja tveganj 62
2.4.2 Ekonomski vidik 63
2.4.3 Sociološki vidik 64
2.4.4 Psihološki vidik 66
2.4.5 Varnostni vidik 70
2.5 KAZALNIKI ZA PRISTOP K OCENJEVANJU TVEGANJ 72
2.5.1 Kazalniki karakterizacije tveganj 72
2.6 PRISTOP K PREPOZNAVANJU TVEGANJA 75
2.7 NADZOR NAD OBLADOVANJEM TVEGANJ 83

3 PREDSTAVITEV PODROČJA OCENJEVANJA TVEGANJ (ANG. RISK ASSESSMENT) S POUDARKOM NA POSEBNOSTIH OCENJEVANJA TVEGANJ NA PODROČJU KRITIČNE INFRASTRUKTURE.....91

3.1 PREDSTAVITEV KRITIČNE INFRASTRUKTURE V REPUBLIKI SLOVENIJI.....91
3.2 PROJEKTNI PRISTOP K OCENJEVANJU TVEGANJ.....94
3.3 PREGLED NEKATERIH MODELOV ZA OBVLADOVANJE TVEGANJ, KI SO PRIMERNI ZA DELOVANJE KRITIČNE INFRASTRUKTURE.....99
3.3.1 Model izrednih dogodkov in posledic.....100
3.3.2 Andersenov model (ang. Universal Business Risk Model Arthur Andersen).....101
3.3.3 Metoda MOSAR (Method Organised for a Systemic Analysis of Risk – sistemska/sistematična analiza tveganj).....104
3.3.4 Model obvladovanja tveganj na bazi notranje integritete in sinergij v gospodarski družbi.....105
3.3.5 Metoda BIA (Business Impact Analysis – analiza poslovnih vplivov), v povezavi s standardom ISO 22301, 22313 , 22317 in ISO/IEC 27005.....107
3.3.6 Model obvladovanja tveganj po enačbi $R = P_A * (1 – P_E) * C$.....107
3.3.7 Model obvladovanja tveganj v KI na bazi posledic izrednih dogodkov, ranljivosti in groženj $R = f (C, V, T)$.....109
3.4 VREDNOSTNA ANALIZA MODELOV OBVLADOVANJA TVEGANJ IN OCENA PRIMERNOSTI ZA DELOVANJE KRITIČNE INFRASTRUKTURE.....110
3.5 OPREDELITEV VRSTE TVEGANJ IN NJIHOVO OCENJEVANJE.....116
3.5.1 Sistemski pristop ocenjevanja tveganj.....116
3.6 SISTEM IN PROCES OCENJEVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE.....125
3.6.1 Proces ocenjevanja tveganj.....125
3.6.2 Določitev kritičnih poslovnih procesov.....127
3.6.3 Rezultati ocenjevanja tveganj.....130
3.6.4 Verodostojnost merjenja posameznih ocenjevanj tveganj.....131

4 PREDSTAVITEV (OPIS IN RAZČLENITEV) PROCESA OCENJEVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE.....135

4.1 POLITIKA UPRAVLJANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE.....138
4.1.1 Korporativno upravljanje.....138
4.1.2 Politika upravljanja tveganj kot segment poslovne politike in razvojne strategije gospodarske družbe, ki upravlja s kritično infrastrukturo.....141
4.1.3 Politika upravljanja tveganj kot sestavni del krovne varnostne politike v sektorjih kritične infrastrukture.....142

4.1.4 Politika upravljanja tveganj kot krovni dokument za upravljanje in obvladovanje vseh tveganj za delovanje kritične infrastrukture 142
4.1.5 Obrazložitev nastajanja in uporabe prilog v politiki upravljanja tveganj 144
4.2 PROCES UPRAVLJANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTRE 145
4.3 IZBRANE METODE ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE....151
4.3.1 Metodologija MOSAR 152
4.4 FMEA (FAILURE MODE AND EFFECTS ANALYSIS - METODOLGIJA ANALIZE MOŽNIH NAPAK IN ŠKODLJIVIH POSLEDIC) 201
4.4.1 Opis korakov za izvedbo metodologije....206
4.5 MODEL ZBIRANJA PODATKOV ZA OCENJEVANJE RANLJIVOSTI, OGROŽENOSTI IN TVEGANJ....217
4.6 OBVLADOVANJE TVEGANJ Z ZAVAROVANJEM PRI ZAVAROVALNICAH....220
4.7 KRIZNO UPRAVLJANJE IN NEPREKINJENO POSLOVANJE 221
4.7.1 Sistem neprekinjenosti poslovanja po ISO 22301 226
4.7.2 Metodologija ISO 22301 skozi PDCA model....226
4.8 USPOSABLJANJE ZA UPRAVLJANJE TVEGANJ V KRITIČNI INFRASTRUKTURI 228
5 VZOREC METODOLOŠKEGA POSTOPKA ZA OCENJEVANJE TVEGANJ NA RAVNI UPRAVLJAVCA KRITIČNE INFRASTRUKTURE 234
5.1 VZPOSTAVITEV SISTEMA UPRAVLJANJA IN OBVLADOVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE....236
5.1.1 Prilagoditev obstoječih ocen tveganj izvirnemu pristopu 237
5.1.2 Ocena tveganj kot vsebinska podlaga za načrtovanje ukrepov za zaščito kritične infrastrukture 239
5.2 VZOREC OCENE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE NA RAVNI UPRAVLJAVCA KRITIČNE INFRASTRUKTURE 239
5.2.1. Razdelilne transformatorske postaje (RTP) kot primer vzorca ocene tveganj v sektorju energetika – v podsektorju električna energija 239
5.2.2 Metodološke, pravne, politične, strokovne in vsebinske podlage za pripravo vzorca ocene tveganj....244
5.2.3 Register (katalog) tveganj kot osnovni vzorec ocene tveganj za delovanje kritične infrastrukture – obvladovanje tveganj na ravni upravljavca kritične infrastrukture....246
5.3 IMPLEMENTACIJA VZORCA REGISTRA (KATALOGA) ZA OCENO TVEGANJ 257
ZAKLJUČEK 298

LITERATURA IN VIRI 303

PRILOGE 318

PRILOGA 1 - OPREDELITEV OSNOVNIH POJMOV 318
PRILOGA 2 - SEZNAM SLIK IN TABEL 325
PRILOGA 3 - PRIMER FMEA DELOVNEGA LISTA 327

POVZETEK

Študija »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture (v nadaljevanju: KI)« je namenjena strokovni javnosti, kot temelj za zagotavljanje metodoloških, vsebinskih in operativnih izhodišč upravljanja ter obvladovanja tveganj. Različni pristopi družboslovnega raziskovanja in vrsta možnih metod in metodologij za ocenjevanje tveganj so pred projektno skupino postavili zahtevno nalogo analize, kateri deli številnih metod in metodologij bi bili lahko uporabni kot primer dobre prakse za ocenjevanje tveganj za delovanje KI v Republiki Sloveniji. Projektna skupina se je osredotočila na širši vidik ocenjevanja tveganj. KI, grožnje, nevarnosti in ranljivost, ocenjevanje tveganj, upravljanje tveganj, njihovo obvladovanje in neprekinjeno delovanje KI so zelo obsežna in medsebojno soodvisna ter vsebinsko povezana področja.

V uvodnem delu je predstavljena metodologija izdelave študije. Pri izvedbi študije smo uporabili različne metode družboslovnega raziskovanja. Za opis metodoloških izhodišč ocenjevanja tveganj pri delovanju KI in navajanje teoretičnih izhodišč smo uporabili opisno metodo dela. Izrazoslovje s področja obravnavanja tveganj je zelo raznoliko, zato smo ga proučili in se odločili, katere izraze bomo uporabili v tej študiji. Namen študije je, da bo ta služila kot strokovno orodje tistim, ki bodo želeli bolj poglobljeno spoznati tematiko, povezano z ocenjevanjem, upravljanjem in obvladovanjem tveganj. Poleg tega so v njej podana lastna razmišljanja, pogledi, strokovne ocene in vsebinske rešitve avtorjev študije. Pomembno omejitev predstavlja dejstvo, da je za temeljito razumevanje omenjene študije potrebno določeno strokovno predznanje. Projektna skupina je izvedla pregled dosedanjih raziskav in druge literature s področja obravnavane tematike. Dosedanje raziskave so služile kot izhodišče študiji, s pomočjo katerih smo predstavili temeljna spoznanja obravnavane tematike.

V predstavitvi področja obvladovanja tveganj je posebna pozornost v študiji namenjena pravni in drugi strokovni podlagi. Sodobno upravljanje KI poteka na podlagi uveljavljenih mednarodnih in nacionalnih standardov, resolucij, strategij in programov. Zlasti analiza standardov je v študiji omogočila organizacijsko, metodološko in izrazoslovno urejen pristop.

Organizacije KI se soočajo z notranjimi in/ali zunanjimi dejavniki, kar vpliva na negotovost in nepredvidljivost razmer ter na doseganje ciljev poslanstva organizacije. Pomembno je, da organizacije KI poskušajo obvladovati tveganja s sistemskim pristopom, ki obsega identifikacijo, analizo, vrednotenje in izvedbo ukrepov, postopkov in aktivnosti, ki tveganja zmanjšajo na še sprejemljiv nivo. Zagotoviti je namreč treba obvladovanje tveganj do te mere, da nimajo pomembnega učinka na osnovne poslovne procese. Ocenjevanje, upravljanje in obvladovanje tveganj za delovanje KI je kompleksno in zahtevno kontinuirano

opravilo na strateški in operativni ravni delovanja organizacij KI. Zato je priporočljivo, da si upravljavci KI pridobijo znanja o poslovnih orodjih in tehnikah (metodah in metodologijah), ki prispevajo k učinkovitejšemu obvladovanju tveganj. To so predvsem orodja kot denimo: npr. benchmarking (primerjanje s konkurenti), business intelligence (pridobivanje pomembnih poslovnih informacij iz okolja in varovanje lastnih zaupnih podatkov), model »dvajsetih ključev« (izboljšanje organiziranosti), BSC sistem uravnoteženih kazalnikov (izboljšanje internih računovodskih, finančnih in drugih evidenc iz poslovanja), filozofija Kaizen (stalne izboljšave) in druga poslovna orodja. Različni avtorji so predstavili tudi različne tipologije tveganj glede na izvor tveganj (naravno, tehnološko), časovno dimenzijo (akutna, kronična), način izpostavljenosti (zrak, voda ipd.), vrsto posledic (poškodbe, smrti) ipd. Upoštevali smo dobro prakso karakterizacije tveganja, ki določa, da je treba oceno tveganja pripraviti na jasen, pregleden in razumen način. V največji meri naj se pri tem upošteva kazalnike preglednosti, jasnosti, doslednosti in razumnosti. Eno od ključnih vprašanj ocenjevanja tveganj je zaznava negotovosti možnih izrednih dogodkov oziroma njihova verjetnost. Gre za vprašanje verjetnostne porazdelitve, saj kdor se odloča v razmerah negotovosti, ne more sklepati o uspešnosti svojih dejanj vnaprej (problem je, ker sklepamo o prihodnosti na podlagi podatkov in informacij iz preteklosti). Prav tako se tudi odločitev ne more presojati v skladu s profilom nagnjenosti k tveganju.

Za osnovna pristopa v študiji smo smiselno uporabili splošni model za presojo tveganj (Vršec, 2010), ki ponazarja tri glavne sklope upravljanja tveganj (analiza tveganj, kontrola tveganj in izravnava tveganj z zavarovanjem) in Nacionalni načrt zaščite infrastrukture v ZDA (National Infrastructure Protection Plan USA, NIPP, 2013), ki podpira okvir za upravljanje tveganj. Okvir omogoča vključevanje strategij, zmogljivosti in strukture upravljanja za sprejemanje odločitev o tveganjih, povezanih s KI. Pristop se lahko uporablja za vse grožnje in nevarnosti, vključno z naravnimi katastrofami in nevarnostmi, ki jih povzroči človek. Obstaja tudi element negotovosti, ki je posledica subjektivnih ocen nevarnosti. Uporabljeni scenariji z razumnimi najslabšimi pogoji, lahko dajejo vrsto možnih rezultatov, ki bi se lahko pojavili pri delovanju organizacij KI. Za pojasnitev teh elementov je treba odgovoriti na naslednja vprašanja: kako lahko določimo in merimo negotovosti, kaj so neželene posledice in kaj so predpostavke o stvarnosti (Renn, 2008). Odgovori (konceptualizacija negotovosti, obseg neželenih posledic, možnost spoznanja stvarnosti) lahko služijo kot vodilo za razlikovanje različnih pogledov na upravljanje in obvladovanje tveganj.

V študiji so analizirani najpomembnejši in najbolj široko uporabljeni modeli ocenjevanja tveganj. Omenjen prikaz in podrobno razumevanje kompleksnosti posameznih metod je pomembna pomoč pri izdelavi metodološkega okvirja za ocenjevanje tveganj za delovanje KI. Vsak upravljavec KI naj bi določil projektno skupino za ocenjevanje tveganj na področju KI v svojem sektorju. Aktivnosti v tem postopku so namenjene vzpostavitvi organizacijske

strukture projekta, kjer so natančno določeni nosilci vlog, njihove naloge in medsebojna razmerja, kar je ključnega pomena za učinkovito izvajanje projekta.

Upravljavec KI z notranjimi postopki in enotno metodologijo določi spremljanje ocenjevanja in upravljanja tveganj (npr. kot »Politika upravljanja tveganj« - ta dokument določa ukrepe, postopke, aktivnosti in pravila za vzpostavitev in delovanje celovitega sistema ocenjevanja, upravljanja in obvladovanja tveganj, ki temelji na opredelitvi ustreznega organizacijskega ustroja in metodološkega okvirja). Pri tem gre za medsebojno sodelovanje strokovnih služb upravljavca KI (lahko tudi s pomočjo zunanjega strokovnjaka), zlasti na poslovnem, upravljavskem, pravnem in varnostnem področju. Zaradi kompleksnosti varnostnih tveganj je obvladovanje tovrstnih tveganj nujna sestavina varnostne politike in izvedenih varnostnih politik. Struktura in vsebina dokumenta o politiki upravljanja tveganj mora biti v skladu z zakonskimi zahtevami in zahtevami standardov, ki dajejo smernice in navodila za upravljanje in obvladovanje tveganj. Poslovna uspešnost organizacij KI izhaja iz poglavitnega cilja, da so poslovni procesi čim manj obremenjeni z možnimi škodami in izgubami. Preprečevanje izrednih dogodkov, posledično pa preprečevanje škod in izgub, je glavni moto varnostne politike.

Kazalci uspešnosti ocenjevanja, upravljanja in obvladovanja tveganj so uspešno poslovanje upravljavca KI (možne nevarnosti in ogrožanja so pod nadzorom in obvladljiva), tekoče preverjanje ustreznosti varnostne strategije in njeno prilagajanje nastalim razmeram. V študiji je priporočilo za celovito identifikacijo tveganj, za uporabo celotnega nabora možnih izrednih dogodkov, ki se lahko zgodijo upravljavcu KI. Kot primer dobre prakse je prikazana operativna uporaba kataloga tveganj (prevzem evra v Republiki Sloveniji 2007). Predstavljen je proces ocenjevanja, upravljanja in obvladovanja tveganj, ki je sestavljen iz petih medsebojno povezanih procesov: identifikacija (prepoznavanje) tveganj, ovrednotenje možnih vplivov, analiziranje možnih rešitev, sprejetje rešitve in spremljanje tveganja, nadzor ter njegovo revidiranje. Celotni proces temelji na določenih poslovnih procesih, virih in vzrokih negotovosti ter kritičnosti poslovnih procesov.

Nadzor nad upravljanjem tveganj se nanaša na razumevanje tveganj, ki jih organizacija KI sprejema in upravlja. Izhodišča za nadzor nad obvladovanjem tveganj so zlasti: pozornost mora biti namenjena strateškim ciljem poslovanja in kritičnim poslovnim procesom, največ pozornosti naj bo namenjeno tistim ciljem poslovanja, od katerih je odvisno uspešno upravljanje finančnih tveganj in zaupanje uporabnikov storitev, vpeljati je treba take metode nadzora, ki ne zahtevajo veliko časa, a so kljub temu proaktivne in učinkovite, zagotoviti je treba učinkovit pretok informacij med vsemi pomembnejšimi organizacijskimi enotami, pomembna je izbira sodelavcev, ki so za delo kompetentni, usposobljeni in motivirani.

Ob analizi raznih ocen ocenjevanja tveganj se pojavlja vprašanje verodostojnosti (veljavnosti merjenja) posameznih ocen oziroma se lahko pojavljajo določene kontradikcije med posameznimi ocenami tveganja. Pri tem je poseben problem zaznavanje ogroženosti ocenjevalcev tveganja. Menimo, da je to opazno zlasti v delu, ki se nanaša na verjetnost in posledice napak zaposlenih, kriminalitete in višje sile.

Pri upravljanju KI se vse bolj uveljavlja procesni pristop, tako pri oblikovanju politik, strategij, planov in projektov, kot tudi pri upravljanju in obvladovanju tveganj, ki lahko vplivajo na doseganje dobičkonosnih poslovnih rezultatov. Z vidika tveganj so poslovodstva in ostali deležniki KI uspešni v primeru, da so vsa tveganja obvladovana z ustreznimi preventivnimi in kurativnimi ukrepi, vključno z zavarovalnim portfeljem.

Pri izdelavi študije smo upoštevali, da mora biti pristop k ocenjevanju tveganj metodično zasnovan na principih sistemskega inženiringa, vsebinsko na preprečevanju možnih škod in izgub, operativno pa na celovitih ter sodobnih rešitvah upravljanja in obvladovanja tveganj.

Pregled metod in metodologij za ocenjevanje tveganj za delovanje KI je bil opravljen na podlagi poglobljene analize literature. Ugotovljenih je bilo več kot tisoč ustreznih referenc, dosegljivi viri informacij pa so bili pomembni za prepoznavanje različnih metod in metodologij. Primernost obeh smo analizirali in vrednotili na podlagi naslednjih izbranih kriterijev: koncept metodologije (metodologija naj določa najprimernejše načine in postopke za upravljanje in obvladovanje tveganj ter določa najbolj ustrezno uporabo strokovnih orodij), načrtovanje (formalen pristop k načrtovanju metodologij za ocenjevanje tveganj naj bi zmanjšal število napak in težo njihovih posledic), proces (niz dejavnosti, ki z interakcijo dosežejo določen rezultat), postopek (temeljit opis postopka je potreben za ustrezno razumevanje metodologije) in delovanje ter upravljanje sprememb (zaradi hitrosti nastajanja sprememb postaja prihodnost vse bolj nepredvidljiva). Na podlagi zgoraj navedenih izbranih kriterijev smo izbrali kombinacijo metodologije MOSAR (Method organised systematic analysis of risk, metoda za sistematično analizo tveganja) in metodologije FMEA (Failure mode and effect analysis, analiza načina in učinka okvar) kot najprimernejši za ocenjevanje tveganj za delovanje KI. V nadaljevanju sta obe metodologiji predstavljeni.

Metodologija MOSAR je sistemska analiza tveganj in kot najbolj poznana »Analiza drevesa napak«, pa tudi diagram vzrokov in posledic (Ishikawa diagram) oziroma diagram »Ribje kosti«. Metodologija sistematično analizira tveganja v okolju in predstavlja sistematičen pristop k ocenjevanju ter vrednotenju tveganja, določevanju prioritet, obravnavanju tveganj in upravljanju z njimi. Razvita je bila na osnovi metode MADS (Method of Disfunctional Systems), ki vsebuje splošni model za popis nevarnosti in pomeni sistematični pristop k razgrnitvi kompleksnih sistemov in vrednotenju potencialne škode na izpostavljenih subjektih

/ objektih, omogoča modeliranje delovanja (tok nevarnosti) med virom nevarnosti in tarčo (izpostavljenim subjektom / objektom).

Metodologija FMEA se uporablja že več desetletij kot metoda za podporo proizvodnih procesov, storitev in vzdrževanja. Je učinkovita, preventivna, timsko orientirana in sistematična analiza napak sistema. Obsega interdisciplinarne postopke, sistematično in funkcijsko obravnavanje, preprečevanje napak, kreativno razmišljanje in kritično ocenjevanje. FMEA je pogosto prvi korak v študiji zanesljivosti sistema. To vključuje pregled komponent, sklopov in podsistemov, kjer se lahko pojavijo okvare in analiza njihovih vzrokov ter učinkov. Obstajajo številne različice navedene metode.

Ocenjevanje tveganj na podlagi navedenih metodologij je le eden od možnih segmentov upravljanja in obvladovanja tveganj v KI in je odvisno od specifike delovanja organizacij KI. Upravljanje tveganj temelji na realnih ocenah ogroženosti, ocenah ranljivosti, SWOT analizi, varnostni politiki, politiki upravljanja tveganj, upoštevanju zakonodaje, standardov kakovosti, varnostnih standardov, standardov upravljanja tveganj, izbranih metod ocenjevanja tveganj in dobre prakse. Končni produkti tega pristopa so: katalog tveganj, kot glavni operativni dokument upravljanja tveganj; vzpostavitev procesa ocenjevanja tveganj; vzpostavitev procesa usposabljanja deležnikov KI (zaposlenih in drugih) za ocenjevanje, upravljanje in obvladovanje tveganj.

Predstavljena je potreba po neprekinjenem delovanju KI, ki je še posebej izražena v določenih kriznih situacijah. Zaradi navedenega je nujno, da skozi analizo ocenjevanja ogroženosti delovanja KI pravilno razumemo procese kriznega upravljanja in vodenja ter vlogo ustreznih sistemskih subjektov v tem procesu. Posebna pozornost je namenjena vzpostavitvi celovitega in stalnega procesa usposabljanja za upravljanje tveganj v KI. Ob tem se postavlja vprašanje katerim strukturam udeležencev usposabljanja, ki so deležniki v KI, je treba podati ustrezna znanja, raziskovalna spoznanja, izkušnje in dobro prakso, da bi znali učinkovito obvladovati tveganja v svojih delovnih okoljih.

V zaključku študije je prikazan vzorec metodološkega postopka za ocenjevanje tveganj za delovanje KI, ki temelji na predhodnih ugotovitvah študije in podaja potrebna metodološka in vsebinska izhodišča za konkreten operativen pristop k upravljanju in obvladovanju tveganj. Prikazan je vzorec ocene tveganj za delovanje KI na ravni upravljavca KI (primer ocene tveganj električno razdelilne transformatorske postaje).

Študija poudarja nujnost celovitega pristopa, saj mora imeti vsaka država razvite sistemske mehanizme za zaščito KI. Pri tem gre v bistvu za socio-tehnične sisteme, kar pomeni, da sistemski mehanizmi zaščite KI zajemajo tako človeške kot tehnične vidike. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile fizične sestavine KI varnejše, po drugi strani pa, kako obravnavati zanesljivost zaposlenih na tem področju.

Zaradi navedenega je potrebno več vlagati v stalno izobraževanje in dograjevanje znanj ter veščin. Področje ocenjevanja tveganj bo v prihodnosti eno od tistih področij, ki bo podvrženo potrebi po neprekinjenem usposabljanju ustreznih strokovnjakov, ki bodo v organizacijah KI izvajali te procese.

Na zaključku študije je prikazana uporabljena literatura in viri, opredelitev osnovnih pojmov ter seznam slik in tabel.

SUMMARY

The »Expert bases for risk assessment for the operation of critical infrastructure (hereinafter: CI)« study is intended for the professional public as a basis for providing methodological, content and operational bases of risk management and control. Different approaches of social research and a number of possible methods and methodologies for risk assessment set up a challenging task before the project team to analyze which parts of a number of methods and methodologies could be useful as an example of good practice for assessing risks for the operation of CI in the Republic of Slovenia. The project team focused on the broader aspect of risk assessment. CI, threats, dangers and vulnerabilities, risk assessment, risk management and control and the continuous operation of CI are very extensive and interdependent and content-related areas.

In the introductory part, the methodology of the study is presented. In the course of the study we used various methods of social research. In order to describe the methodological bases of risk assessment in the operation of CI and the presentation of the theoretical starting points, the descriptive method of work was used. The terminology in the field of risk management is very diverse, so we studied it and decided which terms we will use in this study. The purpose of the study is for it to serve as a professional tool for those who will want to learn more about the topic related to risk assessment, management and control. In addition, it contains the thoughts, views, expert assessments and content solutions of the authors of the study. An important limitation is the fact that a thorough understanding of this study requires a certain professional pre-knowledge. The project team carried out a review of the research so far and other literature in the field of the subject matter. Previous research has served as the starting point for the study, through which we presented the basic findings of the topic.

In the presentation of the risk control field, special attention is paid to the legal and other professional bases. The modern management of CI is based on the established international and national standards, resolutions, strategies and programs. In particular, the analysis of standards enabled the study to provide an organizational, methodological and terminological approach.

Organizations of CI are faced with internal and/or external factors, which affects the uncertainty and unpredictability of the situation and the achievement of the goals of the organization's mission. It is important that the organizations of CI try to control risks with a systematic approach that includes identification, analysis, evaluation and implementation of measures, procedures and activities that reduce risks to a still acceptable level. Risk control should be ensured to the extent that risks do not have a significant impact on the core

business processes. Risk assessment, management and control for the operation of CI are complex and demanding continuous tasks at the strategic and operational level of the operations of CI organizations. It is therefore recommended that CI managers acquire the knowledge of business tools and techniques (methods and methodologies) that contribute to a more effective risk control. These are primarily tools such as: e.g. benchmarking (comparison with competitors), business intelligence (acquisition of important business information from the environment and the safeguarding of its own confidential information), the »twenty keys« model (improvement of organization), the BSC system of balanced indicators (improvement of internal accounting, financial and other records from operations), the Kaizen philosophy (continuous improvement) and other business tools. Different authors have also presented various risk typologies depending on the source of the risks (natural, technological), the time dimension (acute, chronic), the way of exposure (air, water, etc.), the type of consequences (injuries, deaths), etc. We have taken into account the good practice of risk characterization, which stipulates that risk assessment should be prepared in a clear, transparent and reasonable way. To the greatest extent, the indicators of transparency, clarity, consistency and reasonableness should be taken into account. One of the key issues of risk assessment is the detection of the uncertainty of possible emergencies or their likelihood. It is a question of probability distribution, since whoever makes a decision under uncertainty can not conclude on the success of their actions in advance (the problem arises because we conclude about the future on the basis of the data and information from the past). Similarly, the decision can not be judged according to the risk prediction profile.

For the basic approach in the study, we reasonably used the general risk assessment model (Vršec, 2010), which illustrates three main risk management sets (risk analysis, risk control and risk equalization with insurance) and the National Infrastructure Protection Plan USA (NIPP, 2013) that supports the risk management framework. The framework enables the integration of strategies, capabilities and management structures for decision-making on risks related to CI. The approach can be used for all threats and dangers, including natural disasters and human-induced hazards. There is also an element of uncertainty, which is the result of subjective threat assessments. The scenarios used with reasonable worst-case scenarios can provide a range of possible results that could arise in the operation of CI organizations. In order to clarify these elements, the following questions should be answered: how can we determine and measure uncertainties, what are the undesirable consequences and what are the assumptions about reality (Renn, 2008). The answers (the conceptualization of uncertainty, the extent of undesirable consequences, the possibility of recognizing reality) can serve as a guide for distinguishing different views on managing and controlling risks.

The study analyzes the most important and widely used models of risk assessment. The above illustration and a detailed understanding of the complexity of individual methods is an important aid in the elaboration of a methodological framework for assessing the risks for the operation of CI. Each CI manager is expected to designate a risk assessment team in the CI area in his sector. The activities in this process are aimed at establishing the organizational structure of the project, where the role holders, their tasks and mutual relationships are precisely defined, which is crucial for the efficient implementation of the project.

The CI manager determines the monitoring of risk assessment and management with internal procedures and the uniform methodology (eg. as a »Risk management policy« - this document sets out the measures, procedures, activities and rules for the establishment and operation of a comprehensive system of risk assessment, management and control based on the definition of the appropriate organizational structure and methodological framework). This involves the mutual cooperation of the expert services of the CI manager (also with the assistance of an external expert), especially in the business, management, legal and security fields. Due to the complexity of security risks, the management of such risks is a necessary component of the security policy and implemented security policies. The structure and content of the risk management policy document must comply with the legal requirements and the requirements of the standards that provide guidelines and instructions on managing and controlling risks. The business success of CI organizations is derived from the main goal that business processes are minimally burdened with potential damage and loss. The prevention of emergencies, and consequently the prevention of damage and loss, is the main motto of the security policy.

Performance indicators for risk assessment, management and control are a successful operation of the CI manager (potential risks and threats are under control and manageable), the ongoing review of the adequacy of the security strategy and its adaptation to the resulting situation. The study is a recommendation for a comprehensive risk identification for the use of the full range of possible emergencies that may occur to the CI manager. An example of good practice is the operational use of the risk catalog (adoption of the euro in the Republic of Slovenia in 2007). The process of risk assessment, management and control is presented, which consists of five interconnected processes: identifying risks, evaluating potential impacts, analyzing possible solutions, adopting a solution and monitoring the risk, supervision and its auditing. The whole process is based on specific business processes, sources and causes of uncertainty and the seriousness of business processes.

The supervision of risk management refers to the understanding of the risks that the CI organization accepts and manages. In particular, the basics for risk control are: attention must be focused on strategic business objectives and critical business processes, most attention should be paid to those business goals, on which the successful management of

financial risks and the trust of the users of services depend, control methods that do not require a lot of time must be implemented, yet they are proactive and effective, it is necessary to ensure an efficient flow of information between all major organizational units, it is important to select staff who are competent, skilled and motivated.

When analyzing various risk assessment estimates, the question of credibility (validity of measurement) of individual assessments arises, or certain contradictions may occur between individual risk assessments. In this regard, the detection of threats to risk assessors is a particular problem. We believe that this is particularly noticeable in the part that refers to the probability and consequences of employees' errors, crime and force majeure.

In the management of CI, the process approach is increasingly being applied, both in the formulation of policies, strategies, plans and projects, as well as in risk management and control that can influence the achievement of profitable business results. From the risk point of view, the management and other CI stakeholders are successful in the event that all risks are controlled through appropriate preventive and curative measures, including an insurance portfolio.

In preparing the study, we took into account that the approach to risk assessment must be methodically based on the principles of system engineering, substantively on preventing potential damage and loss, and operationally on comprehensive and modern risk management and control solutions.

An overview of the methods and methodologies for assessing the risks for the operation of CI was carried out on the basis of in-depth literature analysis. More than a thousand relevant references were identified, and the sources of information available were important for identifying different methods and methodologies. The suitability of both was analyzed and evaluated on the basis of the following selected criteria: the concept of methodology (the methodology should specify the most appropriate ways and procedures for managing and controlling risks and determining the most appropriate use of professional tools), planning (a formal approach to planning risk assessment methodologies should reduce the number of errors and the severity of their consequences), the process (a set of activities that achieve a certain result by interaction), the procedure (a thorough description of the procedure is necessary for an adequate understanding of the methodology) and the operation and management of change (because of the pace of change, the future is becoming increasingly unpredictable). On the basis of the criteria selected above, we selected a combination of the MOSAR (Method organised systematic analysis of risk) methodology and the FMEA (Failure mode and effect analysis) methodology as the most appropriate for assessing the risks to the operation of CI. In the following, both methodologies are presented.

The MOSAR methodology is a systematic risk analysis and the most well-known »Tree Fault Analysis«, as well as the diagram of causes and consequences (Ishikawa diagram) or »Fish Bones« diagram. The methodology systematically analyzes risks in the environment and presents a systematic approach to risk assessment and evaluation, prioritization, risk treatment and management. It was developed on the basis of the MADS (Method of Disfunctional Systems) method, which contains a general model for the hazard analysis and signifies a systematic approach to the dissemination of complex systems and the evaluation of potential damage to exposed entities/facilities, allows the modeling of the operation (hazard stream) between the source of danger and the target (to the exposed entities/facilities).

The FMEA methodology has been used for decades as a method to support production processes, services and maintenance. It is an effective, preventive, team-based and systematic system error analysis. It covers interdisciplinary procedures, systematic and functional treatment, prevention of mistakes, creative thinking and critical assessment. The FMEA is often the first step in a system reliability study. This includes an overview of components, sets and subsystems, where malfunctions and analysis of their causes and effects may occur. There are many versions of the above method.

Risk assessment based on the aforementioned methodologies is only one of the possible segments of risk management and control in CI and depends on the specific nature of the CI operations. Risk management is based on realistic threat assessments, vulnerability assessments, SWOT analysis, security policy, risk management policy, compliance with legislation, quality standards, security standards, risk management standards, selected risk assessment methods and good practice. The ultimate products of this approach are: a risk catalog as the main operational risk management document; establishing a risk assessment process; establishing a training process for stakeholders of CI (employees and others) for risk assessment, management and control.

The need for a continuous operation of CI, which is especially expressed in certain crisis situations, is presented. Because of this, it is essential that through the analysis of the risk assessment of the operation of CI, we correctly understand the processes of crisis management and governance and the role of the relevant system entities in this process. Special attention is paid to the establishment of a comprehensive and continuous process of risk management training in CI. This raises the question of which structures of training participants who are stakeholders in CI need to be given the relevant knowledge, research findings, experience and good practice in order to be able to effectively manage the risks in their work environments.

At the end of the study, a sample of the methodological procedure for assessing the risks for the functioning of CI is presented, which is based on the preliminary findings of the study and provides the necessary methodological and substantive guidelines for a concrete operational approach to risk management and control. A sample of risk assessment for the operation of CI at the level of the CI operator (an example of the risk assessment of an electrical distribution transformer station) is presented.

The study highlights the need for a comprehensive approach, since each country must have developed systemic mechanisms for CI protection. This is in fact a matter of socio-engineering systems, which means that systematic protection mechanisms of CI cover both human and technical aspects. The question arises as to how much effort should be made to make even more technological progress possible so that the physical components of CI are safer and, on the other hand, how to address the reliability of employees in this field. As a result, it is necessary to invest more in continuous education and upgrading knowledge and skills. The area of risk assessment will in the future be one of those areas that will be subject to the need for continuous training of relevant experts who will implement these processes in CI organizations.

At the end of the study, the literature and resources used, the definition of basic concepts, and a list of figures and tables are presented.

1 UVOD

Živimo v družbenem obdobju, v katerem je kritična infrastruktura Republike Slovenije izpostavljena številnim virom ogrožanja in tveganjem. Ti so posledica procesov, ki potekajo v globalni družbi in so odsev njenega političnega, ekonomskega, socialnega, varnostnega in tehnično tehnološkega razvoja. Izzivi okolja so drugačni, kot so bili nekoč, označujejo pa jih predvsem velike spremembe v načinu poslovanja, terorizem, globalizacija, mednarodna soodvisnost in okoljske spremembe. Družbene in varnostne spremembe so hitre, kompleksne, nestabilne in težko predvidljive. Potrjuje se teza, da smo vstopili v občutljivo obdobje tveganj, ki so sama po sebi vključena v koncept razvoja socialne, pravne in gospodarske rasti družbe (Broder, 2006). Tudi »tehnološke spremembe in sistemske nadgradnje vplivajo na razvoj kritičnih infrastruktur, s tem pa tudi na samo ranljivost kritičnih infrastruktur« (Prezelj, 2010).

Globalno varnostno okolje danes postaja kompleksnejše, kot smo mu bili priča kadarkoli do sedaj. Poleg tradicionalnih nacionalnih in mednarodnih akterjev, ki so imeli do nedavnega pomemben vpliv na urejanje geostrateških razmerij v mednarodnem varnostnem okolju, na sceno stopajo tudi nedržavni subjekti. Ti so dobili v obdobju, ko je terorizem, ena od najbolj izpostavljenih varnostnih groženj, poseben pomen in nevarnost za nemoteno delovanje širše družbene skupnosti. V zadnjem obdobju ni samo terorizem največje varnostno tveganje, temveč smo bili priča nizu kompleksnih varnostnih groženj, kot so neprestani migracijski pritiski na zunanje meje EU in s tem tudi sprejetje bolj restriktivnih mejnih ukrepov na schengenski meji, kibernetska tveganja in obsežni hekerski napadi, niz tveganj, katerim so bile izpostavljene gospodarske organizacije, pa vse do geopolitičnih premikov, ki smo jim priča skoraj vsak dan in nas stalno navdajajo z neprestano dinamiko spreminjanja stabilnega varnostnega okolja, kakršnega smo bili vajeni v preteklosti. Vse to pred strokovno javnost postavlja izzive iskanja ustreznih odgovorov na spremenjene varnostne trende (Čaleta, 2011).

Vse bolj je jasno in prepoznano, da je KI ranljiva in pod udarom vse večje ogroženosti zaradi naravnih, kriminalnih in terorističnih ter drugih vrst ogroženosti. To bi moralo državo, nosilce sektorjev KI, lastnike in upravljavce KI vzpodbuditi, da se bolj kot doslej posvetijo vzpostavljanju učinkovitejših varnostnih mehanizmov v gospodarskih družbah, zavodih, državnih organih in Banki Slovenije, ki upravljajo KI tako z vidika regulative, varnostne politike, upravljanja tveganj in zagotavljanja boljših materialnih ter kadrovskih pogojev delovanja. Vsak upravljavec KI bi moral imeti vsaj enega varnostnega managerja, ki bi na strateški ravni upravljanja znal in zmogel vzpostaviti sistem in proces upravljanja varnosti, v okviru tega pa tudi proces upravljanja tveganj (Vršec, 2014).

1.1. METODOLOGIJA IZDELAVE ŠTUDIJE

Pri izdelavi študije in doseganju zastavljenega cilja smo uporabili različne metode družboslovnega raziskovanja.

Za opis metodoloških izhodišč ocenjevanja tveganj pri delovanju KI ter navajanje teoretičnih izhodišč smo uporabili opisno metodo dela. Z metodo analize primarnih virov (zakoni, podzakonski akti ter drugi pravni viri) in z metodo analize sekundarnih virov (članki, knjige, prispevki, raziskave, metodologije itd.) bodo opredeljena in predstavljena temeljna spoznanja obravnavane tematike. Metodo analize smo uporabili tudi v primeru preverjanja dosedanjih metodoloških pristopov, ki jih organizacije uporabljajo za ocenjevanje tveganj za delovanje KI. S podporo Ministrstva za obrambo smo od osemnjastih upravljavcev KI prejeli podatke o vrsti metodologije za ocenjevanje tveganj, ki jo upravljavci uporabljajo. Na takšen način smo z metodo analize analizirali trenutno stanje, kar je bila tudi ena izmed podlag za nadaljevanje raziskovanja in iskanja smeri, kateri enotni metodološki pristopi bi bili v prihodnje strokovno najbolj ustrezni za ocenjevanje tveganj za delovanje KI. Z metodo zbiranja virov smo zbrali relevantne vire z obravnavanega področja. Z induktivnim in deduktivnim pristopom smo v nadaljevanju obdelali teoretične pojme in tako združili izhodišča obravnavane tematike.

Z razlagalno metodo smo v zaključku razložili neposredne korake uporabe predlaganih metodoloških izhodišč na področju KI.

S pomočjo študije primera in primerjalne metode smo podrobneje prikazali neposredna metodološka izhodišča na izbranem vzorčnem primeru.

Skozi celotno študijo, predvsem pa v zaključku, je do izraza prišla normativna metoda, s pomočjo katere smo podali nastavke za pravno ureditev omenjenega področja v Republiki Sloveniji.

Pri uveljavitvi in preverjanju dognanj, ki jih prinaša študija, bo skozi različne razgovore potekalo tudi preverjanje razumevanja in ustreznosti predlaganih rešitev, kjer bo posebna pozornost namenjena Inšpektoratu za obrambo in Upravi Republike Slovenije za zaščito in reševanje. V okviru preverjanja razumevanja vsebine bo s ciljno izbranimi upravljavci KI, ki delujejo znotraj Slovenskega združenja korporativne varnosti, izvedena delavnica, katere glavni namen bo preverjanje razumevanja predlaganih rešitev in analiziranje določenih posebnosti, ki jih prinašajo posamezni podsektorji KI. S kontrolno skupino (strokovnjaki za tveganja v organizaciji KI) bo preverjena razumljivost in operativnost uporabe predlagane metodologije za ocenjevanje tveganj.

1.2 IZRAZOSLOVJE

Izrazoslovje s področja obravnavanja tveganj je zelo raznoliko, zato ga je treba proučiti in se odločiti, katere izraze bomo uporabili v tej študiji. Najprej je treba preučiti znane in najpogosteje uporabljene izraze, ki neposredno obravnavajo tveganja. To so: upravljanje tveganj, obvladovanje tveganj in ocenjevanje tveganj. Ocenjevanje tveganj je samo del procesa upravljanja tveganj in preozek pojem za celovito obravnavo tveganj za delovanje KI. Zato so v tej študiji uporabljeni vsi trije izrazi, glede na širino in raven obravnave tveganj. Upravljanje tveganj razumemo bolj kot obravnavo tveganj na strateški ravni, torej na ravni nosilcev sektorjev KI, obvladovanje in ocenjevanje tveganj pa bolj na ravni upravljavcev KI. Ob tem razumevanju obravnave tveganj je v ospredju uporaba izraza upravljanje tveganj.

Drugi vidik obravnave tveganj je poimenovanje dogodkov, pojavov, okoliščin in kriznih stanj, ki negativno vplivajo na poslovanje, procese, strategije in človeške vire. Za to, kar negativno vpliva na omenjene segmente poslovanja je kar precej izrazov, kot denimo: tvegan dogodek, škodni dogodek, izredni dogodek, kritični dogodek, škodni pojav, incident, nenormalna situacija, motnja, odpoved, okvara, napaka, izpad, razpad, napad, nesreča, nezgoda ipd. Vse to so dogodki, ki sprožajo nevarnost, ogrožanje, grožnje in tveganja. Glede na to, da je v Zakonu o kritični infrastrukturi (v nadaljevanju: ZKI), v nekaterih standardih in v drugih dokumentih uporabljan izraz izredni dogodek, je ta izraz uporabljen tudi v tej študiji.

Pri upravljanju s tveganji pa zasledimo še nekaj izrazov, kot so: varnostni izzivi (ang. security challenges), varnostne grožnje (ang. security threats), negotovost (ang. uncertainty), izpostavljenost (ang. exposed), nevarnost (ang. danger), proučevanje oziroma analiziranje tveganj (ang. risk analysis), prepoznavanje tveganj (ang. risk identification), obveščanje o tveganjih (ang. risk communication), izogibanje (ang. avoidance) tveganjem, zadržanje (ang. retention) tveganj, zmanjševanje (ang. reduction) tveganj in zavarovanje tveganj (ang. risk insurance). Vse skupaj lahko poimenujemo celovito (korporativno) upravljanje tveganj, ki ga na kratko lahko označimo z izrazom (ang.) »total risk management« oziroma (ang.) »corporate risk management«. Za različna področja dejavnosti obstajajo tudi različne metodologije, ki se medsebojno dopolnjujejo in predstavljajo nabor ali paleto metodologij kot poslovnih orodij za upravljanje tveganj.

Iz zgoraj opisanega izhaja, da morajo biti v študiji uporabljeni že uveljavljeni izrazi in izbrane tiste metode upravljanja tveganj, ki imajo uporabno vrednost v procesu ocenjevanja tveganj za delovanje KI. Kot primeri dobre prakse je navedeni pristop v določenih organizacijah KI že uveljavljen.

1.3 OMEJITVE PRI IZDELAVI ŠTUDIJE

Študija je prvenstveno namenjena nosilcem in upravljavcem KI ter strokovni javnosti, kot temelj za zagotavljanje metodoloških in vsebinskih izhodišč upravljanja tveganj v organizacijah, ki upravljajo KI. Veliko število različnih pristopov in metodologij za ocenjevanje tveganj je pred izdelovalce študije postavilo zahtevno nalogo analize in ugotavljanja, kateri deli posameznih metodologij bi bili lahko uporabni in ustrezni za ocenjevanje tveganj za delovanje KI v Republiki Sloveniji. Namen študije je, da bo le ta služila kot osnovno orodje tistim, ki bodo želeli bolj poglobljeno spoznati tematiko, povezano z upravljanjem, obvladovanjem in ocenjevanjem tveganj. Poleg tega so v njej podana lastna razmišljanja, pogledi, ocene in rešitve avtorjev študije, ki se morebiti v prihodnosti uresničijo v zakonodaji ter v poslovni, organizacijski in varnostni praksi.

Izdelava študije je prinesla nekatere omejitve. Prvo je obširnost in kompleksnost tematike. KI, grožnje, ocenjevanje tveganj, obvladovanje tveganj in neprekinjeno delovanje so vsa zelo obsežna področja, zato je bilo še toliko pomembnejše izluščiti in se fokusirati le na tiste dele, ki so relevantni za našo študijo. Potrebno je bilo pregledati veliko bibliografije in iz nje izluščiti tiste dele, ki so nam pomagali odgovoriti na zastavljena raziskovalna vprašanja. Izpostavimo lahko tudi maloštevilne avtorje (Prezelj, Čaleta ter Vršec in Vršec, Gorišek), ki se v slovenskem prostoru ukvarjajo z obravnavano tematiko, kar prispeva k izvirnosti in aktualnosti študije. Naslednji problem pri izdelavi študije je nedostopnost nekaterih dokumentov, bodisi zaradi stopnje tajnosti, ključnih informacij poslovnih organizacij ali drugih razlogov. V študiji nismo želeli posegati po informacijah ali dokumentih, ki vsebujejo stopnje tajnosti, saj je študija namenjena širšemu krogu uporabnikov in smo jo želeli pripraviti s popolnoma javnimi informacijami. Pri izdelavi omenjene študije smo se srečali tudi z drugimi omejitvami, kot so omejen čas in nenazadnje finančni in drugi viri, namenjeni za izdelavo študije.

Strokovno gledano pa pomembno omejitev predstavlja dejstvo, da je za temeljito razumevanje omenjene študije potrebno določeno predznanje. Vsaka implementacija predlaganih rešitev in metodologije pa bo botrovala k ustrezni in kontinuirani izvedbi usposabljanja določenih struktur v organizacijah KI.

1.4 PREDSTAVITEV DOSEDANJIH RAZISKAV NA PODROČJU KRITIČNE INFRASTRUKTURE

Pred začetkom izdelave študije smo izvedli pregled dosedanjih raziskav in druge literature s področja obravnavane tematike. Dosedanje raziskave so služile kot izhodišče študiji, s pomočjo katerih smo opredelili in predstavili temeljna spoznanja obravnavane tematike. V nadaljevanju navajamo nekaj avtorjev in njihovih del, ki zadevajo tematiko naše raziskave.

S področjem KI so se ukvarjali številni tuji avtorji. Izpostavili bi Lewisa in njegovo delo Critical Infrastructure Protection in Homeland Security (2006), Michel-Kerjana, ki je samostojno ali v soavtorstvu izdal številna dela s področja KI, npr. New Challenges in Critical Infrastructures: A US Perspective (2003), Where public Efficiency Meets Public Vulneravility – The Critical Infrastructure Challenge ipd. in Dunnovo, ki KI obravnava v delu The socio-political dimensions of critical information infrastructure protection (2005) ter skupaj z Abele-Wigert v delu International CIIP Handbook 2006. Zelo poglobljeno pa se z omenjeno tematiko v zadnjem obdobju ukvarjajo v ZDA in sicer v okviru US Department of Homland Security ter Federal Emergency Management Agency (FEMA), kjer je področju metodoloških pristopov in standardizaciji s tega področja namenjena izredno velika znanstvena in strokovna pozornost.

Slovenske literature s področja zaščite KI je relativno malo. Izpostavimo lahko Prezlja in knjigo z naslovom Kritična infrastruktura v Sloveniji (2010), ki je povzetek raziskave iz leta 2008, Definicija in zaščita kritične infrastrukture Republike Slovenije (2008). Raziskava je potekala v okviru Fakultete za družbene vede, financirana pa je bila s strani Ministrstva za obrambo Republike Slovenije.

Poleg te je še nekaj drugih raziskav in projektov, ki se nanašajo na upravljanje tveganj za delovanje KI v slovenskem prostoru.

Projekt »Interaktivno ocenjevanje tveganj na področju KI, z uporabo integriranega geografskega informacijskega sistema – RISKGIS-Končno poročilo (ang. INTERACTIVE RISK ASSESSMENT IN THE FIELD OF CRITICAL INFRASTRUCTURE BASED ON INTEGRATED GEOGRAPHIC INFORMATION SYSTEM-RISKGIS), ki so ga leta 2013 izvedli Ljubljanski urbanistični zavod, d.d., Fakulteta za logistiko, Celje in Evro-Atlantski svet Slovenije, Ljubljana, je prinesel:

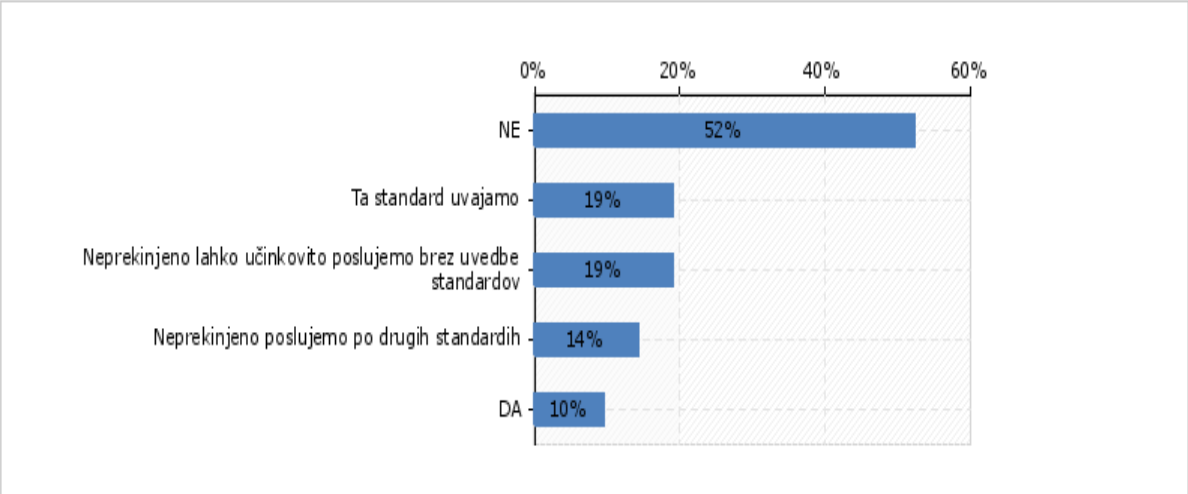
- računalniški program za ocenjevanje tveganj v zvezi z objekti v KI,
- identifikacija ranljivih križišč in zgoščenosti pomembnejše infrastrukture na območju Republike Slovenije,
- simulacija soodvisnosti sektorjev KI.

Omenjeni projekt je koristen pripomoček v procesu nastajanja metodologije upravljanja

tveganj za delovanje KI, zlasti v sektorjih kot so energetika, transport in informacijsko telekomunikacijski sistemi. V tem projektu je eksplicitno poudarjeno, da je soodvisnost med sektorji postala eden od ključnih parametrov ocenjevanja tveganj za delovanje KI.

Zagotavljanje neprekinjenega delovanja KI je pogoj za normalno delovanje države, gospodarstva, civilne družbe in prebivalstva, kar je bil predmet raziskave z naslovom ANALIZA NEPREKINJENEGA POSLOVANJA SISTEMA ZAŠČITE KRITIČNE INFRASTRUKTURE V REPUBLIKI SLOVENIJI, ki so jo izdelali Gea College, Fakulteta za podjetništvo in Inštitut za korporativne varnostne študije. Zagotavljanje neprekinjenega poslovanja oz. delovanja KI ureja ZKI v naslednjih členih: 3. člen 15. točka, 10. člen 3. točka, 16. člen 2. točka, 19. člen 1. točka in 24. člen 1. točka.

Osnovno raziskovalno vprašanje raziskave se je nanašalo na vzpostavljanje neprekinjenega poslovanja v skladu s standardom ISO 22301 (prej BS 23999). Rezultati niso vzpodbudni, kajti iz spodnje slike 1 razberemo, da je pravo profesionalno vzpostavljanje neprekinjenega poslovanja KI šele v začetni fazi razvoja



Slika 1: Analiza raziskovalnega vprašanja »Imate uveden sistem neprekinjenega poslovanja po standardu ISO 22301/2012/2014?«

Ti rezultati opozarjajo tudi na to, da je pri delovanju KI vprašljiva kakovost upravljanja tveganj; kajti razpoznavanje, ocenjevanje in vrednotenje tveganj je eno od osrednjih aktivnosti pri izdelavi in izvajanju načrta neprekinjenega poslovanja oz. delovanja. Izdelava in izvajanje načrta neprekinjenega poslovanja in delovanja namreč odgovorne »prisili«, da se temeljito lotijo tudi upravljanja, obvladovanja in ocenjevanja tveganj.

Nekaj relevantnih ugotovitev je možno izluščiti tudi iz varnostnih projektov s področja KI, ki jih je v preteklih letih izvedel Inštitut za korporativne varnostne študije. Sinteza raziskovalnih rezultatov v teh projektih nam pove, da je ocenjevanje ranljivosti, ogroženosti in (zlasti)

varnostnih tveganj izredno šibko. Zato nastopajo težave pri oblikovanju in sprejemanju varnostih politik, politik upravljajnja tveganj in izdelovanja raznih varnostnih načrtov. Nekaj pozitivnih premikov se kaže na področjih požarne varnosti, zaščite in reševanja (civilne zaščite), varstva okolja, varnosti in zdravja pri delu ter informacijske varnosti, predvsem zato, ker tako terja zakonodaja ne pa ocene ranljivosti, ogroženosti in tveganj.

Z vidika upravljanja tveganj v sektorju energetike je zanimiva publikacija z naslovom Elektroenergetska infrastruktura v Sloveniji: Scenariji izpadov električne energije in pomen kritične redundance, ki jo je izdala Fakultete za družbene vede leta 2017. Upravljanje tveganj, obvladovanje scenarijev in kriznih stanj v elektrogospodarstvu je izrednega pomena za nemoteno in neprekinjeno delovanje vseh drugih sektorjev KI.

Na to temo je Inštitut za korporativne varnostne študije iz Ljubljane, tudi s Slovenskim združenjem za korporativno varnost ter drugimi organizacijami pripravil številne konference in posvete, kjer je bila vsebina razprav povezana s procesi zaščite KI.

Posebej velja v tem okviru pregledati tudi mednarodne projekte, ki so povezani s področjem KI:

- Organization and coordinating NATO Advanced Research Workshop on Managing Terrorism Threats to Critical Infrastructure - Challenges for South Eastern Europe,
- Project coordination “Counter Terrorism challenges in SE Europe” in the framework of »Counter terrorism Fellowship program« cooperation with Embassy of the USA in Ljubljana, Ministry of Defense Republic of Slovenia, Center for Civil Military Cooperation, Monterey USA and ICS-Ljubljana in years 2008, 2009, 2010, 2011, 2013, 2014, 2016, 2018,
- Project »Resilience of Critical Infrastructure Protection in Europe (RECIPE) 2016« - EU »Humanitarian Aid and Civil Protection ECHO/SUB/2014/696006, Feasibility Studies for Croatia, Serbia and Sweden,
- ERASMUS project n. 3413, Safety and diversity in Europe - efficient training modules for prevention of extremism by trainees and staff of private security services in Europe,
- DEFENDER Defending the European Energy Infrastructures (Critical Infrastructure Protection: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe) - Project: H2020–CIP-01-2016–740898,
- ICS is an authorize Contractor for EU Agency for Cooperation of Energy Regulators (ACER) in the area of Physical Security for 2018-2021.

Navedeni projekti se neposredno ne ukvarjajo z ocenjevanjem tveganj v KI, so pa splošna informacija o novih varnostnih izzivih, novih varnostnih tveganjih in potrebnih varnostnih

ukrepih, ki se nanašajo na KI. Aktivni udeleženec teh projektov je tudi Inštitut za korporativne varnostne študije, ki v našo in tujo raziskovalno in izobraževalno sfero vnaša ideje in spoznanja o ocenjevanju tveganj v KI. Na ta način se odpirajo tudi možnosti spoznavanja morebitne dobre prakse na področju ocenjevasnja tveganj – ali širše – na področju upravljanja in obvladovanja tveganj za delovanje KI sosednjih in drugih držav. V tem kontekstu lahko predvidimo, da bo pričujoča študija prispevala k ustvarjanju dobre prakse glede upravljajnja, obvladovanja in ocenjevanja tveganj za delovanje slovenske KI.

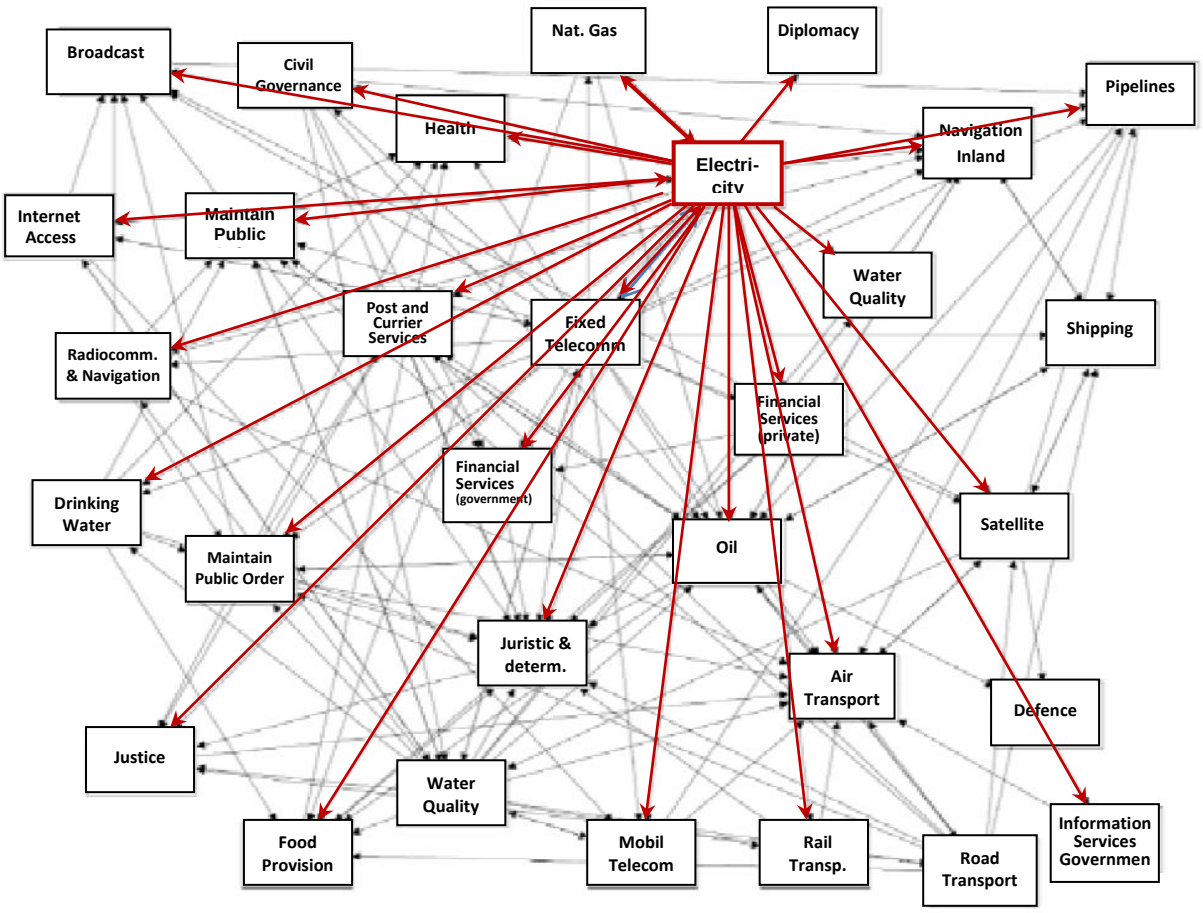
2 PREDSTAVITEV PODROČJA UPRAVLJANJA TVEGANJ (ANG. RISK MANAGEMENT) KOT SPLOŠNEGA TEORETIČNEGA OKVIRJA ZA OCENJEVANJE TVEGANJ

KI je nujna za zagotavljanje nemotenega delovanja širše družbene skupnosti, to je države, gospodarstva, civilne družbe in prebivalstva. Poleg terorističnega ogrožanja, kibernetskih, kriminalnih in drugih tveganj za delovanje KI predstavljajo pomembno tveganje tudi naravne nesreče, katerim se nismo izognili niti v Sloveniji. Spomnimo se žleda in poplav, ki sta nas opomnila kako pomebna je KI za normalno delovanje družbe. Država ima nalogo, da uredi ustrezno normativno podlago s katero opredeli kateri deli nacionalne infrastrukture sodijo v kritični del. Del te infrastrukture ima lahko zaradi soodvisnosti in vpetosti tudi učinke na sosednje države. Pomembno je še poudariti, da določene države KI razdelijo v posamezne sektorje in nato še podsektorje, ki so procesno, vsebinsko in tehnološko zaključene celote. V tem okviru je potrebno posebej izpostaviti podsektorja proizvodnje in prenosa električne energije in komunikacijsko-informacijske tehnologije. Si danes sploh lahko zamišljamo normalno funkcioniranje družbe brez električne energije in delovanja informacijske tehnologije? Iz primera nesreče z žledom, kjer sta bila zelo onemogočena ravno ta dva sektorja in je bil pomemben del države brez električne energije, posledično pa tudi brez ustrezno delujoče informacijske in komunikacijske tehnologije, lahko hitro ugotovimo, da je takšno tveganje zelo resno (Čaleta, 2016).

Za pravilno razumevanje problema upravljanja tveganj pa je potrebno upoštevati še javno zasebno-partnerstvo, ki je v primeru delovanja KI eden od dejavnikov delovanja KI[1]. Privatizacijski procesi in prehajanje lastnine v zasebno poslovno upravljanje je pomembno povečalo del zasebnih lastnikov, ki upravljajo s KI. Obema partnerjema v tem procesu mora biti v interesu neprekinjeno delovanje KI. Državi zaradi neprekinjenosti delovanja in zagotavljanja nemotenega delovanja družbe, zasebnemu lastniku pa ta neprekinjenost in varnost delovanja prinaša ustrezen dobiček in zagotavljanje osnovnega poslovnega

[1] V mednarodnem okolju je pomemben odstotek kritične infrastrukture v upravljanju zasebnih lastnikov. Počasi se ta proces krepi tudi v Republki Sloveniji.

poslanstva organizacije. V tej interakciji je še vrsta dejavnikov, ki so, s stališča države, zelo pomembni in imajo lahko v posameznih primerih resen vpliv na zagotavljanje nacionalne varnosti. Lastništvo v organizacijah, ki upravlja s KI, bi moralo s tega vidika zanimati državo, predvsem s stališča nacionalne varnosti in zagotavljanja neprekinjenosti delovanja ključnih procesov. V tem okviru je informacijsko komunikacijska tehnologija posebej izpostavljen podsektor KI (Čaleta, 2016).



Slika 2: Soodvisnost kritične infrastrukture[2]

Tveganje je neizogibna sestavina hiperpovezanega sveta. Živimo v verjetnostno - deterministčnem svetu in tveganje je posledica in razsežnost okoljskih aktivnosti ter aktivnosti posameznika. Ne moremo izbirati med tveganjem in netveganjem, ampak med različnimi stopnjami in vrstami tveganja. Tudi opustitev aktivnosti je tveganje. Tveganja obstajajo že dolgo, niso nič novega v družbeni praksi, so pa zaradi globalnih razmer v zadnjem obdobju vse bolj kompleksna, razčlenjena, kvantificirano ovrednotena in podprta z raznimi modeli ter analitičnimi orodji.

[2] Luiijf, H.A.M., Burger H.H., and Klaver, M.H.A. (2008), Critical (Information) Infrastructure Protection in the Netherlands, working paper, available at http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.

Predvidevanje tveganj žal ne more biti vselej popolnoma pravilno, še posebej v nestabilnem okolju. Zaradi različnega vrednotenja posameznih interesov družbe, organizacij in posameznikov je prihodnja tveganja zelo težko predvidevati[3]. Pojavlja se tudi nesposobnost za dojemanje tveganj onkraj našega intelektualnega in zaznavnega horizonta, česar pa ne zanika obstoja tveganj. Tveganje pomeni dejstvo, da so posamezniki, procesi in sistemi znotraj organizacije lahko nepopolni in da napake pri izvajanju teh procesov in funkcij lahko povzročijo izgubo (Basel II, 2006). Tveganje se hkrati nanaša tudi na dejavnike zunaj KI, ki lahko negativno vplivajo na izvajanje notranjih (poslovnih) procesov.

Tveganje pomeni verjetnost, da se bo zaradi kakšnih zunanjih ali notranjih dejavnikov zgodila določena škoda oziroma kakršen koli drug negativen izid, izhaja pa iz nestabilnosti in negotovosti bodočih dogodkov. Tveganje je pravzaprav možnost, da izid (prihodnost) ne bo takšen, kot je bil predviden. Če je škodo ali negativen izid možno predvideti, se potem ta lahko nevtralizira s preventivnim dejanjem.

Da lahko govorimo o tveganju, morata biti prisotna vsaj dva dejavnika: (i) negotovost in (ii) izpostavljenost. Če kateri od navedenih dejavnikov ni prisoten, potem ne moremo govoriti o tveganju. Lahko smo negotovi glede prihodnjih dogodkov, toda, če nismo izpostavljeni, potemtakem tveganja preprosto ni. Ali obratno. Če smo izpostavljeni in z gotovostjo vemo kaj se bo zgodilo, težko rečemo, da za nas obstaja tveganje. Tveganje je prisotno le, ko sta združena negotovost in izpostavljenost. Tveganje je vse kar lahko prepreči doseganje določenih ciljev in ustvari izid, ki ni bil predviden.

Koncept tveganja se ukvarja z naslednjimi vprašanji: (i) kaj se lahko zgodi? (ii) kakšna je verjetnost, da se bo to zgodilo? (iii) kakšne so lahko posledice, če se bo to zgodilo? in (iv) kako se izogniti posledicam oziroma jih zmanjšati?

Analiziranje in ukrepanje na podlagi zgornjih vprašanj imenujemo upravljanje s tveganji. Ta postajajo vedno bolj celovita in zahtevnejša aktivnost za zaščito KI pred izrednimi dogodki zaradi namerne ali/in nenamerne povzročitve. Uspešno upravljanje tveganj izhaja iz premišljenega predvidevanja verjetnosti nastanka izrednega dogodka in obvladovanja morebitnih odstopanj od predvidenega. Neustrezno upravljanje tveganj lahko negativno vpliva na uporabnike storitev KI (javno mnenje), lastnike in upravljavce KI.

Tveganje ni le posledica porazdelitve izrednih dogodkov v prihodnosti, temveč je tudi posledica nepopolnih ali nekakovostnih informacij, ki jih vodstvo upravljavca KI uporablja za sprejemanje poslovnih odločitev. S tega zornega kota je ključno vprašanje ali imajo upravljavci KI na razpolago informacije (ugotovitve) iz ocen ranljivosti in ogroženosti in iz

[3] Ameriški general Collin L. Powell je dejal: »Konec je razkošja, ko smo vedeli, na katero grožnjo naj se pripravljamo« (Holmes, 1994).

SWOT analize. Kajti predvsem tovrstne informacije so realna podlaga za odločanje o načrtovanju ukrepov za zaščito premoženja, človeških virov in vrednot v posameznih sektorjih KI**.**

V preteklem obdobju se je v družboslovni teoriji pojavila paradigma »družbe tveganja« (Beck, 1993). Tudi v slovenskem prostoru je bila določena pozornost namenjena proučevanju tveganja, in sicer je na vrednostne dimenzije opozoril Kirn (1995), na nekatere povezave tveganja z varnostjo Mitar (1995), na varnost kot dobrino Bučar (1997), na varnostni inženiring Golob (2013), na ranljivost KI Prezelj (2010) ter na korporativno varnost Vršec in Čaleta (2016, 2017).

Pri proučevanju tveganja je bilo veliko pozornosti namenjeno zbiranju podatkov o vrstah in vzrokih poškodb in smrti, vendar pa kvantitativne analize ne omogočajo potrebnih ekstrapolacij, kajti današnje življenje se sooča s kvalitativnimi spremembami. Zato so različni avtorji oblikovali različne hipotetično - deduktivne modele, deskriptivne in normativne teorije, tako v okviru naravoslovnih kakor tudi v okviru družbenih znanosti. Ugotovljene so bile nekatere kvantitativne zakonitosti, izdelane opisne tipologije, izoblikovani sistemski, vzročni, analoški in procesni modeli ter podane funkcionalistične in kognitivne obrazložitve. V družbenih vedah sta izraziti zlasti dve paradigmi. Prva je paradigma tveganja, ki poudarja primarnost posameznika (psihometrična teorija), druga pa je kulturna teorija tveganja, ki poudarja primarnost skupin (Krimsky, 1992:4).

Starr (1969, po Mitar, 1995) je predstavil tri zakonitosti v zvezi s sprejemljivostjo tveganja: (i) pripravljenost javnosti sprejeti prostovoljna tveganja je tisočkrat večja, kakor pa sprejeti neprostovoljna tveganja; (ii) sprejemljivost tveganja je v razmerju s tretjo potenco koristi; (iii) sprejemljivi nivo tveganja je v obratnem sorazmerju s številom tveganju izpostavljenih posameznikov.

Starrove ugotovitve drugi raziskovalci niso v celoti potrdili, ugotovili pa so, da posamezniki sprejemajo visoka tveganja v primeru pričakovanih velikih koristi oziroma dobičkov. Pozneje so Starr, Rudman in Whipple (1976, po Mitar, 1995) opredelili dva dodatna kvantitativna zakona tveganja: (i) nanašal se je na razmerje med pogostostjo in težo tveganj; (ii) družbena prožnost v razmerju do nesreč. V prvem zakonu so avtorji poudarili, da verjetnost pogostosti dogodka eksponentno upada s težo dogodka. S to ugotovitvijo je povezano še spoznanje, da so za posameznika bolj nesprejemljivi dogodki, ki so v času in prostoru koncentrirani (npr. letalska nesreča, porušitev stavbe ipd.), kakor pa dogodki, ki so v času in prostoru enakomerneje porazdeljeni (npr. prometne nesreče), čeprav je lahko celotno število žrtev večje. V drugem zakonu so opredelili funkcionalno zvezo med družbeno sposobnostjo soočanja z nesrečami in značilnostmi družbe. Avtorji so poudarili neposredno zvezo med družbeno prožnostjo, številom posameznikov in njihovo povprečno življenjsko dobo ter

obratno sorazmerno zvezo z doseženo stopnjo tehnologije, povprečnim časom odprave škode, časom za odkritje vzrokov škode, časom za odpravo napak, povprečno poškodovanostjo prizadetih posameznikov in obsegom prizadetih z dogodkom. Avtorji so poudarili, da so tehnološko razvitejše družbe manj prožne, kajti odpoved enega od kritičnih podsistemov lahko povzroči zlom celotnega sistema. Čeprav je njihova hipoteza zanimiva, pa je sporno funkcionalno razmerje (Krimsky, 1992: 9), kajti sodobne tehnološke družbe niso nujno bolj ranljive kot primitivne. Upoštevati je treba spoznanje, da lahko interakcija naravnih, tehnoloških in družbenih dejavnikov različno vpliva na prožnost družbe. Prožnost sistema je pogojena z naravo povezav med podsistemi in procesi ter z naravo zunanjega ogrožanja. Starr in sodelavci so ugotovili, da je zgornja meja pripravljenosti sprejeti neprostovoljna tveganja v razmerju ena proti sto v primeru različnih bolezni in smrti, spodnja meja v primeru naravnih nesreč pa je ena proti milijon. Njihove opredelitve niso dodatno preverjene.

Na podlagi politike in procesa upravljanja tveganj za delovanje KI bi morali nosilci in upravljavci sektorjev KI stremeti za tem, da preprečujejo izredne dogodke (nesreče, nezgode, napake, okvare, motnje, napade, vdore), kar posledično pomeni preprečevanje škod in izgub (angl: Loss Prevention). Kajti »poslovno in finančno zdravje gospodarske družbe, ki upravlja s KI, izhaja tudi iz tega, da v poslovnih procesih ne prihaja do škod in izgub«. Tu nastopi razvojna strategija, varnostna politika in politika upravljanja tveganj na vseh nivojih implementiranja. Preprečevanje izrednih dogodkov, škod in izgub je potemtakem z ekonomskega, poslovnega, varnostnega in etičnega vidika glavna skrb nosilcev sektorjev in upravljavcev KI (Vršec in Vršec, 2015). Primarni cilj zaščite KI je preprečiti nastanek motenj ali jih odpraviti, ko se pojavijo. Radvanovski (2006:6) sicer ugotavlja, da je koncept zaščite KI predvsem reaktivnega značaja in ne toliko preventivnega, vendar pa avtor opredeljuje tudi pripravljenost na področju KI (ang: Critical infrastructure preparedness) kot proaktivne ukrepe v smeri zmanjševanja groženj, tveganj in ranljivosti KI. Pripravljenost vključuje ocenjevanje ranljivosti, načrte, procedure, politiko, usposabljanja in potrebno opremo (Prezelj, 2010).

V KI je izredno pomembno zagotavljanje neprekinjenosti delovanja in poslovanja gospodarskih družb, ki upravljajo s KI. Kajti neprekinjenost delovanja KI, ki je v veliki meri odvisna tudi od tega, kako uspešno so obvladovana tveganja, zagotavlja primerno raven (poslovne) odpornosti tudi v kriznih okoliščinah. Pri tem igrajo strateško vlogo kritični (poslovni) procesi, ki morajo delovati tudi ob nastanku krize. »Izhajajoč iz napisanega poslovna odpornost pomeni integrirano in nenehno upravljanje pripravljenosti posamezne gospodarske družbe, ki jo doseže s primerno izbiro metodologije upravljanja tveganj, upoštevajoč pravno-formalne predpise, standarde, metode in načrte, kot je načrt neprekinjenega poslovanja (Marinčič in Vršec, 2017).

Pri zagotavljanju neprekinjenega delovanja KI je treba izpostaviti: ranljivost in ogroženost posameznih sektorjev KI, učinkovitost upravljanja tveganj, ukrepe za zaščito KI, (poslovno) odpornost gospodarskih družb, ki upravljajo KI in obvladovanje kriznega vodenja.

Ob tem ne smemo pozabiti odgovornosti vodilnih struktur nosilcev in upravljavcev KI ter drugih deležnikov, ki bodo sodelovali v implementaciji ZKI (Uradni list RS, št. 75/2017) ter drugih podlag in pri uvajanju obveznih ter priporočljivih standardov in orodij upravljanja, obvladovanja in ocenjevanja tveganj.

V nadaljevanju podajamo nekaj ključnih izhodišč za upravljanje, obvladovanje in ocenjevanje tveganj za delovanje KI, ki obsegajo pravne in druge srokovne podlage, nacionalne resolucije, strategije in programe, standarde kakovosti, varnostne standarde in standarde upravljanja tveganj, ter nekatera poslovna orodja za izboljšanje poslovanja kot so benchmarking, business intelligence, sistem uravnoteženih kazalnikov BSC, sistem 20 ključev in izboljšave Kaizen. S temi izhodišči želimo povedati, da je za ocenjevanje tveganj v KI treba poznati širok nabor pravnih, strokovnih in prakseoloških podlag.

2.1 PRAVNA IN DRUGA STROKOVNA PODLAGA

Posamezni sektorji KI morajo delovati, poslovati in se razvijati, pa tudi upravljati s tveganji, v skladu z zakonodajo, ki ureja posamezna področja. Ta področja so: varstvo pred naravnimi in drugimi nesrečami (tudi organiziranost civilne zaščite), varstvo pred požari in gasilstvo, varnost in zdravje pri delu, varstvo okolja, energetika (električna energija, naftni derivati, plin), varnost prometa (cestnega, železniškega, zračnega, vodnega), ravnanje s kemikalijami in nevarnimi snovmi, varnost hrane in pitne vode, zagotavljanje zdravja ljudi in živali, varstvo osebnih in tajnih podatkov, varovanje informacij in komunikacij (kibernetska varnost), zagotavljanje bančnih storitev, zasebno varovanje in druga področja. Pri upravljanju tveganj za delovanje KI je treba upoštevati tudi tista določila, ki urejajo področje poslovanja in ki eksplicitno določajo uporabo varnostnih ter drugih standardov v delovnih, poslovnih in drugih procesih. V tem kontekstu se osredotočimo na ključni zakonodajni okvir (zakoni in podzakonski predpisi) ki so: Zakon o varstvu pred naravnimi in drugimi nesrečami, Zakopn o varstvu pred požari, Zakon o gasilstvu, Zakon o varstvu okolja, Zakon o varnosti in zdravju pri delu. zakon o varstvu olsebnibh podatkov, Zakon o tajnih podatkih, Zakon o informacijski varnosti, Zakon o poslovnih skrivnostih (v javni razpravi in parlamentarni proceduri), Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih, Zakon o kemikalijah, Zakon o eksplozivnih snoveh, vnetljivih tekočinah, plinih ter drugih nevarnih snoveh, Zakon zdravstveni ustreznosti živil in izdelkov ter snovi, ki prihajajo v stik z živili, Zakon o vodah, Energetski zakon, Zakon o letalstvu, Zakon varnosti cestnega prometa, Zakon o železniškem

prometu, Pomorski zakonik, Zakon o zasebnem varovanju, Zakon o bančništvu, Zakon o zavarovalnicah. Je še cela vrsta drugih zakonov, ki urejajo dejavnosti v posameznih sektorjih KI. Neupoštevanje zakonodaje povzroča tveganja neskladnosti, tveganja kaznivih dejanj, etična tveganja in mnoga druga tveganja.

2.1.1 Nacionalne resolucije, strategije in programi

Resolucije, strategije in programe nacionalnega pomena sprejema Državni zbor (nekatere dokumente sprejema tudi Vlada RS -– denimo Obrambno strategiojo Slovenije). To so akti političnega pomena. Določajo politiko ravnanja, ne vsebujejo pa pravno zavezujočih norm. Kljub temu so to pomembni dokumenti, ki analizirajo določeno strateško vprašanje in usmerjajo razreševanje obstoječe problematike, negotovosti, ogroženosti in tveganja. Lahko rečemo, da so politična podpora sprejeti zakonodaji. Ti politični akti so pomembni tudi zato, ker v njih najdemo analitične podatke o določenem področju, ki so uporabni za strateško in operativno načrtovanje.

V nadaljevanju predstavljamo tiste resolucije, strategije in programe, ki so v času izdelave te študije pomembni za KI. Začnemo z Resolucijo o strategiji nacionalne varnosti Republike Slovenije, ki je krovni politični akt za upravljanje nacionalne varnosti.

Resolucija o strategiji nacionalne varnosti Republike Slovenije - ReSNV-1 (Ur. l. RS, št. 27/2010)

V resoluciji nas zanimajo tiste opredelitve, ki se nanašajo na ogrožanja KI, varnostna tveganja za delovanje KI in na ukrepe zaščite KI.

Različnim virom ogrožanja je v sodobnem času še posebej izpostavljena KI, ki s svojim delovanjem zagotavlja izvajanje ključnih funkcij države in družbe. S tega vidika lahko tudi ogroženost KI vpliva na nacionalno varnost Republike Slovenije. S terorističnimi napadi in drugimi grožnjami, motenjem, blokadami in povzročeno škodo na področju KI se lahko resno ogrozi zdravje, varnost ali blaginjo državljanov ter nemoteno delovanje države in javnih služb. V strokovni javnosti se vse bolj govori o globalnih in kompleksnih grožnjah in o novih varnostnih izzivih, ki terjajo kompleksen (celovit, vsestranski) odziv kompetentnih institucij. Kajti KI je ranljiva in dokaj lahka tarča terorističnih, kriminalnih in drugih napadov. Novodobni teroristični napadi v Evropi (zlasti) na KI nakazujejo, da je tovrstna infrastruktura ranljiva, ogrožena in zanimiva tarča teroristov**.**

Strategija razvoja Slovenije 2014 – 2020 (Ministrstvo za gospodarstvo, 2013)

Živimo v času, ko globalna gospodarska in finančna gibanja določajo oblikovanje politik na nacionalni ravni. Prav tako pa se globalno in lokalno soočamo s številnimi izzivi in dolgoročnimi trendi. Veliko izzivov se nanaša tudi na KI, v delovanje in zaščito katere bo potrebno vlagati več sredstev in več skrbi. Navajamo samo nekaj ključnih zavez v pričujoči resoluciji, ki se neposredno ali posredno nanašajo na sektorje KI.

Te zaveze so:

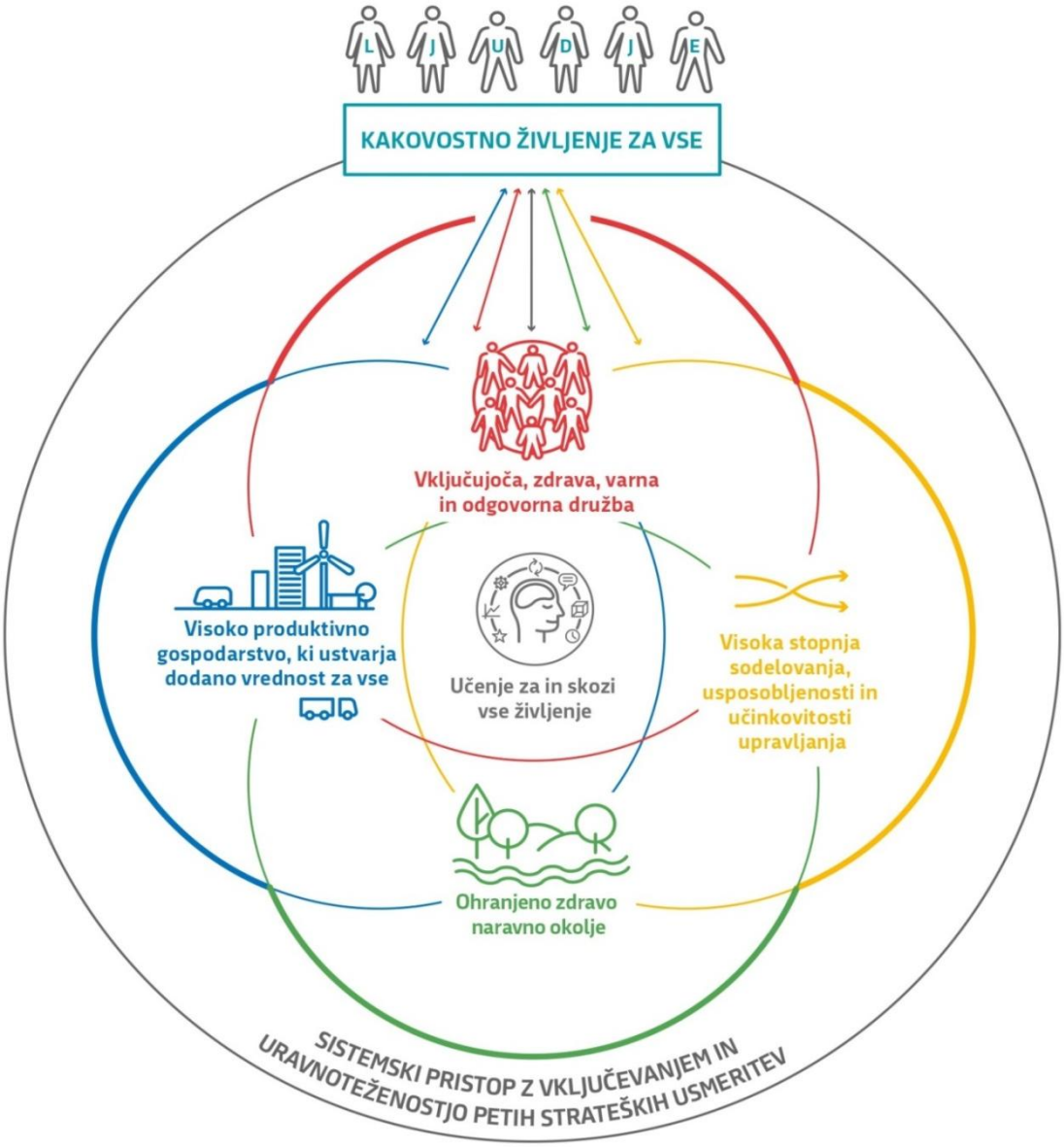
- še naprej je treba razvijati suveren energetski sistem z vsemi razvitimi funkcijami za njegovo delovanje. Potrebna so vlaganja v izgradnjo in modernizacijo energetske infrastrukture za prenos in distribucijo energije, vključno s pametnimi omrežji. Pri tem je treba spodbujati in vlagati v tiste tehnologije, ki podpirajo načelo okoljske, ekonomske in družbene vzdržnosti, ki slovenskemu gospodarstvu omogoči dolgoročno stabilno oskrbo z električno energijo po mednarodno primerljivih cenah; posodabljati je treba obstoječo prometno in logistično infrastrukturo z visokim razvojnim potencialom, ki bo omogočala pretočnost in varnost prometne infrastrukture, skladno z razvojem logističnih rešitev. To velja tako za cestno kot tudi za železniško infrastrukturo;
- v prihodnje je potrebno zagotoviti večjo učinkovitost in konkurenčnost mrežnih dejavnosti (energetika, telekomunikacije, komunala, voda), ki jih je treba posodobiti in dvigniti na višji nivo zadovoljstva uporabnikov;
- voda je strateški vir prihodnosti, zato je trajnostno in kakovostno gospodarjenje z vodnimi viri in vodno mrežo nujna skrb vseh deležnikov njene porabe;
- v prehranski industriji je pomembno dvigovanje prehranske samooskrbe, ki bo dolgoročno zagotavljala zadostno količino in kakovost prehranskih produktov in, ki ne bo strateško odvisna od tujih prehranskih verig;
- za obvladovanje zdravstvene problematike in zdravstvenih tveganj je treba povečati učinkovitost zdravstvenega sistema in zagotoviti dostop do kakovostne in varne zdravstvene obravnave.

Poleg te (srednjeročne) strategije je še bolj pomembna dolgoročna Strategija razvoja Slovenije do leta 2030, ki je okvirno predstavljena v nadaljevanju.

Strategija razvoja Slovenije 2030 (sklep Vlade RS št. 30000-7/2017/7z dne 07.12.2017)

Ta strategija je novi krovni razvojni okvir države. Glavni (osrednji) cilj strategije je zagotoviti kakovost življenja za vse (prikazano na sliki 3 v nadaljevanju). Povzemamo vsebine (5. poglavje: Gospodarska stabilnost in 11. poglavje: Varna in globalno odgovorna Slovenija), ki so relevantne z vidika delovanja in razvoja KI.

V strategiji je zapisano, da je Slovenija ena najbolj varnih držav na svetu, kar vpliva na kakovost gospodarjenja, poslovanja in življenja prebivalcev. Pojavljajo pa se številni novi varnostni in drugi izzivi, s katerimi se je treba pravočasno spoprijeti za ohranjanje varnosti Slovenije. Pri tem je pomembno nenehno zagotavljanje varnosti prebivalcev, varovanje premoženja in okolja ter neprekinjeno delovanje KI. Visoka stopnja varnosti države in državljanov je dosegljiva s spremljanjem in predvidevanjem varnostnih groženj in tveganj, vzpostavitvijo obrambnih in odvračalnih zmogljivosti ter pravočasnim in usklajenim odzivanjem na varnostna tveganja. V tem kontekstu je pomembno tudi preprečevanje varnostnih dogodkov s škodljivimi posledicami. Pomembni sestavini preprečevanja varnostnih dogodkov s škodljivimi posledicami sta tudi krepitev povezanosti z lokalnimi skupnostmi in neposreden stik z državljani. Ti cilji bodo doseženi z naslednjimi aktivnostmi:



Slika 3: Osrednji cilj in strateške usmeritve (Strategija razvoja Slovenije 2030, 2017)

- z zagotavljanjem zaščite pred terorističnimi in drugimi nadnacionalnimi grožnjami,
- z zagotavljanjem visoke ravni varnosti ljudi, njihovega premoženja in nemotenega delovanja KI,
- z vzpostavitvijo celovitega in učinkovitega sistema zagotavljanja kibernetske in informacijske varnosti ter odzivanja na hibridne grožnje,
- s spodbujanjem preventive in krepitvijo zmogljivosti za celovito obvladovanje naravnih in drugih nesreč,
- z zagotavljanjem obrambne sposobnosti države za izvajanje nacionalne obrambe in izpolnjevanje sprejetih mednarodnih obveznosti,
- z zagotavljanjem varnosti državne in zunanje meje EU ter iskanjem celovitih rešitev za učinkovito globalno upravljanje migracijskih tokov s sodelovanjem med izvornimi, tranzitnimi in ciljnimi državami,
- s krepitvijo zunanjepolitičnega sodelovanja na dvostranski in večstranski ravni, s poglabljanjem političnih, gospodarskih, kulturnih in drugih odnosov ter krepitvijo aktivne vloge Slovenije pri uveljavljanju mednarodnega miru in varnosti, spoštovanju človekovih pravic in mednarodnega prava ter doseganju trajnostnega razvoja na globalni ravni, tudi z mednarodnim razvojnim sodelovanjem in humanitarno pomočjo, katere del je uradna razvojna pomoč.

Poleg navedenih aktivnosti je pomembno še naslednje:

- zanesljiva, trajnostna in konkurenčna oskrba z energijo, katere omrežje se razvija v smer digitalizacije elektroenergetskega sistema (pametna omrežja),
- spodbujanje inovacij na področju informacijsko-komunikacijskih tehnologij,
- zmanjševanje izpustov toplogrednih plinov, kar je tudi zaveza Slovenije v okviru pariškega podnebnega sporazuma.

Ugotavljamo, da je v Strategiji razvoja Slovenije 2030 korektno zastopana tudi kritična KI, kar je podlaga tudi za morebitni nastanek Strategije razvoja KI vsaj do leta 2025. Čeprav je kritična infrastruktura v tej strategiji omenjena le dvakrat, jo štejemo za pomemben strateški dokument tudi na področju razvoja KI. Gospodarska stabilnost in gospodarski razvoj sta v veliki meri odvisna od stabilnosti, razvoja in zaščite KI, ki z neprekinjenim delovanjem zagotavlja nemoteno delovanje države, gospodarstva, civilne družbe in prebivalstva.

Resolucija o energetskem konceptu Slovenije (predlog Vlade RS, marec 2018)

Prenosni in distribucijski sistemi in omrežja (električna energija, plin, daljinsko ogrevanje) bodo tudi v prihodnje ustrezno regulirani. Delovali bodo zanesljivo in kakovostno ter se ob tem prilagajali spremembam oz. razvijali na tak način, da bodo zagotavljali zadostno robustnost in hkrati prožnost za vključevanje novih tehnologij in virov ter naprednih sistemov

upravljanja z energijo. Napredna omrežja bodo omogočala aktivno vlogo uporabnikov in razvoj naprednih stavb, skupnosti in mest. Glede na predvideno intenzivno uvajanje manjših, razpršenih in bolj nepredvidljivih OVE (obnovljivi viri energije) ter rast rabe toplotnih črpalk in e-mobilnosti, z implementacijo novih tehnologij in ponudbo storitev za aktivnega odjemalca, bo z vidika zagotavljanja zanesljivosti oskrbe, posebej izpostavljen električni energetski sistem.

Ta resolucija navaja tudi obvladovanje tveganj v proizvodnji, prenosu, distribuciji in porabi energentov, to je elektrike, naftnih derivatov in plina. Oskrba z energijo je poleg oskrbe s hrano, vodo ter pravico do zdravega življenjskega okolja, dela, počitka in varnosti, ena od naših temeljnih potreb. Zagotavljanje zanesljive, varne in konkurenčne oskrbe z energijo je ključno za državo, gospodarstvo, civilno družbo in prebivalstvo. Pri tem mora biti energetska politika in njeni cilji skladni s celotno politiko trajnostnega razvoja Slovenije in podpirati doseganje njenih ciljev.

Energetski koncept Slovenije upošteva tudi ključni izziv Slovenije na področju okolja, ki je trajnostna raba naravnih virov in upoštevanje okoljskih in naravovarstvenih ciljev ter ukrepov za zmanjšanje okoljskih vplivov, kot je to prilagajanje in blaženje podnebnih sprememb, ohranjanje biotske raznovrstnosti, varovanja naravnih vrednot, ohranjanje ugodnega stanja vrst in habitatov ter celovitosti varovanih območij, ohranjanje ugodnega stanja voda in izboljšanje kakovosti zraka, ohranjanje tal, zdravja prebivalcev in kulturne dediščine.

Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v **letih od 2016 do 2020 - RePVND16-22** (Ur. l. RS, št. 75/2016)

Iz uvoda: »Nacionalni program varstva pred naravnimi in drugimi nesrečami upošteva vse nevarnosti naravnih in drugih nesreč, ki ogrožajo ljudi, živali, premoženje, kulturno dediščino in okolje. Upošteva tudi naravne in druge danosti, ki vplivajo na nesreče in varstvo pred njimi, ter človeške in materialne vire, ki jih je mogoče uporabiti pri obvladovanju nevarnosti in varstvu ogroženih. Program poleg nacionalnih interesov upošteva tudi obveznosti Slovenije, ki izhajajo iz sprejetih mednarodnih in regionalnih pogodb, konvencij in sporazumov ter sklenjenih dvostranskih sporazumov s področja varstva pred nesrečami.«

Splošni cilj varstva pred naravnimi in drugimi nesrečami, je: zmanjšati število nesreč ter preprečiti oziroma ublažiti njihove posledice, da bi bilo življenje varnejše in bolj kakovostno. Usmerjen je v preventivo, ki je učinkovitejša in dolgoročno tudi cenejša od drugih oblik varstva pred nesrečami. Ker vseh nevarnosti, ki povzročajo nesreče, ni mogoče odpraviti, so v programu enakovredno obravnavane tudi vse tiste oblike varstva in pripravljenosti, ki omogočajo hitro in učinkovito ukrepanje ob nesrečah.

Zagotavljanje varstva pred naravnimi in drugimi nesrečami zajema tudi okoljske, industrijske ter druge nesreče, ki jih povzroči človek s svojo dejavnostjo in ravnanjem. V ta kontekst uvrščamo tudi dejavnost terorizma in različne oblike množičnega nasilja ter druge nevojaške in vojaške vire ogrožanja. Z vidika obvladovanja ogroženosti in tveganj so v prihodnje pomembne naslednje aktivnosti:

- nadaljevanje ocenjevanja ogroženosti zaradi naravnih in drugih nesreč, ki povzročajo vsestransko škodo in izgubo,
- usklajevanje ocenjevanja tveganj za posamezne nesreče – izhodišče je državna ocena,
- uveljavljanje celovitega ocenjevanja zmožnosti za obvladovanje tveganj na vseh ravneh, od države do gospodarskih in lokalnih okolij,
- prizadevanja za nadaljnji razvoj lastnih zmogljivosti za odzivanje na naravne in druge nesreče, pri čemer bo upoštevan multiplikativni učinek posameznih virov varnostnih groženj in tveganj.

V programu je opredeljen tudi razvoj in posodobljeno delovanje civilne zaščite, gasilskih in drugih služb, ki tvorijo sistem zaščite in reševanja. Gospodarske družbe, ki upravljajo s KI so sestavni del sistema zaščite in reševanja, saj v marsičem s svojimi sredstvi pomagajo pri razreševanju izrednih dogodkov in kriznih stanj. Zato si morajo načrtovati in organizirati ustrezne enote civilne zaščite, požarno varstvo, varstvo pred naravnimi in drugimi nesrečami ter varstvo okolja.
V kontekst varstva pred naravnimi in drugimi nesrečami ter v organiziranost področja zaščite in reševanja je korektno, da uvrstimo tudi državne načrte zaščite in reševanja (Ministrstvo za obrambo-Uprava RS za zaščito in reševanje), kajti njihova implementacija in izvedba segata dokaj globoko tudi v sektorje KI. Ti načrti so izdelani za naslednje izredne dogodke: potres, poplave, veliki požari v naravnem okolju, jedrska ali radiološka nesreča, množični pojav posebno nevarnih bolezni živali, nesreča na morju, železniška nesreča, nesreča zrakoplova, epidemija/pandemija nalezljive bolezni pri ljudeh, uporaba orožij ali sredstev za množično uničevanje v teroristične namene oziroma terorističnem napadu s klasičnimi sredstvi, druge nesreče, ki bi lahko prizadele večji del države oziroma povzročile obsežne posledice.

Resolucija o nacionalnem programu razvoja prometa v Republiki Sloveniji za obdobje do leta 2030 - ReNPRP30 (Ur. l. RS, št. 75/2016)

Prometna infrastruktura (cestno in železniško omrežje, zračni in vodni promet) igra pomembno vlogo pri razvoju industrije in gospodarstva ter celotne države in družbe. Ustrezna prometna infrastruktura, skupaj s funkcijami celotnega prometnega sistema, omogoča vsem zadovoljevanje mobilnostnih potreb v globalnem, regionalnem in lokalnem okolju.

V programu so opredeljeni koncepti razvoja posameznih vrst prometa (cestni, železniški, zračni, vodni), dinamika in viri finančnih vlaganj, prioriteta investicijskih vzdrževanj in novogradenj ter umestitev v evropski prometni sistem. Nakazani so tudi ukrepi varnosti v prometnem sistemu in vpliv vseh prometnih omrežij na okolje.

Strategija kibernetske varnosti v Republiki Sloveniji (sklep Vlade RS št. 38100-12/2015/5 z dne 25.02.2016)

Strategija uvodoma navaja, da »/…/vedno hitrejši razvoj informacijsko-komunikacijskih tehnologij po eni strani prinaša koristi za moderno družbo, po drugi strani pa vpliva na pojav vedno novih in tehnološko vse bolj dovršenih kibernetskih groženj. Vse izrazitejši je trend uporabe informacijsko-komunikacijskih tehnologij za politično, gospodarsko in vojaško prevlado. Nedvomno so prav kibernetski napadi ena izmed najpomembnejših varnostnih groženj sodobnemu svetu, kar je pripomoglo k temu, da je kibernetska varnost že pred časom postala pomemben integralni del nacionalne varnosti držav.«

V sodobni družbi so tako rekoč vsa področja delovanja družbe odvisna od informacijsko-komunikacijskih sistemov, nadaljnji razvoj pa bo to odvisnost le še povečeval. Medsebojna povezanost sistemov pomeni, da ima ranljivost enega lahko posledice na delovanje ostalih. Zagotavljanje popolne varnosti pred kibernetskimi napadi, zlorabami, goljufijami, napakami človeške in tehnološke narave ter drugimi vplivi je nemogoče, zato je pri določanju prioritete posamezne grožnje treba uporabiti pristop, ki temelji na zelo pronicljivi oceni tveganja. Kajti uspešno zagotavljanje visokega nivoja kibernetske varnosti zahteva učinkovito izrabo obstoječih virov in primerno več-nivojsko organiziranost. Slovenija bo vzpostavila osrednji mehanizem za koordinacijo nacionalnega sistema zagotavljanja kibernetske varnosti (glej naslednjo sliko) in zagotovila pogoje za njegovo stabilno delovanje. Mehanizem bo na strateški ravni koordiniral zmogljivosti za zagotavljanje kibernetske varnosti na nižjih ravneh v državi ter predstavljal enotno kontaktno točko pri mednarodnem sodelovanju. O obliki organiziranosti zagotavljanja koordinacijskih funkcij bo odločila Vlada Republike Slovenije.

Na nacionalni ravni zagotavlja kibernetsko varnost Ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in zatiranja kibernetskega kriminala, Slovenska obveščevalno-varnostna agencija (SOVA) na področju protiobveščevalnega delovanja in nastajajoči SIGOV-CERT na področju javne uprave. Na operativni ravni pa kibernetsko varnost s svojimi zmogljivostmi zagotavlja Nacionalni odzivni center za kibernetsko varnost (SI-CERT).

Slika 4: Sistem zagotavljanja kibernetske varnosti (Strategija kibernetske varnosti v Republiki Sloveniji, 2016)

V KI je nosilec zagotavljanja kibernetske varnosti služba ali oddelek informacijsko-komunikacijskih omrežij in sistemov (sektor informacijsko-komunikacijske podpore). Sredstva in tehnologija v sektorju informacijsko-komunikacijske podpore mora biti zasnovana in upravljana tako, da zagotavlja sistemsko informacijsko-komunikacijsko podporo na različnih ravneh. Zagotoviti je treba neprekinjeno delovanje celotne kritične infrastrukture, ki omogoča e-delovanje internetnih sistemov v državi in strojne ter programske opreme, ki podpira ključne funkcije v državi. Vzpostavijo se hitri in učinkoviti mehanizmi za odzivanje na grožnje in odpravljanje napak (sanacija škode), ki so posledica varnostnih incidentov ter mehanizmi preventivnega delovanja, ki grožnje in napake v največji meri preprečujejo. Z vzpostavitvijo samostojnega odzivnega centra za sisteme v javni upravi (SIGOV-CERT) se razbremeni SI-CERT (Slovenski odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij), ki lahko ob ustrezni okrepitvi pozornost usmeri tudi na zagotavljanje kibernetske varnosti v sektorju informacijsko-komunikacijske podpore. Za zagotavljanje neprekinjenega delovanja KI v sektorju informacijsko-komunikacijske podpore se mora izvajati redno ocenjevanje kibernetskih in drugih groženj in tveganj ter načrtovanje ustreznih ukrepov za zaščito ter posodabljanje strojne, programske in druge opreme.

V sistem zagotavljanja kibernetske varnosti bodo povezani tudi drugi deležniki zagotavljanja kibernetske varnosti za delovanje KI. Pomembni so vsi nosilci, lastniki in upravljavci KI, kot so sektor energetike, sektor prometa, sektor prehrane in vode, sektor zdravstva, bančni sektor in sektor varovanja okolja. Kajti zagotavljanje kibernetske varnosti za delovanje KI je strateškega pomena za nacionalno varnost (glej točko 5.3.5: Odzivanje na kibernetske grožnje v Resoluciji o strategiji nacionalne varnosti).

Resolucija o nacionalnem planu zdravstvenega varstva 2016 – 2025 - **Skupaj za družbo zdravja - ReNPZV16-25** (Ur. l. RS, št. 25/2016)

Resolucija je dokument, ki izraža zdravstveno politiko države, s katero predstavlja ključne probleme zdravja in sistema zdravstvenega varstva v Sloveniji ter postavlja temelje za zdravje v vseh drugih politikah. Z vlaganji v zdravje in zdravstvo, ki jih predvideva Resolucija, naj bi v prihodnje tudi bolj učinkovito prispevali k trajnostnemu razvoju Slovenije. Predstavlja torej podlago za razvoj zdravstvenega sektorja v Sloveniji v naslednjih desetih letih in za pripravo ter sprejem ustreznih zakonov s področja zdravstvenega zavarovanja in zdravstvene dejavnosti ter ohranja vizijo kakovostnega in vsem dostopnega javnega zdravstva. V središče je postavljen uporabnik in izvajalec javnih in zasebnih zdravstvenih storitev, ki si mora prizadevati za izvajanje naslednjih aktivnosti:

- krepitev in varovanje zdravja ter preprečevanje bolezni;
- optimizacijo zdravstvene oskrbe;
- povečanje uspešnosti sistema zdravstvenega varstva;
- pravično, solidarno in vzdržno financiranje zdravstvenega varstva.

V resoluciji je zahtevana pripravljenost za obvladovanje groženj in tveganj za zdravje, to je zahteva za celovit in organiziran pristop, ki ga lahko zagotovimo le z usklajenim delovanjem različnih deležnikov oziroma sektorjev, ki sodelujejo pri upravljanju groženj zdravju tako znotraj države kot tudi v okviru EU in širše v mednarodnem okolju. Med grožnje zdravju uvrščamo izbruhe nalezljivih bolezni ali okoljska tveganja, do katerih pride spontano, zaradi nesreč, onesnaženja okolja, bioterorizma ali drugih okoliščin, kot so ekstremni vremenski pogoji. Poseben izziv predstavlja tudi odpornost mikrobov na zdravila. Z vsem tem se v zadnjem desetletju države soočajo predvsem v luči globalizacije. Tudi dejavniki iz okolja lahko pomenijo nenadno grožnjo zdravju in zahtevajo javnozdravstveno ukrepanje. Nekateri dejavniki okolja predstavljajo tveganje za zdravje tudi v primeru, ko smo jim izpostavljeni daljši čas (npr. sevanja, onesnaženost zemlje, zraka, vode ipd.). V sektorju zdravstva pa ne gre samo za t.i. čista zdravstvena tveganja, ki se neposredno nanašajo na bolezni, temveč tudi za številna druga tveganja, ki vplivajo na kakovost zdravstvenih storitev. To so denimo tveganja zdravstvenega kadra, poslovna tveganja, tveganja čakalnih dob, tveganja zastarele opreme in druga tveganja.

Za boljše obvladovanje dejavnikov tveganja za bolezen in preprečevanje bolezni v vseh življenjskih obdobjih in okoljih ter obvladovanje vseh drugih tveganj, bo treba izboljšati preventivno dejavnost v zdravstvu, še posebej v primarnem zdravstvenem varstvu in medicini dela. Ob tem pa bo treba izboljšati tudi kadrovsko politiko, politiko nabave in druge politike. Poleg tega je treba okrepiti sposobnost odziva pristojnih institucij na morebitna zdravstvena tveganja in grožnje zdravju zaradi novih nalezljivih bolezni ter drugih groženj zdravju in zagotoviti najvišjo stopnjo varovanja zdravja na delovnem mestu.

Za obvladovanje groženj za zdravje in obvladovanje dejavnikov tveganja ter zgodnje odkrivanje bolezni poznamo učinkovite politike, ukrepe in programe, ki ob zagotavljanju boljšega zdravja in večje kakovosti življenja pomenijo tudi prihranek za sistem zdravstvenega varstva in družbo kot celoto. S tega vidika je treba k varovanju zdravja pristopiti resno v vseh sektorjih KI in v vseh gospodarskih družbah, ki upravljajo s KI.

