Upravljanje tveganj

Borut Jereb

Univerza v Mariboru
Fakulteta za logistiko

Celje, 2014

Avtor: JEREB, Borut

Naslov: Upravljanje tveganj

Recenzenti: Izr. prof. dr. Bojan Rosi, Izr. prof. ddr. Teodora Ivanuša in Prof. dr. Iztok Podbregar

Lektoriranje: Darja Kukovič, prof. zgod. in uni. dipl. polit.

Založnik: Univerza v Mariboru , Fakulteta za logistiko

Izdano: Decembra 2014 v Celju

Naklada: 200 izvodov

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

005:656(0.034.2)

JEREB, Borut, 1962-
Upravljanje tveganj [Elektronski vir] / Borut Jereb. - El. knjiga. - Celje : Fakulteta za logistiko, 2014

Način dostopa (URL): http://labinf.fl.uni-mb.si/upravljanje-tveganj/
ISBN 978-961-6962-03-2

277108736

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

005:656

JEREB, Borut, 1962-
Upravljanje tveganj / Borut Jereb. - Celje : Fakulteta za logistiko, 2014

ISBN 978-961-6962-04-9

277109248

Knjiga je urejena s programom LaTeX. TeX je blagovna znamka American Mathematical Society.

Pri pošiljanju predlogov za spremembe in dopolnitve te publikacije se STRINJAM Z NASLEDNJO IZJAVO: V kolikor bo avtor publikacije upošteval moje predloge sprememb publikacije in bodo le te dodane v novejšo verzijo publikacije, se odpovedujem vsem materialnim avtorskim pravicam, ki izhajajo iz mojega avtorskega dela in se strinjam z objavo mojega imena med avtorji publikacije. Naslov za pošiljanje predlogov je borut.jereb@fl.uni-mb.si.

Za potrpežljivo delo lektoriranja in za vse nasvete pri nastajanju besedila se zahvaljujem Darji Kukovič, profesorici zgodovine in univerzitetni diplomirani politologinji.

Kazalo

Slike

Tabele

Poglavje 1

Uvod

Organizacije, katerih delovanje je zelo regulirano, kot je to v primeru finančnih institucij, telekomunikacijskih podjetij, energetskega sektorja, zdravstva in farmacevtske industrije ter podobnih, je upravljenje tveganj v veliki meri vpeto v njihovo vsakodnevno poslovanje že mnogo let. Pri mnogih organizacijah pa se šele v zadnjem času stanje spreminja v smeri zavedanja pomena učinkovitega upravljanja tveganj. Praksa kaže, da se vrh upravljavske piramide v organizacijah začenja zavedati pomena upravljanja tveganj, ob tem pa se večje število zaposlenih v poslovnem svetu začenja ukvarjati s tveganji. Upravljanje tveganj se s časom prenese povsem na operativni nivo in od tam nazaj na poslovni nivo upravljanja, saj se tveganja prenašajo iz nivoja na nivo in jih ne moremo upravljati izolirano, vsako zase. Prenašajo se tudi po horizontali med samimi oddelki. Največkrat se organizacija zave upravljanja tveganj, kot samostojnega področja delovanja, v času priprave načrtov za neprekinjeno poslovanje.

Ne glede na dobrodošle spremembe, upravljanje s specifičnimi tveganji, kot so tveganja v IT ali logistiki, običajno še vedno niso sestavni del strateškega načrtovanja v organizacijah. IT, logističnih in drugih specifičnih tveganj v vrhu upravljavske piramide organizacije še vedno ne zaznavajo kot področja, ki bi zahtevalo predstavnika „tveganj" (to je lastnika „tveganj") v vodstvu. Seveda smo tudi pri srednjem upravljavskem nivoju daleč od idealnih razmer: četudi upravljavci tveganj igrajo osrednjo vlogo pri analizi in obravnavi tveganj v organizaciji, še vedno kronično primanjkuje osebja in znanja.

V praksi se pojavlja tudi problem pri učinkoviti in pragmatični realizaciji upravljanja tveganj po tem, ko je že opravljena korektna ocena tveganja, saj ne pride do premišljene odločitve, kaj s tveganjem napraviti – pa čeprav bi to pomenilo odločitev, da glede nekega tveganja ne naredimo ničesar. V takšnem okolju je nastal standard ISO 31000,

ki je nevtralen do kakršnega koli poslovanja organizacije. Predstavlja dobro izhodišče za vse, ki se šele začenjajo ukvarjati z tveganji, in za tiste, ki iščejo nekaj več.

ISO 31000 je pisan v poslovnem jeziku z namenom razumevanja ključnih konceptov in terminologije pri upravljanju tveganj. Prispeva h konsistentnosti upravljanja tveganj s pregledom tehnik in metod. Definira izrazoslovje in tako rešuje pereče probleme uporabe skupnega jezika za opisovanje tveganja, merjenja vplivov, verjetnosti, negotovosti ter ostalih dimenzij upravljanja tveganj med tehnološko in poslovno usmerjenim kadrom v organizaciji in med organizacijami.

Nek vsesplošno priznan standard ali okvir za upravljanje tveganj je namreč potreben, saj mora vsaka organizacija vsaj:

1. poenotiti jezik za delo s tveganji;
2. uporabiti skupno metriko za delo s tveganji ne glede na področje uporabe (poslovno, tehnološko, itd);
3. varnost na vsakem področju delovanja (tudi na področju IT in logistike, na primer) je potrebno integrirati v splošno varnost organizacije;
4. tveganja vsakega področja je potrebno znati predstaviti v kontekstu ali jih prevesti v poslovna tveganja; in navsezadnje
5. vsa tveganja prevesti v jasno sliko investicij.

ISO 31010 podpira standard ISO 31000 v tistem delu, ki se ukvarja s prepoznavanjem in ocenjevanjem tveganj. Oboje je sestavni del upravljanja tveganj. Standard je podlaga za odločanje o najustreznejšem pristopu za obvladovanje posameznega tveganja, je pomoč pri implementaciji principov obvladovanja tveganj (iz ISO 31000).