Nacionalni program varstva okolja 2030 - NPVO 30 (predlog Vlade RS, februar 2018)

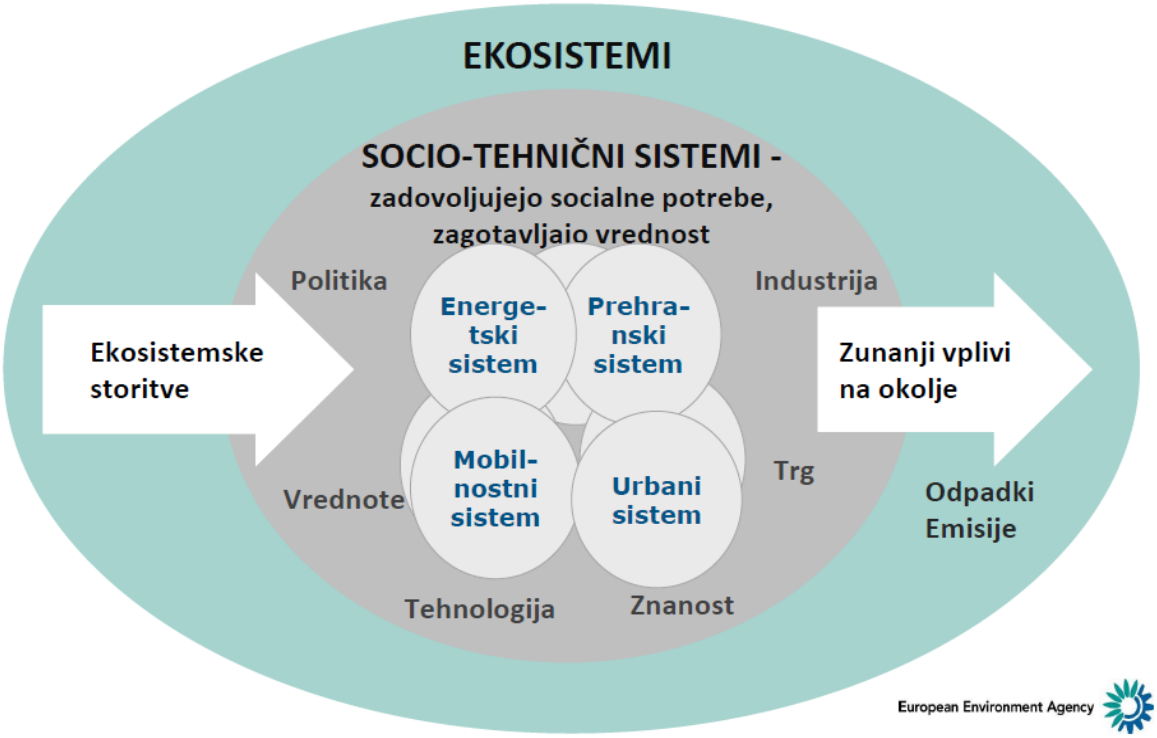
Nacionalni program varstva okolja 2030 je dokument okoljske politike Slovenije, ki na dolgi rok usmerja varstvo okolja in ohranjanje narave ter varstvo tal, zraka in vode.

Ocena je, da se je stanje okolja v Sloveniji v zadnjih letih, glede na rezultate spremljanja stanja okolja, vidno izboljšalo. Izboljšalo se je tudi poznavanje in razumevanje povezav med pritiski na okolje in njihovimi posledicami na stanju okolja, povečala pa se je tudi občutljivost ljudi ter njihova ozaveščenost o pomenu zdravega okolja za kakovost življenja sedaj in v bodoče. Ostali pa so izzivi kot so na primer prekomerno onesnažena območja zaradi preteklih dejavnosti, vsakoletna kratkotrajna slabša kakovost zraka, nezadovoljivo stanje ohranjenosti biotske raznovrstnosti in prepočasno prilagajanje podnebnim spremembam.

Nastali so tudi novi izzivi, ki so predvsem posledica povečanih pritiskov na prvine okolja in naravne vire, predvsem zaradi načina našega življenja, ki ga zaznamujeta netrajnostna proizvodnja in potrošnja. Zato je zaveza za »trajnostni razvoj« morda še pomembnejša kot v preteklosti in zdaj še bolj kliče po udejanjenju v praksi – predvsem z radikalnimi spremembami v socialnem in gospodarskem razvoju, kjer je nujen preobrat k bolj trajnostnemu načinu bivanja, proizvodnje in potrošnje tudi v praksi in vsakodnevnem življenju ter predvsem na podlagi analiz posledic in učinkov, predvsem z družbenim konsenzom.

Za obvladovanje okoljske ogroženosti in okoljskih tveganj je potreben sistem ukrepov države, industrije, gospodarstva, civilne družbe in prebivalstva. KI je močno podvržena okoljskim problemom, težavam, ogroženosti in tveganjem. Zato skrb za okolje ni samo zadeva sektorja varovanja okolja, temveč velika dolžnost vseh sektorjev, ki vsak na svoj način ogrožajo okolje ali prispevajo k izboljšanju stanja.

V nadaljevanju je na sliki 5 prikazan model varstva okolja z vsemi sektorji KI.



Slika 5: Ekosistemski model varstva okolja (Evropska okoljska agencija, The european Environment Agency, EEA)

Varstvo pred okoljsko ogroženostjo in okoljskimi tveganji obsega upravljanje tveganj na naslednjih področjih:

- v preteklosti onesnažena območja,
- okoljski hrup,
- biološka varnost,
- ravnanje s kemikalijami,
- elektromagnetno sevanje,
- svetlobno onesnaževanje,
- prilagajanje podnebnim spremembam.

Konkretno pa se področje varstva okolja spopada z naslednjimi tveganji: tveganja naravnih nesreč, tveganja industrijskih nesreč, požarna tveganja v naravnem okolju, industriji in individualna požarna tveganja, poplavna tveganja, tveganja suše, tveganja obilnih padavin in žleda, tveganja plazov, tveganja elektromagnetnih in drugih sevanj, tveganja izpustov in izlitij nevarnih snovi ter kemikalij, tveganja slabega vzdrževanja vodotokov, tveganja črnih odlagališč, tveganja izpustov toplogrednih plinov, tveganja neobvladovanja odpadkov, tveganja hrupa ipd. Torej gre za globalno, regionalno in lokalno problematiko sodobnega časa, ki je rešljiva na dolgi rok, če sploh je. Posebna pozornost mora biti namenjena

varovanju prebivalcev, ki so lahko na eni strani onesnaževalci okolja, na drugi pa prizadeti državljani, ki se morajo na mnogih mestih soočati z onesnaženostjo in škodljivimi vplivi gospodarskih in drugih subjektov. Če bo program varstva okolja vsaj delno zaživel v praksi, se na področjih varstva okolja obeta izboljšanje stanja.

2.1.2 Standardi

Osnovni namen uvajanja standardov kakovosti, varnostnih standardov, standardov ravnanja s tveganji, standardov družbene odgovornosti in drugih standardov v poslovne procese sektorjev KI je: najprej učinkovitejše obvladovanje tveganj, zagotovItev preglednosti delovanja in poslovanja ter dvigovanje konkurenčnosti, nato pa še zagotavljanje trajnostnega razvoja organizacij, ki upravljajo KI.

Sodobno upravljanje KI torej poteka tudi na podlagi uveljavljenih mednarodnih in nacionalnih standardov. Mislimo zlasti na standarde kakovosti, obvezne varnostne standarde na področjih zasebnega varovanja, varsrtva okolja, varnosti in zdravja pri delu in varnosti živil .Poleg tega je koristno v procese delovanja KI uvesti tudi druge (neobvezne) standarde kot so denimo standardi za varovanje informacij (ISO/IEC 27000), varnost in zdravbe pri delu (OHSAS 18001), neprekinjeno poslovanje (ISO 22301) družbeno odgovornost (ISO 26000) in upravljanje tveganj (ISO 31000), vse v sklopu standardov kakovosti ISO 9001. Uvedba standardov namreč omogoča organizacijsko, metodološko in izrazoslovno urejeno poslovanje. Poleg tega standardi omogočajo primerjanje rezultatov poslovanja in razvoja med gospodarskimi družbami, zavodi, državnimi organi in Banko Slovenije, ki upravljajo s KI.

V nadaljevanju navajamo posamezne standarde tako kot sledi:

a. Obvezni (varnostni) standardi na področju zasebnega varovanja so:

- SIST EN 50518 za sprejem alarmov v varnostno nadzornih centrih,
- SIST EN 50131 za alarme vloma in ropa,
- SIST EN 50132 za video nadzorne sisteme,
- SIST EN 50 133 za alarme nadzora dostopa,
- SIST EN 50136 za opremo za prenos alarmov,
- SIST EN 54 za prenos požarnih alarmov,
- SIST EN 1522 varnostne zahteve za okna in vrata glede odpornosti proti strelnemu orožju.

V kontekstu obveznih standardov na področju zasebnega varovanja je treba opozoriti tudi na gospodarske družbe, ki so po 69. členu Zakona o zasebnem varovanju (Ur. l. RS, št. 17/2011) in po Uredbi o obveznem organiziranju varovanja (Ur. l. RS, št. 80/2012) zavezanci

obveznega organiziranja varovanja. Kot zavezanci obveznega organiziranja svarovanja so dolžni izdelati načrt varovanja, ki obsega:

- oceno stopnje tveganja,
- program varovanja in
- načrt fizičnega varovanja.

Obvezni elementi ocene stopnje tveganja so:

- podatki o zavezancu organiziranja službe varovanja,
- opis varovanega območja,
- analiza ranljivosti,
- analiza ogroženosti,
- analiza tveganj,
- splošna ocena o stopnji tveganja z oceno verjetnosti nastanka posledic.

Ocena stopnje tveganja mora biti izdelana v treh stopnjah:

- nizka stopnja – verjetnost tveganja za nastanek izrednega dogodka (škodnega pojava) je manjša – poslovanje zavezanca je normalno,
- srednja stopnja – verjetnost tveganja za nastanek izrednega dogodka je večja – poslovanje zavezanca je lahko moteno,
- visoka stopnja – verjetnost tveganja za nastanek izrednega dogodka.

Po 69. členu Zakona o zasebnem varovanju so zavezanci obveznega organiziranja varovanja gospodarske in druge družbe, ki:

- uporabljajo ali hranijo radioaktivne snovi, jedrska goriva, odpadke in druge ljudem in okolju nevarne snovi in naprave,
- upravljajo zmogljivosti, sisteme ali njihove dele, ki so bistveni za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imela resne posledice na nacionalno varnost Republike Slovenije zaradi nezmožnosti vzdrževanja teh funkcij (promet, energija, telekomunikacije),
- hranijo arhivsko gradivo in predmete, ki predstavljajo kulturno dediščino,
- upravljajo javna letališča ali morska pristanišča za mednarodni javni promet ali izvajajo prevoze v mednarodnem letalskem in morskem prometu ali
- je iz posebnih varnostnih razlogov nujno potrebno.

Gre torej za gospodarske družbe in druge organizacije (zavezanci obveznega varovanja) katerih dejavnost je prepoznana kot dejavnost pomembna za državo, gospodarstvo, civilno družbo in prebivalstvo. To so: energetika, promet, telekomunikacije, zdravstvo, jedrske snovi in še nekatera druga področja. V bistvu gre torej za področja, ki sodijo v KI.

b. Standard HACCP za prehrambeno industrijo – živila in voda

Prehrana ljudi in živali je vsekakor življenjsko pomemben sektor KI. Posebnost sektorja prehrane je, da mora delovati, se razvijati in obvladovati številna tveganja v skladu z mednarodnim (svetovnim) standardom HACCP – Hazard Analysis Critical Control Point – analiza tveganj in ugotavljanje kritičnih kontrolnih točk. To je zahteva evropskega pravnega reda za to področje in zahteva slovenske živilske zakonodaje – Zakona o zdravstveni ustreznosti živil in izdelkov ter snovi, ki prihajajo v stik z živili in podzakonskimi predpisi izdanimi na njegovi podlagi.

HACCP je torej obvezen za gostinska podjetja, za živilsko predelovalno industrijo (mlekarstvo, pivovarstvo, živinorejstvo, mesno industrijo), za trgovine z živili idr. Velja tudi za transport in skladiščenje prehrambenih izdelkov. Z uvedbo HACCP se podjetje zaveže, da bo vzpostavilo takšen notranji kontrolni sistem, ki bo obvladoval vsa tveganja in vse ugotovljene kritične kontrolne točke v procesih proizvodnje, predelave, transporta, skladiščenja in trgovanja, na katerih lahko pride do nevarnih situacij.

V dobavnih verigah prehranskih izdelkov prihaja do številnih tveganj, ki se še povečajo, če so dobavne verige čezmejne. V takih primerih je potrebno uvesti mednarodni standard ISO 22000 Food Safety Management-upravljanje varnosti živil, ki omogoča zagotavljanje varnosti vseh živilskih proizvodov, ki prečkajo meje. V uporabi je tudi standard IFS (International Food Standard), ki omogoča ocenjevanje proizvajalcev živil in ocenjevanje izvajalcev v logističnih (dobavnih) verigah. Prav tako je v uporabi mednarodni standard ISO 22000 Food Safety Management – sistem zagotavljanja varnosti živil.

Sektor prehrane je torej prepreden z mnogimi tveganji, katerih obvladovanje ima strateško vlogo pri zagotavljanju zdravja ljudi in živali. Zato obvezna uvedba zgoraj omennjenih standardov v procese pridelave, predelave, transporta in trgovanja omogoča nadzorovanje, spremljanje kakovosti in sledljivosti ter varnosti vseh vrst živil. Torej je pod lupo integriranega nadzora celotna prehranska veriga od pridelovalca do potrošnika.

c. Okoljski standard za okoljske zavezance ISO 14001 + EMAS (ECO Management and Audit Sheme) + SEVESO (obrati manjšega in večjega tveganja za okolje)

Organizacijam, kjer obstaja tveganje, da bi prišlo do večjih nesreč sicer ni potrebno pridobiti certifikata, ki bi potrjeval, da imajo vpeljan sistem varovanja okolja, vseeno pa morajo vpeljati osnovne elemente, ki so predvideni za sisteme ravnanja v skladu z ISO 14001. Ob tem velja poudariti, da omenjeni standard že sam po sebi zahteva od organizacije, da vzpostavi in vzdržuje postopke s katerimi prepoznava morebitna tveganja za nastanek nesreč in izrednih razmer. Organizacija mora predvideti tudi odziv in ukrepe za ravnanja ob nesrečah oziroma izrednih razmerah. Ti naj bi bili usmerjeni v obvladovanje in preprečevanje oziroma

omejevanje morebitnih škodljivih učinkov na okolje. Kljub temu, da je okoljska zakonodaja zelo stroga glede varstva okolja, je smiselno, da se okoljski zavezanci certificirajo po okoljskih standardih in po EMAS in si s tem ustvarijo dodano vrednost v skrbi za čisto okolje.

Z vidika obvladovanja tveganj za delovanje KI je dobro vedeti, da je v KI kar nekaj sektorjev oziroma upravljavcev KI, ki se morajo resno, profesionalno ter v skladu z zakonodajo in okoljskimi standardi spopadati z varstvom okolja, kjer igrajo pomembno vlogo ocena ogroženosti, ocena tveganj in učinkoviti ukrepi zaščite. To so v prvi vrsti sektor energetike in sektor prometa, potem pa še sektor zdravstva in sektor varovanja okolja, ki je že sam po sebi zavezan k obvladovanju ogroženosti, obvladovanju tveganj in zagotavljanjuprimerne okoljske zaščite premoženja, zraka, zemlje, vode, človeških virov ter živalskega in rastlinskega življa. Upravljavci KI, ki so okoljski zavezanci po naši zakonodaji in po SEVESO II in SEVESO III se pač morajo prilagoditi predpisanim zahtevam in uvajati okoljske standarde kot so SIST EN ISO 14001 in EMAS ter druge standarde.

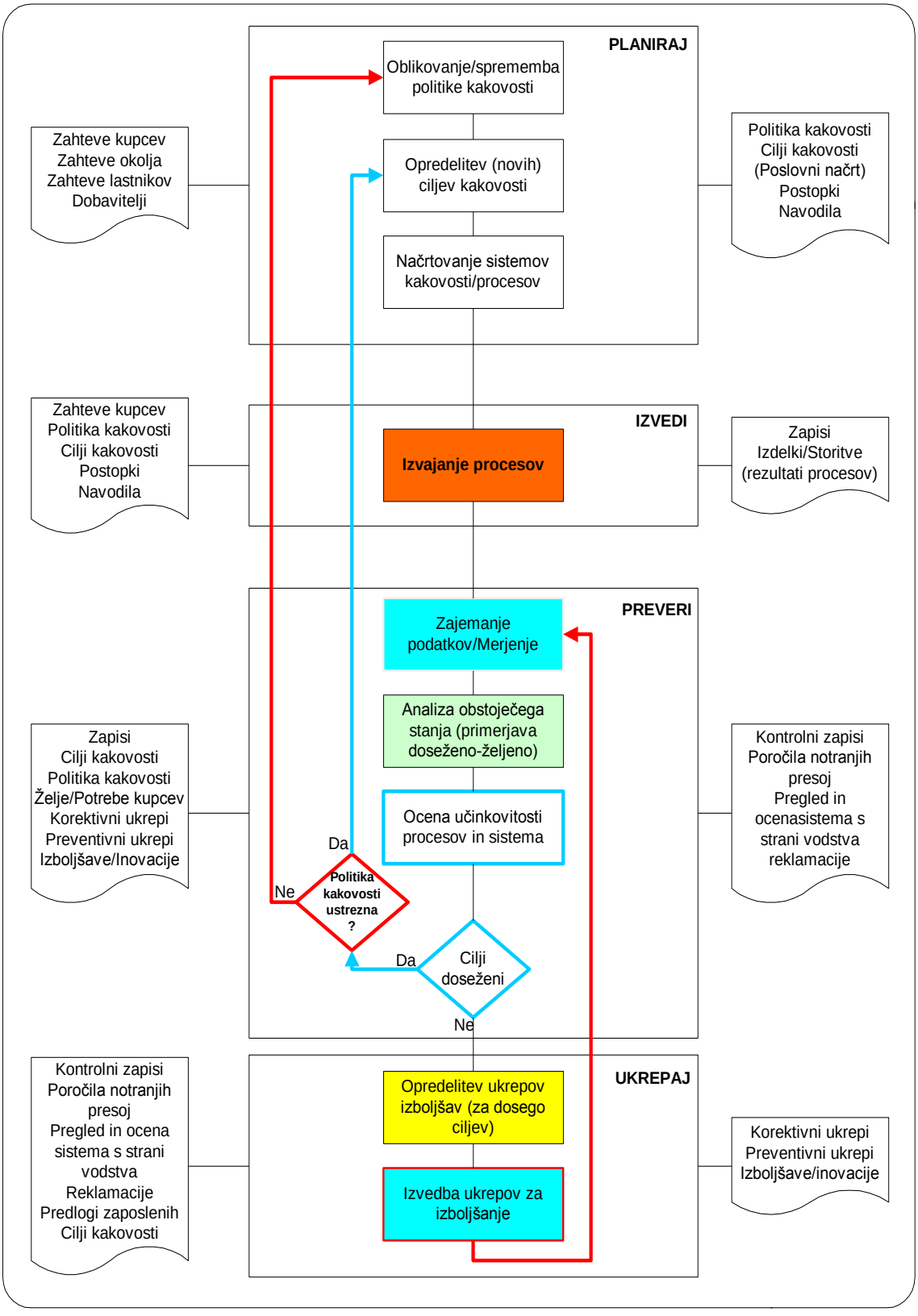
Posebni vidik varovanja okolja se kaže v prešibki povezanosti področja varovanja okolja s področji kot so: varnost in zdravje pri delu, požarno varstvo, zaščita in reševanja ter fizično in tehnično varovanje. Gre za zagotavljanje večje povezanosti pri ocenjevanju ranljivosti, ogroženosti in tveganj, pri načrtovanju skupnih ukrepov v sklopu načrta zaščite in reševanja, načrta fizičnega in tehničnega varovanja ter načrtovanja skupnih finančnih vložkov v področje varstva okolja. Na ta način bi se dalo marsikaj racionalizirati, zmanjšati stroške in povečati preglednost nad stroški in koristmi vlaganja v to področje. Dodana vrednost boljšega povezovanja med navedenimi področji je vsekakor dvig stopnje obvladovanja ekoloških tveganj.

d. Standardi kakovosti

Standardi kakovosti so temeljni standardi delovanja in poslovanja gospodarskih in drugih družb. To še posebej velja za gospodarske družbe, zavode, državne organe in Banko Slovenije, ki upravljajo KI in ki morajo zagotavljati njeno neprekinjeno delovanje.

Upravljavci KI, ki imajo certificiran sistem vodenja kakovosti po standardu ISO 9001 in uporabljajo procesni pristop (ki se zrcali v strukturi standarda ISO 9004:2000) temelječ na konceptu PDCA (Plan-Do-Check-Act), morajo planirati in izvajati procese nadzorovanja, merjenja, analiziranja in izboljševanja procesov, kar velja tudi za varnostni proces in proces upravljanj tveganj ali njegove podprocese oziroma za sistem in proces zagotavljanja integralne varnosti lokacij, objektov, opreme, procesov, omrežij, dobavnih verig in človeških virov.

Na sliki 6 je prikazan splošni model upravljanja kakovosti delovanja in poslovanja katerekoli organizacije. V celoti je uporaben tudi za vse organizacije v sektorjih KI.



Slika 6: Sistem vodenja kakovosti po standardih ISO 9001 in Demingovem modelu PDCA – PLANIRAJ-IZVEDI-PREVERI-UKREPAJ

e. Nekateri drugi pomembni standardi

- Standard ISO/IEC 27000 – standardi varovanja informacij.
- Standard za načrtovanje in upravljanje neprekinjenega poslovanja oziroma standard za izdelavo in implementacijo načrta neprekinjenega poslovanja ISO 22301 Business Continuity Plan.
- Standard družbene odgovornosti ISO 26000.
- Standard družbene odgovornosti SA 8000 (Social Accountability 8000).
- V zdravstvu je prepoznanih kar lepo število poslovnih, finančnih, tržnih in drugih tveganj, ki so zelo slabo obvladljiva. Na tem mestu pa nas zanimajo predvsem specifična zdravstvena tveganja, to so klinična tveganja, ki so obvladljiva s pomočjo standarda AACI (mednarodni akreditacijski standard za zdravstvene organizacije). Ta mednarodni akreditacijski standard (poglavje 9: Obvladovanje tveganj) določa proaktivni pristop k obvladovanju tveganj, ki vključuje:
  - prepoznavanje tveganj,
  - določitev prednostnih tveganj,
  - poročanje o tveganjih,
  - obvladovanje tveganj in zmanjševanje tveganj,
  - preiskovanje neželenih dogodkov in,
  - upravljanje s tem povezanimi zahtevki.

Za analiziranje tveganj so v standardu priporočena analitična orodja kot so analiza možnih napak, analiza učinkov in druge metode.

f. Standardi za upravljanje tveganj

Temeljni standard za upravljanje tveganj je SIST ISO 31000:2018 in njemu podporni standard ISO/IEC 31010 in drugi podporni standardi. Pri pripravi metodologije upravljanja, obvladovanja in ocenjevanjqa tveganj za delovanje KI ga je smiselno in koristno uporabiti v sklopu izbranih metod ocenjevanja tveganj, v sklopu zakonskih zahtev obvladovanja tveganj in v sklopu obveznih varnostnih standardov. Ena od ključnih aktivnosti po tem stanradu je ocenjevanje tveganj, ki zajema prepoznavanje tveganj, analiziranje tveganj in vrednotenje tveganj. Standardi za upravljanje tveganj usmerjajo skrbnike, upravljavce in ocenjevalce tveganj tudi v uporabo enotnih izrazov in v upoštevanje varnostnih vidikov tveganj.

2.1.3 Nekatera poslovna orodja in tehnike, ki prispevajo k učinkovitemu upravljanju tveganj

Upravljanje tveganj za delovanje KI je izredno kompleksno in zahtevno kontinuirano opravilo na strateški in operativni ravni delovanja gospodarskih družb, ki upravljajo z določenimi sredstvi, premoženjem, produkti, storitvami in človeškimi viri s statusom KI. Zato je priporočljivo, da si vodstva in druge odgovorne osebe pri nosilcih sektorjev, zlasti pa pri

upravljavcih KI pridobijo nekaj znanj o poslovnih orodjih in tehnikah, ki prispevajo k učinkovitejšemu obvladovanju tveganj. »To so predvsem orodja kot denimo: benchmarking (slo. primerjanje s konkurenti), business intelligence (slo. pridobivanje pomembnih poslovnih informacij iz okolja in varovanje lastnih občutljivih podatkov), model 20 ključev (izboljšanje organiziranosti), BSC sistem uravnoteženih kazalnikov (izboljšanje internih računovodskih, finančnih in drugih evidenc iz poslovanja), filozofija Kaizen (stalne izboljšave) in druga poslovna orodja. Z uporabo nakazanih orodij si gospodarska družba izboljša konkurenčni položaj, dobro ime in družbeno odgovornost.« (Vršec/Vršec, 2012). Z benchmarkingom ocenjujemo in obvladujemo tržna tveganja, z business intelligence tveganja prisluškovanja in prestrezanja občutljivih poslovnih informacij, z BSC finančna tveganja, z 20 ključi pa organizacijska, tehnično tehnološka, kadrovska in okoljska tveganja. Metoda Kaizen pa uvaja stalne izboljšave v poslovnih procesih, kar je v skladu s standartdi kakovosti in standardi upravljanja tveganj.

2.2 SISTEMATIKA UPRAVLJANJA TVEGANJ

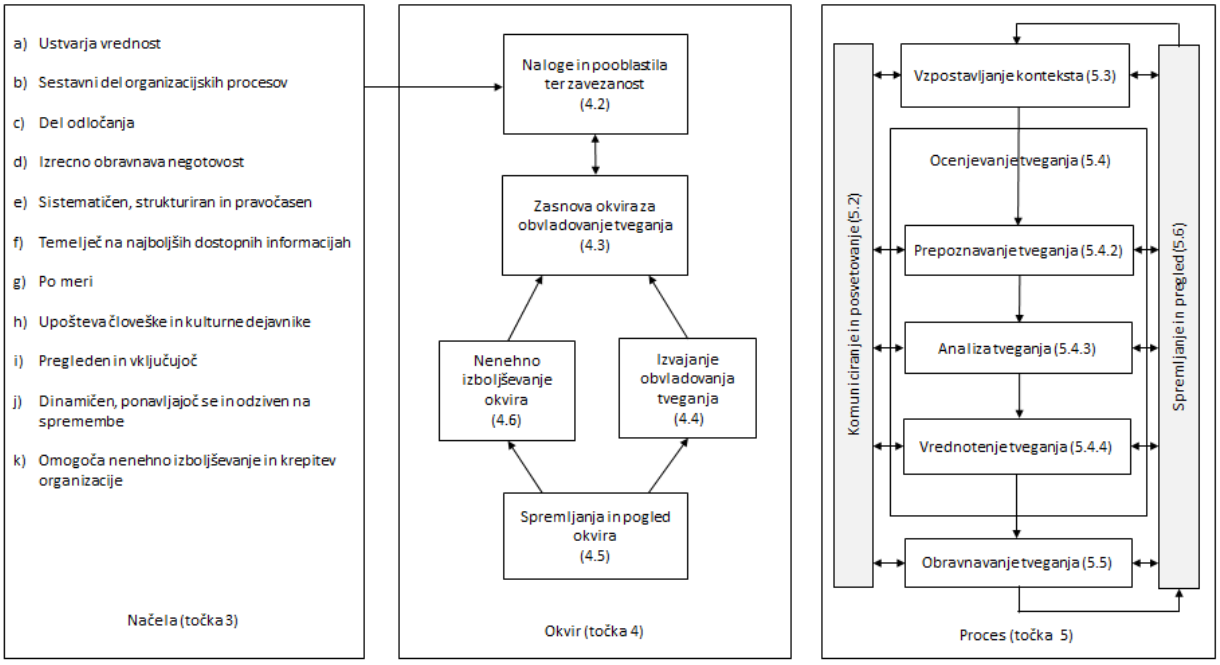
Organizacije vseh velikosti in vrst se soočajo z notranjimi in zunanjimi dejavniki ter vplivi, ki jih postavljajo v negotovost. Ta negotovost ima lahko pomemben vpliv na doseganje ciljev in poslanstva organizacije. V večini vse dejavnosti v organizacijah vključujejo določena tveganja. Pomembno je, da organizacije poskušajo obvladovati tveganja s sistemskim pristopom, ki obsega identifikacijo, analizo, vrednotenje in nenazadnje izvedbo ukrepov, ki ta tveganja zmanjšajo na še sprejemljiv nivo. Zagotoviti je namreč treba obvladovanje tveganj do te mere, da nimajo pomembnega negativnega učinka na poslovne, finančne, proizvodne, delovne, logistične, informacijsko-komunikacijske, kadrovske in druge procese v organizacijah. V poslovnem in organizacijskem okolju je pomembno zagotavljati določeno stabilnost in prepoznavnost ukrepov obvladovanja tveganj, ki je nujna za ustrezno soodelovanje med organizacijami. Zaradi navedenega so pomembna skupna izhodišča, prepoznana v najbolj široko sprejetem standardu SIST ISO 31000:2018, ki opredeljuje Obvladovanje tveganj – Načela in smernice (ang. Risk management – Principles and guidelines).

Ta mednarodni standard postavlja določene okvire in predloge na katerih organizacije lahko razvijejo, izvajajo in nenehno izboljšujejo okvir, katerega namen je vključiti proces obvladovanja tveganj v celoten proces korporativnega upravljanja, strategijo, načrtovanje, vodenje, procese poročanja, politiko, vrednote ter kulturo organizacije. Omenjeni standard organizacijam, ki ga sprejmejo, kot minimalni temelj za obvladovanje tveganj omogoča:

- povečuje verjetnosti za doseganje ciljev,
- spodbuja proaktivno vodenje,

- se zaveda potrebe po identificiranju in obravnavanju tveganj po vseh delih organizacije,
- izboljšuje identifikacijo priložnosti in groženj,
- izpolnjuje ustrezne pravne in regulativne zahteve ter mednarodne normative,
- izboljšuje obvezno in prostovoljno poročanje,
- izboljšuje upravljanje sredstev in premoženja,
- izboljšuje zaupanje deležnikov,
- vzpostavlja zanesljivo podlago za odločanje in načrtovanje,
- izboljšuje ukrepe za obvladovanje tveganja,
- uspešno dodeluje in uporablja vire za obravnavanje tveganja,
- izboljšuje delovno uspešnost in poslovno učinkovitost,
- izboljšuje varnost in zdravje pri delu ter varstvo okolja,
- izboljšuje preprečevanje poškodb in obvladovanje izrednih dogodkov,
- zmanjšuje škode in izgube,
- izboljšuje organizacijsko učenje in
- izboljšuje organizacijsko prilagodljivost (ISO 31000:2011, SIST ISO 31000:2018).

Za boljše razumevanje koristnosti tega standarda si oglejmo razmerja med načeli, okvirom in procesom obvladovanja tveganja, ki so prikazana na sliki 7.



Slika 7: Razmerje med načeli, okvirom in procesom obvladovanja tveganja (ISO 31000, 2011)

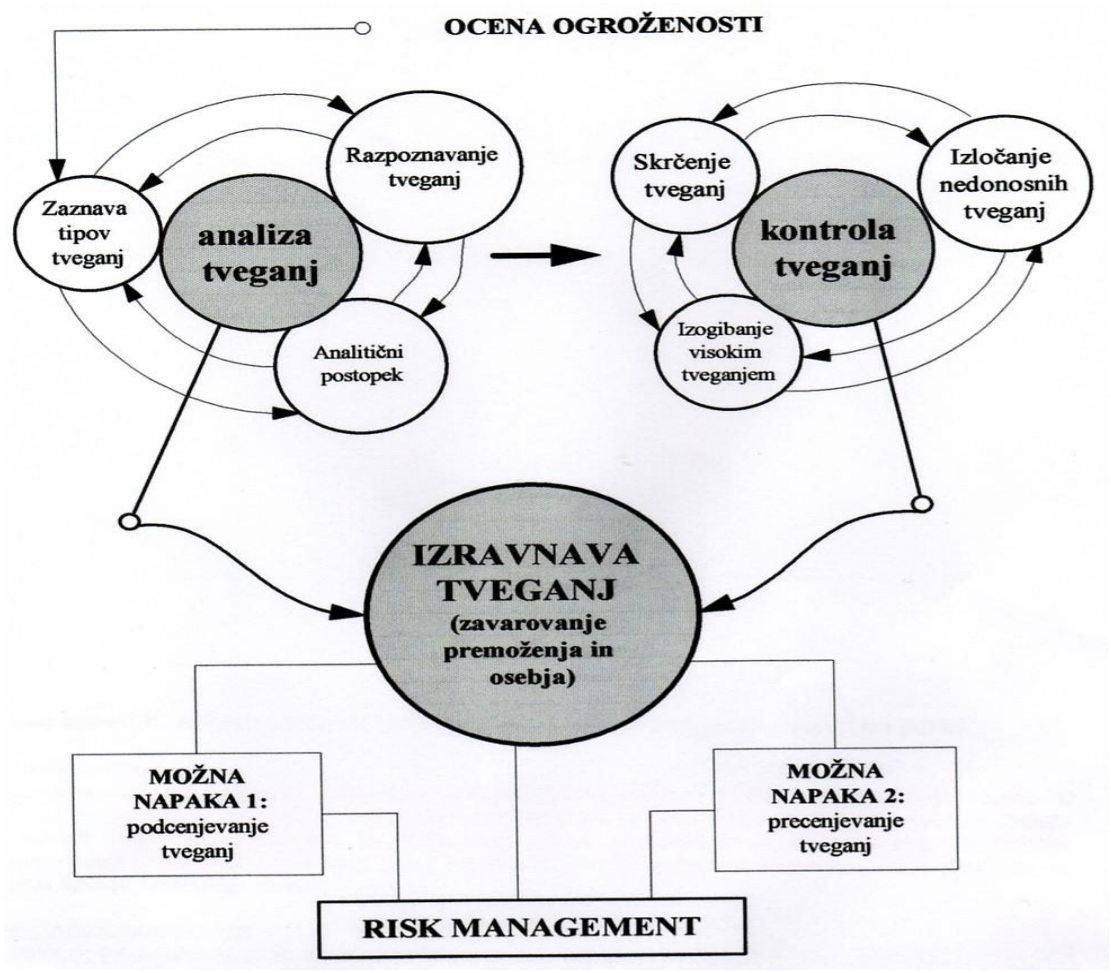
Prepoznavanje vseh vrst tveganj (tudi varnostnih) je eno od najzahtevnejših managerskih opravil, zato je vsak pripomoček dobrodošlo orodje za tovrstna managerska opravila. V

nadaljevanju zato predstavljamo še splošni model, ki dopolnjuje razumevanje pomena ocenjevanja tveganj, saj vključuje vse potrebne osnovne aktivnosti pri obvladovanju tveganj v KI. Splošni model ponazarja tri glavne sklope obvladovanja tveganj, ki so: analiza tveganj, kontrola tveganj in izravnava tveganj z zavarovanjem.

»Prvi korak v analizi varnostnih in drugih tveganj je zaznava in prepoznava groženj in ranljivosti« (Fisher/Green, 1998:169). V splošnem modelu je to analiza tveganj s prvim korakom, ki ga imenujemo zaznava tipov tveganj. Pri zaznavi gre za zavedanje o obstoju tveganj, ki jih povzročajo ranljivost in ogroženost poslovnega sistema. Temeljito poznavanje in zavedanje ranljivih točk v poslovnih procesih in v varnostnih mehanizmih bi morali lastnikom in managementu povzročati nelagoden občutek in potrebo po ustreznem odzivanju.

Pri drugem koraku analize tveganj, ki je označen kot prepoznavanje tveganj, je potrebno ugotoviti od kje tveganje izhaja: iz človekovega, tehnično-tehnološkega ali iz naravnega okolja.

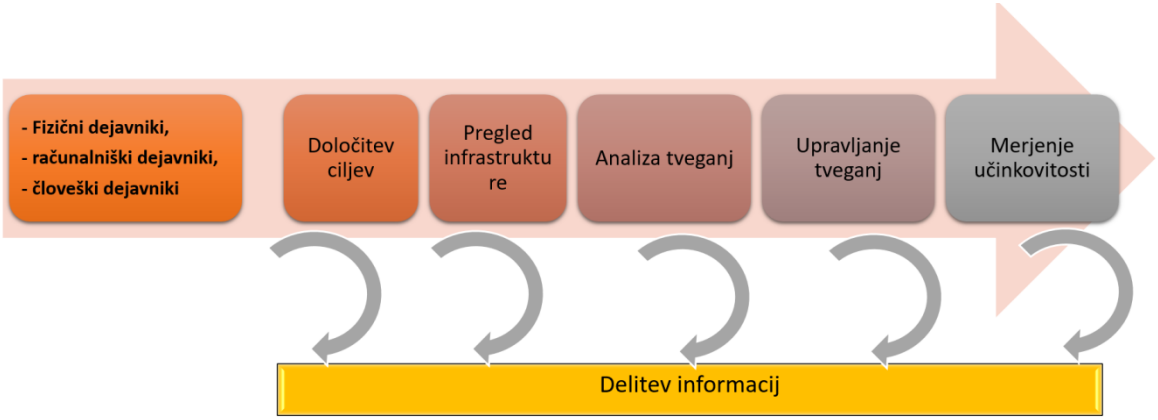
Uporaba analitičnega postopka kot tretjega koraka v analizi tveganj je namenjena razvrstitvi tveganj na tveganja, ki pomenijo hazardiranje (vse dobiš ali vse izgubiš), na ekstremna in zelo visoka tveganja, ki so predmet zavarovanja, na visoka, nizka in zelo nizka (neznatna) tveganja, ki so predmet obvladovanja s procesom upravljanja s tveganji, tako imenovanega risk managementa.



Slika 8: Splošni model za obvladovanje tveganj (Vršec, 1993, 2010)

Drugi sklop obvladovanja tveganj je kontrola tveganj, s katero poskušamo tveganja skrčiti, nekatera izločiti, nekaterim tveganjem pa se preprosto izogniti. Če je analiza tveganj dobro pripravljena, potem je dokaj preprosto izločiti tista tveganja, ki predstavljajo hazardiranje. Sprejemljiva (visoka, nizka in zelo nizka) tveganja, ki so organizacijsko, kadrovsko, strokovno, poslovno in finančno obvladljiva uvrstimo v procese poslovanja in odločanja. Ekstremna in zelo visoka tveganja (visoke rizike) pa prepustimo zavarovanju, torej zavarovalnim storitvam zavarovalnic. Pri tretjem sklopu obvladovanja tveganj, gre torej za izravnavo tveganj, kar pomeni neposredno sodelovaje z zavarovalnicami, ki za primerno zavarovalno premijo prevzamejo upravljanje tveganj (rizikov). Zavarovanje ekstremnih in visokih varnostnih in drugih rizikov uporabnik zavarovalnih produktov sklene pri tistih zavarovalnicah, ki so se pripravljene pogajati o višini zavarovalnih premij. Gre namreč za razne ugodnosti in popuste, ki jih lahko nudijo zavarovalnice, ko gre za organizirano upravljanje tveganj z zavarovanjem in za kakovostne varnostne mehanizme pri zavarovalcu.

V nadaljevanju je prikazan uporaben pristop National Infrastructure Protection Plan USA (NIPP, 2013) za obvladovanje tveganj KI, prikazan na sliki 9. Okvir za obvladovanje tveganj omogoča vključevanje strategij, zmogljivosti in strukture upravljanja za sprejemanje odločitev o tveganjih, povezanih s KI. Pristop se lahko uporablja za vse grožnje in nevarnosti, vključno s kibernetskimi incidenti, naravnimi katastrofami, nevarnostmi, ki jih povzroči človek in terorističnim dejanjem.



Slika 9: Okvir za obvladovanje tveganj na področju KI (prirejeno po NIPP, 2013)

Poleg tega pristopa pri obvladovanju tveganja podpira postopek ocenjevanja nevarnosti in tveganja še metodologija THIRA (Hazard Identification and Risk Assessment, NIPP, 2013). Navedena metodologija je ena izmed mnogih, ki vključuje prepoznavanje groženj in nevarnosti, njihov vpliv na družbeno skupnost, ter določa, kako najbolje ublažiti te grožnje in nevarnosti na podlagi trenutnih zmogljivosti ter zahtev glede virov.

Številne organizacije KI in industrijski partnerji uporabljajo še druge metodologije za upravljanje tveganj, ki so lahko podrobnejše in pogosto prilagojene njihovim posebnim potrebam. Zgornji okvir za obvladovanje tveganj jih ne namerava nadomestiti. Namesto tega podpira skupen in poenoten pristop k obvladovanju tveganj, ki ga lahko vsi ključni infrastrukturni partnerji uporabljajo in povezujejo s svojimi lastnimi metodologijami in dejavnostmi upravljanja tveganj. Upravljanje tveganj se lahko prilagodi in uporablja na sredstvih, sistemu, omrežju ali funkcionalni osnovi, odvisno od njihovih temeljnih značilnosti in narave povezane infrastrukture.

Zgoraj opisani pristop za obvladovanje tveganj (NIPP, 2013) vključuje naslednje aktivnosti:

- določanje ciljev poslovanja: specifični rezultati poslovanja, pogoji, končni cilji uspešnosti, ki skupaj opisujejo učinkovito upravljanje tveganj,
- identificiranje infrastrukture: opredeljevanje sredstev, sistemov in omrežij, ki prispevajo h kritični funkcionalnosti in zbirajo informacije, povezane z upravljanjem tveganj, vključno z analizo odvisnosti in soodvisnosti,

- pristop k ocenjevanju tveganj: upoštevajoč morebitne neposredne in posredne posledice izrednega dogodka, znane ranljivosti za različne potencialne grožnje ali nevarnosti ter splošne ali specifične informacije o nevarnosti,
- izvajanje aktivnosti upravljanja tveganja: sprejemanje odločitev in izvajanje pristopov za nadzor, sprejem, prenos ali preprečevanje tveganj - pristopi lahko vključujejo dejavnosti preprečevanja, zaščite, ublažitve, odzivanja in obnove,
- merjenje učinkovitosti: uporaba meritev in drugih postopkov ocenjevanja za merjenje učinkovitosti preventivnih ukrepov in postopkov za dvig odpornosti KI.

Ta pristop podpira integriran in kontinuiran proces s povratnimi zankami in večkratnimi ponavljajočimi koraki. Upravljavcu KI omogoča, da spremlja napredek in izvaja ukrepe za povečanje odpornosti KI. Fizične, kibernetske in človeške elemente KI je treba obravnavati kot del vsakega pristopa za upravljanje tveganj.

V nadaljevanju je opisano določanje ciljev poslovanja, ocenjevanje tveganj in pristop k upravljanju tveganj.

Določanje ciljev poslovanja

Cilji se bodo razlikovali med sektorji in organizacijami, odvisno od območja tveganja, delovnega okolja in sestave določene industrije, vira ali drugega vidika KI. Na nacionalni ravni je splošni cilj upravljanja tveganj za delovanje KI povečana zanesljivost, varnost in odpornost, dosežena z izvajanjem preventivnih ukrepov in aktivnosti znotraj, ter med sektorji, in na ravni Vlade RS. Cilji so zlasti:

- ocenjevati in analizirati grožnje, ranljivosti in posledice za KI,
- zagotoviti zanesljivo zaščito KI pred človeškimi, fizičnimi in kibernetskimi grožnjami, hkrati pa upoštevati stroške in koristi naložb za preventivo,
- izboljšati odpornost KI z zmanjševanjem škodljivih posledic izrednih dogodkov s pomočjo predhodnega načrtovanja in učinkovitih odzivov za reševanje življenj in sredstev ter zagotovitev hitrega obnavljanja bistvenih storitev,
- deliti pomembne informacije med sektorji KI, da bi povečali ozaveščenost in omogočili sprejemanje odločitev o upravljanju tveganj,
- spodbujati učenje in prilagajanje med vajami in po izrednih dogodkih,
- omogočiti razvoj sektorskih profilov tveganja. Ti profili tveganja opisujejo največja tveganja, s katerimi se soočajo različni sektorji,
- določiti najboljše ukrepe in postopke za zmanjšanje možnih posledic, groženj in/ali ranljivosti ter posledično zmanjšanje tveganj. Nekatere razpoložljive možnosti vključujejo spodbujanje prostovoljnega izvajanja strategij za upravljanje tveganja (npr. preko javno - zasebnih partnerstev), uporaba standardov in najboljših praks, izvajanje

politik in programov, povezanih z gospodarskimi spodbudami in po potrebi dodatno izmenjavo informacij,

- obveščati o upravljanju tveganj in možnostih dodeljevanja sredstev, ne pa le določanja zahtev za lastnike in upravljavce KI,
- razmisliti o sredstvih, sistemih, omrežjih, funkcijah, operativnih procesih, poslovnem okolju in pristopih za upravljanje tveganj.

Infrastrukturni partnerji na podlagi zakonov in svojih posebnih pogojev poslovanja, poslovnih modelov in s tem povezanih tveganj, ocenijo tveganja, ki so jim izpostavljeni. Partnerji, tako javni kot zasebni, prepoznajo infrastrukturo, za katero menijo, da je bistvena za njihovo delovanje in si prizadevajo za izboljšanje njene zaščite ter odpornosti.

KI obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi (ZKI, 2017).

Pristop k ocenjevanju tveganj

Tveganje za delovanje KI je mogoče oceniti z vidika verjetnosti ogrožanj in morebitnih posledic. Skupne opredelitve, scenariji, predpostavke, meritve in postopki lahko zagotovijo, da ocene tveganja prispevajo k skupnemu razumevanju med upravljavci KI. Pristop k upravljanju tveganj (opisan v nadaljevanju) podpira strategijo ocenjevanja, ki temelji na scenarijih možnih izrednih dogodkov, njihovimi posledicami in oceno verjetnosti, da se bo pojavila grožnja ali nevarnost ter posledično določen izredni dogodek.

Pristop k upravljanju tveganj

Upravljavci KI izvajajo ocene tveganj za doseganje ciljev poslovanja in svojih potreb pri sprejemanju odločitev, pri čemer uporabljajo široko paleto metodologij. Enostavne metodologije bodo bolj verjetno izpolnjevale zahteve glede preglednosti in praktičnosti. Metodologije tveganj so pogosto združene v kvalitativne in kvantitativne kategorije, vendar pa lahko, ob dobro načrtovanih obeh vrstah ocen, omogočata uporabne analitične rezultate. Podobno so tako kvalitativne kot kvantitativne metodologije lahko nepotrebno zapletene ali slabo oblikovane. Metodologija, ki najbolj ustreza potrebam odločevalca, je na splošno najboljša izbira, bodisi kvantitativna ali kvalitativna. Ob spoznanju, da se številne metodologije ocenjevanja tveganj razvijajo v dinamičnem okolju, analitična načela za metodologije ocenjevanja tveganja služijo kot vodilo pri prihodnjih prilagoditvah. Osnovna analitična načela zagotavljajo, da so ocene tveganja:

- dokumentirane: metodologija in ocena tveganja morata biti jasno dokumentirani, navedeno mora biti katere informacije se uporabljajo in kako se sintetizirajo, da bi izdelali oceno tveganja. Vse predpostavke, obtežilni faktorji in subjektivne presoje morajo biti pregledne za uporabnike metodologije, za katere se pričakuje, da bodo uporabili rezultate, jasna mora biti vrsta odločitve in časovni okvir ocenjevanja,
- ponovljive: metodologija mora ustvariti primerljive, ponovljive rezultate, čeprav lahko ocene različnih infrastruktur izvajajo različni analitiki ali skupine analitikov. Treba je čim bolj zmanjšati število in vpliv subjektivnih sodb,
- preventivne: metodologija tveganja mora logično vključiti njene komponente, ustrezno uporabljati strokovne discipline, ki so pomembne za analizo, brez pomembnih napak ali opustitev. Analizirati je treba negotovost, povezano z ocenami posledic in zaupanjem v ocene ranljivosti ter nevarnosti.

Ocene tveganja bi morale zajemati tudi scenarije tveganj in jih razdeliti na dele, ki jih je mogoče oceniti in analizirati posamezno. Scenarij je hipotetični položaj, ki ga sestavlja ugotovljena grožnja ali nevarnost, subjekt, na katerega vpliva ta nevarnost in povezani pogoji, vključno s posledicami, kadar je to primerno. Kadar analitiki razvijajo verjetnostne scenarije za ugotavljanje morebitnih tveganj za oceno, mora vrsta scenarijev zajeti celoten obseg ocenjevanja in oblikovalcu odločanja zagotoviti čim bolj popolne informacije. Pri relativno določenem sistemu je pomembno, da se identificirajo tiste komponente ali kritična vozlišča, kjer bi bile morebitne posledice najvišje in kjer je mogoče usmeriti varnostne in preventivne aktivnosti. Analitiki morajo biti pozorni na rezultate, vključno z več scenariji, ki vsebujejo isti dogodek, ta pa lahko povzroči dvojno tveganje.

Tako slovenska, kot tudi mednarodna KI predstavlja potencialne glavne tarče za nasprotnike. Ocene groženj in tveganj morajo obravnavati različne elemente tako naravnih, človeških ali kibernetskih groženj KI, odvisno od vrste in cilja napada. Ocene tveganj temeljijo na zgodovinskih podatkih in prihodnjih napovedih o naravnih nesrečah ali aktivnostih človeka, da bi ocenili verjetnost ali pogostost različnih nevarnosti. To je področje, na katerem različni organi Vlade RS sodelujejo s sektorji KI, lastniki in upravljavci, da bi lahko ocenili kakršnokoli nevarnost. Ocene nevarnosti vse bolj upoštevajo dejavnike, kot so vplivi staranja infrastrukture in podnebne spremembe na splošno varnost in zanesljivost poslovanja.

Ocena posledic izrednega dogodka vključuje:

- javno zdravje in varnost: učinek na človeško življenje in telesno počutje (npr. smrtne žrtve, poškodbe, bolezni),
- ekonomski: neposredne in posredne gospodarske izgube (npr. stroški za obnovo sredstev, stroški za odzivanje na izredni dogodek, stroški prodajnih tokov zaradi

motenj dobave proizvoda ali storitve, dolgoročni stroški zaradi okoljske škode, izguba ugleda ipd.),

- psihološki: vpliv na zaupanje splošne in strokovne javnosti v gospodarske ter politične institucije države. To zajema tiste spremembe v dojemanju, ki se pojavijo po velikem izrednem dogodku, ki vpliva na občutek varnosti in blaginje javnosti in se lahko manifestira v zmotnem vedenju,
- učinek upravljanja: vpliv na zmožnost Vlade RS ali industrije, da zagotovi minimalne bistvene javne storitve, zagotovi javno zdravje in varnost ter izvaja aktivnosti, povezane z varnostjo in javnim redom.

Analiza posledic mora obravnavati neposredne in posredne učinke (tako finančne kot človeške). Veliko sredstev, sistemov in omrežij je medsebojno odvisno od povezave z drugimi KI za delovanje. Na primer, skoraj vsi sektorji se zanašajo na zagotavljanje bistvenih funkcij npr. energije, komunikacij, prevoza in vode. V mnogih primerih bo okvara enega sredstva ali sistema vplivala na zmožnost medsebojno povezanih sredstev ali sistemov v istem ali drugem sektorju za opravljanje potrebnih funkcij. Poleg tega kibernetska soodvisnost predstavlja edinstvene izzive za vse sektorje zaradi brezmejne narave kibernetskega prostora. Soodvisnosti so dvojne narave. Na primer, energetski sektor se zanaša na zanesljivo delovanje računalniškega sistema za upravljanje elektroenergetskega omrežja, računalniški sistem pa ne deluje brez električne energije.

Celovita analiza posledic obravnava večnamenske KI povezave za potrebe ocene tveganja. Raven podrobnosti in specifičnosti, doseženih z uporabo najsodobnejših modelov ocene tveganja in simulacij, morda ne bodo praktična ali potrebna za vsa sredstva, sisteme ali omrežja. V teh okoliščinah lahko poenostavljena analiza odvisnosti in medsebojne soodvisnosti, ki temelji na temeljiti strokovni presoji, zagotovi dovolj vpogleda v pravočasne odločitve o upravljanju tveganj.

Obstaja tudi element negotovosti, ki je posledica ocen nevarnosti. Tudi kadar je jasno naveden in dosledno uporabljen scenarij z razumnimi najslabšimi pogoji, ob subjektivni oceni, obstaja vrsta možnih rezultatov, ki bi se lahko pojavili. Za nekatere dogodke je obseg posledic majhen in preprosta ocena lahko zagotovi zadostne informacije za podporo odločitev. Če je obseg rezultatov velik, lahko scenarij zahteva več specifičnosti pogojev za pridobitev ustreznih ocen rezultatov. Če pa se scenarij razčleni na razumno stopnjo razvejenosti in še vedno obstaja velika negotovost, bi morala ocena tveganja spremljati celoten obseg negotovosti, ki vpliva na odločanje. Najboljši način sporočanja negotovosti bo odvisen od dejavnikov, ki pomembno vplivajo na možen negativen rezultat, ali pa tudi glede količine in vrste informacij, ki so na razpolago.

Rezultati ocene tveganja za delovanje KI pogosto govorijo o izbiri in izvajanju ukrepov ter postopkov za blažitev posledic ter o določitvi prednostnih nalog za upravljanje s tveganji za lastnike in upravljavce KI. Izbira in izvajanje ustreznih aktivnosti za obvladovanje tveganj se nanaša na načrtovanje, povečanje usklajevanja in podpira učinkovito dodeljevanje sredstev ter na odločitve o upravljanju izrednih dogodkov. Primerjava in dajanje prednosti tveganjem, s katerim se soočajo različni subjekti, pomaga ugotoviti, kje je najbolj potrebno zmanjšanje tveganja in pomaga utemeljiti izbiro stroškovno učinkovitih možnosti upravljanja tveganj. To podpira odločitve o dodeljevanju sredstev, usmerja naložbe in poudarja ukrepe, ki ponujajo njihovo največjo donosnost. Zagotavlja tudi osnovo za razumevanje možnih koristi zmanjševanja tveganja, ki se uporabljajo za obveščanje o načrtovanju in odločanju o virih.

Upravljavci KI uporabljajo različne pristope pri upravljanju tveganj, odvisno od njihovih lastnikov, potreb sektorja, regionalnih tveganj, varnostnih pristopov in poslovnega okolja. Na primer, lastniki in upravljavci KI imajo na voljo različne možnosti, da bi zmanjšali tveganje. Programi, namenjeni zmanjšanju ogroženosti KI, bodo prioritetne naložbe, ki varujejo fizična sredstva ali zagotavljajo odpornost na izredne dogodke, odvisno od tega, katera možnost najbolje omogoča stroškovno učinkovito upravljanje tveganj za delovanje KI.

Lastniki in upravljavci KI dajejo prednost in izvajajo dejavnosti za zmanjševanje tveganja na podlagi njihove stroškovne učinkovitosti, izvedljivosti in možnosti za zmanjšanje tveganja. Ukrepi za upravljanje tveganj vključujejo postopke in aktivnosti, namenjene odvračanju, zmanjševanju ranljivosti zaradi izrednega dogodka, zmanjševanju posledic in omogočajo pravočasen, učinkovit odziv ter obnovo po izrednem dogodku. Pristop za obvladovanje tveganj se osredotoča na tiste dejavnosti preprečevanja, zaščite, zmanjšanja, odziva in obnove, ki prinašajo največjo donosnost naložb, in ne zgolj zmanjšanje ranljivosti, ki jo je treba doseči. Varnostne aktivnosti se razlikujejo med sektorji.

Dejavnosti upravljanja tveganja vključujejo tudi sredstva za zmanjšanje posledic izrednega dogodka. Ti ukrepi so osredotočeni na ublažitev, odziv in / ali okrevanje. Pogosto je stroškovno učinkovitejše, da se pravočasno preventivno namenijo sredstva za povečanje varnosti in odpornosti sistemov ter omrežij, kot pa, da se sredstva namenijo za obnovo po izrednem dogodku. Skladno s tem morajo upravljavci KI razmisliti o tem, kako je mogoče učinkovito upravljati tveganja, robustnost in ustrezne izboljšave fizične ter kibernetske varnosti, to pa vključiti v načrtovanje in izgradnjo nove KI ter prenovo ali popravilo obstoječe infrastrukture. V razmerah, kjer sta robustnost in odpornost ključnega pomena za upravljanje KI, je morda bolj učinkovito izvajati preventivne programe na sistemski ravni, ne pa na ravni posameznega dela KI.

Pri ocenjevanju možnosti upravljanja tveganj se mora upoštevati industrijske standarde in najboljše prakse, ukrepe in aktivnosti, ki se učinkovito uporabljajo v drugih sistemih in

sorodnih industrijskih ali drugih panogah ter pridobljene izkušnje iz dejanskih dogodkov ali vaj. Možnosti za upravljanje tveganj bi morale biti dovolj podrobne, da bi opredelile, v kolikšni meri bodo zmanjšale elemente tveganja in oceniti stroške življenjskega cikla vsake možnosti (npr. začetne naložbe ali zagon, delovanje in vzdrževanje, možnosti rušenja in odstranjevanja, ko se je njihova uporabnost končala). Izkoriščanje pozitivnih sinergij in izogibanje negativnim omogoča izbiro stroškovno učinkovitih možnosti za zmanjšanje tveganja. Učinkovite aktivnosti upravljanja tveganj so celovite, usklajene in stroškovno učinkovite. Odločitve o upravljanju tveganj je treba sprejeti na podlagi analize stroškov in drugih vplivov ter predvidenih koristi zaradi smeri ukrepanja, vključno z alternativo brez ukrepanja, če se šteje, da je tveganje že učinkovito upravljano. Pomembno je opozoriti, da se lahko ukrepi za upravljanje tveganj ovrednotijo na podlagi celotnega razpona scenarijev možnih izrednih dogodkov, pa tudi njihove sposobnosti za obvladovanje tveganj, povezanih z enim samim scenarijem; ohranjanje obeh perspektiv je ključnega pomena pri določanju najučinkovitejših ukrepov.

Uporaba meritev učinkovitosti je pomemben korak v procesu upravljanja tveganj za delovanje KI, saj se s tem omogoča ocena izboljšav glede varnosti in odpornosti. Meritve učinkovitosti omogočajo upravljavcem in lastnikom KI, da spremljajo napredek glede na prednostne naloge in cilje. Zagotavljajo osnovo, da se zagotovi pristojnost in odgovornost, dokumentira dejansko učinkovitost, spodbuja učinkovito upravljanje in zagotovi povratne informacije.

Z meritvami učinkovitosti za doseganje nacionalnih in sektorskih prednostnih nalog lahko KI prilagaja svoje varnostne pristope, upošteva doseženi napredek in spremembe možnega ogrožanja. Matrike se uporabljajo za usmerjanje pozornosti na področja varnosti in odpornosti, ki upravičujejo dodatna sredstva ali druge spremembe z analizo izzivov in prednostnih nalog na nacionalni, sektorski in lastniški ravni. Lahko obveščajo o napredku glede na nacionalne in sektorske cilje ter zagotavljajo informacije analitikom, da prilagodijo svoje ocene tveganja.

2.3 RAZLIČNI POGLEDI NA UPRAVLJANJE TVEGANJ

Različni avtorji so predstavili tudi različne tipologije tveganj glede na izvor tveganj (naravno, tehnološko), časovno dimenzijo (akutna, kronična), način izpostavljenosti (zrak, voda ipd.), vrsto posledic (poškodbe, smrti) ipd. Bolj znane so tipologije, ki so jih predlagali Rowe, 1977; Hohenseimer, Kasperson in Kates, 1982; Slovic, Fischoff in Lichtenstein; 1985; Winterfeldt in Edwards, 1984 (po Mitar, 1995), metoda Haimesa in drugih RFRM (Risk Filtering and Ranking Method, 2002) ter model Santosa IIOM (Inoperability Input-Output Model, 2005).

Za proučevanje tveganj so avtorji pogosto uporabili različne sistemske modele, v katerih so opredelili razmerja med enotami in procesi ter oblikovali vzročne modele, ali deterministične ali verjetnostne. Znani so model Hohenseimerja, Kaspersona in Katesa, 1982; Soderstromov model, 1984 in model Renna in sodelavcev, ki je skušal integrirati različne dimenzije tveganja (1992, po Mitar, 1995). Slednji ni opredelil zakonov vzročnosti, ampak je opredelil vzročni proces (tvegan dogodek, viri in kanali okrepitve, družbene in individualne točke okrepitve, skupinski in individualni odzivi, širjenje posledic, učinki) v primerjavi s teorijo komunikacij, ki obravnava izvor, prenos in sprejem signalov.

V nasprotju z vzročnimi modeli, ki naj bi podajali opis tveganja, so procesni modeli, ki predpisujejo proces oziroma korake, ki jih je treba izvesti za dosego določenih ciljev. Najbolj znani so petstopenjski model ocenjevanja tveganja (Rowe, 1977), štiristopenjski model družbenega upravljanja tveganja (NRC, 1983), analiza odločanja večjega števila vključenih (Winterfelds), splošni program upravljanja ogrožanj (Kasperson in sodelavci, 1985), idealizirana shema analize tveganj (Crouch in Wilson, 1982) ter drugi (po Mitar, 1995).

Pojasnitve so lahko individualistične (začetna točka je posameznik) ali pa kontekstualistične (začetna točka so okoliščine, to je skupina, organizacija, življenjski slog ipd.). Primeri individualističnih pojasnitev so teorija znanja[4], teorija osebnosti[5], kognitivna teorija tveganja in ekonomska teorija pričakovane koristnosti.

Vsi družbeni sistemi poskušajo zmanjšati kompleksnost in izbrati področja dejavnosti, ki obetajo koristno uporabo omejenih virov. To je še posebej značilno v primeru soočanja s tveganji. Družbeni sistemi opredeljujejo kriterije, ki omogočajo opredelitev prednostnih akcij in zanemarjanje manj pomembnih tveganj. Zaradi tega se zastavljajo vprašanja o kriterijih za obravnavo tveganja. Nacionalna znanstvena fundacija (National Science Foundation USA) je opredelila deset osnovnih vprašanj v zvezi z ocenjevanjem in upravljanjem tveganja, ki so aktualna še danes (1979, po Goldingu, 1992: 28):

- kako določimo, koliko varno je dovolj varno,
- kako ustrezne so baza znanja in metode ocenjevanja tveganja v zvezi z različnimi tehnologijami,
- kako so ocene tveganja vključene v proces odločanja,
- kako odločevalci obravnavajo negotovosti različnih tveganj in ogrožanj,
- kako značilnosti institucij vplivajo na organe, ki odločajo o tveganjih in ogrožanjih,
- kateri dejavniki vplivajo na zaznave tveganj in koristi posameznikov,
- kako so zaznave tveganj in koristi posameznikov vključene v javno politiko,
- kako družba obravnava tveganja, ki so nesprejemljiva za določen del družbe,

[4] Soočanje posameznika s tveganjem je pogojeno z njegovim znanjem in informacijami o tem.
[5] Posamezniki so nagnjeni k tveganjem ali izogibanju tveganju odvisno od tipa osebnosti.

- kako so normativne presoje (nepristranost, pravičnost) uravnotežene v procesu odločanja o tveganju,
- kateri so kriteriji za primerjavo in ovrednotenje različnih politik upravljanja?

Navedenim vprašanjem sta bili dodani dve izrazito družboslovni tematiki, in sicer: tematika komunikacije o tveganjih in tematika družbenega ter kulturnega konteksta tveganja (Golding, 1992: 27–28). K temu se lahko doda še vprašanji, ali naj družba sprejme določene enotne kriterije za soočanje z vsemi vrstami tveganj, ne glede na okoliščine, in, kdo naj bi bil odgovoren, če se izkaže, da so kriteriji napačni (Renn, 1992: 55).

Odgovori na zgornja vprašanja so pogojeni s perspektivami različnih ocenjevalcev. Če gledamo na tveganje kot na objektivno značilnost dogodka ali aktivnosti, ki jo je mogoče nedvoumno meriti (verjetnost in posledice), potem so ugotovitve za izbor politike jasne, ker objektivno razvrščanje tveganj določa porazdelitev virov.

Obstaja več klasifikacij tveganja, narejenih na podlagi različnih kriterijev. Vse te omogočajo določene vpoglede, vendar jih v bistvu ocenjujemo kot delno enostranske, saj v večini primerov ne obravnavajo predpostavk posameznih pristopov. V znanosti je bilo že nekaj poskusov izoblikovanja interdisciplinarne taksonomije pogledov na tveganje. Bradburry (1989), ki je razlikoval dve vrsti konceptov tveganja (tveganje kot fizična lastnost, tveganje kot družbena konstrukcija), May (1989) je razlikoval tri perspektive (kulturna, individualna izbira, sistemski pristopi), Dietz, Fray in Rosa (1992, po Mitar, 1995: 195) so razlikovali pet perspektiv (tehnična, psihološka, sociološka, antropološka in geografska). Vse te klasifikacije so bolj deskriptivne kakor analitične, saj obstajajo različni teoretični in metodološki pristopi k obravnavi tveganj. Čeprav klasifikacija nujno ne daje nekega skupnega imenovalca, pa je lahko okvir za primerjavo in analizo različnih pogledov na tveganje. Zanimiva je Rennova klasifikacija (1992: 56):

- zavarovalniški pristop, vključno s statističnimi napovedmi,
- toksikološki in epidemološki pristop, vključno z ekotoksikologijo,
- inženirski pristop, vključno z verjetnostno oceno tveganj,
- ekonomski pristop, vključno z analizo in primerjavo tveganj ter koristi,
- psihološki pristop, vključno s psihometrično analizo,
- družbene teorije tveganja.

Za vse navedene pristope je značilno, da na različen način opredelijo osnovno izhodišče, instrumentalno in družbeno funkcijo, metodologijo in merske pripomočke. Vse pa imajo vsaj eno skupno točko, to je razlikovanje med dejanskostjo in možnostjo (Markowitz, 1991; Evers and Nowotny, 1987, po Mitar, 1995). Če je prihodnost vnaprej določena ali neodvisna od posameznikovih prizadevanj, potem pojem tveganja nima smisla. Če to razlikovanje med dejanskim in možnim sprejmemo, potem pojem tveganja označuje možnost uresničitve

neželenega stanja ali kot rezultat naravnih dogajanj ali pa posameznikove aktivnosti. Ta definicija predpostavlja, da lahko posameznik opredeli vzročne povezave med akcijami in njihovimi učinki, prav tako pa tudi možnost izogibanja ali spreminjanja neželenih učinkov. Na eni strani vključuje analizo vzročno - posledičnih razmerij, na drugi strani pa predpostavlja vpliv (lahko tudi vzroke) na določene posledice.

Iz navedenega je razvidno, da pojem tveganja vsebuje vsaj tri bistvene elemente, in sicer: (i) neželene posledice, (ii) možnost pojavljanja ter (iii) sodbe o dejanskosti. Za pojasnitev teh elementov je treba odgovoriti na tri vprašanja: (i), kako lahko določimo in merimo negotovosti, (ii), kaj so neželene posledice, in (iii), kaj so predpostavke o stvarnosti (Renn, 2008). Odgovori (konceptualizacija negotovosti, obseg neželenih posledic, možnost spoznanja stvarnosti) lahko služijo kot vodilo za razlikovanje različnih pogledov na upravljanje tveganj.

2.4 PREGLED RAZLIČNIH VIDIKOV UPRAVLJANJA TVEGANJ

2.4.1 Tehnični vidik upravljanja tveganj

Kot tehnične pristope lahko obravnavamo zavarovalniški pristop, oceno tveganj za zdravje in okolje ter verjetnostno oceno tveganj (Renn, Concepts of Risk: A Classification, 1992: 58). Značilnost teh pristopov je, da predvidijo določeno fizično škodo (za posameznike in okolje), izračunajo povprečje v času in prostoru ter uporabijo relativne frekvence (empirične in hipotetične) za opredelitev verjetnosti. Normativne implikacije pristopa so jasne. Če je fizična škoda opredeljena kot nezaželena (vsaj za večino posameznikov in družbo kot celoto), potem je tehnična analiza potrebna za razkritje, izogibanje ali modificiranje vzrokov, ki lahko pripeljejo do neželenih posledic. Prav tako se analiza lahko uporabi za zmanjševanje posledic, če so vzroki še neznani ali če nanje ni mogoče vplivati. Ti pristopi so bili izpostavljeni kritiki družbenih ved (Renn, 1992: 59), zato ker ne upoštevajo: (i), da je zaznava neželenih posledic pogojena z vrednotami posameznikov, (ii), da so interakcije med aktivnostmi in posledicami bolj kompleksne, kakor domnevajo te analize, (iii), da so organizacije, ki ocenjujejo in upravljajo tveganja lahko tudi same zmotljive in lahko prispevajo k povečanju tveganja ter (iv), da v praksi ni mogoče enakopravno kvantitativno obravnavati dogodkov z majhno verjetnostjo in visoko škodo v primerjavi z dogodki z visoko verjetnostjo in majhno škodo.

Menimo, da so navedene kritike utemeljene toliko, kolikor tehnične analize predstavljajo okvir, ki pa ne more biti edini kriterij za opredelitev, ovrednotenje in upravljanje tveganj. Vendar je ozkost pristopa hkrati šibkost in moč pristopa. Če se izloči samo določena lastnost tveganja (fizična škoda) iz celotnega konteksta tveganja, s tem postane koncept

enodimenzionalen, vendar univerzalno uporaben. Če se analiza omeji na nezaželene fizične posledice, se zanemarijo še druge škode in je fizična škoda tista, o kateri obstaja soglasje v večini organizacij. Izključitev drugih posledic iz konteksta tveganja zagotavlja tehničnim analizam preverljivost in primerljivost, vendar na škodo premajhnega proučevanja procesa družbenega obravnavanja tveganja.

2.4.2 Ekonomski vidik

V izhodišču vseh družboslovnih pristopov je spoznanje, da so vzroki in posledice tveganj posredovani skozi družbene procese. Ekonomski pristop je najbližji tehničnim pristopom, vendar pa se namesto fizične škode za izhodišče analize upoštevajo subjektivne koristi. Osnovna enota je subjektivna koristnost, ki opiše stopnjo (ne)zadovoljstva z mogoče akcijo ali transakcijo. Premik od pričakovane škode k pričakovani koristi služi dvema namenoma: (i) subjektivno (ne)zadovoljstvo omogoča merjenje vseh posledic, tudi psiholoških in družbenih, ne pa samo fizičnih; (ii) »osebno zadovoljstvo« omogoča neposredno primerjavo tveganj in koristi med različnimi možnimi aktivnostmi. Tako je koncept koristnosti širši kot koncept pričakovane škode, vendar je še vedno enodimenzionalen in univerzalen.

Čeprav ekonomski pogled daje enodimenzionalno mero, ki naj bi omogočala primerjavo tveganj in koristi, obstaja problem sinteze individualnih koristnosti, obstoj individualnih preferenc o verjetnosti, problem eksternalizacije posledic na tretje stranke, predpostavka racionalnega posameznika, ki odloča, in utilitarna etika. Ker se koristi izračunavajo v denarnih enotah, je upravičen očitek, da nekaterih škod (izguba življenja, zdravja, ugleda, zaupanja) ni mogoče (iz etičnega zornega kota prav gotovo ne, Aristotel, 1968) izraziti v denarnih enotah. Kljub očitkom pa ekonomski pristopi bistveno prispevajo k procesu oblikovanja politik tveganja, ker: (i) zagotavljajo tehnike in instrumente za merjenje ter primerjavo koristnosti dobičkov različnih možnih aktivnosti; (ii) razširjajo tehnične analize z vključitvijo nefizičnih dimenzij tveganja; (iii) zagotavljajo tehnike za merjenje tveganja in koristi z isto enoto, če predpostavimo, da trg kaže družbeno koristnost; (iv) vključuje modele za racionalno odločanje, ob predpostavki, da je mogoče doseči soglasje med posamezniki, ki odločajo.

Ekonomski koncept tveganja temelji na verjetnostih, družbeni definiciji neželenih učinkov na podlagi individualnih koristnosti in na obravnavi teh kot dejanskih dobičkov ali izgub. V nasprotju s tehničnimi pristopi, verjetnosti niso opredeljene samo kot relativne frekvence, ampak tudi kot moč prepričanja (Renn, 1992: 64).

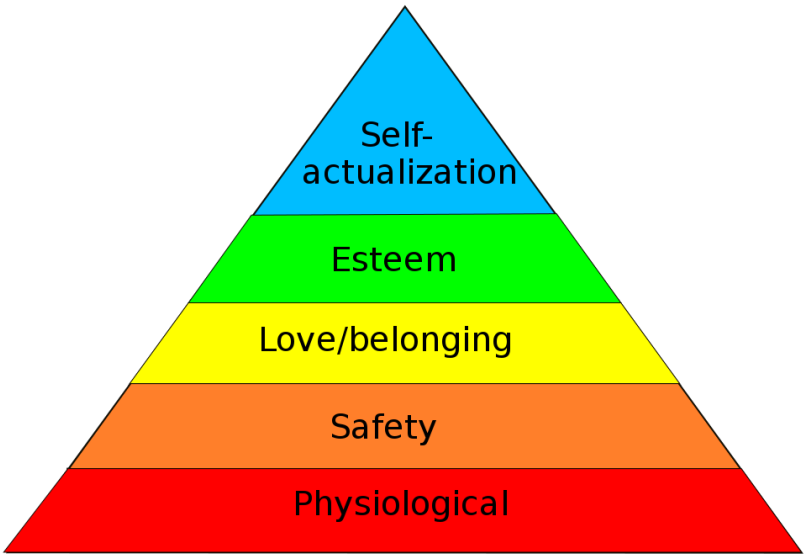
2.4.3 Sociološki vidik

Obstaja vrsta različnih pogledov, za katere je značilno, da predpostavljajo posameznikovo zaznavo sveta skozi perspektive družbe in kulture. Različne sociološke študije (v okviru proučevanja problemov enakopravnosti in pravičnosti) so obravnavale tveganja, kot na primer študije organizacijskih vidikov tveganja (Perrow, Clarke), epistemološke študije in problem legitimizacije znanja o tveganjih, analize porazdelitve tveganj v družbi, proučevanje konfliktov v soočanju s tveganji, analize nepristranosti in pravičnosti, analize medijev (po Mitar, 1995: 199).

Razlikovanje sociooloških teorij o tveganju je mogoče na različne načine, zato je Renn (1992: 68) predlagal, da je treba razlikovati teorije s pomočjo dveh dimenzij. Prva dimenzija je razmerje med individualističnim in strukturalističnim, druga dimenzija pa razmerje med objektivističnim in konstruktivističnim. Glede na obe dimenziji je v koordinatni sistem razvrstil šest glavnih sociooloških pristopov (koncept racionalnega akterja, teorija družbene mobilizacije, organizacijske teorije, sistemske teorije, neomarksistična in kritična teorija, konstruktivistični koncepti).

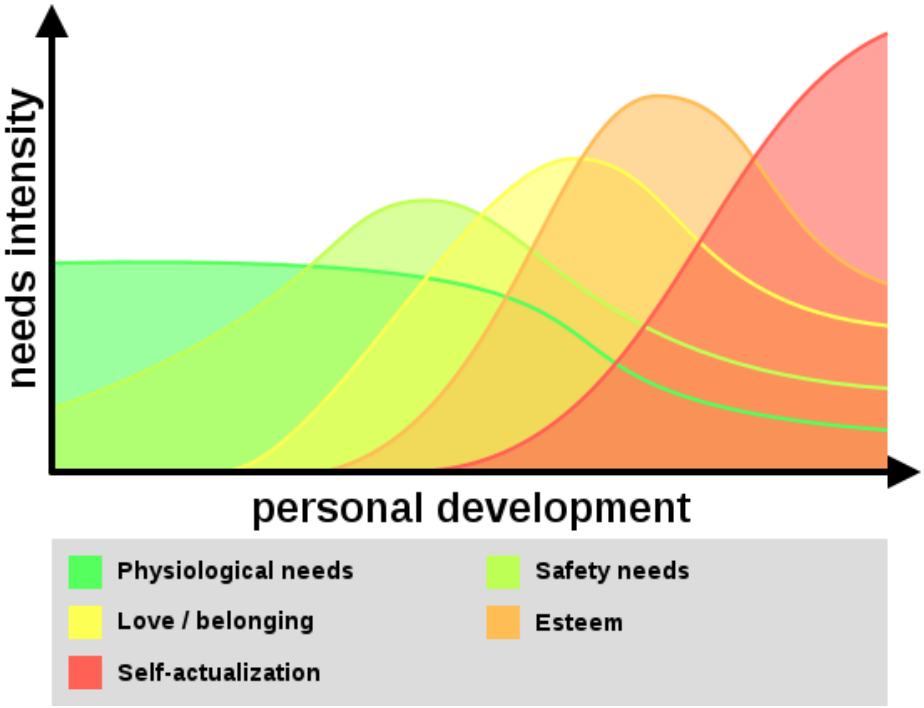
Sociološki pogledi poudarjajo, da so neželeni dogodki družbeno opredeljeni in dostikrat družbeno konstruirani. Dejanske posledice so vedno družbeno interpretirane in povezane z vrednotami ter interesi skupin. Realnost vsebuje tako objektivno (neodvisno od ocenjevalca) kakor tudi subjektivno stran (konstruiran pomen).

Iz sociološkega vidika je pomembno izpostaviti spoznanja Abrahama Maslowa, ki je že davno ugotovil, da je varnost uvrščena med osnovne človekove potrebe (sliki 10 in 12).



Slika 10: Maslowova piramida (hierarhija) potreb (Maslow, 1943)

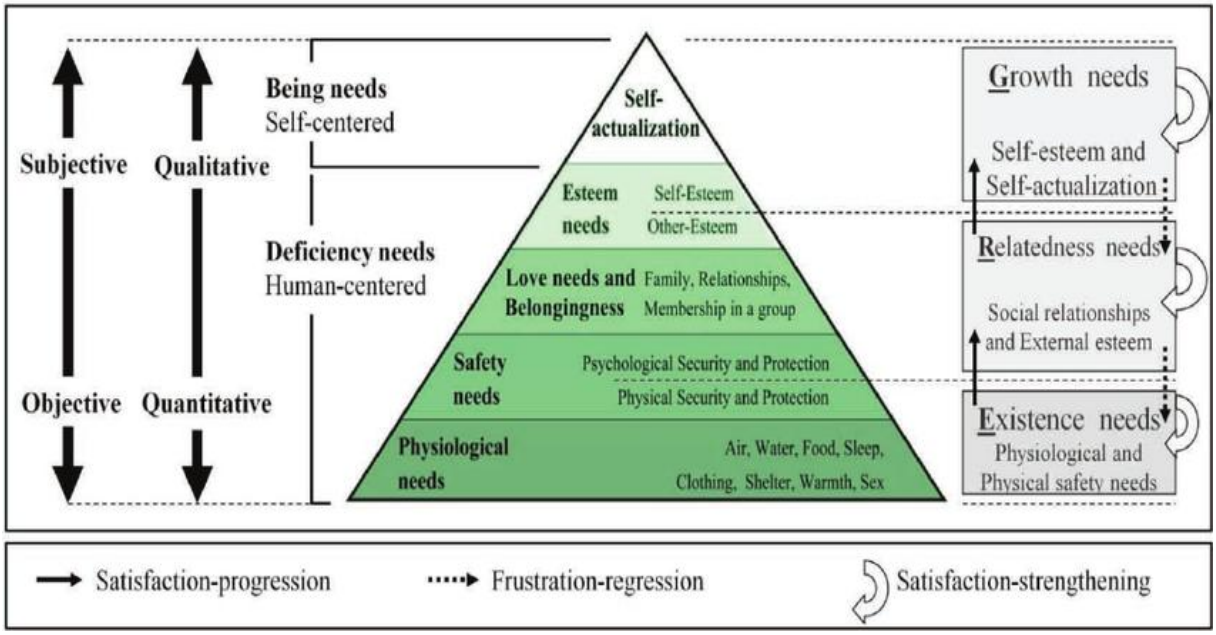
Najbolj temeljne in osnovne štiri nivoje piramide je Maslow imenoval »pomanjkanje potreb«. To so: spoštovanje, prijateljstvo in ljubezen, varnost in fizične potrebe. Če te potrebe (z izjemo najosnovnejše fiziološke potrebe) niso izpolnjene, se to lahko pri posamezniku izkaže ali v fizični obliki, še največkrat pa v obliki notranjih skrbi, napetosti in nelagodnega počutja. Maslowova teorija nakazuje, da je treba najprej izpolniti najosnovnejše človekove potrebe, da se lahko posameznik osredotoči oziroma je motiviran za doseganje ostalih višjih ravni potreb. Ob Maslowu je zanimiva tudi dinamična hierarhija potreb, ki jo je razvil Krech (slika 11), ki v bistvu nakazuje soodvisnost različnih človekovih potreb v času in prostoru.



Slika 11: Dinamična hierarhija potreb s hkratnim prekrivanjem različnih potreb (Krech in drugi, 1962)

Če se osredotočimo na varnostne potrebe, med katere lahko štejemo potrebe po osebni varnosti, varnosti premoženja, čustveni varnosti, finančni varnosti, varnosti zdravja, lahko ugotovimo, da v trenutku zadovoljitve fizioloških potreb posameznik postane relativno zadovoljen in prevladajo njegove varnostne potrebe. V odsotnosti fizične varnosti, do katere lahko pride zaradi vojne, terorizma, naravne nesreče, grožnje, kriminala, družinskega nasilja, zlorabe otrok ipd., posameznik lahko doživi stresno motnjo. Zaradi pomanjkanja gospodarske varnosti, katere razlog je lahko gospodarska kriza in s tem povezano pomanjkanje delovnih mest, se te varnostne potrebe izkazujejo skozi večjo skrb za varnost zaposlitve, večjimi zahtevami po zaščiti posameznika, zmanjšano potrošnjo zaradi varčevanja, povečanim povpraševanjem po zavarovalnih produktih ipd. Povečane varnostne

potrebe povezujemo s potrebo po višji zaščiti pred morebitnimi izrednimi dogodki. Če se posameznik v okolju in družbi ne počuti varno, bodo njegove potrebe po varnosti na Maslowovi lestvici potreb zlezle na višji nivo, v nekaterih izjemnih primerih, ko gre za varnost življenja pa lahko celo pred osnovne fiziološke potrebe.



Slika 12: Maslowova piramida potreb in Alderfersova ERG theorija (Estaji, 2014)

Če ugotovitve Maslowa, Krecha in Alderfelerjeve poizkušamo aplicirati na področje KI in jih implementirati v procese upravljanja z varnostnimi tveganji, lahko pridemo do ključne sklepne misli, ki pravi: »Stopnja varnosti je spremenljivka, ki je neprestano usodno odvisna od stanja razmer v družbi in v okolju, v katerem organizacija deluje ter od delovanja organizacije, skupin in posameznika v tej družbi in tem okolju. Pri tem je pomembno zavedanje, da se lahko stopnja varnosti v trenutku spremeni in povzroči popolnoma novo stanje, ki zahteva takojšen odziv in hitro prilagodljivost.« (Vršec, Mir., 2018). To zavedanje je eno ključnih pri vzpostavljanju sistema upravljanja z varnostnimi tveganji za delovanje KI.

2.4.4 Psihološki vidik

Svet, v katerem živimo, ni stalen in predvidljiv. Brez tveganja bi bilo vse vnaprej jasno in tako bi bilo celotno bivanje odvisno le od sosledja vzrokov in posledic. Prostor med gotovim in negotovim pa nam omogoča svobodno odločanje. Pri odločanju o tveganju se je treba zavedati, da se to ocenjuje v razmerju do neke koristi.

Psihološke vidike tveganja Hale in Glendon (1987) povezujeta s pojmoma varnost in nevarnost. Varnost pojmujeta kot stanje, ko je sistem oz. situacija pod nadzorom in se nevarnost še ni dogodila. Lahko rečemo, da je nekaj varno, če je s tem povezano tveganje sprejemljivo, če ne pride do nesprejemljivega poškodovanja prvin sistema. Tveganje je merilo možnosti, verjetnosti, da bo prišlo do škode v določenem obdobju. Presojanje sprejemljivosti tveganja pa je stvar osebnih in družbenih vrednostnih sodb ter zaznav. Nevarnost sta opredelila kot prisotnost možne poškodbe ene prvine ali več prvin sistema, bodisi zaradi interakcije z drugimi prvinami ali z okoljem.

Ocenjevanje tveganja zahteva presojo verjetnostne narave sveta in zmožnost inteligentnega razmišljanja o malo verjetnih, toda pomembnih dogodkih (Slovic in drugi, 1981, po Poliču, 1995). Tveganjem, povezanim z različnimi dogodki, praviloma pripisujemo verjetnostno naravo in jih ocenjujemo kot bolj ali manj verjetne ter se v skladu s tem tudi vedemo. Rezultati raziskav psiholoških eksperimentov kažejo, da posamezniki niso ravno najboljši ocenjevalci verjetnosti in da sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo. Njihove izbire ne ustrezajo osnovnim zahtevam doslednosti in skladnosti. Pri teh kršitvah se pogosto uporabljajo posebne hevristike (mentalne strategije), s katerimi se težave s presojo realnosti poenostavijo. Simon (1957, po Poliču, 1995) je celo predlagal teorijo omejene razumnosti, v kateri trdi, da posameznik, ki odloča, oblikuje poenostavljen model sveta, da bi ga lahko obvladal. Posameznik išče zadovoljive in ne najboljše rešitve. Izbere tisto pot, ki zadovolji njegove najpomembnejše potrebe, čeprav izbira morda ni najboljša.

Whyteova (1986, po Poliču, 1995) meni, da je dihotomija med razumnim in nerazumnim vedenjem artefakt ekonomskih modelov. V realnosti so posameznikovi cilji dvoumni. Odtod tudi takšno vedenje, pri čemer je treba iskati njegovo razumno razlago in ne razumnosti v njem. Fhaner (1977, po Poliču, 1995) ponuja drugačno razlago. Meni, da sodbe o verjetnosti nimajo pomembne vloge v našem življenju. Zato ima posameznik tako skromne zmožnosti za predelavo verjetnostne informacije. Najbolj očitni lastnosti družbenega sveta, kot ga zaznava posameznik, sta njegova stalnost in predvidljivost. Običajno le redko presojamo o verjetnostih, ki naj bi vplivale na naše življenje. Večina izbir in odločitev, ki jih sprejemamo je stvar navade, ali pa so tako trivialne, da ne zahtevajo ocene verjetnosti. To ne pomeni, da subjektivnih ocen verjetnosti ne dajemo, le prevladujoči značilnosti vsakdanjika sta njegova psihološka stalnost in predvidljivost. Kadar pa mora posameznik oceniti neko verjetnost, pri tem ne uporablja verjetnostnih načel, ampak neko bolj ali manj razumno, pogosto vzročno teorijo o pojavu.

Glavni element, ki vpliva na subjektivno ovrednotenje tveganja, je zaznava tveganj. Sprejme se lahko naslednja trditev: »Če posameznik ali interesna skupina zaznavata določeno tveganje kot nesprejemljivo, potem je to nesprejemljivo«.

Dejavniki, ki vplivajo na zaznavanje in ovrednotenje tveganja, so številni, nekateri so posameznikom bolj, nekateri manj sprejemljivi (Roland in Moriarty, 1990: 307). Bolj sprejemljivi dejavniki so zlasti naslednji: prostovoljni, naravni, pod nadzorom, odloženi učinki, nanašajo se na druge, nujni, zunaj službe, čutno zaznavni, nanašajo se na samooceno, večje koristi, že izkušeni, ni alternativ, podcenjeni, razumljeni, znani, skupni, običajni, medijsko neprivlačni, neprotislovni, pod mojo kontrolo, na področju zabave, nenevarne izkušnje. Manj sprejemljivi dejavniki so zlasti naslednji: neprostovoljni, človeški, zunaj nadzora, takojšnji učinki, nanašajo se name, niso nujni, v službi, čutno nezaznavni, ne nanašajo se na samooceno, manjše koristi, še ne izkušeni, so alternative, precenjeni, nerazumljeni, neznani, različni, dramatični, medijsko privlačni, protislovni, pod kontrolo drugih, pri delu, boleče izkušnje.

V zvezi z zaznavanjem je prisotno podcenjevanje na eni strani in precenjevanje tveganja na drugi strani. Običajno posamezniki podcenjujejo tveganja za znane grožnje in za tiste, ki jih lahko kontrolirajo, precenjujejo pa tveganja za neznane grožnje in za tiste, ki so zunaj zmožnosti človeške kontrole. Prispevek vsake izbire k vrednosti tvegane odločitve je obtežen s svojo verjetnostjo. Raziskave so pokazale, da lahko razlikujemo med objektivno verjetnostjo (vrednost, ki je izračunana na podlagi postavljenih domnev v skladu z zakoni verjetnosti) in subjektivno verjetnostjo (ocena verjetnosti nekega dogodka, ki jo poda posameznik ali lahko o njej sklepamo iz njenega vedenja) (Klein, 2009). Tako se zdi razlika med gotovostjo, da se nekaj bo ali ne bo zgodilo, in možnostjo, da se zgodi, večja od primerljivih razlik v vmesnem obsegu verjetnosti. Nizko verjetnost običajno precenjujemo, srednje in visoke verjetnosti pa podcenjujemo. Precenjevanje nizkih verjetnosti se kaže kot iskanje tveganja na pozitivnem področju in kot izogibanje na negativnem področju.

Mnoge empirične raziskave opozarjajo, da je posameznikova zmožnost pravilne presoje verjetnosti zelo omejena in ne sledi načelom teorije verjetnosti. Kahneman in Tversky (1972, po Poliču, 1995) menita, da posamezniki uporabljajo enostavna hevristična načela, predvsem sodbe o reprezentativnosti in dostopnosti. Menita, da posamezniki ne uporabljajo teh hevristik zgolj zato, ker zmanjšujejo spoznavni napor, ampak verjetno zato, ker so pogosto uspešne.

Pri uporabi hevristike reprezentativnosti posameznik ocenjuje verjetnost nekega negotovega dogodka ali vzorca glede na stopnjo, do katere je: (i) v bistvenih lastnostih podoben rodni populaciji; in (ii) odraža izstopajoče lastnosti procesa, s katerim je nastal.

Hevristika dostopnosti, po kateri za nek dogodek menimo, da je verjeten in pogost, če si z lahkoto zamislimo njegove primere, je med najpogostejšimi. Nasploh velja, da se primerov pogostih dogodkov lažje spomnimo ali si jih zamislimo, kot redkih. Zato je dostopnost pogosto ustrezen znak za presojo pogostosti in verjetnosti. Vendar nanjo vplivajo tudi mnogi

dejavniki, ki niso povezani z verjetnostjo. Posamezniki pogosto precenjujejo verjetnost nedavnih, živih ali čustveno nasičenih dogodkov. Vse prevečkrat jih določa njihova neposredna preteklost, ki omejuje njihova predvidevanja na poenostavljene konstrukte, v katerih je prihodnost zrcalna slika preteklosti. Očitno je, da so precenjeni dogodki dramatični in senzacionalni, podcenjeni pa praviloma nezanimivi.

Ocenjevanje tveganja dodatno otežuje pretirana prepričanost o pravilnosti lastne sodbe. Posamezniki prevečkrat pretirano zaupajo lastnim, napačnim sodbam. Psihološka osnova za to je verjetno njihova neobčutljivost za pomanjkljivost domnev, na katerih slonijo njihove sodbe. Najbrž noben dejavnik presojanja ni bolj odločujoč kot pretirana samozavest. Narava problema in sodbe določa tudi raven samozavesti. Splošno znanje povzroča razmeroma visoko stopnjo pretirane samozavesti, velja pa tudi obratna trditev. Raziskave odnosa med točnostjo in prepričanostjo o svoji sodbi (Plous, 1993, po Poliču, 1995) so pokazale naslednje:

- pretirana samozavest je največja, kadar je točnost blizu naključne;
- pretirana samozavest pojema, ko točnost narašča od 50 do 80 %. Ko preseže 80 %, postanejo posamezniki pogosto premalo prepričani o točnosti svoje sodbe. Razlika med točnostjo in samozavestjo je torej najmanjša pri približno 80 % točnosti in se veča z odmikom od te ravni;
- neskladnosti med točnostjo in samozavestjo niso povezane z inteligenco posameznika, ki odloča.

Psihološki pogledi razširjajo subjektivno presojo tveganja na tri načine: (i) opozarjajo na to, da posamezniki ne oprejo svojega sklepanja samo na pričakovane koristi, ampak upoštevajo tudi verjetnosti. Ljudje se izogibajo tveganjem, če so vloženi deleži in izgube visoke, iščejo pa tveganja, kjer so možnosti visokih dobičkov. Posamezniki uravnotežijo svoje vedenje v razmerju s tveganjem z oblikovanjem optimalne strategije soočanja s tveganji, ki zagotavlja zadostne koristi ob izogibanju glavnim negotovostim (nevarnostim); (ii) psihološke teorije so odkrile različne pristranosti v sklepanju na podlagi verjetnosti. Te pristranosti kažejo intuitivni način obravnavanja negotovosti; (iii) ugotovljen je pomen kontekstualnih značilnosti, ki pomembno vplivajo na ocenjevanje tveganja (možnost katastrof) in kvalitativnih značilnosti tveganja (prepričanje o pravičnosti dobičkov in izgub, možnost opredelitve krivcev prepričanj o vzrokih tveganja). Dejavniki tveganja kažejo na to, da je tveganje večdimenzionalni koncept, ki ga ni mogoče enostavno zmanjšati le na zmnožek verjetnosti in posledic možnih dogodkov. Zaznavanje tveganj se v različnih družbenih in kulturnih okoljih bistveno razlikuje. Vendar je značilno, da posamezniki tveganje zaznavajo večdimenzionalno in da integrirajo svoja prepričanja o značaju tveganja, vzrokih in okoliščinah tveganja v določen konsistentni sistem prepričanj (Renn, 1992: 66).

Psihološki pogled na tveganja v ospredje postavlja posameznika in njegovo subjektivno prepričanje (dostikrat v škodo realnosti), kar je glavna prednost tega pogleda. Širina dimenzij, ki jih posameznik uporablja pri ocenjevanju tveganj, ne omogoča lahkega iskanja skupnega imenovalca za primerjavo prepričanj posameznikov. Postavlja se tudi vprašanje, zakaj posameznik nameni pozornost določenim tveganjem, druga pa ne upošteva ustrezno. Psihološki pristop omogoča, da se oblikuje bolj celovit pogled na možnosti odločanja, da se izrazijo vrednote posameznika in skupin kot izhodišče za oblikovanje skupnih preferenc ter da se prikažejo osebne izkušnje, kar ni mogoče v tehničnih analizah tveganja. Vendar podobno kot drugi pogledi in perspektive psihološki pogled prispeva pomembna spoznanja, na drugi strani pa so njegove ugotovitve omejene.

Grožnje KI po eni strani izhajajo iz mogočega vpliva na posameznika kot uporabnika njenih storitev, po drugi strani pa je kljub visoki stopnji avtomatizacije delovanja posameznik pri upravljanju teh kompleksnih sistemov eden najpomembnejših referentov za njeno varno delovanje. Ta vpliv je lahko neposreden ali posreden. Tehnologija je dosegla točko, ko bo izboljšano varnost mogoče doseči le na podlagi boljšega razumevanja tveganj in možnosti za posameznikovo napako. V okviru verjetnostnih varnostnih analiz se ugotavlja, kateri scenariji groženj KI se lahko zgodijo, kako verjetno je, da se zgodijo, kako hude so lahko njihove posledice in kakšna je pri tem posameznikova zanesljivost (Bertoncelj, 2017).

2.4.5 Varnostni vidik

Delovanje in razvoj KI je močno podvrženo ranljivosti, ogroženosti in varnostnim tveganjem. Če smo zelo natančni in poglobljeno razmišljamo o tveganjih, imajo skorajda vsa tveganja pridih varnosti, nevarnosti, negotovosti in izpostavljenosti nečemu, kar nas spravi v dvom, strah, nelagodje, da se lahko pripeti kaj, kar bo povzročilo določeno škodo. Tako lahko rečemo, da so vsa poslovna, finančna, ekonomska, logistična, kadrovska in druga tveganja podvržena varnostnim vprašanjem. Poznamo pa tudi t.i. »čista« varnostna tveganja, kot so denimo: tveganja naravnih in drugih nesreč, požarna tveganja, ekološka tveganja (onesnaženje zemlje, zraka, vode z odpadki, izlivi, izpusti kemikalij in nevarnih snovi ipd.), tveganja kriminalne narave (tatvine, vlomi, ropi, napadi ipd.), tveganja nezgod na delu, tveganja terorističnih napadov in druga varnostna tveganja. Ko gre za uresničitev »čistih« varnostnih tveganj moramo vedeti, da zagotovo povzročajo določeno materialno, finančno, ekonomsko, socialno in moralno škodo in izgubo. Prav tako moramo vedeti, da varnostna tveganja izhajajo iz ocene ranljivosti in ogroženosti premoženja, procesov, človeških virov in vrednot. Tovrstna tveganja je treba obravnavati v kontekstu zaznavanja, razvrščanja, analiziranja in obvladovanja tveganj okolja, tveganj procesov, tveganj informacij ter poslovnih in drugih tveganj. Kajti navedene vrste tveganj se torej v mnogih točkah prepletajo, pri čemer

pa so najbolj v ospredju prav varnostna tveganja. Tako kot vsa druga tveganja so tudi varnostna tveganja obravnavana z zunanjega in notranjega zornega kota delovanja KI.

Posebnosti varnostnih tveganj

Pri obravnavanju tveganj z varnostnega vidika zasledimo tri pogoste besedne zveze, ki definirajo razsežnost zanesljivosti delovanja KI. To so: varnostni izzivi (ang. security challenges), varnostna tveganja (ang. security risks) in varnostne grožnje (ang. security threats), ki nakazujejo, da imajo varnostna vprašanja pomembno težo v doseganju načrtovanih ciljev delovanja in poslovanja gospodarskih in drugih družb, ki upravljajo kritično infrastrukturo. Varnostne grožnje razumemo kot potencialne ali realne besedne, fizične, oborožene in psihološke napade na posameznika ali skupino, varnostna tveganja pomenijo neobvladovanje ali slabo obvladovanje groženj in izrednih dogodjkov, varnostni izzivi pa se vidijo v tem, ali smo sposobni izboljšati obvladovanje groženj, izrednih dogodkov in varnostnih tveganj. Poleg omenjenih izrazov so v pogosti uporabi še izraza negotovost (ang. uncertainty) in nevarnost (ang. danger). O varnostnih grožnjah in še posebej o neposredni nevarnosti (realna ogroženost) govorimo takrat, ko se dejansko že vidi (slutimo, predvidevamo), da bo nastal nek izredni dogodek, ki bo povzročil zmedo, zastoj ali oviro v določenem procesu ali v večih procesih, v skrajnem primeru pa v vseh procesih. Vidi se tudi, da bo nastala določena škoda in izguba, kar odgovorne opozarja na to, da je treba sprožiti mehanizme kriznega vodenja: aktiviranje kriznega štaba, načrta kriznega vodenja in kriznega komuniciranja na osnovni in/ali rezervni lokaciji. S tega zornega kota se varnostna tveganja pojavljajo v naslednjih varnostno pogojenih poslovnih segmentih:

- ranljivost in ogroženost lokacije, zgradb, opreme in poslovne dokumentacije,
- varnostne politike – krovna varnostna politika in izvedene varnostne politike (politika varovanja informacij, politika varnosti in zdravja pri delu, idr.).
- integralni (celovit) varnostni sistem,
- varnost in zdravje pri delu,
- varstvo pred požari,
- varstvo okolja,
- fizično in tehnično varovanje določenih prostorov (službe informatike, kadrovske službe, razvojne službe, projektne pisarne, VNC, idr.),
- varovanje osebnih in tajnih podatkov ,
- varovanje poslovnih skrivnosti,
- varovanje informacij in elektronskih komunikacij,
- varovanje intelektualne lastnine,
- zaščita in reševanje – civilna zaščita,
- notranja kontrola in revizija,
- interna ali pogodbena služba varovanja,

- pogodbeni izvajalci, ki morajo biti nadzirani tudi glede varnostnih vprašanj,
- vprašljivi poslovni partnerji (ki nimajo urejenih varnostnih mehanizmov),
- protokolarne aktivnosti, v katerih je eno od ključnih vprašanj zagotavljanje varnosti udeležencev.

Glavne posebnosti v opredeljevanju, obravnavanju in obvladovanju varnostnih tveganj so:

- globalni varnostni izzivi in globalna prizadevanja za varnost,
- premajhna pripravljenost za pripravo ocen ranljivosti in ogroženosti kot podlage za varnostno politiko in varnostni sistem,
- vzpostavljanje optimalnega varnostnega sistema šele ob večjem izrednem dogodku,
- zniževanje stroškov varovanja in zaščite, kot prva aktivnost obvladovanja stroškov,
- stanje v povezavi s človeškimi viri na področju zasebnega varovanja (zasebna varnostna podjetja) in pri varovanju za lastne potrebe (interne službe varovanja) je zelo slabo, v nekaterih okoljih celo katastrofalno: zelo nizka izobrazbena struktura, vključevanje invalidov v varovanje, nizke plače, nizka motivacija za kakovostno delo, nizke cene varnostnih storitev,
- posledice izrednega dogodka (nesreče, požara, kriminalnega dejanja, vdora v informacijski sistem, izdaje poslovnih skrivnosti, eksplozije, itd.) so neposredne in na prvi pogled vidne pri oškodovanju premoženja, človeških virov in morale.

Iz opisanih posebnosti varnostnega področja je razvidno, da so varnostna tveganja pomembna. Spoznati jih je možno v okviru ugotavljanja ranljivih točk v procesih in v okviru ocene ogroženosti premoženja, osebja, znanja, informacij ter poznavanja notranjega in zunanjega okolja gospodarskega subjekta.

2.5 KAZALNIKI ZA PRISTOP K OCENJEVANJU TVEGANJ

2.5.1 Kazalniki karakterizacije tveganj

Dobra praksa karakterizacije tveganja določa, da je treba oceno tveganja pripraviti na način, ki je jasen, pregleden, razumen in skladen z drugimi značilnostmi tveganja podobnega obsega (smiselno povzeto po NIPP, 2013). V največji meri naj se upošteva načela preglednosti, jasnosti, doslednosti in razumnosti, ki so predstavljena v nadaljevanju.

a. Kazalniki preglednosti tveganj

Preglednost zagotavlja doslednost in sledljivost v procesu ocene tveganja. Zagotavlja, da vsak uporabnik razume vse korake, logiko, ključne predpostavke, omejitve in odločitve v oceni tveganja in razume podporno utemeljitev, ki vodi k rezultatu.

Preglednost naj doseže popolno razkritje v smislu:

- uporabe strokovnega (znanstvenega) pristopa ocenjevanja,
- uporabe predpostavk in njihovega vpliva na oceno,
- uporabe ekstrapolacij in njihovega vpliva na ocenjevanje,
- uporabe modelov, metodologij in meritev ter njihov vpliv na oceno tveganj,
- verjetnih alternativah in izbirah med temi alternativami,
- vplivov ene izbire glede na drugo in na oceno tveganj,
- pomembne vrzeli v podatkih in njihove posledice za oceno tveganj,
- glavnih sklepov o tveganju in zaupanja ocenjevalcev ter negotovosti v njih,
- opredelitve stopnje pristopa (npr. obsežna karakterizacija) in razlog za to,
- strokovne revizije, z razpravo v strokovni javnosti in naročnikom, po uveljavljenih postopkih.

b. Kazalnik jasnosti tveganj

Jasnost se nanaša na izdelek ocene tveganja. Za večjo jasnost je potrebno, da je ocena tveganj optimizirana in da jo lahko naročnik razume znotraj ter zunaj postopka ocenjevanja tveganja.

Jasnost se doseže z:

- kratkostjo ocene,
- izogibanjem žargona in nestrokovnim izrazom,
- uporabo preprostega jezika tako, da je ocena čim bolj razumljiva,
- izogibanjem uporabe podrobnih tehničnih izrazov, če pa se uporabljajo, pa z opredelitvijo teh izrazov,
- opisovanjem kakršne koli količinske ocene tveganja, z jasno uporabo razumljivih tabel in grafik za predstavitev tehničnih podatkov,
- uporabo jasnih in ustreznih enačb za učinkovito prikazovanje matematičnih razmerij.

c. Kazalnik doslednosti obravnave tveganj

Doslednost zagotavlja kontekst za naročnika in se nanaša na predstavitev gradiva v oceni tveganja. Na primer, ali so sklepi ocene tveganja označeni v skladu z ustrezno politiko, postopkovno usmeritvijo in znanstvenimi utemeljitvami, in če ne, zakaj se sklepi razlikujejo.

Vendar doslednost ne bi smela slepo slediti smernicam za oceno tveganja na račun inovativnega pristopa. Usklajenost se doseže z:

- smiselnim upoštevanjem ustreznih smernic in zakonskih izhodišč za oceno tveganj,
- uporabo računalniškega programskega orodja ali drugih pripomočkov za oceno tveganja, kjer je to primerno,
- ocenjevanje tveganja v povezavi z drugimi podobnimi ocenami tveganja (kako se primerja z drugimi ocenami podobnih sistemov, sredstev ali lokacij; kako se primerja z drugimi ocenami, ki jih izvajajo znanstvene organizacije, druge države in / ali različne interesne skupine; pričakuje se smiselno iskanje podobnih ocen),
- primerjavo, kako se sklepi, ki so jih naredili drugi, razlikujejo od ocene tveganja za naročnika,
- primerjavo, kakšne so prednosti in omejitve v primerjavi z oceno tveganja za naročnika.

d. Kazalnik razumnosti tveganj

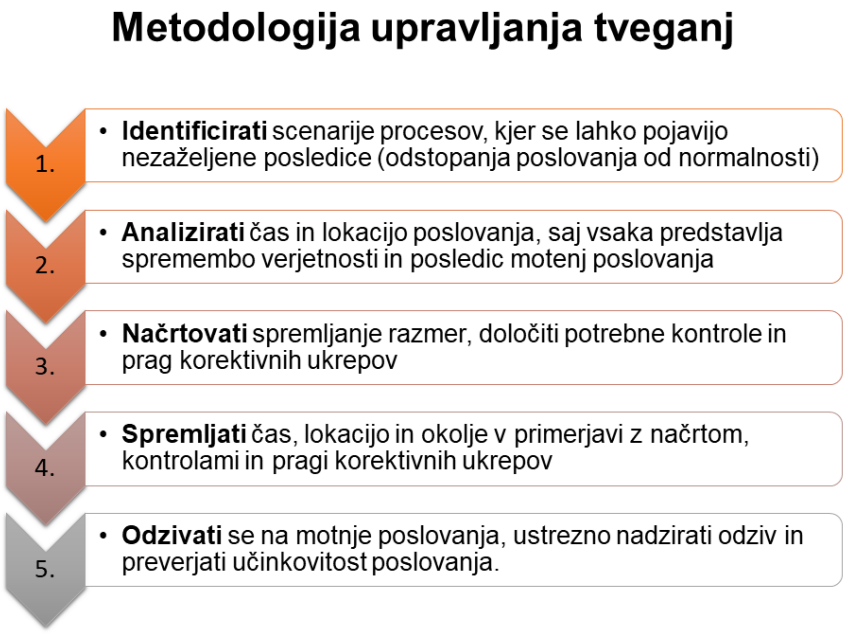
Razumnost se nanaša na ugotovitve ocene tveganja v okviru stanja znanosti, privzetih predpostavk in odločitve o znanstveni politiki, sprejeti v oceni tveganja. Zaželjeno je, da postopek ocenjevanja tveganj sledi sprejemljivi, očitno logični poti in ohrani zdrav razum pri uporabi ustreznih strokovnih smernic. Ocena tveganja temelji na trdni strokovni presoji. Razumnost se doseže, če:

- opredelitev tveganja temelji na strokovnih predpostavkah, predpostavkah tveganj naročnika in strokovne javnosti,
- so komponente tveganja dobro vključene v splošni zaključek tveganja, ki je popoln, informativen, dobro uravnotežen in uporaben za odločanje,
- karakterizacija tveganj temelji na najboljših (po oceni strokovne javnosti) razpoložljivih znanstvenih informacijah,
- presoje, potrebne za izvedbo analize tveganja, uporabljajo zdrav razum v skladu z zakonskimi zahtevami in smernicami naročnika,
- ocena uporablja splošno priznano znanstveno znanje, dobro prakso in izkušnje ocenjevalcev,
- so ugotovljene in pojasnjene ustrezne alternativne ocene tveganj v okviru različnih alternativnih možnosti za upravljanje tveganj,
- so vzpostavljeni postopki strokovne revizije ocene tveganj.

2.6 PRISTOP K PREPOZNAVANJU TVEGANJA

Ohranjanje normalnega in neprekinjenega poslovanja KI je neposredno odvisno od učinkovitega upravljanja tveganj. Ključ do zmanjšanja verjetnosti in posledic ogrožanja poslovanja je v razumevanju profila tveganja upravljavca KI. Profil tveganj izhaja iz metodologije, ki določa, kako se tveganje spremlja med primerljivimi sredstvi in procesi (prikazano na sliki 13). Pri razvijanju profila tveganja upravljavec KI ocenjuje:

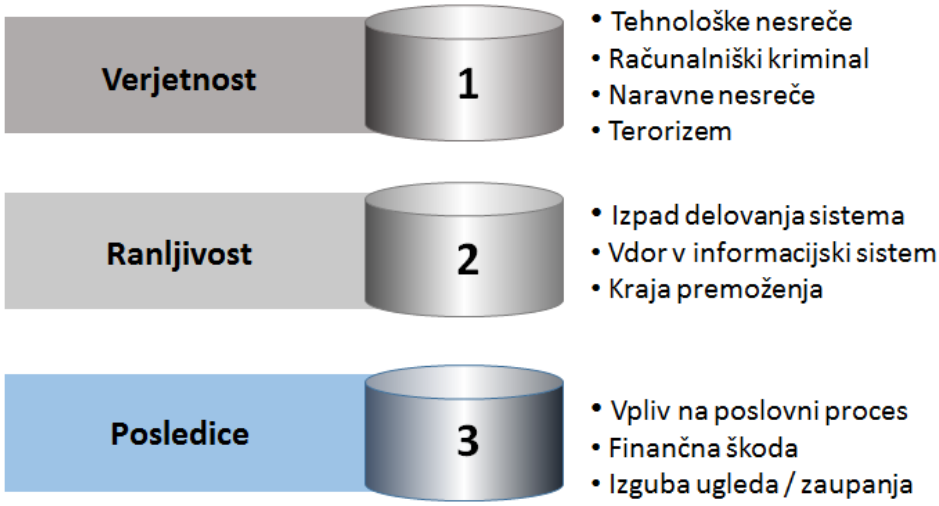
- izvor tveganja,
- sredstva ali procese tveganja,
- ranljivosti in učinkovitosti notranjih kontrol ter revizije,
- verjetnost nastanka in potencialni učinek / posledice ogrožanj,
- ocene in področja visokega tveganja.



Slika 13: Metodološki koraki za ocenjevanje tveganja (interni vir ICS)

Po oceni teh dejavnikov mora upravljavec KI določiti, ali je tveganje na sprejemljivi ravni. Če je to nesprejemljivo, ima upravljavec več možnosti odločanja: lahko uporabi dodatne kontrole, prenese del tveganj na zavarovalnico, loči sredstvo ali postopek od možnega ogrožanja ali sprejme povečano tveganje.

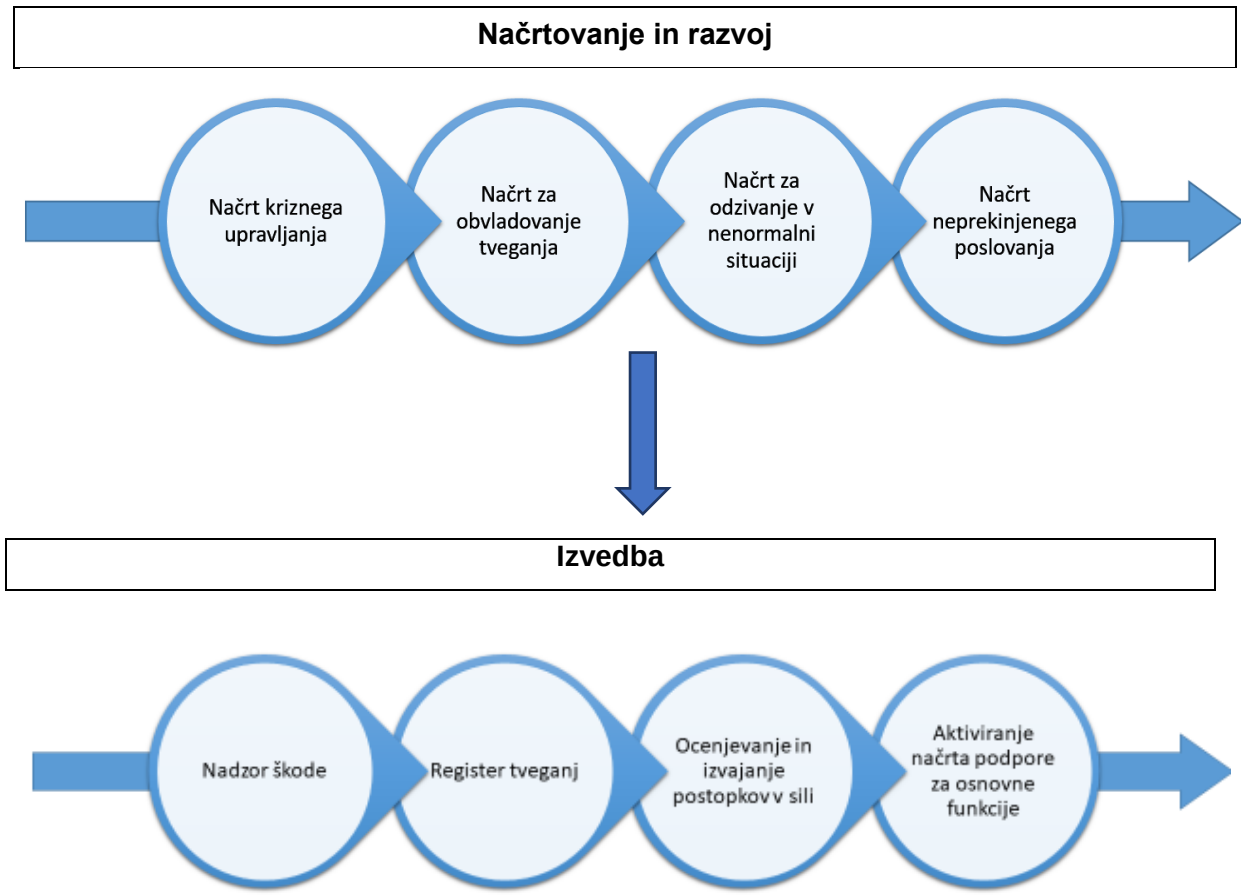
Ocenjevanje tveganj ni statični koncept. Učinkovitost nadzora tveganj se lahko hitro spremeni. Ko se realizira profil tveganja, mora biti upravljavec KI sposoben odkrivati, ocenjevati in se odzivati na notranje ali zunanje spremembe. Odločitve naj temeljijo na dejstvih, da bi ugotovili, kje naj bi krizno načrtovanje delovalo v kontinuumu tveganja.



Slika 14: Faktorji tveganj (interni vir ICS)

Postavlja se vprašanje: Koliko tveganja je dovolj? Problem je lahko, če upravljavec KI preveč odločitev sprejema z nepopolnim razumevanjem profila tveganja in z omejenimi zmogljivostmi, potrebnimi za učinkovito obvladovanje tveganja. Za izravnavo tega je bistvenega pomena, da upravljavec KI opredeli apetit tveganja. V uradnem poročilu upravljavec KI ugotavlja tveganja, za katera meni, da so najpomembnejša za doseganje strateških ciljev poslovanja in izkušnje s tveganji. Ta dokument mora določiti kulturo tveganja, stopnje tveganja in pristop k obvladovanju tveganja. Vsi strateški in operativni načrti ter programi morajo biti skladni s tem ključnim poročilom.

Obstaja več možnosti za upravljanje apetita tveganja. Na sliki 15 so prikazani temeljni elementi. Ta centraliziran programski pristop povezanih načrtov zagotavlja sredstva za proaktivno zmanjšanje in reaktivno upravljanje nenormalnih situacij (postopkov v sili). Ta model zahteva izvršilno sponzorstvo, vodstveno infrastrukturo in potrebno raven načrtovanja. Izvršni sponzor (običajno član vodstva upravljavca KI) zagotavlja strateške cilje poslovanja, medtem ko upravitelji posameznih načrtov ustvarjajo strukturo, dajejo navodila in določajo prednostne naloge. Ta program temelji na trenutnem profilu tveganja in vzpostavlja apetit tveganja. Upravitelji pa določijo pristop k načrtovanju, dodelijo posamezne vloge in odgovornosti, upravljajo vire, nadzorujejo upravljanje sprememb in o rezultatih poročajo izvršnemu sponzorju.



Slika 15: Programski pristop povezanih načrtov (interni vir ICS)

Pomanjkanje zmogljivosti in učinkovitosti obvladovanja tveganj, neustrezno odzivanje na nenormalne situacije in neučinkovito načrtovanje neprekinjenega poslovanja lahko povzročijo, da upravljavec KI ne more več zagotavljati ciljev poslovanja. Za proaktivno delovanje bi upravljavec KI moral izvajati revizijsko in nadzorno funkcijo, da bi preprečil možnosti za nastanek izrednih dogodkov.

Premisleki, ki olajšajo odziv na apetit tveganja vključujejo:

- kakšna je zavezanost upravljavca KI za obvladovanje tveganja?
- kako učinkovit je načrt za obvladovanje tveganja?
- katera merjenja se uporabljajo za ocenjevanje učinkovitosti odzivanja na izredne dogodke?
- kakšna je stopnja načrtovanja neprekinjenega poslovanja?
- kakšna je stopnja usposabljanja zaposlenih?
- kako pogosto se usposabljajo, testirajo in izvajajo načrti?

Ni ustreznega nadomestila za vzpostavitev profila tveganja in nevarnosti apetita tveganja. Brez analize dejavnikov tveganja (morebitne motnje, posledice, ranljivosti in ogrožanja) ni

možno določiti apetita tveganja. Pri tem se moramo zavedati, da bo učinkovitost uporabljenih ukrepov in postopkov za obvladovanje tveganj v veliki meri nedoločeno. Čeprav bodo odločitve za obvladovanje tveganj vedno vsebovale določeno stopnjo negotovosti, morajo te odločitve vedno temeljiti na poglobljeni analizi.

Na sliki 16 so prikazani trije nivoji tolerabilnosti tveganja. Nanašajo se na tveganja, ki niso sprejemljiva, zniževanja tveganj (glede na stroške) in toleriranje tveganj.

Slika 16: Nivoji vzdržnosti tveganja (interni vir ICS)

a. Ocenjevanje tveganj

Ocenjevanje tveganj je ena od sestavin vodenja dela. Ključni dejavniki ocenjevanja tveganja so: (i) tveganje je potrebno obravnavati kot proces; (ii) za ta proces so v skladu s pristojnostmi odgovorni vsi zaposleni; (iii) za ocenjevanje tveganj so potrebne kvantitativne in kvalitativne baze podatkov.

Iz izkušenj in poznavanja dobre prakse je uspešno ocenjevanje tveganj odvisno od:

- vzpostavitve organizacijske kulture upravljavca KI, kjer zaposleni razumejo usmeritve vodstva in cilje ter koristi, ki naj bi jih prineslo učinkovito upravljanje s tveganji,
- formalnega sprejema politike upravljanja tveganj in njena dosledna implementacija v praksi,
- vzpostavitve interne komunikacije za prepoznavo tveganj in sprejemanje ustreznih proaktivnih ukrepov ter postopkov,
- ustanovitev formalne skupine za ocenjavanje in presojanje tveganj (dodelitev odgovornosti) ter vzpostavitev podatkovne baze registra tveganj,

- razkrivanje glavnih zaznanih tveganj in načinov njihovega obvladovanja lastnikom in drugim pristojnim,
- zagotovitev spremljanja in ustreznega vodstvenega nadzora obvladovanja tveganj, vključno z aktivnostjo Notranje revizije,
- vključitev izobraževanja o tveganjih v programe usposabljanja zaposlenih,
- stopnje varnostne kulture in poslovne etike organizacije in zaposlenih,
- nadaljnji razvoj analitičnih metod in tehnik za ocenjevanje in upravljanje tveganj.

Eno od ključnih vprašanj ocenjevanja tveganj je zaznava negotovosti dogodkov oziroma njihova verjetnost. Gre za vprašanje verjetnostne porazdelitve, saj kdor se odloča v razmerah negotovosti, ne more sklepati o uspešnosti svojih dejanj vnaprej (problem je, ker sklepamo o prihodnosti na podlagi podatkov in informacij iz preteklosti!). Prav tako se tudi odločitev ne more presojati v skladu s profilom nagnjenosti k tveganju. Potrebno je vzpostaviti bazo podatkov in informacij ter zagotoviti primerno ravnotežje med nagnjenostjo k tveganju in nadzoru, saj se tako sooča z negotovostjo sodobnega poslovnega sveta[6].

Zanimiva je misel Jawaharlala Nehruja: »Politika nesprejemanja tveganja je največje tveganje.« To misel dopolnjuje tudi razmišljanje generala Colina L. Powella, ki nas opozarja na dejstvo, da upravljanje tveganja ne pomeni vedno oklepanje najprevidnejše strategije[7].

Zato mora v nenehno spreminjajočem se svetu ocenjevanje in upravljanje tveganj veljati za pomembno prioriteto. Stabilnega poslovanja ne smemo utemeljevati z verjetnostjo, da se bo nekaj zgodilo, ampak z možnimi posledicami. Gre za preprosto vprašanje: Ali si lahko na eni strani privoščimo »razkošje velikih škodnih dogodkov«, na drugi strani pa izgubo zaupanja uporabnikov, materialno škodo, slabo vodenje in slabe poslovne odločitve?

Raziskovalci teorije organizacijskega obnašanja menijo, da so pohlep, strah in ego temeljni gonilni dejavniki, ki nas usmerjajo v poslovnem okolju. S pohlepom označujejo osnovno potrebo posameznika po izboljšanju položaja v družbi. To je posledica človekovega razvoja, saj je posameznikom dajal večje možnosti za preživetje. V poslovnem svetu je pohlep prikazan kot želja zaposlenega po čim večjem lastništvu materialnih dobrin (žrtvovanje dolgoročnih kariernih ciljev za kratkotrajne koristi). Strah je motiv, ki nas usmerja, da se ne izgubimo v svetu, kjer so izgube lahko usodne. Z nastopom straha, ta prevzame vodilno

[6] Vzporednico z raznimi vojnimi strategijami lahko vzpostavimo z izjavo specialista za teorijo vojnih iger Marka Hermana: »Vodstvo mora obdržati vrhnji pogled, v same taktične detajle pa naj se ne bi spuščalo. Ni namreč smiselno, da bi vrhovni poveljnik odločal, na katero stran naj se premakne posamezni lovec.« Vodja mora upoštevati tudi dejstvo, da ne ve in ne pozna vseh zadev. Razumni vodja daje pooblastila pristojnim podrejenim in upošteva njihove razlage, argumente ter razumna zagotovila.

[7] Pri odločitvah, ki jih moramo sprejeti, general predlaga formulo 40 / 70 in svetuje: »Ne sprejemajte odločitev, če nimate dovolj informacij oziroma je verjetnost, da bo odločitev povzročila ugodne posledice, manj kot 40 - odstotna. Velja tudi nasprotno. Ne čakajte trenutka, da boste stoodstotno prepričani, da ste na pravi poti, saj bo takrat odločitev sprejeta prepozno oziroma tega trenutka ne boste nikdar dočakali. Ko razpoložljive informacije zadoščajo oziroma ocena verjetnosti ugodnega izida pokaže 40 do 70 odstotkov, postavite želodec na preizkušnjo.«

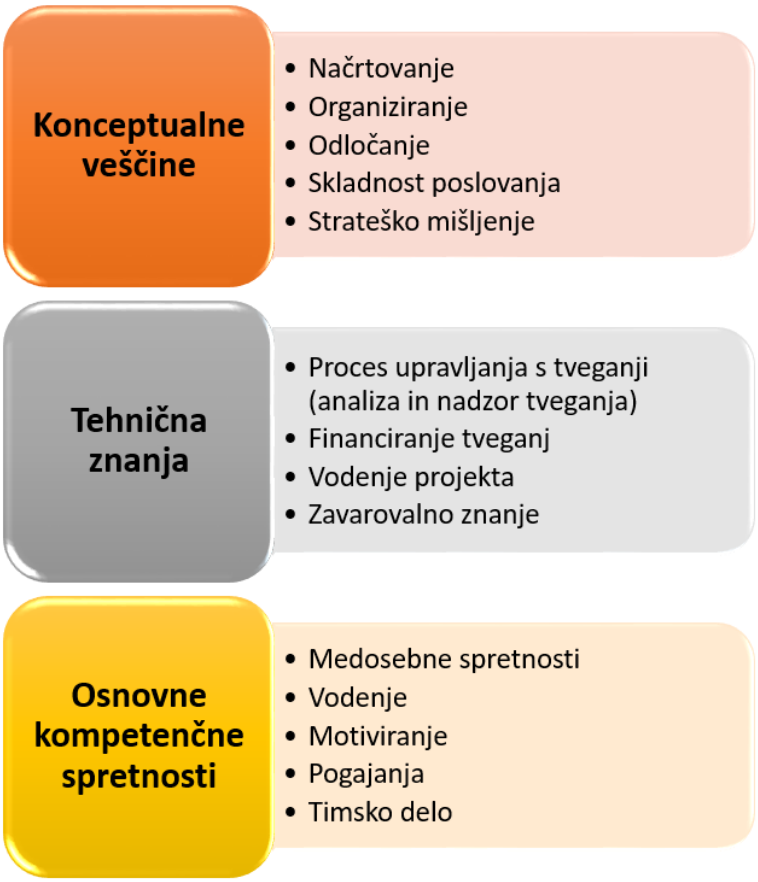
vlogo pred vsemi drugimi motivi. Ko je posameznik ogrožen, se njegovo vedenje nepričakovano in pogosto neprijetno spremeni. V poslovnem svetu lahko zaposlenega zajame strah pred izgubo, da poskusi prikriti že nastale izgube ali pa izgubo nadomestiti s sprejemanjem še bolj tveganih odločitev (teorija odločitvenih oblik obnašanja). Z egom označujemo potrebo posameznika, da je cenjen v družbi. V poslovnem svetu je ego vodilni motiv za strokovnjake, ki se jim zdi ugled navadno osebno pomemben. Grobo rečeno, v večini primerov so pohlep, strah in ego koristni za posameznika, saj pohlep ustvarja premoženje, strah preprečuje izredne dogodke, ego pa gradi poslovni uspeh.

Zavedati se je potrebno, da upravljanje tveganj po srečnem naključju ni, pričakujemo lahko le optimalne rešitve. Tudi veliki napori za njihovo obvladovanje ne zagotavljajo popolnosti in varnosti. Razmere, pogoji poslovanja in vrste ter oblike ogrožanj se stalno spreminjajo, zato ni mogoče izključiti tveganj, saj tudi popolne varnosti ni.

b. Potrebna znanja in spretnosti za ocenjevanje tveganj

V nadaljevanju bo predstavljen dinamičen pristop k ocenjevanju tveganj za delovanje KI, ki ga je treba pregledati vsako leto ali takoj v primeru bistvene spremembe zunanjega ali notranjega okolja.

Model sestavljajo tri spretnosti: veščine kompetentnosti, tehnične spretnosti in konceptualne sposobnosti (prikazan na sliki 17). Diagram predstavlja različne sektorje spretnosti in ne povezuje različnih stopenj pomembnosti ali razvoja posameznega strokovnega znanja o tveganju.



Slika 17: Potrebna znanja in spretnosti za ocenjevanje tveganj (interni vir ICS)

V nadaljevanju so pojasnjeni nekateri pojmi modela v zgornji sliki.

A. Konceptualna znanja (veščine)

To je strateški nivo, ki zahteva sposobnost razumevanja vseh dejavnosti upravljalca KI in kako ta organizacija lahko doseže svoje strateške cilje poslovanja. Te veščine vključujejo:

- načrtovanje: določiti primerne cilje poslovanja in ohranjati globalno perspektivo,
- organiziranje: vzpostavitev področja organizacijske varnosti; ustrezno kadrovanje; vzpostavitev odnosov z drugimi zainteresiranimi stranmi; upravljanje s tveganji; graditi poslovne odnose na področju strateških povezav in partnerstev, pa tudi varnosti,
- odločanje: prepoznati in analizirati ogrožanja, težave in probleme ter odločiti o ukrepih in aktivnostih za upravljanje tveganj v negotovih pogojih dinamičnega globalnega okolja; primerjati domače in tuje podatke sektorja KI; analiziranje priložnosti in prepoznava rešitev,
- skladnost poslovanja: visoka raven etičnega vedenja; razkritje (preglednost) poslovanja in lojalnost zaposlenih; obojestranska korist dogovorov med zaposlenimi in vodstvom,

- strateško mišljenje: vizija ustvarjanja novih inovativnih konceptov ocenjevanja tveganja.

B. Tehnična znanja

To je operativni nivo, kjer je veliko tradicionalnih nalog in specializiranih veščin.

- proces upravljanja tveganj: razumeti model tveganja; prilagoditi model tveganja potrebam upravljavca KI; razumeti kako upravljanje tveganja ustvarja dodano vrednost; analizirati tveganja, prepoznavati rešitve, proces odločanja,
- analiza tveganja: povezovanje tveganj s ključnimi (kritičnimi) poslovnimi procesi; prepoznavanje tveganj, merjenje in analiza tveganja; statistični koncepti in merjenje; ustvarjanje veljavne napovedi tveganja; vzpostavljanje registra tveganj, kartiranje in profiliranje tveganj; določanje stroškov tveganja,
- upravljanje tveganj: sposobnost uporabe teorij nadzora tveganja za preprečevanje in zmanjševanje tveganj; odzivanje na nenormalne situacije; načrt neprekinjenega poslovanja,
- financiranje tveganja: razdelava načrtov za sprejem tveganja in prenos tveganj, vključno z zavarovanjem; ocena stroškov tveganja po stroškovnih enotah,
- vodenje projekta: uspešno načrtovanje in izvajanje projekta ocenjevanja tveganja sektorja KI,
- zavarovalna znanja: razumevanje zavarovalnih pogodb in pravne zakonodaje; upravljanje terjatev; vzpostavitev portfelja zavarovalnih kritij; poznavanje domačega in svetovnega zavarovalnega trga; prenos tveganja; pogajanja in obnova zavarovalnih pogodb.

C. Osnovne kompetenčne spretnosti

Te spretnosti veljajo za »mehke« medosebne ali osebne spretnosti, ampak so tudi osnovna dejavnost vodstvenih veščin.

- medosebne spretnosti: sposobnost vplivati na vedenje zaposlenih za realizacijo ciljev poslovanja; vzpostaviti zaupanje, hkrati pa ohranjati zaupnost,
- vodenje: sposobnost navdihniti zaposlene za doseganje ciljev poslovanja,
- motiviranje: sposobnost pomagati drugim zaposlenim, da dosežejo svoje cilje, ki so skladni s cilji upravljavca KI,
- pogajanja: sposobnost poslušanja in upravljanja konflikta ter doseganja kompromisa pri doseganju smiselnih ciljev; spoštovanje drugih perspektiv; sposobnost združiti razne ideje v kohezivni načrt,
- skupinsko delo: sposobnost poenotiti zaposlene, da dosežejo skupni cilj.

Konceptualna in tehnična znanja ter kompetenčne spretnosti, ki so potrebna za ocenjevanje tveganj, si je možno pridobiti v okviru internega usposabljanja ali pa s pomočjo zunanjega izvajalca, ki nudi tovrstna znanja.

2.7 NADZOR NAD OBLADOVANJEM TVEGANJ

Izredni dogodki, povezani z delovanjem KI Republike Slovenije so v preteklosti vplivali na ugled in zaupanje uporabnikov v ustrezno obvladovanje tveganj za delovanje KI. Manjše število izrednih dogodkov lahko pripišemo poslovnim prevaram in drugim oblikam kaznivih dejanj, večje število pa je bilo posledica nerazumevanja dogajanja na trgu in v organizaciji. Ob tem se postavlja vrsta aktualnih vprašanj, npr.: (i) ali so izdelani ustrezni notranji pravni akti, ki določajo tudi obvladovanje tveganj, (ii) ali so kritični (in ostali) poslovni procesi v organizaciji transparentni in ustrezno dokumentirani, (iii) kakšna je izpostavljenost organizacije raznim vrstam in oblikam tveganj, (iv) ali so preverjeni scenariji možnih izrednih dogodkov, (v) ali ima organizacija vzpostavljene ustrezne preventivne in korektivne ukrepe v poslovnih procesih, (vi) kako se ocenjuje učinkovitost delovanja sistema notranjih kontrol in usposobljenost nadzornikov (npr. vodstvenega nadzora, notranje revizije) nad obvladovanjem tveganj ipd.

Tradicionalno gledano je nadzor nad obvladovanjem tveganj proces, s katerim se zagotovi, da zaposleni, organizacija in družba uresničijo svoje cilje (Velsoft, 2013). Nadzor nad obvladovanjem tveganj je skupek planiranja in nadziranja opravil. Anthony in Govindarajan (2010) ga razširita v proces, preko katerega vodstvo organizacije vpliva na zaposlene, s ciljem zmanjšanja tveganj poslovanja. Pojavile pa so se različne kritike tradicionalnega modela nadzora nad obvladovanjem tveganj, saj ta zanemarja dinamične povezave, motiviranost zaposlenih, premalo upošteva dinamično poslovno okolje, organizacijsko kulturo organizacije in mnogo drugih nefinančnih (»mehkih«) dejavnikov. Avtorji (npr. Kompare in drugi, 2006, Northouse, 2010) so zato sčasoma razširjali tradicionalni vidik nadzora s sociološko - psihološkimi vidiki; vlogo in pomenom okolja, v katerem organizacija posluje, njeno organizacijsko kulturo, kompetentnostjo zaposlenih ipd. Najbolj od vsega naj bi zaposleni cenili varnost in predvidljivost. Motivirala naj bi jih denar in strah pred kaznijo, zato želijo čim bolj predvidljivo netvegano okolje, ki jim zagotavlja občutek varnosti. Dobre (2013) ugotavlja, da navedena teorija ne velja pri tistih zaposlenih, ki čutijo, da imajo fiziološke potrebe in potrebe po varnosti zadovoljene. Njih motivirajo potrebe po socialnem priznanju in samoaktualizaciji.

Nadzor nad upravljanjem tveganj na področju KI je sestavni del upravljanja poslovnih procesov. Učinkovit nadzor nad obvladovanjem tveganj in dobro postavljen sistem notranjih kontrol lahko bistveno pripomoreta k doseganju strateških usmeritev ter planiranih ciljev

poslovanja, poleg tega pa zagotavljata poslovanje v skladu s pozitivno zakonodajo, internimi akti in dobro prakso. S tem se zlasti zmanjšujeta dve pomembni tveganji: finančna izguba in zmanjšanje zaupanja uporabnikov.

V procesu nadzora nad obvladovanjem tveganj je pomembno, da se zazna in odpravi tako možne namerne kot nenamerne napake zaposlenih, zmanjša in odpravi škodni učinek zaradi odpovedi (napake) stroja, naprave ali posledice višje sile. Nadzor nad obvladovanjem tveganj zagotavlja vodstvu organizacije, njenemu nadzornemu svetu in lastniku, da so tveganja obvladovana in da je upravljanje uspešno ter učinkovito.

Z nadzorom nad obvladovanjem tveganj je povezana organizacijska kontrola (temelji na organizacijski strukturi, dodeljevanju pooblastil ter opredelitvi pristojnosti in odgovornosti), kontrola pooblastil (posel se prekine, če ni odobren in dokumentiran) in tekoča kontrola poslovanja (primerjanje stanj sistema).

Področja nadzora nad obvladovanjem tveganj naj bodo:

- funkcijsko določena (kritični poslovni proces mora biti opravljen v določenem času),
- poslovno določena (upoštevajoč specifično naravo poslovanja),
- tehnično določena (uporaba posebnih delovno - tehničnih pripomočkov v odnosu zaposleni-stroj) in
- organizacijsko določena (npr. redni, izredni nadzor).

Sodobna ureditev nadzora nad obvladovanjem tveganj ima vsaj štiri nivoje (glej sliko 18). Prvi nivo nadzora predstavljata opravljanje vodstvenega nadzora in sistem notranjih kontrol; drugi nivo se nanaša na upravljanje s tveganji, delovanje varnostnega sistema, preverjanje kakovosti poslovanja, preverjanje skladnosti poslovanja in preiskovanje zlorab; tretji nivo je povezan z aktivnostmi notranje in zunanje revizije; četrti nivo nadzora pa se nanaša na kontrolo pristojnih državnih organov.

Slika 18: Sodobna ureditev nadzora nad obvladovanjem tveganj (interni vir ICS)

Nadzor nad obvladovanjem tveganj se nanaša tudi na razumevanje tveganj, ki jih organizacija sprejema in upravlja, na skrb, da vodstvo sprejema ustrezne proaktivne ukrepe in postopke ter aktivnosti za merjenje, spremljanje in kontroliranje teh tveganj. Izhodišča za nadzor nad obvladovanjem tveganj so:

- pozornost mora biti namenjena zlasti strateškim ciljem poslovanja in kritičnim poslovnim procesom,
- največ pozornosti naj bo namenjeno tistim ciljem poslovanja, od katerih je odvisno uspešno upravljanje finančnih tveganj in zaupanje uporabnikov storitev,
- vpeljati je treba take metode nadzora, ki ne zahtevajo veliko časa, a so kljub temu proaktivne in učinkovite,
- zagotoviti je treba učinkovit pretok informacij med vsemi pomembnejšimi organizacijskimi enotami,
- pomembna je izbira sodelavcev, ki so za delo kompetentni, usposobljeni in motivirani.

Notranji kontrolni sistem je definiran kot dobro delujoč sistem organizacijskih in operativnih kontrol. Obseg teh kontrol je na eni strani odvisen od velikosti organizacije, narave in raznolikosti kritičnih poslovnih procesov, tveganosti posameznih področij poslovanja, centraliziranosti poslovanja in delegiranja pooblastil, na drugi strani pa od uspešnosti vodenja dela in učinkovitosti informacijskega ter varnostnega sistema, ki podpirata navedeno poslovanje.

Vodstvo organizacije mora uveljaviti visoka merila etičnosti, lojalnosti in organizacijske zavesti, ki poudarjajo pomen nadzora nad obvladovanjem tveganj in notranjih kontrol. Skrbeti mora za primerno ločenost dolžnosti in da zaposleni ne dobivajo nalog z nasprotujočimi si odgovornostmi. Ugotavljati mora, kje bi lahko prihajalo do povečanega tveganja in takšna

področja čim bolj zmanjšati ter jih skrbno spremljati. Vsi zaposleni morajo razumeti svojo vlogo v notranjih kontrolnih postopkih in v njih tudi aktivno sodelovati.

Pomembnejša področja nadzora nad obvladovanjem tveganj

Pomembnejša področja nadzora nad obvladovanjem tveganj na področju KI so zlasti: organizacija, politike, postopki, zaposleni, planiranje in poročanje, kar bo pojasnjeno v nadaljevanju (Bertoncelj, 2013) .

- **Organizacija**

Kot sredstvo nadzora je potrebna ustrezna struktura vlog, pristojnosti in odgovornosti, ki so dodeljene zaposlenim za učinkovito in ekonomično doseganje ciljev poslovanja organizacije. Struktura vlog je naslednja:

- odgovornosti morajo biti razdeljene tako, da noben zaposleni ne kontrolira vseh faz poslovanja (dosledno je treba upoštevati tristopenjski princip: pripravil, kontroliral, odobril),
- vsak vodja organizacijskega dela organizacije mora imeti pristojnost, da zmanjša ali odvzame pooblastilo podrejenim,
- odgovornost zaposlenih mora biti vedno jasno določena tako, da ne bi prišlo do ne seznanjanja z delovnimi zadolžitvami, odstopanj in/ali prekoračitev,
- vodstvo organizacije, ki dodeljuje pristojnosti in odgovornosti podrejenim, mora vzpostaviti učinkovit sistem spremljanja, ki zagotavlja, da so zadolžitve tudi pravilno, kakovostno in pravočasno izvedene,
- zaposleni, kateremu je bila dodeljena neka odgovornost in pristojnost, jo mora realizirati brez stalnega neposrednega nadzora, vsako izjemo pa mora obvezno preveriti pri vodji organizacijskega dela organizacije,
- organizacija poslovanja mora biti dovolj fleksibilna, da se lahko hitro realizirajo spremembe v strukturi poslovanja, v primeru sprememb načrtov, politik in predmetov poslovanja,
- organizacijska struktura organizacije naj bo čim bolj preprosta in enostavna,
- organizacijska struktura organizacije in navodila za delo morajo omogočiti dobro razumevanje organiziranosti, nivoje pooblastil in pristojnosti ter porazdelitev odgovornosti.

- **Politike**

Politika je vsako pravilo, ki zahteva, vodi ali omejuje poslovanje organizacije KI. Politike morajo upoštevati naslednja načela:

- morajo biti jasno določene in zapisane, v obliki poslovnika kakovosti, pravilnikov, delovnih navodil, poslovnih aktivnosti, zapisov kakovosti ipd.,
- morajo biti skladne z zakoni in internimi akti ter konsistentne z vrednotami, vizijo, poslanstvom in strategijo ter družbeno odgovornostjo organizacije,
- morajo biti jasno predstavljene vodjem organizacijskih enot organizacije in zaposlenim,
- oblikovane morajo biti tako, da vzpodbujajo učinkovito in gospodarno opravljanje poslovnih procesov organizacije, zagotavljajo varovanje njenega premoženja in preprečujejo aktivnosti, ki ogrožajo družbeno odgovornost organizacije,
- redno se mora preverjati ustreznost politik in jih ustrezno prilagajati nastalim spremembam in razmeram.

- **Postopki**

Postopki so metode za izvedbo aktivnosti v skladu s predpisano politiko. Poleg zahtev iz zgoraj navedene točke je za postopke pomembno še:

- postopki se morajo izvajati tako, da delo vsakega zaposlenega avtomatično nadzoruje drugi, ko izvaja svoje zadolžitve, kar se ponavlja in izmenjuje (odvisno od vrste posla),
- obseg in intenzivnost avtomatičnih kontrol je odvisna od stopnje tveganosti (izgube in/ali napake), primerjave med stroški in koristmi, števila in usposobljenosti zaposlenih,
- za ne avtomatično delo postopki ne smejo biti preveč podrobni in natančni, saj mora obstajati tudi možnost lastne presoje,
- morajo biti preprosti in učinkoviti kot je le možno, ob upoštevanju načel ekonomičnosti,
- ne smejo biti dvomljivi, nasprotujoči, nerazumljivi, posebna pozornost naj bo namenjena izogibanju podvajanja dela,
- redno se mora preverjati njihova ustreznost in jih prilagajati nastalim spremembam.

- **Zaposleni**

Zaposleni morajo biti za delo, ki jim je dodeljeno, ustrezno usposobljeni, motivirani in nadzorovani. Zato je potrebno, da:

- se morajo zaposleni stalno izobraževati in usposabljati, tako da ostajajo v delovni pripravljenosti in da so seznanjeni s strokovnimi novostmi,
- morajo imeti informacije o delu in odgovornosti ostalih, saj to omogoča boljše razumevanje lastnih zadolžitev in odgovornosti kot sestavnega dela celote,
- delovanje vseh zaposlenih se mora občasno preveriti, zaposlene je potrebno z

ugotovitvami seznaniti in jim dati priložnost, da po potrebi izboljšajo svoje delo ali da se dodatno usposobijo.

- **Planiranje**

Planiranje poslovnih aktivnosti organizacije se nanaša na pričakovane rezultate poslovanja. Pri tem je potrebno upoštevati:

- zaposleni, ki je odgovoren za doseganje določenih postavljenih ciljev, naj tudi sodeluje pri pripravi planov aktivnosti,
- zaposleni morajo biti seznanjeni z ustreznimi informacijami o izdelavi planov in o vzrokih za morebitna odstopanja od planiranih aktivnosti,
- vsi delni plani se morajo povezovati v celotni plan aktivnosti organizacije, skupni plan pa naj bi prikazoval zlasti možne dosegljive cilje poslovanja organizacije,
- predmet planov morajo biti merljive kategorije,
- plani pomagajo pri organizacijskem strukturiranju poslovnih procesov in so oblika, s katero uvajamo družbeno odgovornost ter urejenost poslovanja,
- dejanski poslovni rezultati se primerjajo s planiranim rezultatom in ob ugotovitvi uspešnosti ali neuspešnosti se odgovorne za rezultat nagradi, oziroma sankcionira.

- **Poročanje**

Vodstvo organizacije sprejema odločitve na podlagi prejetih podatkov in informacij. Poročila morajo biti točna, nepristranska, jasna, pravočasna, vsebinsko jedrnata, popolna in ekonomična. Zato je potrebno, da:

- se poročilo izdela brez napak, v skladu z dodeljenimi odgovornostmi in pristojnostmi,
- je nepristransko poročilo pošteno, objektivno, brez predsodkov in izhaja iz strokovno uravnovešenih ocen vseh ustreznih dejstev ter okoliščin,
- morajo zaposleni in organizacijske enote poročati le o stvareh, za katere so odgovorni,
- stroški poročanja niso manjši od ugodnosti, pridobljenih z uporabo poročil,
- je poročilo jedrnato, preprosto in enostavno (razumljivo in logično, brez nepotrebnih izrazov, podati mora vse pomembne podatke in informacije, usmerjeno mora biti v bistvo in se izogibati nepotrebnim dodelavam, odvečnim podrobnostim, podvajanju in gostobesednosti), kot je le mogoče. Izrazoslovje in terminologija naj bo strokovno jasna in dosledna,
- če je primerno, naj poročilo praviloma vsebuje primerjave,
- če poročilo ni numerično, ga mora zaposleni izdelati tako, da bodo uporabniki poročila opozorjeni, z ustreznimi poudarki na posebnosti, odstopanja ipd.,
- vrednost poročila določa pravočasnost, tudi na račun njene popolnosti,

- je letno treba preveriti upravičenost potrebe po posameznih poročilih in njihovi operativni ter analitični uporabnosti.

Celosten vidik nadzora nad obladovanjem tveganj

Celosten vidik nadzora nad obvladovanjem tveganj se je razvil kot odgovor na nekatere pomanjkljivosti tradicionalnega modela in pomeni njegovo razširitev. Tradicionalni vidik nadzora naj bi se pri tem usmerjal preveč na kontrolo zaposlenih, kot pa na kontrolo njihovih aktivnosti znotraj organizacije. Za uspešnost nadzora je potrebno delegirati odgovornost, upoštevati dinamične spremembe in se jim pravočasno prilagajati, znati iskati povezave med preteklimi in sedanjimi tveganji ter jih smiselno prilagoditi za prihodnost.

V teoriji dobri sistemi nadzora spodbujajo, da aktivnosti zaposlenih, ki so povezane z njihovimi lastnimi interesi, pozitivno vplivajo na doseganje ciljev v organizaciji. Zavedamo se, da je popolno skladnost ciljev posameznika s cilji organizacije težko doseči. Pomembno je, da nadzor nad obvladovanjem tveganja doseže vsaj omejen cilj in sicer, da zaposleni ne deluje proti interesom v organizaciji. Zato je potreben ustvarjalni dialog med vodstvom in zaposlenimi, ki razkriva, katere interese imajo zaposleni in ali so ti usklajeni z vizijo, vrednotami in strategijo organizacije. Menimo, da vodje še vedno porabijo preveč časa in energije z zagotavljanjem, da se delo opravlja pravilno, namesto da bi razmišljali o tem, katero delo je pravo in ga je treba prednostno opraviti.

Lastnikova naravna težnja po večanju dobička organizacije se odraža v vse večjih pritiskih na zaposlene, predvsem v smeri večanja storilnosti. S tem se povečujejo tudi tveganja, ki jih vodstvo težko sprejema in obvladuje. Nadzor nad obvladovanjem tveganj je še posebno zanimiv tudi zato, ker se v zvezi z njim zelo neposredno in nazorno soočata dva pomembna interesa. Na eni strani je interes vodstva, da zaposleni čim bolje in učinkoviteje dela, na drugi strani pa je interes zaposlenega, da ga zahteve vodstva povsem ne razčlovečijo in mu tudi na delovnem mestu dopustijo čim večjo zasebnost[8]. Danes moderna tehnologija vodstvu omogoča že skoraj popoln nadzor nad delom in (zunanjim) vedenjem zaposlenih. O tem, koliko je to pravno dopustno, etično in v skladu z deontološkim kodeksom, so mnenja strokovnjakov, vodstva in zaposlenih še vedno različna.

Pojavlja se pojem »pohlepni algoritem«, kjer je dejansko najboljša izbira za nekaj, čemur navadno dajemo prednost. To se navezuje tudi na pohlep po redkih dobrinah, kot na nekaj dobrega. Raziskava je pokazala (Sullivan, Thompson, 2013), da je dolgoročni pohlep morda še sprejemljiv, medtem ko kratkoročni pohlep v smislu »tukaj in zdaj« deluje samo nekaj časa.

[8] Posameznik na delovnem mestu ni pasiviziran, četudi bi to hotel. Organizacija ga usmerja, nadzoruje, prisiljuje in neredko lahko tudi občutno prizadene, kadar se ne ravna po pravilih.

Težko je ugotoviti kdaj se določena situacija postopno slabša in se povečujejo tveganja za nastanek izrednega dogodka. Pogosto se stanje slabša še počasneje od komaj opazne razlike. Vodstvo si mora postaviti jasne kriterije, da bo lahko objektivno spremljalo nadzor nad obvladovanjem tveganj, ugotoviti mora kaj je normalno (pričakovano) poslovanje in kje to ni ter odpraviti napake v poslovanju. Želja po popolnosti preprečuje, da bi bil nadzor nad obvladovanjem tveganj popoln, saj so lahko standardi, ki si jih vodstvo postavi, previsoki. Rešitev je v tem, da naj se sprejme dejstvo, da popolnosti ni mogoče doseči. Pojavlja se nesposobnost zaposlenega s soočanji s tveganji (nerazumevanje tveganja)[9].

Nadzor nad obvladovanjem tveganj z vidika KI se izvaja v različnih sektorjih, z različno organizacijsko kulturo, v organizacijah, ki se razlikujejo po namenu poslovanja, velikosti, zapletenosti in organizacijskem ustroju, izvajajo pa ga posamezniki v organizaciji ali zunaj nje.

Nadzor nad obvladovanjem tveganj zagotovo vpliva na dolgoročen obstoj organizacije. Po nekaterih mnenjih pa je popolni nadzor nad obvladovanjem tveganj organizacije skoraj nemogoč. Poleg splošne družbene negotovosti vedno obstaja tudi določena stopnja prikritega notranjega odpora[10], zato je pomembno, da imajo zaposleni občutek pripadnosti in odgovornosti, ter da povežejo kolektivne interese skozi odprto komunikacijo. Opozarjamo na pojav moralnega hazarda, na šibkost sistema vodenja in upravljanja organizacij, na zlorabo temeljnega načela zaupanja med udeleženci na trgu.

Nadzor nad obvladovanjem tveganj moramo v bodoče še bolj podrobno proučevati, ne samo zato, da bi ga bolje razumeli, temveč zato, da bi ga lahko spreminjali in dopolnjevali.

[9] Posameznik in organizacije, so kljub različnim notranjim in zunanjim ogrožanjem, postali preveč naklonjeni sprejemanju tveganja, nezavedajoč se, kako lahko tvegano je to.

[10] V obliki npr.: odpor do službenih avtoritet in nadrejenih, frustracija zaradi službe, nemotiviranost za delo, maščevanje, neprimerno vedenje v socialnem okolju ipd.

3 PREDSTAVITEV PODROČJA OCENJEVANJA TVEGANJ (ANG. RISK ASSESSMENT) S POUDARKOM NA POSEBNOSTIH OCENJEVANJA TVEGANJ NA PODROČJU KRITIČNE INFRASTRUKTURE

Za pravilno razumevanje procesa ocenjevanja tveganj za delovanje KI je treba podrobno razumeti proces ocenjevanja tveganja za delovanje KI. V nadaljevanju bo podrobno predstavljen vsebinski pregled posameznih korakov metodološkega dela ocenjevanja tveganj. Pred tem je izveden kratek pregled pojma in vloge KI v Republiki Sloveniji. Kot zapisano v uvodu je področje, ki opredeljuje različne metodologije ocenjevanja tveganj, izredno obširno. V študiji želimo prikazati in analizirati tiste najpomembnejše in najbolj široko uporabljene modele za ocenjevanje tveganj. Omenjen prikaz in podrobno razumevanje kompleksnosti posameznih metodologij nam bo v pomembno pomoč v nadaljevanju, pri izdelavi metodološkega okvirja za ocenjevanje tveganj za delovanje KI Republike Slovenije.

3.1 PREDSTAVITEV KRITIČNE INFRASTRUKTURE V REPUBLIKI SLOVENIJI

KI je globalna kategorija v dojemanju pomembnosti določenega dela gospodarstva in določenega dela državnih instirtucij. V novejšem času pa vse bolj prihaja v ospredje tudi v posameznih državah sveta, zlasti ko gre za krizne situacije v katerih morajo neperekinjeno delovati določeni gospodarski in negospodarski sektorji. V državah zahodnega sveta, zlasti v tistih, ki so doživele teroristične napade, katastrofalne naravne in ekološke nesreče, ter odmevna kriminalna dejanja, je kritična infrastruktura povsem udomačen in razumljiv pojem. Navajamo kako je kritična infrastruktura definirana po ameriških merilih. Gre za nekoliko širšo definicijo oziroma obseg kritične infrastrukture kot v Evropi, saj so ZDA doživele šokantne teroristične napade, kot tudi katastrofalne industrijske nesreče (denimo: razpadi elektroenergetskih sistemov), naravne nesreče (orkan Katrina, poplave, ipd.) in ekološke nesreče (izlitja nafte v morje). Tako po ameriških merilih vitalno (ključno) kritično infrastrukturo sestavljajo gospodarski sektorji, poleg tega pa še državno-poslovne zgradbe in institucije, kot sledi (Murray, 2007):

- poljedelstvo, kmetijstvo in (pre)hrana,
- voda in vodovodni sistemi,
- javno zdravstvo (z urgenco),
- zaščita in reševanje,
- obrambna industrija,
- telekomunikacije,
- energetika,

- transport,
- bančništvo in finance,
- kemikalije in nevarne snovi,
- pošta, luke in pomorski promet.

Državno-poslovne zgradbe in državne institucije pa so naslednje:

- spomeniki nacionalnega pomena,
- jezovi, pregrade in nasipi,
- skladišča, deponije in ravnanje z radioaktivnimi snovmi,
- vladne in druge državne zgradbe in osebje,
- pomembne poslovne zgradbe.

V Evropi se je resnejša razprava o KI začela leta 2005, ko je Evropska komisija sprejela Program zaščite kritične infrastrukture (Green Paper on a European programme for critical infrastructure protection, COM (2005) 576 final, Brussels, 17. 11. 2005), ki v Aneksu 2 (Annex 2 – Indicative list of Critical infrastructure sectors), podaja seznam gospodarskih sektorjev, ki so opredeljeni kot KI. Kasneje je Evropska komisija izdala še določene direktive, ki so zavezovale tudi Republiko Slovenijo, da uredi to področje. Tako je Vlada RS je s sklepom št. 80000-2/2010/3, z dne 19. 4. 2010, sprejela definicijo KI, ki je od uveljavitve ZKI vključena tudi v slednjega: »KI državnega pomena v Republiki Sloveniji obsega tiste zmogljivosti in storitve, ki so ključnega pomena za državo, in bi prekinitev njihovega delovanja, ali njihovo uničenje pomembno vplivalo in imelo resne posledice na nacionalno varnost, gospodarstvo, ključne družbene funkcije, zdravje in zaščito ter družbeno blaginjo.«

Sklep Vlade RS, št. 80200-1/2012 z dne 17. 10. 2012 določa sektorje KI, ki so:

- sektor KI, ki zagotavlja energetsko podporo,
- sektor KI, ki zagotavlja prometne povezave,
- sektor KI, ki zagotavlja preskrbo s hrano,
- sektor KI, ki zagotavlja preskrbo s pitno vodo,
- sektor KI, ki zagotavlja zdravstveno oskrbo,
- sektor KI, ki zagotavlja finance,
- sektor KI, ki zagotavlja varstvo okolja,
- sektor KI, ki zagotavlja informacijsko in komunikacijsko podporo (sektor informacijsko-komunikacijskih omrežij in sistemov).

Tej opredelitvi sledi tudi ZKI (Ur. l. RS, št. 75/2017), ki v 4. členu navaja naslednje sektorje KI:

- sektor energetike,
- sektor prometa,

- sektor prehrane,
- sektor preskrbe s pitno vodo,
- sektor zdravstva,
- sektor financ,
- sektor varovanja okolja,
- sektor informacijsko-komunikacijskih omrežij in sistemov.

Po prioritetah delovanja oziroma neposrednem vplivu na delovanje drugih sektorjev je KI razvrščena po naslednjem prioritetnem vrstnem redu (Sklep Vlade RS št. 80200-2/2013/3, z dne 9. januarja 2014):

- zagotavljanje električne energije,
- informacijsko komunikacijska podpora,
- preskrba s pitno vodo,
- preskrba s hrano,
- zagotavljanje zdravstvene oskrbe,
- preskrba z naftnimi derivati,
- zagotavljanje železniškega prometa,
- zagotavljanje letalskega prometa,
- delovanje pristaniške dejavnosti,
- preskrba s plinom,
- delovanje plačilnega prometa,
- zagotavljanje oskrbe z gotovino,
- delovanje državnega proračuna,
- varovanje zdravega okolja.

Razvidno je, da sta zagotavljanje dobave električne energije in informacijsko-komunikacijska podpora najpomembnejši dejavnosti oz. storitvi v RS, saj je – po mnenju medresorske skupine, ki je sklep vlade pripravljala - njuno pravilno in neprekinjeno delovanje krovnega pomena za celotno družbeno dinamiko v RS; torej za državne institucije, gospodarstvo, civilno družbo in prebivalstvo. To pomeni, da brez električne energije, brez informacij in brez komunikacij ni učinkovitega delovanja vseh drugih sektorjev KI.

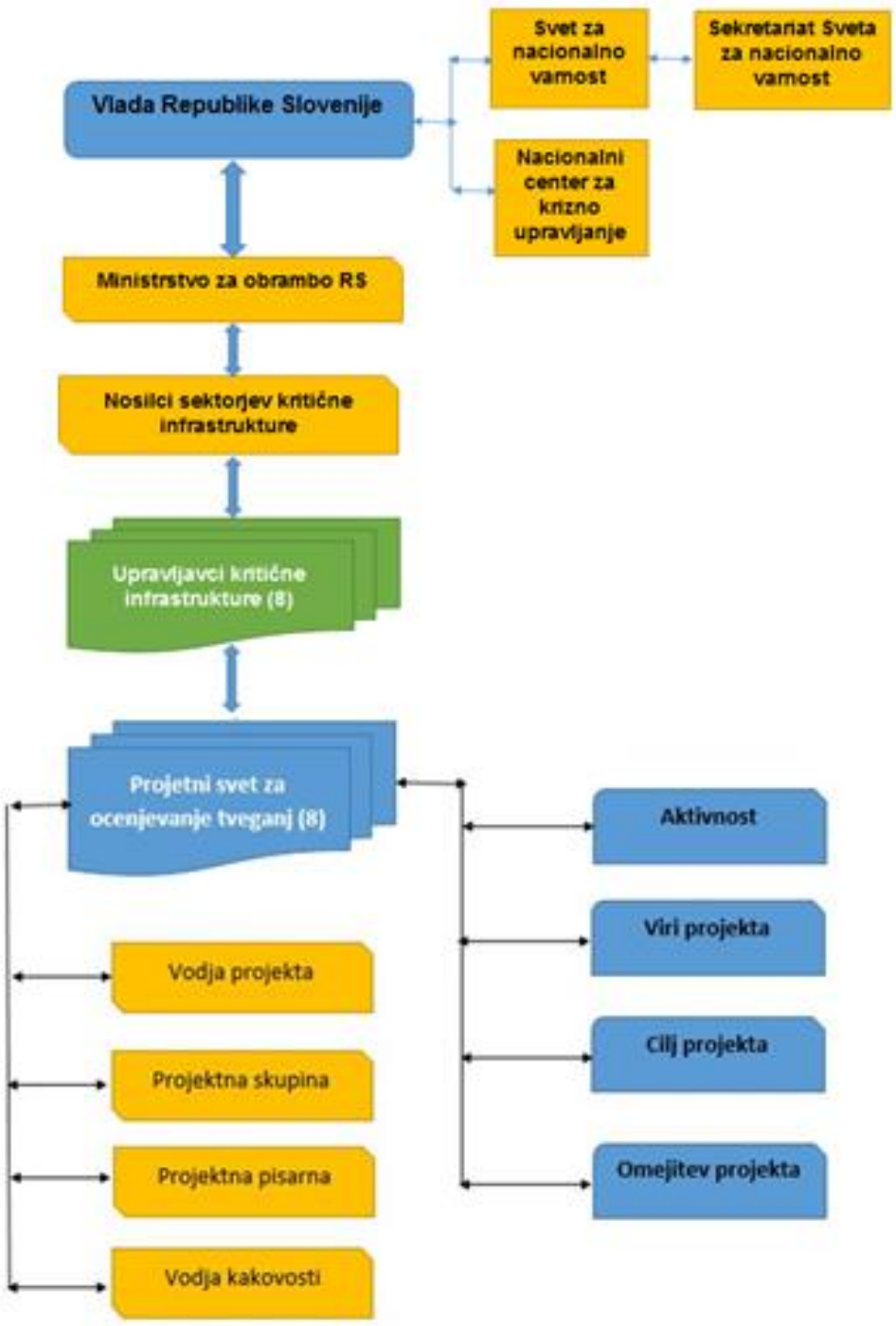
V poglavju 3.4 je predstavljeno obvladovanje tveganj z vidika specifike delovanja posameznih sektorjev KI. Izdelava uporabne metodologije za ocenjevanje tveganj za delovanje KI je v veliki meri pogojena s poznavanjem organiziranosti, delovanja in problematike vseh sektorjev KI.

3.2 PROJEKTNI PRISTOP K OCENJEVANJU TVEGANJ

Splošno je znano, da se k posameznim streteškim nalogam pristopa na projektni način. Tako je smiselno, da se tudi na področju upravljanja tveganj v KI pristopa na podlagi projektne metodologije. Priporočamo, da naročnik na podlagi te študije vzpostavi projekt ocenjevanja tveganj v KI v katerem opredeli organiziranost projekta, cilje projekta, projektno skupino z ustreznimi referencami in kompetencami, potrebe po upravljanju in obvladovanju tveganj v KI, naloge nosilcev in upravljavcev, izhodišča (pravne in strokovne podlage), politiko in proces ocenjevanja tveganj v sektorjih KI ter proces usposabljanja odgovornih oseb za tveganja.

Nekaj informacij o projektnem pristopku je predstavljenih v nadaljevanju.

Metodologija vodenja projektov se ukvarja z različnimi objekti, kot so faze, aktivnosti, viri, izdelki ipd. Nekateri objekti in povezave med njimi so razvidne iz metamodela projektnega pristopa, ki je prikazan na sliki 19.



Slika 19: Metamodel projektnega pristopa za ocenjevanje tveganj (interni vir ICS)

Vsak upravljavec KI določi projektno skupino za ocenjevanje tveganj na področju KI v svojem sektorju. Aktivnosti v tem postopku so namenjene vzpostavitvi organizacijske strukture projekta, kjer so natančno določeni nosilci vlog, njihove naloge in medsebojna razmerja, kar je ključnega pomena za učinkovito izvajanje projekta.

Postopek je naslednji:

- predstavitev projekta: opis obstoječega stanja, cilji projekta, vsebina in obseg projekta, omejitve, predpostavke,
- organizacija projekta: organizacijska shema projekta, imenovanja nosilcev vlog na projektu (v nadaljevanju), komuniciranje, nadzor in poročanje, obveznosti izvajalca,
- imenovanje sponzorja projekta (vodje projektnega sveta), drugih članov projektnega sveta in Vodje projekta. Projektno vodenje je učinkovita uporaba znanja, veščin, tehnik in orodij v aktivnostih projekta za izpolnitev projektnih zahtev, realiziramo ga z uporabo in integracijo procesov projektnega vodenja: zagon, planiranje, izvajanje, spremljanje, kontroliranje, končanje projekta, testiranje ocen, vzdrževanje, izboljšave. Pomembne prvine projektnega vodenja, ki jih projektna skupina mora imeti so: vodenje, timsko delo in menedžment virov,
- imenovanje članov projektne skupine in vodje kakovosti,
- imenovanje projektne pisarne na projektu (opcijsko),
- definiranje ciljev projekta, predpostavk projekta in dejavnikov tveganja projekta. Dobro določen cilj pove: Kaj želimo doseči? Kako bomo to dosegli? Kdo bodo glavni koristniki? Cilj mora biti: jasno in natančno opisan (določimo vmesne in končne cilje), merljiv (cilji morajo omogočati merjenje in ocenjevanje), uresničljiv (postavimo si dosegljive cilje), realističen (postavimo si realne cilje) in imeti končni rok izdelave ocene tveganj,
- omejitve, ki se nanašajo na projekt. Prva vrsta omejitev so časovne omejitve, če mora biti celoten projekt ali del projekta dokončan do vnaprej definiranega roka. Takšno časovno omejitev je treba upoštevati pri pripravi plana. Lahko gre za drugačno vrsto časovne omejitve, kjer določenih aktivnosti ne bo mogoče pričeti, dokler ne bodo dokončane določene aktivnosti na nekem drugem projektu. Druge vrste omejitev so finančne omejitve, ki jih je treba upoštevati na projektu. Omejitev je lahko obseg finančnih sredstev, ki so na voljo za izvedbo projekta, ali pa dinamika razpoložljivosti finančnih sredstev. Finančne omejitve so običajno v konfliktu s časovnimi omejitvami. Zato je pomembno, da se vse vrste omejitev navedejo, potem pa mora rojektni svet odločiti, katere omejitve je treba upoštevati (ali podaljšati rok zaključka projekta ali zagotoviti predvidena sredstva v krajšem časovnem obdobju). Med ostale omejitve lahko spada kadrovska problematika ali razpoložljivost zunanjih strokovnjakov, ki so potrebni za izvedbo aktivnosti in zahtevajo specifična znanja (tehnologija, razpoložljivost človeških virov ipd.),
- predpostavke, na katerih temelji izvedba projekta, zlasti plan projekta. Predpostavke se nanašajo na aktivnosti, dogodke ali odločitve v prihodnosti, ki jih ni mogoče natančno časovno ali vrednostno opredeliti, so pa zelo pomembni za izvedbo projekta in pripravo plana projekta. Predpostavke so tudi v povezavi z omejitvami. Naslednja časovna predpostavka je obseg delovnega časa, ki ga bodo člani projektne skupine

namenili za delo na projektu. Od obsega delovnega časa je namreč odvisna časovna dinamika projekta, kar je treba na ustrezen način upoštevati v terminskem planu projekta,

- komunikacija na projektu, nadzor in poročanje se nanaša na mehanizme za nadzor projekta na različnih nivojih in načine poročanja. Poudarek je na opisu nadzora na nivoju sponzorja projekta (Vodje projektnega sveta). Sponzor projekta ima možnost izvajati nadzor na rednih sestankih projektnega sveta ali preko rednih poročil o napredku. Nadzor, ki ga izvaja Vodja projekta je lahko tudi formaliziran. Poročanje je podlaga za nadzor, zato je treba iz množice poročil izbrati primerna za ta konkretni projekt in določiti njihovo frekvenco,
- krovni plan projekta je razdeljen na več podpoglavij: strukturni diagram ocen, mrežni diagram ocen, krovni terminski plan projekta, plan (kadrovskih) virov, plan stroškov in opredelitev financiranja projekta ter plan kakovosti,
- delegiranje nalog. Vodja projekta predlaga ustrezno metodologijo ocenjevanja tveganj in delegira naloge z vso potrebno dokumentacijo ter informacijami. Vodja projekta preveri, da ima vodja projektne skupine vire za izvedbo naloge. Vodja projekta identificira probleme ali tveganja v povezavi z nalogo in na njih opozori vodjo projektne skupine. Vodja projekta preveri ali vodja projektne skupine pravilno razume delegirano nalogo in jo je pripravljen izvršiti v danih okvirih,
- poročanje o napredku projektnemu svetu in njegovemu vodji zagotovi informacije o stanju in napredovanju projekta. Informacije prejme v obliki poročila o napredku. Frekvenco poročanja določi projektni svet in je zapisana v vzpostavitvenem dokumentu projekta. Vodja projekta zbere informacije iz kontrolnih poročil vodij projektnih skupin, identificira trenutne ali potencialne probleme, izdela poročilo in ga posreduje sponzorju projekta ter ostalim članom projektnega sveta in drugim dogovorjenim prejemnikom,
- presoja kakovosti se nanaša na izvedbo presoje kakovosti in združevanju rezultatov presoje. Presojevalci do določenega roka pregledajo ocene tveganj, vodja kakovosti pa s pomočjo presojevalcev oblikuje seznam korektivnih ukrepov,
- vodja projekta v zaključno poročilo projekta vključi primerjavo planiranega in dejanskega poteka projekta z vidika upravljanja tveganj, stroškov in rokov. Podatki izhajajo iz plana projekta in poročil o presoji kakovosti. Vodja projekta v zaključnem poročilu opiše tudi odstopanja od plana projekta. Zaključno poročilo se predstavi projektnemu svetu. Če se projekt nadaljuje z naslednjo fazo, se priloži zaključnemu poročilu faze plan še naslednje faze in sklep o nadaljevanju projekta.

Več o vodenju projekta je predstavljeno v vodniku znanja projektnega vodenja A Guide to the Project Management Body of Knowledge (PMBOK)[11], ki opisuje 44 procesov projektnega vodenja, na 9 področjih znanja.

Področja znanja projektnega vodenja se nanašajo na obvladovanje integracije projekta, časa projekta, stroškov projekta, obvladovanje kakovosti projekta, človeških virov v projektu, komuniciranja v projektu in obvladovanje oskrbovanja projekta.

Na sliki 20 so predstavljena znanja, ki so potrebna za projektno vodenje. Nanašajo se na znanje s področja korporativne varnosti, upravljanja tveganj, poznavanje poslovnih procesov, standardov in predpisov, razumevanje projektnega okolja, ogrožanj in tveganj v njem, znanja in spretnosti s področja vodenja ter spretnosti v medsebojnih odnosih.

Slika 20: Znanje projektnega vodenja (interni vir ICS)

Pri realizaciji projekta ocenjevanje tveganj se lahko pojavijo naslednji problemi: neustrezni cilji projekta, neustrezno upravljanje s tveganji, kadrovske težave, neustrezen finančni načrt projekta, spremembe projekta ali nejasnost načrtov, neustrezna komunikacija, nerealistični termini izvedbe projekta, neustrezna usposobljenost članov, zunanji vplivi (podizvajalci), neustrezne zmogljivosti, nemotiviranost ali neodgovornost članov ipd.

[11] Več dostopno na http://www.cs.bilkent.edu.tr/~cagatay/cs413/PMBOK.pdf.

3.3 PREGLED NEKATERIH MODELOV ZA OCENJEVANJE TVEGANJ, KI SO PRIMERNI ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Že iz prvega dela te študije je razvidno, da obstaja veliko modelov, metod in metodologij za ocenjevanje tveganj, ki so splošne ali usmerjene na določeno področje. Iz množice metod in modelov v tem uvodnem pregledu navajamo samo nekatere, ki so zanimivejše za obravnavo tveganj za delovanje KI. To so:

- Splošni model obvladovanja tveganj.
- Model izrednih dogodkov in njihovih posledic.
- Andersenov model - Universal Business Risk Model Arthur Andersen.
- Model varnostnih tveganj za delovanje KI na bazi napadov na kritično infrastrukturo in na bazi učinkovitosti ukrepov zaščite $R = P_A * (1 – P_E) * C$.
- Model obvladovanja tveganj za delovanje KI na bazi posledic izrednih dogodkov, ranljivosti in groženj $R = f (C, V, T)$.
- Model obvladovanja tveganj na bazi notranje integritete in sinergije v gospodarski družbi.
- Method Organised for a Systemic Analysis of Risk – MOSAR – sistemska/sistematična analiza tveganj.
- Enterprise Risk Management Framework, The Committee of Sponsoring Organization of the Treadway Commission. COSO.
- Preliminary Hazard Analysis – PHA – predhodna analiza nevarnosti.
- Fault Tree Analysis – FTA – analiziranje verjetnosti napak in (ne)zanesljivosti opreme v procesih.
- Failure Mode Effect Analysis – FMEA – analiza možnih napak in njihovih posledic.
- Control Objectives for Information and Related Technologies – COBIT – ugotavljanje tveganj v informacijski tehnologiji in informacijskih sistemih.
- Hazards and Operability Study – HAZOP – analiza nevarnosti v delovnih procesih – varnost in zdravje pri delu.
- Hazard Identification – HAZID – prepoznavanje nevarnosti v zgodnjih (začetnih) fazah nastajanja proizvoda, storitve in projekta.
- Rapid Risk Assessment – RRA – hitra analiza tveganj.
- Business Impact Analysis BIA – analiza poslovnih vplivov (tudi poslovnih tveganj) v povezavi s standardom ISO 22301, 22313, 22317 in ISO/IEC 27001.
- SPIRS (Seveso Plant Information Retrieval System) – nevarnosti in tveganja na področju varstva okolja in naravnih nesreč – Direktivi EU SEVESO II in SEVESO III/2015, v povezavi s COMAH/2015.

Pri preučevanju navedenih in drugih metod (ki niso navedene v tem gradivu) obvladovanja tveganj je treba ugotoviti katere so primerne za ocenjevanje tveganj za delovanje KI. Ožje

gledano je vsaka metoda uporabna za določeno področje, vprašanje pa je, če jo lahko umestimo kot sistemsko orodje za obvladovanje tveganj v vseh sektorjih KI.

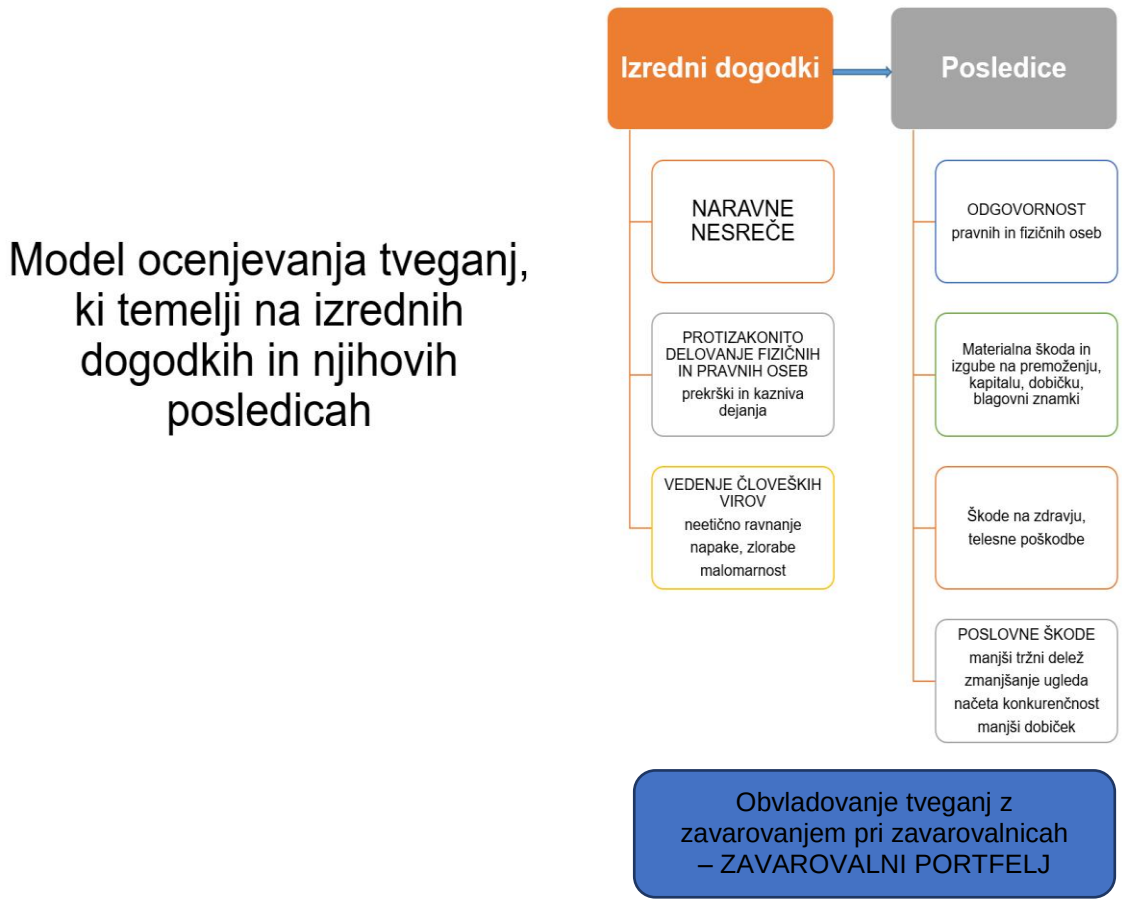
V nadaljevanju so predstavljene samo nekatere metode oziroma modeli, ki so po naši presoji lahko primerni za razpravo o ocenjevanju tveganj za delovanje KI. Osredotočamo se torej samo na nekaj metod ali modelov, ki so na kratko predstavljeni v nadaljevanju.

Seveda je treba proučiti celotno paleto modelov in metod obvladovanja tveganj, da se ugotovi, kateri že znani ali manj znani pristopi k obvladovanju tveganj so uporabni za KI. Iz podatkov nekaterih upravljavcev KI je razvidno katere metode so uporabili za svoje potrebe obvladovanja tveganj, kar je ena od izhodišč za izvedbo študije in pripravo metodologije za ocenjevanje tveganj za delovanje KI.

Možno je uporabiti še Hazard Analysis (Metoda za predhodno analizo tveganj), MOSAR (Method for a Systemic of Risk, slo. Metoda za sistemsko/sistematično analizo tveganj), Business Impact Analysis (BIA analiza – ISO/IEC 27000) in Delfi metodo, ki jo lahko uporabi skupina strokovnjakov, ki raziskuje obvladovanje tveganj v določenih gospodarskih družbah.

3.3.1 Model izrednih dogodkov in posledic

Kot je razvidno iz predstavljenega modela so izredni dogodki (škodni pojavi, nevarni dogodki, incidenti) glavni vir poslovnih, finančnih, informacijskih, varnostnih in drugih tveganj. Vsak izredni dogodek (naravna nesreča, prometna nesreča, delovna nesreča, vdor v informacijako infrastrukturo, vlom, iznos zaupnih dokumentov, požar, eksplozija, goljufija, korupcija, teroristični napad, okvara na ključni opremi, itd.) povzroči poslovne, materialne, finančne, človeške in moralne posledice. Sproža pa tudi objektivno odgovornost posameznika, skupine in organizacije, ki pa se ji (v praksi) vsak po svoje izmikajo.



Slika 21: Model ocenjevanja tveganj, ki temelji na izrednih dogodkih in njihovih posledicah (Vršec, 2010)

Če pri izdelavi metodologije za potrebe obvladovanja tveganj za delovanje KI zanemarimo izdelavo ocene ranljivosti in ogroženosti, ne moremo ugotoviti kateri verjetni izredni dogodki se lahko dogodijo na kompleksu gospodarske družbe, zaradi česar nimamo pravih podatkov za prepoznavanje, ocenjevanje in vrednotenje poslovnih, finančnih, informacijskih, varnostnih in drugih tveganj. Potemtakem lahko rečemo, da je model izrednih dogodkov in njihovih posledic nujno izhodišče ali orodje pri pripravi dokumenta o ocenjevanju tveganj za delovanje (sektorjev) KI.

3.3.2 Andersenov model (ang. Universal Business Risk Model Arthur Andersen)

Obstaja nekaj metodologij obvladovanja tveganj na različnih gospodarskih in negospodarskih področjih. Med znanimi metodologijami je tudi vsesplošen Andersenov model upravljanja tveganj, ki ga uporabljajo tudi nekatere slovenske gospodarske družbe. To je model, ki zajema politična, okoljska, poslovna, ekonomska, proizvodna, tržna, finančna, informacijska, logistična, varnostna in druga tveganja.

V večini tveganj procesov (tveganj delovanja), tveganj pooblaščanja, finančnih tveganj in tveganj informacij, se torej prepletajo tudi varnostna tveganja, ki jih je treba spoznati in vključiti v proces upravljanja s tveganji. V strukturi tveganj je pomembno spoznati zlasti naslednje tipe varnostnih tveganj:

- tveganja zaradi nedorečenosti v povezovanju posameznih področij varnosti (varstvo pred naravnimi in industrijskimi nesrečami, varnost in zdravje pri delu, požarna varnost, varstvo okolja, fizično in tehnično varovanje, civilna zaščita, varovanje informacij, varstvo podatkov, varovanje poslovnih skrivnosti, itd.), kar povzroča neučinkovitost in prevelike stroške,
- požarna in eksplozijska tveganja, ki so sestavni del ravnanja z nevarnimi snovmi, kemikalijami in emisijami,
- tveganja na izpostavljenih (nevarnih) delovnih mestih – tveganja delovnih nesreč,
- informacijska tveganja – proučitev varnostnih mehanizmov v računalniškem omrežju in poslovnem informacijskem sistemu – informacijska nesreča, vdor v informacijski sistem,
- tveganja kriminalne narave,
- logistična tveganja – proučitev varnostnih ukrepov v procesih dobave, proučitev varnostnih ukrepov pri poslovnih partnerjih, proučitev interne logistične varnosti,
- tveganja na področju fizičnega in tehničnega varovanja – proučitev lastnega in pogodbenega fizičnega varovanja ter proučitev učinkovitosti tehničnega varovanja.

ANDERSENOV MODEL PREPOZNAVANJA TVEGANJ		
Tveganja procesov **Tveganja delovanja**	**Tveganja pooblaščanja**	**Finančna tveganja**
• zadovoljstvo kupcev • človeški viri • intelektualni kapital • razvoj novih proizvodov • učinkovitost operative • razmik zmožnosti • proizvodni časi • razpoložljivost virov • prodajni kanali • partnerske povezave • skladnost s predpisi • prekinitev poslovanja • napake na proizvodu/storitvi • onesnaževanje okolja • varnost in zdravje pri delu • zmanjšanje ugleda in dobrega imena	vodenje pooblastila outsourcing nagrajevanje po uspešnosti pripravljenost k spremembam komunikacijski kanali **Tveganja informacijske tehnologije** pomembnost pravilnost dostop v računalniško omrežje razpoložljivost informacij informacijska infrastruktura **Tveganja integritete** prevara poslovodstva prevara zaposlenih/tretjih oseb nezakonita dejanja nepooblaščena uporaba izguba ugleda	**Cena** - obrestne mere - valuta - kapital - blago - finančni inštrumenti **Likvidnost** - denarni tok - oportunitetni stroški - izpostavljenost **Druga stran** (poslovni partnerji) - nezmožnost izpolnitve obveznosti - izpostavljenost - poravnava - kvaliteta zavarovanja
Tveganje informacij za operativno odločanje	**Tveganje informacij za poslovno-finančno odločanje**	**Tveganje informacij za strateško odločanje**
• določanje cen • pogodbene zaveze • spoštovanje dogovorov • usklajenost	finančno načrtovanje • računovodske informacije • finančno poročanje • davki • pokojninsko zavarovanje • investicijski programi • zakonsko poročanje	poslovno okolje • poslovna strategija • portfelj proizvodov • ocenjevanje vrednosti • organizacijska struktura • merjenje izvajanja strategije • razporejanje resursov • planiranje • življenjski cikel proizvodov

Slika 22: Razvrstitev tveganj po vrstah tveganj (prirejeno po metodologiji *Universal Business Risk Model mednarodnega svetovalnega podjetja Arthur Andersen)*

Za uporabo tega modela je treba ustvariti bazo podatkov s pregledom poslovne dokumentacije in dokumentacije o obvladovanju tveganj, s pregledom načrtov zaščite, reševanja, varovanja in neprekinjenega delovanja ter z razgovori s kompetentnimi osebami.

3.3.3 Metoda MOSAR (Method Organised for a Systemic Analysis of Risk – sistemska/sistematična analiza tveganj)

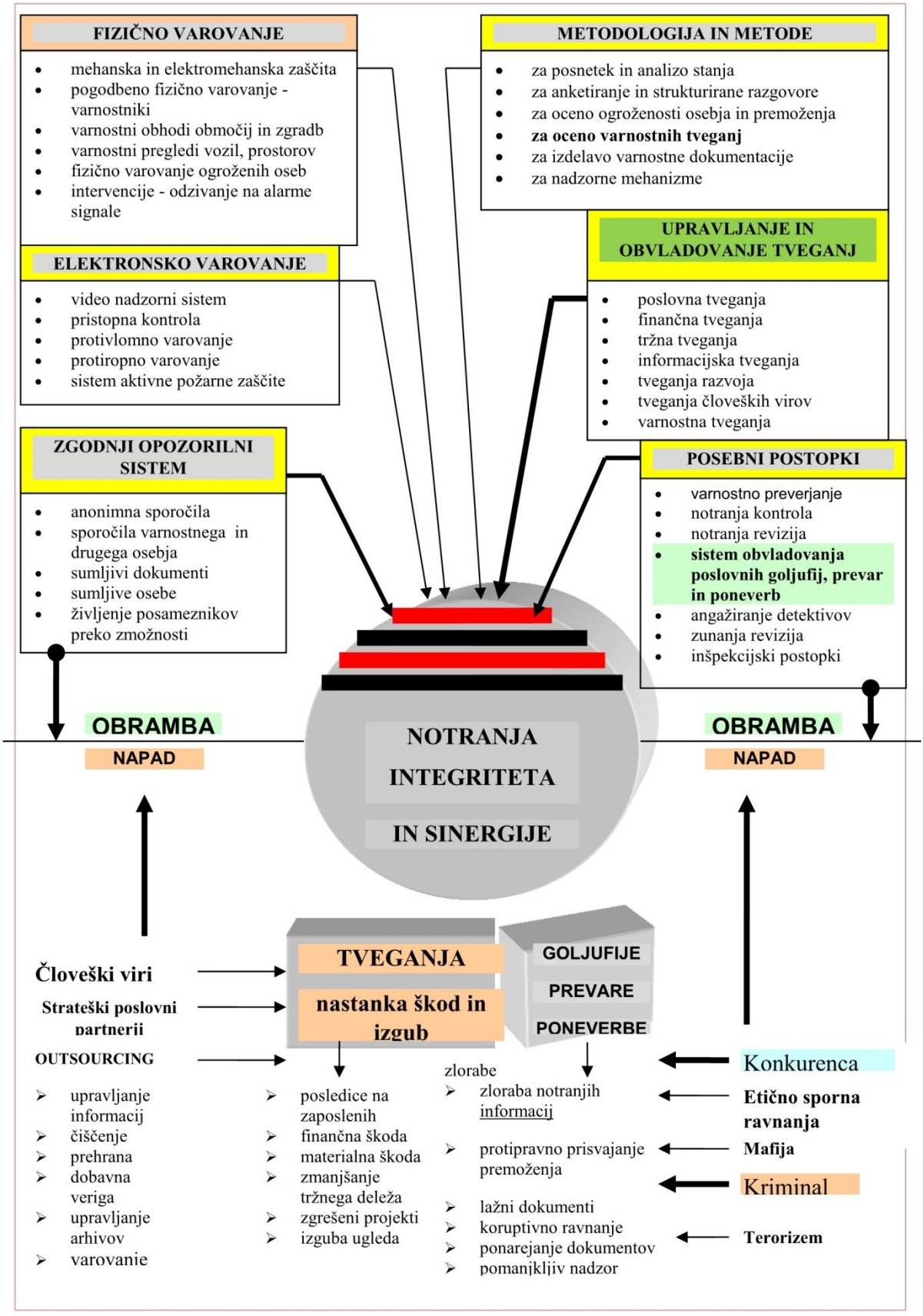
MOSAR je dokaj popularna metoda ocenjevanja oziroma obvladovanja tveganj v gospodarskih družbah, zavodih in drugih organizacijah. Omogoča celovitejši (sistemski/sistematični) pristop in je širše uporabna ob uporabi še nekaterih drugih metodologij in modelov kot npr. FMEA, HAZID, HAZOP, Kinney, PHA, FTA, COBIT, ipd.

- MOSAR lahko na kratko opišemo z nekaterimi karakterističnimi pristopi, kot so izjava iz razpoznavanja in identificiranja nevarnosti oziroma ogroženosti premoženja in človeških virov, pri čemer ni povsem jasno ali upošteva tudi ugotavljanje ranljivosti sistemov, procesov in opreme,
- ima preventivni pristop, kjer se ugotavlja ustreznost preprečevanja izrednih dogodkov in nevarnosti,
- uvaja element medsebojne odvisnosti v procesih obvladovanja tveganj,
- predstavlja pristope k študiji o varnosti in zdravju pri delu z uporabo (opis kratice) FMEA in HAZOP ter služi kot pripomoček pri izdelavi in dograjevanju Izjave o varnosti z oceno tveganj, ki jo zahteva Zakon o varnosti in zdravju pri delu,
- s pomočjo logičnih dreves razčlenjuje razne procese, procedure in postopke v iskanju možnosti napak, okvar in pomanjkljivosti,
- uvaja element resnosti in verjetnosti nastajanja izrednih dogodkov, napak, okvar in drugih škodljivosti,
- ugotavlja pogostost in stopnje resnosti posameznih vrst nevarnosti (kontrolna lista nevarnosti, varnostna analiza),
- ugotavlja tveganja za poškodbe in izgube,
- uvaja izdelavo scenarijev za verjetne izredne dogodke, ki lahko povzročijo znatno materialno, finančno, človeško in moralno škodo,
- uporablja metodo ugotavljanja napak in okvar (FMEA),
- povezuje resnost s cilji zaščitnih ukrepov pri obvladovanju tveganj,
- upošteva tehnološke ovire z vidika zastarelosti in slabega vzdrževanja procesov in opreme,
- upošteva tudi omejitve uporabe opreme, kjer imajo ključno vlogo človeški viri,
- uvaja tabele sprejemljivosti tveganj,
- uvaja določanje prioritet v obvladovanju tveganj.

To je samo nekaj elementov, na podlagi katerih vsaj v osnovi prepoznamo metodo MOSAR.

3.3.4 Model obvladovanja tveganj na bazi notranje integritete in sinergij v gospodarski družbi

Ob Andersenovem modelu je tudi ta model vsebinsko bogat za prepoznavanje skorajda vseh vrst tveganj. Najbliže mu je metoda BIA (Business Impact Analysis – analiza poslovnih vplivov), ki ji je osnova analiza poslovnih vplivov, ki se izražajo tudi z negativnimi, škodljivimi in nezaželenimi dogodki. Obvladovanje tveganj po tem modelu omogoča celovit in sistemski pristop, katerega rezultat je zdrava notranja integriteta (finančno zdravje organizacije, organizacijska in varnostna kultura, poslovna uspešnost), ob ustvarjanju sinergij med človeškimi viri in cilji organizacije.



Slika 23: Model obvladovanja tveganj na bazi notranje integritete in sinergij (Vršec, 2009)

3.3.5 Metoda BIA (Business Impact Analysis – analiza poslovnih vplivov), v povezavi s standardom ISO 22301, 22313 , 22317 in ISO/IEC 27005

V gospodarski družbi potekajo številni delovni, poslovni, informacijski, komunikacijski, varnostni, logistični, kadrovski in drugi procesi, ki ne delujejo vedno tako kot se načrtuje v strategiji ter v letnih in periodičnih planih. Prihaja torej do odmikov od načrtovanega. Tu se pa začne področje raznoterih tveganj, ki jih je treba prepoznati, oceniti in obvladati v smeri doseganja načrtovanih poslovnih in drugih ciljev. V tem kontekstu lahko ugotovimo, da veliko tveganj nastaja znotraj gospodarske družbe, kar lahko poimenujemo poslovni vplivi na nastanek tveganj. Na tej ravni tveganj pride prav metoda BIA (ang. Business Impact Analysis) – analiza poslovnih vplivov, ki omogoča vzpostavitev sistematičnega procesa ugotavljanja in presojanja predvidljivih izrednih notranjih in zunanjih izrednih dogodkov, ki ovirajo, motijo, upočasnjujejo, zavirajo ali celo prekinejo delovanje kritičnih poslovnih procesov. Možno je tudi prepoznavanje ranljivosti in ogroženosti poslovnih procesov in iz tega izvirajoča tveganja. Je tudi metoda, ki se uporablja za načrtovanje neprekinjenega delovanja in poslovanja ter kriznega vodenja, pri čemer se priporoča uporaba standarda ISO 22301 in ISO/IEC 27000. Podatke o poslovnih vplivih na tveganja lahko dobimo z razgovori in intervjuji s kompetentnimi zaposlenimi, anketami in pregledom (analizo) poslovne dokumentacije.

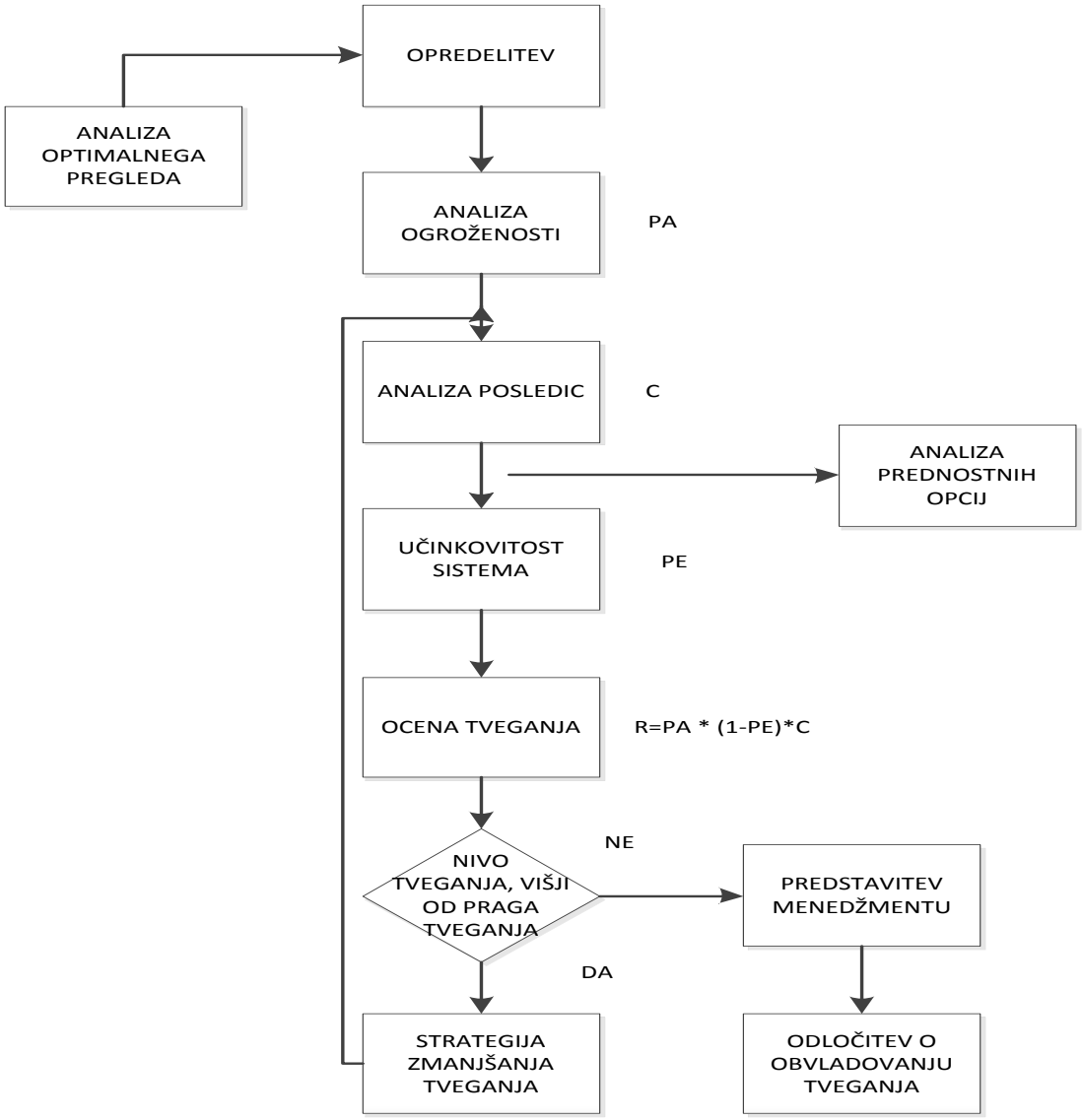
3.3.6 Model obvladovanja tveganj po enačbi $R = P_A * (1 – P_E) * C$

Predstavljamo enačbo varnostnega tveganja (Security Risk Equation), ki jo sestavljajo naslednji parametri (Biringer, B.E., Matalucci, R. V., O Connor,. S. L., 2007), ki pomenijo:

R – Risk associated with adversary attack - tveganje, ki izhaja iz notranje ter zunanje nevarnosti in ogroženosti,
PA – Likelihood of attack – verjetnost ogrožanja in konkretnega (kriminalnega, terorističnega in druge vrste) napada,
PE – Probability that the Security System is effective against the attack – verjetnost, da je varnostni sistem učinkovit proti kriminalnim, terorističnim in drugim napadom,
(1-PE) – System ineffectiveness – učinkovit sistem proti ogrožanju,
C – Consequence of the loss from the attack – posledica izgub zaradi ogrožanja.

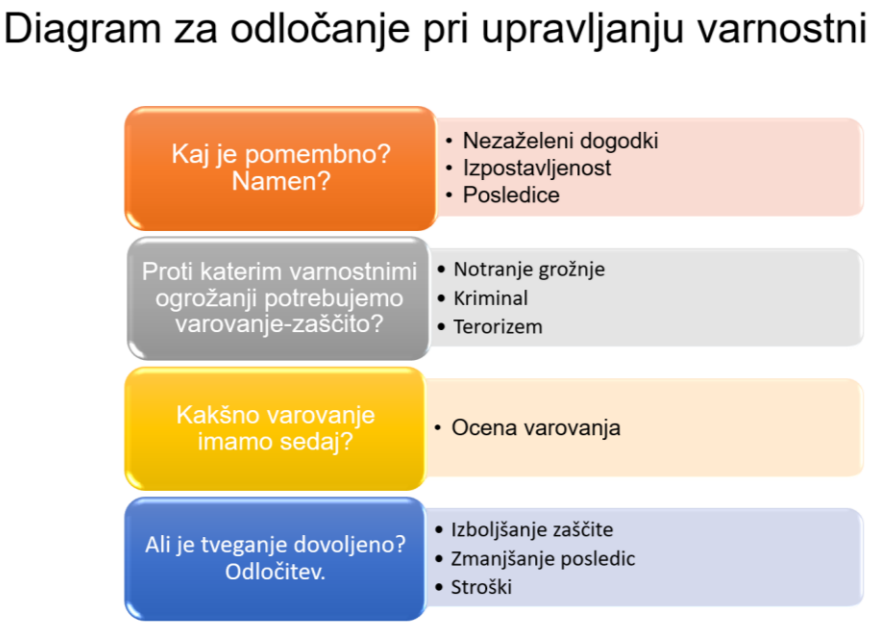
Za delovanje KI je ta model uporaben, če imamo na razpolago dovolj podatkov o ogrožanju KI in dovolj podatkov o učinkovitosti varnostnih sistemov v sektorjih KI. Gre za kompleksnejši model z enačbo tveganja, za katero je treba z raziskavo zbrati relevantne podatke in jih obdelati z multivariantnimi statističnimi metodami, kot so denimo faktorska analiza, korelacijska analiza ipd. Na naslednjih dveh slikah je prikazan proces ocenjevanja tveganj.

Prva slika (24) prikazuje postopek ocenjevanja tveganj, druga (25) pa odločitveni diagram obvladovanja varnostnih tveganj.



Slika 24: Postopek ocene tveganja po enačbi $R= P_A * (1 – P_E) * C$ (Biringer, 2007)

Iz posameznih elementov slik 24 in 25 je razvidno, da ocenjevanje tveganj izhaja iz analize optimalnega pregleda poslovnih procesov, to je pregleda poslovne dokumentacije, zbiranja informacij od kompetentnega menedžmenta, terenskega ogleda lokacije gospodarske družbe in ugotavaljanja učinkovitosti varnostnih mehanizmov. Prav tako je pomembna analiza ogroženosti in analiza posledic izrednih dogodkov ter kot sklepni del postopka oblikovanje strategije zmanjševanja tveganj.



Slika 25: Diagram za odločanje pri upravljanju varnostnih tveganj (Biringer, 2007)

3.3.7 Model obvladovanja tveganj v KI na bazi posledic izrednih dogodkov, ranljivosti in groženj R = f (C, V, T)

Po Chertoffu (2009 - Preface, 32) tveganja v 21. stoletju izhajajo iz človekovih in naravnih nevarnosti, terorističnih napadov, nesreč, naravnih katastrof in drugih izrednih dogodkov. Iz tega razvije tudi obrazec tveganja, ki se glasi:

$$R = f (C, V, T)$$

Tveganje (ang. Risk) je funkcija posledic (ang. Consequence) izrednih dogodkov, ranljivosti (ang. Vulnerability) in groženj (ang. Threat).

Lahko rečemo, da je tveganje produkt ranljivosti in ogroženosti ter posledic, kar je razvidno tudi iz nekaterih drugih metod in standardov obvladovanja tveganj. To je v tej študiji na več mestih poudarjano, saj si drugače težko zamišljamo, da bi prišli do tveganj, ki so jasna, razumljiva in primerno ovrednotena ter učinkovito obvladovana z ustreznimi ukrepi zaščite KI.

3.4 VREDNOSTNA ANALIZA MODELOV OBVLADOVANJA TVEGANJ IN OCENA PRIMERNOSTI ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Pregled metodologij za ocenjevanje tveganj za delovanje KI je bil opravljen na podlagi poglobljene analize literature. Ugotovljenih je bilo več kot tisoč ustreznih referenc, viri informacij pa so bili pomembni za prepoznavanje različnih modelov, metod in metodologij. Podrobnosti vsake metodologije vsebujejo specifične reference, ki opisujejo njen razvoj in uporabo.

Primernost metodologij smo analizirali in vrednotili na podlagi naslednjih izbranih kriterijev:

- koncept metodologije (metodologija naj določa najprimernejše načine in postopke za upravljanje in izvajanje znanstvenih raziskav, določa najboljša pravila uporabe znanstvenih orodij in opredeljuje ukrepe s pomočjo znanstvenih raziskav),
- načrtovanje (formalen pristop k načrtovanju metodologij za ocenjevanje tveganj naj bi zmanjšal število napak in težo njihovih posledic ter izpolnjevanje značilnosti kakovostnega sistema, kot so: zanesljivost, popolnost, spremenljivost, vpogledljivost in pravilna zasnova, z modularnostjo pa naj omogoča lažje obvladovanje kompleksnih primerov iz realnega sveta),
- proces (niz dejavnosti, ki z interakcijo dosežejo določen rezultat),
- postopek (temeljit opis postopka je potreben za ustrezno razumevanje metodologije in je predpogoj za vsebinske opredelitve),
- delovanje in upravljanje sprememb (zaradi hitrosti nastajanja sprememb postaja prihodnost vse bolj nepredvidljiva, obstajajo učinkoviti pristopi k upravljanju sprememb).

Izbrali smo 27 metodologij, ki so prikazane v Tabeli 1, skupaj s splošno uporabljanimi izrazi / kraticami.

Možna je smiselna uporaba naslednjih metod:

- **metoda vrednotenja COSO** (Commitee of Sponsoring Organisation), ki zagotavlja, da bodo vsa identificirana tveganja tudi primerno upravljana in da bodo vzpostavljene ustrezne obrambe pred možnimi tveganji. Ta metodologija se pretežno uporablja kot osnova za vse ostale metodologije,
- **metoda RFRM** (Risk Filtering and Ranking Method, Haimes, Kaplan, Lambert, 2002), po kateri izdelamo izbor scenarijev možnih nenormalnih situacij in s standardiziranim pristopom stopenjsko izvajamo selekcijo scenarijev, ki lahko povzročijo najvišje stopnje tveganja (najslabši možni scenarij). Zanje določimo ustrezne funkcionalne in finančne ukrepe,

- **metoda HHM** (Hierarchical Holograpfic Model, Haimes, Lambert, Li, Schooff, Tulsiani, 1995), s katero pripravimo celovit nabor vseh znanih scenarijev, ki povzročajo tveganje. Sinteza vseh ugotovljenih tveganj iz različnih zornih kotov omogoča celovit pregled sistemskih tveganj,
- **metoda** IIOM (Inoperability Input-Output Model, Santos, 2005) omogoča analizo vplivov nenormalnih situacij v medsebojno odvisnih sistemskih sektorjev. Poudarek je na prepoznavanju odvisnosti možnih nenormalnih situacij v sektorju na drugi sektor (v kolikšni meri nenormalna situacija v posameznem podsistemu vpliva na delovanje celotnega sistema in kolikšne so škodne posledice),
- **metoda FDICIA** (Federal Deposit Insurance Incorporation Improvement Act) za obvladovanje tveganj v finančnih organizacijah,
- **metoda COBIT** (Control Objectives for Information and related Technology) je zelo uporabna za poslovna okolja, ki uporabljajo visoko zahtevno informacijsko tehnologijo, dodatno se uporablja še orodje za analizo procesov PST (Process Survey Tool) in obrazec za oceno tveganja RAF (Risk Assessment Form),
- **metoda PHA** (Preliminary Hazard Analysis) – predhodna analiza tveganj se uporablja na področju varnosti in zdravja pri delu. Lahko se uporablja tudi v sklopu standardov OHSAS 18001,
- **metoda MOSAR** (Method Organised for a Systematic Analysis of Risks) sistemska analiza tveganj in kot najbolj poznana »Analiza drevesa napak«, pa tudi diagram vzrokov in posledic (Ishikawa diagram) oz. diagram »ribje kosti«. Metoda sistematično analizira tveganja v okolju in predstavlja sistematičen pristop k ocenjevanju ter vrednotenju tveganja, določevanju prioritet, obravnavanju tveganj in upravljanju z njimi. Razvita je bila na osnovi metode MADS (Method of Disfunctional Systems), ki vsebuje splošni model za popis nevarnosti in pomeni sistematični pristop k razgrnitvi kompleksnih sistemov in vrednotenju potencialne škode na izpostavljenih subjektih/objektih, omogoča modeliranje mehanizma delovanja (tok nevarnosti) med virom nevarnosti in tarčo (izpostavljenim subjektom/objektom),
- na področju varstva okolja se pogosto uporablja verjetnostna analiza tveganja **PRA** (Probalistic Risk Analysis), kjer je izračun tveganja formaliziran in sicer kot produkt verjetnosti za nastop dogodka in njegovih posledic,
- **metoda »Kaj če?«** je strukturirana metoda z uporabo „možganske nevihte“, za ugotavljanje „kaj gre lahko narobe“ in presojo verjetnosti in škodljivosti takih pojavov. Presoja se sprejemljivost tveganj in določa priporočila za nesprejemljiva tveganja. Za efektivno ocenjevanje je potrebna izkušena skupina presojevalcev,
- analiza drevesa napak **FTA** (Fault Tree Analysis),
- analiza napak in posledic **FMEA** (Failure Mode an Effect Analysis),

- splošno uporabna metoda upravljanja s tveganji je **Universal Business Risk Model** mednarodnega svetovalnega podjetja Arthur Andersen,
- **metoda po Basel II**: dogovor obvladovanja operativnih, informacijskih in drugih bančnih tveganj,
- **metoda KINNEY** je bila prvič predstavljena v Tehničnem dokumentu vojašnice Naval Weapons Center v Kaliforniji. Prvotno je bila namenjena preventivi pred tveganjem eksplozij v vojni industriji, zelo hitro pa je bila sprejeta v Evropi, kot metoda za oceno tveganja pri delu, sedaj je vodilna metoda za oceno tveganja pri delu v več evropskih državah, uporablja se univerzalno, pri večjih in manjših podjetjih,
- **metoda NIST** (The National Institute of Standards and Technology, ZDA) kvantitetno vrednoti materialne dobrine. Z njo se oceni pogostost uresničitve posameznih oblik in izračuna pričakovane letne škode zaradi uresničitve ogrožanj (letna škoda je škodni učinek in pogostost škodnega dogodka),
- **metoda Roland in Moriarty** temelji na matematičnem pristopu in se nanaša na opredelitev sistema, identifikacijo ogrožanj, ocenitev ogrožanj, razrešitev ogrožanj in na nadzor uspešnosti aktivnosti,
- **metoda VECTOR ocenjuje** ranljivost, enostavnost storitve, posledice, grožnje, operativna pomembnost in elastičnost. Pripravljeni so kriteriji za oceno tveganja posameznih poslovnih procesov,
- **metoda scenarijev:** napredni pristopi, ki temeljijo na scenarijih, so vrsta internih modelov za merjenje tveganja. Njihova bistvena značilnost je vnaprejšnje ocenjevanje tveganj organizacije. Tveganje je opredeljeno kot kombinacija med resnostjo in frekvenco potencialne izgube v določenem časovnem obdobju.

Tabela 1: Primernost metod za ocenjevanje tveganj za delovanje kritične infrastrukture (interni vir ICS)

Metoda	Koncept	Načrtovanje	Proces	Postopek	Delovanje	Spremembe
HAZOP	x	x	√	√	√	√
Kaj če?	o	o	√	√	√	√
CHA	√	√	o	x	x	x
CSR	√	o	x	x	x	x
PHA	√	√	o	x	x	x
FTA	o	o	√	√	√	√
CCA	o	o	o	√	√	√
Pre-HAZOP	√	√	o	x	x	x
FIHI	x	o	√	√	√	√
CEX	x	x	√	√	√	√
MOSAR	o	o	√	√	√	√
GOFA	x	x	o	√	√	√
Inherent	o	√	√	o	o	o
FMEA	x	x	√	√	√	√
FMECA	x	x	√	√	√	√
MOp	x	x	√	√	√	√
Block diagram	x	x	√	o	o	o
Structural	x	x	√	o	o	o
Vulnerability	x	x	√	o	o	o
CHAZOP	x	x	√	√	√	√
SADT	x	√	o	x	x	x
State transition	x	√	o	x	x	x
GRAFCET	x	√	x	x	x	x
HTA	x	x	√	√	√	√
AEA	x	x	√	√	√	√
Human reliability	x	x	√	√	√	√
Pattern search	x	x	√	√	√	√

Legenda oznak:

√: zelo primerno; o: primerno; x: neprimerno.

Legenda kratic:

- HAZOP: Hazard and operability study, študija nevarnosti in operativnosti,
- CHA: Concept hazard analysis, analiza nevarnosti koncepta,
- CSR: Concept safety review, varnostni pregled koncepta,
- PHA: Preliminary hazard analysis, predhodna analiza nevarnosti,
- FTA: Fault tree analysis, analiza drevesnih napak,
- CCA: Cause-consequence analysis, analiza vzročnih posledic,
- Pre-HAZOP: Pre-hazard and operability study, študija nevarnosti in operativnosti,
- FIHI: Functional integrated hazard identification, funkcionalna integrirana identifikacija nevarnosti,
- CEX: Critical examination of safety systems, kritični pregled varnostnih sistemov,
- MOSAR: Method organised systematic analysis of risk, metoda za sistematično analizo tveganja,
  GOFA: Goal oriented failure analysis, ciljno usmerjena analiza napak,
- Inherent: Inherent hazard analysis, analiza inherentnih tveganj,
- FMEA: Failure mode and effect analysis, analiza načina in učinka okvar,
- FMECA: Failure modes, effects, and criticality analysis, analiza učinkov in kritičnosti,
- MOp: Maintenance and operability study, študija vzdrževanja in operativnosti,
- Block diagram: Reliability block diagram, blokovni diagram zanesljivosti,
- Structural: Structural reliability analysis, analiza strukturne zanesljivosti,
- Vulnerability: Vulnerability assessment, ocena ranljivosti,
- CHAZOP: Computer hazard and operability study, študija računalniške nevarnosti in operativnosti,
- SADT: Structured analysis and design techniques, strukturirane analize in tehnike oblikovanja,
- State transition: State-transition diagrams, diagrami prehodov,
- GRAFCET: Graphe de commande etat-transition, diagrami prehodov,
- HTA: Hierarchical task analysis, hierarhična analiza nalog,
- AEA: Action error analysis, analiza napak v delovanju,
- Human rel.: Human reliability analysis, analiza zanesljivosti človeka,
- Pattern search: Pattern search method, način iskanja po vzorcu,
- PHEA: Predictive human error analysis, analiza predvidevanja človeške napake.