ISO/IEC 27005 opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost. Ne določa, ne predlaga, ne imenuje kakršne koli metode za analizo tveganj. Določa pa strukturirane, sistematične in natančno določene procese (od analize do izdelave načrtov upravljanja).

ISO/IEC 27001 je mednarodni standard, ki podaja model za vzpostavitev, izvajanje, upravljanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema informacijske varnosti. Učinkovit sistem upravljanja informacijske varnosti predpostavlja sistematično upravljanje informacijskih tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem v katerem organizacija deluje. Navsezadnje mora biti upravljanje informacijskih tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje.

Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje tveganj na področjih in v času, kjer in ko je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Pomembnejši standard s področja varnosti v logistiki, ki se neposredno nanašajo tudi na upravljanje tveganj, je ISO 28000, katerega namen je izboljšanje varnosti oskrbovalne verige. Namenjen je upravljavskemu nivoju organizacije, ki je v pomoč pri vzpostavitvi celovitega sistema upravljanja varnosti oskrbovalne verige tako, da organizacija oceni okolje v katerem deluje in ugotovi, ali so vzpostavljeni ustrezni varnostni ukrepi, in ali organizacija izpolnjuje vse zakonske zahteve.

V tem poglavju bo še opisan model tveganj, ki temelji na segmentaciji javnosti. V tem modelu je bistvena predpostavka, da so tveganja lastna ljudem in ne stvarem ali pojmom. Princip modeliranja tveganj predvideva, da moramo model sistema procesov ter vhode in izhode v procese segmentirati prav tako kakor javnost, pri kateri želimo tveganja modelirati in simulirati. Tovrstni pristop zahteva bistveno kompleksnejše modeliranje tveganj kot je danes najpogosteje v uporabi, vendar po drugi strani prinaša večjo zaupanje v modeliranje, saj je bliže realnosti življenja.

Na koncu poglavja bo opisan še primer kataloga tveganj, kot rezultat konvencionalnega prepoznavanja in ocenjevanja tveganj, ki vsebuje vsa prepoznana in opisana tveganja s področja oskrbovalne verige. Proces upravljanja tveganj je zahteven in zato velikokrat počasen in ne dovolj natančen. Ideja prosto dostopnega kataloga vseh do sedaj prepoznanih tveganj pa organizacijam nudi možnost, da pri procesu uporabijo tudi zunanja znanja, ko se lotevajo upravljanja tveganj. Katalog tveganj vsebuje tveganja v oskrbovalni verigi, ki so bila prepoznana v organizacijah z različnih področij delovanja. Zato je lahko odličen vir informacij za širok spekter organizacij, ki pristopajo k upravljanju tveganj, saj ga lahko uporabljajo kot smernice za prepoznavanje tveganj in kot opomnik, s katerim ugotovijo, katera od že identificiranih tveganj iz kataloga lahko prepoznajo tudi znotraj svoje organizacije.

1.1 Problem definicije in razumevanja pojma tveganje

Tveganja so del našega bivanja in videti je, kot da se ljudje še nikoli do sedaj nismo toliko ukvarjali z izzivi tveganj, kot ravno v današnjem času. Tveganja so predmet obravnave v številnih člankih, komentarjih in pogovorih. Prav tako obstaja veliko različnih doje-

manj in definicij tega pojma. Tudi če se neka javnost uskladi glede definicije tveganja, še ne jamči mnenjske usklajenosti: Kako tveganja zaznati? Kako jih meriti? Katerim tveganjem smo v katerem trenutku izpostavljeni? Kolikšne so posledice izpostavljenosti tveganjem – kakšen je njihov vpliv? Katera in kako velika tveganja so sprejemljiva? Za koga so sprejemljiva in za koga ne? Kako se tveganja spreminjajo skozi čas? Kako vplivajo posamezno, kako združeno? Kakšen je njihov medsebojni vpliv in kakšne so posledice teh interakcij? Kako jih upravljati? Kako ovrednotiti potrebna sredstva za zmanjšanje tveganj? Odprtih vprašanj je še veliko in dajejo slutiti kompleksnost problema, na katerega naletimo, ko skušamo tveganja celovito obravnavati in jih upravljati.

Kaj pomeni pojem tveganje razumemo, vendar ima ta pojem številne različne interpretacije. Poglejmo si nekatere izmed njih:

1. V spletnem slovarju BusinessDictionary.com [1] je podanih šest definicij z različnih področij. Prva definicija je splošna in pravi, da je tveganje: „Verjetnost ali nevarnost za nastanek škode, poškodbe, izgube, kršenja obveznosti ali kakšen drug negativen dogodek, ki ima zunanje ali notranje vzroke in ga je mogoče vnaprej nevtralizirati z zaščitnimi akcijami.” Druga definicija je s finančnega področja in opisuje sedemnajst različnih kombinacij in pomenov besede tveganje. Sledijo še definicije s področja prehrambene industrije, zavarovalništva, trgovine in navsezadnje delovnega mesta. Slednja pravi, da je tveganje: „Produkt resnosti posledic in vpliva verjetnosti nekega tveganega dogodka ali fenomena.”

2. V spletnem slovarju InvestorWords.com [4] je tveganje opisano kot: „. . . merljiva verjetnost za izgubo ali izgubo zaradi zmanjšanja . . . ” Tudi tu ponujajo definicije v dvajsetih kombinacijah besede tveganje s kakšno drugo besedo.

3. Na Wikipediji [26] je v članku o pojmu tveganje napisano, da definicija besede potrebuje dodatno pozornost ekspertov, kar kaže na to, da obstaja mnenje, da beseda ni dovolj dobro definirana, kljub temu, da je prispevek nadpovprečno dolg in upošteva mnoge vidike. Med drugim je v prispevku zapisano, da je tveganje koncept, ki natančno opisuje verjetnosti za posamezne možne izzide. V nadaljevanju je opisano, da je tveganje potrebno opisati kvalitativno in kvantitativno. Citirajo tudi Franka Knighta, ki je v svojem delu [6] razmeji tveganje in negotovost.

4. Adam Green [2] v svojem članku pravi, da vsaka definicija tveganja prinaša subjektiven pogled na to, kaj tveganje je, glede na področje in način uporabe. V svojem delu, ki govori o vodenju projektov, predstavi tudi definicijo, kjer je tveganje enako

produktu med nevarnostjo in izpostavljenostjo in je izpostavljenost enaka vplivu škode na tisto ali tistega, na katerega škoda vpliva. Na vsak način je zanj osrednji pojem nevarnost, da se zgodi slučajni dogodek (hazard).

5. Po Johnathanu Munu [23] sta pojma negotovost in tveganje različna, vendar povezana. Tveganja so nekaj, kar je nekomu ali nečemu lastno in je posledica negotovosti. Isti avtor pravi, da je na začetku vedno negotovost in z njo povezana tveganja, ki s časom, v katerem se izvajajo neke akcije in dogajajo dogodki, preidejo v dejstvo. Mun tudi trdi, da se lahko soočimo z negotovostjo, ki sploh nima tveganja. To opisuje na primeru strmoglavljenja letala, na katerem sta dve osebi in eno staro padalo, za katerega ne vemo, ali se bo ob uporabi sploh odprlo ali ne. Obe osebi sta v enaki negotovosti glede tega, ali se bo padalo odprlo ali ne. Če je objekt negotovosti staro padalo in se obe osebi dogovorita, kdo bo uporabil padalo, potem bo oseba s padalom prevzela vso tveganje glede odprtja padala od trenutka, ko bo oseba izskočila iz padajočega letala, pa do trenutka, ko se bo padalo odprlo oziroma bo ostalo zaprto. Medtem druga oseba, ki nima padala, ne bo v ničemer tvegala glede delovanja padala, obenem pa nima možnosti, da preživi.

Iz različnosti zgornjih definicij je mogoče sklepati, da vsako področje pojem tveganje opredeljuje drugače; tudi v okviru področij se krešejo mnenja o različnih interpretacijah in celo pri posameznem primeru imamo opraviti z različnimi, nemalokrat nasprotujočimi mnenji o tveganjih.

Vsako področje ima tako svojo definicijo tveganj ali prevzame eno od obstoječih. Te definicije niso popolne, saj gre za kompleksen pojem, kar potrjuje že njihova številnost. Uporaba posameznih definicij, ki reducirajo kompleksnost tveganj, je verjetno nujna, da v eksaktnih znanstvenih disciplinah sploh lahko uporabljamo ta pojem. Zavedati se moramo, da so tveganja zanimiva aktualna problematika. Veliko ljudi se ukvarja z modeli tveganj (VaR, SARA, SPRINT), ki so vedno bolj kompleksni in upoštevajo vse več lastnosti tveganj oziroma parametrov. Tu so še standardi in ogrodja za upravljanje tveganj (ISO 31000, AS/NZ 4360 COSO ERM, IT Risk Management Framework).

Pri iskanju definicije tveganja smo v bližnji preteklosti prišli do točke, ko se v okviru mednarodne institucije ISO niso mogli poenotiti glede ključne opredelitve glede definicije tveganja. Tako v standardu ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management manjkala natančna definicija terminov, kot so: nevarnost (grožnja), ranljivost, verjetnost (likelihood), kot je v uporabi pri študiju tveganj ter predstavlja kombinacijo grožnje in ranljivosti, ter navsezadnje tveganje [21].

Kmalu po izidu standarda je v članku na ta problem opozoril Steven J. Ross [24]. V tem primeru, ki pa zdaleč ni edini, smo se soočali z vprašanjem natančne in jasne obravnave problematike, ko osnovni pojmi problematike niso bili nedefinirani. O čem je govoril ISO/IEC 27005 (v stari verziji), če ne vemo, kaj tveganje je? Standard je bil napisan tako splošno, da bi se ga dalo verjetno uporabiti tudi na drugih področjih (na primer na področju logistike). Vsekakor pa so ostajala odprta vprašanja, kaj tveganja so, kako jih določiti in upravljati. Standard je govoril tudi o tem, da tveganja ocenjujemo s splošnega in podrobnega nivoja. Torej smo se lotevali delitve tveganj na splošen in podroben nivo, a še vedno nismo vedeli, kaj tveganje točno je. Takšnemu stanju smo bili priča do nove verzije standarda, ki nosi oznako ISO/IEC 27005:2011 (izšel je leta 2011) in je bila sinhronizirana z ISO 31000. Nedorečena pa ostajajo še številna področja, kjer se pogovarjamo o tveganjih, ne da bi bil sam pojem, za potrebe področja, definiran.

Poglavje 2

Standard ISO 31000:2009

ISO 31000:2009 [7] določa načela in splošne smernice za upravljanje tveganj. Uporablja se za vse vrste tveganj, ne glede na njihovo naravo, in predvideva tako pozitivne kakor tudi negativne posledice. Namenjen je organizacijam vseh vrst, ne glede na njihovo specifičnost. Čeprav določa splošne smernice, pri tem ne zahteva enotnosti pri upravljanju tveganj. Pri vzpostavitvi in implementaciji načrtov in okvirov za upravljanja tveganj upošteva različnost potreb v organizacijah, posebnosti njihovih ciljev, kontekst, strukturo, načina delovanja, procese, funkcije, projekte, izdelke, storitve in sredstva ter specifičnosti obstoječih praks.

Zaradi splošnega konteksta omogoča celovita navodila za upravljanje tveganj na različnih področjih in je tako namenjen organizacijam vseh velikosti in vseh vrst, ne glede na njihovo specifičnost (organizacijam s področja financ, inženirstva, varnosti, in ostalim).