Čeprav je na voljo veliko informacij o uporabi metodologij za ocenjevanje tveganja, obstaja le malo navodil, kako jih operativno uporabiti. Ugotovili smo, da ni nobenega primera, ki bi poskušal enotno razvrstiti to »družinsko drevo« metodologij. Najtežji vidik tega pregleda je bil določiti količino podrobnosti, ki jo je treba vključiti v vsako metodologijo. Subjektivna ocena prednosti in slabosti metodologij je vprašanje identifikacije nevarnosti, ki lahko ogrožajo neprekinjeno delovanje KI.

Na podlagi izbranih kriterijev za ocenjevanje metodologij smo izbrali kombinacijo metodologije MOSAR (Method organised systematic analysis of risk, metoda za sistematično analizo tveganja) in metodologije FMEA (Failure mode and effect analysis, analiza načina in učinka okvar) kot najprimernejši za ocenjevanje tveganj za delovanje KI v Republiki Sloveniji.

Metoda FMEA se uporablja že več desetletij in ima dolgo zgodovino kot metoda za podporo proizvodnih procesov, storitev in vzdrževanja. Je učinkovita, preventivna, timsko orientirana in sistematična analiza napak sistema. Obsega interdisciplinarne postopke, sistematično in funkcijsko obravnavanje, preprečevanje napak, kreativno razmišljanje in kritično ocenjevanje. FMEA je pogosto prvi korak sistema v študiji njegove zanesljivosti. To vključuje pregled komponent, sklopov in podsistemov, kjer se lahko pojavijo okvare in analiza njihovih vzrokov ter učinkov. Za vsako komponento, okvaro in posledično učinke na preostali del sistema, je potrebno beleženje v poseben delovni list FMEA. Obstajajo njene številne različice.

Ne glede na smiselno uporabo raznih matematičnih algoritmov in drugih raziskovalnih pripomočkov ter metodologij za ocenjevanje tveganj je bistveno, da se k obvladovanju tveganj pristopa sistemsko načrtno, organizirano, medsektorsko usklajeno z drugimi upravljavci KI in predvsem z vidika proaktivnosti, s pogledom v bližnjo in daljno prihodnost.

Načrtno ocenjevanje in upravljanje tveganj izhaja iz znanja, sposobnosti in ravnanja upravljavcev KI, da z določenimi metodami in tehnikami dosežejo najugodnejše razmerje med ravnijo prevzetega tveganja in doseganjem zastavljenega cilja poslovanja. Drugače povedano to pomeni, da mora upravljavec KI prevzeti in nadzirati ustrezno raven tveganja, ki mu bo zagotavljala doseganje strateških ciljev poslovanja, ne da bi s tveganjem ogrozili tekoče poslovanje.

Predvidevamo, da so cilji, ki jih želi upravljavec KI z ocenjevanjem tveganja doseči naslednji:

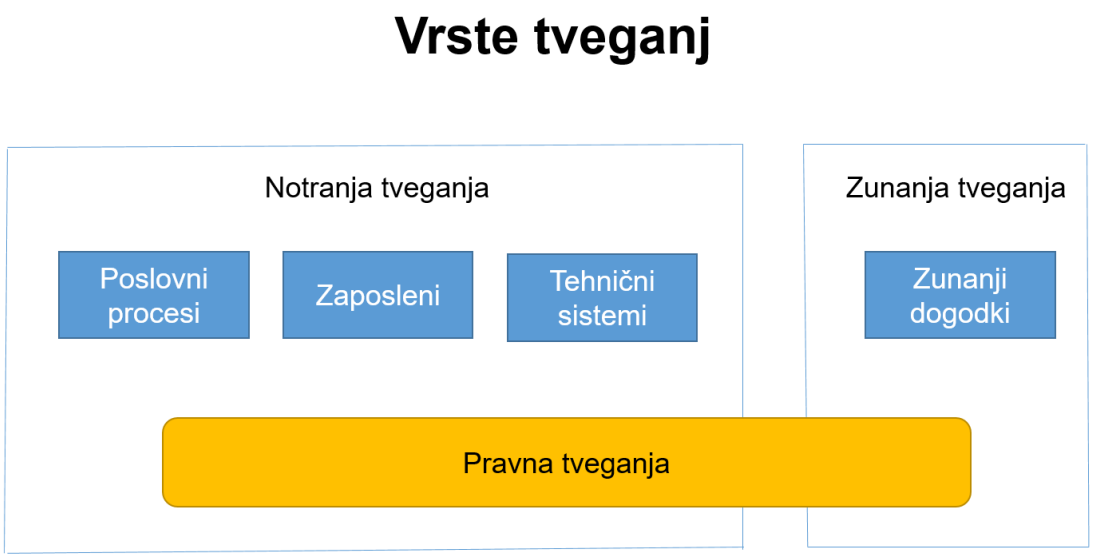
- zanesljivo in neprekinjeno poslovanje: preprečiti, da bi v organizaciji prišlo do prekinitve poslovanja oziroma zmanjšati posledice zunanjega ali notranjega škodnega oz. izrednega dogodka tako, da bi ta čim manj motil normalno poslovanje,
- preživetje organizacije po težkem škodnem oz. izrednem dogodku,
- stabilnost prihodkov in rast organizacije,
- socialna odgovornost: odgovornost za preprečitev tveganj, ki so jim izpostavljeni zaposleni,
- občutek gospodarske varnosti: v primeru slabega upravljanja s tveganji lahko trpi socialna varnost zaposlenih,
- minimiziranje stroškov tveganj: zniževanje stroškov upravljanja tveganj na najnižjo možno raven.

3.5 OPREDELITEV VRSTE TVEGANJ IN NJIHOVO OCENJEVANJE

Da lahko ustrezno razumemo kompleksnost poslovnega in varnostnega okolja je potrebno razumeti vrste tveganj, katerim so izpostavljene organizacije, ki upravljajo KI. V ospredju so naslednja tveganja:

- **poslovnih procesov in postopkov dela** (tveganje navodil, napak v poslovnem procesu – procesiranje storitev in proizvodov, tveganje strategije, organizacije in vodenja, skladnosti z zakonodajo, pravno tveganje, varnostno tveganje, tveganje ogroženosti iz okolja, tveganje izvajanja notranjih kontrol, prikrivanje dejanskega stanja, ponarejanje poročil in dokumentov, tveganje izgube zaupanja javnosti in dobrega imena ipd.),
- **informacijskega premoženja** (tveganje neprekinjenosti in razpoložljivosti delovanja informacijske tehnologije, izgube podatkov in informacij, neučinkovitosti podpor poslovanja, razkritja poslovnih skrivnosti, tveganje razvoja ipd.),
- **človeških virov** (tveganje izgube ključnih sodelavcev, tveganje zanesljivosti in usposobljenosti zaposlenih, motivacije zaposlenih, tveganje spoštovanja načel lojalnosti in poštenosti ipd.),
- **materialnega premoženja** (tveganje izgube materialnega premoženja upravljavca KI, infrastrukture, delovne opreme in strojev, poslovnih prostorov ipd.).

Operativna tveganja so shematsko prikazana na sliki 27. Operativna tveganja so izbor iz kataloga vseh tveganj.



Slika 26: Vrste operativnih tveganj (prirejeno po Basel II, 2006)

3.5.1 Sistemski pristop ocenjevanja tveganj

Pristop k ocenjevanju tveganj mora biti metodično zasnovan na principih sistemskega inženiringa, vsebinsko na preprečevanju možnih škod in izgub, operativno pa na celovitih ter sodobnih rešitvah upravljanja tveganj.

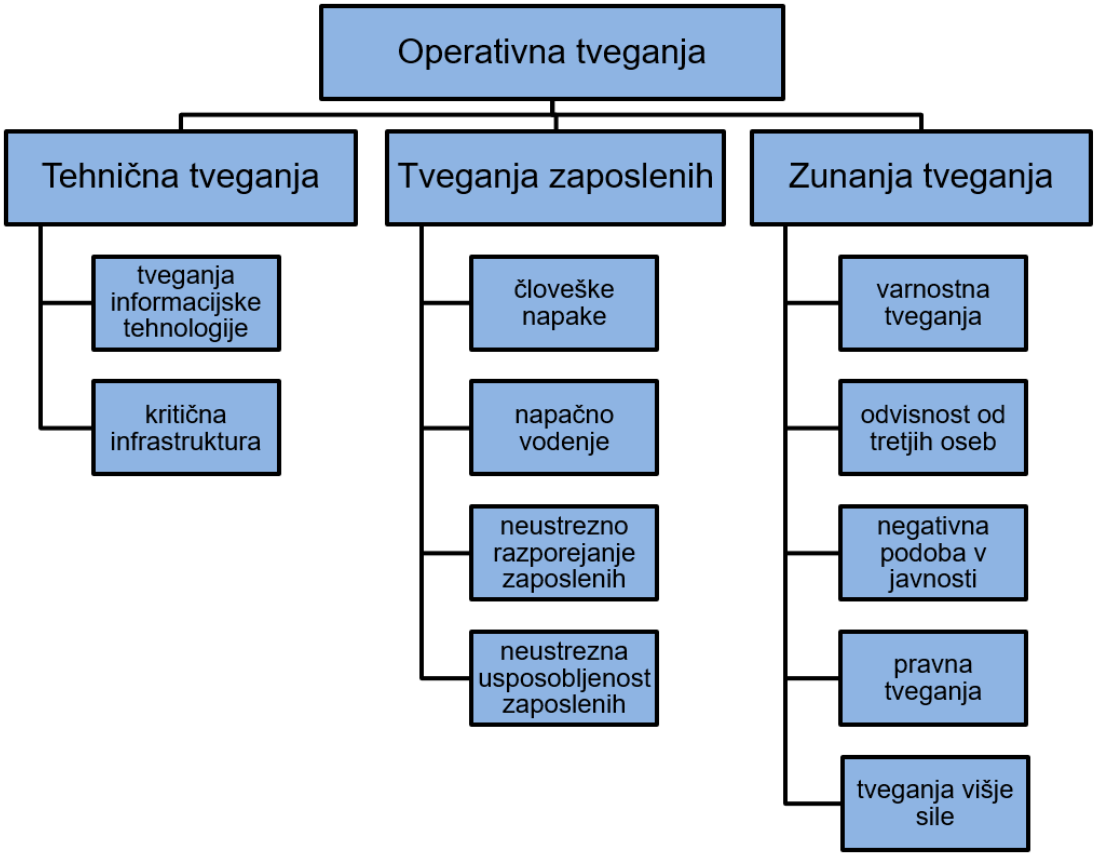
Sistemski pristop k ocenjevanju tveganj vsebuje zlasti naslednje aktivnosti:

- identifikacijo in ovrednotenje ogrožanj (verjetnost, teža posledic),
- ocenjevanje tveganj: upoštevane morajo biti vse vrste tveganja (redek dogodek s težkimi posledicami, pogost dogodek z manjšimi posledicami),
- razviti je potrebno ustrezne protiukrepe, ki so lahko različnih vrst, vendar pa noben protiukrep ne more reducirati tveganja na nič, temveč lahko le do določene sprejemljive mere omeji in nadzira tveganje,
- potrebno je zagotoviti ustrezna finančna sredstva; če ni ustreznih sredstev za zagotovitev zmanjšanja tveganja, potem je to ocenjevanje zgolj opozarjanje na probleme; če predlagani ukrepi zahtevajo več sredstev, kakor jih je na razpolago, je potrebno poiskati ali razviti nove cenejše protiukrepe,
- del tveganja se lahko prenese na zavarovalnico, ob optimalnem upoštevanju zavarovalnih pogojev in stroškov zavarovanja,
- ostanek tveganja je potrebno sprejeti in ob njegovem upoštevanju poslovati.

Upravljavec KI z notranjimi postopki in enotno metodologijo določi spremljanje ocenjevanja in upravljanja tveganj (npr. kot »Politika upravljanja tveganj« - ta dokument določa ukrepe, postopke, aktivnosti in pravila za vzpostavitev in delovanje celovitega sistema ocenjevanja in upravljanja tveganj, ki temelji na opredelitvi ustreznega organizacijskega ustroja in metodološkega okvirja). Pri tem gre za medsebojno sodelovanje strokovnih služb upravljavca KI (lahko tudi s pomočjo zunanjega strokovnjaka), zlasti na poslovnem, upravljavskem, pravnem in varnostnem področju.

Kazalci uspešnosti ocenjevanja in upravljanja tveganj so uspešno poslovanje upravljavca KI (možna ogrožanja so pod nadzorom in obvladljiva), tekoče preverjanje primernosti strategije in njeno prilagajanje nastalim razmeram.

Za celovito identifikacijo tveganj je priporočljivo uporabiti celoten nabor možnih izrednih dogodkov, ki se lahko zgodijo upravljavcu KI. Na sliki 27 so prikazana glavna področja tveganj, ki se nanašajo na tehnična tveganja, tveganja zaposlenih in zunanja tveganja.



Slika 27: Vrste operativnih tveganj (interni vir ICS)

Operativna tveganja so sestavni del kataloga vseh tveganj KI.

Za operativno uporabo smo razširili osnovni nabor tveganj in identificirali 12 skupin tveganj (primer dobre prakse prevzema evra v Republiki Sloveniji 2007) (skupno najmanj 114 področij tveganj), in sicer:

1. tveganje strategije, organizacije in vodenja organizacije (7 področij),
2. tveganje skladnosti z zakonodajo in internimi akti organizacije (6 področij),
3. pravno tveganje (6 področij),
4. finančno tveganje (3 področja),
5. tveganje informacijskega premoženja (9 področij),
6. tveganja opravljanja poslovnih procesov organizacije (20 področij),
7. tveganja človeških virov (22 področij),
8. tehnična tveganja (7 področij),
9. tveganja kaznivih dejanj (14 področij),
10. tveganja okolja (6 področij),
11. tveganja notranjih kontrol (10 področij),
12. tveganje izgube dobrega imena (4 področja).

Identifikacija tveganj je izdelana na podlagi izkušenj, in sicer:

1. Tveganje strategije, organizacije in vodenja

Tveganje strategije pomeni nevarnost sprejemanja napačnih strateških odločitev (usmeritev) upravljavca KI, ki lahko ogrozijo stabilnost realizacije njenih ciljev in aktivnosti poslovanja ter lahko povzročijo nezaupanje uporabnikov njihovih storitev ali izdelkov in posledično izgubo dobrega imena (zmanjšanje ugleda).

Tveganje organizacije je tesno povezano s tveganjem človeških virov, vključuje pa tudi:

- tveganje neustrezne vizije in strategije,
- tveganje nefunkcionalne organizacije,
- tveganje nekoordinacije aktivnosti med strokovnimi službami,
- tveganje neučinkovite izrabe virov poslovanja strokovnih služb,
- tveganje konfliktov interesov zaradi neustrezne razdelitve nalog, pooblastil in odgovornosti,
- tveganje neustrezne vgradnje notranjih kontrol (kontroling in poročanje),
- tveganje vodenja je tveganje premajhne odgovornosti vodij organizacijskih enot in sposobnosti njenega vodstva, za izvajanje strategije in doseganje ciljev poslovanja.

2. Tveganje skladnosti z zunanjo zakonodajo in internimi akti

Tveganje skladnosti z zunanjo in notranjo zakonodajo vključuje:

- skladnost poslovanja s pozitivno zakonodajo in z internimi akti,
- skladnost poslovanja z zahtevami državnih organov,
- kooperativni odnosi z zakonodajnimi institucijami, zunanjimi revizorji in poslovnimi združenji, vključno z objektivnim informiranjem in poročanjem,
- skladnost z zahtevami veljavnih standardov in kodeksov profesionalnega ravnanja (dobra poslovna praksa),
- obstoj in celovitost notranjih politik, aktov, standardov in navodil za poslovne procese,
- ravnanje z zaupnimi podatki in informacijami.

3. Pravno tveganje

Pravno tveganje se odraža v nevarnosti, da bo upravljavec KI utrpel finančno izgubo in zmanjšanje zaupanja ter ugleda zaradi slabo urejenih pogodbenih in drugih pravnih odnosov s tretjimi osebami, ki sodelujejo pri realizaciji poslovnih procesov. Pravno tveganje je

posredno povezano tudi s splošno urejenostjo, delovanjem in učinkovitostjo pravnega sistema v državi in v širšem mednarodnem okolju.

4. Finančno tveganje

Finančno tveganje se nanaša zlasti na naslednje dejavnike:

- tveganje škodnih dogodkov (zaradi zunanjih in notranjih dejavnikov), s posledično finančno izgubo (npr. prva stopnja tveganosti: potencialna finančna izguba je pod 100.000 €, druga stopnja tveganosti: potencialna finančna izguba je med 100.000 in 1.000.000 €, tretja stopnja pa je finančna izguba nad 1.000.000 mio €),
- tveganje nedoseganja tržnih ciljev poslovanja (so kompleksni),
- tveganje finančnega izkaza uspeha poslovanja,
- tveganje notranjih prevar in korupcije.

5. Tveganje informacijske tehnologije

Tveganje informacijske tehnologije se nanaša na pomanjkljivosti in napake pri delovanju informacijskega sistema (in njihov vpliv na realizacijo ciljev poslovanja), zlasti napake pri vhodu ali izhodu informacij in podatkov.

Tveganje informacijske tehnologije je čedalje bolj kompleksno, vključuje pa:

- neučinkovitost podpore poslovanja za doseganje poslovnih ciljev,
- neustrezno odzivanje na potrebne spremembe poslovanja in spremembe tehnologije,
- slabo razpoložljivost informacijskega sistema (daljši izpad električne energije, napake v delovanju telekomunikacij ipd.),
- nesposobnost zagotavljanja neprekinjenega poslovanja,
- tveganje izgube integritete podatkov ali izgube podatkov (s pomočjo goljufije, tatvine, raznih prevar in manipulacij, prestrezanja pretoka podatkov, eksplozije, sabotaže, vandalizma, terorizma ipd.),
- tveganje razkritja zaupnosti podatkov,
- tveganje ogroženosti iz okolja (vdori v informacijski sistem, virusi, spletni napadi, socialni inženiring, delovanje škodljivih računalniških programov ipd.),
- tveganje neustreznega razvoja informacijske tehnologije.

6. Tveganje opravljanja poslovnih procesov in postopkov dela

Tveganje opravljanja poslovnih procesov in postopkov dela se nanašajo zlasti na naslednje napake in pomanjkljivosti:

- neustrezna organizacija in vodenje poslovanja,

- premajhna usposobljenost izvajalcev,
- premajhne izkušnje izvajalcev za doseganje ciljev poslovanja,
- neupoštevanje navodil za delo,
- napake in pomanjkljivosti pri delu,
- prekoračenje pooblastil,
- nepokritost delovnih postopkov z navodili,
- neustrezno procesiranje poslovanja,
- netočnost in nepravočasnost pretoka informacij,
- preveliko naraščanje obsega dela,
- neobvladovanje konic poslovanja, ko organizacijske in kadrovske zmogljivosti presegajo zmožnosti,
- opravljanje nezdružljivih funkcij,
- prikrivanje dejanskega stanja,
- ponarejanje poročil in dokumentov,
- neusklajene evidence poslovnih procesov,
- neusklajenost knjigovodskih poročil,
- neskladnost z zakonodajo in internimi akti,
- neustrezne spremembe tehnologije dela,
- neustrezno izvajanje vodstvenega nadzora in notranjih kontrol,
- neupoštevanje revizijskih ugotovitev in izvajanja priporočil.

7. Tveganje človeških virov

Tveganje človeških virov se nanaša na podmeno, da izvajalci poslovnih aktivnosti dosledno ne upoštevajo internih aktov, moralnih in etičnih načel poslovanja ter drugih zakonskih določil in tako lahko povzročijo možne škodne oz. izredne dogodke (zlasti finančno izgubo in izgubo zaupanja uporabnikov). Tveganje človeških virov lahko povzročijo posamezniki, ki so zaposleni v organizaciji in drugi pogodbeno povezani izvajalci. Vključuje tveganje raznih oblik in vrst nepoštenosti ter kaznivih dejanj (vključno s kršitvijo deontolškega kodeksa vedenja zaposlenih), tveganje sposobnosti vodstva, da tekoče sprejema ustrezne odločitve in tudi tveganje neustrezne motivacije zaposlenih.

Tveganje človeških virov je povezano predvsem z:

- neustreznim organiziranjem in vodenjem dela,
- izgubo ključnih sodelavcev in izgubo njihovega znanja ter sposobnosti,
- nezagotavljanjem razdelitve funkcij, dolžnosti in pooblastil ter nenadomeščanja izvajalcev z ustrezno usposobljenimi zaposlenimi,
- neustreznim obvladovanjem konic poslovanja, ko organizacijske in kadrovske zmogljivosti presegajo zmožnosti,

- neustreznim nagrajevanjem, produktivnostjo, motivacijo in samostojnostjo zaposlenih,
- neustrezno delovno razporeditvijo zaposlenih glede na njihovo strokovno znanje, usposobljenost in delovne izkušnje,
- neustreznim usposabljanjem,
- prekoračitvijo omejitev in pooblastil,
- napakami in kršitvami navodil za delo,
- malomarnostjo zaposlenih,
- nezadovoljstvom zaposlenih,
- nepoštenostjo zaposlenih,
- neupoštevanjem ugotovitev vodstvenega nadzora,
- neupoštevanjem ugotovitev notranje revizije,
- neizvajanjem priporočil eksternih presoj,
- nizko stopnjo pokritosti delovnih postopkov z navodili,
- neustreznimi spremembami internih aktov,
- izdajo poslovnih skrivnosti,
- neustreznim fizičnim varovanjem,
- stavko zaposlenih,
- javnimi nemiri in protesti ter
- pomanjkljivim načrtovanjem poslovanja ob izrednih dogodkih.

8. Tehnična tveganja

Tehnična tveganja se nanašajo na možni izpad električne energije, transportni izpad, izpad strojne, programske in telekomunikacijske računalniške opreme, neučinkovitost tehničnih podpor poslovanja, neustrezno tehnično varovanje ipd.

9. Tveganja zaradi kaznivih dejanj

Tveganja zaradi kaznivih dejanj se nanašajo na širok spekter kriminalnih dejavnosti, kot so goljufija, izdaja poslovne skrivnosti, prestrezanje pretoka podatkov, izsiljevanje, vandalizem, sabotaža, tatvina, eksplozija, razne prevare in manipulacije, vlom, rop in roparska tatvina, terorizem ipd.

10. Tveganje okolja

Tveganje okolja se nanaša na široko vrsto tveganj v okolju, s katerimi se upravljavec KI sooča pri svoji poslovni dejavnosti. Zakonodajno tveganje predstavlja spreminjanje zakonov, ki lahko bistveno vplivajo na pogoje realizacije strategije in ciljev poslovanja. Ekonomsko tveganje se nanaša na spreminjanje meddržavnih ekonomskih dejavnikov, ki ima lahko

pomemben vpliv na uspešnost poslovanja. Vedno so prisotna tudi tveganja naravnih katastrof in višje sile.

Nekatera tveganja okolja so lahko tako interna kot eksterna. Identificirana so naslednja tveganja okolja:

- tveganje sprememb zakonodaje,
- tveganje ekonomskih sprememb,
- tveganje naravnih nesreč (potres, poplava, zemeljski plaz, snežni plaz, visok sneg, močan veter, toča, žled, pozeba, suša, požar v naravnem okolju, množični pojav nalezljive človeške, živalske ali rastlinske bolezni in druge nesreče, ki jih povzročijo naravne sile. Za naravno nesrečo se štejejo tudi neugodne vremenske razmere po predpisih o kmetijstvu in odpravi posledic naravnih nesreč, ki jih povzročijo žled, pozeba, suša, neurje, toča ali živalske in rastlinske bolezni ter rastlinski škodljivci) (povzeto po ZVNDN),
- tveganja industrijskih nesreč (nesreče v cestnem, železniškem in zračnem prometu, požar, rudniška nesreča, porušitev jezu, nesreče, ki jih povzročijo aktivnosti na morju, jedrska nesreča in druge ekološke ter industrijske nesreče, ki jih povzroči človek s svojo dejavnostjo in ravnanjem, pa tudi vojna, izredno stanje, uporaba orožij ali sredstev za množično uničevanje ter teroristični napadi s klasičnimi sredstvi in druge oblike množičnega nasilja) (povzeto po ZVNDN),
- množične in dolgotrajne stavke,
- uporaba orožij ali sredstev za množično uničevanje,
- teroristični napadi,
- izbruh epidemije nalezljivih bolezni,
- porušitev poslovne stavbe organizacije,
- krizna stanja v gospodarstvu,
- kompleksna kriza na državni ravni,
- razglasitev izrednih razmer
- vojna.

11. Tveganje neustreznega izvajanja notranjih kontrol

Omenjeno tveganje se uresniči, če:

- ni vzpostavljena ustrezna organizacija,
- človeški viri, glede na vodenje, število zaposlenih in znanje, niso ustrezni za izvajanje poslovnih aktivnosti,
- poslovni postopki ne podpirajo celovitosti poslovnih aktivnosti,
- ni ustrezna uporaba virov s primerno / zadostno razmejitvijo nezdružljivih funkcij in rotacijo funkcij,

- niso ustrezno določeni standardi notranjega kontroliranja,
- obstaja pomanjkanje kontrolne zavesti pri izvajalcih,
- ni rednega načrtnega izvajanja notranjih kontrol in vodstvenega nadzora,
- so funkcije kontrole in izvajanja združene v eni osebi,
- je od zadnje revizije za posamezna poslovna področja preteklo že daljše časovno obdobje (npr. 3 leta),
- so v razdobju od zadnje revizije poročali o pomanjkljivostih/napakah/ incidentih.

12. Tveganje nezaupanja uporabnikov

Navedeno tveganje je v tesni korelaciji z vsemi drugimi naštetimi tveganji, še zlasti s strateškim in operativnim tveganjem. Deluje na dolgi rok in se v najtežji obliki realizira s finančnimi izgubami (kot posledice izgube zaupanja uporabnikov storitev ali blaga) in izgubo ugleda organizacije v javnosti. Izguba zaupanja uporabnikov se lahko zgodi, če:

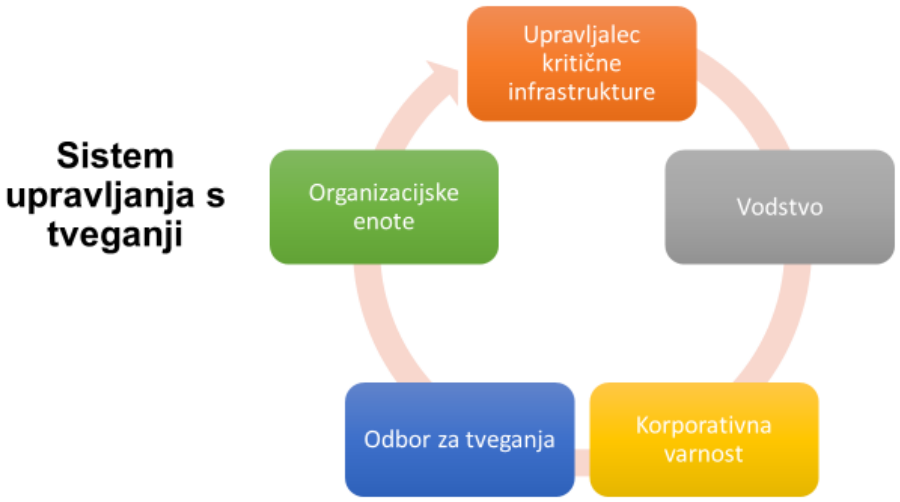
- izredni dogodek na področju KI, prekinitev njihovega delovanja ali njihovo uničenje bi pomembno vplivalo in imelo resne posledice na ključne družbene funkcije, nacionalno varnost, gospodarstvo ter na zdravje, varnost, zaščito in blaginjo ljudi,
- izredni dogodek / pomanjkljivost / napaka / kraja / poneverba pri realizaciji poslovne storitve ali blagu škoduje dobremu imenu upravljavca KI,
- izredni dogodek vodi upravljavca KI v kršenje zakonskih določil in poslovnega deontološkega kodeksa,
- izredni dogodek, pomanjkljivost ali napaka pri poslovnih procesih je osnovna naloga upravljavca KI ali pa je z njo tesno povezana,
- finančna škoda pomembno vpliva na izkaz uspeha.

Pomembno je zavedanje, da je vpliv človeškega dejavnika na ocenjevanje tveganj eden najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni stalno nevarnost na področju upravljanja tveganj in ga ne smemo podcenjevati. Človeški dejavnik (zlasti zaposleni, stranke, možni storilci kaznivih dejanj) z vsemi svojimi potrebami, motivi, stališči in notranjimi osebnostnimi faktorji, predstavlja ključen člen v identifikaciji tveganj, ker zaposleni neposredno vstopa v interakcije s poslovnimi procesi. Pri tem ti ob tekočem delu zaznavajo in nadzirajo možno ogrožanje premoženja organizacije, delajo napake in tudi popravljajo napake. Zlonamerna napaka je vnos v posameznikov voljni in odločitveni proces (odločitev posameznika) ter jo iz sistema upravljanja tveganj ne moremo izločiti. Vloga zaposlenih je negativna v povzročanju naključnih ali zlonamernih napak in pozitivna v odpravljanju napak. Pri tem se moramo zavedati, do so samovarovalne aktivnosti zaposlenih ter preprečevanje in omejevanje možnosti za škodne dogodke pretežno prostovoljna dejanja, pri katerih sta ključna pojma pripravljenost in volja nekaj delati, da ne bi prihajalo do nezaželenih posledic. Motiviranje, kontroliranje in spreminjanje vedenja zaposlenih pri delu pa vsebuje čedalje več

moralno - etičnih vprašanj, ki so tesno povezani z delovnim konformizmom in deontološkim kodeksom upravljavca KI.

3.6 SISTEM IN PROCES OCENJEVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Upravljavec KI oblikuje sistem upravljanja tveganj, ki po zakonu predstavlja osnovo za usmerjeno in aktivno upravljanje tveganj. Sistem je iz organizacijskega vidika sestavljen iz: upravljavca KI, sektorja korporativne varnosti, odbora za tveganja, organizacijske enote, poslovne enote in službe upravljalca KI. Sistem za upravljanje tveganj predstavlja osnovo za usmerjeno in aktivno upravljanje tveganj. Sledi postopek upravljanja tveganj (identifikacija, ocenjevanja, obvladovanje in spremljanje tveganj), podrobno pa je tudi določena metodologija ocenjevanja. Sistem upravljanja tveganj je prikazan na sliki 28.



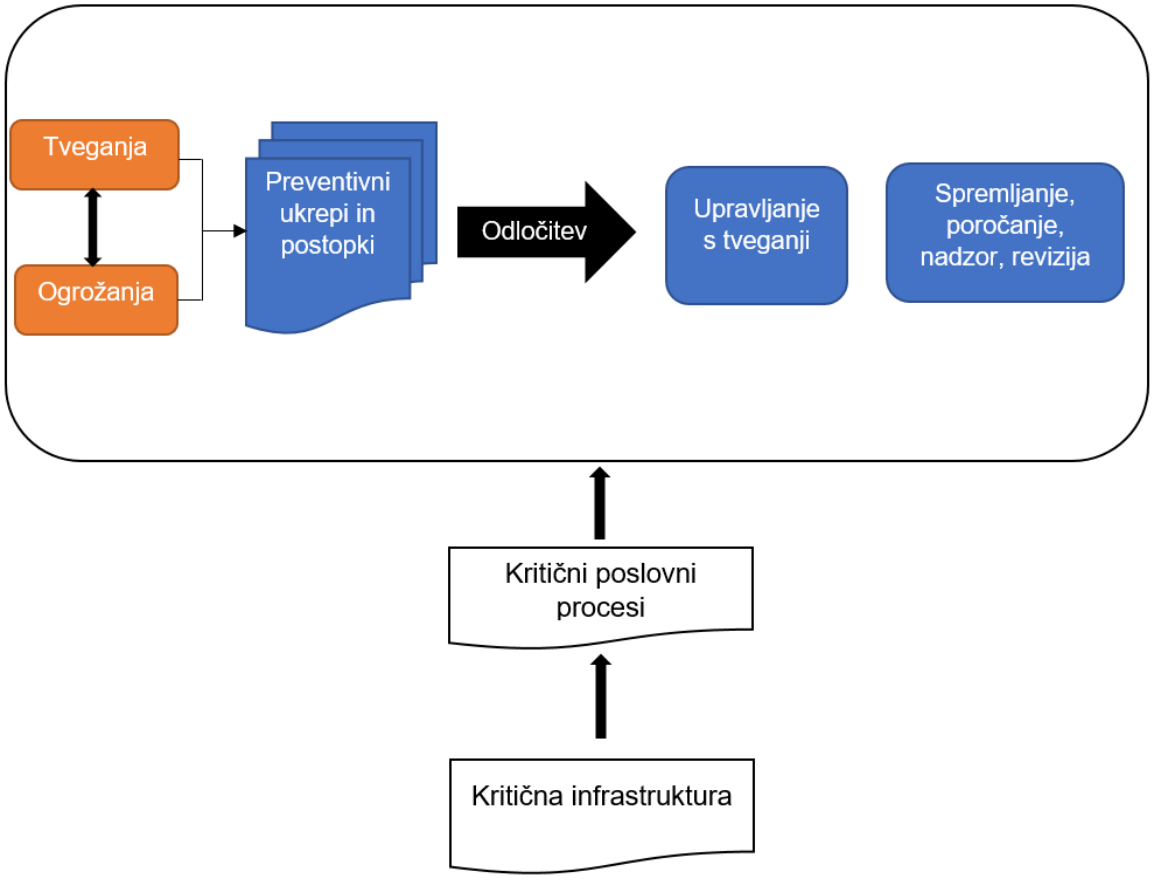
Slika 28: Sistem upravljanja tveganj z organizacijskega vidika (interni vir ICS)

3.6.1 Proces ocenjevanja in upravljanja tveganj

Proces ocenjevanja in upravljanja tveganj je sestavljen iz petih medsebojno povezanih procesov, in sicer: (i) identifikacija (prepoznavanje) tveganj; (ii) ovrednotenje možnih vplivov; (iii) analiziranje možnih rešitev; (iv) sprejetje rešitve in (v) spremljanje tveganja, nadzor in revidiranje. Celotni proces temelji na določenih poslovnih procesih, virih in vzrokih negotovosti ter kritičnosti poslovnih procesov. Prikazan je na sliki 29.

Slika 29: Proces upravljanja tveganj (interni vir ICS)

Metodološko je širši proces upravljanja tveganj prikazan na sliki 30. Nanaša se na določitev kritičnih poslovnih procesov, možna ogrožanja, ocenitev tveganj, določitev preventivnih aktivnosti, ukrepov in postopkov, odločitev vodstva upravljavca KI in spremljanje, poročanje, nadzor ter tekoča revizija tveganj.



Slika 30: Širši proces upravljanja tveganj (interni vir ICS)

3.6.2 Določitev kritičnih poslovnih procesov

Določitev kritičnih poslovnih procesov se nanaša na značilnosti posameznih procesov in njihovega opisa. Določanje kritičnih poslovnih procesov je podrobneje opredeljeno v standardu ISO 22301. Posamezne značilnosti procesa so prikazane v tabeli 2 (cilj procesa, tip procesa, področje procesa, proces, ki se zaključi pred njim, podprocesi in aktivnosti, storitev (produkt) procesa, uporabniki procesa, pomembni notranji in zunanji partnerji, lastnik procesa, ključni informacijski sistemi, ostali ključni viri, ključna potencialna tveganja, ključne notranje kontrole, neprekinjenost poslovanja, krizno upravljanje), z opisom navedenih značilnosti procesa. Kritične poslovne procese je treba bolj podrobno obravnavati tudi (ali predvsem) z vidika zagotavljanja neprekinjenega poslovanja in kriznega vodenja. Kajti kritični poslovni procesi morajo delovati tudi v kriznih razmerah. To še posebej velja za KI, ki mora po ZKI delovati tudi vseh vrstah kriz. Gre torej za ocenjevanje tveganj, ki lahko sprožijo krizo, pri tem pa gre tudi za izdelavo načrtov neprekinjenega poslovanja (v skladu s standardi ali brez), kriznih načrtov in načrtov kriznega komuniciranja. Iz dosedanjih projektov v KI je namreč razvidno, da je področje neprekinjenega poslovanja in kriznega vodenja v KI nedorečeno področje (ugotovitev iz pregleda projektov v KI – Vršec/Vršec 2011, Marinčič 2017).

Tabela 2: Določitev kritičnih poslovnih procesov (interni vir ICS)

Značilnosti procesa	Opis procesa
▪ cilj procesa ▪ tip procesa ▪ področje procesa ▪ proces, ki se zaključi pred njim ▪ podprocesi in aktivnosti ▪ storitev (produkt) procesa ▪ uporabniki procesa ▪ pomembni partnerji ▪ lastnik procesa ▪ ključni informacijski sistemi ▪ ostali ključni viri ▪ ključna potencialna tveganja ▪ ključne notranje kontrole ▪ neprekinjenost poslovanja	

Po oceni kritičnosti se izvede primerjava ocene kritičnosti. Primerja se zlasti scenarije, ki so bili ocenjeni kot najbolj kritični, z ocenami v rdečem polju.

Tabela 3: Ocena kritičnosti procesa (interni vir ICS)

	Ocena kritičnosti procesa	**Ocena tveganja**
Cilj		
Področje		
Tvegani dogodki		
Kontrole		
Verjetnost / vpliv		
Pristop		
Rezultat		

V tabeli 4 so prikazani časi nedostopnosti produkta poslovnega procesa. Od časa, kdaj je vpliv pomemben, so odvisni ukrepi in postopki za neprekinjeno delovanje in tudi potrebna finančna sredstva.

Tabela 4: Nedostopnost produktov poslovnega procesa – kritičnost časa (interni vir ICS)

Poslovni proces	**Stopnja vpliva glede na ORM lestvico**								**Maksimalna dovoljena izguba**	**Čas, kdaj je vpliv pomemben**
	2 uri	**4 ure**	**1 dan**	**2 dneva**	**1 teden**	**2 tedna**	**3 meseci**	**> 3 meseci**		
proces 1									2 uri	
proces 2									2 uri	
proces 3									1 dan	
...									2 dni	
proces n									več kot 3 mesece	

Nedostopnost produkta poslovnega procesa je poleg stopnje tveganja eden od najbolj pomembnih dejavnikov. Nanaša se na predhodno ocenjene kritične poslovne procese, stopnjo vpliva tveganja na posamezni poslovni proces in maksimalno časovno dovoljena nedostopnost produkta.

Prag tolerance določi odbor za tveganja[12], za tveganja v rdeči coni pa vodstvo upravljavca KI. Postopki obvladovanja tveganj vključujejo aktivnosti, ukrepe, postopke in pravila za sprejemanje, zmanjševanje, razpršitev, prenos in izogibanje tveganj. Vsako identificirano tveganje se oceni z vidika vpliva in verjetnosti, skladno s petstopenjsko lestvico (vpliv: 1 - nepomemben, 2 - majhen, 3 - pomemben, 4 - resen, 5 - zelo resen; verjetnost: 1 - malo verjetno, 2 - redko, 3 - možno, 4 - verjetno in 5 - skoraj zanesljivo). Za vsako tveganje izračunamo skupno oceno tveganja, ki predstavlja vrednost (produkt) obeh ocen parametrov vpliva in verjetnosti. Matriko tveganj uporabljamo za razvrščanje tveganj znotraj posameznih kategorij tveganj.

Tabela 5: Analiza tveganj (primer za najbolj tvegane procese in sisteme)

Tveganje »rdeče cone«

Poslovni proces	Opis tveganja	Vzrok	Izredni Dogodek	Trenutni vpliv na proces, zaupanje in finance	Verjetnost nastanka dogodka	Načrt rešitve (kaj, kdo, kdaj)	Ciljni vpliv na proces, zaupanje in finance	Verjetnost	Opombe

Kot pomoč pri določanju vzrokov tveganj služi tabela izrednih dogodkov. Razdeljena je v več kategorij (nivojev): zaposleni, upravljanje in procesi, delovanje sistemov in vpliv zunanjih dogodkov. Tabelo dopolnjujejo konkretni primeri in definicije.

Tabela 6: Izredni dogodki (interni vir ICS)

Kategorije – 1. nivo	Kategorije – 2. nivo	Ponazoritev
Zaposleni	Kadrovski vidik	
	Organizacijska kultura	
	Zanesljivost	
Upravljanje procesov	Proces odločanja	
	Operativni procesi	
	Komunikacija	
	Pravni okvir	
	Fizična in tehnična varnost	
Sistemi	Organizacija IT	
	Informacijska varnost	
Zunanji dogodki	Človeške grožnje	
	Naravne nesreče	

[12] Odbor za tveganja se imenuje na ravni organizacije KI, imenuje ga vodstvo upravljavca KI, sestavljajo ga član vodstva in odgovorni za poslovni proces, pravna vprašanja, stike z javnostmi ter za korporativno varnost.

3.6.3 Rezultati ocenjevanja tveganj

Rezultati ocenjevanja tveganj se nanašajo na seznam tveganj, matriko tveganj z registrom tveganj, načrt upravljanja s tveganji in poročanje o tveganjih. Prikazan je na sliki 31.

Slika 31: Rezultati ocenjevanja tveganj (interni vir ICS)

Za vsa tveganja v rdeči coni se pripravi načrt obvladovanja tveganja, za ostala tveganja pa ta načrt ni potreben (razen v primeru, da se z ukrepom prepreči povečanje tveganja). Načrt naj vsebuje podatke o:

- vsebini tveganja (opis),
- skrbniku tveganja,
- izbrani strategiji upravljanja tveganj,
- vzrokih za pripravo načrta za posamezna tveganja (zakaj?),
- pristopu k obvladovanju tveganja (kako?),
- akcijskem načrtu (kaj, kdo, zakaj?) in
- roku za ponovno identifikacijo in oceno tveganja.

3.6.4 Verodostojnost merjenja posameznih ocenjevanj tveganj

Ob analizi raznih ocen ocenjevanja tveganj se pojavlja vprašanje verodostojnosti (veljavnosti merjenja) posameznih ocen oziroma se lahko pojavljajo določene kontradikcije med posameznimi ocenami tveganja. Pri tem je poseben problem zaznavanje ogroženosti ocenjevalcev tveganja. Menimo, da je to opazno zlasti v delu, ki se nanaša na verjetnost ter posledice napak posameznika, kriminalitete in višje sile. Možnosti za subjektivne napake ali kriminalna dejanja so nekaj neprijetnega za ocenjevalca, ki se ob tem trudi, da sam sebi ne bi priznal te možnosti. Pri tem lahko ugotavljamo zlasti tri vrste pristranosti:

- nagnjenje k pretiravanju**;** to so odgovori, ki kažejo logična protislovja, s tem, da poskuša ocenjevalec pretiravati pri zaznavi verjetnosti in posledic možnih škodnih dogodkov,
- zmanjševanje občutka ogroženosti; prepozna se po nasprotujočih si odgovorih ocenjevalca, ki poskuša skriti nelagodje,
- pretirana racionalizacija**;** ocenjevalec poskuša opravičiti svoje odgovore s preveč logičnimi in racionalnimi stališči.

Prve dve pristranosti je dokaj lahko odkriti, kajti protislovja so očitna. Ta protislovlja imajo lahko za razlog željo ocenjevalca, da pretirava in tako potvarja resničnost. Enako velja za protislovja pri zmanjševanju pomena, ki se v svojem bistvu povezuje z odporom, da bi ocenjevalec priznal svoje možno nelagodje. Nasprotno pa je racionalizacijo težje odkriti, kajti lahko nastaja iz razloga, da ocenjevalec pri odgovorih sledi logično - razumski niti; po drugi strani pa so tudi ocenjevalci, ki imajo osebna stališča zelo racionalna, kar lahko povezujemo z njihovim načinom dela in življenja. Menimo, da racionalizacija nastopi predvsem zaradi zavestne ali podzavestne težnje, da bi odgovore opravičili. Racionalizacija je lahko tudi način samoobrambe, kajti zaposleni, ki je odkril svoj občutek ogroženosti, ga verjetno najrajši razlaga le z zunanjimi vzroki, da bi s tem potrdil, da sam ni prekoračil nobene formalne ali neformalne norme v zvezi z zadevo.

Ne glede na to, da se pri zaznavanju nevarnosti sklicujemo na verjetnost, ocenjevalec lahko določenih nevarnosti ne dojema kot verjetnosti proces. Zaposleni imajo težave pri dojemanju tveganja na verjetnostni način, nekatere ločene dogodke pa zaznavajo, kot da vplivajo drug na drugega (Polič, 1995). Zaznava verjetnosti neke nevarnosti je toliko manj uporabna, kolikor daljši je interval med že realiziranimi dogodki, kolikor so ti težje prepoznavni in, če jih je povzročil posameznik.

Omenili smo, da ocenjevanje ogrožanja zahteva presojo verjetnosti in zmožnost inteligentnega ter deduktivnega razmišljanja o malo verjetnih, toda pomembnih dogodkih. V razpravah o ogrožanjih oziroma tveganjih, povezanih z izrednimi dogodki, ogrožanjem

praviloma pripisujemo verjetnostno naravo, ocenjujemo jih kot bolj ali manj verjetne in se v skladu s to oceno tudi vedemo.

Razpoložljivost ocen je pogosto ustrezen znak za presojo pogostosti in verjetnosti. Vendar nanjo vpliva tudi mnogo dejavnikov, ki niso povezani z verjetnostjo. Ocenjevalci pogosto precenjujejo verjetnost nedavnih, čustveno nasičenih dogodkov. Vse prevečkrat jih pogojuje njihova neposredna preteklost ter omejujejo njihova predvidevanja na poenostavljene konstrukte, v katerih je prihodnost zrcalna slika preteklosti.

Zaznavo ogrožanj dodatno otežuje pretirana prepričanost o pravilnosti lastne sodbe. Ocenjevalci vse prevečkrat pretirano zaupajo lastnim, tudi napačnim ocenam. Zdi se, da je lahko osnova za neupravičeno gotovost njihova neobčutljivost za pomanjkljivost domnev, na katerih slonijo njihove sodbe, tj. na veljavnost hevristike razpoložljivosti. Taka pretirana prepričanost je nevarna, saj kaže, da se pogosto ne zavedamo, kako malo vemo o možnih ogrožanjih in koliko dodatnih obvestil ter interdisciplinarnega pristopa bi potrebovali. Pretirano samozaupanje po svoje spodbuja tudi človekova želja po gotovosti, ki se pogosto kaže tudi kot zanikanje negotovosti.

Zavajajoče izkušnje lahko ocenjevalce vodijo v prepričanje, da so imuni na mnoga ogrožanja, da se »to njim ne more dogoditi«. Raziskave kažejo, da včasih neuspeh pri oceni meja razpoložljivih podatkov vodi ocenjevalce v samozadovoljnost. Iz povedanega izhaja zaključek, da na tisto, česar ne vidimo, tudi ne pomislimo. Dejansko je ocena ogrožanja zelo zapleten proces, zasnovan bolj na teoretičnih analizah kot na neposredni izkušnji.

Postavlja se tudi vprašanje, kaj določa zaznavo ogrožanja. Zakaj čutijo ocenjevalci (in tudi drugi zaposleni) odpor do nekaterih ogrožanj, brezbrižnost do drugih, zakaj pride do neupoštevanja priporočil in navodil vodilnih delavcev, na kaj se nanaša in s čim je povezana ocena nekega tveganja.

Ocena ogrožanja je zapleten proces, ki v posameznih primerih ne temelji na realnosti ocene možnega ogrožanja. Eden od pomembnih dejavnikov ocene je tudi škodni potencial dogodka. Poleg navedenega obstajajo še drugi pomembni dejavniki, ki vplivajo na zaznavo ogrožanja, in sicer:

- osebnostne značilnosti**,** kot so nižji izobrazbeni nivo, spol, starost, anksioznost itd.
- situacijski dejavniki**,** npr. poslovanje ni pod večinskim nadzorom zaposlenega, neprostovoljnost izpostavljenosti ogrožanju, pred kratkim se je dogodila nenormalna situacija, neustrezni viri informacij, nezaupanje v avtoritete, velika medijska pozornost, itd.
- značilnost tveganja**,** npr. grožnja predstavlja takojšnje zdravstvene (osebne) posledice, presenečenje - nizka verjetnost tveganja, strah zbujajoča nevarnost, itd.

Navedeno nazorno kaže na zapletenost zaznave ogrožanja. Zaznava ogrožanja ne poteka le na individualni ravni, ampak tudi skupinsko, kar pojasnjevanje tega problema še dodatno otežuje.

Pri obravnavi zaznave možnega ogrožanja je pomembna baza podatkov o preteklih škodnih dogodkih. V teh primerih predlagamo, da se ocenjevanje tveganja izdela na podlagi strokovnega mnenja, predvsem zaradi naslednjih dejavnikov:

- ni zbranih zgodovinskih podatkov o izrednih dogodkih (raziskanih in neraziskanih),
- zgodovinski podatki niso več ustrezni (spremembe v poslovnem okolju, poslovnih procesih in tehnologiji),
- baza podatkov je pomanjkljiva in je potrebna njena dopolnitev s strokovnim mnenjem in
- področje ocenjevanje tveganj je novo, brez ustrezne zgodovine.

Ocena tveganj na osnovi strokovnih mnenj vsebuje vsaj dva vira negotovosti, in sicer: (i) naravno negotovost spremenljivke, katere negotovost se ocenjuje in (ii) negotovost, ki izhaja iz pomanjkanja specialnosti, znanja in informacij ocenjevalca. V končni oceni tveganja nastopata navedeni negotovosti enotno in ju ni mogoče sintetično ločiti. Največkrat premalo upoštevana vira tveganj sta nekritična uporaba strukture modela ocenjevanja tveganj in nekritična uporaba samo lastnih mnenj. Mnenja in pripombe interdisciplinarno sestavljene skupine analitikov lahko v veliki meri zmanjšajo navedene pristranskosti in ožja razumevanja tveganj.

Pomisleki in težave pri oceni tveganja na podlagi strokovnega mnenja izhajajo iz psiholoških značilnosti odločanja posameznika v razmerah negotovosti. Ocenjevanje tveganja zahteva presojo verjetnostne narave sveta in zmožnost inteligentnega razmišljanja o malo verjetnih dogodkih (proaktivno razmišljanje). Izkušnje kažejo, da nekateri posamezniki niso najboljši ocenjevalci verjetnosti in da v posameznih primerih sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo. Zato njihove izbire (v posameznih primerih) ne ustrezajo osnovnim zahtevam doslednosti in skladnosti ocenjevanja tveganja.

Pogosto se uporabljajo posebne miselne strategije, s katerimi se težave s presojo realnosti poenostavijo. Posameznik išče zadovoljive rešitve, ki zadovoljujejo njegove najpomembnejše potrebe. Obstajajo celo mnenja, da sodbe o verjetnosti nimajo pomembne vloge v življenju posameznika. Večina izbir in odločitev je stvar izkušenj in/ali navad, ali pa so tako preproste, da ne zahtevajo posebne ocene verjetnosti. Prevladujoči značilnosti vsakdanjika sta stalnost in predvidljivost. Ko se ocenjuje verjetnost, se običajno ne uporablja verjetnostnih načel, ampak neko bolj ali manj razumno, pogosto vzročno teorijo o pojavu.

Pri zaznavi ogrožanj se lahko pojavljajo tipične miselne strategije, ki vplivajo na pristranske ocene tveganj. Primeri zavajajočih miselnih strategij so lahko naslednji:

- razpoložljivost preteklih dogodkov. Točnost ocene tveganja je določena s sposobnostjo pomnjenja in zaznavanja preteklih dogodkov. Tipični miselni vzorec je tisti, po katerem za nek dogodek menimo, da je verjeten in pogost, če si z lahkoto zamislimo njegove primere. Dostopnost je pogosto ustrezen znak za presojo pogostosti in verjetnosti. Verjetnost nedavnih, živih intenzivnih dogodkov je običajno precenjena. Navedene ocene tveganj ne upoštevajo spreminjajočega se poslovnega okolja in ne vključujejo predvidenih razmer v prihodnosti (proaktivno razmišljanje),
- reprezentativnost dogodka, ki se odraža v napačnem koncentriranju na posamezne podrobnosti dogodka, pri čemer se lahko izgublja celotna slika možnih ogrožanj. Sem spada tudi napačna ocena, da se narava negotovosti pojava velikega obsega lahko odraža tudi na manjšem vzorcu,
- sidranje, ki je verjetno najpomembnejši vir pristranskosti. Tu se prvi podatek o pojavu dogodka (o verjetnosti pojava) napačno jemlje kot izhodiščni, iz katerega se posledično napačno gradi končna ocena (tveganja) pojava,
- premalo strokovno znanje ocenjevalca,
- organizacijska kultura okolja, iz katerega prihaja ocenjevalec,
- pristranske ocene, ker lahko ima ocenjevalec (materialni) interes v zadevi, v zvezi s katero se ocenjuje tveganje,
- nepripravljenost postavljati ekstremne vrednosti ocen tveganja,
- želja po ponujanju odgovorov, za katere ocenjevalec smatra, da bi jih uporabnik pričakoval (ali želel),
- zaznavanje problema, da se od ocenjevalca pričakuje velika natančnost (opredelitev) določanja tveganj.

Da bi se možne napake (napačne zaznave, dojemanja ali razlage) medsebojno v čim večji meri zmanjšale, predlagamo, da se v praksi soočijo razna mnenja in pripombe za oblikovanjea dokončne ocene tveganja. Kot pomoč za navedeno predlagamo uporabo raznih metod »brainstorminga«, t. i. delphi metode, metode 360°, analitično razstavitev kompleksnega problema na manjše, bolj razčlenjene posamezne (vsebinsko zaokrožene) enote, ki jih lahko ocenjevalec z intuitivno logiko lažje razčleni, vrednoti in klasificira ipd., (vsekakor pa priporočamo skupinsko delo strokovnjakov z različnih področij dela).

4 PREDSTAVITEV (OPIS IN RAZČLENITEV) PROCESA OCENJEVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

V industriji, gospodarstvu in državnih institucijah je kar nekaj sektorjev, znotraj katerih je določena KI. To so tisti sektorji, katerih delovanje je neizogibno potrebno za normalno funkcioniranje celotne družbe – vse od državnih organov, industrije, gospodarstva, civilne družbe, do prebivalstva. Po ameriških merilih vitalno (ključno) KI sestavljajo naslednji gospodarski sektorji: elektroenergetski sistem, telekomunikacije, zdravstvo, transport, bančništvo in finance, vodovodni sistem, intervencijske službe, radioaktivne snovi, jezovi, vladne službe, zaščita in reševanje ter pomembne poslovne zgradbe (Gheorge 2006, Lewis 2006, Murray 2007). Podobno strukturo KI opredeljuje evropski program zaščite KI, ki je bil v Evropski komisiji zasnovan že leta 2005. Zgoraj navedeni avtorji poudarjajo izredno pomembno aktivnost nosilcev sektorjev in upravljavcev KI, to je obvladovanja tveganj in zaščite gospodarskih družb, ki upravljajo s KI. V prvi vrsti gre za proces razpoznavanja in analiziranja tveganj v okviru upravljanja tveganja, tako imenovanega risk managementa, ki ga sestavlja zaporedje 10 korakov (Fennelly, 2003:5), in sicer:

- definiranje problema,
- definiranje predmeta obdelave,
- vrednotenje obstoječih ukrepov in sredstev,
- identificiranje tveganj,
- vrednotenje/ocenjevanje tveganj,
- sortiranje tveganj,
- priprava ukrepov skrčenja (zmanjšanja) tveganj,
- izvedba ukrepov skrčenja tveganj,
- vrednotenje ukrepov skrčenja tveganj,
- redefinicija tveganj in ukrepov.

Gre za enega od pristopov k celovitemu analiziranju tveganj, ki izhaja iz načela objektivnega presojanja in ocenjevanja negotovosti, nevarnosti in groženj, ki jih lansirajo zgodnji opozorilni sistemi ter analize izpeljanih scenarijev razvoja izrednih dogodkov. Nekateri avtorji dajejo poudarek identifikaciji in vrednotenju tveganj (npr. Hearnden/Moore, 1999:12-20), pri čemer izhajajo iz vzrokov za nastanek varnostnih tveganj (naravne nesreče, požari, kriminalna dejanja, industrijske nesreče, človekova malomarnost / brezbrižnost / napake / sabotaže, itd.) in posledic uresničitve tveganj, ki se izrazijo v materialnih, človeških, socialnih in moralnih škodah ter izgubah. Zaradi tega omenjena avtorja pravita, da je treba tveganja obvladovati sistematično. To ponazarja naslednji postopek: izogibanje (avoidance) visokim tveganjem, prenos (transfer) neobvladljivih tveganj na zavarovalnice, zadržanje (retention) nekaterih tveganj zaradi izkoristka poslovnih priložnosti in skrčenje oziroma zmanjšanje (reduction)

tveganj na raven, ki je obvladljiva na strateški in na operativnih ravneh poslovanja. V bistvu postaja skrb za upravljanje s tveganji ena od sodobnih poslovnih in korporacijskih funkcij, s katero se morajo ukvarjati lastniki, nosilci, upravljavci, management in nadzorniki posameznih gospodarskih družb, katerih dejavnost je propoznana kot KI. Kajti »tveganje postaja nov ključ skupnih interesov v poslovnem svetu in zahteva po visoki stopnji korporacijske odgovornosti« (Borodzicz, 2005).

Tveganja za delovanje KI je treba obravnavati, prepoznavati in presojati v sklopu upravljanja korporativne varnosti. Izhodišča in temeljni motivi za upravljanje korporativne varnosti v KI so najprej ranljivost in ogroženost premoženja, kapitala, vrednot, zaupanja uporabnikov in človeških virov, nato pa še razna stanja negotovosti (nepredvidljive okoliščine) in izpostavljenosti poslovnih procesov določenim izrednim dogodkom. Iz tega izhajajo varnostna in druga tveganja, ki jih je treba obvladati do te mere, da je omogočeno neprekinjeno poslovanje in obvladovanje morebitnih kriznih stanj. Tu je še zakonodaja (ZKI in drugi zakoni), ki določa okvire pri vzpostavljanju učinkovitih varnostnih in nadzornih mehanizmov. Vsaka korporacija, koncern, poslovni sistem in gospodarska družba je ranljiva zaradi številnih slabosti in vrzeli v poslovnih procesih ter v nadzornih in varnostnih mehanizmih, kar povečuje možnost za kriminalne, teroristične in druge napade. Poleg tega se gospodarski subjekti soočajo s konkretnimi grožnjami in izrednimi dogodki, ki jih je treba - s pomočjo zgodnjega opozorilnega sistema - zaznati in preprečiti, v primeru nastanka pa učinkovito razrešiti posledice in vzpostaviti poslovne procese v prvotno (normalno) stanje. Gre torej za obvladovanje varnostnih tveganj, ki so največkrat sestavni del poslovnih, finančnih, ekonomskih, tržnih, logističnih in drugih tveganj. Kajti obvladovanje varnostnih tveganj je sestavni del doseganja visoke ravni poslovnih rezultatov v materialni (dobiček, konkurenčna prednost) in nematerialni obliki (kultura, etika, odgovornost, ugled, blagovna znamka). Zato je organiziranost celovitih varnostnih sistemov v sektorjih KI pokazatelj nivoja kakovosti in učinkovitosti obvladovanja tveganj. Pomemben element obvladovanja tveganj je tudi vzpostavitev zavarovalnega portfelja, ki uravnoteži finančne vložke in stroške ter škode in izgube kot posledice izrednih dogodkov.

Pri izdelavi metodologije za ocenjevanje tveganj za delovanje KI bi bilo smiselno razmisliti o naslednjih vprašanjih:

- kako zakonodaja, ki ureja delovanje posameznih sektorjev KI ureja upravljanje in/ali obvladovanje tveganj,
- kako posamezni mednarodni in slovenski standardi, ki posegajo na področje KI, opredeljujejo obvladovanje tveganj,
- kateri že znani modeli in metode obvladovanje tveganj so uporabni (v celoti ali delno) za obvladovanje tveganj za delovanje KI,

- kateri modeli in metode za obvladovanja tveganj so že uporabljeni s strani upravljavcev KI,
- ali imajo upravljavci KI izdelan načrt neprekinjenega poslovanja in krizni načrt,
- ali je pravi koncept obvladovanja tveganj po naslednji shemi: ocena ranljivosti, ocena ogroženost/nevarnosti, iz tega izhajajoča ocena tveganj in vse tri ocene kot podlaga za načrtovanje ukrepov za zaščito KI,
- ali bo treba za pridobitev relevantnih informacij za izdelavo uporabnega modela obvladovanja tveganj za delovanje KI opraviti določeno raziskavo v vzorcu večjih gospodarskih družb, ki upravljajo s KI? Z raziskavo bi pridobili odgovore na zgornja vprašanja.

Poleg teh vprašanj mora biti prisotno zavedanje, da je proučevanje znanih metod in modelov upravljanja in obvladovanja tveganj, z vidika primernosti za uporabo v KI, povezano s tem, da je treba dobro poznati organiziranost in delovanje posameznih sektorjev KI. Upoštevati je treba dejstvo, da so posamezni sektorji specifično ranljivi in ogroženi ter podvrženi splošnim in specifičnim tveganjem.

Na zgoraj opisan način je možno oblikovati model ali metodologijo obvladovanja tveganj za delovanje KI, ki bo vsebovala tveganja v vseh sektorjih KI in v kateri se bo našel vsak upravljavec KI. Na ta način bo sleherni upravljavec KI lahko za revizijo obvladovanja tveganj po novi (denimo izvirni) metodologiji uporabila obstoječe dokumente obvladovanja tveganj. Retorika, pisanja in debate o tveganjih uporabljajo različne izraze ravnanja s tveganji. Najpogosteje so uporabljeni izrazi kot so upravljanje s tveganji, obvladovanje tveganj in ocenjevanje tveganj. Potem so pa tu še naslednji izrazi: vrednotenje tveganj, zaznavanje tveganj, prepoznavanje tveganj, razpoznavanje tveganj, skrčenje tveganj, izogibanje tveganjem, izravnava tveganj, izločanje tveganj, analiziranje tveganj, kontrola tveganj, zavarovanje tveganj, ipd. Denimo, da je za potrebe te študije upravljanje tveganj aktivnost nosilcev sektorjev KI, to je ministrstev, ki potrdijo dokumente in spremljajo ter nadzirajo njihovo izvajanje, obvladovanje tveganj pa aktivnost upravljavcev KI, to je konkretnih gospodarskih družb, zavodov, državnih organov in Banke Slovenije, ki morajo poleg splošnih tveganj obvladovati tudi (svoja) specifična tveganja. Ocenjevanje tveganj po standardu ISO 31000 pa obsega prepoznavanje tveganj analiziranje tveganj in vrednotenje tveganj (glej sliko 33 v nadaljevanju). Dodajmo še nekaj o ključnih pravnih določilih o oceni tveganj v KI iz ZKI. »Upravljavci KI izdelajo oceno tveganj na podlagi navodila za ocenjevanje tveganj za delovanje KI (v nadaljnjem besedilu: navodilo), ki ga sprejme ministrstvo (za obrambo: dodali avtorji) in strokovnih usmeritev, ki jih za posamezne sektorje KI izdelajo nosilci sektorjev KI« (12. čl. zakona ZKI).

»Ocena tveganj za delovanje KI (v nadaljnjem besedilu: ocena tveganj) je rezultat celovitega postopka identifikacije, analize in ovrednotenja različnih virov tveganj za delovanje KI, ki se

izvede za zagotovitev podlage za oblikovanje ukrepov za zaščito KI« (3. čl. 8. točka ZKI). Poleg tega je še tu načelo celovitega pristopa, ki zahteva, da se v zaščito KI pred, med in po motnjah v delovanju KI vključijo vsi pristojni organi in organizacije, pri čemer se upoštevajo različne vrste nevarnosti, ki izhajajo iz ocene tveganj (10. čl. ZKI).

Pri oceni tveganj za delovanje KI je za celovit pristop izredno pomemben profesionalni (ekspertni) pristop projektne ekipe**,** ki vključuje naslednje zahteve iz dobre prakse: podiplomsko izobrazbo, reference na področju KI, poznavanje različnih metod, modelov in metodologij obvladovanja tveganj, dostop do tajnih podatkov in poslovnih skrivnosti, kritično razmišljanje in sposobnost inovativnega pristopa. Kajti izdelava ocene tveganj terja od vpletenih (Vlade RS, nosilcev in upravljavcev KI ter projektne ekipe) tudi visoko stopnjo odgovornosti in zaupanja. Že leta 1996 je Smallman ugotovil, da živimo v času izjemnega dinamizma v naravnem, socialnem in poslovnem svetu, kar povzroča strah, negotovost in dvom. Rezultat tega je prehod obvladovanja tveganja v fazo stalnih dinamičnih sprememb (Smallman, 1996). Več kot dvajset let po tej misli je današnji in prihodnji dinamizem življenja, dela in poslovanja še toliko večji in terja veliko mero znanja, izkušenj, poguma in prodornosti na področju obvladovanja tveganj.

V študiji se ukvarjamo z izborom ustreznih modelov ali metodologij za potrebe ocenjevanja tveganj za delovanje KI. Navsezadnje pa niti ni toliko pomembno s katero metodologijo se lotimo ocenjevanja tveganj za delovanje KI, bolj pomembno je, da bodo s to metodologijo zajeta zares vsa tveganja za delovanje KI.

Glede na to, da je v KI kar nekaj gospodarskih družb, ki morajo za potrebe obveznega organiziranja varovanja v načrtu varovanja izdelati tudi oceno stopnje tveganja, je potrebno proučiti tudi to obveznost teh družb.

4.1 POLITIKA UPRAVLJANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

4.1.1 Korporativno upravljanje

Za upravljanje KI se lahko uporabijo načela OECD, ki govorijo o korporativnem upravljanju gsopdarskih in drugih družb. V tem kontekstu nastajajo poslovni kodeksi in razvojne strategije pa rtudi razne politike upravljajnja industrije in gospodarstva. Potemtakem je tudi ali predvsem umestno, da o korporativnem upravljanju govorimo rtudi na področju KI.

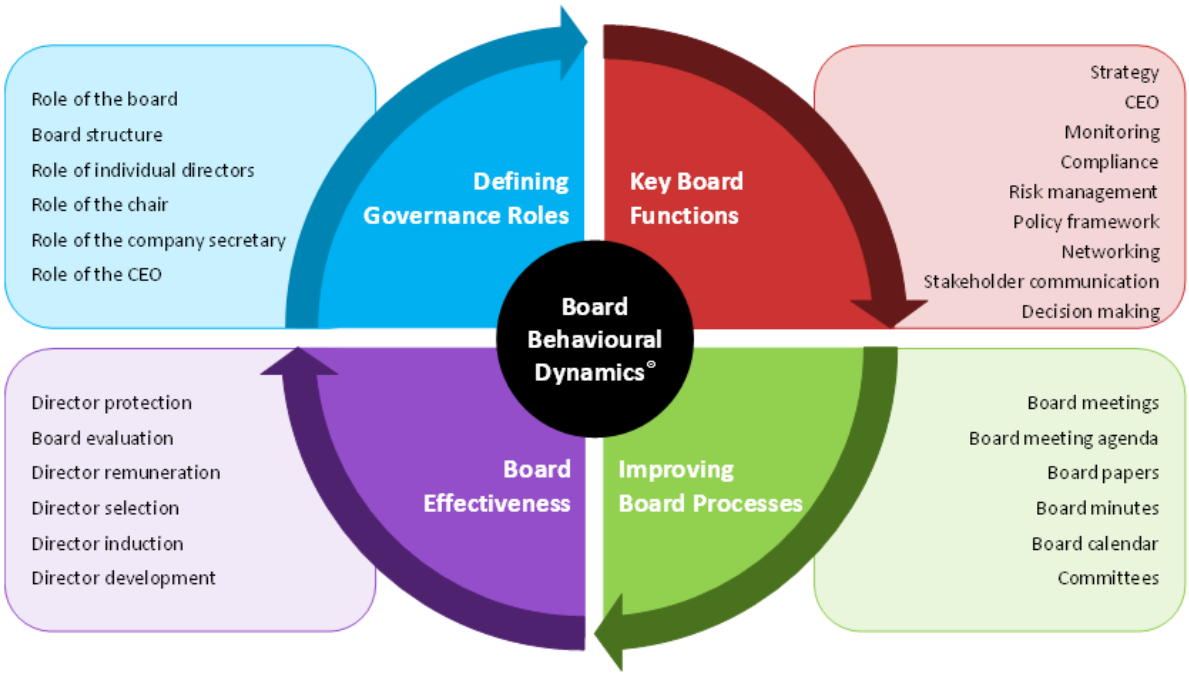
Na tej osnovi lahko nastanejo tudi politikle upravljanja tveganj v KI, ki jih vidimo v treh segmentih. Prvi segment je politika upravljanja tveganj kot sestavni del poslovne politike,

nato kot segment krovne varnostne poliotike in tudi kot neposredno orodje za upravljanje tveganj, ki obsega tudi obvladovanje in ocenjevanje tveganj.

Glede na to, da je KI vendarle prva linija gospodarstva, ki zagotavlja vsestransko oskrbo države, gospodarstva, civilne družbe in prebivalstva tudi v kriznih razmerah, je prav, da se tudi slovenska KI vključi v sodobni trend korporativnega upravljanja gospodarskih in drugih družb, bank, zavodov in državnih institucij. Kajti korporativno upravljanje (ang. corporate governance) je v svetovnem merilu, v sodobnem gospodarsvu in v sodobnem upravljanju države dobro poznano in uveljavljeno v praksi. Če smo malo bolj natančni gre pri korporativnem upravljanju za dve aktivnosti, in sicer za upravljanje (ang. governance) na strateški ravni in za vodenje (ang. management) na operativnih ravneh – torej na izvršnih ravneh poslovanja. Korporativno upravljanje je pravi okvir sodobnega upravljanja in vodenja tudi v KI. Da je temu tako, je razvidno tudi iz dokumentov Ministrstva za gospodarski razvoj in tehnologijo, Gospodarske zbornice Slovenije in Združenja nadzornikov Slovenije.

Korporativno upravljanje je (sistem strukturno in postopkovno opredeljenih odnosov med različnimi udeleženci v družbi. Med upravo, delničarji in nadzornim svetom ter ostalimi organi družbe je vzpostavljeno določeno razmerje in skupek postopkov in medsebojnih odgovornosti. Korporativno upravljanje je torej sistem, v okviru katerega se oblikujejo cilji in načrtuje pot k dolgoročni uspešnosti družbe. Institucionalni vlagatelji prepoznavajo dobro prakso korporativnega upravljanja kot instrument, ki zvišuje dolgoročno vrednost družbe.

Organizacija za gospodarsko sodelovanje in razvoj (OECD – Organization for Economic Co-operation and Development) korporativno upravljanje gospodarskih družb opredeli kot nabor odnosov med poslovodstvom družbe, organom nadzora, lastniki in drugimi interesnimi skupinami.



Slika 32: Governance model diagram (http://www.effectivegovernance.com.au/wp-content/uploads/2012/10/Corporate-Governance-Practice-Framework.png)

Okvir korporativnega upravljanja je določen s kombinacijo zakonodaje, predpisov, kodeksov in priporočil dobre prakse. Kako pomembni so posamezni elementi tega okvirja je odvisno od pravnega sistema. Kodeksi upravljanja so prostovoljni in velja, da jih družbe spoštujejo po lastni presoji.

Pri vzpostavljanju učinkovitega okvirja korporativnega upravljanja na ravni države in na ravni gospodarstva (delniške in druge družbe) je treba izhajati iz naslednjih osnov:

- vzpostaviti je treba tak način korporativnega upravljanja, ki pozitivno vpliva na nastopanje na trgih in preglednost trgov. Upoštevati je treba konkurenčno pravo,
- zakonske in regulatorne zahteve, ki vplivajo na prakso korporativnega upravljanja v določenem pravnem sistemu, morajo biti konsistentne z načeli pravne države, pregledne in izvedljive,
- odgovornosti posameznih organov in institucij morajo v določenem pravnem sistemu biti jasno ločene in v javnem interesu,
- nadzorni, regulatorni in izvršni organi morajo imeti jasna pooblastila, kompetence, integriteto in sredstva za izvrševanje svojih obveznosti na strokoven in objektiven način,
- upošteva se varnostna in etična dimenzija korporativnega upravljanja. V gospodarskih in drugih družbah je treba načrtovati in izvajati ukrepe za preprečevanje korupcije in drugih kriminalnih in neetičnih dejanj.

Iz načel korporativenga upravljana (OECD Principles of Corporate Governance – 2004 Edition) torej izhaja, da je varnostni vidik upravljanja tveganj strateškega pomena za obvadovanje tveganj v poslovnih procesih korporacij in posledično tudi nosilcev sektorjev in upravljavcev KI.

4.1.2 Politika upravljanja tveganj kot segment poslovne politike in razvojne strategije gospodarske družbe, ki upravlja s kritično infrastrukturo

V prihodnje bo KI vedno bolj podvržena raznim notranjim in zunanjim tveganjem. Zato se pred nosilce sektorjev, lastnike, upravljavce, vodstva in nadzornike postavlja zahteva po vedno bolj sofisticiranem (prefinjenem, domišljenem, učinkovitem) upravljanju in obvladovanju vseh tveganj. Postavlja pa se tudi zelo resno vprašanje ali vodstveni kader pri upravljavcih KI prepoznava celovito upravljanje tveganj kot del poslovne politike in jih uvrstijo v razvojno strategijo, letne plane in v vsakodnevno poslovno prakso. Vse bolj je pomemben vpliv tveganj na delovanje, poslovanje in poslovne rezultate gospodarskih družb. Pri tem lahko izhajamo iz opozorila Svetovnega gospodarskega foruma (The World Economic Forum WEF, Ženeva), ki pravi okvirno takole: »…potrebna je večja preglednost in odgovornost za obvladovanje vpliva tveganj na poslovanje, kot je pri tem pomembno tudi kritično vrednotenje vodstvenih sposobnosti vodilnih in vodstvenih timov za upravljanje tveganj. Poleg tega morajo biti člani uprav bolj prilagodljivi spremembam, pri čemer morajo razmišljati strateško kako upravljati naraščajočo nestanovitnost, negotovost, zapletenost in dvoumnost sveta« (povzeto iz standarda ISO 31000:2018, poglavje 3. Spreminjanje konteksta tveganja, Institute of Risk Management, London). Tudi naše ugotovitve (varnostnih) projektov v KI poudarjajo odsotnost celovitih ocen ranljivosti in ogroženosti, redkost politik in metodologij upravljanja tveganj in prešibko vključevanje obvladovanja tveganj v strateške in operativne dokumente.

Delovanje KI je potemtakem močno podvrženo tveganjem na vseh organizacijskih, vodstvenih in strokovnih ravneh. Torej so vsi poslovni procesi KI prepredeni s tveganji, zato je uporaba politike upravljanja tveganj tisto poslovno orodje, ki olajša pristop k učinkovitejšemu ravnanju s tveganji tudi v situacijah, ko so poslovni rezultati odlični. Zato je treba k upravljanju in obvladovanju tveganj za delovanje KI pristopati celovito, profesionalno, domišljeno in na dolgi rok.

4.1.3 Politika upravljanja tveganj kot sestavni del krovne varnostne politike v sektorjih kritične infrastrukture

Varnostna tveganja so pomemben del tveganj za delovanje KI. Lahko celo rečemo, da so varnostna tveganja vraščena v vsa druga tveganja (poslovna, finančna, proizvodna, tržna, logistična, informacijska, človeških virov). Tako lahko govorimo o »čistih« varnostnih tveganjih in »prikritih« varnostnih tveganjih. Čisto varnostno tveganje je denimo tveganje nastanka požara, tveganje naravne nesreče, tveganje vloma, tveganje delovne nesreče, tveganje vdora v informacijski sistem ipd., prikrito varnostno tveganje pa je denimo korupcijsko tveganje v sistemu javnih naročil, goljufija v finančnih transakcijah, podkupovanje v pogodbenih razmerjih, kriminalne nakane človeških virov, kriminalna ozadja financiranja določenega projekta, ipd. Vsa varnostna tveganja imajo izrazito nagnjenost k škodam in izgubam, torej k napadu na poslovne rezultate kateregakoli upravljavca KI. Zaradi kompleksnosti varnostnih tveganj je obvladovanje tovrstnih tveganj nujna sestavina krovne varnostne politike in izvedenih varnostnih politik, to je politike varovanja informacij, politike varstva osebnih in tajnih podatkov ter poslovnih skrivnosti, politike varnosti in zdravja pri delu, politike varstva okolja in drugih izvedenih (področnih) varnostnih politik. **Vsak upravljavec KI bi moral imeti izdelano krovno oziroma celovito varnostno politiko, katere del bi bila tudi politika upravljanja tveganj,** ne samo varnostnih; prav iz razloga, da imajo vsa druga tveganja pridih (ne)varnosti. Torej se vsa druga tveganja vrtijo okoli varnostnih tveganj; to še zlasti velja za KI. V tem kontekstu se mora varnostnim tveganjem za delovanje KI posvečati posebno pozornost.

Poslovno in finančno zdravje KI izhaja torej iz poglavitnega cilja, da so poslovni procesi čim manj obremenjeni s škodami in izgubami. Tu potemtakem nastopa krovna varnostna politika na vseh nivojih njenega nastajanja in implementiranja. Preprečevanje izrednih dogodkov, posledično pa preprečevanje škod in izgub (Loss Prevention) kot glavni moto krovne varnostne politike, bi moral prodreti v miselnost nosilcev sektorjev, lastnikov in upravljavcev KI.

4.1.4 Politika upravljanja tveganj kot krovni dokument za upravljanje in obvladovanje vseh tveganj za delovanje kritične infrastrukture

Struktura in vsebina dokumenta o politiki upravljanja tveganj je v skladu z zakonskimi zahtevami in zahtevami standardov, ki dajejo smernice in navodila za upravljanje in obvladovanje tveganj. V KI je treba upravljati in obvladovati, na podlagi dobre prakse, vsaj naslednje vrste tveganj: (povzeto po projektih v KI, Vršec/Vršec, 1997 – 2016 – glej ICS Raziskovalno področje - raziskave 2018):

- poslovna tveganja,
- finančna tveganja,
- informacijska tveganja,
- komunikacijska tveganja,
- proizvodna tveganja,
- logistična tveganja,
- tehnično-tehnološka tveganja,
- okoljska tveganja,
- tveganja pravne narave,
- tveganja človeških virov,
- tveganja poslovnih partnerjev in outsourcinga,
- varnostna tveganja,
- strateška tveganja,
- operativna tveganja.

Upravljanje navedenih zveganj se nanaša na nosilce in upravljavce KI. V dokumentu o politiki upravljanja tveganj morajo biti zajete vse vrste tveganj, s poudarkom na poslovnih, informacijskih, komunikacijskih in varnostnih tveganjih ter tveganjih človeških virov.

Obvezni segmenti politike upravljanja tveganj, ki je prikazana v spodnji shemi, so priloge**,** ki razčlenjujejo posamezne dele dokumenta in, ki omogočajo implementacijo politike v prakso, torej v sektorje KI. Tako je dokument o politiki upravljanja tveganj krovno poslovno orodje obvladovanja tveganj za delovanje KI.

Tabela 7: Upravljanje tveganj za delovanje KI (interni vir ICS)

Strateški dokument: Politika upravljanja tveganj

Strateški dokument **POLITIKA UPRAVLJANJA TVEGANJ** **(dokument vsebuje)**	**Priloge**	
1 Izhodišča • Ocena ranljivosti • Ocena ogroženosti • SWOT analiza • Zakonodajni okvir • Metodološki okvir • Standardi za upravljanje tveganj • Standard ISO 31000:2018 in ISO/IEC 31010:2018 (SIST ISO 31000:2011) • Dinamičnost tveganj (obvladovanje sprememb)	Matrika ranljivosti **Matrika ogroženosti** Nevarnosti in tveganja iz SWOT analize Ključna zakonodaja **Metodologija upravljanja tveganj za delovanje KI** **Obvezni** in neobvezni standardi **Prikaz standarda ISO 31000:2018 in podpornega standarda ISO 31010**	

2 Namen in cilji • Namen • Cilji		
3 Načela in proces upravljanja tveganj	**Prikaz procesa obvladovanja tveganj**	
4 Kompetence, potrebna znanja in izkušnje za upravljanje tveganj		
5 Veriga odgovornosti • Vodstvo (uprava, upravni odbor) • Glavni upravljavec tveganj (»risk manager«) • Nadzorni svet • Odbor za upravljanje tveganj • Notranja kontrola in revizija • Vodstveno osebje na vseh ravneh • Zaposleni	Seznam pooblastil, pristojnosti, nalog (obveznosti) in odgovornosti za posamezne deležnike v verigi odgovornosti	
6 Klasifikacija tveganj – vrste tveganj	Matrika klasifikacije	
7 Register tveganj	**Elementi registra tveganj**	
8 Strategija in protokoli upravljanja tveganj	Elementi protokola	
9 Obrambne linije v obvladovanju tveganj		
10 Načrt obvladovanja tveganj	Elementi načrta	
11 Vodstveni pregled in sistem notranjih kontrol		
12 Sistem notranjega poročanja	Monitoring spremljanja učinkovitosti	
13 Zagotavljanje neprekinjenega poslovanja	**Elementi načrta neprekinjenega poslovanja – standard ISO 22301** Prikaz standarda neprekinjenega poslovanja ISO 22301 in ISO/IEC 27005 v povezavi z ISO 9001	
14 Krizno vodenje in scenariji za načrtovanje in izvajanje vaj obvladovanja verjetnih izrednih dogodkov	**Elementi kriznega načrta in elementi načrta kriznega komuniciranja** **Metodika izdelave scenarijev**	
15 Usposabljanje za zavedanje o obstoju tveganj in o njihovem obvladovanju		
16 Implementacija politike upravljanja tveganj		

4.1.5 Obrazložitev nastajanja in uporabe prilog v politiki upravljanja tveganj

Osnovni pogoj uporabnosti dokumenta o politiki upravljanja tveganj za delovanje KI je priprava posameznih prilog. Prilog je 18 in terjajo proučitev ustrezne zakonodaje, ustreznih standardov in ustrezne literature in virov. »Obvezne« priloge, ki omogočajo celovito

implementacijo politike upravljanja tveganj, so (priporočamo na podlagi raziskovalnega gradiva o KI, ICS 2018):

- matrika ogroženosti,
- metodologija upravljanja tveganj za delovanje KI,
- obvezni standardi,
- prikaz standarda obvladovanja tveganj ISO 31000:2018,
- prikaz procesa obvladovanja tveganj,
- elementi registra tveganj,
- elementi načrta neprekinjenega poslovanja s prikazom standarda neprekinjenega poslovanja ISO 22301,
- elementi kriznega načrta in načrta kriznega komuniciranja,
- metodika izdelave scenarijev.

Polovica (devet) vseh nakazanih prilog je dejansko potrebnih za umeščanje politike upravljanja tveganj sektorjev KI in upravljavcev KI.

Pri nastajanju (pripravi, izdelavi) prilog je potreben domišljen in inovativen pristop, ki upošteva kompleksnost KI ter vso specifiko organiziranosti, delovanja, poslovanja in problematike KI, ki se mora podrediti vsem zahtevam po neprekinjenem poslovanju in razreševanju kriznih stanj. Le na ta način lahko nastanejo priloge, ki bodo uporabne za nosilce sektorjev, upravljavce KI in njihovo vodstvo. Tako pripravljena politika upravljanja tveganj bo omogočala celovito in profesionalno obvladovanje vseh vrst tveganj, predvideno v ZKI in bistvo usmeritev uporabljenih standardov. Pričakujemo, da bo nakazan pristop k pripravi in uporabi politike upravljanja tveganj v KI dobil podporo pri nosilcih in upravljavcih KI.

4.2 PROCES UPRAVLJANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTRE

Pri upravljanju KI se vse bolj uveljavlja procesni pristop, tako pri oblikovanju politik, strategij, planov in projektov kot tudi pri upravljanju tveganj, ki lahko zagrenijo ali osrečijo vodstveno filozofijo o doseganju dobičkonosnih poslovnih rezultatov. Z vidika tveganj so poslovodstva in ostali deležniki srečni in zadovoljni samo v primeru, da so vsa tveganja obvladovana z ustreznimi preventivnimi in kurativnimi ukrepi, vključno z zavarovalnim portfeljem. Neobvladovanje tveganj posledično pomeni neobvladovanje ranljivosti in ogroženosti, neučinkovito razreševanje nastalih izrednih dogodkov, vse to pa povzroča škode, izgube in nepotrebne stroške. Prav zato je procesni pristop k upravljanju tveganj priljubljen in zahteven ter se ga lotevajo v razvoj usmerjena poslovodstva. Sodobno in vse pogostejšim

spremembam podvrženo upravljanje terja, da morajo strateška in operativna vodstva v poslovne procese uvajati standarde kakovosti, varnostne standarde, standarde upravljanja tveganj in druge obvezne in neobvezne standarde. V tem kontekstu je zelo pomemben segment upravljanja tveganj vzpostavitev procesa upravljanja in obvladovanja tveganj, ki ga določa politika upravljanja tveganj. Že standard kakovosti SIST EN ISO 9001:2015 eksplicitno postavlja zahtevo za procesni pristop na temelju modela PDCA (plan –do – check - act) ter zahtevo za upravljanje sistema kakovosti na podlagi upravljanja s tveganji. Tiste gospodarske družbe v sektorjih KI, ki imajo v poslovne procese uvedene standarde kakovosti, so že v sklopu tega standarda zavezane k vzpostavitvi procesa upravljanja s tveganji. Nekatere gospodarske družbe v sektorjih KI imajo uvedene tudi standarde SIST EN ISO 14001:2015 (okoljska tveganja), standard OHSAS 18001 in ISO 45001:2018 (tveganja varnosti in zdravja pri delu), HACCP in ISO 22000 (tveganja varnosti in sledljivosti živil) in druge standarde, kar še upravljavcem KI dodatno nalaga obveznosti po obvladovanju (specifičnih) tveganj v določenih sektorjih KI.

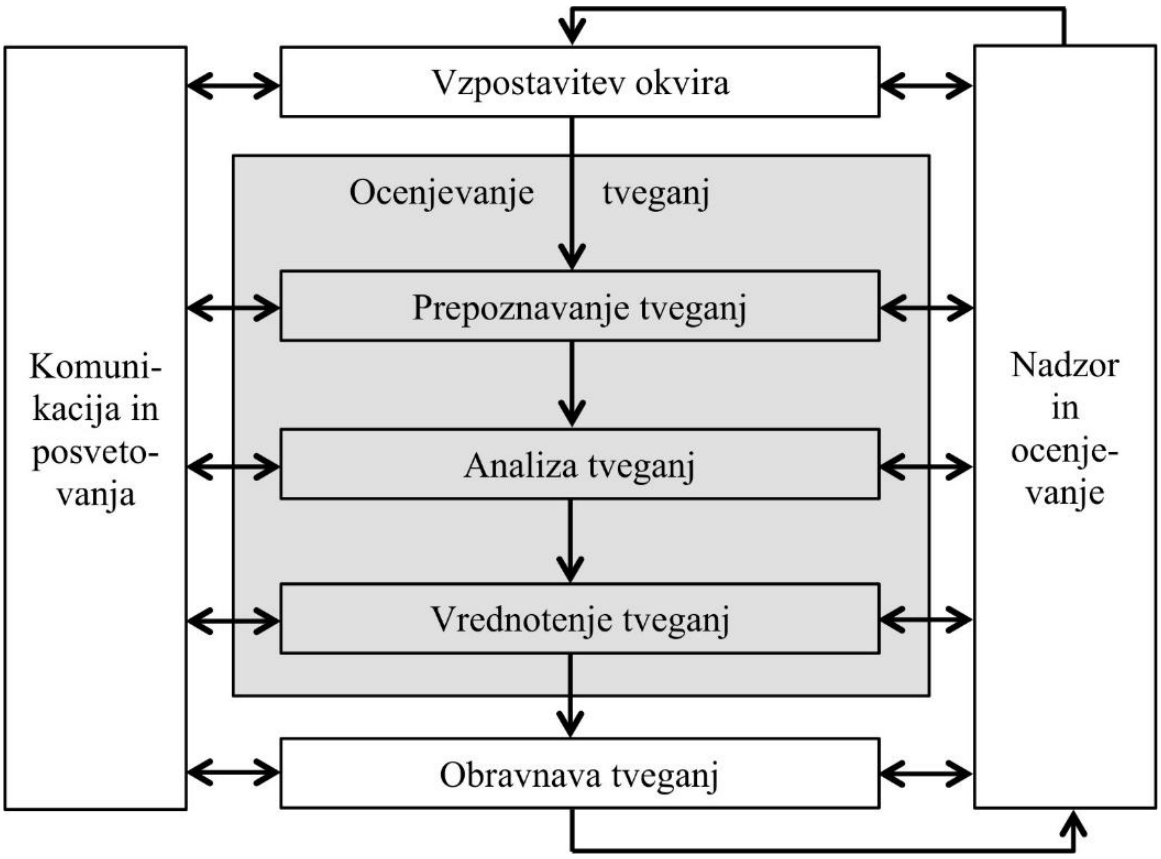
Če so standardi kakovosti, s spremljajočimi varnostnimi standardi, prvi okvir za proces upravljanja tveganj za delovanje KI, lahko rečemo, da je drugi okvir za oblikovanje procesa upravljanja tveganj za delovanje KI posodobljeno poslovno orodje COSO ERM 2017 (The Committee OF Sponsoring Organizations of the Treadway Commission-Enterprise Risk Management). To poslovno orodje prinaša sodobne in učinkovite metodološke usmeritve za vzpostavljanje sistemov upravljanja s tveganji v katerikoli organizaciji. Je torej splošno uporabna metodologija, ki ob primerni implementaciji zagotavlja uspešno obvladovanje tveganj. Poleg tega je COSO ERM neke vrste podlaga tudi za standard obvladovanja tveganj ISO 31000:2018, ki je po naši presoji eno od ključnih izhodišč za proces upravljanja in obvladovanja tveganj za delovanje KI. Po COSO ERM 2017 je proces upravljanja tveganj neprekinjen proces, ki ga vzpostavi najvišje vodstvo organizacije (minister, uprava, upravni odbor, generalni direktor) in to tako, da je proces upravljanja tveganj vključen v poslovno politiko, razvojno strategijo, notranje akte, poslovne procese in poslovne načrte, na vseh organizacijskih in managerskih nivojih. To je skladno z zakonsko zahtevo po neprekinjenem poslovanju KI (ZKI, členi 3/15., 10/3., 19., 24.), kakor tudi z vsebino standarda neprekinjenega poslovanja ISO 22301. Proces upravljanja tveganj mora biti oblikovan tako, da pravočasno identificira ranljive točke, preteče nevarnosti in verjetne izredne dogodke, ki bi lahko zaviralno vplivali na upravljanje in razvoj organizacije. Poleg tega vzpostavljen proces omogoča, da ostanejo tveganja znotraj določenih toleranc, kar nadalje zagotavlja doseganje poslovne uspešnosti in vzdrževanje neprekinjenega delovanja. Iz te osnove so v COSO ERM 2017 po našem videnju nakazane naslednje usmeritve, ki so pomembne za oblikovanje procesa upravljanja tveganj za delovanje KI:

- preprečevanje posledic in drugih negativnih vplivov na družbo,

- vzpostaviti je treba močno korelacijo tveganj s poslanstvom, vizijo in strategijo, poslovno uspešnostjo, poslovno učinkovitostjo, organizacijsko in varnostno kulturo, poslovno etiko, blagovnimi znamkami in vrednotami,
- obvladovanje notranjih in zunanjih sprememb zagotavlja poslovno odpornost, razvoj in doseganje strateških in operativnih ciljev,
- pri upravljanju in obvladovanju tveganj ne gre samo za to, da se preprečujejo škode in izgube ampak tudi za to, da se povečuje donosnost (dobičkonosnost, konkurenčnost) poslovanja,
- ni dovolj, da z obvladovanjem tveganj računamo samo na preživetje organizacije temveč je treba računati na stabilen obstoj in razvoj organizacije,
- proaktiven pristop k tveganjem nadomešča oziroma dopolnjuje preventivne mehanizme, kar vpliva na zmanjšanje kurativnih ukrepov in s tem na zmanjšanje stroškov obvladovanja izrednih dogodkov,
- tveganja ne obravnavamo samo v negativnem smislu temveč jih razumemo tudi kot pozitivne poslovne izide,
- proces obvladovanja tveganj mora med drugim zagotoviti zmanjšanje negativnih presenečenj – torej zmanjšanje izrednih dogodkov,
- hitro in strokovno odzivanje na izredne dogodke je ena od prioritet obvladovanja tveganj,
- načrtovanje neprekinjenega poslovanja in obvladovanje krize so sestavni del neprekinjenega procesa obvladovanja tveganj,
- v sistemu obvladovanja tveganj mora biti zagotovljeno merjenje uspešnosti obvladovanja posameznih vrst tveganj,
- v procesu obvladovanja tveganj se mora povečati uporaba informacijske in komunikacijske tehnologije,
- sodobni pristopi k procesu obvladovanja tveganj omogočajo tudi uporabo računalništva v oblaku razen, če ne gre za tveganja zaupne narave.

Navedene sestavine COSO ERM 2017 so v veliki meri sorodne z vsebino standarda obvladovanja tveganj ISO 31000:2018, zato vzamemo za tretji okvir oblikovanja procesa upravljanja tveganj za delovanje KI družino standardov, in sicer: ISO 31000:2018 – ISO/IEC 31010:2018 – ISO Guide 73 in ISO/IEC 51:2014. Prvi standard se razume kot osnovni standard, naslednji trije pa v bistvu dopolnjujejo osnovnega in se razumejo kot podporni standardi.

V pomoč nam je tudi naslednja shema iz družine omenjenih standardov, v kateri je določeno katere aktivnosti v sistemu upravljanja tveganj neposredno sodijo v proces ocenjevanje tveganj.



Slika 33: Proces upravljanja tveganj po standardu ISO 31000

Iz slike 33 je razvidno, da v osrednji del procesa ocenjevanja tveganj sodijo naslednje aktivnosti:

- prepoznavanje tveganj,
- analiza tveganj,
- vrednotenje tveganj.

Prednost splošnega modela je tudi v tem, ker izhaja iz ocene ogroženosti, ki pove, kje so nevarnosti, in kateri verjetni izredni dogodki se lahko pripetijo upravljavcu KI. Z nakazanim razumevanjem procesa upravljanja tveganj za delovanje KI si torej pripravimo zahtevani celovit pristop, ki ga sestavljajo:

- posodobljeno poslovno orodje COSO ERM:2017, ki daje sodobne in učinkovite metodološke usmeritve pri vzpostavljanju sistemov in procesov upravljanja s tveganji,
- osnovni standard upravljanja s tveganji ISO 31000:2018, ki poudarja, da je upravljanje s tveganji sestavni del delovanja in poslovanja, prične se pri najvišjem vodstvu, ki mora zagotavljati skladnost, kakovost, varnost, neprekinjenost (tudi v krizi), preprečevanje škod in izgub ter zagotavljanje odpornosti in donosnosti poslovanja,

- podporni standard upravljanja s tveganji ISO/IEC 31010:2018, ki predstavlja tehnike ocenjevanja tveganj (ang. Risk Assessment Techniques) kot so: brainstorming, strukturirani intervju, notranja kontrola in revizija, predhodna analiza tveganj, (PHA), Delphy metoda, študija izpostavljenosti tveganjem (HAZOP), študija človeške (ne)zanesljivosti (HRA), cost/benefit, analiza poslovnih vplivov (BIA), analiza vzrokov in posledic, obvladovanje sprememb ipd.,
- podporni standard upravljanja s tveganji ISO/IEC 51:2014 (Safety Aspects – Guidelines for Their Inclusion in Standards) ki določa varnostne vidike standardov in procesov upravljanja s tveganji,
- podporni standard upravljanja s tveganji ISO Guide 73:2009/2016 – Risk Management Vocabulary (Upravljanje s tveganji: Besednjak), ki določa izraze za področje tveganj s ciljem, da se v procesih upravljanja s tveganji uporabi enotna terminologija.

Vse tri okvirje, torej standarde kakovosti SIST EN 9001:2015, COSO ERM 2017 in družino standardov ISO 31000 uporabimo za oblikovanje procesa upravljanja tveganj v sektorjih KI. Seveda so potrebne razumne prilagoditve, pri čemer (z vidika vsebine upravljanja s tveganji) upoštevamo tudi metodo BIA (vpliv poslovnih procesov) in Andersenov model in model obvladovanja tveganj na bazi notranje integritete in sinergij, ki dokaj kompleksno urejata ravnanje s tveganji. S tem načinom pristopa se v bistvu lotevamo oblikovanja integriranega procesa upravljanja s tveganji, ki je dokaj široko uporaben v praksi delovanja KI.

Okvirni prikaz procesa upravljanja s tveganji v sektorjih KI prikazujemo v naslednji tabeli.

Tabela 8: Upravljanje tveganj za delovanje KI

Strateški dokument: Proces upravljanja tveganj (interni vir ICS)

Strateški dokument PROCES UPRAVLJANJA TVEGANJ Koraki – stopnje – faze ocenjevanja (širše obvladovanja) tveganj	**Priloge za implementacijo procesa upravljanja tveganj**
1 Osnovna vprašanja z vidika ocene ranljivosti, ocene ogroženosti in SWOT analize: • Kaj se v naši organizaciji lahko zgodi in zakaj ? • Kakšna je verjetnost, da se tveganje uresniči? • Kakšne bodo (v negativnem smislu) posledice uresničitve tveganja ? • Ali je možno preprečiti ali vsaj omiliti škode in izgube in s tem prispevati k donosnosti poslovanja? • Ali z obvladovanjem tveganj omogočamo neprekinjeno poslovanje? • Ali smo pripravljeni na krizno stanje – ali imamo izdelane in z vajami preizkušene scenarije obvladovanja kriznega stanja?	Izdelava razčlenitve vprašanj, ki so podrobnejša podlaga za oblikovanje odgovorov.

2 **10** NAJTEŽJE OBVLADLJIVIH TVEGANJ, ki jih v procesu ravnanja s tveganji opredelimo kot prioritetna tveganja za doseganje ciljev organizacije. To so lahko strateška in operativna tveganja. Tveganje 1 Tveganje 2 Tveganje 3 Tveganje 4	Priprava obrazca za izdelavo seznama najtežje obvladljivih tveganj in opredelitev kriterijev za odločitev o tem katera tveganja so najtežje obvladljiva
3 OPREDELITEV SPECIFIČNIH TVEGANJ v lastni organizaciji z vidika organiziranosti, dejavnosti, logistike, zakonodaje, konkurence na trgih, razvoja in človeških virov	Vsak sektor oziroma upravljavec KI ima specifična tveganja, ki terjajo specifične metode obvladovanja
4 Analiza tveganj – ZAZNAVA (IDENTIFICIRANJE) TIPOV IN VRST TVEGANJ	Izdelava seznama notranjih in zunanjih tveganj, seznama vrst tveganj, ki so predmet kontinuirane obdelave v procesu upravljanja tveganj
5 Analiza tveganj – PREPOZNAVANJE IN RAZPOZNAVANJE TVEGANJ	Vodstvena odločitev o tem, da v procesu upravljanja tveganj ne bo hazardiranja in da se lotevamo samo obvladljivih tveganj
6 Analiza tveganj – ANALITIČNI POSTOPEK	Priprava postopka proučevanja tveganj z vidika notranjih in zunanjih vplivov, ranljivih točk in groženj in z vidika razvrščanja v strateška in operativna tveganja
7 Analiza tveganj – VREDNOTENJE TVEGANJ	Izdelava matrike tveganj glede na verjetnost in na višino posledic ter vpliv na poslovanje, razvoj in človeške vire
8 KONTROLA TVEGANJ – strategija obvladovanja tveganj • Izogibanje visokim tveganjem • Skrčenje tveganj na raven obvladljivosti • Izločanje nedonosnih tveganj – tveganj, ki močno negativno vplivajo na doseganje načrtovanih poslovnih rezultatov	Izdelava strategije obvladovanja tveganj
9 IZRAVNAVA TVEGANJ – OBVLADOVANJE TVEGANJ Z ZAVAROVANJEM PRI ZAVAROVALNICAH	Opredelitev katera tveganja bodo obvladovana z zavarovanjem Določitev pogajalskih izhodišč, ključnih določb pogodbe o zavarovanju ter okvirna ugotovitev realizacije odškodninskih zahtevkov
10 VODSTVENI IN STROKOVNI NADZOR NAD PROCESOM UPRAVLJANJA S TVEGANJI • Nadzor, ki ga po ZKI opravlja inšpektorat, pristojen za obrambo • Nadzor s strani nosilcev sektorjev KI (ministrstev) • Interni nadzor s strani vodstva gospodarske družbe, ki upravlja s KI	Izdelava protokolov nadzora, ki omogočajo reden, izreden, strokoven, celovit in kakovosten nadzor nad procesom upravljanja tveganj za delovanje KI
11 STROŠKI implementacije procesa upravljanja tveganj	Izdelava dokumenta o stroških

v sektorje KI	
12 NAČRT implementacije procesa v sektorje KI	Izdelava načrta
13 DELOVNA SKUPINA ZA IMPLEMENTACIJO	Imenovanje delovne skupine
14 PREVETRITEV IMPLEMENTIRANEGA PROCESA UPRAVLJANJA TVEGANJ (po enem letu izvajanja procesa v praksi)	
15 Revidiranje procesa upravljanja s tveganji	

Glede na to, da je po ZKI ocena tveganj eden od dokumentov načrtovanja zaščite KI in neposredna podlaga za izdelavo načrta ukrepov, je jasno, da je proces upravljanja tveganj eden od osrednjih poslovnih procesov, ki je vpet v vse druge procese upravljavca KI. Kajti z oceno tveganj dobijo nosilci sektorjev in upravljavci KI tiste informacije, ki v procesih njihovega odločanja omogočajo uresničevanje, poslanstva, vizije, strategije in načrtovanih poslovnih in drugih ciljev.

4.3 IZBRANE METODE ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KI

Na podlagi izbranih kriterijev za ocenjevanje metod (prikazani so v 2. poglavju tega gradiva) smo izbrali metodo MOSAR (Method organised systematic analysis of risk, metoda za sistematično analizo tveganja – v nadaljevanju: MOSAR), ki vključuje tudi metodologijo FMEA (Failure mode and effect analysis, analiza načina in učinka okvar – v nadaljevanju: FMEA), kot najprimernejšo za ocenjevanje tveganj za delovanje KI. Metodo MOSAR smo smiselno uporabili po standardu SIST EN ISO 12100:2011, Varnost strojev - Splošna načela načrtovanja - Ocena tveganja in zmanjšanje tveganja (ISO 12100:2010, slovenski prevod), v originalu Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO).

Ta mednarodni standard določa osnovno terminologijo, načela in metodologijo za doseganje varnosti že med njenim načrtovanjem. V pomoč načrtovalcem pri doseganju tega cilja določa načela ocenjevanja in zmanjševanja tveganja. Ta načela temeljijo na znanju in izkušnjah pri načrtovanju, uporabi, incidentih, nezgodah in tveganjih, v originalni verziji povezanih s stroji. Podani so postopki za prepoznavanje nevarnosti in ugotavljanje ter vrednotenje tveganja med posameznimi obdobji življenjske dobe stroja ter za odstranitev nevarnosti ali zadovoljivo zmanjšanje tveganja. Predstavljena so tudi navodila glede dokumentacije in preverjanja procesov ocenjevanja in zmanjševanja tveganja.

FMEA smo smiselno uporabili po standardu SIST EN 60300 - 3-4, Upravljanje zanesljivosti – 3.-4. del: Vodilo za uporabo - Vodilo za specifikacijo zahtev zanesljivosti (IEC 60300-3-

4:2007) - Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements (IEC 60300-3-4:2007).

Ta del IEC 60300 standarda podaja smernice za razvoj politik upravljanja z napakami za opremo in konstrukcije z uporabo analiznih tehnik, vzdrževanja, s poudarkom na zanesljivosti in razpoložljivosti.

4.3.1 Metodologija MOSAR

MOSAR je metododologija za sistematično analizo tveganj zlasti v industrijskem okolju, smiselno pa se lahko uporablja tudi za kritično infrastrukturo. Predstavlja sistemski in sistematičen pristop k ocenjevanju ter vrednotenju tveganja, določevanju prioritet, obravnavanju tveganj in upravljanju s tveganji proučevanega sistema. Razvita je bila na osnovi metodologije MADS[13] (Method of Disfunctional Systems, Metoda disfunkcijskih sistemov), ki vsebuje splošni model za popis nevarnosti.

Na sliki 34 je shematsko prikazan metodologija MOSAR. Ocena tveganja tehnoloških procesov v industrijskem okolju je področje, ki je povezana celota tako z vidika znanstvenega znanja kot tudi s socialno prakso. Tehnološkim procesom KI kjer obstajajo potencialne grožnje za zaposlene, javnost, okolje in lastnino, je treba nameniti več pozornosti. V času povečanih zahtev glede varnosti tehnoloških procesov (ki so tudi del ocene tveganja) prevladuje ideja preprečevanja nevarnosti. Predstavljen je sistematičen pristop, ki zagotavlja zaporedje faz za oceno tveganja tehnoloških procesov v industrijskem okolju in pojasnjuje vsebino izpolnjevanja posameznih korakov, kar nedvoumno prispeva k procesom ocen tveganja. Ustvarjena metodologija je skladna z veljavnimi pravnimi predpisi na področju preprečevanja industrijskih nesreč in je v ravnotežju z uporabljenimi postopki za praktično oceno tveganja.