Namenjen je uporabi skozi celotno življenjsko dobo organizacije z najširšim razponom dejavnosti, ki vključuje tudi vzpostavitev strategij, odločanje, poslovanje, izvajanje projektov, izvajanje ostalih funkcij organizacije, proizvodnjo in upravljanje z izdelki, storitvami in sredstvi ter podobnim.

Standard že takoj na začetku definira tveganje, ko pravi: Organizacije različnih tipov in velikosti so soočene z notranjimi in zunanjimi faktorji in vplivi, ki povzročajo negotovost glede časa, v katerem bo organizacija dosegla svoje cilje in glede tega, če jih sploh bo dosegla. Učinek negotovosti glede doseganja ciljev organizacije je „tveganje".

Standard ni namenjen temu, da bi se organizacije v skladu z njim certificirale.

Proces upravljanja tveganj v organizaciji ali v celotni oskrbni verigi je priporočljivo zastaviti v okviru cikla Plan-Do-Check-Act (PDCA), ki je že uveljavljen procesni cikel, tudi v okviru standarda ISO 9001. Osnovna ideja cikla je, da proces najprej zasnujemo in

načrtujemo (Plan), nato ga uvedemo oziroma izvedemo (Do), ga preverjamo in nadzorujemo (Check) ter na podlagi ugotovitev prilagajamo, spreminjamo in dopolnjujemo, ter stalno izboljšujemo (Act). Standard ISO 31000 pri svojem okvirju za upravljanje tveganj uporablja cikel PDCA, prirejen za namene upravljanja tveganj. Slika 2.1 prikazuje relacije med principi, okvirom in procesom upravljanja tveganj po ISO 31000. V splošnem standard določa arhitekturo za učinkovito upravljanje tveganj. Gradniki te arhitekture pa so principi, okvir in proces.

2.1 Struktura dokumenta ISO 31000

Standard sestavlja pet poglavij in dodatek – skupaj 23 strani.

Po uvodu sledi pomembno poglavje z definicijami in opisom posameznih terminov. Gre za povzetek dokumenta ISO Guide 73:2009, Risk Management – Vocabulary [9]. To poglavje je za razumevanje celotnega standarda nepogrešljivo in zavzema polnih šest strani.

Tretje poglavje predstavi ključnih enajst principov uspešnega upravljanja tveganj v neki organizaciji. Za predstavitev teh principov porabi dobro stran. V dodatku je opisanih nekaj nadaljnjih usmeritev za organizacije, ki si želijo učinkoviteje upravljati tveganja.

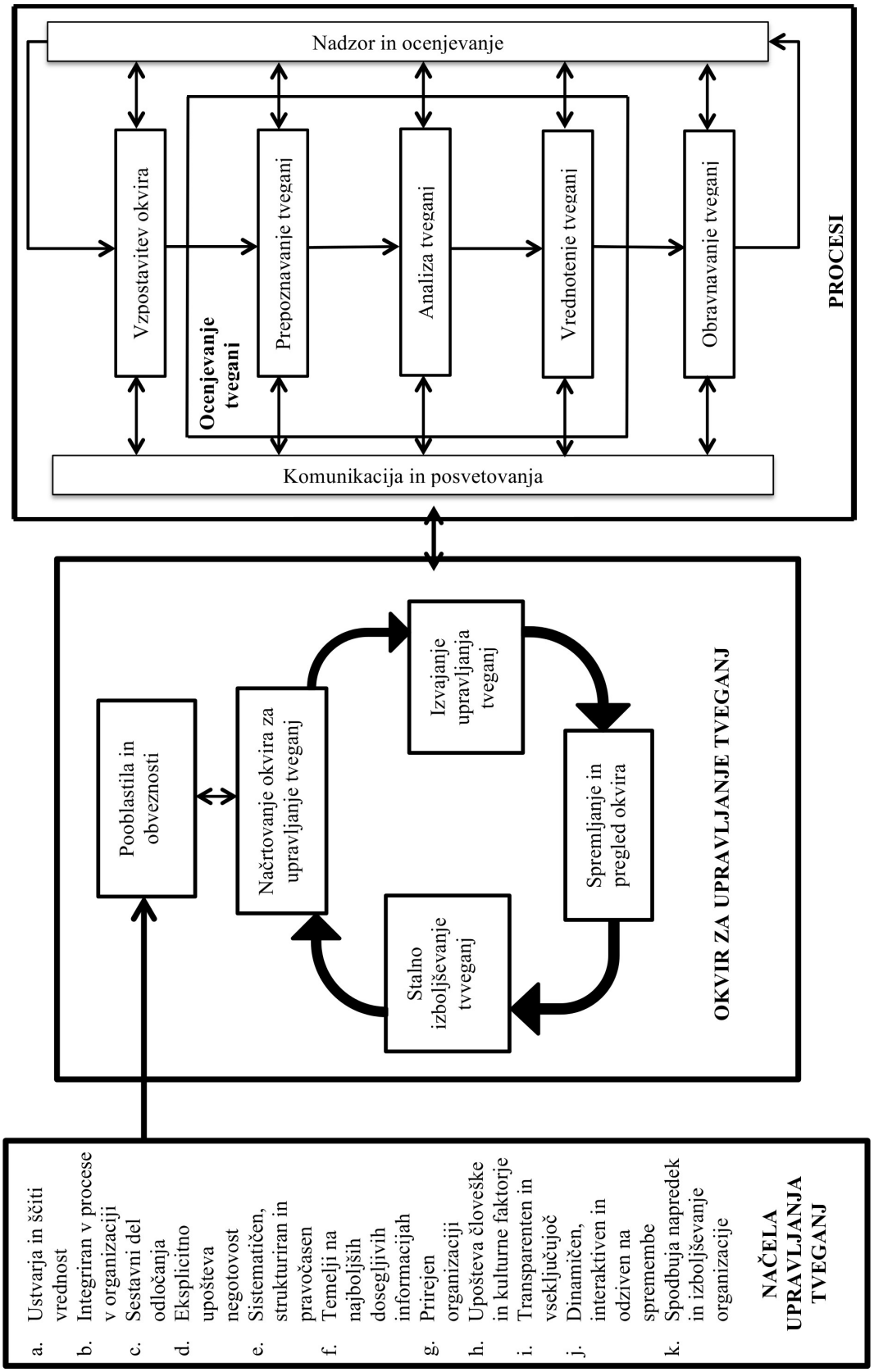
Četrto poglavje opisuje okvir za učinkovito upravljanje tveganj, ki naj bi bil vsebovan na vseh nivojih organizacije. Okvir zagotavlja, da se o tveganjih ustrezno poroča tako, da je mogoče na osnovi informacij (informacije nastanejo v procesu upravljanja tveganj) sprejemati ustrezne odločitve – seveda na vseh nivojih vodenja organizacije. Okvir je opisan na petih straneh.