[13] MADS model je sistematični pristop k razgrnitvi kompleksnih sistemov in vrednotenju potencialne škode na izpostavljenih delih sistema. Omogoča modeliranje mehanizma delovanja (tok nevarnosti) med virom nevarnosti in izpostavljenemu delu sistema.

Slika 34: Metodologija MOSAR (SIST EN ISO 12100:2011)

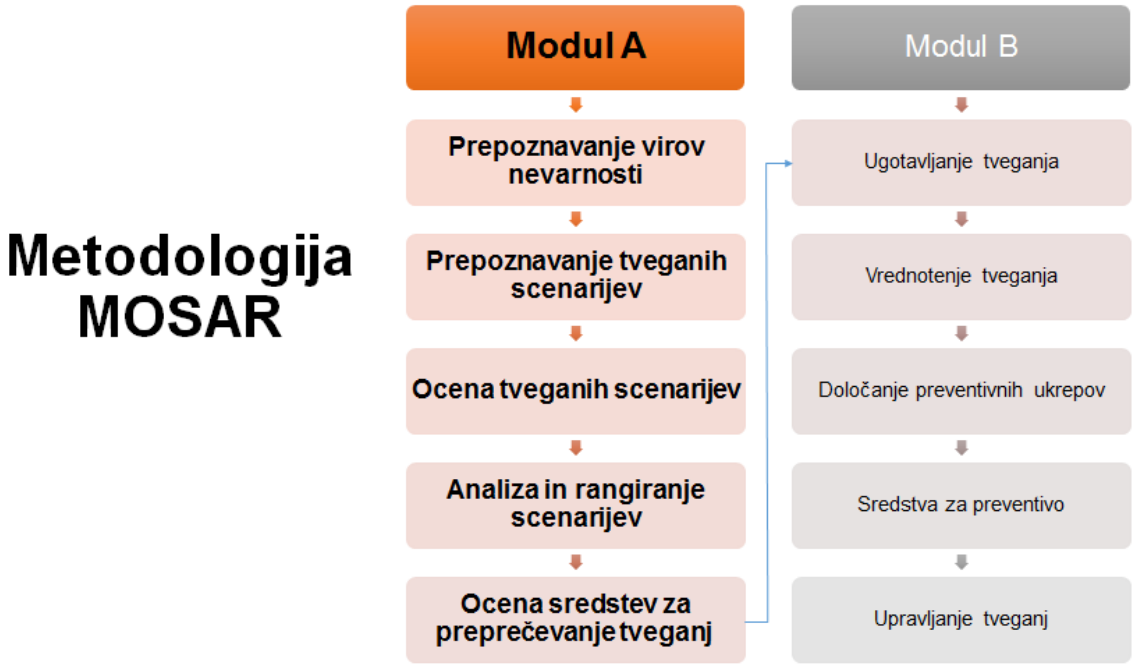
Metodologija je sestavljena iz opisa zmogljivosti sistema, s podsistemi. Cilj zmogljivosti opredeljuje uspeh zmogljivosti in mora biti specifičen ter merljiv. Sledi prepoznavanje nevarnosti delovanju sistema. Na podlagi kombinacije izkušenj, napovedovanja, strokovnega znanja o sistemu in drugih razpoložljivih virih se določi kontekst groženj in nevarnosti, ki primarno skrbijo družbeno skupnost, KI, njene uporabnike ali kažejo določen vpliv na njih. Z analizo tveganja in vrednotenjem tveganja se oceni vsako grožnjo in nevarnost v kontekstu ugotavljanja specifičnih ciljev zmogljivosti za vsako glavno zmogljivost. Ocenjevanje tveganja upošteva tudi možnost, da se varnostni ukrepi preprečijo ali zaobidejo. Ocenjevanje upošteva vse tisto, kar spodbuja preprečevanje ali obhod varnostnih ukrepov, na primer: varnostni ukrep upočasnjuje delovanje sistema ali pa ovira katerokoli drugo dejavnost oziroma želje uporabnika, varnostni ukrep, ki se težko uporablja, poleg upravljavca sistema so vključeni še podizvajalci, upravljavec sistema ne priznava ali ne sprejema varnostnega ukrepa kot primernega za to funkcijo ipd.

Sprejemljiva tveganja ustvarjajo nova tveganja, ko se jih ponovno vrednoti.

Za nesprejemljiva tveganja je treba za vsako ključno zmogljivost oceniti preventivne ukrepe, postopke in sredstva, potrebna za doseganje ciljev zmogljivosti (ustvariti ustrezen sistem zmanjševanja tveganj, upoštevati hierarhijo nadzora poslovnih procesov, izločiti ali nadomestiti nevarnosti, vodstveni nadzor ipd.). Zmanjšanje tveganj se lahko doseže z odstranitvijo nevarnosti ali z ločenim ali hkratnim zmanjšanjem vsakega od dveh elementov, ki določata pripadajoče tveganje:

- resnost škode, glede na obravnavano nevarnost in
- verjetnost nastanka te škode.

Po uporabi navedenih ukrepov in postopkov se delovanje sistema ponovno vrednoti. Osnovni elementi in struktura MOSAR so predstavljeni na sliki 35.



Slika 35: Metodologija MOSAR (prirejeno po standardu SIST EN ISO 12100:2011)

Cilj metodologije MOSAR je odkrivanje disfunkcij (neustreznega delovanja) in upravljanje s tveganji kompleksnega sistema. Uporablja strukturirane elemente, vsebuje splošen pristop k analizi tveganj in določa ukrepe ter postopke za zmanjševanje tveganj. Je pripomoček za lažje odločanje, iskanje glavnih scenarijev odpovedi sistema, določa potrebne ukrepe varovanja in zaščite za nevtraliziranje ali redukcijo izrednega dogodka. MOSAR je primeren za pripravo idejne zasnove novega sistema ali pri diagnosticiranju obstoječega sistema.

MOSAR v desetih korakih ocenjuje obseg interakcij podsistemov, in sicer: prepoznavo virov nevarnosti, ustreznost preprečevanja nevarnosti, soodvisnost sistema, uporaba metodologije

FMEA, drevo dogodkov, tabela resnosti škode, povezava resnosti škode s cilji varstva, upoštevanje tehnoloških in človeških ovir, izkoriščenost ovir (vključno s človeškim posredovanjem) in sprejemljivost tabele za preostalo tveganje.

Prednosti MOSAR so:

- sistematična tehnika analize tveganja,
- okvir metodologije sistematično ovrednoti vire nevarnosti in nato količinsko opredeljuje s tem povezano tveganje,
- dodatne prednosti, ki veljajo za tehniko prepoznavanja virov nevarnosti.

Slabosti MOSAR so:

- zamudni postopek,
- tehnika vključuje dolgotrajno identifikacijo nevarnosti kot del njene metodologije, nato pa tveganje za ugotovljene nevarnosti izračuna,
- vprašanje, ali obstajajo pri ugotavljanju virov nevarnosti še dodatne možne pomanjkljivosti?

Modul A MOSAR omogoča izvedbo analize tveganja sistema, ki ga je potrebno razdeliti na podsisteme, za vsak podsistem pa je potrebno poiskati (določiti) relevantne vire aktiviranja nevarnosti in jih povezati z izpostavljenimi deli sistema (tarče). Hierarhijo in prioriteto obravnavanih podsistemov se določi s projektnim delom s pomočjo skupine strokovnjakov. Za vsak scenarij aktiviranja nevarnosti se razvije vrsta posledic, ki prikazujejo možen potek dogodkov, kar se lahko prikaže z drevesi dogodkov (odpovedi sistema). Na podlagi v nadaljevanju prikazanih matrik se določi tudi pogostost in stopnjo resnosti posameznih vrst nevarnosti. Tveganje poškodb se nato določi s pomočjo matrike poškodb. Modul A MOSAR se zaključi z določanjem in oceno sredstev za preprečevanje oziroma zmanjševanje tveganj.

Modul B MOSAR omogoča podrobno analizo določenih delov sistema, še posebej z uporabo orodij za oceno zanesljivosti, s katerimi se odkriva morebitne tehnične disfunkcionalnosti v delovanju sistema s pomočjo metodologije (npr. FMA = Fault Mode Analysis) in orodij, s katerimi se odkriva disfunkcionalnosti v delovanju sistema (npr. HAZOP = HAZard and OPerability analysis ali FMEA = Failur Mode Effect Analysis)**.** Izrazoslovno so določene razlike med Modulom B MOSAR in metodologijo FMEA, vsebinsko pa predstavljajo okvirno enoten pristop (npr. korak Modula B MOSAR- korak FMEA: ugotavljanje tveganja - identifikacija vseh možnih odpovedi produkta ali procesa, identifikacija tipičnih načinov odpovedi). FMEA zagotavlja strukturirano in sistematično metodologijo ter je standardno orodje pri vzdrževanju in diagnostiki v industriji. Več o uporabi metodologije FMEA bo predstavljeno v posebnem poglavju.

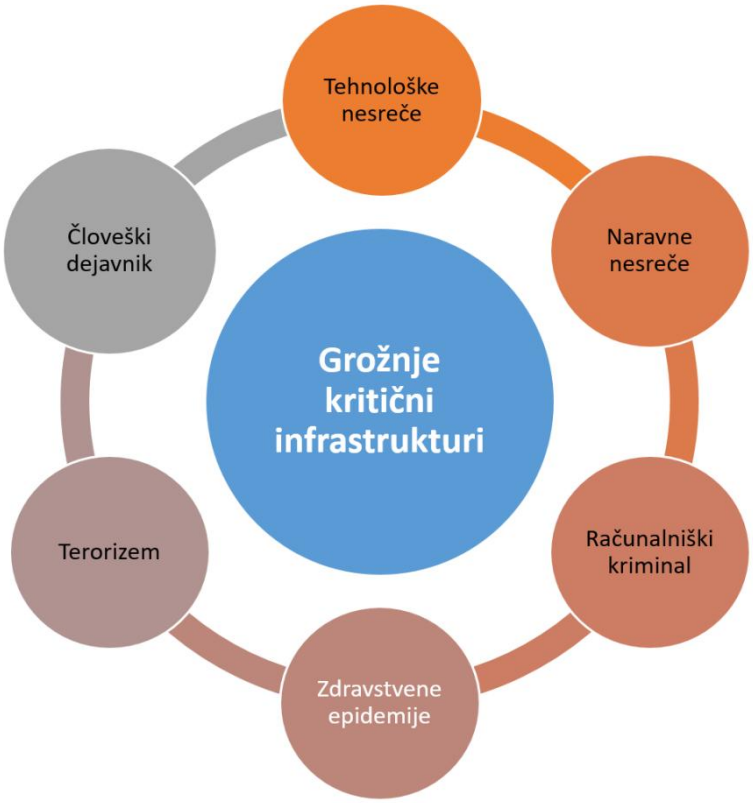
V nadaljevanju bo predstavljeno pet elementov (korakov) modula A MOSAR.

4.3.1.1. Prepoznavanje virov nevarnosti (1. korak)

Nevarnost nastopi v trenutku, ko ogrožajoči dejavniki, ki po svojem številu, intenzivnosti in pogostosti delovanja prekoračijo določeno vrednost, s tem pa je sistem toliko moten v svojem dejanskem stanju in delovanju, da ne more več opravljati svoje funkcije v prejšnjem obsegu. Gre za aktiviranje virov nevarnosti, ki prekoračijo prag sprejemljivega tveganja, tako da sistem ne more več opravljati svoje prvotne funkcije.

Nevarnost lahko povzročijo različni dejavniki, kot na primer posameznik, naravni pojavi in zakonitosti, kompleksni splet okoliščin ter dejavnosti. Viri nevarnosti so lahko klasificirani glede na vzrok, vsebino, čas, prostor, posledice in kontekst. Na splošno velja trditev, da je nevarnost karkoli, kar bi lahko povzročilo škodo.

Na sliki 36 so prikazani globalni viri nevarnosti. Nanašajo se na tehnološke nesreče, naravne in druge nesreče, računalniški kriminal, zdravstvene epidemije, terorizem in nevarnosti zaradi človeškega dejavnika. V nadaljevanju bodo posamezni viri šestih nevarnosti podrobneje opisani in predstavljeni.



Slika 36: Globalni viri nevarnosti (interni vir ICS)

a. Globalna tveganja

Živimo v času globokih sprememb. Globalna tveganja se uresničujejo na novih in nepričakovanih področjih, njihove posledice pa bodo dosegle ljudi, institucije in gospodarstva

v prihodnosti. Priča smo velikim vplivom podnebnih sprememb, naraščajočim frekvencam in intenzivnostim pomanjkanja vode, poplavam in nevihtam po vsem svetu. Stabilne družbe postajajo vedno bolj razdrobljene, svetovno gospodarstvo je še vedno šibko (World Economic Forum, 2016). Globalna tveganja so razdeljena na 29 področij, kategorizirana so kot družbena, tehnološka, gospodarska, okoljska ali geopolitična tveganja (v 10-letnem časovnem obdobju), vsako izmed njih pa se vrednoti glede na zaznano verjetnost, da se zgodi in možnega vpliva na družbo.

Med pet največjih svetovnih tveganj v naslednjih 10 letih sodijo:

- pomanjkanje vode,
- obsežne ilegalne migracije,
- ekstremno vreme,
- pomanjkanje hrane in
- velika družbena in socialna nestabilnost (World Economic Forum, 2016).

Obstaja še vrsta indikatorjev, ki pomembno vplivajo na globalno varnost, kot so: neuspeh globalnega upravljanja družbe, računalniški kriminal, pomanjkanje naravnih virov, globalni učinki regionalnih nestabilnosti, podnebne spremembe, nedelovanje KI, mednarodna varnost (zlasti nezakonita uporaba drog, trgovina z orožjem in ljudmi, pranje denarja in financiranje terorizma), nepredvidene posledice pravne ureditve, resno neskladje dohodkov, kronična fiskalna neravnovesja, velika sistemska finančna kriza, nevzdržna rast prebivalstva, veliko povečanje cen energentov, hrane ipd. (World Economic Forum, 2016).

Na globalno varnost vplivajo še mobilnost brez meja (ta je že delno omejena), obseg uporabnosti gotovine (za kriminalne namene in pranje denarja, financiranjje terorizma), obvladovanje operativnih tveganj, upoštevanje varnostnih standardov, povečanje števila storilcev kaznivih dejanj, že uspešno izvedeni škodni dogodki in izvajanje preventivnih ukrepov ter postopkov.

Prisotne so tudi spremembe v okolju organiziranega kriminala, ki se kažejo tudi v nejasni razliki med legalnim in ilegalnim, finančni kriminal in ponarejanje plačilnih sredstev, ponarejanje in trgovanje z različnim blagom (droge, ljudje, dobrine, farmacija), energetika (strupeni odpadki, jedrska energija, energetski viri), informacijska varnost (internetne prevare, kraja identitete, socialni inženiring), korupcija in prevare.

b. Izredni dogodki (škodni pojavi) kot glavni vir nevarnosti in kriznih stanj

Izredni dogodki večjega in velikega obsega vnesejo v vsakodnevno relativno mirno obratovanje, delovanje in rutino sistema nemir, preplah, strah, negotovost, tveganje ali celo šok, paniko, grozo in obup. Situacija je lahko še hujša, če sistem ni na nevarnost pripravljen

(Vršec 2008) V tem primeru je nepripravljenost na tveganja velika odgovornost sistema, kajti posledice so lahko usodne za širšo družbeno skupnost in uporabnike.

Med izredne dogodke velikih razsežnosti in posledic uvrščamo:

Naravne nesreče so potres, poplava, zemeljski plaz, snežni plaz, visok sneg, močan veter, toča, žled, pozeba, suša, požar v naravnem okolju, množični pojav nalezljive človeške, živalske ali rastlinske bolezni in druge nesreče, ki jih povzročijo naravne sile. Za naravno nesrečo se štejejo tudi neugodne vremenske razmere po predpisih o kmetijstvu in odpravi posledic naravnih nesreč, ki jih povzročijo žled, pozeba, suša, neurje, toča ali živalske in rastlinske bolezni ter rastlinski škodljivci. Druge nesreče so nesreče v cestnem, železniškem in zračnem prometu, požar, rudniška nesreča, porušitev jezu, nesreče, ki jih povzročijo aktivnosti na morju, jedrska nesreča in druge ekološke ter industrijske nesreče, ki jih povzroči človek s svojo dejavnostjo in ravnanjem, pa tudi vojna, izredno stanje, uporaba orožij ali sredstev za množično uničevanje ter teroristični napadi s klasičnimi sredstvi in druge oblike množičnega nasilja (povzeto po Zakonu o varstvu pred naravnimi in drugimi nesrečami (ZVNDN).

c. Tehnološke in druge nesreče

Izčrpne opredelitve nesreč, ki bi zajele vse njene dele, so razmeroma redke. Nesreča je dogodek ali sosledje dogodkov, ki lahko povzroči poškodbe ali smrt in škodo ter ni bil namerno izzvan (Polič, 1995).

Tehnološke nesreče so navadno posledica izgube nadzora nad tehnološkimi procesi sistema. Raziskave, opisi nesreč in dobra praksa ukrepanja nam omogočajo boljše poznavanje možnih odpovedi varnostnih sistemov in varovanje pred ponovitvami.

Vpletenost posameznika v vzrok nesreče lahko delimo na neizogibne naravne nesreče (zunaj človeškega nadzora), izogibne naravne nesreče (obstaja možnost ublažitve izgub), nesreče, ki jih sproži posameznik (nezanesljivost posameznika povzroči izredni dogodek) in nesreče, ki jih povzroči posameznik (zaradi slabega načrtovanja posameznik ustvari razmere za nesrečo, ki jo sproži narava). Dynes (Polič, 1995:20) je nesreče razdelil na devet kategorij glede na njihove razsežnosti:

- pogostost,
- napovedljivost,
- nadzorljivost,
- vzrok,
- hitrost izbruha (počasni, nagli izbruh),
- trajanje možnega opozarjanja,

- trajanje nesreče,
- obseg vpliva,
- uničevalni potencial.

Načrti za preprečevanje nesreč morajo vsebovati vse elemente varnosti, od varnosti in zdravja pri delu do varovanja materialnih dobrin in informacij, požarne varnosti ter varstva okolja. Pri tem je pomembna vloga posameznih udeležencev (vodstva, varnostnih strokovnjakov, drugih zaposlenih) v takem integriranem sistemu, varnostna kultura zaposlenih in njihov odnos do varnosti in varovanja: osveščenost, znanje, kompetentnost, zaupanje, motivacija, nadzor in odgovornost ter komunikacija med vsemi, ki so vključeni v poslovni proces. Prav komunikacija omogoča izmenjavo znanj in izkušenj ter vodenje dela in nadzor. Potrebujemo integrirani sistem varnosti, ki hkrati zmanjša možnost napake posameznika in zaposlene ozavešča za varno delo in ravnanje.

Sistemi in naprave za preprečevanje nesreč so:

- varnostni sistem ugotavlja vsako odstopanje od normalnih obratovalnih stanj, alarmira operaterje in aktivira vse preostale varnostne sisteme,
- tehnične - varnostne naprave skrbijo za preprečevanje izrednih dogodkov,
- zadrževalni sistem skrbi za zadrževanje nevarnih snovi in za preprečevanje njihovega nekontroliranega uhajanja v okolico,
- sistemi za napajanje v sili zagotavljajo razpoložljivosti električne energije za varnostne sisteme v vseh stanjih sistema.

Ukrepi za primer izrednega dogodka so:

- upoštevanje mednarodnih varnostno - tehničnih predpisov,
- vzdrževanje monitoringa opozorilnih naprav,
- sodelovanje z mednarodnimi institucijami (obveščanje).

Ukrepi za pripravljenost so:

- obveščanje zaposlenih in prebivalstva o nevarnosti izrednega dogodka,
- povečanje zavedanje zaposlenih o nevarnosti,
- ustrezno načrtovanje za primere nesreče v sistemu,
- usposabljanje posebnih enot za reševanje.

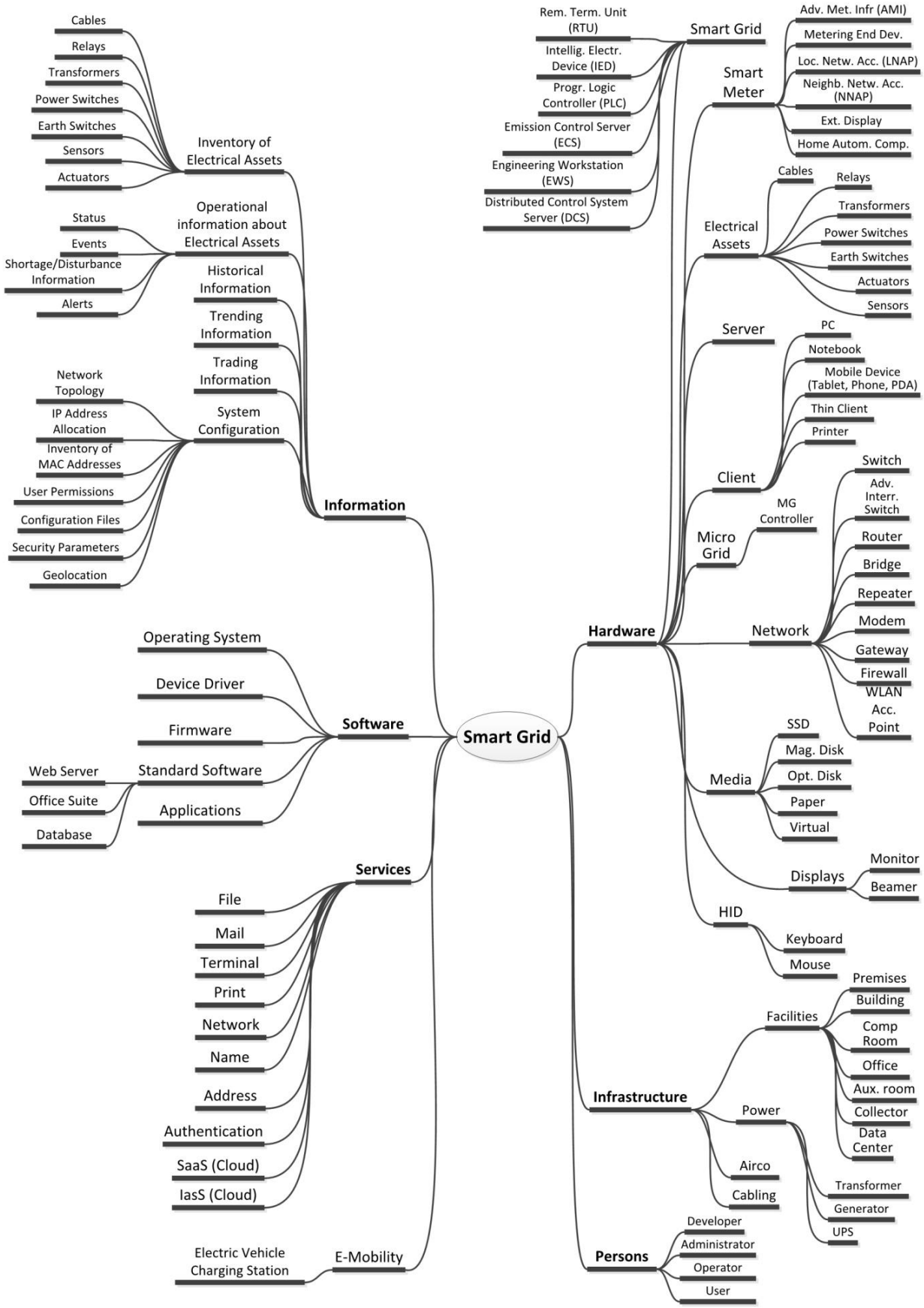
d. Informacijska ogroženost

Dramatično povečanje računalniške medsebojne povezanosti predstavlja znatno tveganje za računalniške sisteme KI, ki podpirajo njeno poslovanje. Prav tako tudi hitrost in dostopnost, ki sicer ustvarja velike koristi podpore poslovanja, če pa ni ustrezno nadzorovana omogoča

storilcem kaznivih dejanj in organizacijam motnje delovanja z oddaljenih lokacij za nevarne ali zlonamerne namene, vključno z goljufijo, krajo ali sabotažo.

V nadaljevanju so prikazane grožnje informacijski varnosti v letu 2015. Nanašajo se na petnajst vrhunskih kibernetskih groženj, ocenjenih med zbiranjem in analiziranjem informacij, in sicer:

- zlonamerna programska oprema (Malware),
- napadi izvršeni na sistem/uporabnika preko spletne strani, katero zlorabijo za prenos zlonamerne programske opreme na ciljan sistem (Web based attacks),
- napadi na spletne aplikacije (Web application attacks),
- mreža okuženih elektronskih naprav, katere komunicirajo s strežnikom ali med sabo čakajoč na ukaz upravljavca mreže, lahko se jih uporablja za dobre ali slabe namene. Mreža je lahko sestavljena iz več 100 ali celo več 1000 »robotov« (Botnets) za onemogočanje storitve, takrat gre za Distributed Denial of Service (DDoS),
- napad, s katerim tarča prejema večjo količino podatkov določenega protokola, s čimer se znatno upočasni ali celo popolnoma zaustavi funkcioniranje storitve (spletne strani ipd.) (Denial of service - DoS),
- fizična škoda / protipravna odtujitev ali kraja / izguba (Physical damage / theft / loss), notranja grožnja bodisi namerna ali nenamerna (Insider threat (malicious, accidental),
- phishing ali spletno ribarjenje je prevara s katero se pridobi občutljive podatke, kar posledično lahko omogoči nepooblaščeni vstop, s pomočjo pošiljanja v ta namen prirejenih e-mail sporočil, kjer se izdajajo za nekoga drugega (oseba, podjetje),
- spam je nadležna, vsiljena, nezaželena ali nenaročena elektronska pošta,
- zbirka kod za avtomatsko skeniranje in zlorabljanje oziroma izkoriščanje ranljivosti sistema (exploit kits),
- incident pri katerem so nepooblaščene osebe prišle do občutljivih, tajnih ali drugače zaščitenih podatkov (data breaches),
- kraja identitete pri čemer nekdo prevzame osebno ime in ostale osebne informacije neke druge osebe (identity theft),
- kadar sistem, ki je bil zasnovan tako, da ščiti podatke pred zunanjimi prisluškovanji izda informacije nepooblaščenim uporabnikom (information leakage),
- kriptovirusi, kateri šifrirajo podatke in ponujajo dešifrator proti plačilu (Ransomware),
- oblike kibernetskega napada pridobimo, kjer se pridobijo tajni in občutljivi podatki ali intelektualna last z namenom pridobitve prednosti ali konkurenčnosti pred drugim podjetjem ali državno ustanovo (cyber espionage) (European Union Agency For Network And Information Security, ENISA, 2015).


Smart Grid
Information
Inventory of Electrical Assets
Cables
Relays
Transformers
Power Switches
Earth Switches
Sensors
Actuators
Operational information about Electrical Assets
Status
Events
Shortage/Disturbance Information
Alerts
Historical Information
Trending Information
Trading Information
System Configuration
Network Topology
IP Address Allocation
Inventory of MAC Addresses
User Permissions
Configuration Files
Security Parameters
Geolocation
Software
Operating System
Device Driver
Firmware
Standard Software
Web Server
Office Suite
Database
Applications
Services
File
Mail
Terminal
Print
Network
Name
Address
Authentication
SaaS (Cloud)
IasS (Cloud)
E-Mobility
Electric Vehicle Charging Station
Hardware
Smart Grid
Rem. Term. Unit (RTU)
Intellig. Electr. Device (IED)
Progr. Logic Controller (PLC)
Emission Control Server (ECS)
Engineering Workstation (EWS)
Distributed Control System Server (DCS)
Smart Meter
Adv. Met. Infr (AMI)
Metering End Dev.
Loc. Netw. Acc. (LNAP)
Neighb. Netw. Acc. (NNAP)
Ext. Display
Home Autom. Comp.
Electrical Assets
Cables
Relays
Transformers
Power Switches
Earth Switches
Actuators
Sensors
Server
Client
PC
Notebook
Mobile Device (Tablet, Phone, PDA)
Thin Client
Printer
Micro Grid
MG Controller
Network
Switch
Adv. Interr. Switch
Router
Bridge
Repeater
Modem
Gateway
Firewall
WLAN Acc. Point
Media
SSD
Mag. Disk
Opt. Disk
Paper
Virtual
Displays
Monitor
Beamer
HID
Keyboard
Mouse
Infrastructure
Facilities
Premises
Building
Comp Room
Office
Aux. room
Collector
Data Center
Power
Transformer
Generator
UPS
Airco
Cabling
Persons
Developer
Administrator
Operator
User

Slika 37: Ponazoritev tveganj povezanih z delovanjem informacijske tehnologije v KI (ENISA)[14]

Izhajajoč iz proučevanja delovanja in razvoja KI se kaže, da je ogroženost informacij in elektronskih komunikacij v vseh sektorjih precej visoka. Z vidika notranje ogroženosti je pomembno zavedanje o možnostih odtekanja zaupnih podatkov, informacij in/ali določenih dokumentov v klasični ali elektronski obliki, ki lahko poteka tudi z neposrednim verbalnim komuniciranjem, skozi računalniško, telefonsko, elektronsko, osebno in drugo komuniciranje. Iznos zaupnih gradiv iz sistema so dejanja, ki se lahko dogodijo ob vprašljivi organizacijski in varnostni kulturi določenega dela zaposlenih, nedorečeni poslovni etiki managementa, še zlasti pa takrat, ko taka dejanja zaposlenega ali organizirane skupine niso pod internim (in eksternim) nadzorom. Zaradi tega je poznavanje informacijske ogroženosti, informacijskih tveganj, upravljanje varovanja informacij, zaščite osebnih in tajnih podatkov ter poslovnih skrivnosti prioriteta in stalna aktivnost nosilcev sektorjev in upravljavcev KI. Iz raziskave o varovanju informacij v slovenskih gospodarskih družbah, med katerimi je bilo tudi nekaj upravljavcev KI, je razvidno, da varovanje informacij (v času raziskave) še ni bilo na dovolj visoki ravni. Ugotovitve iz raziskave (Erjavec/Vršec, 2010) so naslednje:

- upravljanje z informacijsko varnostjo po standardu ISO/IEC 27001 (ali ISO 17799) ima (le) 10 % organizacij, kar kaže na to, da je informacijska varnost podhranjena,
- pogodbeno urejeno upravljanje informacij ima urejeno 24% organizacij,
- 75% anketiranih gospodarskih družb je zmanjšalo vložke v informacijsko varnost,
- brez obvladovanja tveganj je 44% organizacij,
- pooblaščeni revizor informacijskih sistemov deluje v 24 % organizacij, kar ni malo, če upoštevamo, da ima samo 10% organizacij urejeno varovanje informacij po standardu ISO/IEC 27001,
- spodbuden podatek iz raziskave je, da kar 75% organizacij navaja, da so lastniki, vodstvo in nadzorniki pravočasno informirani s problematiko, ogroženostjo in potrebami s posodabljanjem omrežne in računalniške varnosti.

[14] Smart Grid Threat Landscape and Good Practice Guide, 2013, https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide, accessed 15 August 2017, p. 13.

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	⊃	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	⊃	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	⊃	11. Data breaches	⊃	↓
12. Information leakage	↑	12. Identity theft	⊃	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Slika 38: Pregled in primerjava najbolj izpostavljenih groženj na področju kibernetske varnosti za leti 2015 and 2014[15]

Problematika ogroženosti zaradi odtekanja (iznosa) zaupnih podatkov in zaupnih gradiv se v svetu vohunstva in v sklopu korporacijskih varnostnih politik in varnostnih strategij obravnava skupaj z informacijsko, teroristično, vohunsko, sabotažno in konkurenčno ogroženostjo. Navedene ogroženosti in varnostna tveganja imajo veliko skupnega. Glavne skupne točke so: stroga tajnost, prefinjena kraja poslovnih skrivnosti (business intelligence), težavno odkrivanje, preiskovanje in dokazovanje, velike premoženjske koristi za vpletene, velike poslovne, finančne in etične škode sistemu ipd. S teh zornih kotov je treba morebitno problematiko nepooblaščenega odtekanja zaupnih gradiv obravnavati tudi v okviru zagotavljanja visoke stopnje računalniške in informacijske varnosti.

Problematika odtekanja zaupnih podatkov in zaupnih gradiv je dobro znana tako v tujini kot tudi pri nas. V Sloveniji se v nekaterih delih sistema dogajajo poslovno in varnostno zanimive

[15] ENISA Threat Landscape 2015, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape, p. 7, accessed 01. July 2017

zadeve, ki pa širši javnosti niso dovolj znane. Prihaja do iznosa določene zaupne in druge poslovne dokumentacije, ko gre npr. za menjave vodstva, prestrukturiranje lastništva, razne afere, javne razpise, kazniva ravnanja, za t. i. sovražne (ali pa tudi prijazne) prevzeme, za namerno oškodovanje podjetja ipd.

Ko obravnavamo informacijsko ogroženost je pomembno:

- jasno je treba opredeliti kaj vse sodi pod zaupnost (tajnost) gradiv, prav tako je treba opredeliti ukrepe, postopke in sledljivost poslovne dokumentacije zaupne narave,
- vprašati se je treba ali je varovanje osebnih in tajnih podatkov, informacij in poslovnih skrivnosti usklajeno v notranjih aktih, to je v Pravilniku o varovanju poslovnih skrivnosti, Pravilniku o varstvu osebnih podatkov in v Pravilniku o varovanju tajnih podatkov. Pomembno je tudi vprašanje ali so določeni zaposleni za zaščito, urejanje in vodenje sistema varovanja podatkov, informacij ter dokumentov zaupne narave,
- vse bolj se čuti potreba po sodobnem urejanju in varovanju arhivov – problem ustreznosti prostorov (vlaga, temperatura, poplava, požarna ogroženost, ustrezni regali, protipožarne in protivlomne omare za zaupni del arhivskega gradiva, nadzor pristopa ipd.), nekateri deli arhivov so zaradi prostorske stiske nakopičeni in nepregledni, varovanje je šibko in ogroženost arhivov ter arhivskih prostorov je pretirano visoka,
- v prostorih (pisarnah) s poslovno dokumentacijo je potrebno vzpostaviti ustrezni varnostni režim, tako glede ravnanj z osebnim računalnikom in ravnanj s poslovno dokumentacijo,
- nad iznašanjem poslovne dokumentacije z delovnih mest domov ali na druge lokacije, bodisi s shranjevanjem podatkov v oblaku, s prenosnimi računalniki in prenosnimi mediji (USB ključi, zgoščenke ipd.) ali v pisani obliki (dokumenti, gradiva), se kaže potreba po sistemski transparentnosti, da se zagotovi varnost poslovanja in odgovornost za napake,
- računalniško omrežje in poslovni informacijski sistem proučujejo in analizirajo informatiki ter računalničarji, da bi z gotovostjo prišli do realne ocene informacijske ogroženosti in informacijskih tveganj,
- vzpostaviti je treba projekt ravnanja s človeškimi viri, ki bi identificiral stopnjo organizacijske in varnostne kulture zaposlenih, pogodbenih podizvajalcev, poslovnih partnerjev in poslovno etiko vodstva, kajti to so glavni preventivni dejavniki v sistemu varovanja informacij,
- informacijska ogroženost je veliko bolj obvladljiva, če se v sistem varovanja informacij uvedejo informacijski standardi po ISO/IEC 27000. Glede na to, da mora biti zagotovljeno neprekinjeno delovanje in poslovanje sektorjev sistema je ob

navedenem standardu potrebno uvesti tudi standard neprekinjenega poslovanja ISO 22301 ter standard obvladovanja tveganj ISO 31000:2018.

Na navedene ugotovitve je treba biti pozoren pri oblikovanju in implementaciji Politike varovanja informacij in poslovnih skrivnosti ter pri vzpostavljanju integralnega varnostnega sistema. Sem sodijo tudi vprašanja o uvedbi primerjalne analize »benchmarkinga« in poizvedovanje o poslovnih informacijah »business intelligence«.

»Benchmarking« je zahtevna naloga za vodstvo, ki zahteva visoko stopnjo načrtnosti, pa tudi angažiranje zunanjega strokovnjaka - svetovalca. To pomeni, da se »bencmarking« poslovnega orodja uspešno loti vodstvo podjetja, ki ima pravo razvojno strategijo, ki zna razumno tvegati in je pripravljeno za profesionalni spopad s konkurenti. Gre za naslednje aktivnosti »benchmarkinga«:

- ocenitev / presoja tistih podjetij na slovenskem trgu, ki sodijo v razred najboljših in hkrati ugotavljanje njihovih konkurenčnih prednosti in slabosti v vodenju, organiziranosti, kadrih, ceni, kakovosti in tržnih potezah,
- načrtno spremljanje aktivnosti nekaterih tujih podjetij, ki bi utegnila kupiti določen delež slovenskih podjetij kot kapitalsko naložbo,
- iskanje drugih podjetij, ki so pripravljena poslovno, kapitalsko in logistično sodelovati v »benchmarkingu«, kar dviga konkurenčno sposobnost obeh sodelujočih partnerjev.

Še bolj zahtevna aktivnost v sistemu je »business intelligence« (poslovna inteligenca, poslovno poizvedovanje ipd.). Poslovno poizvedovanje pomaga sistemu pridobiti bolj poglobljena znanja o zadevah, ki vplivajo na njihovo poslovanje, kot so različni kazalci prodaje, proizvodnje, internega poslovanja ipd., kar omogoča boljše poslovno odločanje. Prednost tovrstnega poslovnega orodja je, da uporablja tako strukturirane kot nestrukturirane vire podatkov oziroma informacij. Viri za tovrstno iskanje podatkov in informacij so lahko obstoječa podatkovna skladišča, transakcijski sistemi, notranji in zunanji portali, informacijski sistemi dobaviteljev, sistemi za upravljanje z dokumenti, mediji, knjige, konkurenti, internet, druge javno dostopne baze podatkov ipd. Pomembne so tudi neformalne poti do kupcev, dobaviteljev, poslovnih partnerjev. Poslovno poizvedovanje se uporablja na različnih področjih, z njimi lahko analiziramo uspešnost projektov, poslovne aktivnosti, kot je poslovno planiranje, nabavne verige ipd. Dobri sistemi poizvedovanja omogočajo spremljanje poslovanja, primerjavo planov z realizacijo, opozarjajo na odmike od planiranih vrednosti in iskanje vzrokov od teh odmikov. To poslovno orodje je namenjeno tudi analizi dolgoročnih trendov, medletni primerjavi načrtov in njihove realizacije na vseh poslovnih področjih. Nadalje, to učinkovito poslovno orodje združuje veščine, znanja, tehnologijo, aplikacije, kakovost in varnostne vidike za boljše razumevanje trga. Gre za usmerjenost v raziskavo služb za prodajo, marketing, oddelke za tržne raziskave, zunanje svetovalce, informacije o

poslovnem okolju, konkurentih, priložnostih in tveganjih. »Business intelligence« je orodje vodstva, s katerim pridobiva ključne informacije, potrebne za odločanje. Je torej orodje »z očmi in ušesi«, ki omogoča zbiranje, analiziranje in uporabo informacij na legalen in etično nesporen način. Praksa tovrstnega poseganja v druge sisteme pa lahko prinaša tudi sporne rešitve in posege v poslovanje konkurentov na strateški in operativni ravni.

e. Zdravstvene epidemije

Med možnimi zdravstvenemi epidemijami posebej izstopa pandemija kot vir nevarnosti. Pandemija je pojav posamezne nalezljive bolezni, ki se v obliki epidemij lahko pojavlja v več regijah, državah in celinah. Pandemija gripe običajno nastane, ko se pojavi nov virus gripe, ki je pomembno drugačen od virusov, ki so krožili do tedaj in je sposoben:

- okužiti zaposlene,
- se širiti od posameznika na posameznika,
- povzročiti bolezen pri večini okuženih in
- hitrega širjenja med zaposlenimi zaradi nizke ali neobstoječe odpornosti.

Virus pandemične gripe se širi na enak način kot virus običajne sezonske gripe, razlika je v tem, da ne obstaja predhodna imunost zaposlenih, zato oboli večji odstotek v populaciji in tudi klinična slika je običajno težja.

Strokovnjaki napovedujejo verjetnost nove pandemije v bližnji prihodnosti (Načrt pripravljenosti na pandemijo gripe na področju zdravstva, 2006).

Čeprav obstaja glede bodoče pandemije veliko neznank (čas, obseg in resnost pandemije), pa je mogoče predvideti, da bi se bolezen zelo hitro razširila po svetu. Ob današnjem hitrem in obsežnem mednarodnem letalskem prometu pa se domneva, da bo pandemični virus obkrožil svet v manj kot 3 mesecih.

Pandemija gripe za razliko od epidemije običajne gripe ne predstavlja samo pomembnega javno zdravstvenega problema, ampak širši družbeni problem, saj lahko zboli od 25 - 45% posameznikov. Za razliko od običajne sezonske gripe ni mogoče s tako veliko stopnjo verjetnosti napovedati, katere starostne skupine bodo bolj prizadete.

Pandemija gripe bo povzročila še večjo odsotnost z dela kot običajna sezonska gripa, kar bo imelo velik vpliv na delovanje sistema. V času pandemije gripe bi se dramatično povečala bolniška odsotnost, obisk v ambulantah, zaradi težje klinične slike pa bo povečana tudi potreba po sprejemu v bolnišnice. Delovanje sistema bo močno oteženo, prav tako tudi celotnega zdravstvenega sistema, ker se za razliko od epidemije običajne gripe v primeru pandemije gripe pričakuje, da bo obolelo tudi veliko število zdravstvenih delavcev. Ocenjuje se, da bi bila smrtnost zaradi pandemije gripe bistveno večja kot pri običajni sezonski gripi.

Za razliko od običajne sezonske gripe v boju proti pandemični gripi, vsaj na začetku, ni na razpolago ustreznega cepiva.

Pandemija gripe bi nedvomno povzročila izredni dogodek v sistemu, zato je pravočasno in ustrezno načrtovanje ključno za učinkovitost ukrepanja. Pričakujemo, da bo delovanje vseh služb lažje, če bodo zaposleni v naprej vedeli, kaj lahko pričakujejo in kako morajo ukrepati.

Načrtovanje poteka po posameznih fazah pandemije, ki jih je sprejela Svetovna zdravstvena organizacija (v nadaljevanju: SZO; ang. WHO - World Health Organization). Faze so opredeljene po treh obdobjih in sicer:

- interpandemično obdobje,
- obdobje povečane budnosti,
- obdobje pandemije.

Cilji načrta pripravljenosti sistema na pandemijo gripe so naslednji:

- zagotoviti enotno razumevanje izhodišč za načrtovanje,
- obveznost prijave nalezljive bolezni,
- obvezna osamitev, prevoz in obvezno zdravljenje zaposlenega,
- vzpostaviti sistem kriznega upravljanja,
- sprejeti kadrovske ukrepe za nadomeščanje obolelih,
- opredeliti in razmejiti vlogo in pristojnosti služb sistema, posameznih organov in institucij,
- posebni ukrepi: delovna in materialna dolžnost zaposlenih, prepoved potovanj v državo, v kateri obstaja možnost okužbe z nevarno nalezljivo boleznijo in za prihod iz teh držav; omejitev gibanja na okuženih ali neposredno ogroženih območjih; prepoved zbiranja zaposlenih na skupnih mestih ipd.,
- zagotoviti kontinuirano ocenjevanje tveganja,
- zagotoviti pravočasno in učinkovito izvajanje javnozdravstvenih preventivnih ukrepov,
- vzpostaviti učinkovit sistem komuniciranja in informiranja,
- analizirati ustreznost pravnih podlag za ukrepanje,
- natančno načrtovati ukrepe v vsaki od šestih faz, kot jih je definirala SZO na petih področjih (načrtovanje in koordinacija, spremljanje in ocena tveganja, preprečevanje širjenja in omejevanje, zdravstveni sistem in obveščanje) z odgovornimi nosilci in ustreznimi prilogami.

Zdravstvene grožnje se najbolj nanašajo na sektor zdravstva, v katerem gre – poleg poslovnih tveganj - v veliki meri tudi za upravljanje s kliničnimi tveganji in tveganji pri uporabi zdravstvene tehnologije ter tveganji pri uporabi zdravil. Pri ocenjevanju tveganj v drugih

sektorjih KI pa je treba biti pozoren tudi na zadravstvena tveganja tako z vidika delovnih pogojev, delovnih odnosov, zaščitne opreme v delovnih in proivodnih procesih, kot tudi z vidika uporabe nevarnih snovi in kemikalij.

f. Viri varnostnih groženj

Z vidika individualnih, nacionalnih in mednarodnih prizadevanj za varnost se vse bolj kaže potreba po »oblikovanju in razvoju učinkovitih varnostnih ukrepov na vseh ravneh, z uporabo najboljših znanstvenih in strokovnih metod, zaradi objektivnega spoznavanja vseh virov s ciljem pravočasnega vzpostavljanja tistih ukrepov, ki imajo odločilno vlogo v razvijanju želenih politično - pravnih, varnostnih in drugih odnosov v družbi« (Masleša; v Umek, 2009:32). Po slovenskih javnomnenjskih raziskavah (npr. FDV v letih 2008-2016) so viri ogrožanja globalne in nacionalne varnosti naslednji: širjenje orožja za množično uničevanje, onesnaževanje okolja, mamila, organizirani kriminal, naravne in tehnološke nesreče in terorizem. Ti viri in visoka varnostna tveganja so primarni zato, ker imajo močna ozadja; tako v kapitalu, organiziranosti, vztrajnosti, pa tudi v nacionalnih in verskih prepričanjih. Zato je v borbi zoper terorizem in organizirani kriminal prvenstveno obvladovanje ozadij. Za obvladovanje ozadij pa so potrebne učinkovite obveščevalne in protiobveščevalne institucije ter urejen varnostni informacijsko - komunikacijski sistem, ki poleg dobre organizacije in usposobljenosti varnostnega osebja uporablja tudi visoke tehnologije na zemlji in v atmosferi (satelitska navigacija: ameriški GPS, evropski Galileo, ruski Glonass, kitajski Kompas). Približno enako velja tudi za druge tipe groženj naravne, okoljske, socialne, gospodarske, finančne, energetske, vohunske, informacijske in zdravstvene narave. Potreba po še bolj natančnem spoznavanju ranljivosti državnih institucij, gospodarstva, industrije, računalniških omrežij, infrastrukture, turizma, prometa in drugih področij je še bolj izrazita. Ali drugače povedano: obstaja potreba po celoviti analizi in oceni ogroženosti in varnostnih tveganjih – od spoznanj o naravni ogroženosti, vse do - denimo - konkurenčne ogroženosti gospodarstva. Pri naravni ogroženosti izstopajo potresna ogroženost, ogroženost podtalnice, poplavna ogroženost, požara in ogroženost od slabo urejenega sistema ravnanja s komunalnimi in industrijskimi odpadki.

Pri kriminalni ogroženosti na mednarodni (globalni) ravni pa vse bolj izstopa organizirani kriminal v mnogih pojavnih oblikah širokih razsežnosti, ki jih lahko označimo kot transnacionalne grožnje. Razvite oblike organiziranega kriminala so zlasti: ilegalna trgovina z orožjem, prodaja in razpečavanje mamil, trgovina z ukradenimi osebnimi avtomobili, trgovanje z ljudmi (»belim blagom«), ilegalne migracije, ponarejanje in pranje denarja, korupcija, izsiljevanja, ugrabitve, atentati ipd. Organizirani kriminal se vse bolj globalizira in s tem prehaja v »univerzalni kriminal«. Poleg klasičnih in sodobnih oblik organiziranega kriminala se vse bolj razširjajo »hekerski«, »krekerski« in vohunski vdori v računalniška

omrežja, uničevanje računalniških programov in informacijskih sistemov z »virusi«, »črvi«, »trojanskimi konji« in drugimi oblikami organiziranih ali posamičnih napadov. Tudi Slovenija, kot razvita informacijska družba, postaja vse bolj ranljiva na področju informacijske varnosti. Zaradi tega je priporočljivo, da sistemi, ki imajo kompleksna računalniška omrežja, z občutljivimi poslovnimi informacijskimi sistemi, ki so zanimivi za konkurenco in vohunsko delovanje, odločajo o uvedbi zaščitnih standardov – npr. uvedbo standardov varovanja informacij ISO/IEC 27000.

Ogroženost slovenskega prostora od terorizma je posebno varnostno vprašanje, ki bo najbrž še dolgo zaposlovalo varnostno - obveščevalne institucije. Na nekaj realnosti, zlasti pa potencialnosti in prikritosti terorističnih aktivnosti na slovenskih tleh, je v prihodnje treba računati, kajti terorizem – tako kot organizirani kriminal – ne pozna prostorskih meja, prav tako pa ne pozna omejitev v uporabi sredstev. Pomembna je tudi motivacija za delovanje teroristov, ki skrbno in načrtno izbirajo atraktivne lokacije.

Po nekaterih ocenah se število varnostnih tveganj in groženj povečuje, kar zapleta iskanje mehanizmov za njihovo omejevanje, nadzorovanje in odpravljanje. Poleg tega je ena izmed značilnosti sodobnih varnostnih groženj tudi njihova velika povezanost in medsebojna prepletenost z organiziranim kriminalom, s čimer se finančno napajajo. Terorizem je zaradi tega tesno povezan s pranjem denarja, tihotapljenjem drog, orožja in belega blaga. Govorimo lahko o t.i. »vsestranski grožnji«, ki terja prav tako vsestranske preventivne in represivne ukrepe; prepletene v tem smislu, da je učinkovitost zoperstavljanja virom ogrožanja – na globalni ravni - odvisna od stopnje sodelovanja med državami. Upravljanje oziroma obvladovanje tveganj - Risk Management (Berk, 2005), še posebej varnostnih tveganj (Vršec 1993, 2003, 2007, Biringer 2007), ki izhajajo iz narave, terorističnih in kriminalnih napadov, je tako odvisno od uspešnosti izvajanja univerzalne (ožje evropske) varnostne politike ter varnostnih politik in varnostnih strategij posameznih držav.

V prihodnje se bo treba vse bolj spopadati z najhujšimi oblikami tveganj nastanka »kriminalno - terorističnih« dejanj, ki se nanašajo na atentate, nastavljanje eksploziva (bombne grožnje), trgovanje in zlorabo biološkega, kemičnega in nuklearnega orožja ter na trgovanje s človeškimi organi. To so nevojaške grožnje najvišjega ranga, ki ne smejo uiti nadzoru kompetentnih institucij.

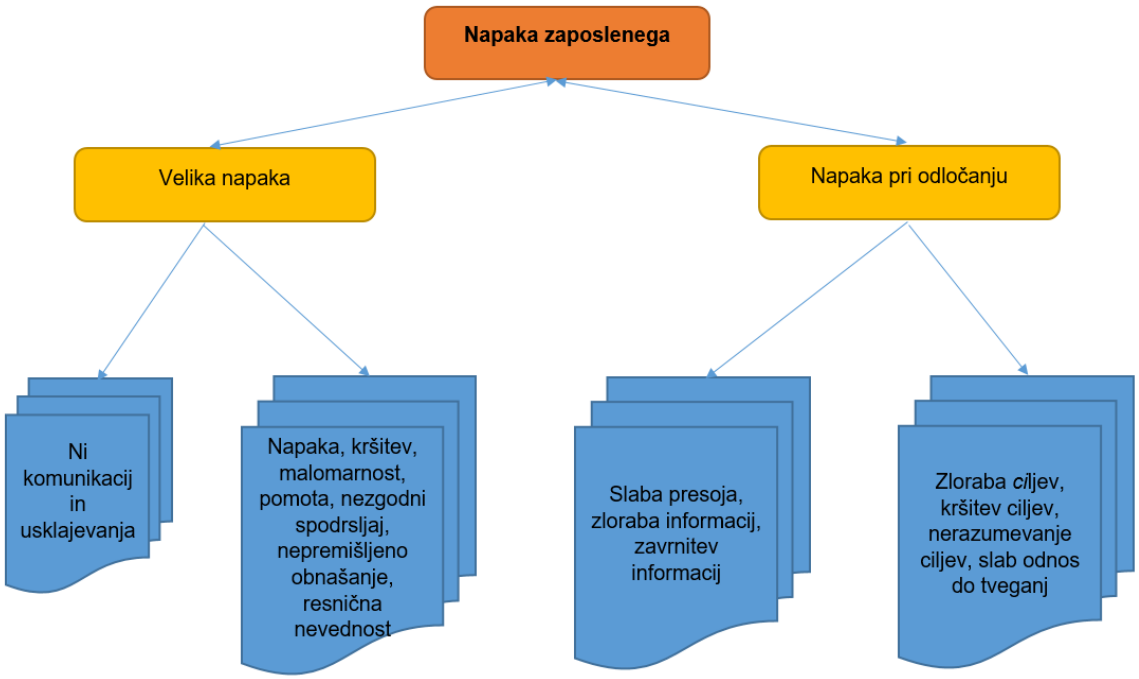
g. Tveganje človeškega dejavnika

Obravnavanje zanesljivosti zaposlenega pri delovanju sistema ni novo, v zadnjem času pa se je zaradi terorističnih napadov, groženj in izrednih dogodkov zanimanje za to področje močno povečalo.

Vpliv zaposlenega na delovanje sistema je eden najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanj stalno nevarnost, ki je ne smemo podcenjevati (Bertoncelj, 2012, 2017). Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile tehnološke in fizične sestavine sistema varnejše, po drugi strani pa kako obravnavati zaposlenega pri upravljanju teh kompleksnih sistemov, saj ta postaja vse pomembnejši referent za njeno zanesljivo delovanje. Zanesljivost zaposlenega v izrednih dogodkih je najbolj odvisna od stopnje njegove motiviranosti, usposobljenosti in pripadnosti sistemu. Samovarovalne dejavnosti in preprečevanje možnosti za izredne dogodke so pretežno prostovoljna dejanja, pri katerih sta najpomembnejša pojma pripravljenost in volja nekaj koristnega delati za sistem.

Zaposleni z vsemi svojimi pristojnostmi, potrebami, motivi, stališči in notranjimi osebnostnimi dejavniki pomeni pomemben ter kritični člen sistema, ker vstopa v interakcije z njim, zaznava in nadzira nevarnosti ter dela napake in jih popravlja. Zlonamerna napaka je odločitev zaposlenega in je iz delovanja sistema ne moremo izločiti, lahko pa s preventivnimi ukrepi in postopki zmanjšamo njen škodljivi učinek. Vloga zaposlenega je negativna, kadar povzroča naključne ali zlonamerne napake, in pozitivna, kadar jih odpravlja (Polič idr., 1995).

Neustrezne dejavnosti zaposlenega lahko delimo na namerne ali nenamerne oziroma naključne, ki se zgodijo zaradi napak ob neustrezni odločitvi, strokovnem neznanju ali napačni zaznavi ali zaradi kršitev (malomarnost). Možne napake zaposlenega so prikazane na sliki 39.



Slika 39: Možne napake zaposlenega (interni vir ICS)

Poleg navedenega so vzroki za napako zaposlenega brez posebnega vrstnega reda z vidika pomembnosti še:

- pomanjkljiva zakonska ureditev sistema,
- ocena tveganj ne obravnava resničnega stanja,
- neustrezno organiziranje in vodenje dela,
- slab vodstveni nadzor,
- neupoštevanje zakonov in predpisov,
- neustrezna navodila,
- nejasne pristojnosti in odgovornosti,
- pomanjkljivo usklajevanje dela,
- premajhna usposobljenost zaposlenih,
- slaba organizacijska in varnostna kultura,
- nelojalnost do delodajalca,
- neetično delo,
- pomanjkljiv varnostni sistem,
- neupoštevanje zahtev notranje in zunanje revizije,
- navzkrižje interesov,
- neustrezni odzivi na prejšnje neobičajne razmere,
- nasilje na delovnem mestu,
- neučinkovito usposabljanje in komuniciranje,
- neustrezni dejavniki dela (npr nelogično oblikovanje strojev, opreme in instrumentov, stalne motnje in napake, slabo vzdrževana oprema, visoka delovna obremenitev, neustrezne delovne razmere, slabo upravljanje zdravja in varnosti pri delu ipd.).

Vzroki za napako zaposlenega so tudi:

- zahteve po delovni zmogljivosti, ki presega njegove zmožnosti,
- težke delovne naloge,
- nevarne ali neprijetne naloge,
- ponavljajoče se ali dolgočasne naloge,
- utrujenost,
- stres,
- delovna izgorelost,
- mobing,
- spolno nasilje,
- pomanjkanje spanja,
- poškodbe,
- zdravstvene težave ipd.

Posledice izrednih dogodkov zaradi izgube življenja zaposlenega ali strank oziroma ugleda in zaupanja javnosti, nedelovanja sistema ali škode na premoženju so za družbo in sistem drage in jih je težko vnaprej predvideti ter materialno oceniti.

Analiza različnih metod raziskovanja zanesljivosti zaposlenega (Bell idr., 2009) se do zdaj nanaša na kar 39 pristopov. Med bolj uporabljenimi metodami je tehnika za napovedovanje napake zaposlenega, ki je povezana s programom za vrednotenje nesreč.

Sprejemanje odločitev je eden temeljnih kognitivnih procesov zaposlenega. Najboljše mogoče odločanje otežuje pretirana prepričanost o pravilnosti svoje sodbe. Zaposleni preveč zaupa svojim, tudi napačnim predpostavkam in sodbam. Podlaga za to je verjetno neobčutljivost za pomanjkljivost domnev in predpostavk, na katerih temeljijo njegove ocene. Najbrž noben dejavnik slabe odločitve ni bolj odločujoč kot pretirana samozavest.

Na sprejemanje odločitve vpliva več dejavnikov, in sicer strokovno znanje in izkušnje (Juliusson idr., 2005), kognitivne pristranskosti (Stanovich idr., 2008), starost in individualne razlike (Bruin idr., 2007) ter samozaupanje (Acevedo idr., 2004).

Uspešnost ali neuspešnost spoprijemanja z viri nevarnosti je tesno povezana z osebnostnimi lastnostmi zaposlenega, ki se nanaša na njegovo strokovno znanje, realno oceno izrednih dogodkov, zavestnim razčlenjevanjem razmer, osebni trdnosti, vključno z zaupanjem v svoje sposobnosti. Pomemben je tudi aktiven odnos do stvarnosti, namesto togosti in bega iz stvarnosti, prilagodljivo iskanje rešitev, konstruktivno sodelovanje z drugimi, namesto pasivnega pričakovanja pomoči ter sprejemanje in prenašanje čustvene obremenitve, namesto neorganiziranosti in panike. Na splošno velja, da se bo zaposleni toliko učinkoviteje spoprijel z izrednim dogodkom in njegovimi posledicami, kolikor bolj bo nanje pripravljen.

V nadaljevanju bodo predstavljeni nekateri najpogostejši notranji izredni dogodki, torej tisti, ki se lahko zgodijo v sistemu in izredni dogodki, ki od zunaj vplivajo na sistem.

IZREDNI DOGODKI

Obvladovanje izrednih dogodkov (naravnih in drugih nesreč, požarov, kriminalnih dejanj, terorističn napadov, afer in drugih izrednih dogodkov), ki jih členimo na notranje in zunanje, je ena od glavnih kategorij obvladovanja ranljivosti, ogrožernosti ter varnostnih in drugih tveganj, v državi, gospodarstvu, civilni družbi in prebivalstvu (tudi pri posamezniku). Najprej gre za vzpostavitev sistema učinkovite preventive, ki preprečuje in omejuje nastanek teh dogodkov, ter njihovih posledic škod in izgub (Loss Prevention), po tem pa gre še za učinkovito (hitro in strokovno) odzivanje na nastale izredne dogodke. Tako je zagotavljanje neprekinjenega delovanja usodno odvisno od učinkovitosti obvladovanja izrednih dogodkov, ki lahko upočasnijo ali celo prekinejo izvajanje določenih proizvodnih, poslovnih, logističnih

informacijsko-komunikacijskih in drugih procesov. Poleg tega je obvladovanje izrednih dogodkov ključna paradigma upravljanja tveganj in kriznega vodenja.

a. Notranji izredni dogodkI

Splošna spoznanja o izrednih dogodkih (škodnih pojavih) v sistemu še zdaleč ne povedo vsega, kar se škodljivega dogaja v sistemu in z njim povezanimi gospodarskimi subjekti. Del tega, kar je v kateremkoli sistemu škodljivo, ima kazenskopravni značaj (kazniva dejanja in prekrški), pretežni del škodnih pojavov pa je treba obravnavati z ekonomsko - varnostnega vidika in z vidika poslovne (ne)uspešnosti ter kulture.

Seštevek vseh škod in izgub v sistemu je lahko resno svarilo in opozorilo. Sistem bi moral imeti natančno evidenco o možnih in nastalih škodnih pojavih, ki bi bili finančno, poslovno in moralno ovrednoteni. Na ta način bi sistem imel pregled nad škodami in izgubami ter osnovo za preventivno in kurativno ukrepanje. V vsakem sistemu je škodljivo vse tisto, kar prinaša finančno, poslovno in moralno škodo, kar slabi poslovne rezultate (izide), povzroča entropijo in zmanjšuje ugled ter zaupanje javnosti v sistem. Med notranje škodne pojave lahko uvrščamo tudi: namerno kvarjenje kvalitete izdelave in namerno upočasnitev dela sistema, lažno prikazovanje nesreče pri delu, delo pod vplivom alkohola ali mamil, opravljanje osebnih opravil med delovnim časom, pomoč pri krajah (tatvinah), malomarno ravnanje in poškodovanje inventarja, nenamenska uporaba službenih vozil, orodij, naprav, strojev v privatne namene, namerno poškodovanje blaga zaradi nakupa po nižji ceni, sprejemanje podkupnin in druga neetična dejanja, lažne bolniške odsotnosti, izplačevanje nadurnega dela, ki ga ni bilo, podaljšane odmore med delovnim časom, zamude na delo, potrjevanje časovne kartice za sodelavca, predčasno zapuščanje dela, uporabo kopirnega stroja in potrošnega materiala za privatne potrebe, privatne telefonske pogovore ipd. Takšni vsakodnevni škodni pojavi na prvi pogled ne predstavljajo veliko škodo, so pa odraz kulture zaposlenih in neke vrste podlaga za nastanek finančnih, poslovno in moralno še težjih škodnih dogodkov in pojavov. Če so organizacijska in varnostna kultura zaposlenih ter poslovna etika managementa nizke, je možno take pojave preprečit z učinkovitejšim vodstvenim nadzorom, notranjo kontrolo in preprečevalnimi ukrepi ter postopki. Glavno vlogo pri tem morajo prevzeti vodstva v posameznih delih sistema, kadrovska služba in služba Notranje kontrole (revizije). S tem bi zmanjšali priložnost za notranje škodne pojave, ki povzročajo znatne (večje) škode in izgube. »Znatne škode in izgube v sistemu povzročajo naslednji notranji škodni pojav« (Vršec 1993, 2003, 2008):

- neustrezne poslovne odločitve in uporaba kapitala,
- nekontrolirana prodaja znanja in izkušenj podjetja (tudi v zvezi s konkurenčno klavzulo),

- investiranje v nedonosne projekte in posle, upoštevajoč zakonitost poslovanja,
- izdaja ali zloraba poslovne skrivnosti,
- neurejeno varovanje poslovne skrivnosti in slab pregled nad izvirnim znanjem ter izkušnjami sistema,
- prikrivanje slabih rezultatov poslovanja,
- računalniški kriminal (izdaja šifer, zloraba programov, prodaja izvirnih računalniških aplikacij, reprogramiranje z namenom zlorabe ipd.),
- goljufije (preslepitve, ponarejanje, zavajanja, sleparjenje ipd.),
- tatvina dragocenega materiala in orodij ter denarja,
- poškodovanje alarmnega sistema z določenim namenom,
- sabotaže (namerno poškodovanje stroja, naprave, procesa, postopka),
- eksplozije,
- požari, požigi in samovžigi,
- delovne nesreče in prometne nezgode,
- stavke in druge vrste socialnih nemirov zaposlenih,
- zastrupitve,
- poklicne bolezni,
- zdravstvene epidemije, ki se izražajo tudi v zdravstvenih težavah zaposlenih,
- razlitja nevarnih snovi (malomarnost, nesreča ali kaznivo ravnanje, izven nadzora).

Vsak sistem na podlagi ocene ogroženosti oziroma varnostne ocene ali varnostne študije ugotovi, kateri škodni pojavi so po obsegu in strukturi škod primarnega in kateri sekundarnega pomena. To je izhodišče za varnostno politiko, obvladovanje tveganj in vložke v varnostne ukrepe.

b. Izredni dogodki zunanjega izvora

Sistem ni imun pred zunanjimi izrednimi dogodki, ki izvirajo iz zunanjih neugodnih vplivov in spleta okoliščin. Zunanjim izrednim dogodkom se sistem težje upira kot notranjim, ker so nosilci teh izven sistema. Nekateri zunanji izredni dogodki lahko sistemu povzročijo veliko trenutno in dolgoročno škodo, motnje v poslovnih procesih, izgubo zaupanja javnosti, uporabnikov storitev, lastnikov, zaupanja borze, zastoj v razvoju ali celo postopek ukinitve. Zato bi bila strateška napaka, če bi vodstva in strokovnjaki za varnost pri oblikovanju varnostne politike in varnostnega koncepta sistema prezrli zunanje izredne dogodke.

Pregled možnih zunanjih izrednih dogodkov je naslednji (Vršec 1993,2003, 2008):

- zapiranje izvoznega trga (izpad prodaje in projektov),
- zakonske omejitve, ki so v nasprotju z mednarodno sprejetimi pravili poslovnega vedenja,

- preobremenitev poslovnih rezultatov sistema z davki in prispevki (kreativno računovodstvo),
- prevzem dela tržišča od tistih, ki so odšli iz sistema in ustanovili lastno podjetje,
- odhod težko nadomestljivih strokovnjakov v konkurenčna podjetja,
- nakup zastarele tehnologije,
- sklenitev škodljivih pogodb,
- prešibka zavzetost organov pregona za obvladovanje kriminala v sistemu,
- odsotnost profesionalnih zunanjih in notranjih revizorjev,
- podkupovanje strokovnjakov, inovatorjev, vodstva in komercialistov,
- ekonomsko vohunjenje v škodo sistemu,
- vdor v računalniški sistem sistema,
- vlom, rop in diverzija v posamezne dele sistema,
- potres, povodenj, požig, ipd.

Navedenimizrednim dogodkom se sistem kolikor toliko uspešno upira le, če ima sposobno vodstvo, prodorne strokovnjake za varnost, učinkovito otranjo revizijo in kontrolo ter pravočasne in prave informacije o zametkih nastajanja posameznega izrednega dogodka. V ta namen si mora vodstvo vzpostaviti učinkovit zgodnji opozorilni sistem in informacijski sistem, da bi lahko pravočasno reagirali v smeri obvladovanja posameznih virov nevarnosti. Za tak pristop le rutinske informacije niso dovolj. Treba se je lotiti prodornejših načinov pridobivanja informacij, kjer v nekaterih delih pridejo v poštev tudi metode načrtnega poslovnega poizvedovanja (business intelligence).

Za vse navedeno so potrebno ustrezna finančna sredstva, pri čemer je treba iskati optimalno razmerje med stroški in potrebnimi zaščitnimi ukrepi. Potrebna so usposabljanja, izobraževanja in izpopolnjevanja, ki lahko hkrati predstavljajo strošek in investicijo. Lahko bi rekli, da gre v bistvu za »cost/benefit« metodo ugotavljanja stroškov in koristi varnostnega sistema. Tak pristop zagotavlja razumno vlaganje v varnostni sistem, v obvladovanje tveganj, v zgodnji opozorilni sistem in v oblikovanje (finančno) učinkovitega portfelja zavarovanj. Ključno vprašanje varnosti sistema je, kako vzpostaviti varnostni sistem in hkrati ekonomsko, poslovno ter moralno učinkovito poslovanje. Pri tem vodstvo zanima predvsem varnostno delovanje, ki bo finančno znosno in bodo investicije v varnostni sistem na daljši rok opravičljive in opravile svojo preventivno dejavnost. Upravljanje ogroženosti, poslovnega in varnostnega tveganja, daje možnost, da se sistem čim bolj približa teoretično zasnovanemu finančnemu ravnotežju med finančno ovrednotenimi škodami / izgubami in stroški zaščite ter finančnimi in drugimi koristmi varnostnega sistema. Novi varnostni koncepti temeljijo na prvinah ekonomike in poslovnosti, pa tudi na pozitivnih prvinah vedenja lastnikov, vodstva in zaposlenih. Ključen je odgovor na vprašanje, kako doseči največjo optimalno varnost ob določenih izdatkih ali najmanjše izdatke ob določeni učinkovitosti.

»Cost/benefit« analiza kaže razmerje med uporabljenimi sredstvi in doseženo varnostjo in zaščito ter privede do vpogleda v stroške in njihovo zmanjševanje, do naravnanosti v ukrepe in aktivnosti, ki so cenejši. Varnostni ukrep je uspešen, kadar stane manj kot druge možnosti, vključno z možnostjo, da ne storimo ničesar.

Vložek v varnostni sistem je investicija in ne poslovni strošek, v primerjavi s škodo, ki se lahko zgodi, pa je zanemarljiv. Pravočasna preventiva je nujna - ko se izredni dogodek zgodi, je že prepozno. Včasih se na varnost gleda zgolj kot na strošek, zato vodstvo kakšne organizacije išče predvsem cenovno ugodne rešitve, ki pa pogosto ne zagotavljajo ustreznega nivoja varnosti, ki je za sistem nujen. Dinamika družbenega in gospodarskega razvoja je pripeljala do tega, da obravnavanje organizacijske varnosti že dolgo ni več zgolj državna zahteva, temveč je postala obveznost sistema za poslovno preživetje.

Zunanje izredne dogodke je vedno treba obravnavati skupaj z notranjimi škodnimi pojavi oz. izrednimi dogodki; velikokrat obstaja povezanost med enimi in drugimi. To pa med drugim pogojuje tudi sodelovanje med notranjo kontrolo in revizijo ter zunanjimi nadzornimi in revizijskimi organi. Ko lastniki, vodstvo, upravljavci, strokovnjaki, razvojniki in nadzorniki v sistemu spoznajo kje in koliko so ranljivi, ugotovijo, kaj jih ogroža, kdo jih ogroža, kako jih ogroža in v kakšnem obsegu, so napravili enega od prvih korakov k zgraditvi modela učinkovitega obvladovanja tveganj, kar je realni pogoj za načrtovanje in izvajanje ukrepov ter postopkov zaščite (vzpostavitev integralnega varnostnega sistema).

»Zaradi notranjih in zunanjih izrednih dogodkov nastanejo škode in izgube, ki se lahko izrazijo« ko (Vršec 1993, 2003, 2008):

- stroški vzpostavljanja v prvotno stanje (npr. po velikem požaru),
- zastoji v proizvodnji zaradi poškodovanih ali uničenih proizvodnih sredstev in opreme,
- izgubljeni delovni dnevi (zaradi zastoja v proizvodnji, transportu ipd.),
- zastoji v razvoju,
- izpad delov tržišča,
- pogodbene kazni zaradi prekoračitve rokov,
- neupravičena uveljavitev bančne garancije,
- zmanjšanje storilnosti in kakovosti,
- izpad investicije ali najetje dodatnega kredita,
- zastoj določenega projekta,
- odhod težko nadomestljivih strokovnjakov,
- nadomestila plač za čas nezmožnosti za delo,
- stroški zdravljenja zaradi delovnih nesreč in zaradi poklicnih bolezni,
- invalidnost in neugodne posledice v zvezi s tem,

- denarna pomoč oškodovancem in poškodovancem,
- nadomestila za čas v bolniškem staležu,
- stroški sodnih postopkov ipd.

Vse to so znatne škode (in hkrati izgube), ki se v pretežni meri izrazijo kot finančne izgube. Če temu še dodamo, da z odškodninskimi zahtevki pri zavarovalnicah dosežemo le del načrtovanega izkupička, je jasno, da so izgube zaradi večjega izrednega dogodka varnostne in poslovne narave (velik požar, potres, poplava proizvodnih in/ali poslovnih prostorov, izguba trga, premoč konkurence, teroristični napad, velika stavka, korupcija večjih razsežnosti, idr.) tako velike, da lahko v določenem časovnem obdobju ogrozijo stabilnost poslovanja sistema.

Prepoznavanje in ocenjevanje ranljivosti premoženja, objektov, procesov, omrežij, človeških virov in ugotavljanje varnostno ranljivih točk

V splošnem ranljivost pomeni različne slabosti posameznika (malomarnost, nenačrtnost, škodljivost, odlašanje ipd.), vrzeli, pomanjkljivosti, luknje, šibke točke in ozka grla v zgradbah, prostorih, proizvodnji, poslovnih procesih, logistiki, informacijskem sistemu, komunikacijah, človeških virih ipd., ki bi jih lahko nekdo znotraj ali zunaj sistema izkoristil kot lažjo pot do povzročitve škode in izgube na premoženju, kapitalu, sredstvih za delo in poslovanje, zaposlenih in v informacijskem sistemu. Analiza ranljivih točk na območju sistema (velikost območja, zgradbe, dovozne poti, parkirišča, poslovni procesi, logistika, proizvodi in storitve, podatki in informacije, človeški viri, poslovni partnerji, pogodbeni podizvajalci ipd.) je potrebno proučiti in izdelati oceno ranljivosti. Ta ocena je – poleg ocene ogroženosti - ena od poglavitnih virov za prepoznavo virov nevarnosti.

Drugo vprašanje, ki ga lahko obravnavamo v sklopu ranljivosti je ugotavljanje varnostno vitalnih točk na območju sistema. Varnostno vitalne točke so tiste točke na območju in zgradbah sistema ter njegovi infrastrukturi, ki izstopajo z realno in / ali potencialno ogroženostjo. To so lahko posamezna (kriminogena) delovna mesta, več delovnih mest, posamezni zaposleni ali več zaposlenih (združba, ki škodljivo in kaznivo deluje), določeni deli območja sistema, določene zgradbe in deli zgradb (prostori), določeni deli prostora, izpostavljeni deli infrastrukture, določeni materiali (surovine, polizdelki, izdelki, načrti, recepti, patenti ipd.). Opredeliti varnostno vitalne točke torej pomeni določiti tiste točke, območja, lokacije, prostore, vhodne komplekse, poslovne dogodke, občutljiva delovna okolja in drugo, ki jih je treba posebej fizično, tehnično ali kako drugače varovati (zaščititi) in zavarovati (pri zavarovalnicah), da preprečimo in / ali omejimo kakršnekoli napade nanje. Če pa pride do napada (ogrožanja) na katerokoli varnostno vitalno točko, pa je treba v varnostnem sistemu zagotoviti zgodnji opozorilni sistem, zanesljiv alarmni sistem in hitre ter strokovne odzive na alarmna sporočila.

Na splošno se varnostno vitalne točke v sistemu vidijo v naslednjih varnostno zanimivih segmentih (povzeto po Vršec 1993, 2010):

- poslovni dogodki, ki ogrožajo intelektualno in industrijsko lastnino ter državno, uradno in poslovno skrivnost (npr. sklepanje škodljivih pogodb, neupoštevanje konkurenčne klavzule, izdaja poslovnih skrivnosti, podkupovanje, računalniški kriminal ipd.),
- finančno in moralno škodljive poslovne in tržne transakcije, malverzacije, špekulacije in mahinacije (korupcijska tveganja),
- kriminogena delovna in poslovna okolja (npr. delovna mesta računovodij, finančnikov, komercialistov in drugih, ki so nagnjeni k goljufijam, zlorabi položaja, zlorabi notranjih informacij, ipd., delovna mesta v skladiščih, ekspeditu, proizvodnji in drugod, kjer obstajajo priložnosti za kraje (tatvine), vlome in tudi rope,
- lokacije požarne ogroženosti,
- delovna mesta, kjer obstaja večja nevarnost nastanka poškodb pri delu in zdravju škodljivih snovi ali postopkov,
- lokacije in območja ekološke ogroženosti,
- mesta logistične ogroženosti (v notranjem transportu, prometu),
- eksplozivno nevarna mesta – lokacije, prostori z nevarnimi snovmi,
- elektroenergetske in druge naprave podvržene eksploziji (transformatorji ipd.),
- arhivski prostori,
- skladišča dragih izdelkov ali polizdelkov,
- prostori kadrovskih, razvojnih in informacijskih služb,
- vhodi na območja in v zgradbe, prostor z zaupno dokumentacijo in tajnimi podatki,
- druga nevarna mesta glede na posebnosti v dejavnostih in poslovanju sistema.

Kaj imajo skupnega ranljive in varnostno vitalne točke sistema? Gre za to, da so nekatere ranljive točke tudi varnostno vitalne točke. Karakteristke ranljivih točk so človeške slabosti, vrzeli, ozka grla, šibke točke ipd., karakteristike varnostno vitalnih točk pa so predvsem točke, ki temeljijo na zakonskih zahtevah in varnostnih standardih ter že »samoumevnih zahtevah« po zaščiti (rampe na vhodih v sistem, pristopna kontrola na vhodih v zgradbo in določene prostore, zaščita informacijskega sistema, avtonomna energijska podpora, senzorji za požarni alarm ipd.). Ranljive in obenem varnostno vitalne točke so tudi slabo varovani tajni podatki ali slabo varovana dokumentacija o poslovni skrivnosti, ker gre za dokumentacijo, ki je zanimiva za konkurenco in druge zainteresirane, ali pa slabo varovane nevarne snovi kot ranljiva točka, ki so obenem tudi varnostno vitalna točka (te snovi so po naravi poslovanja varnostno zanimive in jih je treba že po zakonu ustrezno varovati in zaščititi).

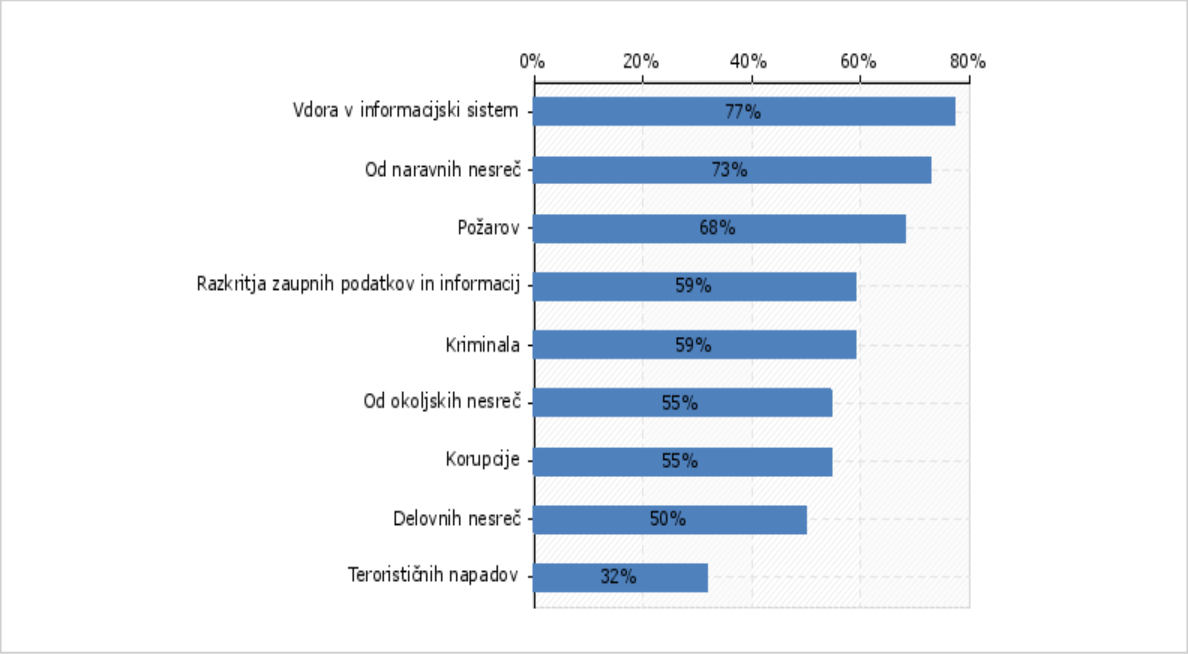
V varnostni stroki poznamo dejansko (resnično), potencialno (pretečo) in latentno (prikrito) ogroženost. Dejansko ogroženost predstavljajo izredni dogodki, ki so se že pripetili, kot so

denimo požar, eksplozija, delovna nesreča, informacijska nesreča, izpad komunikacije, tatvina, rop, vlom, grožnja z bombo, fizični napad na določeno osebo, poslovna goljufija ipd.

O potencialni ogroženosti govorimo, ko na območju zgradb, v zgradbah, v poslovnih procesih in v logistiki obstajajo nevarne okoliščine in nevarna stanja, ki omogočajo nastanek izrednih dogodkov, kot npr.: dokazano slabi ergonomski in materialni pogoji za delo zaposlenih, ni sistema aktivne požarne zaščite, zastarel video nadzorni sistem, nestrokovni in slabo psihofizično usposobljeni varnostniki, šibko tehnično varovanje, neurejeno varovanje dokumentov zaupne narave, nezanesljiv alarmni sistem, niso zagotovljene rezervne komunikacije, dotrajana električna instalacija (nevarnost požara), prešibka avtonomna energijska podpora (nevarnost informacijskega kolapsa, ipd.).

O latentni ogroženosti govorimo, ko nevarne okoliščine in nevarna stanja niso vidna »na prvi pogled« in šele sistematično nadziranje ter poglobljeno analiziranje posameznih poslovnih in varnostnih procesov razkrije prikrito nevarnost, kot npr.: sum notranjih tatvin, namig o izdaji poslovne skrivnosti, sum iznosa zaupnih dokumentov, v ozadju se skriva poslovna goljufija, šušlja se o aferi, konkurenca pripravlja tržni napad, premalo nadzirani pogodbeni izvajalci, nizka varnostna kultura zaposlenih, grozeči terorizem, pričakovane grožnje ipd. Realna, potencialna in latentna ogroženost predstavljajo za sistem določeno nevarnost in tveganje pri tekočem izvajanju poslovnih funkcij ter pri uresničevanju razvojne strategije. Ogroženost poslovnih funkcij in razvoja je obvladljiva zlasti s posodobitvijo strojne in programske opreme, izboljšanjem zanesljivosti in varnosti komunikacij, z vzpostavitvijo profesionalnega fizičnega in tehničnega varovanja ter strožjih varnostnih režimov znotraj in zunaj zgradb sistema ter z dvigom varnostne kulture zaposlenih.

Po izvirni metodologiji klasificiranja, analiziranja in ocenjevanja ogroženosti (Vršec, 2003, 2010), so potrebne posebne pozornosti naslednje vrste (oblike) ogroženosti: ogroženost od naravnih nesreč; požarna in eksplozijska ogroženost; ogroženost od nevarnih snovi in kemikalij; ekološka ogroženost; kriminalna, teroristična, vohunska in informacijska ogroženost; ogroženost osebnih in tajnih podatkov; ogroženost identitete, ogroženost poslovnih skrivnosti, prometna in logistična ogroženost; socialna in sabotažna ogroženost, ogroženost javnega reda in miru; konkurenčna ogroženost in tehnično - tehnološka ogroženost. Nabor navedenih vrst ogroženosti je klasificiran glede na vir varnostnih groženj, glede na predmet in subjekt ogrožanja ter glede na območje ogrožanja (globalno, mednarodno, nacionalno, lokalno). S tega zornega kota je treba v vsakem sektorju sistema oceniti ogroženost premoženja, objektov, procesov, omrežij in človeških virov. V raziskavi o neprekinjenem poslovanju KI so respondenti odgovarjali tudi na vprašanje od česa so v lastni gospodarski družbi, zavodu ali organu ogroženi. Odgovori so podani na sliki 40, iz katere je razvidno, da so v KI najbolj ogroženi od vdora v informacijski sistem, od naravnih nesreč, požarov, razkritja zaupnih podatkov in informacij ter od kriminala.



Slika 40: Ogroženost KI (Marinčič, 2017)

Smiselna in koristna bi v procesu nastajanja modela ali metodologije ocenjevanja tveganj za delovanje KI, bila raziskava, v okviru katere bi prišli tudi do relevantnih informacij o ogroženosti posameznih sektorjev sistema.

a. Požarna in eksplozijska ogroženost

Požari in eksplozije so izredni dogodki, ki jih je smiselno obravnavati skupaj. Kajti požari sprožajo eksplozije in obratno: eksplozije povzročajo požare. Iz ocene požarne ogroženosti, ki mora biti izdelana po predpisani metodologiji, morajo biti razvidne stopnje ogroženosti in požarna tveganja v zgradbah, prostorih in procesih. Stopnje požarne ogroženosti so:

- zelo majhna požarna ogroženost,
- majhna požarna ogrožernost,
- srednja požarna ogroženost,
- srednja do povečana požarna ogroženost,
- velika požarna ogroženost,
- zelo velika požarna ogroženost.

Za potrebe ocenjevanja požarne ogroženosti je treba imeti na razpolago naslednje podatke o:

- številu ljudi na območju, za katerega se ocenjuje požarna ogroženost,
- količini sredstev za gašenje (voda in druga sredstva),
- zaposlenemu, ki je odgovoren za varstvo pred požari,

- kakovosti vzpostavljenega sistema aktivne požarne zaščite,
- količini nevarnih snovi,
- dostopih do zgradb in intervencijskih poteh.

Iz prakse ocenjevanja požarne ogroženosti – tudi v sistemu – je potrebno pridobiti še podatke, informacije in dokumente o naslednjih zadevah:

- tveganja v notranjem transportu za potrebe proizvodnje,
- količina, lokacija, stopnja tveganja in zaščita kemikalij in drugih nevarnih snovi na območju in v zgradbah,
- visoko tvegani objeti, ki sprožajo ekološko, požarno in eksplozijsko ogroženost,
- oprema v prostorih (lesena oprema, podi, zavese, drugi lahko gorljivi materiali ipd.),
- red in vsebina skladiščnih prostorov,
- red in vsebina arhivov,
- požarne nevarnosti v omrežjih,
- stanje elektroinstalacij,
- kakovost vzdrževanja elektroinstalacij,
- lokacije vodnih virov in drugih sredstev za gašenje,
- organiziranost požarnih straž v preteklih primerih, potrebe po teh stražah (razvidno iz obstoječe dokumentacije),
- obstoj in kakovost študij ter drugih analiz požarne varnosti,
- urejenost dohodnih poti do zgradb in intervencijskih poti,
- stanje obstoječe protipožarne zaščite,
- organiziranost lastne gasilske službe ali pogodbeno najete gasilske intervencije,
- število in teža posledic preteklih požarov,
- usposobljenost varnostnikov za požarno preventivo in za aktivno sodelovanje v primeru požara (licenca in dejanska usposobljenost),
- zanesljivost požarnega alarmnega sistema,
- hitrost odzivanja na požarne alarmne signale,
- usposobljenost zaposlenih za požarno preventivo in za ukrepanje v primeru požara,
- obstoj in izvajanje načrta evakuacije za primer požara ter za druge izredne dogodke, ki terjajo evakuacijo zaposlenih in strank.

To so dejavniki, ki vplivajo na tveganje nastanka požara, in ki določajo stopnjo požarne ogroženosti ter zahteve pri vzpostavljanju sistema aktivne požarne zaščite. Gostota naseljenosti, oddaljenost in kategorija gasilske enote niso primarni dejavniki za ocenjevanje požarne ogroženosti. Bližina gasilske enote ne vpliva na tveganje nastanka požara, odločilno pa lahko vpliva na obvladovanje požara, to je na gašenje, omejitev in obvladovanje požara.
Področje varstva pred požari in gasilstva urejajo številni predpisi, ki med drugim, poleg ocene požarne ogroženosti, določajo izdelavo požarnega reda, načrta protipožarnih ukrepov načrta

evakuacije, usposabljanje gasilcev in zaposlenih ter druge zahteve. Za obvladovanje eksplozijske ogroženosti pa referenčna zunanja institucija izdela elaborat eksplozijske ogroženosti in protieksplozijskih ukrepov.

b. Ogroženost in tveganja na delovnih mestih

Varnost in zdravje pri delu je eden od osrednjih problemov pri upravljanju s človeškimi viri. Ogroženost in tveganja varnosti in zdravja pri delu imajo še eno veliko specifiko. Tesno so namreč povezana s požarnimi, eksplozijskimi, okoljskimi in logističnimi tveganji. Zaradi tega je celovito obvladovanje tveganj na področju varnosti in zdravja pri delu nujno povezano z obvladovanji tveganj v sistemu aktivne požarne zaščite, tveganj v procesu upravljanja okoljskih tveganj in tveganj v logistiki. Glavni dokument o ogroženosti in tveganjih na delovnih mestih je izjava o varnosti z oceno tveganj, ki jo mora po Zakonu o varnosti in zdravju pri delu imeti vsaka organizacija. Posebna pozornost mora biti namenjena delovnim mestom, ki so izpostavljena raznim nevarnostim in številnim tveganjem za poškodbe in bolezni.

Predpostavke o tveganjih varnosti in zdravja pri delu so:

- glavno tveganje se nanaša na bojazen, da morda še niso podrobno definirana delovna mesta z visokimi stopnjami tveganja in da za ta delovna mesta še ni izdelan jasen načrt celovitega obvladovanja (zmanjševanja, skrčenja) tveganj,
- z vidika nesreč pri delu se je treba prepričati ali ima enota Civilne zaščite za prvo pomoč ustrezna sredstva in opremo za prvo pomoč poškodovanemu delavcu (lahko je poškodovanih več delavcev hkrati), ali delavcu, ki ima trenutno zdravstveno težavo. Vprašanje je tudi ali imata vodja Službe varstva pri delu in poverjenik za Civilno zaščito usklajene potrebe po prvi pomoči in po zaščitni opremi,
- odlašanje z uvedbo standarda varnosti in zdravja pri delu OHSAS 18001, in standarda ISO 45001:2018 se lahko pripeti, da ogroženost in tveganja na izpostavljenih delovnih mestih ne bodo obvladovana – to pomeni, da obstajajo tveganja nastanka delovnih nezgod
- izjava o varnosti z oceno tveganj mora eksplicitno definirati katera delovna mesta in katera delovna okolja imajo status »izpostavljenega delovnega mesta«, za katera je potreben poseben načrt obvladovanja tveganj,
- zdravstveni pregledi delavcev na izpostavljenih delovnih mestih morajo biti pod posebno kontrolo zaposlenega, ki je odgovoren za varnost in zdravje pri delu ter je pod kontrolo zunanjih institucij, Delovne inšpekcije in Zdravstvene inšpekcije ali drugega inšpekcijskega organa,

- če ni dovolj dobro (v skladu z zakonodajo in v skladu z oceno ogroženosti in tveganj) poskrbljeno za področje varnosti in zdravja pri delu, ni realno pričakovati, da bodo učinkovito obvladovana vsa ogrožanja in tveganja.

Ogroženost in tveganja varnosti in zdravja pri delu so »interdisciplinarna tveganja«, ki močno vplivajo na notranje zadovoljstvo zaposlenih in notranjo integriteto, kakovost dela, način razreševanja socialne problematike in na poslovno uspešnost, ugled ter razvoj kadrovske funkcije v sistemu.

c. Ekološka (okoljska) ogroženost

V sistemu je nekaj sektorjev, ki se morajo resno, profesionalno in v skladu z zakonodajo ter okoljskimi standardi spopadati z varstvom okolja, kjer ima pomembno vlogo ocena ogroženosti, ocena tveganj in učinkoviti ukrepi zaščite. To so v prvi vrsti sektor energetike in sektor prometa, potem pa še sektor zdravstva in sektor varovanja okolja, ki je že sam po sebi zavezan za profesionalno obvladovanje ogroženosti, obvladovanje tveganj in zagotavljanje primerne okoljske zaščite premoženja, zraka, zemlje, vode, človeških virov ter živalskega in rastlinskega sveta. Upravljavci KI, ki so okoljski zavezanci po naši zakonodaji in po SEVESO II ter SEVESO III se morajo prilagoditi predpisanim zahtevam in uvajati okoljske standarde kot so SIST EN ISO 14001 in EMAS.

Posebni vidik ekološke ogroženosti se kaže v prešibki povezanosti področja varstva okolja, s področji kot so: varnost in zdravje pri delu, požarno varstvo, zaščita in reševanja ter fizično in tehnično varovanje. Gre za zagotavljanje večje povezanosti pri ocenjevanju ogroženosti, pri načrtovanju skupnih ukrepov v sklopu Načrta zaščite in reševanja, Načrta fizičnega in tehničnega varovanja ter načrtovanja skupnih finančnih vložkov v področje varstva okolja. Na ta način bi se lahko posamezne aktivnosti racionalizirale, zmanjšali stroški in povečala preglednost nad stroški in koristmi vlaganja v to področje.

d. Ogroženost zaradi neučinkovitega fizičnega in tehničnega varovanja

V praksi fizičnega in tehničnega varovanja obstajajo pomanjkljivosti, kljub temu, da za to področje obstaja zakonodaja, varnostni standardi in trg varnostnih storitev. Operativni posnetki in številne analize stanja fizičnega, tehničnega in požarnega varovanja v gospodarskih družbah so pokazale naslednje pomanjkljivosti (povzeto po Vršec/Vršec 2008):

- naročniki zasebnega varovanja nimajo izdelanih načrtov varovanja v skladu z varnostno stroko, kot tudi ni jasnih strokovnih navodil za delo na posameznih delovnih mestih - obstajajo navodila, ki so metodološko, vsebinsko in strokovno šibka, da praktično niso uporabna,

- prav tako se kaže nedodelanost načrtov preventivnih protipožarnih ukrepov, strokovnih navodil za delo in ustvarjanje potrebnih evidenc,
- delodajalci pogodbeno najetih varnostnikov, niti naročniki, nimajo profesionalnega nadzora nad delom varnostnikov in gasilcev,
- načrti alarmiranja izrednih dogodkov in odzivov na izredne dogodke so nezanesljivi in pomanjkljivi,
- pogodbeni izvajalci varovanja ne poznajo dovolj dobro in v posameznih primerih ne obvladujejo varnostno vitalnih točk v zgradbah in v okolici zgradb; prav tako ne poznajo ocen ogroženosti, požarnih redov, sistema evakuacije, videonadzornega sistema, kontrole pristopa, sistema aktivne požarne zaščite in organiziranosti sistema zaščite in reševanja,
- varnostniki ne obvladujejo dinamike znotraj zgradb kot tudi dinamike (parkirišča, dovozne poti, intervencijske poti) zunaj zgradb,
- pogodbeni izvajalec ne zagotavlja potrebne stalnosti varnostnikov na delovnih mestih, menjave so pogoste in neustrezne,
- večina varnostno nadzornih centrov (VNC) sicer deluje v skladu s standardom SIST BS 5979, vendar je vprašljiva zanesljivost delovanja teh centrov v izrednih dogodkih, ko se pokažejo težave s sistemom avtonomne energijske podpore, potrebne za neprekinjeno delovanje alarmnega in odzivnega sistema,
- na delovnih mestih varnostnikov se v posameznih primerih kažejo težave v tem, da ni ustrezne opreme, niti potrebnih evidenc, niti ustreznega sistema dela, niti ustreznega opisa del in nalog,
- pogodbeni izvajalci varnostnih storitev le redko predlagajo varnostne izboljšave, ker ne poznajo ocen ogroženosti in varnostnih tveganj ter stopnjo učinkovitosti varnostnega sistema,
- nad fizičnim in tehničnim varovanjem se dosledno ne izvaja presoja kakovosti varovanja, niti ni uravnoteženega inšpekcijskega nadzora nad zasebnim varovanjem internega in eksternega značaja.

Pri ugotavljanju ogroženosti šibkega fizičnega in tehničnega varovanja so primerna naslednja merila (Vršec/Vršec 2008):

- vloga varnostne službe oziroma pogodbeno najetega izvajalca fizičnega varovanja oseb in premoženja v varnostnem sistemu,
- načrt varovanja oseb in premoženja,
- načrt obvladovanja izrednih dogodkov,
- navodila za delo varnostnikov na posameznih delovnih mestih,
- upoštevanje zakonodaje s področja zasebnega varovanja,

- upoštevanje zakonodaje s področja varstva osebnih podatkov, kjer so določila o urejanju video nadzornega sistema,
- upoštevanje zakonodaje s področja varovanja tajnih in osebnih podatkov,
- upoštevanje zakonodaje s področja varovanja poslovnih skrivnosti,
- vključenost varnostne službe (pogodbenega izvajalca) v sistem zaščite in reševanja,
- vključenost varnostne službe (pogodbenega izvajalca) v sistem aktivne požarne zaščite,
- oprema in sistem dela izvajalca pri izvajanju pogodbenih obveznosti,
- dokumentacija pogodbenega izvajalca o varovanju oseb in premoženja naročnika,
- obstoj projekta oziroma elaborata (projekt za izvedbo PZI in projekt izvedenih del PID) za potrebe tehničnega varovanja (PZI in PID po gradbeni zakonodaji)
- organiziranost alarmnega in odzivnega sistema,
- organiziranost varnostno nadzornega centra pogodbenega izvajalca varovanja,
- sistem nadzora nad pogodbenim izvajanjem varovanja.

Fizično varovanje z usposobljenimi varnostniki in tehnično varovanje s sodobno opremo je kompleksno merilo učinkovitega varovanja premoženja, objektov in (poslovnih, športnih, zabavnih, kulturnih) dogodkov. Poleg prej navedenih projektov PZI in PID je za profesionalno varovanje potrebno izdelati načrt varovanja, ki temelji na oceni ranljivosti, ogroženosti in tveganj in ki je v skladu z zakonskimi zahtevami.

e. Tehnično - tehnološka ogroženost

Pri tej vrsti ogroženosti gre za stanje obstoječe tehnično - tehnološke opreme, ki je potrebna za delovanje posameznih sektorjev sistema. Gre za vprašanja kot so kakovost investicijskega in rednega vzdrževanja posameznih delov in sistemov (proizvodnih procesov, informacijske tehnologije, omrežij, logistike in ostalega, kar vpliva na učinkovitost delovanja in poslovanja) in vprašanja o problematiki stalnega investiranja v posodobitev ter razvoj. Posebno vprašanje, z vidika zastarelosti in problemov investiranja v sistem je obvladovanje tehnično - tehnološke ogroženosti električnih, komunikacijskih, plinovodnih, naftovodnih in drugih infrastrukturnih omrežij, katerih delovanje je lahko ovirano ali celo prekinjeno za krajši ali daljši čas. Prepletanje in soodvisnost omrežij terja usklajevanje gradbenih, investicijskih in vzdrževalnih posegov različnih organizacij, da se preprečijo problemi načrtovalne, projektne, tehnično - tehnološke in finančne narave. Nosilci in upravljavci sistema se večinoma zavedajo o stalnem posodabljanju informacijske tehnologije, ki med drugim omogoča neprekinjeno delovanje in obvladovanje izrednih dogodkov.

4.3.1.2 Prepoznavanje tveganih scenarijev (2 KORAK)

Proces odgovarjanja na vprašanje: »Kaj se zgodi, če…« se imenuje prepoznavanje scenarijev. Njihova bistvena značilnost je vnaprejšnje prepoznavanje tveganih scenarijev organizacije.

Velika razširjenost uporabe scenarijev na različnih področjih družbenega življenja, tudi na področju KI, je prispevala k njihovi popularizaciji. Scenariji se uporabljajo za prepoznavanje verjetnega tveganega prihodnjega stanja. Namen prepoznavanja scenarijev je razširiti okvir razmišljanja o prihodnosti z različnimi verjetnimi prihodnjimi stanji, ki se lahko razvijejo iz sedanjega stanja. Alternative pa vključujejo elemente vizij, projekcij, statističnih podatkov, znanja presojevalca ipd. Od njih se razlikujejo v tem, da pri alternativah tvegana prihodnost ni povsem enoznačno opredeljena, tako se izognemo občutku, ki ga prinaša uporaba samo enega scenarija – da se bo določen tvegan scenarij dejansko dogodil.

Pogosto nekritična raba tega izraza žal ne prispeva k razvoju scenarijev kot znanstvene metode. Več avtorjev (npr. Barbieri Masini in Medina Vasquez, 2000) kritično menita, da se raziskovalci scenarijev lotevajo »na pamet«, brez poznavanja njihovih tipov in namena. Scenariji so postali priročno orodje, ki omogoča, da si sodelujoči z različnih sektorjev KI ter z različnim znanjem in poznavanjem problematike lažje predstavljajo prihodnji tvegan razvoj ali spremembe, pa naj gre za možne izredne dogodke ali zaznavo tveganja.

Pojem scenarij je za poimenovanje dolgoročnih vizij prihodnosti prvi uporabil Kahn (Kahn in Wiener,1969). Navedeni pojem v širšem pomenu združuje različne tehnike oziroma študije, usmerjene v preučevanje prihodnosti, kot so analize trendov, napovedi, variantne analize in strategije. Temeljne opredelitve scenarijev, njihovega razvoja in uporabe so med drugimi podali Schwartz (1991), Lindgren in Bandhold (2003). Tako obstaja veliko različnih opredelitev, ki so prilagojene posameznim oblikam in uporabi scenarijev na različnih področjih. Ožjo opredelitev sta postavila Veeneklass in van den Berg (1995: 11): »Scenarij je opis ali podoba sedanjega stanja, verjetnega ali želenega prihodnjega stanja in tudi serije dogodkov, ki vodijo od sedanjega do tega želenega ali verjetnega prihodnjega stanja.«

Z razvojem in uporabo scenarijev za različne namene so se oblikovale tudi različne tipologije, ki scenarije na podlagi njihove vsebine, namena, načina izdelave, uporabe ali kombinacije njihovih značilnosti uvrščajo v določen tip.

Najbolj splošna je delitev scenarijev na normativne ali proaktivne (ang. proactive scenario) in deskriptivne, ki jih imenujemo tudi napovedovalni ali perspektivni (ang. prospective scenario). Delitev temelji na različnih dojemanjih prihodnosti, kot jih je opredelil Ackoff (1981). Podlaga za normativne scenarije je tako imenovano proaktivno stališče: prihodnost je odvisna od dejanj v sedanjosti. Deskriptivni scenariji temeljijo na stališču, da posamezniki in organizacije

ne morejo dejavno spreminjati prihodnosti, saj je ta odvisna od različnih zunanjih dejavnikov, na katere pa nimajo bistvenega vpliva. Odnos do prihodnosti je torej prvi korak k razumevanju prepoznavanja tveganih scenarijev.

Oba tipa scenarijev, normativni in deskriptivni, se uporabljata kot pomoč pri odločanju, vendar vsak drugače. Normativni scenariji so usmerjeni v iskanje želene prihodnosti, deskriptivni pa v ugotavljanje verjetne prihodnosti, ne glede na preference. Normativni scenariji so očitno usmerjeni k določenemu cilju in opredeljeni z različnimi vrednotami; uporabljajo se kot okvirni načrti za prihodnost, pri čemer se odločitev izvede na podlagi več možnosti, ki temeljijo na različnih predpostavkah. Tudi pri deskriptivnih scenarijih je mogoče z različicami preverjati verjetni razvoj glede na zaznane trende, namenjeni so predstavitvi različnih možnosti razvoja in opozarjanju na morebitne izredne dogodke in tveganja. Deskriptivni scenariji naj bi bili nevtralni, vendar kljub temu implicitno vključujejo različne vrednote in poglede ocenjevalcev (Shearer, 2005).

Čeprav so scenariji koristno orodje imajo tudi slabosti, na katere opozarjajo različni avtorji. Gre za lahko predstavljivost, zaradi katere posamezniki včasih sprejmejo scenarij kot dejstvo, da se bo ta res zgodil v predvideni pojavni obliki. Ob tem se moramo zavedati, da posamezniki niso ravno najboljši ocenjevalci verjetnosti izrednih dogodkov in da sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo.

Na splošno je proces izdelave scenarijev prikazan na sliki 41. Nanaša se na vsaj pet korakov: izdelava scenarija (kako določiti in prepoznati vire možnih zunanjih ali notranjih izrednih dogodkov), ocena scenarija (opisna ocena tveganih scenarijev v organizaciji), kvaliteta podatkov in informacij (kako zanesljivi so ti ob negotovi prihodnosti), določitev vrednosti parametrov tveganih scenarijev (kvalitativna ali kvantitativna) in rezultati modela (ocena posledic realiziranega izrednega dogodka).

Slika 41: Proces izdelave scenarijev možnih izrednih dogodkov (interni vir ICS)

Za namen tega projekta je treba prepoznane vire nevarnosti za določen sektor KI vnesti v tabelo 9.

Tabela 9: Identifikacija nevarnosti za določen sektor KI (smiselno prirejeno po MOSAR)

Sektor energetike (možni primeri):

Sektor energetike z viri nevarnosti	Zunanje nevarnosti	Notranje nevarnosti	Scenarij nevarnosti	Posledice
Kritična distribucija in pomanjkanje goriva (diesel, bencin)	naravne nesreče: požar, potres, poplava, žled; zastoj cestnega in/ali železniškega prometa; izpad dobave elektrike; stavka zaposlenih	neustrezno sklepanje dobavnih pogodb	večje okvare distribucijskih vozlišč, ni distribucije goriv	velike izgube v gospodarstvu, izguba zaupanja uporabnikov
Prenehanje dobave zemeljskega plina	naravne nesreče: požar, potres, poplava, žled; zastoj cestnega in/ali železniškega prometa; izpad dobave elektrike; stavka zaposlenih	neustrezno sklepanje dobavnih pogodb	ni prenosa zemeljskega plina in obratovanja plinovodnega omrežja	velike izgube v gospodarstvu, izguba zaupanja uporabnikov
Poškodba omrežja za prenos električne energije	naravne nesreče: požar, potres, poplava, žled; terorizem	namerno poškodovanje dela omrežja pomanjkljivo vzdrževanje omrežja premalo investicij v posodabljanje omrežja	naravna nesreča – žled, ki bo trgal pomembne daljnovode, motena bo zanesljiva in kakovostna oskrba z energijo	izgube v gospodarstvu, nedelovanje državne uprave, stroški izpada in kompletne obnove 400 kV omrežja, stroški vzpostavitve prvotnega stanja

Sektor prometa (možni primeri):

Prometni sektor z viri nevarnosti	Zunanje nevarnosti	Notranje nevarnosti	Scenarij nevarnosti	Posledice
Verižno trčenje večjega števila osebnih in tovornih vozil	poledica in megla	neupoštevanje cestnih predpisov in voznih razmer	težke vozne razmere na avtocesti, nepazljivost voznikov	večje število mrtvih, velika materialna škoda, dalj časa neprevozna avtocesta, kritičen odziv javnosti

Trčenje tovornega in potniškega vlaka ter izlitje strupenih snovi	tehnična napaka	napaka in malomarnost zaposlenega kontrolorja prevoza	trčenje dveh kompozicij vlakov na istem tiru	v primeru izpada železniškega tovornega prometa se lahko pojavi kritično pomanjkanje energentov
Padec potniškega letala	odpoved dela opozorilnih sistemov, odpoved motorja	tehnična napaka, neustrezen odziv pilota	neupoštevanje pravil letenja, terorizem	večje število mrtvih, velika materialna škoda

Sektor prehrane (možni primeri):

Preskrbovalni sektor z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Nezagotavljanje hrane in njene neoporečnosti	ob popolnem izpadu dobave hrane država hitro ne bi mogla več zagotavljati osnovnih funkcij delovanja, možnost bioterorizma	neupoštevanje zunanjih in notranjih standardov kvalitete hrane s strani zaposlenih	brez hrane se težko zagotavlja osnovne državne storitve, saj lakota in pomanjkanje hrane hitro rušita družbeni in javni red. Pojav bolezni, ki so posledica uživanja okužene hrane, predstavlja enega pomembnejših javno zdravstvenih problemov	povzročitelji okužb s hrano so številne bakterije, virusi, zajedavci in glive, težava pa je največkrat driska. Okužbe se pojavljajo posamično in v večjem številu (izbruh, epidemija). Izguba ugleda javnosti.
Nezagotavljanje prehranske varnosti s stabilno pridelavo varne, kakovostne in potrošniku dostopne hrane	celotna prehranska veriga je zelo občutljiva zaradi visoke ravni odvisnosti od drugih zunanjih dejavnikov, npr. energije, brez katere ni možna proizvodnja hrane, zlasti ni možno dosegati standardov kakovosti	vnos patogenov, nameren ali nenameren, se lahko zgodi kjerkoli in kadarkoli v prehrambeni verigi	pojav vrste naravnih in umetnih agensov, od bolezni, organizmov, narave in je odvisen od vremenskih pogojev. Pri izdelavi hrane je ogrožena vsaka stopnja obdelave	nezmožnost zagotoviti temeljne storitve več kot en teden, izguba zaupanja uporabnikov

Povečanje zdravju škodljivih aktivnih snovi v hrani in pitni vodi	neprimerna uporaba zaščitnih snovi, nekakovostni prehranski dodatki	vnos patogenov, nameren ali nenameren s strani zaposlenega, se lahko zgodi kjerkoli in kadarkoli v prehrambeni verigi	zmanjšanje ravni zdravju škodljivih aktivnih snovi v hrani in pitni vodi, vključno z nadomeščanjem najnevarnejših snovi z bolj varnimi (vključno z ne-kemičnimi nadomestki)	ljudje so lahko negativnim vplivom izpostavljeni na več načinov, najbolj so lahko izpostavljeni delavci pri proizvodnji fitofarmacevtskih sredstev. Poleg tega je možna posredna izpostavljenost FFS uporabnikov hrane in vode, izguba ugleda.

Sektor preskrbe s pitno vodo (možni primeri):

Oskrba s pitno vodo z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Kritično pomanjkanje vode za pitje in osebno higieno	ogroženi so pomembni vodni viri, vodovarstvena območja, neustrezni ukrepi za preprečevanje onesnaženj cevovodov in črpališč, vključno z nezagotavljanjem ukrepov za zmanjševanje bioloških, kemičnih in fizikalnih tveganj, možnost bioterorizma	namerno ali nenamerno ogrožanje dobave vode s strani zaposlenega pomanjkljiv register pitne vode	vse pogostejši izredni vremenski dogodki (poplave, neurja z vetrom, zmrzali, žled, nalivi ipd.) neposredno (npr. zalitje zajetja, poškodba cevi omrežja ipd.) ali posredno (npr. z izpadom električne energije) ogrožajo oskrbo s pitno vodo in njeno kakovost	posledice sanacij vodnih virov in infrastrukture zaradi naravnih in drugih nesreč ter namernih napadov (človeške napake in dejavnosti, razlitje nevarnih snovi), bioterorizma. Nezmožnost temeljnih storitev več kot en teden, izguba zaupanja uporabnikov
Zajezitev in nadzor nad količino vode	primeri namerne povzročitve škode, napada, tehnološke okvare ali naravne nesreče	neustrezna prioriteta v dobavi vode v kriznih okoliščinah nereden in neučinkovit nadzor nad vodovodnim omrežjem	poplavni val vpliva tako na naravo, prebivalstvo kot gospodarstvo (udarni val, človeške žrtve, porušitve objektov, uničenje transportnih in drugih komunikacij, kontaminacija pitne vode, vpliv na delovanje energetskih objektov). Vodohrani in črpališča so problematični predvsem v primeru	velika gospodarska škoda, sistem nadzora je zelo obremenjen med hudimi poplavami oziroma vodno ujmo, ko je naenkrat zajeto veliko območje, kadrovska podhranjenost in manjše kapacitete izvajalcev, negativen odziv javnosti

			namerne povzročitve škode oziroma napada oziroma tehnološke okvare, še posebej so ogroženi manjši sistemi, ki nimajo ustreznega varovanja	
Mikrobiološka in fizikalna neustreznost vode	vodovodno omrežje je problematično, ker vsak vodovodni priključek ali hidrant predstavlja potencialno mesto, kjer je možno v sistem vnesti strupeno snov, možnost bioterorizma	namerna ali nenamerna površnost v laboratorijskih raziskavah -namerna površnost je prikrivanje slabih rezultatov	rezultati mikrobioloških in fizikalno – kemijskih preskusov (tudi terenskih meritev) so neustrezni v vodnjakih, črpališčih zajetij pitne vode, v vodooskrbnih objektih in na mestih uporabe	neuporaba vode za pitje in osebno higieno, izguba zaupanja uporabnika

Sektor zdravstva (možni primeri):

Zdravstveni sistem z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Epidemija norovirusa	v zadnjih letih so norovirusi prepoznani kot najpogostejši povzročitelji virusnih prebavnih okužb	nerealna ocena zdravstvene ogroženosti prepočasno odzivanje na pojav epidemije	norovirusi povzročajo akutni gastroenteritis pri osebah vseh starosti. Povprečna inkubacijska doba je od 24 do 48 ur. Bolezen se začne akutno, z nekrvavo drisko, bruhanjem, slabostjo in trebušnimi krči. Norovirusi so zelo kužni. Okužba se zlahka širi med ljudmi	norovirusi krožijo v različnih okoljih in povzročajo sporadične ali skupinske primere okužb. So tudi najpogostejši vzrok izbruhov gastroenteritisa. Izbruh obolenj zaradi okužbe z norovirusi v okolju, kjer prebivajo ljudje z zmanjšano imunsko odpornostjo predstavlja veliko tveganje za njihovo zdravje in delo. Okužba izrazito oslabi organizem

Pandemija gripe	bolezen lahko predstavlja čezmejno nevarnost za zdravje ljudi. Pandemija se širi v valovih, dolžina vsakega vala je od 6 do 8 tednov. Drugi val se navadno pojavi v 3 do 9 mesecih od začetnega in lahko povzroči še višjo stopnjo smrtnosti	površno spremljanje in prepočasno odzivanje na grožnjo pandemije pomanjkljivo komuniciranje med zdravstvenimi institucijami	pandemija je množičen pojav, ko se v okolju pojavi nov povzročitelj nalezljive bolezni, s katerim se ljudje še nikoli nismo srečali in smo zato zanj bolj dovzetni. V kratkem času za gripo zboli veliko število ljudi. Virus gripe je zelo nalezljiv. Čeprav obstaja glede časa pojava, obsega in resnosti prihodnje pandemije gripe veliko neznank, je mogoče predvideti, da bi se bolezen zaradi intenzivnih migracijskih tokov in prometnih povezav lahko hitreje razširila po vsem svetu	pandemija gripe lahko močno ohromi delovanje ključnih državnih organov in vpliva na gospodarstvo, infrastrukturo, finančno stabilnost, ima mednarodni vpliv, povzroča veliko število zbolelih in umrlih. Pandemija gripe povzroči pomembne javnozdravstvene težave, saj lahko zboli od 25 do 45 odstotkov prebivalstva
Težave z zdravniško in bolnišnično oskrbo prebivalstva	težave z zdravstveno oskrbo povzročijo večje naravne nesreče, kot so požar, poplava in potres, namerne nesreče (vojna in bioterorizem), epidemije nalezljivih bolezni in zastrupitve ali zunanji razlogi: izpadi glavnih energentov, vode in medicinskih plinov	slaba organiziranost javnega zdravstva zastarela zdravstvena oprema kadrovska problematika	najbolj kritični objekti so: splošne bolnišnice, in sicer tiste, ki imajo urgentne, kirurške, internistične in rentgen oddelke; strojnice v teh bolnišnicah (zaradi dobave medicinskih plinov); laboratoriji in lekarne v teh bolnišnicah	treba je upoštevati čas in naravo dogodka. V primeru najbolj kritičnega možnega dogodka bi se lahko izvajale le nujne operacije, osnovna urgenca in operativa, dializa, takšno stanje bi imelo posledice za vse dobavitelje in na izpad delovne sile. Stroški vpliva na gospodarstvo bodo veliki, izguba zaupanja pacientov

Kritično pomanjkanje zdravil, serumov, cepiv in farmacevtskih proizvodov	zdravila, cepiva in tudi druge medicinske pripomočke je v večini primerov mogoče zagotoviti izključno z uvozom	neustrezno sklepanje dobavnih pogodb, malomarnost zaposlenih problematika javnega naročanja korupcijska tveganja	predvideti je treba izdajno mesto in opremo ter to tudi ustrezno zaščititi, če bi bilo treba v kratkem času pokriti veliko število ljudi. Potrebno bo mobiliziranje in usposabljanje ljudi ter zagotoviti njihovo dolgotrajnejšo razpoložljivost in operativnost	finančni stroški izdaje, razdeljevanja in hranjenja potrebnih zdravil, cepiva, krvi ter drugih medicinskih pripomočkov, kritičen odziv javnosti

Sektor financ (možni primeri):

Finančni sistem z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Odpoved podpore poravnalnega in/ali klirinškega agenta	virusi, socialni inženiring, avtomatizirane metode napada, strela, potres, vandalizem, sabotaža, terorizem, bombni napad, prekinitev dobave električne energije, prekinitev klimatiziranja prostorov, prekinitev komunikacijskih linij, prevelika delovna obremenitev sistema, škoda zaradi nepravilnega delovanja sistema ipd.	požar, poplava, eksplozija, neustrezno fizično, mehansko in tehnično varovanje, namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega	obsežno število scenarijev nevarnosti, saj so plačilni sistemi del gospodarske in finančne infrastrukture, ki omogoča prenos denarnih sredstev in finančnih inštrumentov, izvajalci so organizirane kriminalne združbe	ni podpore poravnalnega in/ali klirinškega agenta več kot 4 ure, visoka finančna škoda, izguba zaupanja javnosti
Nedelovanje celodnevne poravnave vrednostnih papirjev preko KDD	virusi, socialni inženiring, avtomatizirane metode napada, naravne nesreče	namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega	obsežno število scenarijev nevarnosti saj se preko zakladniških računov omogoča normalno delovanje države, preko plačilnih instrumentov, ki jih	velik vpliv na poslovanje države, visoka gospodarska škoda, izguba ugleda mednarodne in domače javnosti

			zagotavljajo predvsem banke in hranilnice pa poslovanje gospodarstva in prebivalstva	
Pomanjkanje gotovine v obtoku	naravne nesreče (potres, požar, žled, poplave ipd.) nedelovanje bančnih avtomatov zaradi izpada dobave elektrike	neučinkovito doziranje bankomatov zmanjašanje dvigov gotovine v bankah	zaradi višje sile se na določenem območju države za določen čas pojavi pomanjkanje gotovine v obtoku	vpliv na ugled Banke Slovenije in evrosistema, nemirni odziv javnosti
Napad na depotno banko	organizirana kriminalna združba izvede napad	sodelovanje zaposlenih pri napadu (izdaja podatkov)	napad na trezor depotne banke, napad na bančni prevoz gotovine	izguba gotovine, možnost poškodovanja zaposlenih ali smrtna žrtev, višji zavarovalni stroški, materialna škoda, odškodninske tožbe, izguba zaupanja komitentov

Sektor varovanja okolja (možni primeri):

Varstvo okolja z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Večji problemi pri proizvodnji, predelavi ali shranjevanju nevarnih snovi in kemikalij	naravne nesreče predstavljajo najhujšo grožnjo, saj na uničujoče in zelo obsežno delovanja narave ni mogoče vplivati, zato so lahko posledice večletne ali stoletne (kontaminacija zemlje in podtalnice)	malomarnost zaposlenih nerealna varnostna navodila pomanjlljiva zaščitna oprema nerealni načrti zaščite in reševanja počasno odzivanje na izredne dogodke	najbolj kritični objekti so z vidika ogrožanja skladiščne zmogljivosti (cisterne), v katerih se shranjujejo večje količine kemičnih snovi. Sledijo cevovodi (vključno z vsemi ventili), po katerih se znotraj proizvodnih obratov pretakajo kemične snovi	v primeru izpusta bo največja neposredna in posredna škoda na okoliškem prebivalstvu in industriji, možne so tudi smrtne žrtve; negativni učinek na javnost

Večji problem pri kopičenju, separaciji, ekstrakciji, zajemu stranskih produktov, uničenju in razredčenju nevarnih kemičnih snovi	nenamerna – tehnološka ogrožanja imajo praviloma zaradi sistemsko vgrajenih zaščitnih ukrepov sorazmerno majhne lokalne posledice	zaradi vnetljivosti in eksplozivnosti snovi, ki se uporabljajo pri proizvodnji in predelavi kemikalij prihaja do relativno velikega števila požarov	zaradi višje sile ali malomarnosti zaposlenih nastane okoljski problem, delovna nesreča ali požar predstavljata najbolj verjeten način ogrožanja	za dalj časa degradirano okolje, vpliv na zdravje ljudi, visoki materialni in finančni stroški, velik odmev v javnosti

Sektor informacijsko-komunikacijskih omrežij in sistemov (možni primeri):

Informacijska in komunikacijska podpora z viri nevarnosti	**Zunanje nevarnosti**	**Notranje nevarnosti**	**Scenarij nevarnosti**	**Posledice**
Nedelovanje računalniške infrastrukture	povečanje računalniške medsebojne povezanosti predstavlja znatno tveganje za računalniške sisteme. Prav tako tudi dostopnost, če pa ta ni ustrezno nadzorovana, omogoča storilcem kaznivih dejanj motnje delovanja z oddaljenih lokacij za nevarne ali zlonamerne namene, vključno z goljufijo, krajo ali sabotažo. Možne so tudi okvare strojnega ali programskega izvora, namerno ali nenamerno ogrožanje	namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega površno ocenjevanje informacijkih tveganj zastarela informacijska infrastruktura šibko avtonomno napajanje z električno energijo ni rezervne lokacije za delo informacijske službe v krizi neredne in nedosledne varnostne kopije tveganja z zunanjim upravljkavcem računalniškega omrežja in informacijskega sistema	naravne nesreče (lahko tudi antropogene nesreče, ki ne izhajajo iz same informacijsko-komunikacijske tehnologije, lahko pa jo ogrožajo); namerna ogrožanja (terorizem, informacijski napadi, zlonamerno delovanje zunanjih ali notranjih dejavnikov); nenamerna – tehnološka ogrožanja (človeške napake, zlasti ko gre za avtomatizirane procese). Možen je računalniški napad na vozlišča omrežja, povezave med vozlišči, mednarodne povezave in povezave do drugih ponudnikov	zanesljiva in zmogljiva infrastruktura je osnova za uspešno zagotavljanje storitev. V primeru izpada vse programske opreme škoda ni predstavljiva (zlom borze, nedelovanje bankomatov, finančnih transakcij ipd.). V primeru nedelovanja interneta, kjer večina aktivnosti gospodarstva temelji na spletnih aplikacijah, predstavlja veliko ranljivost centrov vodenja, ogrožena je dostopnost do podatkov. Velika gospodarska škoda in izguba zaupanja uporabnikov

Nezagotavljanje mobilnih telekomunikacij	izpad delovanja komunikacijskih centrov, nadzornih centrov, nedelovanje mednarodnih central, strežnikov, baznih postaj, radijskih povezav	namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega nerealna ocena tveganj v eletronskih in mobilnih komunikacijah prešibka kapaciteta baznih postaj neupoštevanje problemov zasičenosti v kriznih okoliščinah povzročanje namernih ali nenamernih izadov mobilnih omrežij	zaradi višje sile in/ali nezakonitih dejavnosti mobilni telekomunikacijski sistemi in naprave ne delujejo	finančni stroški, odškodninske tožbe zaradi kršenja pogodb, izguba zaupanja uporabnikov, vpliv na mednarodni ugled države
Vdor v informacijski sistem	avtomatizirane metode napada hekerski, krekerski in vohunski vdori v informacijaki sistem prisluškovanje in prestrezanje občutljivih poslovnih informacij virusi, črvi in drugi zlonameni vdori	namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega vrzeli v sistemu zaščite lastnega informacijskega omrežja premalo znanja in zavedanja informacijskega menedžmenta o obvladovanju tveganj prepočasno posodabljanje strojne in programske opreme	preko spleta vdor v informacijski sistem	stroški večdnevnega nedelovanja državne uprave in posameznih podjetij, vpliv na zaupanje uporabnikov

Finančni sistem z viri nevarnosti	Zunanje nevarnosti	Notranje nevarnosti	Scenarij nevarnosti	Posledice
Odpoved računalniškega komunikacijskega sistema SWITH	virusi, socialni inženiring, avtomatizirane metode napada, strela, potres, vandalizem, sabotaža, terorizem, bombni napad, prekinitev dobave električne energije, prekinitev klimatiziranja prostorov, prekinitev komunikacijskih linij, prevelika delovna obremenitev sistema, škoda zaradi nepravilnega delovanja sistema ipd.	požar, poplava, eksplozija, neustrezno fizično, mehansko in tehnično varovanje, namerno ali nenamerno ogrožanje poslovanja s strani zaposlenega	obsežno število scenarijev nevarnosti, saj ja ta sistem osnova finančne infrastrukture, ki omogoča prenos denarnih sredstev, izvajalci so organizirane kriminalne združbe	ni poravnave v sistemih TARGET2-Slovenija in TARGET2-Securities, visoka finančna škoda, izguba zaupanja mednarodnih trgov in uporabnikov

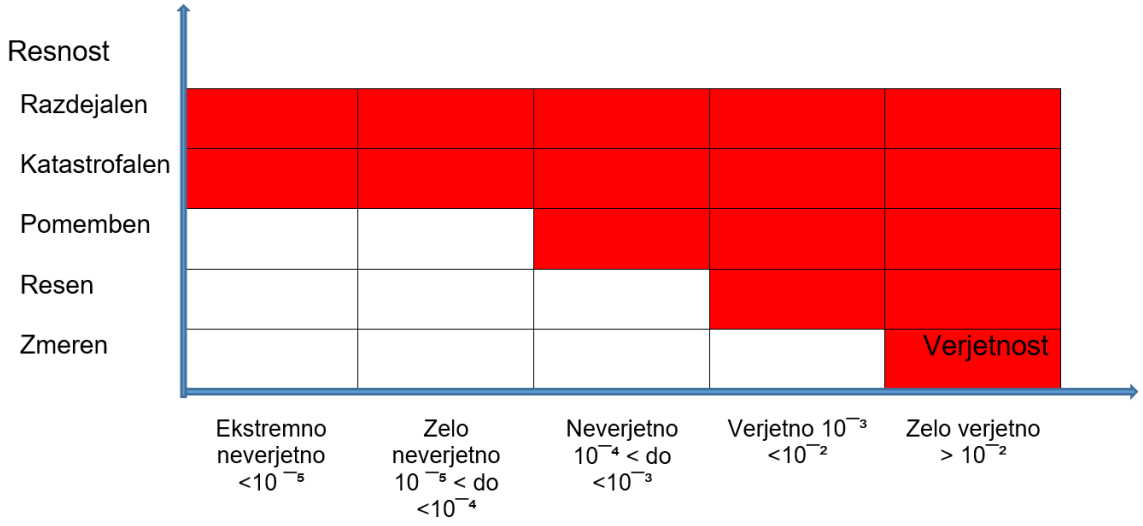
4.3.1.3 Ocena tveganih scenarijev (3. KORAK)

Ocena tveganih scenarijev je izdelana na podlagi kriterijev možne škode v primeru izrednega dogodka (Tabela 10) in resnosti ter verjetnosti izrednega dogodka (Tabela 11)

Tabela 10: Tabela škode (smiselno prirejeno po MOSAR)

Človeška življenja	Materialna škoda
Več kot eden mrtev	Popolno uničenje
Eden mrtev	Škoda z ustavitvijo sistema
Težje poškodovani	Škoda z delno ustavitvijo sistema
Lažje poškodovani	Manjša materialna škoda
Brez poškodb	Brez materialne škode

Tabela 11: Matrika scenarijev (smiselno prirejeno po MOSAR)



Resnost ogrožanja se nanaša na razdejalni, katastrofalen, pomemben, resen ali zmeren učinek. Verjetnost se nanaša na ekstremno neverjetno (en primer na sto tisoč primerov), zelo neverjetno (en primer na sto tisoč primerov do en primer na deset tisoč primerov), neverjetno (en primer na deset tisoč primerov do en primer na tisoč primerov), verjetno (en primer na tisoč primerov do en primer na sto primerov) in zelo verjetno (en primer pod sto primeri).

4.3.1.4 Analiza in rangiranje tveganih scenarijev (4. KORAK)

Iz Tabele 11 se prenesejo scenariji iz rdeče cone in se jih analizira s pomočjo kazalcev v Tabeli 12.

Tabela 12: Ocena kritičnosti - okvir najslabših možnih scenarijev (NMS)

Opis najslabšega možnega scenarija (NMS)	Vpliv na poslovni cilj	Vpliv na zaupanje uporab.	Vpliv na finančna sredstva	Verjetnost dogodka	Obrazložitev ocene	Končni produkt
NMS 1						
NMS 2						
NMS 3						
NMS 4						
NMS 5						
NMS n						

Najslabšim možnim scenarijem se določi oceno ogroženosti. Kot pomoč pri ocenjevanju ogroženosti lahko služijo spodnji kazalniki, ki določajo vpliv na poslovne cilje, zaupanje javnosti in finančni vpliv. Analiza scenarijev je najpogosteje uporabljana metodologija ocenjevanja tveganj, žal pa obstajajo tudi določene omejitve. Metodologija namreč zahteva opredelitev razumnega nabora različnih scenarijev. Samostojno tveganje je na splošno odvisno od posameznikove presoje (povezana je z osebnostnimi lastnostmi ocenjevalca, motivi, percepcijo, znanjem ipd.). Izkušnje iz prakse kažejo, da je težko natančno oceniti verjetnost posameznega scenarija, kar je omejitev te metode.

Kazalniki vpliva na poslovne procese so lahko: poslovni proces je deloma ohromljen, procesa ni mogoče izvesti, proces vpliva na druge procese in jih upočasnuje, proces vpliva na druge procese in jih onesposoblja ipd.

Kazalniki vpliva na zaupanje so lahko: zaupanje splošne javnosti, zaupanje strokovne javnosti, zaupanje lastnika, zaupanje vodstva sektorja KI, ustreznost informiranja ipd.

Kazalniki finačnega vpliva so lahko: brez škode, škoda je manjša od 50.000 EUR, je med 50.000 in 500.000 EUR, škoda je med 500.000 in 5.000.000 EUR, in škoda je večja od 5.000.000 EUR ipd.

Verjetnost izrednega dogodka je odvisna od njegove pogostosti, motivacije zaposlenih, spretnosti in znanj zaposlenih, sledljivosti poslovnih procesov, stroškov izrednih dogodkov in časa njihovega trajanja, kompleksnosti poslovnih procesov, odpornosti sistema na izredne dogodke, kompleksnosti zunanjega okolja ipd.

Drevo odpovedi

Za lažjo preglednost analize tveganja se uporablja tudi drevo odpovedi. Drevo odpovedi (ang. Fault Tree Analysis) predstavlja deduktiven pristop za analizo dogodkov (vzrokov), ki vodijo v odpoved sistema. Za identifikacijo vzrokov za odpoved se uporabljajo Booleanova algebra (2003) in logični diagrami. Pri tem se postavlja vprašanje »Kaj je napaka in kaj okvara?«. Vsaka okvara je napaka, vsaka napaka pa ni nujno okvara.

Potrebno se je zavedati, da je omenjeni pristop samo eden od možnih, ki pa ga zaradi določenih prednosti procesa predlagamo v tem delu.

Prednosti drevesa odpovedi:

- obravnava vzporedne, odvečne ali alternativne poti odpovedi,
- omogoča poiskati možne vzroke za odpoved, ki niso bili predvideni,
- zelo uporabno orodje za osredotočeno analizo, kjer je analiza zahtevana za enega ali dva glavna rezultata.

Slabosti:

- vsaka odpoved zahteva svoje drevo odpovedi,
- težko je analizirati kompleksne sisteme,
- različni ocenjevalci lahko razvijejo za isti problem različna drevesa, kar pomeni tudi različen rezultat analize,
- isti dogodek se lahko pojavi v različnih delih drevesa, kar povzroča začetne probleme.

Postopek izdelave drevesa odpovedi je naslednji:

- definicija sistema,
- izbor glavnega dogodka,
- priporočljivo je slediti logično pot od ideje do izvora,
- ugotovitev dogodkov, ki lahko direktno povzročijo uresničitev glavnega dogodka.

Postopek omogoča identifikacijo osnovnih vzrokov za odpoved, in sicer:

- spremljanje in nadzorovanje varnega delovanja kompleksnega sistema,
- identificiranje vpliva človeških napak,

- minimiziranje in optimiziranje virov,
- pomaga razumeti, kako popraviti oziroma preprečiti napake.

Dostikrat se je težko odločiti, kaj je odpoved in ali je posamezen del sistema odpovedal. Nekateri delijo odpovedi glede na:

- vzrok: napačna uporaba, inherentna slabost opreme,
- čas: nenadna odpoved, počasna degradacija,
- stopnja: delna odpoved, popolna odpoved,
- katastrofalna: odpoved je nenadna in popolna; degradacija: odpoved je postopna in delna.

Primarna odpoved se zgodi, če oprema odpove pri pogojih za katere je bila predvidena, sekundarna odpoved pa se zgodi, če oprema odpove pri pogojih za katere ni bila predvidena. Pri komandni odpovedi oprema sicer deluje, vendar v napačnem času ali na napačnem kraju. Pasivne odpovedi se nanašajo na komponente kot so nosilci mehanskih obremenitev, aktivne odpovedi pa so aktivne komponente, ki prispevajo k funkciji sistema na dinamičen način.

Sestava drevesa odpovedi:

- drevo odpovedi prestavlja logični model relacij med odpovedjo in njenimi vzroki – osnovnimi dogodki, ki do nje pripeljejo,
- vrhnji dogodek v drevesu predstavlja neželen dogodek – odpoved,
- pod dogodkom odpovedi se nahajajo vmesni dogodki, v listih pa se nahajajo osnovni dogodki – vzroki,
- logične relacije med dogodki so predstavljene z uporabo logičnih simbolov - logičnih vrat.

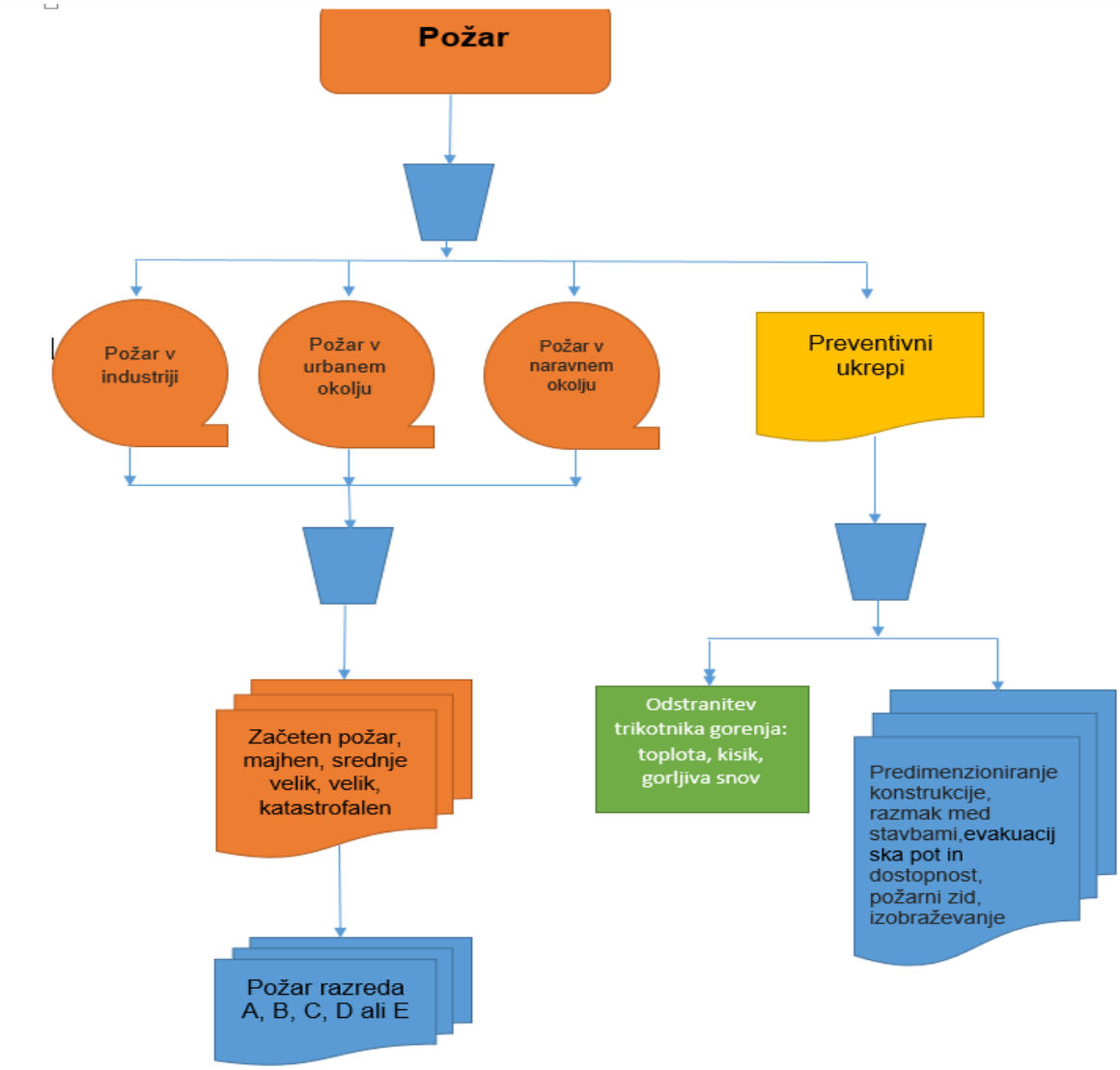
Proces analize drevesa odpovedi je prikazan na sliki 42.

Slika 42: Proces analize drevesa odpovedi (interni vir ICS)

Relacije med odpovedjo (dogodek na vrhu) in dogodki se modelira - prikaže z uporabo logičnega diagrama, ki se imenuje drevo odpovedi. Dogodkom na dnu drevesa se lahko pripiše verjetnosti nastopa dogodka, na podlagi katerih je mogoče pridobiti verjetnost pojava dogodka odpovedi.

V enostavnem primeru je verjetnost za odpoved odvisna od vira nevarnosti in od časa.

Nabor posledičnih dogodkov je prikazan na sliki 43 z drevesom dogodkov za primer požara.



Slika 43: Drevo dogodkov za primer požara (interni vir ICS)

4.3.1.5 Ocena sredstev za preprečevanje tveganj (5 KORAK)

Na zaključku uporabe MOSAR se je treba odločiti o načinih odpravljanja ali obvladovanja tveganj**.** Na tej stopnji je treba razmisliti o naslednjem:

- ali je mogoče tveganja odpraviti,
- če to ni mogoče, kako je mogoče tveganja obvladovati, da ne bodo ogrožala neprekinjeno poslovanje sistema,
- zagotoviti ustrezna finančna sredstva in kadre.

Pri preprečevanju in obvladovanju tveganj je treba upoštevati naslednja splošna načela**:**

- izogibanje tveganjem,
- zamenjava nevarnega tveganja z nenevarnim ali manj nevarnim,
- obvladovanje tveganj pri viru,
- uvajanje kolektivnih varnostnih ukrepov ima prednost pred individualnimi varnostnimi ukrepi,
- prilagajanje tehničnemu napredku,
- prizadevanje za izboljšanje ravni varnosti v sistemu.

Naslednji korak je vzpostavitev preventivnih ali varnostnih ukrepov**.** Pomembno je, da se v postopek vključijo pristojni zaposleni ali njihovi predstavniki. Za učinkovito izvajanje je med drugim treba sestaviti načrt, ki določa:

- ukrepe, ki se bodo izvajali,
- kdo bo kaj storil (pooblastila vodstva) in kdaj,
- do kdaj mora biti naloga opravljena,
- pomembno je, da ima za izvajanje ukrepov za odpravljanje ali preprečevanje tveganj prednost pred drugimi nalogami.

Z določitvijo posameznih kategorij scenarijev znotraj Tabele 11 (Matrika scenarijev) se določi način odzivanja (ukrepanja) na določene scenarije. Scenariji v beli barvi se nahajajo v področju dovoljene tolerance do tveganja. Tveganje je potrebno spremljati, odziv na tveganje je v pristojnosti nižje organizacijske enote sistema.

Scenariji v rdeči barvi predstavljajo tveganje z najvišjo prioriteto (predstavljeni v Tabeli 13), ki jih je potrebno v najkrajšem možnem času obravnavati pri vodstvu upravljavca KI in sprejeti ukrepe ter postopke za zmanjševanje tveganja (kaj, kdo in kdaj).

Tabela 13: Scenariji »rdeče cone« (interni vir ICS)

Opis scenarija	Poslovni proces	Vzrok	Dogodek	Trenutni vpliv na proces, zaupanje in finance	Verjetnost	Načrt rešitve (kaj, kdo, kdaj)	Ciljni vpliv na proces, zaupanje in finance	Verjetnost	Opombe

Najprimernejša strategija obvladovanja tveganja:

- podpira dolgoročne poslovne cilje sistema,
- zagotavlja poslovno in javno »preživetje« po težkih posledicah izrednega dogodka,
- na najbolj varčen način poskrbi, da se škoda povrne najhitreje ter v največji možni meri,
- zagotavlja optimalno razmerje med nadzorom tveganja, zadrževanjem tveganja in prenosom tveganja,
- sprejem tveganj, ko so koristi večje od stroškov.

4.4 FMEA (FAILURE MODE AND EFFECTS ANALYSIS - METODOLGIJA ANALIZE MOŽNIH NAPAK IN ŠKODLJIVIH POSLEDIC)

Za dokončanje drugega celovitega segmenta metodološkega pristopa, kot nadaljevanje metodologije MOSAR, smo se odločili za uporabo metodologije analize možnih napak in škodljivih posledic (FMEA - Failure Mode and Effects Analysis). Omenjena metodologija bo uporabljena za korake od 6-10, ki bodo podrobno prikazani in obrazloženi v nadaljevanju. Uporabniki storitev sistema so zahtevni in pričakujejo visoko stopnjo zanesljivosti poslovanja.

V sistemu je potrebno premisliti, kako doseči te cilje. Medtem ko je bilo v preteklosti dovolj, da se sistem osredotoči na preizkušanje in analiziranje poslovanja kot primarni metodi za zagotavljanje visoke zanesljivosti, sedaj to ni več dovolj, saj lahko to traja predolgo in je predrago. FMEA je orodje, ki pomaga pri zajemu znanja iz izkušenj strokovnjakov.

Treba je zagotoviti visoko kakovost in zanesljivost poslovanja že v zgodnjih fazah razvoja sistema. Najprej se je treba osredotočiti na problem preprečevanja, ne pa zgolj na reševanje problemov in predvidevanje virov nevarnosti, ki lahko privedejo do problemov poslovanja. Uporaba metode FMEA (analiza načina in učinka okvar) lahko predvidi in prepreči težave ter pomaga sistemu doseči visoko zanesljivost storitev in proizvodov. Pri tem je potrebno upoštevati omejitveni faktor, da slaba presoja, neustrezne in nepopolne informacije lahko vodijo k slabim odločitvam.

FMEA se uporablja že več desetletij in ima dolgo zgodovino kot metoda za podporo proizvodnih procesov, storitev in vzdrževanja. Je učinkovita, preventivna, timsko orientirana in sistematična analiza napak sistema. Obsega interdisciplinarne postopke, sistematično in funkcijsko obravnavanje, preprečevanje napak, kreativno razmišljanje in kritično ocenjevanje.

FMEA je pogosto prvi korak sistema v študiji njegove zanesljivosti. To vključuje pregled komponent, sklopov in podsistemov, kjer se lahko pojavijo okvare in analiza njihovih vzrokov ter učinkov. Za vsako komponento, okvaro in posledično učinke na preostali del sistema, je potrebno beleženje v poseben delovni list FMEA. Obstajajo številne različice takšnih delovnih listov, primer bo predstavljen v nadaljevanju.

Obstaja nekaj različnih vrst FMEA, kot so:

- funkcionalna,
- oblikovna,
- procesna.

Prednosti FMEA so:

- zagotavlja dokumentiran in sistematičen način za izbiro modela z veliko verjetnostjo uspešnega poslovanja in varnosti,
- dokumentira enotno metodo ocenjevanja možnih odpovedi mehanizmov, okvar, napak in njihov vpliv na delovanje sistema. Seznam načinov okvare je razvrščen glede na resnost učinkov sistema in verjetnost pojava nevarnosti,
- zgodnje prepoznavanje točk odpovedi delovanja in vmesnik za težave, ki so lahko ključnega pomena za neprekinjenost poslovanja,
- učinkovita metoda za oceno učinka predlaganih sprememb načrta in / ali operativnih postopkov,
- podlaga za tekoče odpravljanje težav in za spremljanje ter odkrivanje napak,
- merilo za načrtovanje stresnih in drugih testov.

Pomanjkljivosti FMEA so lahko:

- postopek ocenjevanja je lahko dolgotrajen. Zapleteni, kritični (tudi tvegani) poslovni procesi imajo veliko elementov, ki jih je treba raziskati, pri čemer je treba preučiti vse možne kompleksne vrste izpadov poslovanja sistema,
- težave pri ugotavljanju virov nevarnosti zaradi več kot ene napake. Težko je upoštevati učinek večkratnih načinov izpada elementov sistema za določitev kombiniranih virov nevarnosti,
- težave pri iskanju vseh načinov izpadov. Večina izpadov je bila že raziskana, identificirani so njihovi različni načini odpovedi, novejša oprema pa bi bila lahko manj dokumentirana,
- zahteva veliko količino podatkov, različne stopnje napak za vsako postavko morajo biti znane,

- kompleksnost (težavnost, obsežnost postavk) FMEA lista, ki ga je težko pripraviti, prebrati in razumeti.

Elementi sistema obsegajo strojno opremo (stroji, naprave, surovine, merilni sistemi, poslovni prostori ipd.), strojno, programsko in komunikacijsko opremo ter zaposlene (vodstvo, sistemski in razvojni inženirji, operaterji, vzdrževalci, podporne službe ipd.). Sistem je prikazan je na sliki 44.

Slika 44: Elementi sistema (prirejeno po SIST EN 60300-3-4:2008)

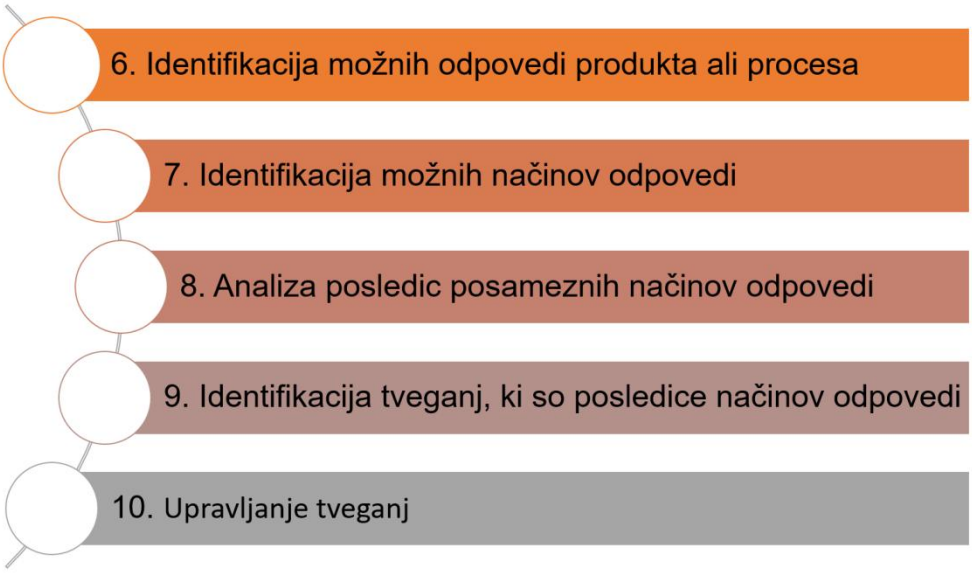
FMEA je treba posodobiti ob:

- začetku novega poslovnega cikla (nov proizvod / proces),
- spremembah pri oblikovanju,
- novih pravnih in tehničnih predpisih,
- povratnih informacijah uporabnikov, ki kažejo na določen problem.

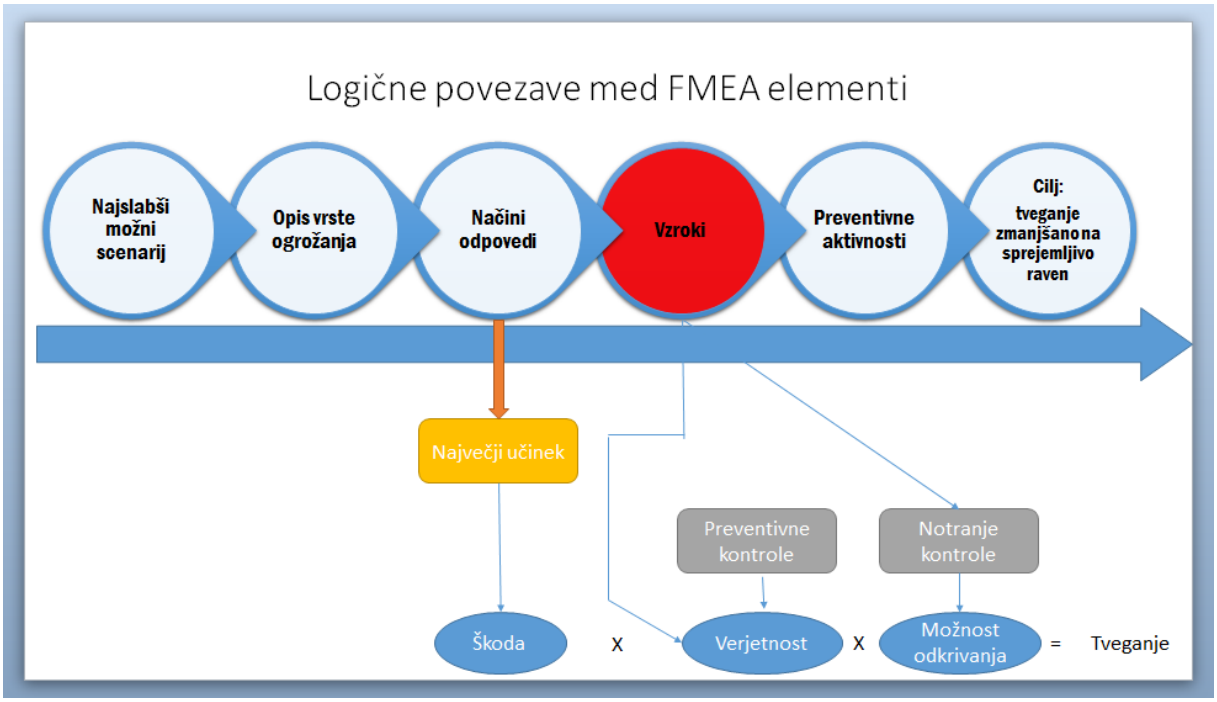
Koraki metodologije:

- identifikacija vseh možnih odpovedi (napak, motenj) produkta ali procesa,
- identifikacija tipičnih načinov odpovedi,
- analiza posledic posameznih načinov odpovedi,
- identifikacija tveganj, ki so posledice načinov odpovedi, ▪ upravljanje tveganj.

Koraki metodologije so shematsko prikazani na sliki 45, na sliki 46 pa logične povezave med FMEA elementi.



Slika 45: Koraki metodologije FMEA (prirejeno po standardu SIST EN 60300 - 3-4)



Slika 46: Logične povezave med FMEA elementi (SIST EN 60300 - 3-4)

Logične povezave se nanašajo na identifikacijo najslabših možnih scenarijev, opis vrste ogrožanja, način in vzroke odpovedi, oceno tveganja, preventivne aktivnosti (ukrepi in postopki, odgovornosti, roki izvedbe aktivnosti), ponovno oceno izvedenih aktivnosti in oceno tveganj. Vse navedeno je treba opisati in analizirati na delovnem listu FMEA (prikazan na sliki 47).

Primer FMEA delovnega lista

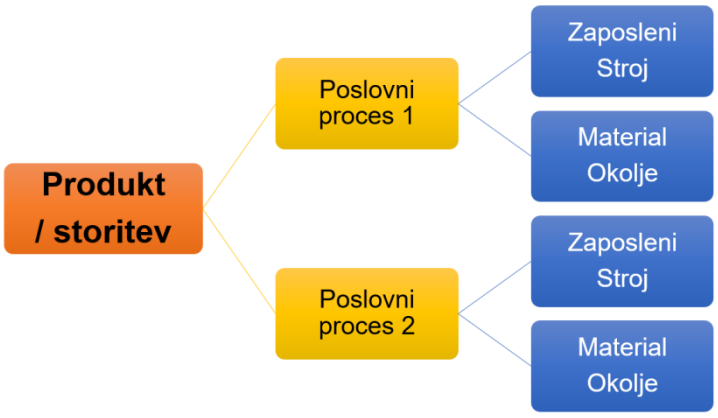
Proces /produkt: _____ Številka FMEA: _____

Projektna skupina: _____ Datum izdelave: _____

Vodja skupine: _____ Datum revizije: _____

FMEA ref.	Element (proces, produkt)	Možni način odpovedi	Možni vzrok odpovedi	Učinek odpovedi	Ocena resnosti (S)	Ocena verjetnosti (O)	Ocena odkrivanja (D)	Tveganja na ravni RPN=SxOxD	Predlagani ukrepi	Odgovoren	Izvedene aktivnosti	Ponovna ocena S, O, D, RPN

Slika 47: Primer delovnega lista FMEA (prirejeno po standardu)



Slika 48: Struktura produkta /storitve (interni vir ICS)

V delovnem listu FMEA je pomembna postavka razdelava strukture produkta / storitve. Struktura se nanaša na številne poslovne procese (od poslovni proces 1 do poslovni proces n), vsak poslovni proces pa je razčlenjen na zaposlene, strojno opremo, uporabljen material in delovno okolje.

4.4.1 Opis korakov za izvedbo metodologije

6. korak:

- prepoznavanje funkcij sistema (kaj je cilj poslovanja sistema, kaj uporabniki pričakujejo od sistema ipd.). Opravi se temeljit pregled produkta / procesa v ločenih podsistemih, elementih, delih, sklopih in opredeli njihove funkcije.

7. korak:

- osnova je identifikacija načinov odpovedi (najbolj kritične scenarije iz rdeče cone po metodi MOSAR se prenese v delovni list FMEA),
- za vsako funkcijo se identificira način odpovedi poslovanja (npr. možni načini okvar / napak),
- sledi identifikacija posledic načinov odpovedi sistema, z njim povezanih podsistemov, procesov, povezanih procesov, izdelkov, storitev, uporabnikov. To so potencialni učinki odpovedi. Vprašanje je »Kaj se zgodi, ko se pojavi ta napaka?« Za vsak način odpovedi se določi možni vzrok (npr. sistemska napaka, degradirano delovanje, odpovedi stanja sistema, takojšnji učinek ipd.),
- določi se lokalni učinek odpovedi, naslednja višja raven učinka in končni učinek.

8. korak:

- oceni se resnost posledic Si (ang. Severity of effects), pogostost pojava Oi (ang. Occurence of failures) in možnost pravočasnega zaznavanja (odkrivanja) odpovedi Di (ang. Detection of failures),
- ugotovi se, kako resen je vsak učinek, z določevanjem Si, Oi, Di, za vsak način odpovedi,
- vsak način in kriterij ocenimo z ocenami od 0 do 10 na podlagi spodaj naštetih dejavnikov resnosti, pogostosti in pravočasnosti zaznavanja načinov odpovedi,
- ocena resnosti (S) je ocenjena na lestvici od 1 do 10, kjer 1 je nepomembna in 10 je katastrofalna (prikazana je v Tabeli 14). Če ima odpoved več kot en učinek, se v delovni list FMEA vpiše samo najvišja ocena resnosti.

Ocena resnosti (S)

Osnovno vprašanje je: »Kaj bi lahko šlo narobe?«. Določi se resnost odpovedi (v najslabšem primeru neželeni končni učinek). Te učinki se nanašajo na ugotovitve uporabnika ali izkušnje s področja funkcionalne okvare sistema. Primeri teh učinkov so npr.: popolna izguba funkcije, omejena učinkovitost delovanja, prepozno ali neredno delovanje ipd. Resnost se obravnava

na osnovi stroškov in / ali izgube življenja. V nadaljevanju je v Tabeli 14 prikazana tipična razvrstitev. Možne so tudi druge klasifikacije.

Tabela 14: Kriteriji za resnost odpovedi (prirejeno po standardu)

Ocena	Učinek	Kriterij za resnost (škodo)
1	Ni	Ni učinka. Brez ustreznih učinkov na zanesljivost in varnost sistema
2	Nepomemben	Zelo majhen vpliv na sistem. Zelo majhen učinek, brez poškodb, le posledice pri vzdrževanju sistema
3	Zelo nizek	Majhen vpliv na lastnosti sistema
4	Nizek	Majhen učinek na lastnosti sistema, proizvod ne potrebuje popravila
5	Srednji	Proizvod potrebuje popravilo. Manjši učinek, nizka škoda, lahko lažja telesna poškodba
6	Pomemben	Nekatere funkcije proizvoda ne delujejo
7	Velik	Sistem morda ni več operativen
8	Zelo velik	Sistem ni več operativen
9	Resen	Odpoved povzroča nevarnost za ljudi in premoženje. Kritična škoda (povzroča izgubo delovanja primarne funkcije, izgubo varnostne rezerve, hude poškodbe, možna smrt)
10	Zelo resen	Nevarnost za ljudi in premoženje nastopi brez opozorila. Katastrofalen učinek (storitev / produkt je nedosegljiv, popolno nevarno delovanje, mogoče več smrti)

- za vsak vzrok se določi verjetnost pojavljanja napake (O). Pojav je ocenjen na lestvici od 1 do 10, kjer je 1 zelo malo verjeten in 10 je neizogiben (prikazan v Tabeli 14). V delovni list FMEA se vpiše rating za vsak vzrok,
- za vsak element se opredeli tudi trenutni proces notranje kontrole. To so testi, ukrepi, postopki ali mehanizmi, ki so vzpostavljeni do končnega uporabnika storitev. Te kontrole lahko preprečijo vzrok in zmanjšajo verjetnost, da se bo napaka zgodila ali odkrivajo napake preden je prizadet uporabnik.

Ocena verjetnosti (O)

Osnovno vprašanje je: »Zakaj bi se zgodila napaka?«. Verjetnost pojava se oceni s pomočjo izračunov, statističnih podatkov, analize podobnih procesov, dobre prakse in raznih odpovedi, ki so bile dokumentirane v preteklosti. Vzrok za napake je treba obravnavati kot slabost sistema. Vse možne vzroke odpovedi naj se dokumentira in tako se ustvari baza podatkov. Vzroki so lahko: človeška nezanesljivost, napake pri ravnanju, proizvodnja, ki povzroča napake, obrabe, napačni tehnični algoritmi, nepravilno delovanje ipd. V nadaljevanju je v Tabeli 15 prikazana tipična razvrstitev.

Tabela 15: Kriteriji za verjetnost odpovedi (prirejeno po standardu)

Ocena	Pogostost odpovedi	Kriteriji za verjetnost
1	<= 1×10^{-6} 1 na 1.000.000	Skoraj nemogoča odpoved, napaka odpravljena z notranjo kontrolo
2	1×10^{-5} 1 na 100.000	Zelo majhna verjetnost odpovedi
3	1×10^{-4} 1 na 10.000	Majhna verjetnost odpovedi
4	4×10^{-4} 1 na 25.000	Relativno nizka verjetnost odpovedi
5	2×10^{-3} 1 na 500	Srednje nizka verjetnost. Občasna napaka
6	1×10^{-2} 1 na 100	Srednje visoka verjetnost odpovedi
7	4×10^{-2} 1 na 25	Visoka verjetnost odpovedi
8	0,2 1 na 10	Ponavljanje odpovedi
9	0,33 1 na 3	Zelo visoka verjetnost odpovedi
10	>= 0.55 1 na 2	Odpoved skoraj neizogibna, nova tehnologija, sistem brez zgodovine

- za vsak kontrolni ukrep se določi oceno odkrivanja (ugotavljanja), z oznako D. S tem se ocenjuje, kako dober je sistem vodstvenega nadzora in notranjih kontrol ter ali je možno odkriti vzrok za odpoved preden je prizadet uporabnik. Odkrivanje je ocenjeno

na lestvici od 1 do 10, kjer 1 pomeni zelo učinkovit nadzor in 10 pomeni slab nadzor (ali nadzora sploh ni!), kriteriji so prikazani v Tabeli 15),

- ali je odpoved povezana s kritično značilnostjo? Kritične značilnosti so meritve ali kazalniki, ki odražajo skladnost poslovanja s predpisi,
- izdelava prioritetne lestvice odprav vzrokov odpovedi glede na urejeni padajoči vrstni red načinov odpovedi glede na vrednosti faktorja tveganja RPNi.

Ocena odkrivanja (D), detektabilnosti

Sredstva ali metode, s katerim odkrijemo napake, lahko trajajo nekaj časa. To je pomembno za nadzor vzdrževanja (razpoložljivost sistema) in je še posebej pomembno za več scenarijev okvar. Ta vključuje mirujoče načine (npr. sistem neposrednega učinka) ali latentne napake (npr. poslabšanje kvalitete materialov, kot so kovine ipd.). Potrebno je pojasniti kako je napake ali vzrok odkril operater ali vzdrževalec ali samodejni odzivni sistem. V nadaljevanju je v Tabeli 16 prikazana tipična razvrstitev.

Tabela 16: Kriteriji za oceno odkrivanja (prirejeno po metodologiji)

Ocena	Ocena odkrivanja napak
1	Skoraj zanesljiva detekcija, napako odkrije operater ali vzdrževalec
2	Zelo visoka verjetnost detekcije, napaka odkrita z avtomatsko kontrolo
3	Visoka verjetnost detekcije
4	Srednje visoka verjetnost detekcije
5	Srednja verjetnost detekcije
6	Nizka verjetnost detekcije
7	Zelo nizka verjetnost detekcije
8	Malo verjetna možnost detekcije
9	Zelo nizka verjetnost detekcije, napako je težko odkriti
10	Absolutno nemogoča detekcija, brez trenutne detekcije ali se ne analizira sistem

Mirovanje (nedelovanje) sistema ali latentna doba

Sistem lahko deluje:

- normalno,
- nenormalno, ko je sistem pokvarjen ali ne deluje stalno,
- napačno, zaradi okvare ali odpovedi indikatorja (npr. instrumenta, zaznavanje naprave, vizualne ali zvočne opozorilne naprave).

Povprečen čas, ko je napaka lahko neopažena, je npr.:

- nekaj minut (računalniki),
- pol do ene ure, pregled strojev in naprav,
- ena do dve uri (pregled distribucije),
- dve do štiri ure (informacija upravljavcu KI),
- delovni dan (opozorilo javnosti),
- nekaj dni (remont),
- teden (resna okvara sistema).

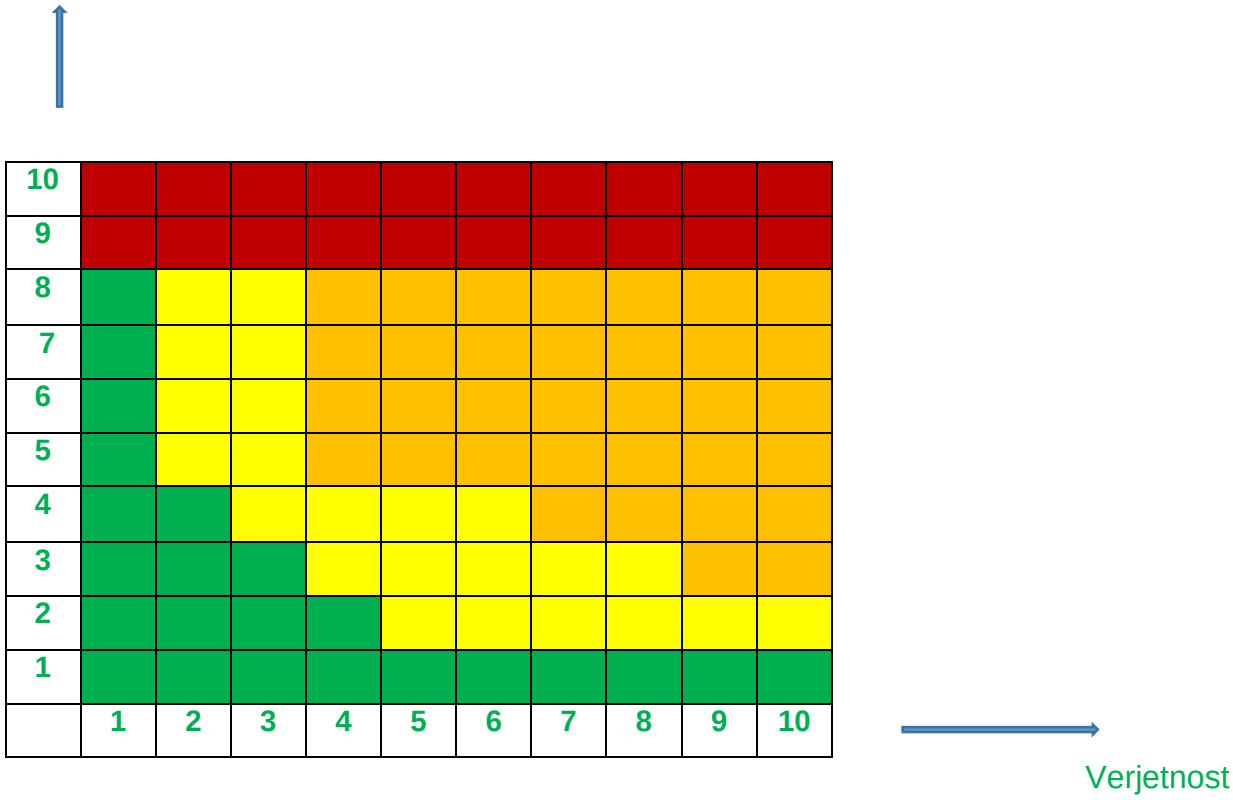
- izračuna se faktor tveganja RPNi (angl. Risk Priority Number) = Si x Oi x Di (zmnožek treh ocen: RPN = resnost x pogostost x odkrivanje),
- faktor tveganja RPN uredimo po velikostnem redu, kjer je skupni RPN = ∑{i=1..n} RPNi,
- če je ocena faktorjev S,O ali D med 1 in 2, to pomeni manjši vpliv, med 9 in 10 pa večji vpliv na sistem, pri čemer je $RPN_{max} = 10 \times 10 \times 10 = 1000$, $RPN_{min} = 1 \times 1 \times 1 = 1$,
- **prag za KI je RPN 10, prag za nekritične sisteme pa je RPN 100,**
- ključni vprašanji: ali so načini odpovedi z vrha liste resnično kritični za zanesljivost produkta / procesa in ali je finančni vložek za odpravo načinov odpovedi z vrha liste sprejemljiv?

9. korak:

- prepoznavanje priporočenih aktivnosti iz navodil in dobre prakse. Ti ukrepi in postopki se nanašajo na zmanjšanje ali odpravo vzrokov odpovedi, so lahko načrt ali proces sprememb, dodatni sistemi in kontrolni sistemi za izboljšanje detekcije odpovedi. Upošteva se tudi, kdo je odgovoren za te aktivnosti in ciljni datumi zaključka,
- ko so aktivnosti izvedene, se v določenem časovnem obdobju po zaključku implementiranja preventivnih ukrepov in postopkov ponovno vrednoti O, S in D in nove RPNs,

- po prvi oceni RPN se za kritične poslovne procese izvedejo preventivni in korektivni ukrepi. Po njihovi implementaciji se postopek FMEA v razumnen roku ponovi z izdelavo novega delovnega lista FMEA.
- **Matrika tveganj**

V matriko tveganj (prikazana na sliki 49) se vnesejo rezultati faktorjev tveganja RPNi.



Slika 49: Matrika tveganj FMEA (smiselno prirejeno po standardu SIST EN 60300 - 3-4)

Legenda:

Kritično tveganje | Visoko tveganje | Srednje tveganje | Nizko tveganje

Izvajalec metodologije FMEA:

- s sklepom vodstva se ustanovi FMEA projektna skupina, ki je organizirana multidisciplinarno, npr.: razvojnik, tehnolog, kontrolor, delovodja, IT predstavnik, varnost, skupno 4 do 6 zaposlenih,
- različni člani v skupino prinašajo različna znanja,
- vsaj vodja ekipe mora praktično dobro poznati koncept FMEA analize,

- zaželjene lastnosti vodje ekipe: sklepanja kompromisov, vodenja projektne dokumentacije, generiranja idej in vodenja »možganske nevihte« (ang. brainstorming), prenašanja konkretnih rezultatov v ustrezne končne predstavitve.

Projektna usmerjenost:

- uporaba FMEA metodologije ni trajen proces, vodi se projektno, kar pomeni, da ima predviden časovni začetek in konec ter je časovno omejena,
- pred začetkom je potrebno določiti: časovni termin trajanja z začetkom in koncem, ekipo in njeno vodjo, finančna sredstva za izvedbo, cilje, ki jih predstavlja analiza odpovedi in predlogi popravkov z njihovo implementacijo ter ustrezne ostale vire (kontaktne osebe, materiale ipd.),
- način podajanja rezultatov.

Delovni list FMEA je prikazan na sliki 47.

10. korak: Upravljanje tveganj

Strokovnjaki poudarjajo, da je popolna varnost in zaščita skoraj neuresničljiva naloga. Vendar se najvišji možni stopnji varnosti in upravljanja s tveganji s primerno izbiro ustreznih zaščitnih ukrepov, postopkov, aktivnosti ter z njihovo izvedbo v praksi lahko zelo približamo.

Upravljanje s tveganji se ne nanaša samo na skladnost s predpisi, temveč tudi na način razumevanja poslovanja organizacije, kar ima dolgoročen vpliv nanjo. Tveganje lahko predstavlja priložnost za zagotovitev konkurenčne prednosti, upravljanje tveganj pa je odločilno za uspešno poslovanje in je v središču pozornosti vodstva.

Prednosti upravljanja s tveganji so zlasti:

- boljše upravljanje s sredstvi,
- hitrejša odzivnost na notranje in zunanje spremembe,
- večja verjetnost doseganja poslovnih ciljev,
- boljše razumevanje ključnih tveganj in njihovih posledic,
- večja pozornost vodstva na najpomembnejša vprašanja poslovanja,
- manjša možnost nastanka izrednih dogodkov,
- večja pozornost je namenjena temu, da se poslovni procesi izvajajo na pravilen način,
- večja je verjetnost za izvajanje pobud za izboljšave,
- boljša informiranost o prevzemanju tveganj in odločanju.

Upravljanje tveganj se nanaša na tri večje sisteme:

- tehnični sistem (v obliki opreme, strojev, naprav ipd.),
- pravni in organizacijski sistem (v obliki internih splošnih aktov, ki določajo postopke in način delovanja),
- izvajanje posameznih poslovnih procesov v smislu razmerja posameznik - posameznik in posameznik - oprema.

Upravljanje tveganj je kompleksna naloga, najširši niz tveganj pokrivajo zlasti naslednji ukrepi in aktivnosti:

- ocenjevanje sposobnosti sistema za neprekinjeno poslovanje in v primeru potrebe tudi krizno upravljanje. Določitev posebnih zmogljivosti in dejavnosti za upravljanje tveganj in temeljnih zmogljivosti, povezanih z zaščito, preprečevanjem, ublažitvijo, odzivanjem in okrevanjem sistema.
- izgradnja in vzdrževanje zmogljivosti. To vključuje tudi najboljši način za uporabo omejenih virov za izgradnjo zmogljivosti. Pomembna je prioriteta uporabe virov za reševanje največje verjetnosti izrednega dogodka ali najvišje posledice virov nevarnosti.
- načrtovanje zagotavljanja zmogljivosti. Pripravljenost na izredne dogodke vključuje in vpliva na celotno družbo. Pomembno je, da so aktivnosti sistema usklajene z drugimi organi in organizacijami.
- preverjanje zmožnosti sistema. Pomembno je, da posamezne aktivnosti sistema delujejo kot je načrtovano. Koristno je sodelovanje v vajah, simulacijah ali drugih dejavnostih, ki bodo pomagale prepoznati pomankljivosti načrtovanja in zmogljivosti. Navedene aktivnosti tudi pomagajo prepoznati napredek k uresničevanju ciljev pripravljenosti.
- pregledovanje in posodabljanje. Pomembno je, da se redno in tekoče pregledujejo ter posodabljajo vse zmogljivosti, viri in načrti.
- vodenje dela. Zaposlene je potrebno stalno in na razne načine tekoče informirati o vseh relevantnih vprašanjih, zlasti pa jim povedati, kaj od njih pričakujemo in v čem se nanje zanesemo (zaupamo). Kadar zaposleni ne storijo, kar od njih pričakujemo, je to veliko pogosteje posledica napake v medsebojni komunikaciji, kot pomanjkanje motivacije, volje ali namena.
- vodstveni nadzor. Vodstvo oziroma od njih pooblaščeni zaposleni mora nadzirati in opazovati odklone zaposlenih od izvajanja predpisanih ukrepov ter postopkov in pravočasno ustrezno reagirati na to. Vodstveni nadzor je najbolj splošen, fleksibilen in učinkovit od vseh nadzorov.
- motivacijski dejavniki. Poudarek naj bo na organizacijski kulturi sistema in na naslednjih motivacijskih dejavnikih, ki naj jih vzpodbuja vodstvo: ustrezne delovne

razmere, dobra obveščenost o dogodkih, ustrezna plača in druge materialne ugodnosti, dobri odnosi s sodelavci, možnost vplivanja na soodločanje pri delu, s prizadevanjem pri delu in dodatnim strokovnim izobraževanjem, povečanje možnosti za napredovanje (gradnja kariere zaposlenih), več samostojnosti pri delu, izboljšanje pogojev za bolj ustvarjalno delo, povečanje občutka varnosti (socialne in fizične) pri delu, ustrezen odnos do nadrejenih, dosledno uveljavljanje kodeksa zaposlenih.

- interni splošni akti. Glede na posamezna področja tveganj je potrebno izdelati ustrezne interne splošne akte, v katerih se določijo splošna in posebna pravila za upravljanje tveganj. O tem je potrebno informirati in usposobiti zaposlene,
- znanje in upravljanje informacij. Potrebno je učinkovito upravljati znanje zaposlenih in pridobivanje informacij, ki naj zagotavljajo verodostojne, zanesljive in pravočasne podatke,
- kombinacija potrebnih organizacijskih in tehničnih ukrepov. »Utrjevanje možnih tarč« (bolj tveganih in kritičnih poslovnih procesov dejavnosti) sistema, omejevanje dobička in povečanje tveganja možnih storilcev izrednih dogodkov je tesno povezano z ustrezno kombinacijo potrebnih organizacijskih in varnostno - tehničnih ukrepov ter postopkov.
- nadzor nad dostopom. Čim bolj selektivno in dosledno je potrebno omejiti dostop do premoženja sistema večje vrednosti. Pri tem je potrebno izhajati iz podmene, da čim bolj je premoženje vredno, tem več stopenj organizacijskega, mehanskega, tehničnega in fizičnega nadzora naj bo nad tem in tem manj zaposlenih ali drugih oseb, ki bodo imeli dostop do njega.
- načrtovanje nepredvidenega. Načrtovati in vaditi je potrebno odzive zaposlenih na razne scenarije možnih izrednih dogodkov. Nedvomno velja, da se bodo zaposleni toliko učinkoviteje soočili z možnimi izrednimi dogodki in njihovimi posledicami, kolikor bolj bodo nanje pripravljeni. Del teh priprav je tudi ustrezno načrtovanje in vadba primerov.
- tveganja je treba razvrstiti po pomembnosti in odločiti: ali se ugotovljeno tveganje sprejme, poskuša ublažiti, prenese na zavarovalnico ali pogodbenega izvajalca, ali se ukine dejavnost, ki nastanek tveganja povzroča.
- ukrepi za upravljanje tveganj so: preprečevalni–preprečiti nastanek tveganja, popravljalni–popraviti nezaželene rezultate, ki so že nastali, usmerjevalni–preprečiti uresničitev tveganja tako, da se za izvajanje vsake dejavnosti zahteva upoštevanje določenih postopkov in odkrivalni–ugotoviti ali se je tveganje že uresničilo.
- upravljanje s tveganji mora biti pregledno, usklajeno, splošno sprejeto, vodje morajo dobro poznati in razumeti svojo vlogo in odgovornosti glede tveganj, pri ugotavljanju

in ocenjevanju tveganj morajo sodelovati zaposleni, nosilci tveganj morajo prevzeti svojo odgovornost glede tveganj in sprejemati ustrezne ukrepe.

Strokovna podpora FMEA

Ob koncu predstavitve metodologije FMEA predstavljamo še štiri orodja za pomoč pri njeni realizaciji. To so:

- Systems2win v obliki excellovih tabel, ki je dosegljiv na http://www.systems2win.com/c/QuickStart/index.htm in http://www.systems2win.com/solutions/support.htm.
- najnovejši ameriški program za oceno tveganj: https://www.hawksightsrm.com/ HawkSight, ki zagotavlja svetovanje, programsko opremo in usposabljanje upravljavcev KI v ZDA (in po svetu, letnik 2018) ter preglednost stroškov upravljanja varnostnih tveganj. HawkSight programska oprema je kombinacija orodij za oceno tveganj, poročanje, grafični prikaz in je uporabnikom prijazna, omogoča hitro in tekoče odločanje v vedno bolj kompleksnem okolju.
- APIS-IQ računalniška programska oprema: FMEA in funkcionalno varnost - Software, ki temelji na uporabi nekaterih grafičnih orodij in metod. Je v pomoč pri izdelavi delovnega lista in zmanjšuje možnosti za manjkajoča pomembna področja tveganja. Dosegljiva je na https://www.apis-iq.com/.
- s standardiziranim in izvedljivim pregledom tveganje Silver Bullet pomaga sistematično prepoznavati in obravnavati vsa kritična področja, ki ogrožajo učinkovitost in zdravje KI. Celovit vpogled, intuitivna armaturna plošča in različni moduli Silver Bullet Tool predstavljajo številko na platformi za vse poslovne menedžerje in nosilce odločanja, ki želijo zmanjšati tveganja. Programska oprema je dosegljiva na https://www.silverbulletrisk.com/.

Register tveganj

Register tveganj je vzpostavljen na podlagi Politike upravljanja tveganja. Register tveganj vsebuje seznam prepoznanih tveganj v okviru procesa ocenjevanja tveganja. Vsako tveganje v registru opredeljujejo naslednji parametri:

- poslovni proces v okviru katerega je prepoznano tveganje,
- oznaka tveganja, ki je unikatna in je sestavljena iz zaporedne številke prepoznanega tveganja in skrajšane šifre poslovnega procesa, iz katerega primarno izhaja, ali na katerega primarno vpliva,

- naziv tveganja (opredeljenih v glavnih vzrokih za nastanek tveganja, opis razlogov za uresničitev tveganja),
- identifikacija glavnih razlogov (zaposleni, sistemi, upravljanje in procesi, zunanji dogodki),
- opredelitev vpliva tveganja, in sicer: na nedoseganje poslovnih ciljev, izgubo zaupanja in nedoseganje finančnih ciljev,
- določitev verjetnosti nastanka tveganja,
- območje tveganja, ki izhaja iz tolerančnega okvira iz Politike upravljanja tveganja:
    - belo območje - spremljanje tveganja, brez načrtovanih aktivnosti,
    - rdeče območje - pripravi se načrt za upravljanje tveganja, ki ga obravnava vodstvo upravljavca KI.
- v komentarju se poda informacija o obstoječih kontrolah, kontrolnih ciljih in utemeljitev ocene tveganja.
- Strategija obvladovanja tveganja se nanaša na:
    - izogibanje tveganju (odstranitev vzroka, zmanjšanje obsega poslovanja),
    - prenos tveganja (prenos tveganja na drugo pravno osebo, zavarovanje, pogodbeni izvajalec ipd.),
    - zmanjšanje tveganja (z ukrepi in postopki zmanjšamo verjetnost in/ali vpliv tveganja),
    - sprejem tveganja (verjetnost tveganja je zanemarljiva oziroma vpliv tveganja je majhen).

Za vsa tveganja iz rdeče kategorije je treba pripraviti načrt obvladovanja tveganja. Za preostala tveganja ukrepanje ni potrebno, razen v primeru, da se z ukrepom prepreči poslabšanje stanja oziroma, da se ohrani enaka raven tveganja.

Najprimernejša strategija obvladovanja tveganja:

- podpira dolgoročne poslovne cilje,
- zagotavlja poslovno in javno (medijsko) »preživetje« po težkih posledicah izrednega dogodka,
- na najbolj varčen način poskrbi, da se škoda povrne najhitreje ter v največji možni meri,
- zagotavlja optimalno razmerje med nadzorom tveganja, zadrževanjem tveganja in prenosom tveganja,
- sprejem tveganj, ko so koristi večje od stroškov.

Register izrednih dogodkov

Register izrednih dogodkov v organizaciji je vzpostavljen na podlagi Politike upravljanja tveganj. Register izrednih dogodkov vsebuje seznam ugotovljenih incidentov in škodnih dogodkov, ki so nastali v določenem obdobju. Vsak incident oziroma škodni dogodek v registru opredeljujejo naslednji parametri:

- oznaka izrednega dogodka, ki je unikatna in je sestavljena iz zaporedne številke te situacije in leta nastanka,
- podrobnosti izrednega dogodka, ki zajemajo navedbo naslednjih elementov:
  - datum nastanka,
  - okvirni čas nastanka,
  - organizacijska enota, v kateri se je zgodila ta situacija,
  - posledice - posledice so zaznane (dogodek je imel posledice na delo) oziroma posledice še niso zaznane (dogodek bi lahko imel posledice na delo organizacijske enote),
- opis izrednega dogodka zajema kaj se je zgodilo, koliko časa je trajalo in na kateri proces je vplivalo,
- vpliv, ki ga ima izredni dogodek na nedoseganje poslovnih ciljev, izgube zaupanja uporabnikov, lastnika in strokovne javnosti, finančnih ciljev. Pri tem se upošteva Politika upravljanja tveganja,
- opis glavnih vzrokov zajema kratek opis sprožilca škodnega dogodka ali izrednega dogodka. Pri tem se v pomoč in orientacijo upošteva Politika upravljanja tveganja. V poljih zaposleni, sistem, upravljalni in poslovni proces ter zunanje okolje, se s križcem označi, kaj je sprožilo dogodek,
- sprejeti ukrepi zajemajo kratek opis: (i) kakšni so bili takojšnji sprejeti ukrepi za reševanje nastalega dogodka; (ii) kakšni bodo dolgoročni ukrepi za zmanjšanje vpliva in/ali verjetnosti ponovnega nastanka dogodka; (iii) kakšna so glavna spoznanja, ki izhajajo iz opisanega dogodka.

4.5 MODEL ZBIRANJA PODATKOV ZA OCENJEVANJE RANLJIVOSTI, OGROŽENOSTI IN TVEGANJ

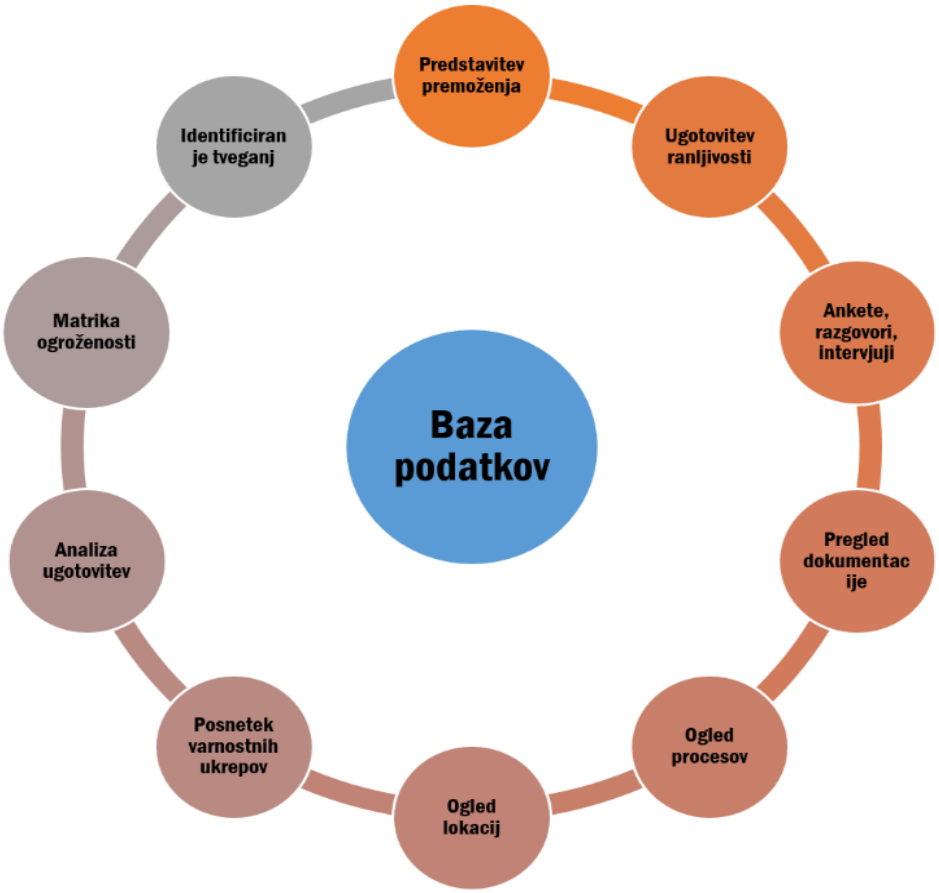
Vsak sistem je v določeni meri podvržen ranljivosti, še zlasti tisti, ki je neustrezno organiziran, ki ima neustrezno lastninsko strukturo in ki ga vodi neučinkovito vodstvo. Pri ugotavljanju ranljivosti gre za to, da se v sklopu presojanja in ocenjevanja delovanja, razvoja ali stagnacije ugotovijo šibke točke, ozka grla, vrzeli in pomanjkljivosti v organiziranosti

podjetja, v vodstvu, v poslovanju, v trženju proizvodov in storitev (obvladovanju tržnih tekmecev), v lastniški strukturi ter v poslovni politiki, varnostni kulturi in strategiji razvoja.

Pri tem se uporablja ena od metod tovrstnega ugotavljanja ranljivosti poslovnega sistema, in sicer t. i. SWOT analiza (ang. Strenghts, Weakness, Opportunities, Threats). Ta analiza pokaže na prednosti, slabosti, priložnosti in nevarnosti (grožnje) v procesu poslovanja določenega subjekta. Praksa je pokazala, da so ugotovitve in spoznanja iz SWOT analize koristna metoda ugotavljanja stopnje ranljivosti proizvodnih, poslovnih, logističnih, informacijskih, komunikacijskih in varnostnih procesov.

Za ocenjevanja ogroženosti uporabljamo model zbiranja podatkov v desetih korakih (prikazan na sliki 50) o stanju sistema z vidika varnosti (predstavitev premoženja sistema, ugotovitev ranljivosti sistema, zbiranje podatkov z anketami, razgovori, intervjuji, pregled pravne, poslovne in tehnične dokumentacije, ogled poslovnih procesov, ogled lokacij sistema, posnetek in analiza varnostnih ukrepov, analiza ugotovitev, izdelava matrike ogoženosti, identificiranje tveganj). Na ta način ustvarimo bazo podatkov, ki jih obdelamo z multivariantnimi statističnimi metodami in / ali s kvalitativnimi metodami, glede na obseg in strukturo podatkov.

Proces zbiranja podatkov se lahko izvede na dva načina. Prvi je, da podatke zberemo na podlagi dosegljive dokumentacije in razgovorov s pristojnimi zaposlenimi, drugi način pa je izvedba načrtovane raziskave, s katero izvedemo vse druge aktivnosti v procesu zbiranja podatkov. Prvi način je okrnjen način zbiranja podatkov, drugi način pa omogoča profesionalni pristop k ocenjevanju ranljivosti, ogroženosti in tveganj.



Slika 50: Proces zbiranja podatkov potrebnih za oceno ogroženosti in identificiranje tveganj (Vršec, 2009)

Nasveti za lažje prepoznavanje virov nevarnosti:

- preučiti vrste in oblike dolgoročnih nevarnosti za realizacijo strategije in neprekinjenega delovanja sistema,
- ugotoviti bolj zapletena ali manj očitna tveganja delovanja sistema, na primer tehnične, poslovne, organizacijske ali psihosocialne dejavnike tveganja,
- analizirati poročila o nezgodah in incidentih v sistemu in v panogi,
- pridobiti informacije iz drugih virov, na primer: navodil za uporabo opreme in strojev, podatkovnih listov proizvajalcev in dobaviteljev (risbe, skice, sistemske opise ali druga sredstva, ugotavljanje narave sistema), primere dobre prakse, spletne strani o varnosti in tveganjih, poročila državnih organov ali panožnih združenj,
- ugotoviti raven usposabljanja, izkušenj ali sposobnosti zaposlenih in pogodbenih izvajalcev,
- analizirati izpostavljenost drugih oseb nevarnostim, povezanih s sistemom, kjer je to mogoče razumno predvideti,

- upoštevati deontološke kodekse, pravne predpise in tehnične standarde.

Prepoznava virov nevarnosti je pomemben del ocene tveganja, ker tveganje, ki ni ugotovljeno, lahko ustvari znatno neznano tveganje. Znani so številni različni pristopi, ki so odvisni od kompleksnosti sistema, uporabne metode pa lahko vključujejo:

- uporabo intuitivne operativne, inženirske in varnostne presoje,
- preučitev specifikacij in pričakovanj sistema,
- anketiranje sedanjih ali nameravanih uporabnikov sistema in / ali operaterjev,
- posvetovalni kontrolni seznami,
- pregledovanje študij iz drugih podobnih sistemov,
- »brainstorming«.

Pri tem je treba upoštevati, da je tveganje možnost, velika ali majhna, da bodo uporabniki storitev sistema zaradi nastopa nevarnosti prizadeti in da bo nastala škoda. V nadaljevanju bo treba oceniti tveganje, ki ga predstavlja vsaka nevarnost. Razmislek zahteva odgovore na naslednja vprašanja:

- kako verjetno je, da bo nevarnost povzročila škodo,
- kako resna bo verjetno povzročena škoda,
- kako pogosta je realizacija nevarnosti.

Ocenjevanje tveganj je samo eden od segmentov upravljanja s tveganji v KI. Zato je nujno, da ocenjevanje tveganj obravnavamo v kontekstu celovitega upravljanja in obvladovanja tveganj. Potemtakem je že v fazi ocenjevanja tveganj treba razmišljati o tem, da bo treba določena tveganja prenesti na zavarovalnice, ki prevzamejo odškodninsko odgovornoet za nastale izredne dogodke in njihove posledice. Ker si brez prenosa določenih (recimo neobvladljivih) tveganj na zavarovalnice ni mogoče predstavljati celovitega upravljanja tveganj, predlagam, da večji del tega podpoglavje ostane v študiji.

4.6 OBVLADOVANJE TVEGANJ Z ZAVAROVANJEM PRI ZAVAROVALNICAH

Glede na to, da vsa tveganja ni možno obvladovati z organizacijskimi ukrepi, s fizičnimi in tehničnimi varnostnimi ukrepi ter z varnostno kulturo zaposlenih, je z vidika obvladovanja stroškov, finančnih škod in izgub, smiselno – poleg obveznega zavarovanja - uporabiti tudi zavarovalne storitve na področju prostovoljnega zavarovanja, ki ga nudijo vse zavarovalnice. Zavarovalnice za primerno zavarovalno premijo zavarujejo požarne, kriminalne, poslovne in druge rizike. Zavarovanje ekstremnih in visokih varnostnih rizikov sklenemo pri tistih zavarovalnicah, ki so se pripravljene pogajati o višini zavarovalnih premij. Gre namreč za

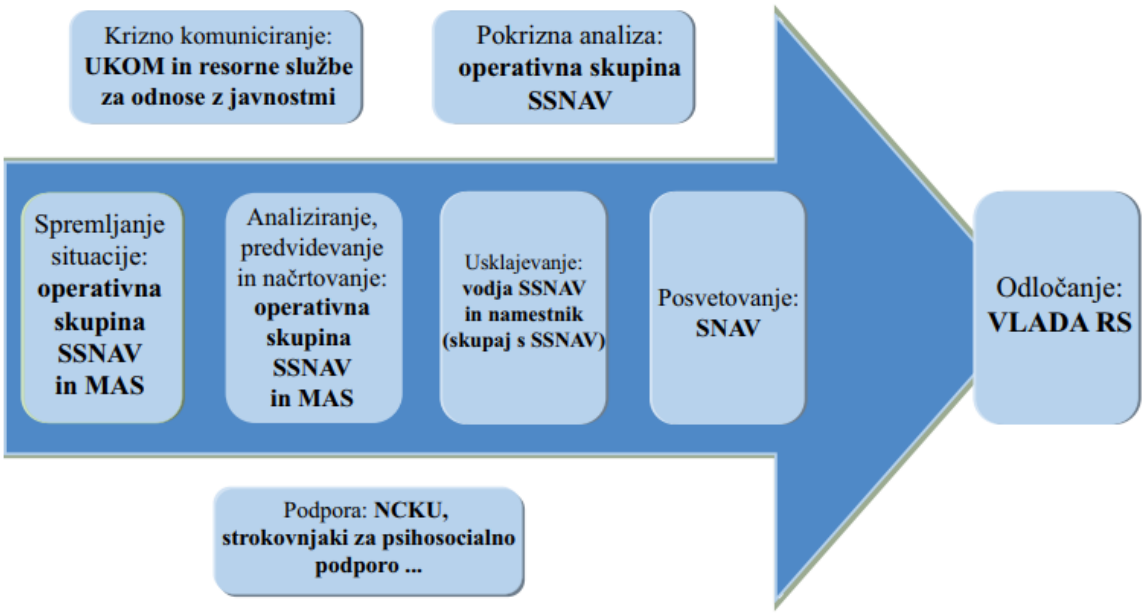
razne ugodnosti in popuste, ki jih lahko nudijo zavarovalnice, ko gre za učinkovito obvladovanje tveganj in za kakovostne varnostne mehanizme pri zavarovancu.

Obvladovanje tveganj z zavarovanjem je seveda velik (vsakoletni) strošek. Zato je vzpostavitev sistema in procesa celovitega obvladovanja tveganj koristno opravilo tistih odgovornih oseb, ki se v podjetju profesionalno ukvarjajo s pogajanji in sklepanjem pogodb z zavarovalnicami. Kajti z dokazljivim celovitim obvladovanjem tveganj, z dokazljivim integralnim varnostnim sistemom in s statistiko zniževanja izrednih dogodkov, ima podjetje odlična pogajalska izhodišča za proces postopnega (vsakoletnega) zniževanja zavarovalnih premij, ali vsaj zadrževanje premij na isti ravni.

4.7 KRIZNO UPRAVLJANJE IN NEPREKINJENO POSLOVANJE

Potreba po neprekinjenem delovanju KI je še posebej izražena v določenih kriznih situacijah. Zaradi navedenega je nujno, da skozi analizo ocenjevanja ogroženosti delovanja KI pravilno razumemo procese kriznega upravljanja in vodenja, vlogo ustreznih sistemskih subjektov v tem procesu in predvsem, da razumemo vlogo ter pomen procesa neprekinjenega poslovanja v Republiki Sloveniji in seveda vsaki posamezni organizaciji, ki upravlja KI. Na tem mestu je namen opozoriti na določene vidike, ki so nujno povezani z ocenjevanjem tveganja za nemoteno delovanje KI v Republiki Sloveniji. Kriza vedno predstavlja situacijo, kjer je čas za oblikovanje varnostnih politik in sprejemanje odločitev zelo omejen. Zaradi navedenega je potrebno v predhodnih fazah izvesti ustrezno pripravo določenih procesov, ki zagotavljajo, kasneje v času krize, neprekinjenost delovanja. Hermann (v Malešič, 2004) je odločevalsko krizo definiral kot situacijo, ki ogroža prednostne cilje odločanja, omejuje čas, ki je na razpolago za sprejemanje in izvajanje odločitev in s svojim pojavom preseneti odločevalce v organizaciji. Najbolj široko je definicijo krize opredelil Rosenthal s sodelavci (1989), ki je poudaril krizo kot resno grožnjo ključnim strukturam ter temeljnim vrednotam in normam družbenega sistema, ki pod časovnim pritiskom in v zelo negotovih razmerah, zahteva sprejemanje kritičnih odločitev. Beršnak in drugi (Beršnak in Ferlin, 2018:24) v nadaljevanju pojasnjujejo, da »kompleksna kriza namreč presega odzivne zmožnosti posameznih ministrstev in podsistemov sistema nacionalne varnosti ter terja usklajeno delovanje vseh organov, vendar ne presega odzivnih zmožnosti države in ne ogroža obstoja države, zaradi česar bi bila potrebna razglasitev vojnega ali izrednega stanja«. Obvladovanje kompleksnih kriz zahteva večinstitucionalni pristop in aktiviranje velikega števila akterjev ter virov na strateški in izvedbeni ravni, ki jih je treba med seboj uskladiti in voditi. Učinkovito odzivanje na krize lahko torej dosežemo le z določeno strukturo, ki zagotavlja usklajevanje kriznega odziva in druge nujne funkcije. Kot so že pred leti ugotovili strokovnjaki, je za

pravočasen odziv na kompleksne krize nujen enoten sistem kriznega upravljanja in vodenja na ravni vlade, ki zagotavlja vse funkcije kriznega upravljanja in vodenja (Beršnak in Ferlin, 2018:29)

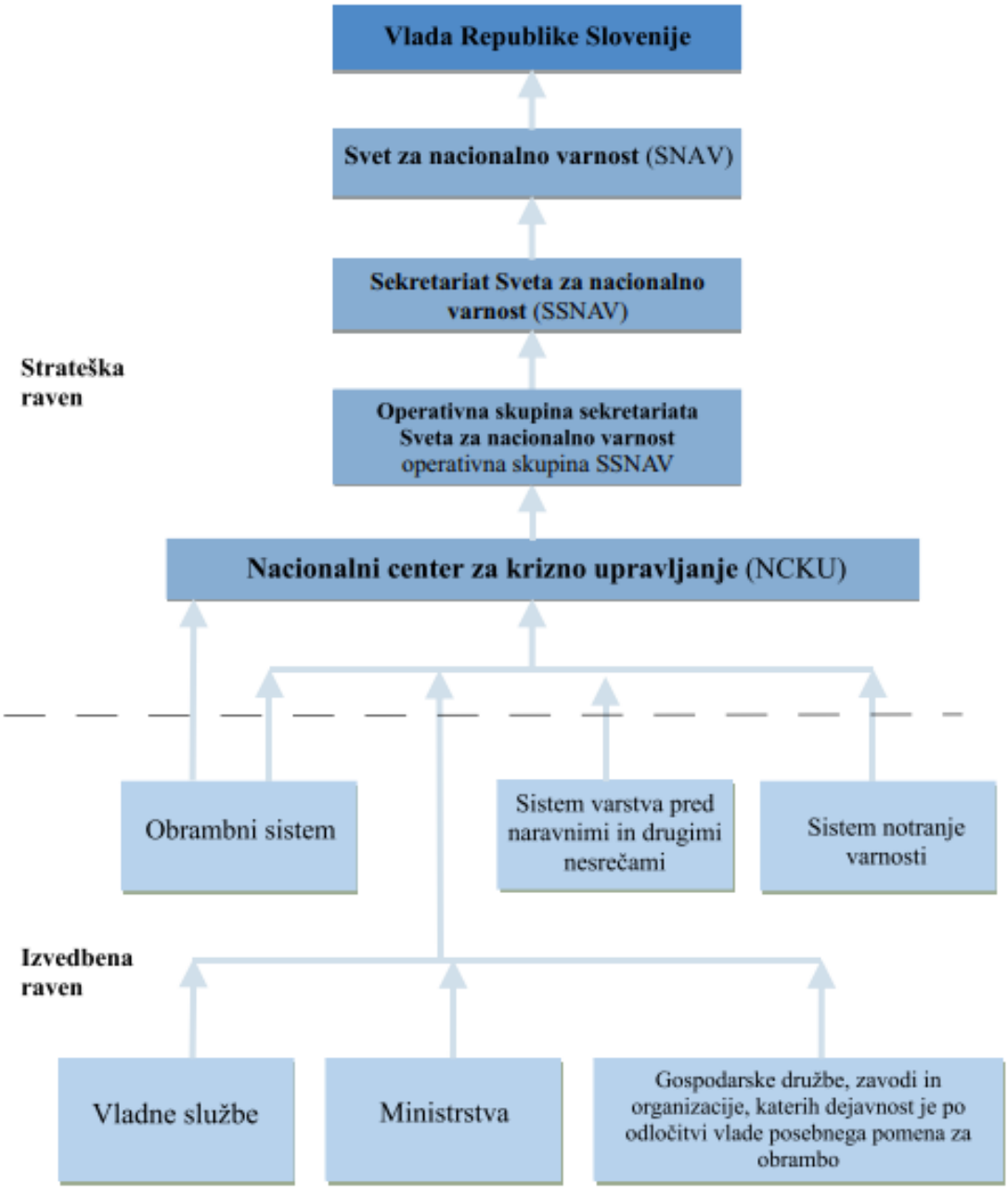


Slika 51: Nosilci funkcij kriznega upravljanja in vodenja (Beršnak in Ferlin, 2016)

V dopolnilo programskega pristopa povezanih načrtov za ocenjevanje tveganj, ki smo ga predstavili v sliki 15 dopolnjujemo podrobno obrazložitev strukture kriznega upravljanja in vodenja za zagotavljanjee vseh ključnih funkcij, ki so nujne za učinkovit krizni odziv. Pri tem se opiramo na opredelitev, ki sta jo ponudili Beršnak in Ferlin (2018: 29-30):

- Vlada RS sprejema odločitve,
- Svet za nacionalno varnost (SNAV) je posvetovalno telo Vlade,
- sekretariat Sveta za nacionalno varnost (SSNAV) podpira SNAV, po odločitvi Vlade RS pa v kompleksni krizi opravlja tudi naloge usklajevanja odziva na kompleksno krizo med ministrstvi, vladnimi službami in podsistemi sistema nacionalne varnosti ter pripravlja predloge ukrepov za odzivanje na kompleksno krizo,
- operativna skupina SSNAV je stalno telo, ki v omejenem obsegu deluje pri vodji SSNAV in v običajnih razmerah zagotavlja analitično in strokovno podporo delovanju SSNAV, spremlja situacijo na področju nacionalne varnosti, ocenjuje ogroženost, pripravlja metodologijo za pokrizno analiziranje ter izvaja dejavnosti, ki so potrebne za učinkovito delovanje teles kriznega upravljanja, po kompleksni krizi pa še usklajuje pripravo analize,

- Nacionalni center za krizno upravljanje (NCKU) zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje ter pripravlja redna poročila o stanju na področju nacionalne varnosti,
- medresorska analitična skupina (MAS) se aktivira ob pojavu kompleksne krize, v izrednih razmerah ali vojni in ob teh dogodkih zagotavlja analitično in strokovno podporo. Ocenjuje varnostne razmere ter potek dogodkov, pripravlja zbirne ocene stanja in prihodnjega razvoja dogodkov,
- krizno komuniciranje usklajuje Urad Vlade Republike Slovenije za komuniciranje (UKOM), z javnostmi pa v kompleksni krizi komunicirata predsednik vlade ali minister iz pristojnega ministrstva ter vodja SSNAV, ali njegov namestnik.



Slika 52: Struktura kriznega upravljanja in vodenja na ravni države v običajnih razmerah (Beršnak in drugi, 2016)

V tem okviru kriznega upravljanja, tudi skozi perspektivo zagotavljanja neprekinjenosti delovanja KI, ima NCKU izredno pomembno vlogo. Zaradi potrebnega razumevanja te vloge bomo v nadaljevanju podrobneje predstavili osnovne naloge NCKU. Naloge NCKU[16]:

[16] Uredba o kriznem upravljanju in vodenju ter Nacionalnem centru za krizno upravljanje, 2018.

- zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delovanje vlade ter teles kriznega upravljanja v kompleksnih krizah ter ob drugih pojavih ali dogodkih v državi oziroma v regionalnem ali mednarodnem okolju, ki lahko pomembno ogrozijo nacionalno varnost, in v drugih primerih, skladno s predpisi,
- zagotavlja informacijske in komunikacijske povezave za izmenjavo podatkov in informacij z ministrstvi, državnimi organi, vladnimi službami ter vsemi gospodarskimi družbami, zavodi in drugimi organizacijami, katerih dejavnost je po odločitvi vlade posebnega pomena za obrambo,
- pripravlja tedenska poročila o stanju na področju nacionalne varnosti za SSNAV in operativno skupino SSNAV na podlagi poročil, ki jih v NCKU posredujejo ministrstva in vladne službe, ki morajo v NCKU tedensko poročati o ključnih dogodkih in odzivanju s področja nacionalne varnosti,
- obvešča vodjo SSNAV o pojavu ali dogodku, ki lahko v kratkem času povzroči večje varnostno tveganje ali ogrožanje temeljnih družbenih vrednot. Omenjeni dogodek zazna NCKU ali organ, ki mora v NCKU ob pojavu takšnega dogodka posredovati izredno poročilo,
- zagotavlja administrativno-tehnično podporo SNAV, SSNAV in operativni skupini SSNAV,
- izvaja usposabljanje članov MAS za uporabo informacijskih in komunikacijskih orodij za delo v MAS,
- izvaja tudi naloge spremljanja in obveščanja v podporo odločanju v drugih primerih v skladu s predpisi,
- opravlja druge naloge skladno s predpisi, ki urejajo sestavo, delo in organizacijo vlade ter področje kriznega upravljanja in vodenja.

Državni načrt kriznega upravljanja in vodenja je razčlenjena zamisel delovanja strukture kriznega upravljanja in vodenja, njenih sestavnih delov, organov na izvedbeni ravni in drugih udeležencev ob konkretni kompleksni krizi. Temelji na opredelitvi mogočih kompleksnih kriz, oceni ogroženosti, predlogih za ukrepanje in razpoložljivih zmogljivostih. Naredi se za vsako kompleksno krizo posebej in obsega[17]:

- opredelitev kompleksne krize,
- **ažurno oceno ogroženosti za kompleksno krizo**,
- zmogljivosti za odzivanje,
- organizacijo dela za odzivanje,
- aktivnosti organa za odzivanje in obvladovanje krize,
- vključevanje sodelujočih subjektov ter usmeritve za obvladovanje kompleksne krize,

[17] Uredba o kriznem upravljanju in vodenju ter Nacionalnem centru za krizno upravljanje, 2018: 14. - 15. člen.

- opredelitev komunikacijskih poti in sredstev,
- pregled odgovornih oseb za usklajevanje ter vodenje odzivanja,
- načrt kriznega komuniciranja za konkretno kompleksno krizo.

Če to apliciramo na sistem zagotavljanja zaščite KI, je na vseh nivojih delovanja tega sistema analiziranje ogroženosti delovanja KI nujen proces.

V celotnem sistemu pa nikakor ne moremo spregledati pomena neprekinjenega poslovanja. Pri vzpostavljanju sistema neprekinjenega poslovanja je smiselno izhajati iz standarda ISO 22301, ki ga na kratko povzemamo v nadaljevanju.

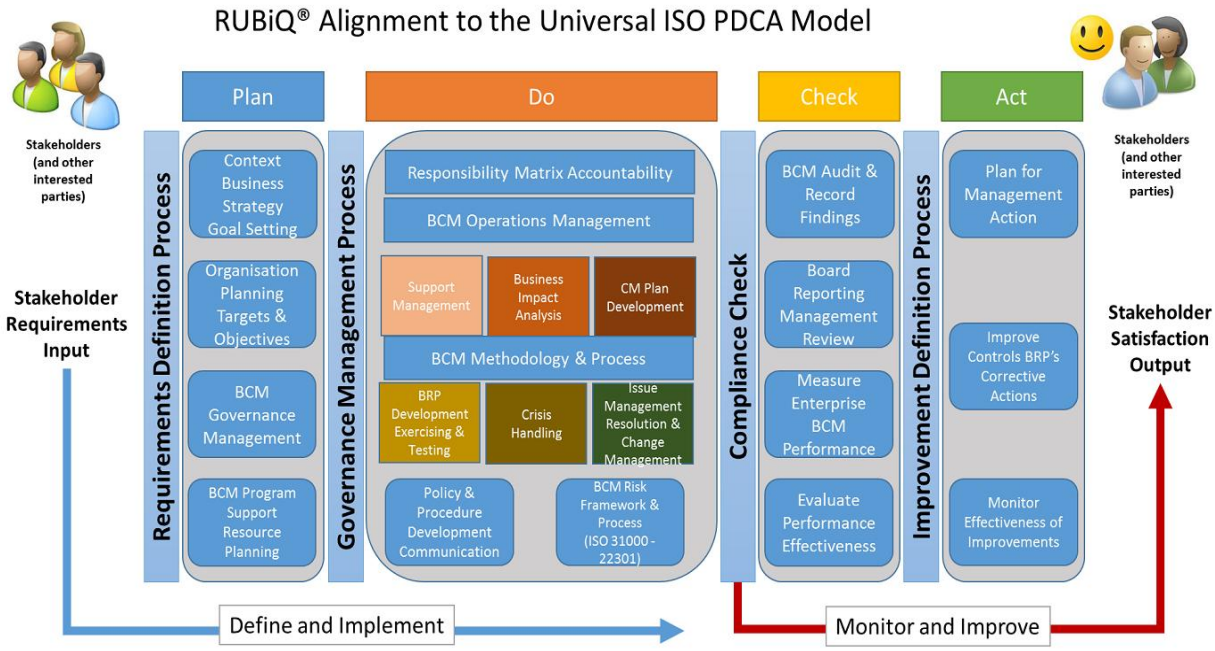
4.7.1 Sistem neprekinjenosti poslovanja po ISO 22301

Mednarodni standard ISO 22301 je bil razvit s strani ISO Tehničnega odbora in je bil prvič izdan 15.6.2012. Namen ureditve sistema neprekinjenega poslovanja po standardu ISO 22301 je, da je organizacija sposobna po incidentu nadaljevati z dobavo proizvodov in/ali storitev na sprejemljivi vnaprej določeni način. Upravljanje neprekinjenega poslovanja je definirano kot holističen pristop, ki identificira potencialne grožnje organizacije ter njihov vpliv na vse poslovne procese. Obenem sistem upravljanja neprekinjenega poslovanja predstavlja osnovni okvir za vzpostavitev sistema poslovne odpornosti na vsa tveganja, ki vplivajo na ugled, ključne nosilce organizacije, dodano vrednost in ostale pomembne elemente uspešnega in stabilnega poslovnega razvoja organizacije, ne glede na tip in obseg (povzeto po ISO 22301:2012).

Standard ISO 22301 je sestavljen iz medsebojno povezanih elementov, ki jih organizacija uporablja za sistem neprekinjenega poslovanja. V vseh elementih so vključeni ljudje, postopki, pravilniki, procesi, struktura in viri. V naslednjem podpoglavju bomo opredelili ključne faze ISO 22301, skozi PDCA model.

4.7.2 Metodologija ISO 22301 skozi PDCA model

Vsi mednarodni standardi imajo svoje zahteve in poudarke, ki so vse bolj usmerjeni k procesom in kupcem in zagotavljanju njihovega zadovoljstva. V zadnjem obdobju se kaže trend v smeri uvajanja več različnih standardov v organizacije (integracija standardov v enovit pristop), zato je mednarodna institucija za mednarodne standarde uvedla skupno metodologijo PDCA modela, z namenom lažje integracije različnih standardov znotraj posamezne organizacije. Zaradi navedenega je PDCA model vključen tudi v standard ISO 22301, kar je razvidno iz slike 53.