Zadnje poglavje na osmih straneh podrobno opisuje proces upravljanja tveganj. Sestavljen je iz petih glavnih aktivnosti. Osrednja aktivnost je ocenjevanje tveganj, ki ga pa podrobneje opisuje ISO/IEC 31000, in je skupno ime za (pod)aktivnosti identifikacije, analize in vrednotenje tveganj.

2.2 Termini in definicije po ISO 31000

2.2.1 Tveganje

Učinek negotovosti pri doseganju ciljev.



Slika 2.1: Relacije med principi, okvirom in procesom standarda ISO 31000

Opomba 1 Negotovost je odklon od pričakovanega (pozitiven in/ali negativen).

Opomba 2 Cilji organizacije lahko imajo različne vidike (kot npr. finančni, vidik zdravja in varnosti te okoljevarstveni) in se lahko upoštevajo na različnih nivojih (kot npr. strateški, nivo celotne organizacije, nivo izdelkov in procesov).

Opomba 3 Tveganje je pogosto opisano kot referenca morebitnim *dogodkom* in *posledicam* oziroma kombinacij obeh.

Opomba 4 Tveganje je pogosto izraženo kot kombinacija posledic nekega dogodka (tukaj so vštete tudi možne spremembe okoliščin) in s tem povezane *verjetnosti* določenega pojava.

Opomba 5 Negotovost je stanje, ki se delno pojavi takrat, ko se zgodi pomanjkanje informacij in/ali znanj, povezanih z razumevanjem oziroma poznavanjem dogodka, njegovih posledic ali verjetnosti.

2.2.2 Upravljanje tveganj

Koordinirane aktivnosti upravljanja in kontroliranja organizacije v povezavi s tveganjem, ki dajejo okvir za učinkovito upravljanje *tveganj*.

2.2.3 Okvir za učinkovito upravljanje tveganj

Gre za sklop sestavin, ki zagotavljajo temeljne in organizacijske ureditve za oblikovanje, vpeljavo, *nadzorovanje*, poročanje in nenehno izboljšavo *upravljanje tveganj* celotne organizacije.

Opomba 1 Temelji, ki vključujejo politiko, cilje, pooblastila in zavzetost upravljanju *tveganj*;

Opomba 2 Organizacijski dogovori, ki vključujejo plane, razmerja, odgovornosti, sredstva, procese in aktivnosti; ter

Opomba 3 Okvir za učinkovito upravljanje tveganj, ki sovpada s splošno organizacijsko strategijo in aktivnostmi te organizacije.

2.2.4 Politika ukvarjanja s tveganji

Izjava, ki zajema splošne namene in usmeritve organizacije v povezavi z *upravljanjem tveganj*.

2.2.5 Odnos do tveganja

Odnos do *tveganja* pomeni pristop organizacije, s katerim ta tveganja oceni ter jim posledično sledi oziroma se jim izogne.

2.2.6 Planiranje upravljanja tveganj

Shema znotraj *okvira za učinkovito upravljanje tveganj*, ki navaja pristop, komponente upravljanja in sredstva, ki so dodeljena upravljanju *tveganj*.

Opomba 1 Komponente upravljanja ponavadi vključujejo postopke, prakse, dodeljevanja odgovornosti, zaporedja in tempiranje aktivnosti.

Opomba 2 Plan upravljanja tveganj se lahko nanaša na določen produkt, proces in projekt ter lahko zajema le del organizacije ali pa celotno.

2.2.7 Lastnik tveganja

Oseba ali subjekt z odgovornostjo in pooblastili za upravljanje *tveganja*.

2.2.8 Proces upravljanja tveganj

Sistematična uporaba politike upravljanja, postopkov in praks v zvezi z aktivnostmi komuniciranja, svetovanja, identificiranja, analiziranja, ocenjevanja in opazovanja *tveganj* ter ravnanja z njimi.

2.2.9 Vzpostavitev okvirov

Definiranje zunanjih in notranjih parametrov, ki jih je treba vzeti v ozir pri upravljanju tveganj, ter določitve obsega in *kriterijev tveganja* za politiko *upravljanja tveganj*.

2.2.10 Zunanji okvir

Zunanje okolje, v katerem si organizacija prizadeva izpolniti zadane cilje. Pod zunanje okolje lahko spada:

- kulturno, socialno, politično, pravno, regulativno, finančno, tehnološko, naravno in konkurenčno okolje, ne glede na to ali je mednarodno, državno, regionalno ali lokalno;
- ključni dejavniki in trendi, ki imajo vpliv na cilje organizacije; ter
- odnosi, dojemanje in vrednotenje zunanjih zainteresiranih strani (deležniki itd.).