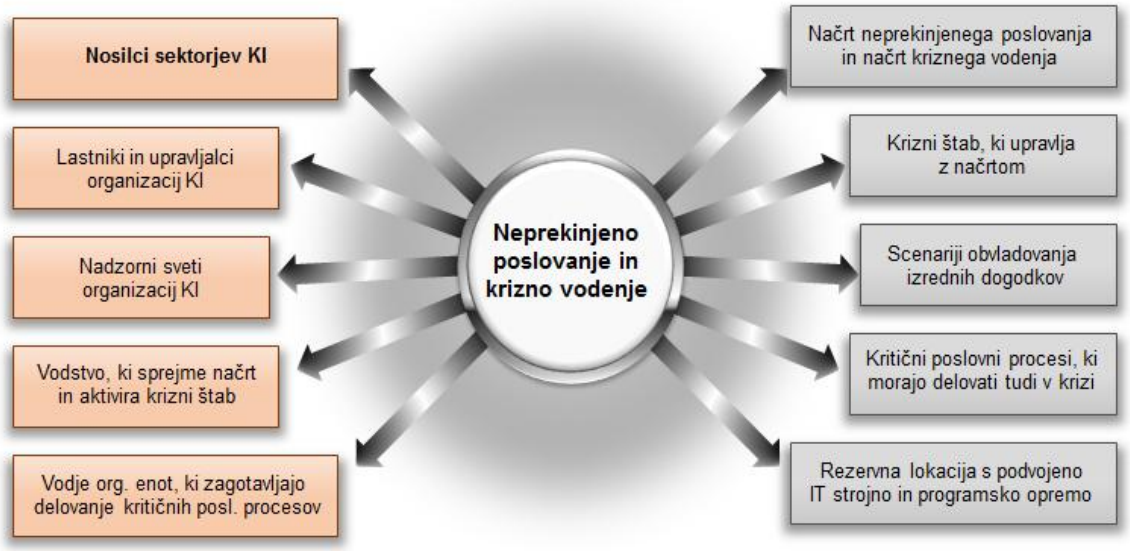


Slika 53: PDCA model za vpeljavo sistema neprekinjenega poslovanja[18]

Iz zgornjega PDCA modela vidimo, da fazo Načrtovanja (Plan) ISO 22301, zajemajo poglavja ISO 22301, od 4. do 7. (kontekst, vodstvo, načrtovanje, podpora), kjer je ključ izvajanje načrtovanja za vzpostavitev sistema neprekinjenega poslovanja. Sledi najpomembnejša, obsežna in zahtevna izvedbena faza (Do) ISO 22301, opredeljena skozi poglavje 8. (Izvedba analize tveganj in analiza poslovnih učinkov kot najpomembnejši del), kjer je poudarek na izvedbi raznovrstnih analiz in postopkov ter načrta neprekinjenega poslovanja. Tretja stopnja PDCA kroga za ISO 22301 pomeni ocenjevanje (Check), opredeljeno v poglavju 9., in nazadnje še četrta stopnja nadgradnje (Act), opredeljeno skozi poglavje 10. Izvedbena faza PDCA modela ISO 22301 predstavlja osrednji, najobsežnejši in krovni del sistema neprekinjenega poslovanja (Vršec/Vršec 2011, Marinčič, 2017).

V sistemu neprekinjenega poslovanja je ključnega pomena tudi odgovornost , ki je prikazana na sliki 54.

[18] Dosegljivo na http://www.rubi-q.com/rubiq-business-continuity-management)



Slika 54: Odgovornost za neprekinjeno poslovanje (interni vir ICS)

4.8 USPOSABLJANJE ZA UPRAVLJANJE TVEGANJ V KRITIČNI INFRASTRUKTURI

Vzpostavitev celovitega in stalnega procesa usposabljanja za upravljanje tveganj v KI (v smislu 10. čl. ZKI) je področje, ki ga bo treba razviti pri nosilcih in upravljavcih KI. Slediti je treba naslednjemu vprašanju: Katerim strukturam udeležencev usposabljanja, ki so deležniki v KI, je treba podati ustrezna znanja, raziskovalna spoznanja, izkušnje in dobro prakso, da bi znali in hoteli učinkovito obvladovati tveganja v svojih delovnih in poslovnih okoljih ter širše. Struktura udeležencev usposabljanja je naslednja:

- vodstvena struktura pri nosilcih KI - to so ministri in državni sekretarji, ki so odgovorni za delovna področja na katera spada KI,
- vodstvena struktura pri upravljavcih KI – to so direktorji in predsedniki uprav gospodarskih družb, zavodov, državnih organov in Banke Slovenije,
- strokovna struktura pri nosilcih in upravljavcih KI – to so od vodstva imenovane odgovorne osebe za sisteme varnosti in za upravljanje s tveganji,
- najširša operativna struktura – to so zaposleni na posameznih delovnih mestih v gospodarskih družbah, zavodih, državnih organih in Banki Slovenije.

Da bi se izognili nevarnosti podajanja neustreznih vsebin in nevarnosti podajanja prevelike ali preozke širine vsebin, je smiselno natančno določiti katere vsebine in v kolikšnem obsegu

potrebujejo posamezne strukture udeležencev usposabljanja. Ne navajamo konkretnih (sklopov) in časovnih okvirov vsebin usposabljanja za posamezne strukture udeležencev, ker osnovne vsebine že navaja Predlog programa usposabljanja upravljavcev KI, ki ga je v letu 2018 pripravilo MO- Direktorat za obrambne zadeve. Zato v nadaljevanju podajamo samo nekatera izhodišča, ki so lahko pripomoček k uvedbi navedenega programa v prakso.

Vodstvena struktura pri nosilcih KI mora vedeti kateri dokumenti so potrebni za upravljanje s tveganji v KI ter kdo jih mora izdelati in implementirati.

Ključni dokumenti za upravljanje tveganj za delovanje KI so:

- politika Vlade o upravljanju KI (17. čl. ZKI),
- zakon o KI,
- navodilo za ocenjevanje tveganj za delovanje KI in strokovne usmeritve za ocenjevanje tveganj za delovanje KI v posameznih sektorjih KI (12. čl. ZKI),
- dokumenti načrtovanja zaščite KI (ocena tveganj in načrt ukrepov za zaščito KI - 11. čl. ZKI),
- predlog programa usposabljanja upravljavcev KI (MO-Direktorat za obrambne zadeve),
- politika upravljanja tveganj,
- ocena ranljivosti, ocena ogroženosti in SWOT analiza, ,
- katalog (register) tveganj,
- načrt neprekinjenega poslovanja
- krizni načrt z načrtom kriznega komuniciranja,
- načrt zaščite in reševanja,
- načrt fizičnega in tehničnega varovanja v skladu z zakonodajo in standardi zasebnega varovanja,
- načrt protipožarne zaščite,
- načrt zaščite osebnih podatkov, tajnih podatkov, informacij in poslovnih skrivnosti,
- načrt evakuacije,
- drugi specifični načrti v posameznih sektorjih KI, ki jih zahteva zakonodaja,
- certifikati uvedenih standardov in drugi certificati (družbena odgovornost, idr.).

Poleg informacije o namenu in ciljih uporabe dokumentov, ki so potrebni za upravljanje s tveganji na vseh ravneh je treba predstaviti tudi ključno pravno podlago in standarde na podlagi katerih se pripravijo in implementirajo navedeni dokumenti. Na tej ravni usposabljanja je smiselno poudariti še naslednje zadeve:

- potrebe po izboljšanju kadrovske strukture, (odgovornih oseb), ki upravlja z varnostjo in s tveganji,
- kontinuirano zagotavljanje finančnih sredstev za potrebe usposabljanja,
- velika soodvisnost med sektorji, ki se izrazi zlasti pri sodelovanju in komuniciranju ob izrednih dogodkih in kriznih razmerah,
- zagotavljanje neprekinjenega delovanja in poslovanja KI, ki mora biti zagotovljeno tudi v času krize (3., 10., 16., 19., in 24. čl. ZKI),
- vzpostavitev sistema spremljanja in nadzorovanja nad upravljanjem tveganj in izvajanjem načrtov ukrepov za zaščito pri upravljavcih KI.

Z nakazanim pristopom bi bila vodstvena struktura pri nosilcih KI primerno seznanjena z vlogo in potrebnimi aktivnostmi posameznih ministrstev, ki bi morala pokazati ustvarjalen in motiviran pristop do upravljavcev KI.

Vodstvena struktura pri upravljavcih KI mora poznati vlogo in naloge nosilcev KI, da lahko postavlja določene zahteve in predloge za izboljšanje procesa upravljanja varnosti in upravljanja tveganj. To pomeni, da vodilni in vodstveni kader v gospordarskih družbah, v zavodih in drugih organizacijah, ki upravljajo s kritično infrastrukturo dobro pozna vlogo tistih ministrstev, v čigar pristojnost sodi upravljanje določenih sektorjev KI. Ena od glavnih nalog nosilcev KI je, da pripravijo STROKOVNE USMERITVE, ki - poleg navodila Ministrstva za obrambo - omogočajo metodološko in vsebinsko enotno ocenjeva je tveganj za delovanje kritične infrastrukture. Ključno pa je, da ta struktura udeležencev pridobi znanja in usmeritve kako tudi izdelati in uporabljati politiko upravljanja tveganj, oceno ranljivosti, ogroženosti in tveganj, SWOT analizo, in zgoraj navedene načrte v praksi. Izhodišče za izdelavo vseh prej omenjenih dokumentov je posnetek stanja ali revizija obstoječih rešitev, ki omogoča izdelavo ali prenovo ocene ranljivosti, ocene ogroženosti in ocene tveganj. Te ocene so nato vsebinska podlaga za izdelavo ali posodobitev politik, strokovnih usmeritev, načrtov, navodil in drugih notranjih aktov. Vodstva pri upravljavcih KI potrebujejo tudi znanja, spoznanja in dobro prakso pri imenovanju in ugotavljanju sposobnosti ter motiviranosti odgovornih oseb za upravljanje varnosti in tveganj. Od teh odgovornih oseb, ki predstavljajo strokovno strukturo pri nosilcih in upravljavcih KI, je namreč odvisna operativna učinkovitost upravljanja s tveganji in uspešnost izvajanja ukrepov za zaščito KI.

Strokovna struktura pri nosilcih in upravljavcih KI so posamezne odgovorne osebe za upravljanje varnosti in tveganj, ki jih imenuje vodstvo nosilca in upravljavca KI. Ti udeleženci usposabljanja morajo dobiti znanja za izdelavo, implementacijo in obnovitev (posodobitev) vseh tistih dokumentov (ocena ranljivosti, SWOT analiza, ocena ogroženoeti, ocena tveganj, varnostna politika, politika upravljanja tveganj, načrti varovanja, zakonodaja, varnostni

standardi, standardi upravljanja tveganj, metode upravljanja tveganj, katalog tveganj idr.), ki so potrebni za upravljanje varnosti in upravljanje tveganj v lastnem delovnem in poslovnem okolju (ministrstvu, gospodarski družbi, zavodu, banki, idr.). V ta namen morajo spoznati kako in na podlagi česa pristopiti k ugotavljanju vrzeli (pomanjkljivosti) v obstoječi dokumentaciji, in kako izdelati nove (manjkajoče) dokumente, ki morajo biti odsev ocene ranljivosti, ocene ogroženosti, SWOT analize, zakonskih zahtev in uvedenih standardov. Iz nekaterih projektov, ki so bili izvedeni v KI je razvidno, da imajo odgovorne osebe za področje varnosti in obvladovanja tveganj pri upravljavcih KI, premalo znanja in izkušenj za upravljanje celovite varnosti in varnostnih tveganj. To – delno preverjeno domnevo – bi zlahka dokazali z ustrezno raziskavo o stanju menedžmenta korporartivne varnosti v KI. Vsekakor je tudi pravilna ugotovitev, da bi osebe s kompetencami obvladovanja varnosti in tveganj omenjena znanja že morale imeti kot pogoj za imenovanje na tak položaj.

Operativna struktura udeležencev usposabljanja so zaposleni na konkretnih delovnih mestih. Gre zlasti za varnostno izpostavljena delovna mesta, ki so navedena v oceni tveganj na področju varnosti in zdravja pri delu, v oceni požarnih in eksplozijskih tveganj v oceni informacijsko-komunikacijskih tveganj, v oceni tveganj kriminalne narave in v drugih ocenah tveganj, ki opozarjajo na nevarnosti, grožnje in tveganja. To strukturo udeležencev usposabljajo notranje odgovorne osebe za upravljanje z varnostjo in tveganji, lahko tudi s sodelovanjem določenih odgovornih oseb pri nosilcih KI in zunanjih referenčnih strokovnjakov. Bistvo tovrstnega usposabljajnja je, da zaposleni spoznajo osnovne pravne podlage in standarde, ob natančneem spoznavanju notranjih dokumentov (načrtov, navodil idr.), ki urejajo poslovanje, varnostna vprašanja in področje tveganj. Zaposlene je treba seznaniti in motivirati, da se zavedajo nevarnosti, tveganj in odgovornosti na svojem delovnem mestu in v širšem delovnem okolju. V tem okviru se jih seznani tudi o tem kako se gradi in krepi varnostna kultura in poslovna etika ter družbena odgovornost organizacije v kateri delajo.

Ob pregledu programa usposabljanja Direktorata za obrambne zadeve, v katerem so ponazorjena usposabljanja v posameznih državah, je tudi našo ekipo – z vidika ogroženosti in varnostnih tveganj - zanimalo kako usposabljanje za upravljanje celovite varnosti in varnostnih tveganj v KI in širše, vidijo nekateri tuji avtorji. Obstaja kar nekaj tuje literature, ki se ukvarja z izobraževanjem in usposabljanjem za potrebe KI. Kljub temu, da imajo nekatere države kar spodoben sistem usposabljanja za potrebe KI pa nekateri avtorji opozarjajo na vrzeli v izobraževalnih programih (Jones, 2009, Hope, 2017, Zahav, 2017), ki se v družbi tveganja nanašajo na korporativno upravljanje in na varnostne mehanizme v KI. Ameriški specialist za upravljanje tveganj za delovanje KI Robert J. Chapman navaja, da je k upravljanju tveganj potreben strukturiran pristop, da je treba dati poudarek na obvladovanju

energetskih, tržnih, tehnoloških, finančnih, operativnih in varnostnih tveganj, da se je treba odgovorno lotiti tveganj in da je pri upravljanju s tveganji pomembna vloga notranjih kontrol (Chapman, 2011). Pri izrednih dogodkih v KI ta avtor med drugim uporablja tudi Bayesov teorem pogojne verjetnosti nastanka nekega dogodka – npr. eksplozija nastane zaradi nesreče ali zaradi požara, kar pri nas označimo s t.i. »verižno reakcijo«. Prav tako se pri ocenjevanju ranljivosti in tveganj naslanja na SWOT analizo poslovanja, kar je v skladu z BIA metodo obvladovanja tveganj.

V številnih korporacijah se nepravilno in neučinkovito lotevajo obvladovanja tveganj, kar uničujoče vpliva na poslovanje in na konkurenčnost (Lam, 2014). Pri obvladovanju tveganj se je treba osredotočiti na številna in v mnogih primerih katastrofalna okoljska tveganja, ki jih povzročajo naravne in druge nesreče (Shaw, 2014, Vasović in drugi, 2017). Nekateri avtorji pa se zavzemajo za izobraževalne programe, ki celoviteje dajejo znanja za obvladovanje ranljivosti, ogroženosti in tveganj za delovanje KI (Flammini, 2012, Gritzalis, 2018). Ameriška univerza George Mason University je v sodelovanju s Centrom za zaščito KI in Ministrstvom za domovinsko varnost (ang. Department of Homeland Security) razvila visokošolski študijski program, ki zajema vsebine o upravljanju s tveganji, o medsektorski odvisnosti, kibernetski varnosti, ranljivosti in drugih segmentih zaščite KI (George Mason University, 2017, Homeland Security, 2018).

Z usposabljanjem za potrebe zaščite KI se v precejšnji meri ukvarja tudi Ameriško združenje za industrijsko varnost ASIS (American Society for Industrial Security), ki s programi seminarjev za 3-dnevna usposabljanja nudi znanja za celovit pristop k upravljanju tveganj, načrtovanju neprekinjenega poslovanja in kriznega vodenja; in to s predavanji, študijami primerov in delavnicami. (ASIS, 2018). Okvirno program usposabljanja zajema naslednje tematske sklope:

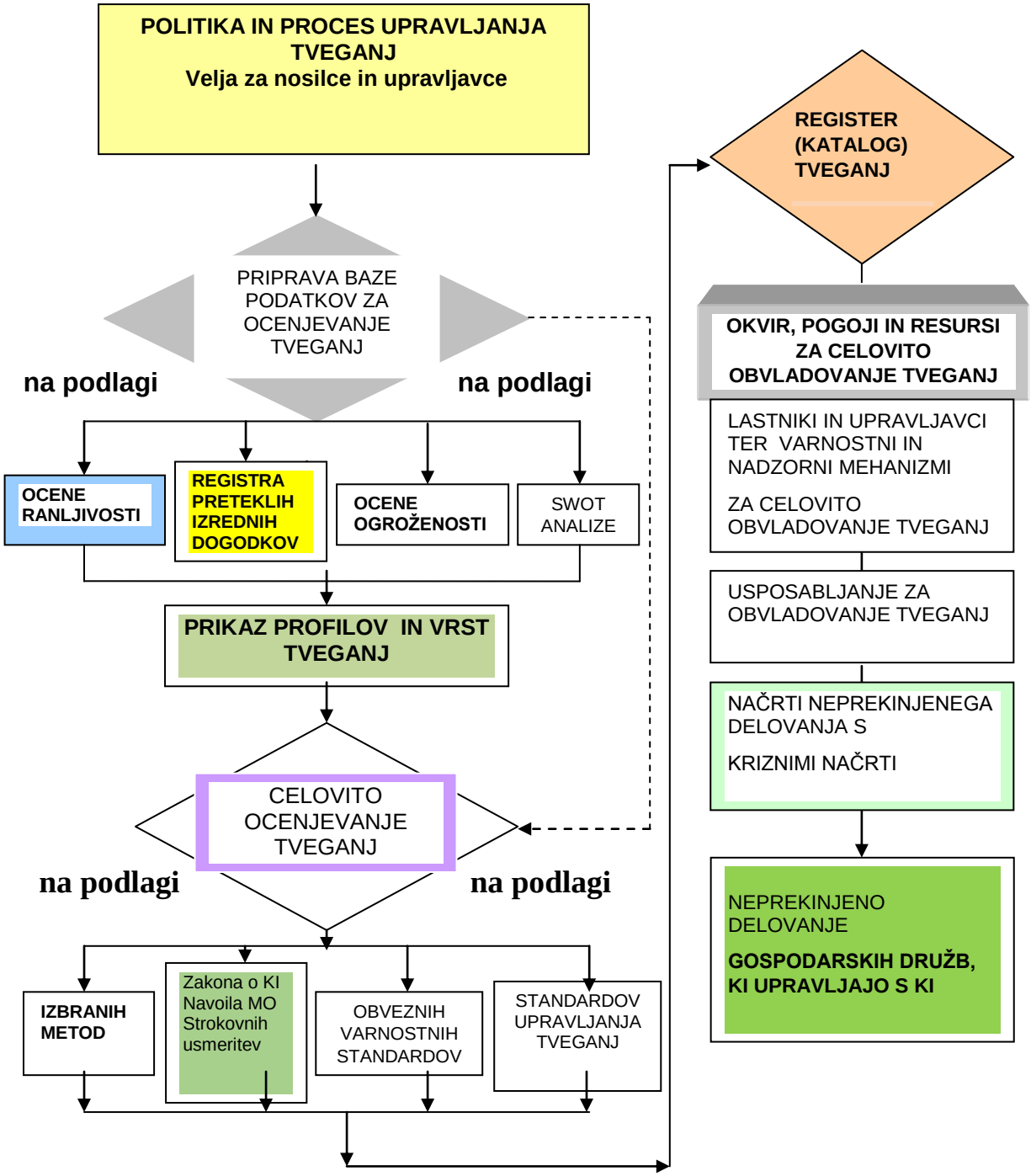
- upravljanje varnosti,
- proces upravljanja s tveganji,
- analiza tveganja,
- obravnava tveganja,
- odpornost na tveganja,
- upravljanje programa za oceno tveganja,
- komuniciranje in razvoj v poslovnih procesih,
- načrtovanje neprekinjenega delovanja in upravljanje s krizo,
- kritično razmišljanje.

To so vsekakor prave teme za obvladovanje tveganj, ki bi jim po naši presoji lahko dodali še teme o ranljivosti, ogroženost, načrtovanju zaščitnih (varnostnih) ukrepov in varnostni kulturi.

Naš izobraževalni sistem in posamezni izobraževalni procesi na vseh ravneh izobraževanja ne daje(jo) dovolj znanja za področje upravljanja tveganj v gospodarskih in drugih družbah. Še tiste izobraževalne ustanove ki se nanašajo na družbene, varnostne in podobne vede so šibke na tem segmentu korporativnega upravljanja. Smiselni in pogumen korak je naredila GEA College-Fakulteta za podjetništvo, ki je pred nekaj leti v sodelovanju z Institutom za korporativne varnostne študije pripravila in sprejela magistrski program z naslovom »Upravljanje tveganj in korporativna varnost«. Omenjeni študijski program nudi kompleksna znanja za upravljanje tveganj na strateških in operativnih ravneh države, industrije, gospodarstva in civilne družbe.

5 VZOREC METODOLOŠKEGA POSTOPKA ZA OCENJEVANJE TVEGANJ NA RAVNI UPRAVLJAVCA KRITIČNE INFRASTRUKTURE

Priprava vzorca metodološkega postopka za ocenjevanje tveganj za delovanje KI in vzorca ocene tveganj, temelji na prvem, drugem in tretjem delu študije, ki podajajo potrebna metodološka in vsebinska izhodišča za konkretnejši pristop k upravljanju in obvladovanju tveganj v sektorjih KI. Oblikovani vzorec metodološkega postopka za ocenjevanje tveganj za delovanje KI je shematsko prikazan v naslednji sliki.



Slika 55: Metodološko vsebinski pristop za vzpostavitev sistema upravljanja in obvladovanja tveganj za delovanje KI (izvirni pristop)

Če nekoliko poenostavimo strukturo in vsebino zgornje slike gre za predstavitev metodologije upravljanja, obvladovanja in ocenjevanja tveganj v KI, ki zajema tudi zagotavljanje neprekinjenega delovanja in kriznega vodenja. Drugače povedano, pri vzorcu izvirnega metodološkega pritopa gre v bistvu za opredelitev sistema upravljanja in obvladovanja tveganj za delovanje KI, ki zajema vse elemente sistemskega pristopa, pristopa od

splošnega h konkretnemu in obratno, pri čemer se opiramo tudi na interdisciplinarnost uporabe znanj, izkušenj in dobre prakse ter na doseganje sinergije med nosilci sektorjev in upravljavci KI. Tak pristop zagotavlja upoštevanje načel zaščite KI (10. člen ZKI), ki so: načelo celovitega pristopa, načelo odgovornosti, načelo zaščite pred različnimi vrstami nevarnosti, načelo stalnega načrtovanja zaščite KI (tudi stalni proces ocenjevanja tveganj) in načelo izmenjave ter varovanja podatkov in informacij.

5.1 VZPOSTAVITEV SISTEMA UPRAVLJANJA IN OBVLADOVANJA TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Dobesedno upravljanje tveganj v KI razumemo kot aktivnost nosilcev KI (strateška raven upravljanja s KI), obvladovanje tveganj pa aktivnost upravljavcev KI (operativna raven upravljanja tveganj). Torej gre samo za prenos upravljanja tveganj na operativno raven – konkretno na raven gospodarskih družb, zavodov in drugih organizacij, ki upravljajo s KI. Preprosto gre za dve ravni upravljanja tveganj, v katerih izstopa celovito ocenjevanje tveganj, ki rezultira v katalogu tveganj, kot je dinamičnem dokumentu, ki je na podlagi tekočih ocen tveganj podvržen določenim dopolnitvam.

Za pristop k celovitemu ocenjevanju tveganj (3. Čl. ZKI) je treba najprej izdelati, sprejeti in implementirati politiko upravljanja tveganj v proces upravljanja tveganj, ki zagotavlja trajnost in kontinuiranost upravljanja in obvladovanja tveganj v KI. Sledi priprava baze podatkov, ki so podvrženi ocenam in analizam tako, da je možno razkriti in prikazati profile in vrste tveganj. Ko imamo jasno sliko o profilih in vrstah tveganj se lotimo celovitega ocenjevanja tveganj, ki je podlaga za pripravo registra oziroma kataloga tveganj z vsemi potrebnimi elementi.

Ko je ocenjevalni del v sistemu upravljanja in obvladovanja tveganj dokumentiran, lastniki in upravljavci – ob podpori nosilcev sektorjev KI zagotovijo potrebni organizacijski okvir, finančne, tehnološke in kadrovske vire ter varnostne in nadzorne mehanizme za celovito (operativno) obvladovanje tveganj. Podpora nosilcev sektorjev KI (ministrstev) se odraža v strokovnih usmeritvah, ki pa ta čas še niso izdelane in v tekočih napotkih kako razreševati morebitbe težave. To pa še ni zadostni pogoj za celovito obvladovanje tveganj na ravni upravljavcev KI, kajti poleg kakovostnega vodenja sistema obvladovanja tveganj na strateški (pri nosilcih sektorjev KI) in srednji ravni je treba usposobiti in motivirati človeške vire (zaposlene, poslovne partnerje in pogodbene izvajalce, da v poslovnih procesih in vsak v svojem poslovnem in delovnem okolju prispeva k obvladovanju tveganj. Z vidika zagotavljanja neprekinjenega delovanja KI je potrebno od poslovnih partnerjev in pogodbenih izvajalcev zahtevati, do svoje dobave zagotovijo tudi ob nastanku izrednih dogodkov in v

času kriznih situacij. S tistimi, ki niso sposobni zagotavljati neprekinjenega poslovanja (dobavljanja) se perekine pogodba. To pomeni, da nosilci sektorjev KI pri sebi in pri upravljavcih KI najprej vzpostavijo proces usposabljanja odgovornih za obvladovanje tveganj, ki ga koordinira ministrstvo, pristojno za strokovno usmerjanje in usklajevanje na področju KI. Krona obvladovanja tveganj pa je načrtovanje in izvajanje neprekinjenega delovanja upravljavcev KI. Pri tem je ključnega pomena pripravljenost na hitro in strokovno odzivanje na izredne dogodke ter pripravljenost na razreševanje verjetnih kriznih situacij. Da bi se zagotovil čim bolj enoten in primerljiv pristop k zagotavljanju neprekinjenega delovanja KI je priporočljivo uporabiti standarde za vzpostavljanje neprekinjenega delovanja kot so ISO 22301 in ISO/IEC 27001 in 27005, ob tem pa še standarde obvladovanja tveganj ISO 31000 in ISO/IEC 31010. Tak pristop na eni strani terja znanje in sredstva, na drugi strani pa zagotavlja učinkovitejše in uspešnejše zagotavljanje neprekinjenega delovanja, ob nastanku izrednih dogodkov in v morebitnih kriznih situacijah. Nosilci sektorjev in upravljavci KI se morajo zavedati odgovornosti za morebitne napake, malomarnosti, slabe ocene tveganj in neučinkovite ukrepe za zaščito KI, ki lahko ohromijo ali onemogočijo delovanje sektorja in/ali določene gospodarske družbe, zavoda, državnega organa ali Banke Slovenije, kar – z vidika soodvisnosti – lahko ohromi delovanje drugih sektorjev, širšega gospodarstva, državnih in civilnih institucij ter družbe.

5.1.1 Prilagoditev obstoječih ocen tveganj izvirnemu pristopu

12. člen ZKI določa, da lastniki in upravljavci KI, to je gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti in/ali upravljajo s KI, izdelajo oceno tveganj na podlagi navodila za ocenjevanje tveganj za delovanje KI, ki ga sprejme ministrstvo, pristojno za strokovno usmerjanje in usklajevanje na področju KI, in strokovnih usmeritev, ki jih za posamezne sektorje KI izdelajo nosilci sektorjev KI, to je posamezna ministrstva.

15. člen navedenega zakona pa določa, da se pri izdelavi dokumentov načrtovanja zaščite KI - torej pri izdelavi ocene tveganj in pri izdelavi ukrepov za zaščito KI – lahko upoštevajo dokumenti, ukrepi, postopki in rešitve, izdelani ali sprejeti na podlagi veljavnih predpisov (npr. Zakona o zasebnem varovanju, Zakona o varstvu pred naravnimi in drugimi nesrečami, Zakona o varstvu pred požari, Zakona o varnosti in zdravju pri delu, Zakona o varstvu okolja) zlasti s področja zasebnega varovanja, varstva pred naravnimi in drugimi nesrečami in tehnološke varnosti, in poslovnih odločitev upravljavcev KI. Iz tega izhaja, da ocene tveganj, ki so izdelane po navedenih zakonih lahko upoštevamo pri implementaciji zgoraj opisanega izvirnega pristopa k upravljanju in obvladovanju tveganj za delovanje KI. Smiselno je torej upoštevati že izdelane in ažurirane ocene tveganj in na njih temelječe načrte zaščite oziroma

načrte varovanja, ki temeljijo na veljavni zakonodaji in s tem olajšamo prilagoditev ocenjevanja tveganj po našem izvirnem pristopu.

Po oceni avtorjev študije imajo gospodarske družbe, zavodi, državni organ in Banka Slovenije, ki upravljajo KI izdelane naslednje ocene tveganj:

- oceno tveganj naravnih in drugih nesreč,
- oceno okoljskih tveganj,
- Izjavo o varnosti z oceno tveganj (področje varnosti in zdravja pri delu),
- ocene požarnih tveganj,
- oceno informacijskih tveganj in
- oceno stopnje tveganja (po zakonu o zasebnem varovanju in po uredbi o obveznem organiziranju varovanja), ki vsebuje tudi analizo ranljivosti, analizo ogroženosti in analizo tveganj.

Izpostavljamo oceno stopnje tveganja na področju zasebnega varovanja**,** ki bi jo morale imeti izdelano praktično vsi upravljavci KI (zavezanci obveznega organiziranja varovanja) – konkretno denimo upravljavci v sektorjih energetike, prometa, zdravstva in informacijsko-komunikacijskih omrežij in sistemov ter druge družbe, katerih dejavnosti so bistvene za delovanje ključnih družbenih funkcij, zdravje in varnost ter zaščito gospodarstva, civilne družbe in prebivalstva. Tudi po ZKI so upravljavci KI zavezanci obveznega organiziranja varovanja (13. člen 6. točka zakona o KI). Torej morajo poleg ocene tveganja imeti izdelan tudi program varovanja in načrt fizičnega varovanja.

Poleg zgoraj navedenih ocen tveganj, ki temeljijo na veljavni zakonodaji, pripravljajo upravljavci KI še vrsto drugih ocen, analiz, študij, elaboratov, ekspertiz in druge dokumentacije, ki se nanašajo na raznovrstna specifična tveganja (denimo klinična tveganja v zdravstvu, kriterij n-1 v prenosnem omrežju električne energije, idr.), ogrožanja, nevarnosti in grožnje. Največ tovrstnih dokumentov je na področju proizvodnje, transporta, skladiščenja, predelave in uporabe nevarnih snovi, kemikalij, radioaktivnih snovi, sevanj, nevarnih izpustov, hrupa in drugih specifičnih nevarnosti in tveganj, ki so škodljiva za zdravje in počutje ter za doseganje poslovnih ciljev. Tudi te (že izdelane) ocene, analize in študije se lahko upošteva pri izdelavi dokumentov načrtovanja zaščite KI zlasti, če na njihovi podlagi uspešno potekajo določeni procesi in podprocesi.

5.1.2 Ocena tveganj kot vsebinska podlaga za načrtovanje ukrepov za zaščito kritične infrastrukture

Ocena tveganj za delovanje KI je rezultat celovitega postopka identifikacije, analize in vrednotenja različnih virov tveganj za delovanje KI, ki se izvede za zagotovitev podlage za oblikovanje ukrepov za zaščito KI (3. člen 8. točka ZKI). Pri tem je pomembno upoštevanje načel zaščite KI, ki zagotavljajo kakovost in uporabnost izdelanih ocen tveganj. Če so ocene tveganj kakovostne, je pričakovati, da bodo kakovostni, uporabni in učinkoviti tudi ukrepi za zaščito KI To je cilj pri pripravi navodila za ocenjevanje tveganj za delovanje KI in pri pripravi strokovnih usmeritev za izdelavo konkretnih ocen tveganj v posameznih sektorjih KI.

5.2 VZOREC OCENE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE NA RAVNI UPRAVLJAVCA KRITIČNE INFRASTRUKTURE

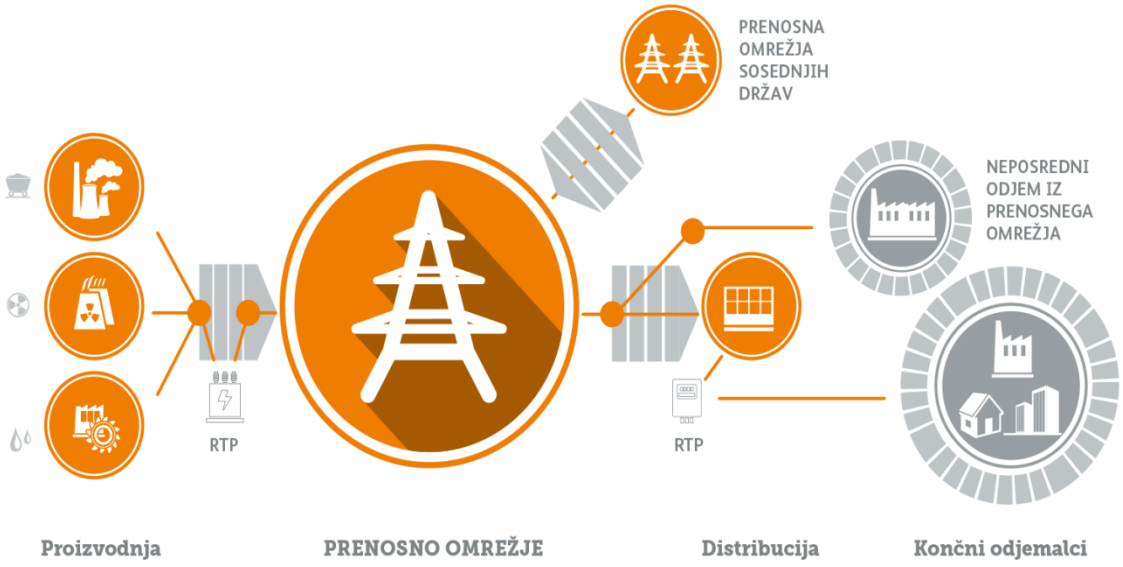
Glede na to, da je energetski sektor (zlasti električna energija) v prvi liniji pomembnosti za nemoteno delovanje države, gospodarstva, civilne družbe in prebivalstva smo se odločili, da kot primer vzorca ocene tveganj izberemo RTP, ki je v elektroenergetskem sistemu eden od glavnih elemenotv prenosa in distribucije elektrfične energije.

5.2.1. Razdelilne transformatorske postaje (RTP) kot primer vzorca ocene tveganj v sektorju energetika – v podsektorju električna energija

Glede na to, da je sektor energetike, s podsektorjem električna energija, eden izmed ključnih sektorjev KI smo se za primer vzorca ocene tveganj v konkretnem objektu odločili za RTP, ki je ključni segment v prenosnem in distribucijskem električnem omrežju, s tem pa tudi v celotnem elektroenergetskem sistemu (EES) Slovenije (slika 56). Iz tega izhaja, da je glavna vloga RTP (slik 57.) izvajanje naslednjih nalog:

- zbiranje električne energije, ki jo proizvedejo elektrarne,
- transformiranje zbrane električne energije na razne napetostne nivoje, in
- distribucija (razdeljevanje) električne energije porabnikom.

V tem kontekstu nas zanimajo velike in največje RTP, ki so – po presoji avtorjev študije – bolj izpostavljene negotovosti in tveganjem kot druge, oziroma je njihova pomembnost v sistemu večja kot pri ostalih RTP. Nekaj izhodišč za pripravo vzorca metodologije za oceno tveganj na primeru RTP je podanih v nadaljevanju.



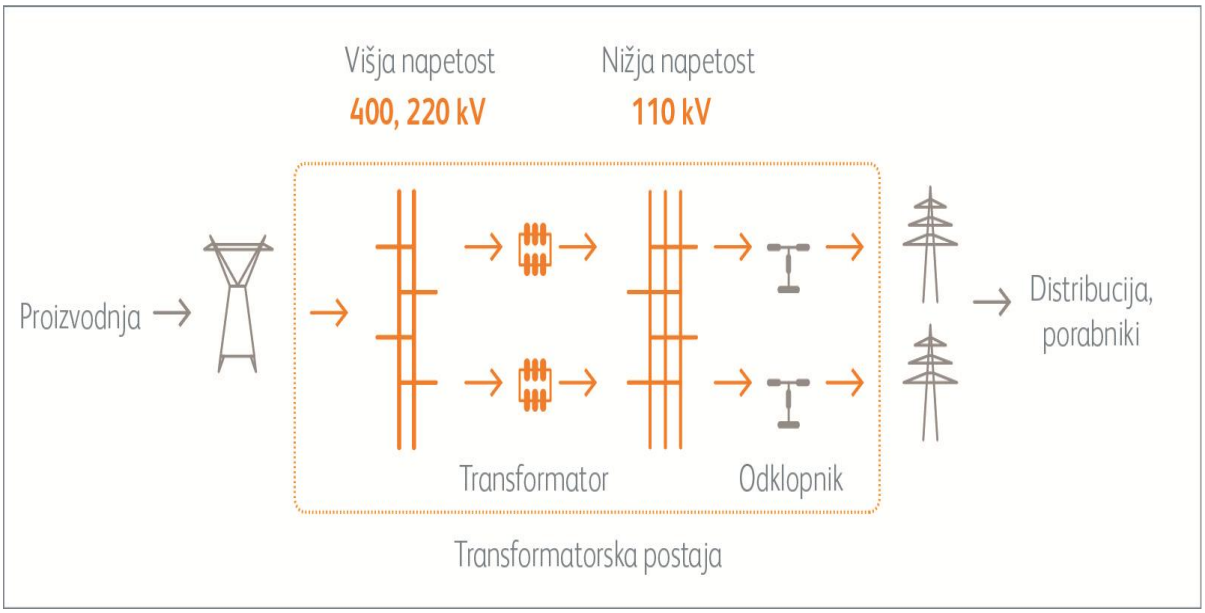
Slika 56: Položaj (mesto, lokacija) in umeščenost RTP v elektroenergetskem sistemu Slovenije (ELES, 2018)

Z vidika vloge RTP v EES poznamo v glavnem dve vrsti RTP:

- napajalne RTP, ki so postavljene med elektrarnami in prenosnim omrežjem,
- distribucijske RTP, ki so postavljene med prenosnim in distribucijskim omrežjem.

Na lokaciji RTP so zgrajena električna stikališča in druge elektroenergetske naprave ter potrebne zgradbe in sicer:

- visokonapetostno stikališče, ki je na prostem,
- energetski in/ali drugi transformatorji,
- srednje napetostno stikališče, ki je v zgradbi,
- prostori za upravljanje in vodenje RTP (komandni prostori),
- pomožni prostori za telekomunikacijske naprave, klimatske naprave, gasilsko opremo, prvo pomoč in druge naprave.



Slika 57: Pomen in vloga RTP v elektroenergetskem sistemu, od proizvodnje in prenosa električne energije, preko transformacije električne energije, vse do distribucije odjemalcem oziroma porabnikom (ELES , 2018)

Pri obravnavi tveganj, ki se nanašajo na RTP je treba izhajati tudi iz stanj obratovanja EES, ki je (če ni nenačrtovanih prekinitev in drugih motenj) normalno, sicer pa moteno z naslednjimi stanji:

- stanje pripravljenosti, ko se utemeljeno pričakuje kakšna nepričakovana prekinitev ali druga motnja (okvara, nesreča, kriminalno dejanje, ipd.),
- krizno stanje, ko je treba aktivirati krizni načrt s kriznim komuniciranjem,
- stanje razpadanja, ko so prekinitve in druge motnje trenutno neobvladljive, s kriznim upravljanjem in vodenjem EES (prekop centrov vodenja) pa z odpravo motenj vzpostavljanormalno stanje,
- stanje ponovnega vzpostavljanja v normalno stanje, ki se doseže z angažiranjem vseh deležnikov EES.

Prav tako se kaže potreba, da se pri ocenjevanju tveganj v RTP upošteva načrtovan sistem vzdrževanja RTP, ki ga sestavljajo:

- redno vzdrževanje v določenih rokih,
- intervencijsko vzdrževanje, ko gre za odpravo okvar,
- revizija, ki je poglobljen pregled RTP,
- remont, ko gre za investicijsko vzdrževanje in posodabljanje RTP.

Iz povedanega izhaja, da je obvladovanje tveganj, ki se nanašajo na RTP zahtevna naloga vodstva, strokovnjakov, razvojnikov, nadzornikov in zaposlenih v EES Slovenije.

5.2.1.1 Nekaj izhodišč za pripravo vzorca za izdelavo drugih ocen tveganjana primeru RTP

Pri izdelavi vzorca ocene tveganj za RTP izhajamo iz položaja in vloge RTP v EES. To pomeni, da je treba upoštevati delovanje RTP v odnosu do:

- proizvajalcev električne energije (elektrarn),
- v odnosu do sistemskih upravljavcev prenosnega in distribucijskega omrežja (ELES, SODO),
- v odnosu do številnih transformatorskih postaj (TP) in
- v odnosu do velikih in malih odjemalcev oziroma porabnikov električne energije.

V konglomeratu proizvodnje, transformacije, razdeljevanja, dobave in porabe električne energije je treba upoštevati tudi druge deležnike EES Slovenije kot so denimo: elektro podjetja (dobavitelji električne energije), drugi sektorji KI (kot porabniki električne energije), EES sosednjih držav (čezmejna izmenjava električne energije, čezmejna vloga RTP), Holding slovenskih elektrarn (HSE), prodajalci električne energije in veliki porabniki električne energije. Posebno področje v EES je informacijsko komunikacijski sistem, ki omogoča upravljanje posameznih delov EES in sistema kot celote, ter vsestransko komuniciranje med deležniki EES. Vse to so področja pri katerih je pričakovati vpliv raznovrstnih tveganj na delovanje RTP in obratno.

Dokument, ki omogoča izdelavo ocene tveganj za delovanje RTP se lahko imenuje npr. register tveganj ali pa upravljavec, ki upravlja posamezno KI, ta dokument imenuje drugače. Vsebina registra tveganj je podana v nadaljevanju študije.

Z vidika položaja in vloge RTP v EES so izpostavljene naslednje vrste tveganj pri delovanju, spremljanju delovanja, vzdrževanju, upravljanju, posodabljanju in razvoju RTP:

- operativna tveganja okvar na lokaciji RTP – okvare na visokonapetostnem in srednje napetostnem stikališču, okvare na energetskih, prečnih in drugih transformatorjih, okvare na drugih elektroenergetskih napravah (EEN) (dovodi/odvodi, zbiralke, ločilniki, odklopniki, stikala, releji, dušilke, tokovniki, kompresorji, varovalke, izolatorji, računalniška tehnologija, telekomunikacijske naprave, idr.), zastarelost in/ali neustreznost EEN, šibki zaščitni sistemi, problematika upravljanja in vodenja RTP na bazi vzpostavljenega informacijsko-komunikacijskega sistema, itd.;
- tveganja pri zagotavljanju neprekinjenega delovanja RTP – tveganja, ki izhajajo iz varnostnega kriterija n-1, tveganja dolgotrajnih nenačrtovanih prekinitev (tri minute in

več), tveganja kratkotrajnih nenačrtovanih prekinitev (manj od treh minut), nenatančno načrtovanje neprekinjenega delovanja RTP, vrzeli v rednem vzdrževanju EEN v RTP, zamujene rekonstrukcije, posodobitve in novogradnje RTP, nedodelan informacijsko-komunikacijski sistem za potrebe zagotavljanja neprekinjenega delovanja RTP, vključno z morebitnimi težavami v centrih vodenja, nedodelan sistem odzivanja na nastale okvare, nedorečen sistem kriznega vodenja RTP;

- tveganja lastnih vzrokov za prekinitve in motnje v delovanju RTP in širše – človeške napake, malomarnosti, slabo načrtovanje izvajanja nalog in aktivnosti;
- tveganja zunanjih vzrokov za prekinitve – naravne sile, škodljivo delovanje raznih deležnikov EES;
- tveganja prepočasnih in strokovno slabo pripravljenih odzivov na izredne dogodke na lokaciji RTP – odzivi na požar, povodenj, neurje, potres, vlom, vdor, nedovoljeno gibanje in odzivi na druge izredne dogodke;
- tveganja zagotavljanja standardizirane kakovosti napetosti ter zanesljivosti in razpoložljivosti dobave električne energije porabnikom, na bazi tehničnih standardov SIST EN 50160, SIST EN 61-2-4 in drugih;
- tveganja pogodbenih izvajalcev za vzdrževanje, rekonstrukcije in novogradnje RTP ter za vzdrževanje posameznih EEN;
- tveganja čezmejne izmenjave električne energije s sosednjimi državami;
- tveganja, ki izhajajo iz proizvajalcev električne energije (elektrarn);
- tveganja, ki izhajajo iz prenosnega omrežja;
- tveganja, ki izhajajo iz distribucijskega omrežja;
- tveganja, ki izhajajo iz velikih in malih odjemalcev oziroma porabnikov električne energije;
- varnostna tveganja – tveganja naravnih in drugih nesreč (potres, povodenj, obilne padavine, vihar, zmrzali, požarna tveganja), tveganja delovnih nesreč, informacijska in komunikacijska tveganja, tveganja zlorabe osebnih in tajnih podatkov, tveganja izdaje poslovnih skrivnosti, tveganja vlomov, tveganja nepooblaščenih pristopov in gibanja na lokaciji RTP, tveganja namernega poškodovanja naprav in druga varnostna tveganja;
- zavarovalna tveganja – vrzeli v zavarovanju RTP.

Glede na to, da v EES delujeta (v grobem rečeno) dve glavni vrsti RTP-jev, to so napajalne RTP med elektrarnami in prenosnim omrežjem ter distribucijske RTP med prenosnim in distribucijskim omrežjem, morajo ocenjevalci tveganj upoštevati tudi specifiko lokacij, namena, ter procesov delovanja obeh vrst RTP.

Predhodno navedeno je le vzorec, ne celotna ocena.

5.2.2 Metodološke, pravne, politične, strokovne in vsebinske podlage za pripravo vzorca ocene tveganj

V prejšnji točki 5.1 je predstavljen metodološko vsebinski pristop za vzpostavitev sistema ocenjevanja, upravljanja in obvladovanja tveganj za delovanje KI, ki je povsem izvirne narave in - ob dosledni uporabi - zagotavlja učinkovito obvladovanje vseh vrst tveganj (vključno s specifičnimi tveganji) v sektorjih KI in v vseh gospodarskih družbah, zavodih, državnih organih in Banki Slovenije, ki upravljajo KI. To je izhodišče za pripravo vzorca ocene tveganj za delovanje KI, ki upravljavcem KI na razumljiv, uporaben in učinkovit način prikazuje proces ocenjevanja, upravljanja in obvladovanja tveganj.

Pri izdelavi vzorca ocene tveganj smo upoštevali metodološke, pravne, strokovne in vsebinske podlage tako, da smo se izognili morebitnim vrzelim, ki so prisotne v sistemih upravljanja in obvladovanja tveganj v gospodarskih in drugih družbah ter v državnih institucijah. To domnevno pomeni, da je upravljajnje, obvladovanje in ocenjevanje tveganj v zasebnem in javnem sektorju metodološko neurejeno in podvrženo pomanjkljivostim v obvladovanju poslovnih in varnostnih izzivov. V nadaljevanju skrčeno predstavljamo navedene podlage in sicer:

- **Metodološke podlage** – MOSAR, FMEA, BIA, Splošni model, model Andersen, Model integritete in sinergije, ki omogočajo snovanje osnovnega metodološkega ogrodja za upravljanje, obvladovanje in ocenjevanje tveganj za delovanje KI;
- **Ključne pravne podlage** – evropska pravna podlaga za delovanje KI in nacionalna pravna podlaga kot so: ZKI, Zakon o gospodarskih družbah, Zakon o varstvu pred naravnimi in drugimi nesrečami, Zakon o varstvu okolja, Energetski zakon, Zakon o varnosti in zdravju pri delu, Zakon o varstvu pred požari, Zakon o informacijski varnosti, Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih, Zakon o zasebnem varovanju, Zakon o eksplozivnih snoveh, vnetljivih tekočinah, plinih ter drugih nevarnih snoveh, Zakon o kemikalijah;
- **Strateške podlage** z vidika nacionalne varnosti – nacionalne resolucije in nacionalne strategije, ki se nanašajo tudi na ocenjevanje tveganj za delovanje KI, izhajajoč iz Resolucije o strategiji nacionalne varnosti v Republiki Sloveniji;
- **Strokovne podlage** – standardi za upravljanje tveganj (ISO 31000:2018, ISO/IEC 31010:2018, ISO Guide 73:2009, ISO/IEC 51:2014, ISO/TC 262:2011); obvezni varnostni standardi na področju zasebnega varovanja, varnosti in zdravje pri delu, varstva pred požari, varstva okolja, varnosti in sledljivosti živil; standard neprekinjenega poslovanja in kriznega vodenja (ISO 22301), s standardi varovanja informacij (ISO/IEC 27000);

Strokovne podlage so ključno izhodišče za vzpostavljanje sistema upravljanja tveganj v gospodarskih družbah, zavodih in državnih institucijah s posebnim poudarkom na organizacijah KI, kajti dokaj razumljivo in usmerjevalno določajo, kako in katerih tveganj se je treba lotiti v raznih organizacijah, ne glede na njihovo velikost in dejavnosti. Tako denimo standard za upravljanje tveganj ISO 31000, s podpornim standardom ISO/IEC 31010 opredeljuje naslednje:

- zavezanost najvišjega vodstva, da usmerja, svetuje in odloča o vzpostavljanju učinkovitega sistema upravljanja tveganj; pomembno je upravljanje, obvladovanje in ocenjevanje vseh vrst tveganj – navedena so strateška, pravna, finančna, poslovna, integracijska, varnostna, operativna, informacijska in še nekatera druga tveganja;obvladovanje tveganj mora potekati v vseh procesih in na vseh ravneh odločanja – torej je sestavni del delovanja in poslovanja; zahteva se visoka stopnja odgovornosti za napake, stranpoti, malomarnosti in odmike od ciljev – vsi v celotni verigi odgovornosti se morajo zavedati, da je učinkovitost obvladovanja tveganj odvisna od vsakega posameznika in od vsake organizacijske enote;natančno je treba določiti vloge, kompetence in pristojnosti oseb, ki so določene in imenovane za profesionalno vodenje sistema upravljanja tveganj; v sklop tveganj je treba uvrstiti tudi obvladovanje sprememb in poslovnih, varnostnih in drugih izzivov; človeški viri (zaposleni in drugi) morajo biti deležni ustreznega informiranja, komuniciranja in usposabljanja za obvladovanje tveganj v vseh delovnih in poslovnih okoljih; zagotoviti je treba vnašanje nenehnih izboljšav v procese upravljanja, obvladovanja in ocenjevanja tveganj; vodstva so dolžna zagotoviti potrebne finančne, kadrovske in logistične vire za učinkovito obvladovanje tveganj. Pod strokovne podlage uvrščamo tudi nekatera znana poslovna orodja, ki prispevajo k učinkovitejšemu obvladovanju tveganj, zlasti na področju kibernetskih, informacijskih in komunikacijskih tveganj ter tveganj zlorabe osebnih in tajnih podatkov ter poslovnih skrivnosti. To so strategije, taktike in tehnike »benchmarkinga« in »business intelligence«. Oboje se v mnogih točkah nanaša na sodobna tveganja prestrezanja in prisluškovanja elektronskim komunikacijam, ki so nadzorovane s sodobno satelitsko navigacijo in drugimi tehnično-tehnološkimi sredstvi.

- **Vsebinske podlage –** varnostni projekti v KI, raziskovalni izsledki o KI, bodisi v obliki projektov, raziskav ali diplomskih del, analize in študije o delovanju KI, obstoječi sistemi ravnanja s tveganji v KI in drugi dokumenti, ki se nanašajo na ranljivost, ogroženost, nevarnost in tveganja za delovanje KI.

Tej široki paleti podlag sledi tudi vzorec ocene tveganj, ki najprej opredeljuje vse vrste možnih tveganj za delovanje KI, nato pa še glavne elemente, ki jih povzročajo tveganja, vse do zahtev po izdelavi scenarijev za najtežje izredne dogodke.

5.2.3 Register (katalog) tveganj za delovanje kritične infrastrukture – obvladovanje tveganj na ravni upravljavca kritične infrastrukture

Iz vzorca registra (kataloga) tveganj, ki sledi, je razvidno, da so tveganja za delovanje KI izredno kompleksna. To je v tej študiji večkrat poudarjeno. Po naši oceni se družba in KI sooča s 17 vrstami tveganj, ki terjajo sistemski in interdisciplinarni (v nekaterih segmentih pa tudi multidisciplinarni) pristop k vzpostavitvi sistema upravljanja tveganj. Sestavni del tega pristopa je tudi pričujoči vzorec, ki po vrstah tveganj nakazuje konkretna tveganja z osnovnimi parametri ocenjevanja. Opredeljene vrste tveganj s konkretnimi tveganji so rezultat varnostnih projektov ter drugih študij, analiz in projektov, ki so se nanašali na KI. Vsekakor vrste tveganj in konkretna tveganja niso popolni, zato vzorec ocene tveganj v obliki registra nastopa kot osnova, ki je pri posameznih upravljavcih KI potrebna določene dopolnitve oziroma prilagoditve.

Izpolnitev rubrik oziroma parametrov od 1 do 6 v vzorcu spodnjega registra je naloga upravljavcev KI, ki bodo, na podlagi izbranih metod in modelov ocenjevanja tveganj, lastna tveganja ocenili ter ovrednotili in na koncu v rubriki 6 določili za katera tveganja oziroma katere izredne dogodke je treba pripraviti tudi načrte obvladovanja in jih preveriti z načrtovanimi vajami.

Po standardu upravljanja tveganj ISO 31000:2018 se ocenjevanje tveganj izvede s tremi aktivnostmi, to so: prepoznavanje (razpoznavanje) tveganj, analiza tveganj in vrednotenje tveganj, kar je v spodnjem vzorcu registra (kataloga) tveganj opredeljeno v rubrikah 2, 3 in 4.

Vzorec registra (kataloga) tveganj na ravni upravljavca KI (izvirni pristop)

3. člen 5. točka ZKI določa, da so upravljavci KI »gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti ali upravljajo KI«.

Tabela 17: Vzorec registra tveganj

Št.	VRSTE TVEGANJ	1 Verjetnost nastanka tveganja	2 Prepoznavanje tveganj	3 Analiza tveganj	4 Vrednotenje tveganj	5 Materialne, poslovne, človeške in druge posledice	6 IZDELAVA SCENARIJA Označiti z X
1	**POSLOVNA TVEGANJA**						
1.1	Tržna tveganja- tveganja tržnega deleža						
1.2	Tveganja napada konkurence						
1.3	Tveganja poslovnih partnerjev						
1.4	Tveganja pogodbenih izvajalcev						
1.5	Projektna tveganja						
1.6	Napačne poslovne odločitve						
1.7	Neurejeno neprekinjeno poslovanje in krizno vodenje						
1.8	Tveganja iznosa zaupne poslovne dokumentacije						
1.9	Tveganja v razvojni strategiji						
1.10	Tveganja škodljivih pogodb						
1.11	Tveganja na javnih razpisih						
1.12	Tveganja razkritja zaupnih elektronskih komunikacij						
1.13	Tveganja zaradi slabega vodenja in neučinkovite kontrole						
	Druga tveganja						
2	**FINANČNA TVEGANJA**						
2.1	Cenovna tveganja						
2.2	Kreditna tveganja						
2.3	Obrestna tveganja						

2.4	Tveganja neplačnikov						
2.5	Napačne finančne odločitve						
2.6	Korupcijska tveganja						
2.7	Tveganja, povezana s sistemom javnega naročanja						
2.8	Tveganja nezadostnega zavarovanja premoženja in človeških virov						
	Druga tveganja						
3	**PRAVNA TVEGANJA**						
3.1	Nedodelani notranji akti						
3.2	Neredno spremljanje zakonskih sprememb						
3.3	Nezakonito poslovanje						
3.4	Računovodske mahinacije						
3.5	Šibka notranja kontrola in revizija						
3.6	Vrzeli v sistemu javnega naročanja						
3.7	Tveganja tožb na sodiščih						
	Druga tveganja						
4	**TVEGANJA NESKLADNOSTI**						
4.1	Slaba skladnost z zakonodajo						
4.2	Slaba skladnost s standardi						
4.3	Slaba skladnost delovanja in poslovanja z opredeljenimi cilji						
4.4	Neskladnost z notranjimi akti in vrednotami						
	Druga tveganja						
5	**TVEGANJA NOTRANJE INTEGRITETE in ŠIBKE SINERGIJE**						
	Organizacijska tveganja, vrzeli v organiziranosti dela in						

5.1	poslovanja						
5.2	Slabi delovni odnosi						
5.3	Nepovezanost procesov						
5.4	Vrzeli v korporativnem upravljanju						
5.5	Kadrovska problematika						
5.6	Ni sinergijskih učinkov med procesi upravljanja, vodenja in nadzorovanja						
5.7	Tveganja družbene odgovornosti - uvedba SA 8000, ISO GSR 26000						
	Druga tveganja						
6	**TEHNOLOŠKA TVEGANJA**						
6.1	Okvare na sistemih						
6.2	Okvare na strojih						
6.3	Okvare na opremi						
6.4	Zastarelost tehnologije						
6.5	Nevarnost visokih pritiskov in temperatur						
6.6	Nevarnost izpustov, sevanj in razlitij						
	Druga tveganja						
7	**LOGISTIČNA TVEGANJA**						
7.1	Vrzeli v notranjem, transportu						
7.2	Tveganja v dobavnih verigah						
7.3	Tveganja v prometu						
7.4	Skladiščna tveganja in tveganja v zbirnih centrih						
	Druga tveganja						
8	**KIBERNETSKA TVEGANJA**						
8.1	Izpostavljenost neželeni el. pošti						
8.2	Izpostavljenost spletnim goljufijam						

8.3	Izpostavljenost motnjam v delovanju informacijsko - komunikacijskih sistemov						
8.4	Izpostavljenost kibernetskemu kriminalu - spletne goljufije						
8.5	Izpostavljenost kraji identitete						
8.6	Izpostavljenost pridobivanju informacij o posameznikih in združbah						
8.7	Izpostavljenost digitalnem piratstvu						
8.8	Izpostavljenost pastem interneta						
8.9	Izpostavljenost kibernetskemu terorizmu						
	Druga tveganja						
9	**INFORMACIJSKA TVEGANJA**						
9.1	Tveganja vdora v informacijski sistem						
9.2	Tveganja informacijske nesreče/incidenta						
9.3	Tveganja z zastarelo tehnologijo						
9.4	Tveganja v notranjem zagotavljanju informacij-šifre, gesla idr.						
9.5	Tveganja z zunanjim izvajalcem upravljanja informacijskega sistema						
9.6	Tveganja zaradi nizke stopnje varnostne kulture zaposlenih						
9.7	Nedoslednost pri vzpostavljanju sistema varovanja informacij						
9.8	Tveganja zaradi neurejenosti rezervne lokacije						
9.9	Tveganja zaradi neobvladovanja neprekinjenega						

	delovanja/poslovanja						
9.10	Tveganja zaradi prešibke avtonomne energijske podpore (UPS + agregat)						
9.11	Druga tveganja						
10	**KOMUNIKACIJSKA TVEGANJA**						
10.1	Problematika baznih postaj						
10.2	Nedodelanost delovanja v kriznih stanjih						
10.3	Tveganja zastarele tehnologije						
10.4	Tveganja v času zasičenosti komuniciranja						
10.5	Tveganja prestrezanja in prisluškovanja						
10.6	Izpad omrežja						
10.7	Pomanjkljiv varnostni načrt z oceno tveganj						
10.8	Tveganja okvar v kom. infrastrukturi						
	Druga tveganja						
11	**OKOLJSKA TVEGANJA**						
11.1	Tveganja naravnih in drugih nesreč -potres, poplava, vihar, obilne padavine, suša, toča, hude zmrzali						
1.2	Onesnaženje z nevarnimi snovmi-izpusti, izlitja						
11.3	Onesnaženje s kemikalijami						
11.4	Radioaktivna in druga sevanja						
11.5	Prekomeren hrup						
11.6	Izpusti toplogrednih plinov-CO2, N2O						
11.7	Slabosti v načrtovanju zaščite in reševanja						
	Nedodelani scenariji						

11.8	Neredno izvajanje vaj po scenarijih						
11.9	Slabosti v procesu koordinacije akcij						
11.10	Druga tveganja						
12	**TVEGANJA ČLOVEŠKIH VIROV**						
12.1	Nizka varnostna kultura						
12.2	Insajderstvo						
12.3	Sabotažne nakane						
12.4	Interne tatvine						
12.5	Izdaja zaupnih podatkov						
12.6	Iznos zaupnih dokumentov (fizično in z računalnikom)						
12.7	Površno varnostno preverjanje						
12.8	Slaba izobrazbena struktura						
12.9	Nedodelan sistem notranjega usposabljanja						
12.10	Zdravstveni problemi						
12.11	Neupoštevanje varnostnih navodil in procedur						
12.12	Izguba ključnih človeških virov						
12.13	Neupoštevanje konkurenčne klavzule						
12.14	Premalo zavesti o kakovosti dela in poslovanja						
12.15	Podkupljivo osebje						
	Druga tveganja						
13	**VARNOSTNA TVEGANJA**						
13.1	Ni učinkovitih varnostnih politik in varnostnih strategij						
13.2	Tveganja varnosti in zdravja pri delu						
13.3	Požarna tveganja						
13.4	Eksplozijska tveganja						
13.5	Tveganja kriminala						

13.6	Tveganja nepooblaščenih pristopov in gibanj						
13.7	Tveganja počasnih odzivov na izredne dogodke						
13.8	Tveganja evakuacij						
13.9	Tveganja neurejenih intervencijskih poti						
13.10	Nedodelani načrti varovanja in nejasna varnostna navodila						
13.11	Vrzeli v varstvu osebnih podatkov						
13.12	Vrzeli v varovanju zaupnih podatkov						
13.13	Vrzeli v varovanju tajnih podatkov						
13.14	Neurejeno varovanje arhivov						
13.15	Tveganja okoljskih nesreč						
13.16	Tveganja industrijskih nesreč						
13.17	Tveganja naravnih nesreč						
13.18	Teroristična tveganja						
3.19	Tveganja zasebnega varovanja-problem kakovosti in cen storitev, plač, strokovnosti in odgovornosti						
13.20	Neurejen sistem uvajanja varnostnih standardov v sistem varovanja						
	Druga varnostna tveganja						
14	**OPERATIVNA TVEGANJA**						
14.1	Tveganja na delovnih mestih						
14.2	Procesna tveganja						
14.3	Tveganja enkratnih poslov						
14.4	Tveganja tekočih operativnih odločitev						
14.5	Tveganja manjših okvar in napak						

14.6	Tveganja reklamacij						
	Druga tveganja						
15	**STRATEŠKA TVEGANJA**						
15.1	Finančna tveganja						
15.2	Neobvladovanje poslovnih potez, ki vodijo v propad						
15.3	Projektno razvojna tveganja						
15.4	Nepoznavanje ranljivosti in ogroženosti						
15.5	Zanemarjanje SWOT analize						
15.6	Nesposobnost zajemanja poslovnih priložnosti						
15.7	Neobvladovanje trga						
15.6	Zanemarjanje človeških virov						
15.9	Neobvladovanje konkurence						
	Druga strateška tveganja						
16	**SPECIFIČNA TVEGANJA V SEKTORJIH KI**						
16.1	**Sektor energetike:** Kriterij n-1 Izpad PO Izpad DO Razpad EES Motnje v dobavi naft. derivatov Motnje v dobavi plina Motnje v ogrevalnih sistemih Druga tveganja						
16.2	**Sektor zdravstva** Klinična tveganja Kadrovska tveganja Tveganja zdravstvene opreme						

16.3	**Sektor preskrbe s pitno vodo** Omejitve v preskrbi s pitno vodo Ogroženost pitne vode z onesnaževanjem Problem kakovosti pitne vode Tveganja kontrolnih točk v sistemu oskrbe s pitno vodo po standardu HACCP Tveganja mikrobiološke skladnosti Tveganja zastrupitve pitne vode Druga tveganja						
16.4	**Sektor prehrane/živila** Tveganja pri proizvajalcih živil Tveganja v procesu predelave surovin Tveganja v prevozih živil Tveganja pri skladiščenju živil Tveganja v procesu prodaje živil Problematika notranjega nadzora nad živili po HACCP, ISO 22000 in IFS						
16.5	**Sektor prometa** Tveganja prometnih nesreč Tveganja večjih zastojev v cestni mreži Tveganja pri prevozu nevarnih snovi (ADR) Tveganja pri prevozu naftnih derivatov in kemikalij Tveganja pri prevozu izrednih tovorov						
16.6	**Sektor informacijsko-komunikacijskih**						

	omrežij in sistemov Tveganje kolapsa mobilne telefonije v krizi Tveganja komuniciranja po posebnih sredstvih zvez med državnimi institucijami (ZARE, TETRA in drugi sistemi) Tveganja globalnega prestrezanja in prisluškovanja elektronskega komuniciranja						
16.7	**Sektor financ** Sistemska tveganja Tveganja neučinkovitega nadzora nad bankami Tveganja nezaupanja v bančni sistem						
16.8	**Sektor varovanja okolja** Tveganja onesnaževanja okolja Tveganja podnebnih sprememb Tveganja katastrofalnih posledic naravnih nesreč						
17	**ZAVAROVALNA TVEGANJA**						
17.1	Slaba pogajalska izhodišča za sklepanje pogodb z zavarovalnicami						
17.2	Neuravnotežena varnostna in zavarovalna kultura - ni upoštevana metoda cost/benefit						
17.3	Nedodelan sistem upravljanja tveganj						
17.4	Slabo poznavanje storitev in politike zavarovalnic						
	Šibko poznavanje strukture, vsebine in posledic zavarovalnih pogodb – slabo upravljanje						

17.5	zavarovanja						
17.6	Nedodelana evidenca izrednih dogodkov, ki so predmet zavarovanja						
17.7	Nedoslednost pri izterjavi škod						
	Druga zavarovalna tveganja						

Vsako tveganje po posameznih vrstah tveganj v vzorcu registra in vsako tveganje, ki ga bodo dodali posamezni upravljavci KI, mora biti definirano z verjetnostjo nastanka, z oceno (prepoznavanje, analiza, vrednotenje), s predvidenimi posledicami in označeno z **X,** ko gre za tveganja oziroma izredne dogodke, ki jih je treba obvladovati tudi s scenariji. Scenariji z načrti izvedbe vaj so potrebni samo za tista tveganja oziroma izredne dogodke (denimo požar-požarna tveganja, vdor v informacijski sistem-informacijska tveganja), ki so ocenjeni z visoko verjetnostjo nastanka in z visokimi ali celo katastrofalnimi posledicami.

5.3 IMPLEMENTACIJA VZORCA REGISTRA (KATALOGA) ZA OCENO TVEGANJ

Po proučitvi vzorca registra za oceno tveganj upravljavci KI najprej:

- pregledajo obstoječo dokumentacijo o upravljanju tveganj, še zlasti lastni register tveganj,
- primerjajo obstoječe metodologije ocenjevanja oz. upravljanja tveganj z novo metodologijo,
- ugotovijo ali bodo pri uvajanju nove metodologije potrebni manjši ali večji posegi v obstoječo metodologijo.

V procesu proučevanja vzorca registra upravljavci KI preverijo ali imajo izdelano oceno ranljivosti, oceno ogroženosti, SWOT analizo, celovito (krovno) varnostno politiko, izvedene varnostne politike (politiko varovanja informacij, politiko varnosti in zdravja pri delu idr.) ter politiko upravljanja s tveganji. Če teh dokumentov nimajo ali so pomanjkljivi, ni mogoče zanesljivo opraviti prenovo ocene tveganj, kajti brez ustreznih analitičnih podatkov ni realne slike tveganj. Poleg tega se pojavlja še strateško vprašanje, ali imajo upravljavci KI izdelane načrte neprekinjenega delovanja in poslovanja ter krizne načrte z načrtom kriznega komuniciranja in z opredeljenimi scenariji in načrti vaj. V sklopu ocenjevanja tveganj je treba ugotoviti obstoj ali neobstoj teh načrtov, kajti obvladovanje tveganj je sestavni del načrtovanja in zagotavljanja neprekinjenosti delovanja KI. Pri tem je treba poudariti, da je

nujno potrebno v načrte neprekinjenega delovanja vključiti tudi strateške poslovne partnerje, ki so ključnega pomena za delovanje posameznega upravljavca KI. Iz tega vidika je od teh partnerjev pričakovano neprekinjeno delovanje tudi ob najhujših izrednih dogodkih.

Oceno tveganj na podlagi vzorca registra (verjetnost nastanka tveganja, prepoznavanje tveganj, analiza tveganj, vrednotenje tveganj, posledice in scenariji) upravljavci KI opravijo na podlagi MOSAR in FMEA metode, ki sta predstavljeni v nadaljevanju in na podlagi drugih metod in modelov, ki so predstavljeni v tej študiji.

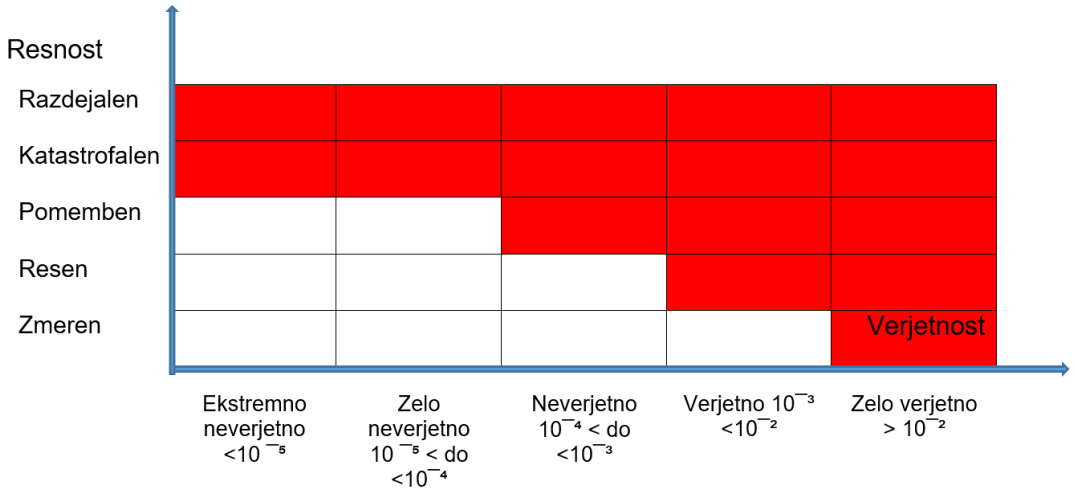
Prepoznane vire nevarnosti, prepoznane tvegane scenarije, oceno tveganega scenarija, analizo in rangiranje tveganega scenarija za sektor energetike, vnesemo v Tabelo 21.

Koraki so izdelani na podlagi metodologije MOSAR (navedeni kot »koraki od ena do štiri«). Vire tveganj (1. korak) ugotavljamo na podlagi možnih globalnih ogrožanj (zunanjih in notranjih) delovanja organizacije KI, navedene v predhodnem gradivu. Za vsak vir nevarnosti se prepozna tvegani scenarij (2. korak). Namen prepoznavanja scenarijev je razširiti okvir razmišljanja o prihodnosti z različnimi verjetnimi prihodnjimi stanji, ki se lahko razvijejo iz sedanjega stanja. Prepoznava scenarijev vključuje elemente vizij, projekcij, statističnih podatkov in znanja presojevalca. Ocena tveganih scenarijev (3. korak) se izdela na podlagi kriterijev možne škode (resnosti) v primeru izrednega dogodka (Tabela 18) in matrike resnosti ter verjetnosti izrednega dogodka (Tabela 19).

Tabela 18: Tabela škode - resnost (smiselno prirejeno po MOSAR)

Človeška življenja	**Materialna škoda**	**Resnost**
Več kot eden mrtev	Popolno uničenje	Razdejalna
Eden mrtev	Škoda z ustavitvijo sistema	Katastrofalna
Težje poškodovani	Škoda z delno ustavitvijo sistema	Pomembna
Lažje poškodovani	Manjša materialna škoda	Resna
Brez poškodb	Brez materialne škode	Nizka

Tabela 19: Matrika scenarijev (smiselno prirejeno po MOSAR)



Resnost ogrožanja se nanaša na razdejalni učinek (ocena 5), katastrofalen (ocena 4), pomemben (ocena 3), resen (ocena 2) ali nizek učinek (ocena 1). Če se zgodi primer brez telesnih poškodb in s škodo z ustavitvijo sistema, potem se upošteva najvišja vrednost (resnost bi bila v tem primeru katastrofalna, čeprav ni bilo smrtnih žrtev).

Verjetnost ogrožanja se nanaša na ekstremno neverjetno (en primer na sto tisoč primerov, ocena 5), zelo neverjetno (en primer na sto tisoč primerov do en primer na deset tisoč primerov, ocena 4), neverjetno (en primer na deset tisoč primerov do en primer na tisoč primerov, ocena 3), verjetno (en primer na tisoč primerov do en primer na sto primerov, ocena 2) in zelo verjetno (en primer pod sto primeri, ocena 1).

Analiza in rangiranje tveganih scenarijev (4. korak)

Iz Tabele 19 se prenesejo scenariji iz rdečega območja in se jih analizira s pomočjo kazalcev v Tabeli 20.

Tabela 20: Vzorec: Ocena kritičnosti - okvir najslabših možnih scenarijev (NMS)

Opis najslabšega scenarija (NMS)	Vpliv na poslovni proces	Vpliv na zaupanje uporabnikov	Vpliv na finančna sredstva	Vsebinska obrazložitev ocene	Končni produkt treh ocen vplivov	Rang scenarija
NMS 1						
NMS 2						
NMS 3						
NMS 4						
NMS 5						
NMS n						

Najslabšim možnim scenarijem (iz rdečega območja) se določi oceno ogroženosti. Kot pomoč pri ocenjevanju ogroženosti služijo spodnji kazalniki, ki določajo vpliv na poslovne cilje, zaupanje uporabnikov in finančni vpliv.

Kazalniki vpliva na poslovne procese so: poslovni proces poteka z napakami (ocena 1), proces je deloma ohromljen (ocena 2), procesa ni mogoče izvesti (ocena 3), proces vpliva na druge procese in jih upočasnjuje (ocena 4), proces vpliva na druge procese in jih onesposablja (ocena 5).

Kazalniki vpliva na zaupanje so: zaupanje uporabnikov, zaupanje strokovne javnosti, zaupanje lastnika, zaupanje vodstva sektorja KI, ustreznost informiranja ipd. (ocena 5: visoko zaupanje, ocena 3: srednje zaupanje, ocena 1: nizko zaupanje).

Kazalniki finančnega vpliva so: brez škode (ocena 1), škoda je manjša od 50.000 EUR (ocena 2), je med 50.000 in 500.000 EUR (ocena 3), je med 500.000 in 5.000.000 EUR (ocena 4), je večja od 5.000.000 EUR (ocena 5).

Tabela 21: Identifikacija virov nevarnosti za sektor energetike

Zap. številka	Vir nevarnosti (1. korak)	Prepoznavava tveganega scenarija (2. korak)	Ocena tveganega scenarija (3. korak)	Analiza in rangiranje tveganega scenarija (4. korak)
1.	neustrezno poslanstvo, vrednote, vizija in strategija organizacije	ni strateškega načrtovanja in razumevanja pomembnosti ter prispevka posameznih strateških ciljev k uresničevanju strateških usmeritev KI	4 (resnost) / 1 (verjetnost) (produkt) 4	**Prikazane ocene nad 5**
2.	neustrezno upravljanje organizacije	upravljanje ni v skladu z zakoni, z Aktom o ustanovitvi, s Kodeksom korporativnega upravljanja in pričakovanji lastnika ter Nadzornega sveta	4 / 1 4	
3.	informiranje in poročanje	informiranje in poročanje Nadzornemu svetu ni v skladu z ZGD-1 in slovenskimi standardi računovodskega poročanja	3 / 1 3	
4.	korporativna integriteta	ni ničelne tolerance do prevar in nezakonitih dejanj, Etični kodeks ne obstaja, pooblaščenec za korporativno integriteto ni imenovan	3 / 1 3	
5.	okoljska tveganja	ni nadzorovanja in merjenja vplivov, ki so določeni z okoljsko politiko	3 / 1 3	
6.	zakonska ureditev KI	pomanjkljiva zakonska ureditev KI	4 / 1 4	
7.	obvladovanje projektov	z internimi splošnimi akti niso določeni postopki in	2 / 2	

		pravila obvladovanja projektov, IT sistem ne podpira obvladovanja projektov	4	
8.	Kodeks omrežja	neupoštevanje evropskih ciljev na področju energetike (zagotavljanje varnosti obratovanja sistema in dobave električne energije, omogočanje preskrbe evropskega trga z električno energijo)	4 / 2 **8**	
9.	zagotavljanje sistemskih storitev	ni aktivnega pristopa do domačih ponudnikov, izmenjava viškov energije med sosednjimi sistemskimi operaterji je neustrezna, ni sporazumov o zagotavljanju vzajemne pomoči ob izrednih dogodkih	4 / 2 **8**	
10.	oddaja energije	neustrezna oddaja električne energije v prenosno omrežje in njen prevzem iz prenosnega omrežja	4 / 2 **8**	
11.	obremenitev prenosnega omrežja	neustrezno upravljanje koničnih obremenitev prenosnega omrežja		
12.	čezmejne prenosne zmogljivosti (ČPZ)	neusklajenost izračuna čezmejnih prenosnih zmogljivosti, ni nadomestnih procedur v primeru okvar platform za dodeljevanje ČPZ	4 / 2 **8**	
13.	tehnični strateški kazalniki	neustrezni kazalniki preseganja maksimalnih dopustnih vrednosti napetosti, nedobavljene energije, količine prenesene električne energije, delež izgub pri prenosu električne energije, načrtovanih prenosnih zmogljivosti, zagotavljanje zanesljivih zvez	4 / 2 **8**	

14.	investicije	neustrezna in negospodarna vlaganja na področju obratovanja sistema	3 / 2 **6**	
15.	graditev prenosnega omrežja	ni proaktivnega delovanja z vsemi deležniki graditve omrežja, uvedba celovitega vodenja projektov z analitsko podporo vodenju projektov je pomanjkljiva	3 / 2 **6**	
16.	vzdrževanje prenosnega omrežja	pomanjkljiva kadrovska politika in sistem varnosti ter zdravja pri delu, ni prehoda iz časovno orientiranega načina vzdrževanja v zanesljivo orientirano vzdrževanje	3 / 1 3	
17.	neizvajanje presoj	ne izvajajo se integrirane presoje (notranje in zunanje) certificiranih sistemov upravljanja po mednarodnih standardih (sistem kakovosti, ravnanja z okoljem, varnost in zdravja pri delu, varovanja informacij, kriznega upravljanja, poslovne odličnosti ipd.)	3 / 1 3	
18.	neustrezen sistem upravljanja	sistem upravljanja ne temelji na podlagi uveljavljenih modelov in procesnega pristopa ter ne zagotavlja vodstvu metodološko podporo	3 / 1 3	
19.	koordinacija aktivnosti med strokovnimi službami	nekoordinacija aktivnosti med strokovnimi službami	2 / 1 2	
20.	viri poslovanja strokovnih služb	neučinkovita izraba virov poslovanja strokovnih služb	2 / 1 2	
21.	konfliktov interesov	konfliktov interesov zaradi neustrezne razdelitve nalog, pooblastil in odgovornosti	3 / 2 **6**	

22.	neustrezna vgradnja notranjih kontrol	neustrezna vgradnja notranjih kontrol (kontroling in poročanje)	3 / 1 **6**	
23.	nekooperativni odnosi	nekooperativni odnosi z zakonodajnimi institucijami, regulatorji, zunanjimi revizorji in poslovnimi združenji	2 / 1 2	
24.	neskladnost z zahtevami norm	neskladnost z zahtevami zakonodaje, standardov in kodeksov profesionalnega ravnanja	3 / 1 3	
25.	neobstoj notranjih politik	neobstoj in celovitost notranjih politik, aktov, standardov in navodil za poslovne procese	3 / 2 **6**	
26.	napake / kraje / poneverbe / izgube	napake / kraje / poneverbe / izgube, s posledično finančno izgubo	3 / 1 3	
27.	nedoseganja ciljev poslovanja	bilanca stanja: struktura sredstev in struktura obveznosti do virov sredstev, nista ustrezni	3 / 1 3	
28.	slab finančni izkaz	analiza uspeha poslovanja in računovodski izkazi ne dosegajo tržnih ciljev poslovanja	3 / 1 3	
29.	podpore poslovanja	neučinkovitost podpore poslovanja za doseganje poslovnih ciljev	3 / 2 **6**	
30.	spremembe poslovanja	neustrezno odzivanje na potrebne spremembe poslovanja	3 / 2 **6**	
31.	spremembe tehnologije	neustrezno odzivanje na potrebne spremembe tehnologije	4 / 2 **8**	
32.	organizacija dela	neustrezna organizacija in vodenje poslovanja	2 / 2 4	
33.	pogodbeni odnosi	slabo urejeni pogodbeni in drugi pravni odnosi s	2 / 2	

		tretjimi osebami	4	
34.	neurejenost pravnega sistema	neurejenost, nedelovanje in /ali neučinkovitost pravnega sistema v državi in / ali v širšem mednarodnem okolju	2 / 1 2	
35.	opozorilni sistem	namerna poškodba opozorilnega sistema	3 / 1 3	
36.	ocena tveganj	ocena tveganj ne obravnava resničnega stanja	4 / 2 **8**	
37.	eksplozija	eksplozija na industrijskem objektu	4 / 1 4	
38.	omrežje za prenos energije	poškodba omrežja za prenos električne energije	3 / 2 **6**	
39.	varnostno - tehnični predpisi	neupoštevanje mednarodnih varnostno -tehničnih predpisov	4 / 1 4	
40.	vzdrževanje opozorilnih naprav	slabo vzdrževanje opozorilnih naprav	3 / 1 3	
41.	nesodelovanje z institucijami	nesodelovanje z mednarodnimi in domačimi institucijami (obveščanje)	4 / 2 **8**	
42.	odgovornosti vodij organizacijskih enot	premajhne odgovornosti vodij organizacijskih enot in sposobnosti za izvajanje strategije in doseganje ciljev poslovanja	3 / 2 **6**	
43.	neustrezni dejavniki dela	nelogično oblikovanje strojev, opreme in instrumentov, stalne motnje in napake, slabo vzdrževana oprema	3 / 1 3	

44.	delovna obremenitev	visoka delovna obremenitev zaposlenega	3 / 2 **6**	
45.	neustrezne delovne razmere	dokazano slabi ergonomski in materialni pogoji za delo zaposlenih	3 / 1 3	
46.	delovne naloge	težke delovne naloge	2 / 1 2	
47.	nevarne naloge	nevarne ali neprijetne delovne naloge	3 / 1 3	
48.	ponavljajoče naloge	ponavljajoče se ali dolgočasne naloge	3 / 2 **6**	
49.	upočasnitev dela sistema	namerna upočasnitev dela sistema, sabotaža	4 / 2 **8**	
50.	nesreča pri delu	lažno prikazovanje nesreče pri delu	2 / 2 4	
51.	usposobljenost zaposlenih	premajhna usposobljenost in kompetentnost zaposlenih	2 / 1 2	
52.	delovne izkušnje	premajhne delovne izkušnje za doseganje ciljev poslovanja	3 / 1 3	
53.	delovni postopki	nepokritost delovnih postopkov z navodili	4 / 1 4	
54.	procesiranje poslovanja	neustrezno procesiranje poslovanja	4 / 1 4	

55.	pretok informacij	netočnost in nepravočasnost pretoka informacij	2 / 1 2	
56.	naraščanje obsega dela	preveliko naraščanje obsega dela	2 / 1 2	
57.	konice poslovanja	neobvladovanje konic poslovanja	2 / 1 2	
58.	nezdružljive funkcije	opravljanje nezdružljivih funkcij, neupoštevanje delitev pooblastil	3 / 2 **6**	
59.	dejansko stanje	prikrivanje dejanskega stanja	2 / 2 4	
60.	poročila in dokumenti	ponarejanje poročil in dokumentov	3 / 1 3	
61.	evidence poslovnih procesov	neusklajene evidence poslovnih procesov z dejanskim stanjem	3 / 1 3	
62.	knjigovodska poročila	neusklajenost knjigovodskih poročil	4 / 1 4	
63.	zakonodaja in interni akti	neskladnost z zakonodajo in internimi splošnimi akti	4 / 1 4	
64.	spremembe tehnologije dela	neustrezne spremembe tehnologije dela	4 / 1 4	
65.	vodstveni nadzor in notranje kontrole	neustrezno izvajanje vodstvenega nadzora in notranjih kontrol	3 / 1 3	

66.	revizijske ugotovitve in izvajanje priporočil	neupoštevanje revizijskih ugotovitev in izvajanja priporočil, od zadnje revizije je za posamezna poslovna področja preteklo daljše časovno obdobje (3 leta), so v razdobju od zadnje revizije poročali o pomanjkljivostih / napakah / incidentih	4 / 1 4	
67.	potres	potres je sunkovito nihanje tal, ki nastane zaradi premikanja zemeljskih plošč, velika materialna škoda, možno poškodovani in mrtvi zaposleni	5 / 1 **5**	
68.	povodenj	zaradi obilnih padavin, ki jih spremlja močan veter, narastejo vodotoki po državi, reke prestopijo bregove, **piha tudi močan veter,** možne poškodbe omrežja in RTP	4 / 2 **8**	
69.	orkan	vrteča se površina oblakov in vetrov z močno nevihtno dejavnostjo, poškodbe omrežja, ranjeni in mrtvi, velika materialna škoda, lahko tudi tornado, ciklon, vihar	4 / 1 4	
70.	žled	žled nastane, ko dežuje ali rosi pri temperaturah pod lediščem oziroma ko padavine v tekoči obliki padajo na podhlajeno podlago, žled oziroma žledenje najpogosteje nastane po obdobju hladnejšega vremena ob dotoku toplejšega in vlažnega zraka v višinah, poškodbe omrežja, prekinitev dobave energije	4 / 2 **8**	
71.	razlitja nevarnih snovi	razlitja velikih količin nevarnih snovi v zemljo (ogrožanje podtalnice)	4 / 2 **8**	

72.	gozdni požar	velik gozdni požar, poškodbe omrežja, ogroženost RTP	3 / 1 3	
73.	požar v mestu	večji požar v mestu, ogroženost RTP	4 / 1 4	
74.	zimska nevihta	močna zimska nevihta, poškodbe omrežja	3 / 1 3	
75.	požar v poslovni stavbi	požar v poslovni stavbi iz malomarnosti ali tehnične napake ali namerno	4 / 1 4	
76.	eksplozija	silovita sprostitev energije zaradi hitrega zvišanja tlaka in temperature, kar ima za posledico rušilno delovanje na okolico	3 / 1 3	
77.	IT sistem v poslovnih procesih	ni podvajanja kritičnih IT sistemov, ni preventivnega nadomeščanja stare strojne, programske in komunikacijske opreme, upravljanje centra za delovanje po katastrofi je pomanjkljivo, ni enotne točke interne komunikacije z odjemalci IT storitev (prijava napak in zahtev), nedodelan sistem za prepoznavanje in preprečevanje vdorov, uporaba mehanizmov za celostno spremljanje sistemov ni dosledna	4 / 1 4	
78.	telekomunikacija za obratovanje sistema	graditev TK omrežja ni vključena v strateški poslovni načrt, ni spremljanja razvoja TK storitev	3 / 2 **6**	

79.	zlonamerna programska oprema	obstoj zlonamerne programske opreme (Malware)	3 / 1 3	
80.	napad preko spletne strani	napad na sistem uporabnika preko spletne strani, katero zlorabijo za prenos zlonamerne programske opreme na ciljan sistem (Web based attacks)	3 / 2 **6**	
81.	napad na spletne aplikacije	napad na spletne aplikacije (Web application attacks)	3 / 2 **6**	
82.	mreža okuženih elektronskih naprav	mreža okuženih elektronskih naprav, ki komunicirajo s strežnikom ali med sabo, čakajoč na ukaz upravljavca mreže, mreža je lahko sestavljena iz »robotov« (Botnets), onemogočanje storitve	3 / 1 3	
83.	prejem večje količine podatkov	napad, s katerim tarča prejema večjo količino podatkov določenega protokola in s tem se znatno upočasni ali celo popolnoma zaustavi funkcioniranje storitve (Denial of service)	4 / 1 4	
84.	fizična škoda na IT sistemu	fizična škoda / protipravna odtujitev ali kraja / izguba (Physical damage / theft / loss)	3 / 1 3	
85.	notranja grožnja IT sistemu	notranja grožnja, lahko namerna ali nenamerna (Insider threat: malicious, accidental)	3 / 1 3	
86.	spletno ribarjenje	spletno ribarjenje (Phishing) je prevara, s katero se pridobi občutljive podatke, kar posledično lahko omogoči nepooblaščeni vstop, s pomočjo pošiljanja v ta namen prirejenih e-mail sporočil, kjer se izdajajo za	3 / 1 3	

		nekoga drugega		
87.	nezaželena elektronska pošta	spam je nadležna, vsiljena, nezaželena ali nenaročena elektronska pošta	2 / 2 4	
88.	zbirka kod za skeniranje IT sistema	zbirka kod za avtomatsko skeniranje in zlorabljanje oziroma izkoriščanje ranljivosti sistema (Exploit kits)	3 / 1 3	
89.	nepooblaščen pristop do tajnih podatkov	incident, pri katerem je nepooblaščena oseba prišla do občutljivih, tajnih ali drugače zaščitenih podatkov (Data breaches),	3 / 1 3	
90.	kraja identitete	kraja identitete, pri čemer nekdo prevzame osebno ime in ostale osebne informacije neke druge osebe (Identity theft)	3 / 1 3	
91.	izdaja informacije nepooblaščenemu uporabniku	IT sistem je zasnovan tako, da ščiti podatke pred zunanjimi prisluškovanji, lahko pa izda informacije nepooblaščenemu uporabniku (Information leakage)	3 / 2 **6**	
92.	dešifrator proti plačilu	kriptovirusi, ki šifrirajo podatke in ponujajo dešifrator proti plačilu (Ransomware)	3 / 1 3	
93.	pridobitev prednosti pred drugimi	oblika kibernetskega napada, kjer se pridobijo tajni in občutljivi podatki ali intelektualna last, z namenom pridobitve prednosti ali konkurenčnosti pred drugimi (Cyber espionage)	3 / 1 3	
94.	slaba razpoložljivost IT sistema	daljši izpad električne napetosti, napake v delovanju telekomunikacij	4 / 2 **8**	
95.	neprekinjeno poslovanje	nesposobnost zagotavljanja neprekinjenega	3 / 1	

		poslovanja, strankam se storitve ne zagotavlja neprekinjeno in na različnih platformah, neprekinjeno poslovanje je v kompleksnih IT-okoljih in procesih vedno težje dosegljivo	3	
96.	izguba integritete, zaupnosti podatkov ali izgube podatkov	s pomočjo goljufije, tatvine, raznih prevar in manipulacij, prestrezanja pretoka podatkov, eksplozije, sabotaže, vandalizma, terorizma	4 / 1 4	
97.	razkritja zaupnosti podatkov	podatki, ki so smatrani kot zaupni že po naravi, so dostopni, uporabljeni ali razkriti osebi, ki nima pooblastila za dostop do njih, izraba zaupanja zaposlenega	3 / 1 3	
98.	ogroženost iz okolja	masovni napad IT, delovanje škodljivih računalniških programov	3 / 1 3	
99.	razvoj informacijske tehnologije	neustrezni razvoj informacijske tehnologije, ne sledenje tehnološkim spremembam	3 / 1 3	
100.	socialni inženiring	gre za tehniko, s katero napadalec od žrtve pridobi zaupne podatke in informacije s pomočjo zlorabe zaupanja, je manipulacija, ki je psihološko pogojena, saj napadalec uporablja različne psihološke tehnike kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva	3 / 2 **6**	
101.	izdaja šifer	izdaja šifer za različne dostope, kontrolo dostopa, vstop v računalniški sistem, vstop posebej varovana	4 / 1 4	

		območja in prostori		
102.	prodaja izvirnih računalniških aplikacij	kraja intelektualne lastnine, protipravna pridobitev premoženja	3 / 1 3	
103.	reprogramiranje z namenom zlorabe	reprogramiranje IT sistema z namenom zlorabe, pojavijo se znaki zlorabe	3 / 1 3	
104.	korporativna varnost	neustrezna organiziranost korporativne varnosti, ni celote pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov ter skrbi za ohranitev reda, spoštovanje zakonov in internih splošnih aktov ter varnost zaposlenih in premoženja, ogrožanje poslovanja organizacije	4 / 2 **8**	
105.	notranje prevare	notranja prevara se pojavlja kot namerno zavajanje sodelavcev ali strank, izkoriščanje delovnega mesta, strokovnega znanja, zloraba virov in lastnine, nepošteno delovanje, vse z namenom pridobitve osebne materialne ali drugačne koristi ali v povezavi s sostorilci, ni ničelne tolerance do tega pojava	4 / 2 **8**	
106.	tehnično in mehansko varovanje	pomanjkljivo tehnično in mehansko varovanje, pojav škodnih dogodkov	3 / 1 3	
107.	neustrezno delovanje varnostne službe	pogodbeno najeti izvajalec fizičnega varovanja oseb in premoženja ne opravlja dejavnost v skladu z zakonodajo, s pravili stroke in z dobro prakso	3 / 1 3	
108.	alarmiranje	načrti alarmiranja izrednih dogodkov in odzivov na izredne dogodke so nezanesljivi in pomanjkljivi	3 / 2 **6**	

109.	pogodbeni izvajalec varovanja	pogodbeni izvajalec varovanja ne pozna in ne obvladuje varnostno vitalne točke v zgradbah in v okolici zgradb, ne pozna ocen ogroženosti, požarnega reda, sistema evakuacije, videonadzornega sistema, kontrole pristopa, sistema aktivne požarne zaščite in organiziranosti sistema zaščite ter reševanja	3 / 1 3	
110.	predlogi varnostnih izboljšav	pogodbeni izvajalec varnostnih storitev redko predlaga varnostne izboljšave, ker ne pozna ocen ogroženosti in varnostnih tveganj ter stopnjo učinkovitosti varnostnega sistema	3 / 1 3	
111.	izsiljevanje s talci	izsiljevanje vodstva organizacije s talci, tveganje ugleda, neprekinjenosti poslovanja	3 / 1 3	
112.	večji vlom	škodni dogodek	3 / 1 3	
113.	roparski napad	škodni dogodek	3 / 1 3	
114.	atentat na zaposlenega	poškodba, smrt zaposlenega	3 / 1 3	
115.	ugrabitev zaposlenega	finančna škoda	2 / 1 2	
116.	goljufije	preslepitve, ponarejanje, zavajanja, sleparjenje	3 / 1 3	

117.	dragoceni material in orodja	tatvina dragocenega materiala in orodij	2 / 1 2	
118.	alarmni sistem	poškodovanje alarmnega sistema z določenim nezakonitim namenom	3 / 1 2	
119.	sabotaža	namerno poškodovanje stroja, naprave, procesa, postopka	4 / 1 4	
120.	poslovanje v izrednih dogodkih	pomanjkljivo načrtovanje poslovanja v izrednih dogodkih	3 / 1 3	
121.	neprekinjeno poslovanje	pomanjkljivo načrtovanje neprekinjenega poslovanja	4 / 1 4	
122.	krizno vodenje	pomanjkljivo krizno vodenje, izguba ugleda	5 / 1 **5**	
123.	pandemije raznih bolezni	značilni znaki raznih pandemij in drugih bolezni	4 / 1 4	
124.	norovirus	značilni znaki norovirusa	3 / 1 3	
125.	okužba s hrano	značilni znaki zastrupitve s hrano	2 / 1 2	
126.	nalezljiva bolezen	pojav nalezljive bolezni	2 / 1 2	
127.	onesnaženje zraka	zdravstveni problemi, prekinitev poslovanja, finančna škoda	3 / 1 3	

128.	terorizem	kemični (uporaba strupov kot so sarin, soman, VX, novičok ipd.), biološki (razni biološki agensi), radioaktiven, strelski, ostrostrelski ali bombni napad, nacionalističen terorizem, verski terorizem, samomorilni napad	5 / 1 **5**	
129.	AMOK situacija	nasilno, morilsko in brezupno dejanje na območju organizacije, dejanje je naključno ali namerno	5 / 1 **5**	
130.	radikalizacija zaposlenega	nasilna **radikalizacija** in rekrutiranje zaposlenega za razna teroristična dejanja	3 / 1 3	
131.	viri nevarnosti	nizko zavedanje zaposlenih o virih nevarnosti	2 / 2 4	
132.	nasilje na delovnem mestu	fizično, verbalno ali neverbalno nasilje nad zaposlenem	2 / 2 4	
133.	neustrezno varovanje podatkov	neustrezno varovanje osebnih in tajnih podatkov, informacij in poslovnih skrivnosti	3 / 1 3	
134.	industrijsko vohunstvo	oviranje konkurence na različnih trgih, informacijsko bojevanje kot del obveščevalne dejavnosti organizacije	3 / 1 3	
135.	odločitev zaposlenega	neustrezna odločitev zaposlenega, na sprejemanje odločitve vpliva strokovno znanje, izkušnje, kognitivne pristranskosti, starost, samozaupanje, zaradi nepopolnih informacij zaposleni sprejema pogojno	3 / 1 3	

		dobre odločitve		
136.	zaznava nevarnosti	napačna zaznava nevarnosti, ki je odvisna od poznanosti nevarnosti, obsega, nedavnosti, ocenjena relativna pogostost, ki je povezana s številom različnih obnovljenih dogodkov in izstopanje nevarnosti	3 / 1 3	
137.	organiziranje in vodenje dela	neustrezno organiziranje in vodenje dela, nedoseganje ciljev poslovanja, finančna škoda	3 / 1 3	
138.	vodstveni nadzor	slab vodstveni nadzor, kaže se na naslednjih področjih: slabo načrtovanje, ni pregleda nad doseganjem zastavljenih ciljev, pomanjkljivo organiziranje dela, šibka koordinacija aktivnosti, pomanjkljivo spodbujanje zaposlenih in dodeljevanje nalog	3 / 1 3	
139.	nejasne pristojnosti in odgovornosti	niso ustrezno določeni standardi notranjega kontroliranja, obstaja pomanjkanje kontrolne zavesti pri izvajalcih, ni rednega načrtnega izvajanja notranjih kontrol in vodstvenega nadzora, funkcije kontrole in izvajanja so združene v eni osebi	3 / 1 3	
140.	izguba ključnih sodelavcev	odhod težko nadomestljivih strokovnjakov v konkurenčne organizacije	3 / 2 **6**	
141.	razdelitev funkcij, dolžnosti in pooblastil	nezagotavljanje razdelitve funkcij, dolžnosti in pooblastil, škodni dogodek, izguba ugleda	3 / 1 3	

142.	nadomeščanje zaposlenih	nenadomeščanje zaposlenih z ustrezno usposobljenimi zaposlenimi	2 / 1 2	
143.	spremembe internih aktov	neustrezni postopki sprememb in dopolnitev internih aktov	2 / 1 2	
144.	nagrajevanje dela	neustrezno nagrajevanje dela, slabša motiviranost, deviantno vedenje zaposlenega	2 / 2 4	
145.	produktivnost	neustrezna produktivnost zaposlenega, nedoseganje rezultatov dela	2 / 1 2	
146.	motivacija	neustrezna motivacija zaposlenih, povezano s slabo delovno uspešnostjo, ni eksplicitnih in implicitnih nagrad, ni pripadnosti organizaciji	2 / 1 2	
147.	samostojnost zaposlenega	neustrezna samostojnost zaposlenega, kar je posledica nekompetentnosti zaposlenega	3 / 1 3	
148.	neustrezna razporeditev zaposlenih	neustrezna razporeditev zaposlenih glede na njihovo strokovno znanje, kompetence, izkušnje	2 / 1 2	
149.	nepoštenost zaposlenih	nepoštenost na delovnem mestu se nanaša na namerno vedenje zaposlenega, ki ga organizacija ocenjuje kot nasprotujočega njenim legitimnim interesom, vedenje, ki krši pomembne organizacijske norme	3 / 1 3	
150.	javnimi nemiri in protesti	gre za nekonvencionalno participacijo izražanja nezadovoljstva, kot so **protesti,** demonstracije, javni **nemiri, izguba ugleda, finančna škoda**	3 / 1 3	

151.	usklajevanje dela	pomanjkljivo usklajevanje dela, napake, malomarnost, finančna škoda	2 / 1 2	
152.	nelojalnost	nelojalnost do delodajalca, nasilje in kršitve zakonskih aktov ter internih splošnih aktov	2 / 1 2	
153.	neetično delo, disciplinska odgovornost	sklepanje škodljivih pogodb, neupoštevanje konkurenčne klavzule, podkupovanje strokovnjakov, inovatorjev, vodstva in komercialistov, lažne bolniške odsotnosti, izplačevanje nadurnega dela, ki ga ni bilo, zamude na delo, uporabo potrošnega materiala za privatne namene	2 / 1 2	
154.	prejšnji izredni dogodki	neustrezni odzivi na prejšnje izredne dogodke	2 / 1 2	
155.	usposabljanje in komuniciranje	neučinkovito usposabljanje in komuniciranje	2 / 2 4	
156.	uporabniki storitev	demonstracija uporabnikov storitev pred poslovnimi objekti organizacije iz raznih razlogov	2 / 1 2	
157.	malomarnost	malomarnost ali napaka zaposlenega	2 / 1 2	
158.	pomota	pomota zaposlenega pri opravljanju procesa	2 / 2 4	
159.	vedenje na delovnem mestu	nepremišljeno vedenje na delovnem mestu	1 / 1 1	

160.	zdravje in varnost pri delu	slabo upravljanje zdravja in varnosti pri delu	2 / 1 2	
161.	delovna zmogljivost	zahteve po delovni zmogljivosti, ki presega zmožnosti zaposlenega	2 / 1 2	
162.	utrujenost	utrujenost zaposlenega, pojav škodnega dogodka	2 / 1 2	
163.	stres	posledice nezmožnosti zaposlenega, da se ta pravilno odzove na čustvene ali fizične grožnje, bodisi dejanske ali zamišljene, pojav škodnega dogodka	3 / 2 **6**	
164.	delovna izčrpanost	značilna je kronična utrujenost zaposlenega, čezmeren stres in pretirana obremenitev pripeljeta do delovne izčrpanosti, ki je posledica pretiranega dela	3 / 2 **6**	
165.	mobing	je oblika psihičnega nasilja na delovnem mestu, žrtev je izpostavljena sistematičnemu in dlje časa trajajočemu psihičnemu nasilju	3 / 1 3	
166.	spolno nadlegovanje	spolno nadlegovanje je kakršna koli oblika neželenega verbalnega, neverbalnega ali fizičnega vedenja spolne narave z namenom prizadeti dostojanstvo zaposlenega	3 / 1 3	
167.	pomanjkanje spanja	pomanjkanje spanja se lahko odrazi v škodnem dogodku zaradi omejenih sposobnosti zaznavanja poslovnih procesov	2 / 1 2	
168.	delovne poškodbe	pojav delovne poškodbe vpliva na nemotenost	2 / 1	

		poslovanja in finančno škodo	2	
169.	poklicne zdravstvene težave	neustrezno upravljanje varstva pri delu, finančna škoda	2 / 1 2	
170.	pranje denarja	pranje denarja je kaznivo dejanje in pomeni prikrivanje izvora denarja, ki je pridobljen iz nelegalnih poslov, oziroma dejavnosti in prelivanje denarja v legalne posle	3 / 1 3	
171.	korupcija	konflikt interesov, podkupovanje, neprimerna darila, prepovedane poslovne dejavnosti, nakup zastarele tehnologije	4 / 1 4	
172.	ponarejanje dokumentov	izdelava ponarejenega dokumenta ali predrugačenje pravega dokumenta z namenom, da bi se ta uporabil kot pravi	3 / 1 3	
173.	stavka zaposlenih	stavka in/ali druge vrste socialnih nemirov zaposlenih	2 / 1 2	
174.	alkohol ali mamilo	delo pod vplivom alkohola ali mamil, tveganje napak in malomarnosti	3 / 1 3	
175.	osebna opravila	opravljanje osebnih opravil med delovnim časom	2 / 1 2	
176.	kraja	pomoč zaposlenega pri kraji (tatvini)	2 / 1 2	
177.	inventurni manki	lahko se pojavijo v virih in sredstvih, do katerih je dostop manj nadziran, gre za dejanje, ko si zaposleni	2 / 1 2	

		protipravno prilasti del tujega premoženja, ki mu je zaupano		
178.	poškodovanje inventarja	malomarno ravnanje in poškodovanje inventarja	2 / 1 2	
179.	nenamenska uporaba službene opreme	nenamenska uporaba službenih vozil, orodij, naprav, strojev v privatne namene	2 / 1 2	
180.	finančna tveganja	letno, mesečno in dnevno planiranje denarnih tokov je pomanjkljivo, zavarovanje terjatev ni ustrezno, ne upošteva se načela razpršenosti deponiranih denarnih sredstev, uporaba instrumentov za obvladovanje obrestnih tveganj ni dosledno	4 / 1 4	
181.	naročanje blaga in storitev	neustrezno obvladovanje javnih naročil, nedosledni postopki in razmejene odgovornostmi	3 / 2 **6**	
182.	zavarovalne pogodbe	neustrezna analiza obstoječih zavarovalnih pogodb	3 / 1 3	
183.	izplačane odškodnine	ni analize stroškov in učinkov zavarovanja, notranji ukrepi za preprečevanje škod in izgub niso določeni	3 / 1 3	
184.	pogajanja z zavarovalnico	priprava argumentov za pogajanja z zavarovalnico	3 / 1 3	

Analiza in rangiranje skupno 184 virov nevarnosti in tveganih scenarijev (produkt ocene resnosti in verjetnosti ogrožanj je bil nad 5) kaže na skupino virov nevarnosti, kateri mora vodstvo organizacije posvetiti posebno pozornost pri obvladovanju tveganj. To so: upoštevanje Kodeksa omrežja, zagotavljanje sistemskih storitev, oddaja energije, čezmejne prenosne zmogljivosti, tehnični strateški kazalniki, investicije, graditev prenosnega omrežja, konfliktov interesov, vgradnja notranjih kontrol, izdelava notranjih politik, podpore poslovanja, spremembe poslovanja, spremembe tehnologije, ocena tveganj, omrežje za prenos energije, nesodelovanje z institucijami, odgovornosti vodij organizacijskih enot, delovna obremenitev zaposlenih, ponavljajoče naloge, upočasnitev dela sistema, opravljanje nezdružljivih funkcij, potres, povodenj, žled, razlitja nevarnih snovi v zemljo, graditev telekomunikacijskega omrežja za obratovanje sistema, napad preko spletne strani, napad na spletne aplikacije, izdaja informacije nepooblaščenemu uporabniku, slaba razpoložljivost IT sistema, socialni inženiring, organiziranost korporativne varnosti, notranje prevare, alarmiranje o izrednem dogodku, krizno vodenje, terorizem, amok situacija, izguba ključnih sodelavcev, stres zaposlenih, delovna izčrpanost zaposlenih, naročanje blaga in storitev. Skupno 41 od 184 virov nevarnosti in tveganih scenarijev (22%) sodi med tiste, katerim mora vodstvo organizacije posvetiti posebno pozornost.