2.2.11 Notranji okvir

Notranje okolje, v katerem si organizacija prizadeva izpolniti zadane cilje. Pod notranje okolje lahko spada:

- vodstvo, organizacijska struktura, vloge in odgovornosti posameznikov;
- politika, cilji in strategije ki so realno zastavljene;
- zmogljivosti, ki se razumejo pod pojmom sredstev in znanja (npr. kapital, čas, ljudje, procesi, sistemi in tehnologije);
- informacijski sistemi, pretok informacij in procesi odločanja (formalni in neformalni);
- odnosi, dojemanje in vrednotenje notranjih zainteresiranih strani;
- organizacijska kultura;
- standardi, navodila in modeli privzeti s strani organizacije; ter
- oblika in obseg pogodbenih razmerij.

2.2.12 Komunikacija in posvetovanje

Stalni in ponavljajoči se procesi, ki jih vodi organizacija, da zagotavlja, deli in pridobiva informacije, ter da se vključi v dialog z *deležniki* v zvezi z obvladovanjem *tveganj*.

Opomba 1 Informacije se lahko nanašajo na obstoj tveganj, njihovo naravo, obliko, *verjetnost*, pomen, vrednost, sprejemljivost ter na siceršnjo obravnavo tveganj.

Opomba 2 Posvetovanje je dvosmerni proces informirane komunikacije med organizacijo in zunanjimi vlagatelji v zvezi z odločitvijo ali determiniranjem usmerjenosti glede te odločitve.

Posvetovanje je:

- proces, ki vpliva na odločitev s pomočjo vpliva (raje kot moči) in
- prispevek k odločanju (vendar pa to ni skupno odločanje).

2.2.13 Interesna skupina

Oseba ali organizacija, ki lahko vpliva, sama čuti vpliv, ali pa sama zazna odločitev ali aktivnost.

Deležnik je lahko tisti, ki sprejema odločitve.

2.2.14 Ocenjevanje tveganja (Risk Assesment)

Proces, ki združuje *prepoznavanje* (Risk Identification), *analizo* (Risk Analysis) in *vrednotenje* (Risk Evaluation) tveganj.

2.2.15 Prepoznavanje tveganja (Risk Identification)

Proces iskanja, prepoznavanja in opisovanja *tveganja*.

Opomba 1 Identifikacija tveganja vključuje identifikacijo *virov tveganja*, *dogodkov*, njihovih namenov in potencialnih *posledic*.

Opomba 2 Identifikacija tveganja lahko vključuje zgodovinske podatke, teoretične analize, informacijska mnenja in mnenja specialistov ter potrebe *vlagateljev*.

2.2.16 Vir tveganja

Element, ki lahko sam ali v kombinaciji z drugimi določi od kod izvira *tveganje*. Vir tveganja je lahko oprijemljiv ali neoprijemljiv.

2.2.17 Dogodek

Pojav ali sprememba določenega sklopa okoliščin.

Opomba 1 Dogodek je lahko en ali več pojavov, in lahko ima več namenov.

Opomba 2 Dogodek je lahko sestavljen iz nečesa, kar se dejansko ne dogaja.

Opomba 3 Dogodek je lahko včasih naslovljen kot „incident" ali „nesreča".

Opomba 4 Dogodek brez *posledic* se lahko imenuje tudi, „nevaren pojav", „incident", „skorajšnji zadetek", „tesen izid".

2.2.18 Posledice

Rezultat *dogodka*, ki vpliva na cilje.

Opomba 1 Dogodek lahko privede do različnih posledic.

Opomba 2 Posledice so lahko določene ali nedoločene in imajo pozitivne ali negativne učinke na cilje.

Opomba 3 Posledice so lahko izražene kvalitativno ali kvantitativno.

Opomba 4 Začetne posledice se lahko stopnjujejo do verižne reakcije.

2.2.19 Verjetnost (Likelihood)

Verjetnost, da se bo nekaj zgodilo.

Opomba 1 V terminologiji upravljanja tveganj je beseda verjetnost (likelihood) uporabljena kot možnost, da se nekaj zgodi, kar je lahko definirano, izmerjeno, determinirano, subjektivno ali objektivno, kvalitativno ali kvantitativno. Opisana je z uporabo splošnih matematičnih terminov.

Opomba 2 »Likelihood« v drugih jezikih nima sopomenke, zato se uporablja tudi »probability«. V angleščini je »probability« dostikrat uporabljan kot ozek matematični pojem. V tej terminologiji je torej »likelihood« izraz, ki zajema enako obsežnost kot »probability« v drugih jezikih.

2.2.20 Profil tveganja

Opisi celote *tveganj*.

Opomba Celota tveganj zajema tista tveganja, ki se nanašajo na celotno organizacijo, del organizacije ali je definirana kako drugače.

2.2.21 Analiza tveganja (Risk Analysis)

Proces razumevanja narave *tveganja* in določitve *stopnje tveganja*.

Opomba 1 Analiza tveganja predstavlja osnovo za *vrednotenje tveganja*, na tej podlagi pa odločitev glede morebitnega *obravnavanja tveganja*.

Opomba 2 Analiza tveganja se zaključi z vrednotenjem tveganja.

2.2.22 Vrednotenje tveganja (Risk Evaluation)

Naloge, s katerimi ocenimo pomen *tveganja*.

Opomba 1 Vrednotenje tveganja temelji na osnovi organizacijskih ciljev in *notranjega* ter *zunanjega okvira*.

Opomba 2 Vrednotenje tveganja mora izhajati iz standardov, zakonov, politike in drugih zahtev.

2.2.23 Nivo tveganja

Obseg *tveganja* ali kombinacije tveganj, izražene v kombinacijah *posledic* in njihovih *verjetnosti*.

2.2.24 Ocena tveganja (Risk Assesment)

Proces primerjanja rezultatov z *analizo tveganja* in *vrednotenjem tveganja*, da ugotovimo ali je *tveganje* in njegov obseg sprejemljiv.

Opomba Ocena tveganja pomaga pri odločitvi glede obravnavanja tveganja.

2.2.25 Obravnava tveganja (Risk Treatment)

Proces za modificiranje *tveganj*.