Tabela 22: Ocena kritičnosti - okvir najslabših možnih scenarijev

Vzorec opisa najslabših scenarijev	Vpliv na poslovni proces	Vpliv na zaupanje uporabnikov	Vpliv na finančna sredstva	Obrazložitev ocene	Produkt ocen vplivov	Rang scenarija
Neupoštevanje Kodeksa omrežja	1	2	5	oneomogočanje preskrbe evropskega trga z električno energijo	10	5.
Nezagotavljanje sistemskih storitev	1	4	4	izmenjava viškov energije med sosednjimi sistemskimi operaterji je neustrezna	16	4.
Neustrezni tehnični strateški kazalniki	2	3	4	neustrezni kazalniki nedobavljene energije, delež izgub pri prenosu električne energije	24	3.
Konflikt interesov	1	4	2	konflikt interesov zaradi neustrezne razdelitve nalog, pooblastil in odgovornosti	8	6.
Žled	4	4	5	poškodbe omrežja, prekinitev dobave energije, velika škoda	80	1.
Napad preko spletne strani	3	4	3	napad na spletne aplikacije organizacije	36	2.

Iz zgornje tabele so razvidni trije najslabši možni scenariji ogrožanja poslovanja organizacije, in sicer: naravna nesreča žled na večjem območju RS, IT napad na spletne aplikacije in neustrezni tehnični strateški kazalniki oskrbe z električno energijo.

Ocena sredstev za preprečevanje tveganj (5. korak)

Na zaključku uporabe metodologije MOSAR za navedeni primer se je treba **odločiti o načinih odpravljanja ali obvladovanja tveganj.** Na tej stopnji je treba razmisliti o naslednjem:

- ali je mogoče tveganja odpraviti,
- če to ni mogoče, kako je mogoče tveganja obvladovati, da ne bodo ogrožala neprekinjenegao poslovanja sistema,
- zagotoviti ustrezna finančna sredstva in kadre.

Pri preprečevanju in obvladovanju tveganj je treba upoštevati naslednja **splošna načela:**

- izogibanje tveganjem,
- zamenjava nevarnega tveganja z nenevarnim ali manj nevarnim,
- obvladovanje tveganj pri viru,
- uvajanje kolektivnih varnostnih ukrepov ima prednost pred individualnimi varnostnimi ukrepi in postopki,
- prilagajanje tehničnemu napredku,
- prizadevanje za izboljšanje ravni varnosti v sistemu,
- določena tveganja prenesti na zavarovalnico.

Naslednji korak je **vzpostavitev preventivnih ali varnostnih ukrepov**. Pomembno je, da se v postopek vključijo pristojni zaposleni ali njihovi predstavniki. Za učinkovito izvajanje je med drugim treba sestaviti načrt, ki določa:

- ukrepe, ki se bodo izvajali,
- kdo bo kaj storil (pooblastila vodstva) in kdaj,
- do kdaj mora biti naloga opravljena,
- pomembno je, da ima izvajanje ukrepov za odpravljanje ali preprečevanje tveganj prednost pred drugimi nalogami.

Prepoznavanje funkcij sistema (6. korak)

Izdela se prepoznavanje funkcij sistema, npr. cilj poslovanja sistema je, da sistemski operater elektroenergetskega prenosnega omrežja skrbi za varen, zanesljiv in neprekinjen prenos energije. Z vpetostjo v evropsko KI soustvarja energetsko prihodnost RS s tem, da vzdržuje, načrtuje, gradi in posodablja prenosno omrežje, za zadovoljitev naraščajočih potreb pravnih in fizičnih oseb po električni energiji. Uporabniki storitev sistema pričakujejo neprekinjeno, kvalitetno, zanesljivo in nizko cenovno oskrbo z elektriko.

Opravi se temeljit pregled produkta / procesa v ločenih podsistemih, elementih, delih, sklopih in opredeli njihove funkcije. V našem primeru bomo analizirali vpliv opreme v elektroenergetiki in sicer delovanje RTP in njen vpliv na delovanje sistema.

Elektroenergetski sistemi imajo vrsto mest, primer RTP, kjer se tokokrogi stikajo in ločujejo, vežejo razne dele elektroenergetskih naprav v sistemske kombinacije, spreminjajo v mreži napetosti in opravljajo stikalne manevre. RTP je povezana z več vodi prenosnega ali razdelilnega omrežja in je stičišče določene napetosti, kjer se preko transformatorjev transformira napetost na nižji napetostni nivo. Ob tem obstaja možnost, da se v RTP-ju selektivno izloči napake ipd.

Analizirali bomo tveganja napajalne RTP kot objekta javne gospodarske infrastrukture, ki se nanašajo na projektno delo za izgradnjo RTP, izdelavo gradbeno - tehnične dokumentacije, izbor lokacije RTP, gradnjo RTP, tveganja poslovnega procesa, armirano-betonsko stavbo (s koritom za odpadna olja in ograjo), električno opremo (komandna plošča, transformator, energetski kabli, kabelski snopi, naprave zaščite, vodenja in meritev, zaščitni releji, naprave za prenos kriterijev, razvodi lastne porabe, usmerniki, napajalniki, ozemljitvene povezave, notranja oprema, osnovna zaščitna oprema, hlajenje RTP), komunikacijske opreme (programska in strojna oprema ter naprave, ki so potrebne za nemoteno delovanje RTP), varnostnega sistema (mehanska zaščita, kontrola pristopa, protivlomni sistem, protipožarni sistem, video nadzor, prenos alarmnega signala), vzdrževanja RTP, vodstveni nadzor, notranje kontrole, Notranja revizija, poročila.

Identifikacija načinov odpovedi (7. korak)

Osnova je identifikacija načinov odpovedi (najbolj kritične scenarije iz rdeče cone po metodi MOSAR se prenese v delovni list FMEA).

Vprašanje je »Kaj se zgodi, ko se pojavi ta odpoved?« Za vsako funkcijo RTP bomo identificirali način odpovedi poslovanja po naslednjih kriterijih: zaposleni, stroji, materiali,

okolje, varnost. Sledi identifikacija posledic načinov odpovedi delovanja RTP in z njim povezanih podsistemov ter procesov. To so potencialni učinki odpovedi. Za vsak način odpovedi se določi možni vzrok (npr. sistemska napaka, degradirano delovanje, odpoved delovanja RTP, takojšnji učinek, popolna napaka, delna napaka, prekinitvena napaka, deluje zunaj specifikacije, nenamerna funkcija ipd.) in določi se končni učinek odpovedi.

Ocena tveganja (8. korak)

Za vsak način odpovedi se oceni resnost posledic **Si** (angl. Severity of effects), pogostost pojavitve **Oi** (angl. Occurence of failures) in možnost pravočasnega zaznavanja (odkrivanja) odpovedi **Di** (angl. Detection of failures). Vsak način in kriterij ocenimo z ocenami od 0 do 10 na podlagi spodaj naštetih dejavnikov resnosti, pogostosti in pravočasnosti zaznavanja načinov odpovedi.

Ocena resnosti (S) je ocenjena na lestvici od 1 do 10, kjer 1 je nepomembna in 10 je katastrofalna (prikazana je v Tabeli 23). Če ima odpoved več kot en učinek, se v delovni list FMEA vpiše samo najvišja ocena resnosti.

Ocena resnosti (S)

Osnovno vprašanje je: »Kaj bi lahko šlo narobe?«. Določi se resnost odpovedi (v najslabšem primeru neželeni končni učinek). Te učinki se nanašajo na ugotovitve uporabnika, izkušnje s področja funkcionalne okvare RTP ali dobre prakse. Primeri teh učinkov so npr.: popolna izguba funkcije, omejena učinkovitost delovanja, prepozno ali neredno delovanje ipd. Resnost se obravnava na osnovi stroškov in / ali izgube življenja zaposlenih in drugih. V nadaljevanju je v Tabeli 23 prikazana tipična razvrstitev.

Tabela 23: Kriteriji za resnost odpovedi (smiselno prirejeno po standardu)

Ocena	Učinek	Kriterij za resnost
1	Ni	Ni učinka na kvaliteto, neprekinjenost, zanesljivost in varnost RTP
2	Nepomemben	Zelo majhen vpliv na funkcije RTP. Zelo majhen učinek, brez poškodb, le posledice pri vzdrževanju sistema
3	Zelo nizek	Majhen vpliv na funkcije RTP
4	Nizek	Majhen učinek na funkcije RTP, ni potrebno popravilo

5	Srednji	RTP potrebuje popravilo. Manjši učinek, nizka škoda, lahko lažja telesna poškodba
6	Pomemben	Nekatere funkcije RTP ne delujejo, neredno delovanje
7	Velik	RTP morda ni več operativen, omejena učinkovitost delovanja
8	Zelo velik	RTP ni več operativen, izguba ugleda, finančna škoda
9	Resen	Odpoved primarnih funkcij RTP povzroča izgubo ugleda pri uporabnikih, lastnikih in upravljavcih, nevarnost za zaposlene (hude poškodbe, možna smrt), visoka finančna škoda
10	Zelo resen	Popolna izguba funkcije, nevarnost za zaposlene in premoženje nastopi brez opozorila. Katastrofalen učinek (ni dobave električne energije, popolno nevarno delovanje, mogoče več smrti zaposlenih), zelo visoka finančna škoda

Za vsak vzrok odpovedi se določi verjetnost pojavljanja (O). Pojav je ocenjen na lestvici od 1 do 10, kjer je 1 zelo malo verjeten in 10 je neizogiben (prikazan v Tabeli 24). V delovni list FMEA se vpiše rating za vsak vzrok. Za vsak vzrok (element) se opredeli tudi trenutni proces notranje kontrole. To so testi, ukrepi, postopki ali mehanizmi, ki so vzpostavljeni. Te kontrole lahko preprečijo vzrok in zmanjšajo verjetnost, da se bo vzrok odpovedi zgodil ali odkrivajo napake preden je prizadet uporabnik.

Ocena verjetnosti (O)

Osnovno vprašanje je: »Zakaj bi se zgodila odpoved?«. Verjetnost pojava se oceni s pomočjo izračunov, statističnih podatkov, analize podobnih procesov, dobre prakse in raznih odpovedi RTP, ki so bile dokumentirane v preteklosti. Vzrok za odpoved je treba obravnavati kot slabost RTP-ja. Vse možne vzroke odpovedi se dokumentira in tako se ustvari zgodovinska baza podatkov. Vzroki so lahko: neskladnost poslovanja s predpisi, nezanesljivost zaposlenega, napake pri upravljanju in delovanje RTP ipd. V nadaljevanju je v Tabeli 24 prikazana tipična razvrstitev.

Tabela 24: Kriteriji za verjetnost odpovedi (smiselno prirejeno po standardu)

Ocena	Pogostost odpovedi	Kriteriji za verjetnost
1	<= 1×10^{-6} 1 na 1.000.000	Skoraj nemogoča odpoved, napaka na RTP odpravljena z notranjo kontrolo
2	1×10^{-5} 1 na 100.000	Zelo majhna verjetnost odpovedi
3	1×10^{-4} 1 na 10.000	Majhna verjetnost odpovedi
4	4×10^{-4} 1 na 25.000	Relativno nizka verjetnost odpovedi
5	2×10^{-3} 1 na 500	Srednje nizka verjetnost. Občasna napaka
6	1×10^{-2} 1 na 100	Srednje visoka verjetnost odpovedi
7	4×10^{-2} 1 na 25	Visoka verjetnost odpovedi
8	0,2 1 na 10	Ponavljanje odpovedi
9	0,33 1 na 3	Zelo visoka verjetnost odpovedi
10	>= 0.55 1 na 2	Odpoved skoraj neizogibna, nov tehnološki proces RTP, RTP brez zgodovine

Ocena odkrivanja (D), detektabilnosti

Za vsak kontrolni ukrep se določi oceno odkrivanja (ugotavljanja), oznaka D. S tem se ocenjuje, kako učinkovit je vodstveni nadzor, notranje kontrole, notranja revizija in ali je možno odkriti vzrok odpovedi preden je prizadet končni uporabnik. Odkrivanje je ocenjeno na lestvici od 1 do 10, kjer 1 pomeni zelo učinkovit nadzor in 10 pomeni slab nadzor (ali nadzora sploh ni!).

Sredstva ali metode, s katerim odkrijemo odpovedi, lahko trajajo nekaj časa. To je pomembno za nadzor vzdrževanja (razpoložljivost RTP) in je še posebej pomembno za več scenarijev odpovedi. Ta vključuje mirujoče načine (npr. sistem neposrednega učinka) ali

latentne napake (npr. poslabšanje kvalitete materialov, kot so energetski kabli, kabelski snopi, kovine ipd.). Potrebno je pojasniti kako je napako ali vzrok odkril operater ali vzdrževalec ali jo je odkril – javil samodejni odzivni sistem. V nadaljevanju je v Tabeli 25 prikazana tipična razvrstitev.

Tabela 25: Kriteriji za oceno odkrivanja (smiselno prirejeno po metodologiji)

Ocena	Ocena odkrivanja napak
1	Skoraj zanesljiva detekcija, napako na RTP odkrije operater ali vzdrževalec
2	Zelo visoka verjetnost detekcije, napaka odkrita z avtomatsko kontrolo
3	Visoka verjetnost detekcije
4	Srednje visoka verjetnost detekcije
5	Srednja verjetnost detekcije
6	Nizka verjetnost detekcije
7	Zelo nizka verjetnost detekcije
8	Malo verjetna možnost detekcije
9	Zelo nizka verjetnost detekcije, napako na RTP je težko odkriti
10	Absolutno nemogoča detekcija, brez trenutne detekcije ali se ne analizira napak RTP

Izračun faktorja tveganja

Izračuna se faktor tveganja RPNi (angl. Risk Priority Number) = Si x Oi x Di (zmnožek treh ocen: RPN = resnost x pogostost x odkrivanje). Faktorje tveganja RPN uredimo po velikostnem redu, kjer je skupni RPN = ∑{i=1..n} RPNi.

Če je ocena faktorjev S,O ali D med 1 in 2, to pomeni manjši vpliv, med 9 in 10 pa večji vpliv na sistem, pri čemer je RPN_{max} = 10 × 10 × 10 = 1000, RPN_{min} = 1 × 1 × 1 = 1, **prag za kritično infrastrukturo je RPN 10.**

Zmanjšanje ali odpravo vzrokov odpovedi (9. korak)

Prepoznavanje priporočenih aktivnosti, ukrepov in postopkov iz navodil in dobre prakse se nanaša na zmanjšanje ali odpravo vzrokov odpovedi in so lahko proces sprememb in dopolnitev pogojev delovanja RTP, dodatna oprema ali kontrolni sistem za izboljšanje detekcije odpovedi. Aktivnosti, ki jih je treba sprejeti, so podrobno opisane, kakšni ukrepi in postopki so bili izvedeni s strani odgovornega zaposlenega, in rezultati teh aktivnosti. Pri tem je potrebno upoštevati:

- ukrepe je treba izpolniti do končnega cilja,
- če ni odpravljen način vzroka odpovedi, se resnost ne sme spremeniti,
- vzrok odpovedi se lahko ali ne zniža na podlagi rezultatov ukrepanja,
- odkrivanje se lahko zmanjša ali ne zniža na podlagi rezultatov aktivnosti,
- če se ocene resnosti, pogostosti ali odkrivanja ne izboljšajo, je treba dodatno opredeliti priporočene ukrepe.

Upošteva se tudi, kdo je odgovoren za te aktivnosti (ime in priimek, ne le delovna funkcija) in ciljni datumi zaključka.

Ko so aktivnosti izvedene, se v določenem časovnem obdobju po zaključku implementiranja preventivnih in korektivnih ukrepov ter postopkov ponovno vrednoti O, S in D in nove RPNs.

Po njihovi implementaciji se postopek FMEA v razumnem roku ponovi z izdelavo novega delovnega lista FMEA.

Tabela 26: Primer FMEA delovnega lista

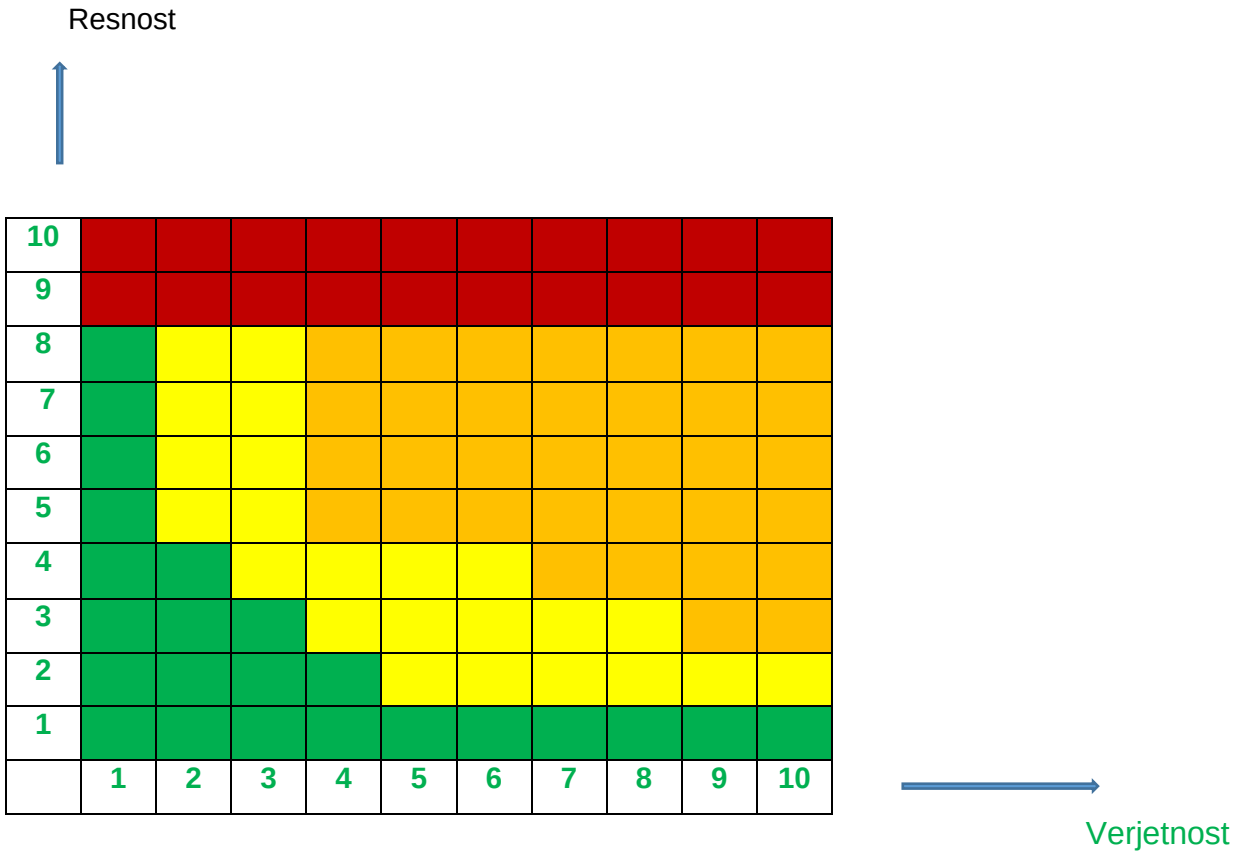
Primer FMEA delovnega lista												
Proces:	RTP							Številka FMEA:	1			
Projektna skupina:	ICS							Datum izdelave:	1.10.2018			
Vodja skupine:	NN							Datum revizije:				
Primer delovnega lista FMEA												
FMEA ref.	RTP	Možni način odpovedi	Možni vzrok odpovedi	Končni učinek	Ocena resnosti (S)	Ocena verjetnosti (O)	Ocena odkrivanja (D)	Tveganja na ravni RPN=SxOxD	Predlagani ukrepi	Odgovoren	Izvedene aktivnosti	Ponovna ocena S, O, D, RPN

Razdelani delovni list je posebej prikazan v nadaljevanju.

Matrika tveganj

V matriko tveganj (prikazana v Tabeli 27) se vnesejo rezultati faktorjev tveganja RPNi.

Tabela 27: Matrika tveganj FMEA (smiselno prirejeno po standardu)



Legenda:

Kritično tveganje | Visoko tveganje | Srednje tveganje | Nizko tveganje

V delovnem listu FMEA smo analizirali 29 možnih vzrokov za odpoved delovanja RTP. Iz matrike tveganj izstopa kritično tveganje pojav žleda (resnost 10, verjetnost 1, odkrivanje 1) in več srednjih tveganj (nepopolna specifikacija del projektne skupine za izgradnjo RTP 5/2/1; izgube pri prenosu energije 7/2/1; neustrezna mehanska zaščita RTP 6/2/1 in nevgradnja notranjih kontrol delovanja RTP 6/2/1), skupno 5 vzrokov odpovedi.

Upravljanje tveganj (10. korak)

Strokovnjaki na podlagi dobre prakse poudarjajo, da je popolna varnost in zaščita skoraj neuresničljiva naloga. Vendar se najvišji možni stopnji varnosti in upravljanju tveganj s primerno izbiro ustreznih zaščitnih ukrepov, postopkov, aktivnosti ter z njihovo izvedbo v praksi lahko zelo približamo.

Iz vsebinskega vidika lahko v splošnem upravljanje tveganj razvrstimo v naslednje skupine:

- osebno tveganje (personal risk) – v ekonomskem smislu pomeni možnost izgube / škode prihodka in/ali sredstev,
- tveganje pri premoženju (property risk) – to je prisotno pri lastništvu sredstev ali premoženja. Dejavniki tveganja premoženja so možnost poškodbe, uničenja ali kraje,
- tveganje v zvezi z odgovornostjo (liability risk) – ki ga ureja pravni sistem in pomeni tveganje v odnosu do tretjih oseb in/ali njihove lastnine,
- tveganje, ki nastane kot posledica neuspeha drugih in se kaže kot neizpolnitev pogodbenih obveznosti in vključuje tudi finančne posledice.

Upravljanje s tveganji se ne nanaša samo na skladnost s predpisi, temveč tudi na način razumevanja poslovanja organizacije, kar ima dolgoročen vpliv nanjo. Tveganje lahko predstavlja priložnost za zagotovitev konkurenčne prednosti, upravljanje tveganj pa je odločilno za uspešno poslovanje in mora biti v središču pozornosti vodstva organizacije.

Upravljanja tveganj se opredeljuje kot nenehen proces, ki poteka v organizaciji in se nanaša na prepoznavanje negotovosti (tveganj in priložnosti); ocenjevanje tveganj z vidika resnosti, pogostosti in možnosti odkrivanja ter s tem povezano določanje prednostnih tveganj (rangiranje ali prioritiziranje tveganj); odločanje o tem, kako ravnati s prepoznanimi tveganji in nadziranja tveganj.

Tveganje obsega tako tveganja, povezana s strategijami in poslovanjem, gospodarskim okoljem, v katerem deluje organizacija, tveganja povezana s skladnostjo z zakoni in predpisi ter računovodskim poročanjem in nenazadnje tveganja povezana z upravljanjem organizacije. Več o tem je predstavljeno v uvodnih poglavjih študije.

Tabela 28: Primer izpolnjenega FMEA delovnega lista

Proces:	RTP	Številka FMEA:	1
Projektna skupina:	ICS	Datum izdelave:	1.10.2018
Vodja skupine:	NN	Datum revizije:	

Primer delovnega lista FMEA

FMEA ref.	RTP	Možni način odpovedi	Možni vzrok odpovedi	Končni učinek	Ocena resnosti (S)	Ocena verjetnosti (O)	Ocena odkrivanja (D)	Tveganja na ravni RPN=SxOxD	Predlagani ukrepi	Odgovoren	Izvedene aktivnosti	Ponovna ocena S, O, D, RPN
1.	**Projektna skupina**											
	Specifikacija delov	Nepopolna specifikacija del	Nepoznavanje, napaka, malomarnost	Škoda	5	2	1	**10**	Upoštevanje standardov in dobre prakse	NN		
	Finance	Prekoračitev proračuna	Napačna kalkulacija	Pomanjkanje vira sredstev	5	1	1	5	Ustrezno planiranje investicije	NN		
	Rok	Časovna stiska	Slabo planiranje, dodatne naloge	Plačilo penalov, škoda	3	1	1	3	Uskladiti aktivnosti z delovnimi načrti	NN		
2.	**Gradnja RTP**											
	Naročanje blaga in storitev	Neskladno z zakonom	Pohlep	korupcija	8	1	1	8	Upoštevanje zakonskih določil	NN		

	Dokumentacija	Nepopolna dokumentacija	Malomarnost	Konstrukcijske napake	5	1	1	5	Upoštevanje zakonskih določil	NN		
	Nadzor	Pomanjkljiv nadzor nad gradnjo	Napaka	Neskladnost z načrti	4	2	1	8	Upoštevanje zakonskih določil	NN		
3.	**Objekt RTP**											
	Bazen za olje	Izpust olja	Tehnična napaka, malomarnost	Onesnaženje okolja, škoda	9	1	1	9	Proučiti zmogljivosti za najslabši scenarij	NN		
	Žled	Poškodba omrežja, prekinitev dobave energije	Naravna nesreča	Izguba ugleda, velika škoda	10	1	1	**10**	Simulacija razmer, vaja	NN		
4.	**Električna oprema**											
	Komandna plošča	Prekinitev delovanja	Sistemska tehnična napaka	Degradirano delovanje	5	1	1	5	Upoštevanje navodil za delo	NN		
	Transformator	Prekinitev delovanja, okvara	Tehnična napaka, slabo vzdrževanje	Prekinitvena napaka, deluje izven specifikacije	4	1	1	4	Upoštevanje navodil za delo	NN		
	Kabelski snopi	Poškodba kablov	Tehnična napaka, slabo vzdrževanje, višja sila	Prekinitvena napaka	4	2	1	8	Upoštevanje navodil za delo	NN		
5.	**Poslovni procesi**											
	Preskrba trga z energijo	Delna ali popolna odpoved oskrbe	Sistemska napaka	Škoda, izguba ugleda	8	1	1	8	Simulacija scenarija, priprava ukrepov	NN		
	Izmenjava viškov energije	Ni izmenjave ali je le delna	Sistemska napaka	Škoda	4	2	1	8	Upoštevanje dobre prakse	NN		

	Dopustne vrednosti napetosti	Preseganja dopustnih vrednosti napetosti	Sistemska napaka	Škoda	3	1	1	3	Upoštevanje dobre prakse	NN		
	Nedobavljena energija	Težave z dobavo	Degradirano delovanje	Škoda, izguba ugleda	4	1	1	5	Simulacija scenarija, priprava ukrepov	NN		
	Prenos energije	Izgube pri prenosu energije	Sistemska napaka	Škoda	7	2	1	**14**	Upoštevanje dobre prakse	NN		
6.	**Komunik-acijska oprema**											
	Programska oprema	Slaba razpoložljivost IT sistema	Sistemska napaka, degradirano delovanje, vpad v sistem	Nepregledno st poslovanja	7	1	1	7	Vpeljava standarda ISO 27001	NN		
	Strojna rač. oprema	Okvara strojne rač. opreme	Okvara	Popolna ali delna prekinitev delovanja	6	1	1	6	Nabava kvalitetne oprema v skladu s standari, vzpostavitev sekundarne lokacije	NN		
7.	**Varnostni sistem**											
	Mehanska zaščita	Neustrezna mehanska zaščita	Pomanjkljivo načrtovanje, sabotaža	Škoda	6	2	1	**12**	Analiza terorističnih dejanj	NN		
	Kontrola pristopa	Nekontroliran vstop v objekt	Varnostno tveganje	Škoda	3	1	1	3	Navodila za delo	NN		
	Protivlomni sistem	Nedelovanje sistema	Nepravilna konfiguracija, tehnična napaka	Škoda	3	1	1	3	Upoštevanje dobre prakse	NN		
	Protipožarni sistem	Nedelovanje sistema	Nepravilna konfiguracija, tehnična napaka	Velika škoda	5	1	1	5	Upoštevanje dobre prakse	NN		

	Video nadzor	Nedelovanje sistema	Nepravilna konfiguracija, tehnična napaka	Škoda	3	1	1	3	Navodila za delo	NN		
	Prenos alarmnega signala	Ni prenosa signala za alarmiranje o izrednem dogodku	Tehnična napaka, sabotaža	Velika škoda	7	1	1	7	Navodila za delo	NN		
8.	**Vzdrževa-nje RTP**											
	Zaposleni	Delovna izčrpanost zaposlenih	Izraba zaposlenih	Škoda	5	1	1	5	Varna kadrovska politika	NN		
	Skrbnost dobrega gospodarja	Popolno ali delno nedelovanje RTP	Neustrezno organiziranje in vodenje dela	Škoda	6	1	1	6	Načrt vzdrževanja	NN		
9.	**Vodstveni nadzor**											
	Konflikt interesov	Neustrezna razdelitev nalog, pooblastil in odgovornosti	Pohlep, nejasne odgovornosti	Izguba ugleda, škoda	6	1	1	6	Etični kodeks, organiziranje del	NN		
	Notranje kontrole	Nevgradnja notranjih kontrol delovanja RTP	Možnost notranje prevare	Izguba ugleda, velika škoda	6	2	1	**12**	Sistematična vgradnja notranjih kontrol	NN		
	Sledljivost postopkov	Netransparent nost postopkov	Pomanjkljiv nadzor	Škoda	5	1	1	5	Vzpostavitev standarda poslovne odličnosti ISO 9001, EFQM	NN		

ZAKLJUČEK

Potrebno se je zavedati groženj, ki jih v sistem nacionalne varnosti prinašajo spremenjene varnostne razmere v svetu. Politično, socialno, ekonomsko in ekološko destabilizirana območja, teroristične organizacije, mednarodni organiziran kriminal, množične migracije, naravne in tehnološke nesreče bodo v prihodnje temeljni viri ogrožanja varnosti in posledično KI.

V kontekstu razmerja zaščite KI do obvladovanja tveganj govorimo o zelo pomembnih dilemah pred katerimi se danes nahajajo posamezne države pri zaščiti in sploh opredeljevanju KI, ki je nujna za delovanje celotne družbe. Rešitve so obremenjene z različnimi dejavniki, ki vplivajo na njihovo sprejemanje in izvajanje in jih najlažje umestimo v dileme povezane z razmerji javnega in zasebnega in na drugi strani določanja pomembnosti posameznega področja KI. Povezovanje tega segmenta v celovit sistem zagotavljanja nacionalne in posledično tudi mednarodne varnosti, bo ravno s stališča koordinacije in zavedanja o potrebnosti ureditve, zelo zahteven projekt, ki bo pri vseh vpletenih straneh pomenil pomembno spremembo v pristopih in miselnosti. Vsekakor pa je potrebno vzpostaviti ustrezno zavedanje, da je samo učinkovita ocena ogroženosti tista podlaga za sprejemanje celovitih odločitev v procesu obvladovanja tveganj za delovanje KI.

Navedene postavke v kombinaciji z nujnostjo celovitega pristopa nas navajajo k ugotovitvi, da mora imeti vsaka država razvitih nekaj osnovnih sistemskih mehanizmov za zaščito KI. Pri KI gre v bistvu za socio-tehnične sisteme, kar pomeni, da se njihova zaščita ne nanaša samo na reševanje tehničnih vprašanj, temveč socio-tehničnih vprašanj, kar vključuje tudi sistemska vprašanja. To tudi pomeni, da sistemski mehanizmi zaščite KI zajemajo netehnične in tehnične vidike. Asimetrična načela so izdelana na podlagi asimetričnega razumevanja groženj KI. Zato je mrežno delovanje odgovor na mrežne probleme, ki se lahko oblikujejo. Pri tem pa je treba zaščititi predvsem centralne točke v mreži in ne toliko periferije. Da pravilno razumemo pomen posameznega dela sistema KI je nujno, da v osnovi izvedemo učinkovito in metodološko ustrezno ocenjevanje, upravljanje in obvladovanje tveganj za neprekinjeno delovanje te KI.

Želja po popolnem nadzoru je utopija, tako kot je utopija popolna varnost. V tem okviru je vedno potrebno vsak varnostni mehanizem tehtati v razmerju do virov, ki jih imamo na voljo in na drugi strani vedno ocenjevati tudi realnost in operativnost izvedenih ukrepov za povečanje ali izboljšanje nadzora nad določenim delom sistema KI.

Kljub različnim pristopom do odpravljanja oziroma zmanjševanja groženj KI se v vseh družbenih strukturah nacionalnega ali mednarodnega okolja kot celote, vendarle dajo razbrati posamezne ugotovitve, ki jih lahko povežemo na skupni imenovalec. Ta skupni imenovalec pa obsega potrebo po sodelovanju, izmenjavi informacij, dobrih praks delovanja in izkušenj ter skupni koordinaciji subjektov na nacionalni in še bolj na mednarodni ravni pri zoperstavljanju grožnjam, ki najbolj ogrožajo nemoteno delovanje KI.

Povezovanje predhodno navedenega segmenta v celovit sistem zagotavljanja nacionalne varnosti in posledično tudi mednarodne, bo ravno s stališča koordinacije in zavedanja o potrebnosti ureditve zelo zahteven projekt, ki bo pri vseh vpletenih straneh pomenil pomembno spremembo v pristopih in miselnosti. Država se bo morala zavedati potrebe po racionalnosti opredeljevanja kritičnosti posamezne infrastrukture in bo morala poleg normativne ureditve ugotoviti tudi določene finančne predpogoje za dokončno realizacijo minimalnih standardov varovanja te infrastrukture. Na drugi strani pa bo moral zasebni sektor omenjene procese dojeti, kot nujno potrebne za svoj obstoj v zahtevnem konkurenčnem okolju in bo omenjene procese varovanja KI sprejel kot korak k odličnosti, povečanju konkurenčnosti in sposobnosti preživetja v zahtevnem globalnem finančnem okolju.

V širši družbenih skupnostih bo treba spremeniti zavedanje o pomembnosti ustreznega procesa analiziranja tveganj za nemoteno delovanje KI.

V tej študiji poskušamo poiskati ustrezne odgovore na del zgoraj zastavljenih vprašanj. Kombinacija različnih pristopov, modelov, metodologij, konceptov in analiz različnih primerov, precej, če ne že popolnoma, pa v veliki večini podaja ustrezno podlago za ocenjevanje tveganj za delovanje KI Republike Slovenije. Seveda pa se avtorji zavedamo, da to ne pomeni končnega stanja, in da področje zahteva nadaljnjo znanstveno in strokovno obdelavo. To pomeni tudi, da pozdravljamo določeno uporabo sistemskih orodij na področju ocenjevanja tveganj, ki bodo zagotavljala upoštevanje predlaganega modela. Eden od takih primerov je orodje »Silver Bullet Risk«, ki predstavlja slovenski proizvod, in s katerim se sistematično identificirajo in upravljajo tveganja na vseh področjih, ki ogrožajo delovanje KI. Produkt vsebuje celovit vpogled v vire ogrožanja, ima več različnih modulov za odgovorne osebe organizacije, ki želijo za zmanjšanje tveganj, dosegati skladnost in preventivno ukrepanje v ustreznem času.

Ugotovitve oziroma neka nova spoznanja so navadno končni produkt raziskovanja. Kako realne in uporabne so te ugotovitve, pa je odvisno predvsem od različnih, zapletenih in med seboj bolj ali manj tesno povezanih elementov, dejavnikov in dogodkov, s katerimi pridemo v stik pri raziskovanju.

Vpliv zaposlenega na delovanje KI v sodobni državi je eden izmed najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanjo stalno nevarnost, ki je ne smemo podcenjevati. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile tehnološke in fizične sestavine KI varnejše, po drugi strani pa, kako obravnavati zaposlenega pri upravljanju teh kompleksnih sistemov, saj ta postaja vse pomembnejši referent za njeno zanesljivo delovanje. Če v ta okvir dodamo še nevarnosti, ki jih prinašajo procesi radikalizacije, potem lahko ugotovimo, da bo tem ukrepom v prihodnje potrebno nameniti večjo pozornost.

Sodobne grožnje varnosti, s strani različnih virov ogrožanja, so kompleksne, zato se upravičeno zastavljajo vprašanja, kaj sploh lahko naredi sodobna država in posamezni upravljavci KI, da se s svojim varnostnim sistemom hitro in učinkovito odzivajo na navedene grožnje. V vsakem primeru je učinkovit in neprekinjen sistem analiziranja tveganj za delovanje KI eden izmed ključnih temeljev zagotavljanja ustrezne zaščite in neprekinjenosti delovanja.

Ob temeljiti analizi različnih metodoloških pristopov in uporabljenih metodologij za analiziranje tveganj smo se odločili za smiselno uporabo metodologije MOSAR, ki je temeljito razdelana in v določenih izvedbenih korakih dopolnjena z metodologijo FMEA. Splošna ugotovitev temeljite analize že na prvi pogled kaže, da je večina podsektorjev KI povezana s tehnološkim procesom. Ta ugotovitev je bila, poleg ostalih, tudi ena izmed pomembnejših za sprejem metodologije analiziranja tveganj MOSAR, ki je predvsem uporabljena v tehnoloških sistemih. Omenjena študija daje širše podlage za izvedbo enovitega ocenjevanja tveganj v KI Republike Slovenije, kot najmanjšega skupnega imenovalca (oz. minimalnih standardov). Organizacije lahko, zaradi specifike, glede na sektor delovanja KI, v nadgraditvi teh minimalnih standardov uporabljajo še druge metode ali pristope ocenjevanja tveganj.

Pri uveljavljanju skupnega pristopa na področju ocenjevanja tveganj je treba zagotoviti naslednje predpogoje:

- strokovnjaki, ki se bodo v okviru sektorjev KI in upravljavcev KI ukvarjali s procesom ocenjevanja tveganj, morajo imeti določena predznanja s področja analiziranja tveganj. To pomeni, da bo potrebno za te strokovnjake izvesti različne oblike delavnic in usposabljanj, kjer se bodo v podrobnosti usposobili z metodološkim aparatom in procesi analiziranja tveganj po predvidenem metodološkem pristopu,
- proces bo potrebno v organizacijah izvajati kot kontinuirano aktivnost, ki bo del celotnega procesa zagotavljanja neprekinjenosti delovanja KI v Republiki Sloveniji,

- določene procese v okviru analize tveganj, kot so penetracijski testi in preverjanje informacijskih sistemov bo nujno izvajati v dokaj pogostih intervalih, kot kontinuirano nalogo,
- omenjene rešitve analiziranja tveganj bo potrebno podrobneje opredeliti in izpeljati v vsakem podsektorju KI. Določene specifike v teh podsektorjih nujno potrebujejo podrobno opredelitev posameznih korakov predlaganega metodološkega procesa ocenjevanja tveganj v KI. Zaradi navedenega bo verjetno potrebno izvesti določene sektorske študije ali projektno uveljavitev predlaganega pristopa, ki bo strokovno podprta z ustreznimi ekspertnimi institucijami.

Za konec velja poudariti, da je treba zaščito KI in procese ocenjevanja tveganj za delovanje le te umestiti v celovit proces zagotavljanja neprekinjenosti delovanja ključnih nacionalnih sistemov in učinkovito krizno upravljanje v Republiki Sloveniji.

Raznovrstni varnostni problemi ostajajo in jih moramo v nenehnem spremljanju aktivno analizirati. Vse to pred strokovnjake s področja varnosti postavlja dileme, kako biti v takih razmerah, pri vodenju razvejanih organizacij, učinkovito orodje v rokah strateškega managementa. Ravno pri strateškem managementu se varnostno zavedanje o pomenu varnosti nasploh počasi dviguje in prihaja v ospredje. Vendar se vse prevečkrat dogaja, da strokovno znanje in sposobnost varnostnega managementa v organizacijah ni na ustreznem nivoju, da bi izkoristil ta »zvezdniški trenutek« in se v določenih situacijah izkazal kot učinkovit mehanizem za ustrezno obvladovanje tveganj. Ta lažna zazibanost in samozadovoljnost je v svetu takih dinamičnih sprememb, kakršne se vsakodnevno dogajajo, praktično obsojena na takojšen neuspeh. Zaradi navedenega je potrebno, bolj kot kadarkoli do zdaj, vlagati v stalno izobraževanje in dograjevanje svojih znanj ter veščin. Ravno področje ocenjevanja tveganj bo v prihodnosti eno od tistih področij, ki bo podvrženo potrebi po neprekinjenem izvajanju usposabljanja ustreznih strokovnjakov, ki bodo v organizacijah izvajali te procese.

Literatura in viri

1. Acevedo, M. in Krueger, J. I., (2004). Two egocentric sources of the decision to vote: The voter's illusion and the belief in personal relevance. Political Psychology, 25 (1), 115– 134.
2. Ackoff, R. L. (1981). Creating the corporate future: Plann or be planned for. New York: John Wiley.
3. Adizes, I. (1996). Obvladovanje sprememb. Ljubljana: Gospodarski vestnik.
4. Alexander, C. (2003). Operational risk: regulation, analysis and management. Harlow: Pearson Education.
5. Allen, G., Derr, R.: Threat Assessment and Risk Analysis: An Applied Approach, Kindle Edition, 2015.
6. Alpar, P. (2007). Informationsmanagement: IT-Sicherheit. Marburg. Philip's Universität Marburg.
7. Andersen, J. T. (2010). Strategic Riak Management Practice. New York. Cambridge University Press.
8. Anonymous. 1997. Maximum security: A Hacker´s Guide to Protecting Your Internet Site and Network. Indianapolis, Indiana: Sams. Net Publishing.
9. Anthony, S. D., Govindarajan, V. (2010). Reverse Innovation: Create Far from Home, Win Everywhere. Harvard Business Review Press.
10. Aristotel. 1968. Nikomahova etika. Ljubljana: Cankarjeva založba.
11. ASIS International (2018). Risk,Threat, and Vulnerability Assessment. American Society for Industrial Security. Virginia, Alexandria. USA.
12. Atlas, R.I. (2008). 21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention. Florida. CRS Press Taylor&Francis Group.
13. Barbieri Masini, E., Medina Vasquez, J. (2000). Scenarios as seen from a human and social perspective. Technological Forecasting and Social Change, 65, 49–66.
14. Barlow, Lyde and Gilbert. Scott, A. (ed). (2000). Risk management for accountants. London: ABG Professional Information.
15. Bartol, R. C. (1995). Criminal Behavior: A Psychosocial Approach. New Jersey: A Simon & Schuster Company, Englewood Cliffs.
16. Barton, L. (2007). Crisis Leadership Now: A Real-World to Preparing for Threats, Disaster, Sabotage, and Scandal. McGraw-Hill.
17. Basel Committee on Banking Supervision (BIS), (2003). Sound Practices for the

Management and Supervision of Operational Risk.
18. Basel Committee on Banking Supervision. (2006). Core Principles Methodology. https://www.bis.org/publ/bcbs130.pdf. 8.5.2018.
19. Basel III: A global regulatory framework for more resilient banks and banking systems. Pridobljeno na http://www. bis.org/publ/bcbs128.pdf
20. Beck, U. (1993). Risk Society. London: Sage.
21. Beck, U. (2003). Kaj je globalizacija? Zmote globalizma – odgovori na globalizacijo (prevod dela: Was ist Globalisierung? Irrtumer des Globalismus – Antworten auf Globalisierung). Krtina. Krt. Knjižna zbirka Krt.
22. Berk, A., Peterlin, J., Ribarič, P. (2005). Obvladovanje tveganja – Skrivnosti celovitega pristopa. Ljubljana, GV Založba.
23. Beršnak Vuga J., Ferlin, A. (2016). Krizno upravljanje in vodenje v Republiki Sloveniji: predlog strukture KUV pri Vladi RS. V: Vuga Beršnak, Janja (ur.): Upravljanje kompleksnih kriz v Republiki Sloveniji, 9–32 .Ljubljana: Ministrstvo za obrambo.
24. Beršnak Vuga, J., Ferlin A., (2018). Priprave in odziv na kompleksno krizo. Ljubljana: Ministrstvo za obrambo.
25. Beršnak Vuga, J., Ferlin, A., Bizjak, M., Žnidaršič, F., Humar, D., Šestan, S., Purkart, M., Utroša, I., Čargo, A., Prezelj, I. (2016). Zaključno poročilo projekta P7: Sistem kriznega upravljanja in vodenja v Republiki Sloveniji. Ljubljana: Ministrstvo za obrambo.
26. Bertoncelj, B. (2012). The individual and security. V: Čaleta, Denis (ur.). Corporate security in dynamic global environment : challenges and risks. Ljubljana: Institute for Corporative Security Studies, 2012, str. 129-150, graf. prikazi. [COBISS.SI-ID 4668366]
27. Bertoncelj, B. (2013). Vodstveni nadzor kot sestavni del korporativne varnosti. Korporativna varnost, ISSN 2232-6170, nov. 2013, št. 5, str. 8-10, ilustr. [COBISS.SI-ID 274911744].
28. Bertoncelj, B. (2017). Zanesljivost posameznika pri delovanju kritične infrastrukture sodobne države. Sodobni vojaški izzivi, letn. 19, št. 4, str. 111-131.
29. Biringer, B. E. Matalucci, R. V., O Connor (2007). Security Risk Assessment and Management: Professional Practice Guide for Protecting Buildings and Infrastructures. Wiley&Sons.
30. Boole, G. (2003) (1854). An Investigation of the Laws of Thought. Prometheus Books. ISBN 978-1-59102-089-9.
31. Borodzicz, E. (2005). Risk, Crisis and Security Management. New York. John Wiley&Sons.

32. Broder, J. F. (1999). Risk Analysis and the Security Survey. Boston, Oxford. Butterworth Heinemann.
33. Broder, J. F. (2006). Risk Analysis and the Security Survey. Boston, Oxford. Butterworth-Heinemann.
34. Bruine de Bruin, W. B., Parker, A. M. in Fischhoff, B., 2007. Individual differences in adult decision–making competence. Journal of Personality and Social Psychology, 92 (5), 938–956.
35. Bučar, F. (1997). Ogrožanje nacionalne istovetnosti. Nova revija : mesečnik za kulturo. ISSN 0351-9805. - Let. 16, št. 177/178 (1997), str. 1-7.
36. Buzan, B. 1993. The Idea of the State and National Security. V: Little, R., Smith. Perspectives on World Politics. London and New York.
37. Carlson, C. S.: Understanding the Fundamental Definitions and Concepts of FMEAs. John Wiley & Sons, Hoboken, New Jersey, 2012.
38. Chapman, R.J. (2011). Simple Tools and techniques for Enterprise Risk Management. John Wiley&Sons, Ltd.
39. COSO. Enterprise Risk Management Framework: Executive Summary. Draft, The Committee of Sponsoring Organization of the Treadway Commission, 103 strani, 2003.
40. Crandall, W. R., Parnell, J. A., Spillan, J. E. (2013). Crisia Management: Leading in the New Strategy Landscope. Los Angeles. Sage Publications, Inc.
41. Čaleta, D. (2008). Vloga poslovnih procesov pri preprečevanju gospodarskega vohunstva (The role of business processes in countering economic espionage). V: Rajkovič Vladislav (ur.). 27. mednarodna znanstvena konferenca o razvoju organizacijskih znanosti. Znanje za trajnostni razvoj, Portorož, 19.-21. marec 2008. Zbornik. Kranj: Moderna organizacija, str. 448-454.
42. Čaleta, D. (2010). Varovanje kritične infrastrukture v razmerju do obvladovanja tveganj. V: Čaleta Denis (ur). Mednarodni posvet s področja varnostnega managementa, na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture. Ljubljana, 17. maj 2010. Zbornik. Ljubljana. Inštitut za korporativne varnostne študije, stran 52-62.
43. Čaleta, D. (2011). A comprehensive approach to the management of risks related to the protection of critical infrastructure: public-private partnership. V: Čaleta D. (Ed.), Shemella P. (Ed.) Counter terrorism cahalenges regarding the process of critical infrastructre protection«. Ljubljana, Monterey, ICS, CCMR, 2011, str. 15-26.
44. Čaleta, D. (2013). Ali je kriza lahko priložnost. Korporativna vanost, junij 2013, št. 4. Ljubljana. Inštitut za korporativne varnostne študije.
45. Čaleta, D. (2016). Kritična infrastruktura in tveganja stečajnih postopkov.

Korporativna vanost, oktober 2016, št. 11. Ljubljana. Inštitut za korporativne varnostne študije, str.20-23.

46. Čaleta, D. (2017). Nujno sprejetje paradigme o celovitosti pristopov obvladovanja tveganj. Korporativna vanost, junij 2017, št. 14. Ljubljana. Inštitut za korporativne varnostne študije, str.11-12.
47. Čaleta, D. (2018). Radicalization Risks in the Employees of Critical Infrastructure Organizations. V: ČALETA, Denis (editor), ROBINSON, Corinna (editor). Violent Extremism and Radicalisation Processes as Driving Factors to Terrorism Threats. Ljubljana: Ministry of Defence, Institute for Corporative Security Studies – ICS; Tampa: Joint Special Operations Univeristy, 2018, str. 45-64.
48. Davis, E. (2005). Operational risk: practical approaches to implementation. London: Risk Books.
49. Davis, E. (2006). The advanced measurement approach to operational risk. London: Risk Books.
50. DeLoach, J. (2000). Enterprise-wide risk management: strategies for linking risk and opportunity. Harlow: Financial Times/Prentice Hall.
51. Direktiva EU 2016/1148 evropskega parlamenta in Sveta z dne 6. Julija o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji /ULL 194, 19. 7. 2016, str. 1.
52. Direktiva Sveta Evropske unije o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite (ES), št. 114/2008.
53. Dobre, O. I., (2013). Employee motivation and organizational performance. Review of Applied Socio-Economic Research, 5(1), 53–60.
54. Doherty, A. N.: Integrated Risk Management. Techniques and Strategies for Reducing Risk, McGraw-Hill, 2000.
55. Dowd, K. (1998). Beyond value at risk: the new science of risk management. Chichester: Wiley. (Wiley Series in Frontiers in Finance).
56. ELES, Letno poročilo 2018.
57. Enterprise risk management: integrated framework. Executive summary. Committee of Sponsoring Organisations of the Treadway Commission (COSO), September 2004. Available from: http://digbig.com/4xeqm, [Accessed 16 July 2008].
58. Erjavec, A., Vršec, M. (2010). Varovanje informacij v skladu s serijo standardov ISO/IEC 27000 kot sestavni del integralnega varnostnega sistema gospodarske družbe. Zbornik posveta. Ljubljana. Fakulteta za varnostne vede, str. 82-93.
59. Estaji, H. (2014). “Flexible Spatial Configuration in Traditional Houses, The Case of Sabzevar”, pp. 26–35 - International Journal of Contemporary Architecture ”The

New ARCH“ Vol. 1, No. 1 (2014).
60. European Union Agency For Network And Information Security, ENISA, 2015
61. Evropska okoljska agencija, The european Environment Agency, EEA
62. Federal Emergency Management Agency (FEMA), Threat and Hazard Identification and Risk Assessment Guide Comprehensive Preparedness Guide (CPG) 201, Second Edition, THIRA, 2013, https://www.fema.gov/media-library data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf, 12.1.2017.
63. Fennelly, L. (2003). Effective Phisical Security. Butterworth-Heinemann.
64. Fink, S. (2013). Crisis Communikations: The Definitive Guide to Managing the Message. New York. McGraw Hill.
65. Flammini, F. (2012). Critical Infrastructure Security: Assessment, Prevention, Detection, Response. Boston. WIT Press.
66. George Mason University, Christie Jones (2017). Critical Infrastructure Higher Education, George Mason University, Arlington, USA.
67. Gheorghe, A. V. (2006). Critical Infrastructures at Risk: Securing the European Elektric Power System (Topics in Safety, Risk, reliability and Quality. Springer.
68. Gibson, J. L. (2003). Organizations: behavior, structure, processes. McGraw-Hill / Irwin, Boston.
69. Golding, D.: A Social and Programmatic History of Risk Research, iz Krimsky, S. in Golding, D. (ur.): Social Theories of Risk, Connecticut, Praeger, 1992.
70. Golob, R.: Varnostni sistem – Ocena varnostnih tveganj in varnostni ukrepi, Ljubljana – samozaložba, 99 strani, 2013.
71. Governance model diagram, pridobljeno na http://www.effectivegovernance.com.au/wp-content/uploads/2012/10/Corporate-Governance-Practice-Framework.png
72. Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (2018). Critical Infrastructure Security and Resilience: Theories, Mthods, Tools, and Techologies (Advanced Sciences and Technologies for Security Applications).Springer International Publishing.
73. Grody, A.D. Operational risk management to the rescue. Securities Industry News, 26/05/2008, Volume 20, Issue 21, pp 4-10.
74. Haimes, Y. Y., Kaplan, S., and Lambert, J. H. (2002). Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, Risk Analysis, 22(2), pp. 383-397.
75. Hale, A. R.; Glendon, A. I.: Individual Behaviour in Control of Danger, Amsterdam, Elsevier, 1987.

76. Hanssen, J. Corporate culture and operational risk management. Bank Accounting and Finance, February/March 2005, Volume 18, Issue 2, pp 35-38.
77. Hearnden, K., Moore, A. (1999). The Handbook Business Security. A Practical Guide to Managing the Security Risk. London. Kogan Page.
78. Herman, M., L. and Frost, M., D. (2009). Wargaming for Leaders: Strategic Decision Making from the Battlefield to the Boardroom. The McGraw hill Companies. New York.
79. Hoffman, D. (2002). Managing operational risk: 20 firmwide best practice strategies. New York: Jonn Wiley and Sons. (Wiley Finance Series).
80. Hollnagel, E., 2010. The diminishing relevance of human–computer interaction. V Boy, G. (ur.), Handbook of Human–Machine Interaction. Farnham, UK: Ashgate.
81. Holmes, J., (1994). The Clinical Implications of Attachment Theory. British Journal of Psychotherapy.
82. Homeland Security (2018): Critical Infrastructure Training. Department of Homeland Security – Office of Infrastructure Protection. U.S.
83. Hope, A., Oliver, P. (2017). Risk, Education and Culture. Routledge.
84. IEC 31010:2009 Risk management : Risk assessment techniques https://www.iso.org/standard/51073.html, 4.5.2018.
85. Jerman, B. Delovne priprave in naprave II, Metode ocene tveganja. Univerza v Ljubljani - Fakulteta za kemijo in kemijsko tehnologijo, Katedra za tehniško varnost. http://lab.fs.unilj.si/lasok/index.html/gradivo_jerman_OTV/DPN_2_OCENA_TVEGANJA.pdf , 1.6.2018.
86. Jones, J. (2009). Case Studies on Risk Management Education.
87. Jullisson, E. A., Karlsson, N. in Garling, T., (2005). Weighing the past and the future in decision–making. European Journal of Cognitive Psychology, 17(4), 561–575.
88. Kahn, H., Wiener, A. J. (1969). The year 2000: A Framework for Speculation on the Next Thirty- three Years. London: Macmillan.
89. Kaiser, T. (2006). An introduction to operational risk: a practitioner guide. London: Risk Books.
90. Kaufman, R.B., Moiseichik. M. L. (2013). Integratet Risk Management for Leisure Services. Champaign, US Illinois. Human Kinetics.
91. Klein, G., 2009. Streetlights and Shadows: Searching for the Keys to Adaptive Decision Making. Cambridge, MA: MIT Press.
92. Kirn, A. (1995). Tveganje kot družbenovrednotna kategotija. Teorija in praksa, št. 3 / 4, str. 212-219. Ljubljana: Fakulteta za družbene vede.

93. Kompare, A., Stražišar, M., Dogša, I., Vec, T., Curk, J. (2006). Psihologija: Spoznanja in dileme. Ljubljana: DZS.
94. Kovačič, A., Vukšič, V., (2005). Management poslovnih procesov : prenova in informatizacija poslovanja s praktičnimi primeri, Ljubljana: GV Založba.
95. Krech, D./Crutchfield, R. S./Ballachey, E. L. (1962), Individual in society, Tokyo etc. 1962, str. 77.
96. Krimsky, S., Golding, D. (ur.). 1992. Social Theories of Risk. Connecticut, Praeger: Wesport.
97. Lam, J. (2014). Enterprise Risk Management: From Incentives to Controls. John Wiley&Sons, Ltd.
98. Landoll, D. J.: The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Second Edition), 2016.
99. Lee, E. (2008). Homeland Security and Private Sector Business: Corporations Role in Critical Infrastructure Protection. Auerbach Publications.
100. Lewis, T.G. (2006). Critical Ifrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience.
101. Lindgren, M., Bandhold, H. (2003). Scenario planning; The link between future and strategy. New York: Palgrave Macmillan.
102. Lindseth, S. Operational risk management. DM Review, February 2005, Volume 15, Issue 2, pp 30-33.
103. Loader, D. (2006). Operations risk: managing a key component of operational risk. Oxford: Elsevier. (Elsevier Finance Series)
104. Lobnikar, B., Sotlar, A. (2006). Celovito upravljanje z varnostnimi tveganji kot dejavnik dolgoročne uspešnosti podjetja. V: Dvoršek, A., Selinšek, L. (ur.), Kriminalni napadi na premoženje gospodarskih subjektov (varnostni, pravni in zavarovalni vidiki). Maribor, Univerza v Mariboru, Pravna fakulteta in Fakulteta za policijsko-varnostne vede.
105. Luiijf, H.A.M., Burger H.H., and Klaver, M.H.A. (2008), Critical (Information) Infrastructure Protection in the Netherlands, working paper, available at http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.
106. Malešič, Marjan (Ed.) (2004). Krizno upravljanje in vodenje v Sloveniji – Izzivi in priložnosti. Ljubljana: Fakulteta za družbene vede.
107. Marinčič, A. (2017). Analiza neprekinjenega poslovanja sistema zaščite kritične infrastrukture v Republiki Sloveniji. Magistrsko delo. Ljubljana. Fakulteta za podjetništvo.
108. Maslow, A. H. (1943). A Theory of Human Motivation, Originally Published in *Psychological Review*, 50, 370-396.

109. McDermott R.E., Mikulak R. J., Beauregard M. R.: The basics of FMEA, Productivity Press, New York, USA. 2009
110. McDermott, R. E., Mikulak J. R. in Beauregard, M. R., 2009. The basis of FMEA. 2nd Edition, CRC Press, Taylor & Francis Group, LLC, New York.
111. Metodologija Universal Business Risk Model mednarodnega svetovalnega podjetja Arthur Andersen
112. Mitar, M. (1993). Sistemski pristop k ocenjevanju varnostnih razmer v sodobni družbi. Ljubljana: FDV.
113. Mitar, M. Pregled teorij o tveganju v družbenih vedah. Ljubljana: VŠNZ, Zbornik strokovno-znanstvenih razprav, 190–203, 1995.
114. Murray, A. (2007). Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science).New York. Springer.
115. Musek, J. (1993). Znanstvena podoba osebnosti. Ljubljana: Educy.
116. Nacionalni program varstva okolja 2030 - NPVO 30 (predlog Vlade RS, februar 2018)
117. National Science Foundation. 2017. Enterprise Risk Management (ERM). https://www.nsf.gov/nsb/meetings/2017/0221/presentations/20170221-AF-Open-NSF-ERM-Approach.pdf. 5.5.2018.
118. NIPP, 2013. Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/, 12.1.2017.
119. Norman, T. L.: Risk Analysis and Security Countermeasure Selection (Second edison), CRC Press, New York, 2016.
120. Northouse, P. G. (2010). Leadership: theory and practice. Los Angeles: Sage Publications.
121. ORM: ESCB / Eurosystem Operational Risk Management, 2008 (ni javno objavljeno).
122. P.-X. Thivel et al. Method Organised for a Systematic Analysis of Risks ali The Organized and Systemically Method of Risk Analysisi) / Journal of Hazardous Materials 151 (2008) 221–231)
123. PMBOK. Learn more about **A** Guide to the Project Management Body of Knowledge (PMBOK Guide) – Sixth Edition. http://www.cs.bilkent.edu.tr/~cagatay/cs413/PMBOK.pdf. 22.5.2018.
124. Polič, M. in drugi. 1995. Psihološki vidiki nesreč. Ljubljana: Uprava za zaščito in reševanje, Ministrstvo za obrambo RS.
125. Polič, M. in drugi. 1995. Zaznava ogroženosti zaradi nesreč. Ljubljana: Ujma.
126. Predlog programa usposabljanja upravljavcev kritične infrastrukture, Ministrstvo za obrambo, 2018

127. Prezelj, I., (2010). Kritična infrastruktura in sodobna varnost. V: Prezelj, I. (ur.): Kritična infrastruktura v Sloveniji. Ljubljana: FDV.
128. Prezelj, Iztok et.al. (2008). Definicija in zaščita kritične infrastrukture v RS. Končno raziskovalno poročilo. Obramboslovni raziskovalni center, Univerza v Ljubljani, Fakulteta za družbene vede.
129. Pritchard. C. L.: Risk Management: Concepts and Guidance (Fifth Edition), CRC Press, Taylor@Francis Group, 2015.
130. Purpura P. P.: The security handbook. Butterworth-Heinemann. Amsterdam, Boston: 2003.
131. Purpura, P. P. (1991). Modern Security and Loss Prevention Management. London: Butterworth Publishers.
132. Rael, R. (2017). Strategy and Risk Management: An Integrated Practical Approach. New York. Wiley&Sons.
133. Renn, O. (1992). Concepts of Risk: A Classification. Iz Krimsky, S.; Golding, D. (ur.): Social Theories of Risk. Connecticut: Praeger, Westport, 53–79.
134. Renn, O. (1992). The Social Amplification of Risk: Theoretical Foundations and Empirical Applications. The Journal of Social Issues, SPSSI International United Nations.
135. Renn, O. (2008) Risk Governance: Combining Facts and Values in Risk Management. Springer Science+Business Media B.V.
136. Resolucija o strategiji nacionalne varnosti Republike Slovenije - ReSNV-1 (Ur. l. RS, št. 27/2010)
137. Resolucija o energetskem konceptu Slovenije (predlog Vlade RS, marec 2018)
138. Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v letih od 2016 do 2020 - RePVND16-22 (Ur. l. RS, št. 75/2016)
139. Resolucija o nacionalnem planu zdravstvenega varstva 2016 – 2025 - Skupaj za družbo zdravja - ReNPZV16-25 (Ur. l. RS, št. 25/2016)
140. Resolucija o nacionalnem programu razvoja prometa v Republiki Sloveniji za obdobje do leta 2030 - ReNPRP30 (Ur. l. RS, št. 75/2016)
141. Risk and Insurance Management Society (RIMS): Risk manager core competency model https://www.rims.org/education/Documents/RMCCM.pdf. 21.5.2018.
142. Roland, H. E., Moriarty, B. (1990). System Safety Engineering and Management. New York: John Wiley & Sons.
143. Rosenthal, U. in sodelavci (1989). The World of Crises and Crisis Management. V Coping with Crises: The Management of Disasters, Riots and Terrorism. Spriengfield: Charels C. Thomas.

144. Saleh, Y. D. (2016). Crisis Management. The Art ofSuccess and Failure 30 case Studis in Business and Politics.Minneapolis. Mill City Press, Inc.
145. Santos, R. J. (2005). IIOM (Inoperability Input-Output Model. Wiley InterScience, (www.interscience.wiley.com).
146. Scandizzo, S. (2007). The operational risk manager's guide: how to understand methodologies, policies and procedures. London: Risk Books.
147. Schwartz P. (1991). The art of the long view. New York: Doubleday.
148. Self-Assessment of Compliance with the Basel Core Principles for Effective Banking Supervision by the U.S. Federal Banking Agencies. 2009. https://www.treasury.gov/resource-center/international/standards-codes/Documents/Banking%20Self-Assessment%207-31-09.pdf. 8.5.2018.
149. Shaw, G.R., Oikava, Y. (2014). Education for Sustainable Development and DisasterRisk Reduction. New York, London. Springer.
150. Shearer, A. W. (2005). Approaching scenario based studies: Three perceptions about the future and considerations for landscape planning. Environment and Planning B: Planning and Design, 32(1), 67–87.
151. Sklep Vlade RS št. 80200-2/2013/3, z dne 9. januarja 2014.
152. Sklep Vlade RS, 2015. Osnovne in sektorske kriterije kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji.
153. Smallman, C. (1996). Risk and organizational behaviour: a research model, Disaster Prevention and Management: An International Journal, Vol. 5 Issue: 2, pp.12-26.
154. Smart Grid Threat Landscape and Good Practice Guide, 2013, https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide, accessed 15 August 2017, p. 13.
155. Standard SIST EN ISO 12100:2011. Varnost strojev - Splošna načela načrtovanja - Ocena tveganja in zmanjšanje tveganja (ISO 12100:2010).
156. Standard SIST EN 60300-2:2004. Vodenje zagotovljivosti-2. del: program zagotovljivosti (IEC 60300-2:2004).
157. Standardi kakovosti ISO 9001:2015.
158. Okoljski standard SIST EN ISO 14001 in EMAS (Environmental Management and Audit Scheme).
159. Standard varnosti in zdravja pri delu OHSAS 18001 (Occupational Health and Safety Management System).
160. Standard družbene odgovornosti SA 8000 (Social Accountability 8000).

161. Standard varnostnih zahtev in varnostnih storitev DIN 77200 - standard za ponudnike/izvajalce -outsourcing varnostnih storitev (varnostna podjetja – Wach- und Sicherheitsunternemen-Wus).
162. Standard za varnostno nadzorne centre SIST BS 5979:2005 - Pravila ravnanja za sprejemne centre pri sprejemu signalov iz varnostnih sistemov – vključuje popravek št. 1 (Remote centres receiving signals from security systems – incorporating Corrigendum No. 1).
163. Standardi tehničnega varovanja IEC EN - standardi za alarmne sisteme EN 50136, SIST IEC 60839-5, SIST EN 50136-1-1, SIST IEC 60839-7-1 do SIST IEC 60839-7-7, SIST IEC 60839-7-11, SIST IEC 60839-7-12, SIST IEC 60839-7-20; standard pristopne kontrole EN 50133-1.
164. Standardi varovanja informacij ISO/IEC 27000:2018 Information Technology-Security Techniques-Information Security Management Systems-Overview and Vocabulary.
165. Standardi upravljanja tveganj ISO 31000:2018 Risk Management-Guidelines in ISO 31010:2018.
166. Stanovich, K. E. in West, R. F., (2008). On the relative independence of thinking biases and cognitive ability. Journal of Personality and Social Psychology, 94 (4), 672–695.
167. Strategija kibernetske varnosti v Republiki Sloveniji (sklep Vlade RS št. 38100-12/2015/5 z dne 25.02.2016).
168. Strategija kibernetske varnosti v Republiki Sloveniji, 2016.
169. Strategija razvoja Slovenije 2014 – 2020 (Ministrstvo za gospodarstvo, 2013)
170. Strategija razvoja Slovenije 2030 (sklep Vlade RS št. 30000-7/2017/7z dne 07.12.2017).
171. Strategija razvoja Slovenije 2030, 2017.
172. Sullivan, B. and Thompson, H. (2013). The Plateau Effect: Getting from Stuck to Success. Pridobljeno na http://plateaueffect.com/. 30.8.2018.
173. Taleb, N. Nicholas: The Black Swan: The Impact of the Highly Improbable, Random House, ZDA, 2007.
174. Thivel, P.-X., et al (2008). Method Organised for a Systematic Analysis of Risks. Journal of Hazardous Materials 151 str. 221–231.
175. Uredba o kriznem upravljanju in vodenju ter Nacionalnem centru za krizno upravljanje (2018), Uradni list RS, št.28/18 z dne 20.4.2018.
176. Varnost in kakovost živil HACCP (Hazard Analysis and Critical Control Point System).

177. Vasović, D., Janacković, G.L., Musicki, S. (2017). Integrative Education Model for Resources and Critical Infrastructure Protection, Based on Risk Assessment, Resources Valorization Threat Ranking. Conference paper. Springer Science+Business Media B.V. Dordrecht 2017.
178. Veeneklaas, F. R., Berg, van den, L. M. (1995). Scenario building: Art, craft or just a fashionable whim? V: Schoute, J. F., Finke, P. A., Veeneklaas, F. R., Wolfert, H. P. (ur.): Scenario studies for the rural environment; Selected and edited proceedings of the symposium Scenario studies for the rural environment, Wageningen, 12.-15. september 1994. Dordrecht: Kluwer academic publishers, 11–13.
179. Velsoft. (2013). Customizable Training Material: The Professional Supervisor, Courseware Version: 3.0. Pridobl*jeno na* http://www.velsoft.com. 30.8.2018.
180. Vršec, M. (1993). Varnost podjetja – tokrat drugače. Ljubljana.Viharnik.
181. Vršec, M. (1997): Management varovanja podjetja, Naše gospodarstvo 5-6/97, Ekonomsko – poslovna fakulteta, Maribor, 1997.
182. Vršec, M. (2002). Poslovno varnostni management - upravljanje in vodenje varnostnih podjetij ter služb varovanja v gospodarskih družbah. V: Pagon, Milan (ur.). Dnevi varstvoslovja : zbornik prispevkov. Ljubljana: Visoka policijsko-varnostna šola, 2002, 17 str.
183. Vršec, M. (2003). Ocena ogroženosti in varnostnih tveganj kot ena od ključnih podlag za varnostno politiko in varnostni sistem. V: Pagon, Milan (ur.). Dnevi varstvoslovja. Ljubljana: Visoka policijsko-varnostna šola, 2003, 21 str., graf. prikazi, tabele.
184. Vršec, M. (2003). Ocena ogroženosti in varnostnih tveganj kot ena od ključnih podlag za varnostno politiko in varnostni sistem. 4. Slovenski dnevi varstvoslovja, CD-21 strani. Bled. Visoka policijsko-varnostna šola.
185. Vršec, M. (2007). Obvladovanje tveganj in sprememb v poslovnih procesih. Študijsko gradivo za magistrski in doktorski študij. Ljubljana. Fakulteta za varnostne vede.
186. Vršec, M. (2008). Management varovanja kot poslovni mehanizem obvladovanja izrednih dogodkov in kriznih situacij. Mednarodna konferenca Znanost za trajnostni razvoj v Portorožu, 19.03 - 21.03.2008. Kranj. Fakulteta za organizacijske vede. 14 str.
187. Vršec, M. (2008). Redefiniranje ranljivosti in ogroženosti podjetij z izvirnim metodološkim pristopom. Mednarodna konferenca Znanost za trajnostni razvoj v Portorožu, 19. 03 – 21. 03. 2008. Kranj. Fakulteta za organizacijske vede.

188. Vršec, M. (2010). Satelitski navigacijski sistemi : prestrezanje in prisluškovanje elektronskim komunikacijam - varnostni ukrepi. Študijsko gradivo: univerzitetni in magistrski študij. Ljubljana. Fakulteta za varnostne vede. 48 str.
189. Vršec, M. (2011). Managing corporate security in the energy sector : energetics as a vital (critical) infrastructure for the functioning of a state, economy and civil society. V: Čaleta, Denis (ur.), Shemella, Paul (ur.). Counter terrorism challenges regarding the process of critical infrastructure protection. Ljubljana: Institute for Corporative Security Studies - ICS; Monterey: Center for Civil-Military Relations, 2011, str. 107-131.
190. Vršec, M. (2011). Pomen neprekinjenega poslovanja za poslovno učinkovitost organizacije, s poudarkom na kritični infrastrukturi. Dnevi korporativne varnosti, marec 2011. Ljubljana. Inštitut za korporativne varnostne študije. 25 str.
191. Vršec, M. (2012). Upravljanje poslovnih, varnostnih in drugih tveganj v multinacionalnih gospodarskih družbah. Dnevi korporativne varnosti, marec 2012. Ljubljana. Inštitut za korporativne varnostne študije. 16 str.
192. Vršec, M. (2014). Sinergija v upravljanju korporativne varnosti. Korporativna varnost, št. 7, 2014. Ljubljana. Inštitut za korporativne varnostne študije.
193. Vršec, M. (2014).Vodstveni nadzor v procesu upravljanja korporativne varnosti. Korporativna varnost, št. 8, 2014. Ljubljana. Inštitut za korporativne varnostne študije.
194. Vršec, M. (2016). Ranljivost, varnostne grožnje in varnostna tveganja si podajajo roke. Korporativna varnost, oktober 2016, št. 12. Ljubljana. Inštitut za korporartivne varnostne študije.
195. Vršec, M., Čaleta, D.: Korporativna varnost - varnostni sistemi podjetij. Inštitut za korporativne varnostne študije. Ljubljana: 2011.
196. Vršec, M., Vršec, Mir. (1995-2007). Projekti na področju nacionalne, industrijske, gospodarske in poslovne varnosti (raziskave, izdelava in implementacija varnostnih elaboratov) v naslednjih državnih institucijah in gospodarskih družbah posebnega pomena: Aerodrom Ljubljana (1995-1997), Državni zbor (1999), Zavarovalnica Triglav - Območna enota Ljubljana (2000), ELES Elektro Slovenija (2002-2003), LPP-Ljubljanski potniški promet (2003), Termoelektrarna Toplarna Ljubljana (2003-2005), PETROL (2005), ENERGETIKA Ljubljana (2006), Vodovod Kanalizacija VO-KA Ljubljana (2006), ACRONI (2006), Ministrstvo za pravosodje (2006), Diners Club International (2007). Ljubljana. Nova Panorama d.o.o./Panorama Security s.p.
197. Vršec, M., Vršec, Mir. (2006). Vzpostavljanje celovitega varovanja kot preventivnega dejavnika v gospodarskih družbah. V: Dvoršek, Anton (ur.),

Selinšek, Liljana (ur.). Kriminalni napadi na premoženje gospodarskih subjektov : (varnostni, pravni in zavarovalni vidiki). [Maribor: Pravna fakulteta; Ljubljana: Fakulteta za policijsko-varnostne vede], 2006, str. [83]-101.

198. Vršec, M., Vršec, Mir. (2007) Obvladovanje tveganj in sprememb v poslovnih procesih. Študijsko gradivo. Magistrski študij. Ljubljana. Fakulteta za varnostne vede. str.51.
199. Vršec, M., Vršec, Mir. (2007). Industrijska, gospodarska i poslovna sigurnost. Konferencija hrvatskih menadžera sigurnosti na temu: Uloga i položaj menadžera sigurnosti u hrvatskom gospodarstvu, 17.-18. 2007, Biograd na Moru. Zbornik radova, str. 117-139, ur. Alen Javorović. Zagreb 2007. SIGURNOST EDUCA i Udruga hrvatskih menadžera sigurnosti.
200. Vršec, M., Vršec, Mir. (2009). Obvladovanje hudih motenj poslovanja z načrtom neprekinjenega poslovanja in s kriznim načrtom = Controlling serious disturbances in business operations with a plan for uniterrupted [!] operations and a contingency plan. V: Rjkovič, Vladislav in drugi (ur.). Nove tehnologije, novi izzivi : zbornik 28. mednarodne konference o razvoju organizacijskih znanosti : proceedings of the 28th International Conference on Organizational Science Development. Kranj: Moderna organizacija, 2009, str. 1575-1587.
201. Vršec, M., Vršec, Mir. (2009). Obvladovanje varnostnih groženj v gospodarskem sektorju. Študijsko gradivo. Magistrski študij. Ljubljana. Fakulteta za varnostne vede.
202. Vršec, M., Vršec, Mir. (2010). Obvladovanje tveganj v kritični infrastrukturi. Strokovni posvet na temo Zaščita kritične infrastrukture, 19. Oktober 2010. Ljubljana. Inštitut za korporativner varnostne študije.
203. Vršec, M., Vršec, Mir. (2010). Obvladovanje varnostih tveganj in izboljšanje varnostnih mehanizmov v kritični infrastrukturi. Gradivo za temeljno raziskavao. Ljubljana. Inštitut za korporativne varnostne študije.
204. Vršec, M., Vršec, Mir. (2014). Strateško načrtovanje procesov korporativne varnosti. Korporativna varnost, marec 2014, št. 6. Ljubljana, Inštitut za korporativne varnostne študije.
205. Vršec, M., Vršec, Mir. (2015). Kaj sploh je korporativna varnost. Korporativna varnost, št. 9, 2015. Ljubljana. Inštitut za korporativne varnostne študije.
206. Vršec, M., Vršec, Mir. (2015). Revizija varnostnih sistemov v kritični infrastrukturi. Korporativna varnost, št. 14, 2017. Ljubljana. Inštitut za korporativne varnostne študije.

207. Vršec, M., Vršec, Mir. (2016). Ranljivost, varnostne grožnje in tveganja si podajajo roke. Korporativna varnost, št.12, 2016.Ljubljana. Inštitut za korporativne varnostne študije.
208. Vršec, Mir. (2006). Uvajanje integralne varnosti v poslovni proces podjetja. Magistrsko delo. Portorož. Visoka šola za podjetništvo.
209. Vršec, Mir. (2008). Kritična infrastruktura kot predmet zaščite in varovanja v slovenskih gospodarskih družbah. Dnevi varstvoslovja, Bled 2008. Zbornik povzetkov, str. 61. Ljubljana. Fakulteta za varnostne vede.
210. Vršec, Mir. (2008). Zaščita kritične infrastrukture v slovenskih organizacijah po evropskih merilih. Mednarodna konferenca Znanje za trajnostni razvoj v Portorožu, 19. 03. - 21. 03. 2008. Kranj. Fakulteta za organizacijske vede.
211. Vršec, Mir. (2014). Zaščita in reševanje ter zagotavljanje neprekinjenega poslovanja. Se splača vlagati v preventivo ali hazardirati in prekomerno tvegati. Korporativna varnost, št. 2, 2014. Ljubljana. Inštitut za korporativne varnostne študije.
212. Vršec, Mir., Brumnik, R., Vršec, M. (2009). Approach's to estimate vulnerability and threats of information critical infrastructure. Sist. obrobki ìnf., 2009, 79, 7, str. 7-11.
213. Walker, C., Broderick, J., Civil Contingencies Act 2004, The: Risk, Resilience and the Law in the United Kingdom. Oxford University Press, 2006.
214. White, J. M.: Security Risk Assessment, Elsevier, Oxford UK, 2014.
215. World Economic Forum (2016). The Global Risks Report 2016, 11th Edition. http://wef.ch/risks2016. 15.5.2018.
216. Zahav, A. E., Hazzan, O. (2017). Risk Management of Education System: The Case of STEM Education in Israel. Springer. Switzerland.
217. Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17).
218. Zakon o informacijski varnosti (Uradni list RS, št. 30/18).
219. Zakon o varstvu pred naravnimi in drugimi nesrečami Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 97/10 in 21/18 – ZNOrg).
220. Zakon o varstvu pred požarom (Uradni list RS, št. 3/07 – uradno prečiščeno besedilo, 9/11, 83/12 in 61/17 – GZ).
221. Zakon o varnosti in zdravju pri delu (Uradni list RS, št. 43/11).

PRILOGE

PRILOGA 1 - OPREDELITEV OSNOVNIH POJMOV

V tekstu uporabljeni pojmi imajo naslednji pomen:

- **analiza ogroženosti:** je nenehen in sistematičen proces proučevanja vseh podatkov in informacij, ki so povezana s sposobnostmi, aktivnostmi in namerami subjektov, ki potencialno ogrožajo KI in določanje ustreznih ukrepov, povezanih z zaznanimi nevarnostmi;
- **analiza tveganja:** (i) celovit koncept opredeljevanja in analiziranja ogrožanj dobrin upravljavcaKI (izvor - grožnja - izpostavljenost dobrin) in je povezan z odločitvami na področju obvladovanja tveganja; (ii) proces, ki služi izdelavi ocene pričakovane izgube kot posledice različnih ogrožanj poslovnega procesa KI; (iii) proces identifikacije, analiziranja in vrednotenja določenega tveganja;
- **človeški viri in ravnanje z njimi:** (i) pomeni znanja, sposobnosti, usposobljenosti, vrednote, motiviranosti, pripadnosti, stališča, ipd., ki jih imajo zaposleni v KI; (ii) pomeni proces analiziranja, urejanja in upravljanja človeških virov v KI za zadovoljevanje njenih strateških poslovnih ciljev;
- **dobrina:** je enota, ki je potrebna za nemoteno delovanje KI in jo pri analizi tveganja samostojno obravnavamo. Dobrine so lahko materializirane (materialne dobrine, zaposleni, poslovna zgradba, oprema, računalniški center, strojna in komunikacijska računalniška oprema ipd.) ali nematerializirane (storitve, podatki in informacije, programska računalniška oprema ipd.) stvari, ki so pomembne za delovanje KI;
- **dogovorjeni tolerančni okvir**: predstavlja tveganje, ki ga je KI pripravljena sprejeti, tolerirati oziroma biti do tveganja izpostavljena;
- **fizična varnost:** sklop pravnih, organizacijskih in kadrovskih ukrepov ter postopkov, ki onemogočajo nekontroliran fizični pristop, protipravno pridobitev premoženja, poškodbo, onesposobitev ali uničenje dobrin;
- **frekvenca**: kolikokrat se določen tip tveganega dogodka pojavi v določenem času;
- **grožnja:** je potencialno ogrožanje dobrin;
- **havarija**: je delno drugi izraz za katastrofo, vendar je razlika v tem, da pri havariji gre za popolno uničenje denimo tovornjaka, ki je popolnoma zgorel z bogato robo, ladja,

ki je potonila, letalo, ki je strmoglavilo, proizvodni obrat, ki je popolnoma pogorel, vlak, ki je iztiril in je v celoti uničen idr.;

- **hazardiranje:** je najslabša oblika obvladovanja tveganj, kajti pri tem lahko veliko dobiš ali vse izgubiš - sreča tu ne igra nobene vloge;
- **hevristika:** (i) nauk o metodah raziskovanja; (ii) hevristika dostopnosti nastopi, kadar za neki dogodek menimo, da je verjeten ali pogost, če si z lahkoto zamislimo njegove primere;
- **incident**: situacija, ki je povzročila oziroma lahko povzroči izgubo, nesrečo ali katastrofo;
- **izpostavljenost dobrin:** je rezultat procesa, ki ga sproži uresničeno ogrožanje poslovnega procesa KI;
- **izpostavljenost**: to je stanje, ko je posameznik, skupina, del organizacije ali kar vsa organizacija izpostavljena določeni nevarnosti, določenemu tveganju, določenim neizbežnim dogodkom ali določenim napadom – v mnogih primerih je izpostavljenost neizbežna , kajti že sama dejavnost, že sama naprava ali že sama snov povzroča nevarnost – npr. pri delu na višini si izpostavljen padcu, pri delu z nevarnimi snovmi si izpostavljen okužbi, eksploziji, napadu kriminalcev, itd.;
- **izredni dogodek**: najprimernejši izraz za razne dogodke in pojave kot denimo nesreča, napad, motnja, nenormalna situacija, napaka, ovira, blokada, ki nastajajo v naravnem okolju, v organizacijah in pri ljudeh, ki ima tudi zakonsko podlago (npr. v zakonu o kritični infrastrukturi) in v nekaterih standardih;
- **katastrofa:** je izredni dogodek v obliki nesreče, požara, eksplozije, razpada sistema, ki ima ogromne materialne, finančne, človeške, socialne in moralne posledice, ki lahko za daljši čas onemogočijo delovanje organizacije, ali jo celo uničijo;
- **kontrola:** dejavnosti, kot so preiskovanje ali ocenjevanje ene ali več karakteristik delovanja poslovnega procesa KI in primerjanje rezultatov s predpisanimi zahtevami, da se ugotovi, če je dosežena skladnost za vsako karakteristiko;
- **korporativna varnost:** je proces v integralnem varnostnem sistemu organizacije, ki jo sestavljajo vsa področja varnosti – fizična in tehnična varnost, zagotavljanje neprekinjenega poslovanja, varnost in zdravje pri delu, požarna varnost, varstvo okolja, varovanje informacij idr.; in, ki jo upravlja management korporativne varnosti;
- **kritične aktivnosti**: funkcije ali poslovni procesi, ki jih je potrebno izvajati za doseganje najpomembnejših in časovno pogojenih storitev in produktov KI;
- **krizni štab**; krizni štab, ki ga imenuje vodstvo gospodarske družbe je sestavljen iz kompetentnih odgovornih oseb, ki imajo izkušnje, ki so pogumni, ki so sposobni

odzivanja na krizna stanja, ki so stalno dosegljivi in ki imajo fizično in psihično kondicijo za časovne presežke delovanja (12 ali več ur na dan);

- **krizno vodenje**; v kritični infrastrukturi morajo nosilci in upravljavci sektorjev obvladovati tudi krizna stanja in krizne okoliščine ter konkretne krize, ki nastanejo zaradi neobvladovanja tveganj in zaradi nenadnih, nepričakovanih ali presenečenih izrednih dogodkov – za obvladovanje krize mora imeti gospodarska družba izdelan krizni načrt poslovanja na osnovni in/ali rezervni lokaciji, vzpostavljen krizni štab in pripravljen načrt kriznega komuniciranja – sestavni del kriznega vodenja je tudi preizkušanje scenarijev verjetnih kriznih stanj;
- **metoda:** je načrtno ravnanje, s katerim želimo doseči neki cilj in tehnika preučevanja pojavov. Temelji na zbiranju opazljivih, empiričnih in merljivih dokazov, podvrženih določenim merilom razmišljanja;
- **metodologija ocenjevanja tveganj:** je proces, ki poteka na podlagi metodologije, ki je sestavljena iz izbranih metod/modelov ocenjevanja tveganj, upoštevajoč zakonske zahteve o načinih ocenjevanja tveganj, nacionalne resolucije in strategije, standardov za ocenjevanja tveganj ter specifičnosti tveganj v sektorjih kritične infrastrukture;
- **model:** je pomanjšan posnetek realnosti, narejen v določenem razmerju, ki nam pove dejanske mere predmeta. Pri modelu izločimo lastnosti realnosti, ki nam v danem trenutku ne koristijo in se osredotočimo na lastnosti, ki so nam pomembne;
- **motivacija:** pomeni splet raznih silnic, ki vplivajo na vedenje zaposlenega v KI in ga vzdržujejo v določeni smeri;
- **motivatorji:** so razni dejavniki, ki vplivajo na zaposlenega v KI in povzročajo visoko stopnjo motiviranosti. Mednje sodijo: dosežki, odgovornost, razvoj, napredovanje, vrsta dela;
- **motnja**: pričakovan ali nepričakovan dogodek, ki povzroči nenačrtovan ali negativen odklon od pričakovanih storitev in produktov KI;
- **negotovost:** življenje, delo, poslovanje, potovanje, gibanje je tu pa tam negotovo, ker je premalo informacij, premalo znanja, premalo izkušenj, da bi natanko vedeli kaj vse nas čaka v bližnji in daljši prihodnosti;
- **nelagodje:** neprijetno, neugodno razpoloženje; duševno nelagodje;
- **neprekinjeno poslovanje** (delovanje): po zakonu o kritični infrastrukturi morajo upravljavci kritične infrastrukture zagotavljati neprekinjeno delovanje gospodarskih družb, ki upravljajo s kritično infrastrukturo – to pomeni delovanje 24 ur na dan vse

leto-četudi v poslovnih in drugih procesih prihaja do motenj, okvar, napak in drugih motečih dejavnikov;

- **nesreča**: je izredni dogodek, ki se pripeti v cestnem, železniškem, zračnem in vodnem prometu, v gorah, v jamah, v športu, v prostočasnih aktivnostih in povsod tam, kjer gre lahko kaj narobe;
- **nevarnost:** prisotnost naključne (nenamerne) ali namerne grožnje dobrinam;
- **nezgoda:** je izredni dogodek v delovnem procesu, kjer prihaja do delovnih nezgod zaradi napak delavca, okvar na delovni opremi in okvar v raznih procesih;
- **notranje kontrole**: aktivnosti, ki se izvajajo na vseh nivojih upravljanja in delovanja z namenom, da se upravljajo tveganja na učinkovit in uspešen način;
- **obvladovanje tveganj:** je pogosto uporabljen izraz v obravnavanju in razglabljanju o tveganjih in najbolj jasno pove, da smo na poti zmage nad tveganji, obsega pa ocenjevanje tveganj, vzpostavitev procesa upravljanja tveganj, načrtovanje ukrepov za premagovanje tveganj ter spremljanje in nadzor nad uspešnostjo premagovanja tveganj;
- **ocenjevanje ogroženosti:** analiziranje zbranih podatkov o ogroženosti narave, okolja, delovnih in poslovnih procesih, logistike, opreme in človeških virov imenujemo ocenjevanje ogroženosti po stopenjski lestvici – nizka ogroženost, srednja ogroženost, povečana ogroženost in visoka ogroženost;
- **ocenjevanje ranljivosti:** pregled lokacij šibkih točk na lokaciji organizacije, v zgradbah, prostorih in opremi, v delovnih, proizvodnih, poslovnih in logističnih procesih ter pregled slabosti pri človeških virih, poslovnih partnerjih in pogodbenih izvajalcih imenujemo ocena ranljivosti organizacije;
- **ocenjevanje tveganj:** je ena od ključnih faz upravljanja s tveganji, ki obsega prepoznavanje tveganj, analiziranje tveganj in vrednotenje tveganj;
- **operativno tveganje**: tveganje je tveganje nastanka izgube, vključno s pravnim tveganjem, zaradi naslednjih okoliščin: (i) neustreznosti ali nepravilnega izvajanja notranjih procesov; (ii) drugih nepravilnih ravnanj zaposlenih v KI; (iii) neustreznosti ali nepravilnega delovanja sistema KI; (iv) zaradi zunanjih dogodkov ali dejanj;
- **organizacijska kultura organizacije:** (i) je vzorec temeljnih domnev, ki jih je KI ugotovil pri urejanju problemov eksterne adaptacije in interne integracije ter se je pokazal kot dovolj dober vzorec; (ii) je vzorec temeljnih domnev in prepričanj, ki so skupne zaposlenim v KI in se po njih ravnajo;
- **politika upravljanja tveganj:** (i) načelne usmeritve in strateški cilji KI na področju upravljanja tveganj, ki jo določi najvišje vodstvo; (ii) je ključni dokument zagotavljanja

zanesljivosti in varnosti poslovanja KI ter opredeljuje obvladovanje tveganj v skladu s standardi poslovanja. Določa smernice za zaščito dobrin KI;

- **poslovni procesi**: postopki in aktivnosti, ki iz vhodnih elementov ustvarijo predvideni izdelek ali storitev. Poslovni proces sestavlja zaporedje opravil, ki jih je potrebno izvesti, da je rezultat končni izdelek ali storitev. Vsak proces ima svoj vhod in izhod, ki predstavljata začetek in konec poslovnega procesa. Uspešnost procesa se običajno meri s stroški, časom ali kvaliteto. Kot proces se šteje vsaka aktivnost, ki se izvaja, vendar so potrebne le tiste aktivnosti, ki povečujejo dodano vrednost končnega izdelka ali storitve (Kovačič, Vukšić, 2005, 29−30).
- **preprečevanje škod in izgub (Loss Prevention):** to je prizadevanje za preventivo, da preprečimo nastanek izrednih dogodkov, ali se jih omeji, s tem pa posledično zmanjšamo ali izničimo škode, stroške in izgube na premoženju, procesih in človeških virih;
- **preventivni ukrep:** ukrep za odstranitev vzroka potencialne neskladnosti, napake ali neželene situacije, da bi preprečili škodni dogodek;
- **prevzemanje tveganja**: dokumentirana odločitev vodstva KI o prevzemanju določenega tveganja;
- **proces upravljanja tveganj**: izhaja iz ocene ranljivosti in ogroženosti in iz SWOT analize poslovanja in delovanja ter iz rezultatov ocenjevanja tveganj, in se izvaja na vseh ravneh organiziranja in vodenja organizacije, pri čemer se ovrednotijo tudi stroški procesa in v okviru tega tudi vzpostavitev ustreznega zavarovalnega portfelja (zavarovanje visokih rizikov pri zavarovalnicah); vzpostavitev procesa omogoča trajno in kontinuirano upravljanje tveganj na vseh ravneh;
- **ranljivost:** vsako odstopanje dejanskega stanja od določene varnostne politike oziroma varnostnih rešitev;
- **raven tveganja**: obseg tveganja izražen v kombinaciji vpliva in verjetnosti;
- **scenarij:** je operativni načrt delovanja za potrebe obvladovanja izrednega dogodka, ki lahko pripelje oziroma povzroči krizno stanje – krizni štab in drugi deležniki obvladovanja preizkušajo scenarij z vajami, pri čemer ugotavljajo pripravljenost in usposobljenost človeških virov in opreme za premagovanje in razreševanje krizne situacije;
- **sistem:** je posebna organizirana celota, sestavljena iz dveh ali več sestavin (delov ali podsistemov) in odnosov med njimi ter je jasno opredeljena do zunanjega in/ali notranjega okolja. Sistem je sestavljen iz podsistemov in je sam del suprasistema;

- **sistemizacija tveganj**: sistematično urejen nabor vzrokov in posledic ter tveganj in njihovih vplivov na poslovanje KI;
- **škodni dogodek:** nepričakovan dogodek ali sosledje dogodkov v KI, v katerem se lahko pojavi škoda na dobrini zaradi naključne (nenamerne) ali namerne dejavnosti zaposlenega ali zunanjih posameznikov ali skupin;
- **tvegan dogodek**: dogodek, ki se lahko zgodi oziroma ga sprožita motnja ali incident;
- **tveganje:** (i) je merilo možnosti izpostavljenosti dobrin ogrožanjem, verjetnost, da bo prišlo do škodnega dogodka v določenem obdobju. Pri merjenju tveganja lahko ugotovimo le verjetnost, da do škodnega dogodka lahko pride, ne moremo pa napovedati noben konkretni dogodek. Je produkt verjetnosti (pogostosti) in škodnega učinka uresničitve ogrožanja dobrin ali stroškov, ki jih uresničitev ogrožanja povzroči. Tveganje je sprejemljivo, če ne pride do škodnega dogodka. Presojanje sprejemljivosti tveganja je stvar subjektivnih in družbenih vrednostnih sodb; (ii) je stanje, v katerem KI lahko definira problem, izračuna verjetnost pojavljanja določenih dogodkov, identificira alternativne rešitve in določi verjetnost, s katero posamezna rešitev daje želeni rezultat; (iii) negotovost, povezana s finančnimi izgubami, z odstopanji med dejanskimi in pričakovanimi rezultati ter verjetnostjo, da se je dogodek, ki povzroča izgubo, že zgodil ali pa se bo zgodil; (v) nekaj, kar se lahko zgodi in vpliva na doseganje ciljev poslovanja KI;
- **upravljanje poslovnih procesov:** predstavlja prizadevanja organizacije, da procesi, ki se odvijajo v organizaciji, pripomorejo k uresničitvi strateških ciljev poslovanja. Delimo jih v tri vrste procesov: temeljni procesi: gre za procese, ki so vezani na izdelke, storitve, ki jih organizacija ponuja, informacijski procesi: zagotavljanje kakovostnih informacij ob pravem času, na pravem mestu in na prav način, procesi upravljanja : zagotavljajo smotrno delovanje preostalih dveh;
- **upravljanje tveganj:** proces, ki kontinuirano in sistematično omogoča identifikacijo, obvladovanje, nadziranje in poročanje o tveganjih;
- **varnost:** (i) stanje, v katerem je tveganje glede škode omejeno na sprejemljivo raven; (ii) je situacija, ko je varnostni sistem KI pod nadzorom in se izredni dogodek še ni dogodil;
- **varnostna grožnja:** skoraj vsaka grožnja posameznika, skupine ali organizacije ima varnostni prizvok; zlasti pa direktna, anonimna, elektronska ali klasična grožnja s fizičnim, strelskim in/ali eksplozivnim napadom, pomeni takojšnje organiziranje učinkovite obrambe – če je taka grožnja uresničena, pa so potrebni učinkoviti ukrepi sanacije;

- **varnostni sistem:** načrtno urejena množica varnostnih sestavin (elementov) in povezav med njimi za normalno, zanesljivo in celovito poslovanje KI. Varnostni sistem opravlja, pri določenih pravnih, organizacijskih, kadrovskih in tehničnih pogojih, predvidene funkcije za preprečevanje škodnih dogodkov;
- **vedenje:** je reagiranje zaposlenega na dražljaj, dogodek. Vedenje se kaže v njegovem mišljenju (kognitivno področje), v njegovem početju (motorično področje) in v njegovem občutenju, hotenju in vrednotenju (afektivno področje);
- **verjetnost:** verjetnost, da se določen dogodek lahko zgodi;
- **vpliv tveganja**: ocenjena posledica določene motnje ali incidenta.
- **vrste tveganj:** za uspešno poslovanje je treba obvladovati vse vrste tveganj, ki so lahko: poslovna tveganja (finančna, tržna, razvojna, strateška, projektna ipd.), tveganja človeških virov, tehnično-tehnološka tveganja, logistična tveganja, pravna tveganja, varnostna tveganja (tveganja nesreč, korupcijska tveganja, tveganja gospodarskega kriminala ipd.).

PRILOGA 2 - Seznam slik in tabel

Slika 1: Analiza raziskovalenga vprašanja »Imate uveden sistem neprekinjenega poslovanja po standardu ISO 22301/2012/2014«
Slika 2: Soodvisnost kritične infrastrukture
Slika 3: Osrednji cilj in strateške usmeritve (Strategija razvoja Slovenije 2030, 2017)
Slika 4: Sistem zagotavljanja kibernetske varnosti (Strategija kibernetske varnosti v Republiki Sloveniji, 2016)
Slika 5: Ekosistemski model varstva okolja (Evropska okoljska agencija, The european Environment Agency, EEA)
Slika 6: Sistem vodenja kakovosti po standardih ISO 9001 in Demingovem modelu PDCA – PLANIRAJ-IZVEDI-PREVERI-UKREPAJ
Slika 7: Razmerje med načeli, okvirom in procesom obvladovanja tveganja (ISO 31000, 2011)
Slika 8: Splošni model za ocenjevanje tveganj (Vršec, 1993, 2010)
Slika 9: Okvir za ocenjevanje tveganj na področju KI (prirejeno po NIPP, 2013)
Slika 10: Maslowova piramida (hierarhija) potreb (Maslow, 1943)
Slika 11: Dinamična hierarhija potreb s hkratnim prekrivanjem različnih potreb (Krech in drugi, 1962)
Slika 12: Maslowova piramida potreb in Alderfersova ERG theorija (Estaji, 2014)
Slika 13: Metodološki koraki za ocenjevanje tveganja (interni vir ICS)
Slika 14: Faktorji tveganj (interni vir ICS)
Slika 15: Programski pristop povezanih načrtov (interni vir ICS)
Slika 16: Nivoji vzdržnosti tveganja (interni vir ICS)
Slika 17: Potrebna znanja in spretnosti za ocenjevanje tveganj (interni vir ICS)
Slika 18: Sodobna ureditev nadzora nad obvladovanjem tveganj (interni vir ICS)
Slika 19: Metamodel projektnega pristopa za ocenjevanje tveganj (interni vir ICS)
Slika 20: Znanje projektnega vodenja (interni vir ICS)
Slika 21: Model ocenjevanja tveganj, ki temelji na izrednih dogodkih in njihovih posledicah (Vršec, 2010)
Slika 22: Razvrstitev tveganj po vrstah tveganj (prirejeno po metodologiji *Universal Business Risk Model mednarodnega svetovalnega podjetja Arthur Andersen)*
Slika 23: Model obvladovanja tveganj na bazi notranje integritete in sinergij (Vršec, 2009)
Slika 24: Postopek ocene tveganja po enačbi $R= P_A * (1 – P_E) * C$ (Biringer, 2007)
Slika 25: Diagram za odločanje pri upravljanju varnostnih tveganj (Biringer, 2007)

Slika 26: Vrste operativnih tveganj (prirejeno po Basel II, 2006)
Slika 27: Vrste operativnih tveganj (interni vir ICS)
Slika 28: Sistem upravljanja tveganj z organizacijskega vidika (interni vir ICS)
Slika 29: Proces upravljanja tveganj (interni vir ICS)
Slika 30: Širši proces upravljanja tveganj (interni vir ICS)
Slika 31: Rezultati ocenjevanja tveganj (interni vir ICS)
Slika 32: Governance model diagram (http://www.effectivegovernance.com.au/wp-content/uploads/2012/10/Corporate-Governance-Practice-Framework.png)
Slika 33: Proces upravljanja tveganj po standardu ISO 31000
Slika 34: Metodologija MOSAR (SIST EN ISO 12100:2011)
Slika 35: Metodologija MOSAR (prirejeno po standardu SIST EN ISO 12100:2011)
Slika 36: Globalni viri nevarnosti (interni vir ICS)
Slika 37: Ponazoritev tveganj povezanih z delovanjem informacijske tehnologije v KI (ENISA)
Slika 38: Pregled in primerjava najbolj izpostavljenih groženj na področju kibernetske varnosti za leti 2015 and 2014
Slika 39: Možne napake zaposlenega (interni vir ICS)
Slika 40: Ogroženost KI (Marinčič, 2017)
Slika 41: Proces izdelave scenarijev možnih izrednih dogodkov (interni vir ICS)
Slika 42: Proces analize drevesa odpovedi (interni vir ICS)
Slika 43: Drevo dogodkov za primer požara (interni vir ICS)
Slika 44: Elementi sistema (prirejeno po SIST EN 60300-3-4:2008)
Slika 45: Koraki metodologije FMEA (prirejeno po standardu SIST EN 60300 - 3-4)
Slika 46: Logične povezave med FMEA elementi (SIST EN 60300 - 3-4)
Slika 47: Primer delovnega lista FMEA (prirejeno po standardu)
Slika 48: Struktura produkta /storitve (interni vir ICS)
Slika 49: Matrika tveganj FMEA (smiselno prirejeno po standardu SIST EN 60300 - 3-4)
Slika 50: Proces zbiranja podatkov potrebnih za oceno ogroženosti in identificiranje tveganj (Vršec, 2009)
Slika 51: Nosilci funkcij kriznega upravljanja in vodenja (Beršnak in Ferlin, 2016)
Slika 52: Struktura kriznega upravljanja in vodenja na ravni države v običajnih razmerah (Beršnak in drugi, 2016)
Slika 53: PDCA model za vpeljavo sistema neprekinjenega poslovanja
Slika 54: Odgovornost za neprekinjeno poslovanje (interni vir ICS)
Slika 55: Metodološko vsebinski pristop za vzpostavitev sistema upravljanja in obvladovanja tveganj za delovanje KI (izvirni pristop)
Slika 56: Položaj (mesto, lokacija) in umeščenost RTP v elektroenergetskem sistemu Slovenije (ELES, 2018)

Slika 57: Pomen in vloga RTP v elektroenergetskem sistemu, od proizvodnje in prenosa električne energije, preko transformacije električne energije, vse do distribucije odjemalcem oziroma porabnikom (ELES, 2018)

Tabela 1: Primernost metod za ocenjevanje tveganj za delovanje kritične infrastrukture (interni vir ICS)
Tabela 2: Določitev kritičnih poslovnih procesov (interni vir ICS)
Tabela 3: Ocena kritičnosti procesa (interni vir ICS)
Tabela 4: Nedostopnost produktov poslovnega procesa – kritičnost časa (interni vir ICS)
Tabela 5: Analiza tveganj (primer za najbolj tvegane procese in sisteme)
Tabela 6: Izredni dogodki (interni vir ICS)
Tabela 7: Upravljanje tveganj za delovanje KI (interni vir ICS)
Tabela 8: Upravljanje tveganj za delovanje KI
Tabela 9: Identifikacija nevarnosti za določen sektor KI (smiselno prirejeno po MOSAR)
Tabela 10: Tabela škode (smiselno prirejeno po MOSAR)
Tabela 11: Matrika scenarijev (smiselno prirejeno po MOSAR)
Tabela 12: Ocena kritičnosti - okvir najslabših možnih scenarijev (NMS)
Tabela 13: Scenariji »rdeče cone« (interni vir ICS)
Tabela 14: Kriteriji za resnost odpovedi (prirejeno po standardu)
Tabela 15: Kriteriji za verjetnost odpovedi (prirejeno po standardu)
Tabela 16: Kriteriji za oceno odkrivanja (prirejeno po metodologiji)
Tabela 17: Vzorec registra tveganj
Tabela 18: Tabela škode - resnost (smiselno prirejeno po MOSAR)
Tabela 19: Matrika scenarijev (smiselno prirejeno po MOSAR)
Tabela 20: Vzorec: Ocena kritičnosti - okvir najslabših možnih scenarijev (NMS)
Tabela 21: Identifikacija virov nevarnosti za sektor energetike
Tabela 22: Ocena kritičnosti - okvir najslabših možnih scenarijev
Tabela 23: Kriteriji za resnost odpovedi (smiselno prirejeno po standardu)
Tabela 24: Kriteriji za verjetnost odpovedi (smiselno prirejeno po standardu)
Tabela 25: Kriteriji za oceno odkrivanja (smiselno prirejeno po metodologiji)
Tabela 26: Primer FMEA delovnega lista
Tabela 27: Matrika tveganj FMEA (smiselno prirejeno po standardu)
Tabela 28: Primer izpolnjenega FMEA delovnega lista

PRILOGA 3 - Primer FMEA delovnega lista

Proces /produkt: _____ Številka FMEA: _____

Projektna skupina: _____ Datum izdelave: _____

Vodja skupine: _____ Datum revizije: _____

FMEA ref.	Element (proces, produkt)	Možni način odpovedi	Možni vzrok odpovedi	Učinek odpovedi	Ocena resnosti (S)	Ocena verjetnosti (O)	Ocena odkrivanja (D)	Tveganja na ravni RPN=SxOxD	Predlagani ukrepi	Odgovoren	Izvedene aktivnosti	Ponovna ocena S, O, D, RPN