Opomba 1 Obravnava tveganj lahko pomeni:

- izogniti se tveganju tako, da ne začnemo ali ne nadaljujemo aktivnosti, ki tveganje povzroča;
- povečanje tveganja za priložnost;
- odpraviti *vir tveganja*;
- spremeniti *verjetnost* dogodka;
- spremeniti *posledice* dogodka;
- deliti tveganje z drugimi pogodbeniki (vključujoč pogodbe in rizično financiranje); in/ali
- s premišljenimi odločitvami ohraniti tveganje.

Opomba 2 Obravnave tveganj, ki se ukvarjajo z negativnimi posledicami, se včasih nanašajo na blaženje tveganja, odpravljanje tveganja in zmanjšanje tveganja.

Opomba 3 Obravnava tveganj lahko ustvari tudi nova tveganja ali modificira obstoječa tveganja.

2.2.26 Nadzor (Supervision)

Ukrep, ki spreminja/modificira *tveganje*.

Opomba 1 Nadzor vključuje vse procese, politiko, naprave, prakse in druge akcije za modificiranje tveganja.

Opomba 2 Nadzor ne izvaja vedno namenjenega modifikacijskega učinka.

2.2.27 Preostalo tveganje (Residual Risk)

Tveganje, ki ostane po *obravnavi tveganja*.

Opomba 1 Preostalo tveganje lahko vsebuje nedefinirano tveganje.

Opomba 2 Preostalo tveganje je lahko znano kot zadržano tveganje.

2.2.28 Spremljanje (Monitoring)

Konstantno preverjanje, nadzor, kritično opazovanje in definiranje statusa, da bi se definirala pričakovana in želena sprememba.

Opomba Spremljanje/monitoring se lahko aplicira v *okvir upravljanja tveganja*, v *proces upravljanja tveganja*, v *tveganje* ali v *kontrolo*.

2.2.29 Pregled (Review)

Dejavnost za zagotavljanje primernosti, učinkovitosti in ustreznosti predmeta za dosego postavljenih ciljev.

Opomba Pregled se lahko aplicira v *okvir upravljanja tveganja*, v *proces upravljanja tveganja*, v *tveganje* ali v *kontrolo*.

2.3 Principi

Organizacija naj bi za učinkovito upravljanje tveganj na vseh nivojih upoštevala naslednje principe:

1. **Upravljanje tveganj ustvarja in ščiti vrednost.** Dokazljivo prispeva k doseganju ciljev in izboljšanju učinkovitosti, kot je to v primeru človeškega zdravja in varnosti, zaščiti vseh vrst, pri usklajevanju s pravnimi predpisi, javnemu odobravanju, zaščiti okolja, kvaliteti proizvodov, projektnemu managementu, učinkovitosti pri poslovanju, upravljanju in ugledu.

2. **Upravljanje tveganj je sestavni del vseh procesov v organizaciji.** Upravljanje tveganj ne predstavlja samostojne aktivnosti, ki je ločena od glavnih aktivnosti in procesov organizacije. Upravljanje tveganj je del odgovornosti celotnega managementa in glavni del vseh organizacijskih procesov, vključno s strateškim planiranjem ter s procesi upravljanja projektov in procesi uvajanja sprememb.

3. **Upravljanje tveganj je sestavni del odločanja.** Upravljanje tveganj pomaga odločevalcem, da se ozaveščeno odločajo glede ukrepov in razlikujejo med alternativnimi postopki načinov delovanja.

4. **Upravljanje tveganj izrecno obravnava negotovost.** Upravljanje tveganj izrecno upošteva negotovost, naravo negotovosti in način, s katerim jo je mogoče obravnavati.

5. **Upravljanje tveganj je sistematično, strukturirano in pravočasno.** Sistematičen, pravočasen in strukturiran pristop k upravljanju tveganj prispeva k učinkovitosti in doslednim, primerljivim in zanesljivim rezultatom.

6. **Upravljanje tveganj temelji na najboljših informacijah, ki jih je mogoče pridobiti.** Vložek v proces upravljanja tveganj temelji na informacijskih virih kot so: zgodovinski podatki, izkušnje, odziv deležnikov, opazovanja, napovedi in strokovna presoja. Vendar pa bi se morali odločevalci pozanimati glede dostopnosti in primernosti podatkov ter upoštevati morebitne omejitve glede te dostopnosti, načina modeliranja ali možnosti razhajanja mnenj različnih strokovnjakov.

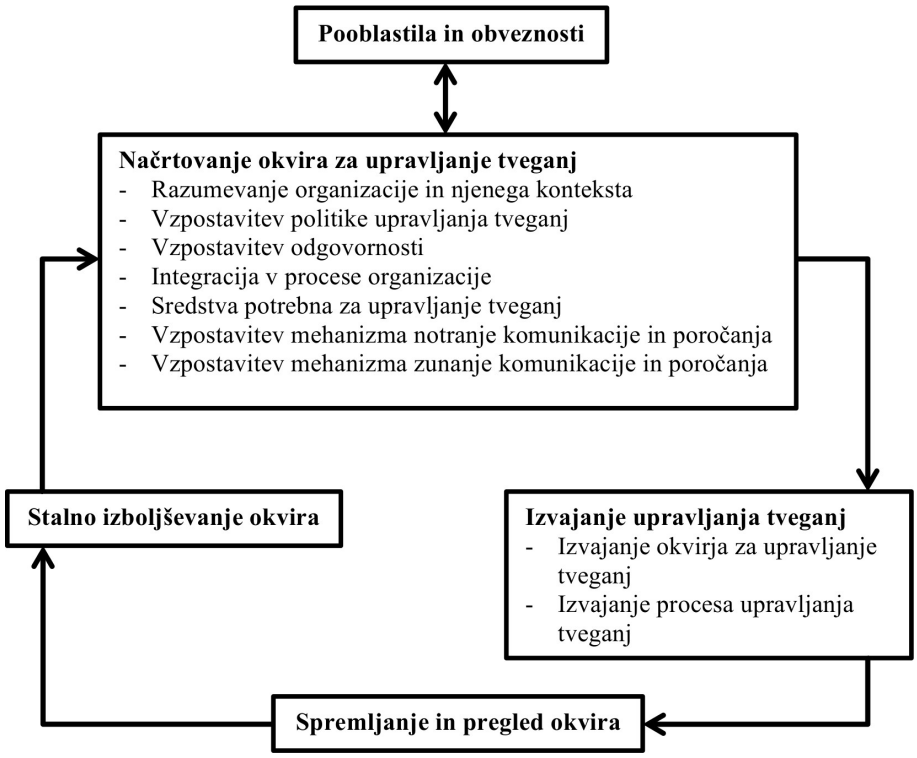
7. **Upravljanje tveganj je prilagojeno.** Upravljanje tveganj je potrebno prirediti glede na notranji in zunanji kontekst organizacije ter glede na vrsto tveganj.

8. **Upravljanje tveganj upošteva kulturne in človeške faktorje.** Z upravljanjem tveganj prepoznamo sposobnost, dojemanje in namene zunanjih in notranjih ljudi, ki lahko pospešijo ali zavirajo doseganje ciljev organizacije.

9. **Upravljanje tveganj je pregledno in neizključujoče.** Upravljanje tveganj vključuje različne deležnike in upravljavce na vseh nivojih organizacije. Primerna in pravočasna vključitev deležnikov in še posebej odločevalcev na vseh nivojih organizacije zagotavlja, da upravljanje tveganj ostaja vselej pomembno in posodobljeno. Vključitev deležnikov dovoljuje, da so primerno zastopani in da so njihova mnenja upoštevana pri določanju kriterijev glede tveganj.

10. **Upravljanje tveganj je dinamično, ponavljajoče se in sposobno odziva na spremembe.** Upravljanje tveganj nenehno zazanava in se odziva na spremembe. Ko se zgodijo zunanji in notranji dogodki, se spremeni kontekst in znanje, potekata spremljanje in pregled tveganja, lahko se pojavi novo tveganje, lahko se neko tveganje spremeni, lahko pa celo izgine.

11. **Upravljanje tveganj spodbuja in omogoča neprestano izboljševanje organizacije.** Organizacija bi morala razviti in izvajati strategije za izboljševanje zrelosti upravljanja tveganj, vzporedno z vsemi ostalimi vidiki v organizaciji.



Slika 2.2: Relacije med komponentami okvira upravljanja tveganj

2.4 Okvir

Uspeh obvladovanja tveganja je odvisen od učinkovitosti okvira upravljanja, ki zagotavlja temelje in ureditve, ki so vgrajeni v celotno organizacijo na vseh ravneh. Poleg tega okvir zagotavlja, da se informacije o tveganjih, ki nastanejo v procesu upravljanja tveganj, ustrezno sporočajo in uporabljajo kot osnova za odločanje in vzpostavitev odgovornosti na vseh ravneh organizacije. Slika 2.2 prikazuje okvir, iz katerega je mogoče razbrati, da se njegovi posamezni deli povezujejo na interaktiven način. Elementi slike 2.2 so zajeti tudi v sliki 2.1.

Okvir ni namenjen temu, da bi predpisoval samostojen sistem upravljanja, temveč je bolj v pomoč organizaciji pri integraciji sistema upravljanja tveganj v vsesplošen sistem upravljanja neke organizacije.

2.4.1 Pooblastila in obveznosti

Za vzpostavitev upravljanja tveganj in za zagotavljanje stalne učinkovitosti tega upravljanja so potrebna trdna in trajna prizadevanja vodstva organizacije kot tudi strateško in dosledno načrtovanje za doseganje zavezanosti na vseh ravneh organizacije. Vodstvo organizacije naj bi:

1. definiralo in podpiralo politiko upravljanja tveganj;
2. zagotovilo, da je politika upravljanja tveganj v sozvočju z organizacijsko kulturo;
3. določilo kazalnike uspešnosti upravljanja tveganj, ki so v sozvočju s kazalniki uspešnosti organizacije;
4. uskladilo cilje upravljanja tveganj s cilji in strategijami organizacije;
5. zagotovilo skladnost z zakoni;
6. dodelilo pooblastila in odgovornosti na vseh ravneh organizacije;
7. zagotovilo potrebna sredstva za upravljanje tveganj;
8. izmenjevalo informacije o novostih, idejah in prednostih obvladovanja tveganj z vsemi deležniki; in
9. zagotovljalo primernost in učinkovitost okvira za upravljanje tveganj.

2.4.2 Oblikovanje okvira za upravljanje tveganj

Razumevanje organizacije in njenega konteksta

Še pred začetkom načrtovanja in implementacijo okvira za upravljanje tveganj je pomembno oceniti in razumeti notranji in zunanji kontekst, v katerem organizacija živi. Oboje lahko pomembno vpliva na oblikovanje okvira.

Ocenjevanje organizacijskega zunanjega konteksta lahko vključuje, ni pa nujno omejeno na:

1. socialno in kulturno, politično, pravno, finančno, tehnološko, ekonomično, naravno in konkurenčno okolje, bodisi internacionalno, nacionalno, regionalno ali lokalno okolje;
2. ključne dejavnike in trende, ki vplivajo na cilje organizacije; in

3. odnose z zunanjimi deležniki, njihovo dojemanje ter vrednote.

Ocenjevanje organizacijskega notranjega konteksta lahko vključuje, ni pa nujno omejeno na:

1. upravljanje, organizacijsko strukturo, vloge in odgovornosti;
2. politiko, cilje in strategije, ki so namenjene za doseganje le-teh;
3. zmogljivosti v smislu virov in znanja (kapital, čas, ljudje, procesi, sistemi in tehnologije);
4. informacijske sisteme, informacijske tokove in odločitvene procese (formalne in neformalne);
5. odnos z notranjimi deležniki, njihovo dojemanje ter vrednote;
6. organizacijsko kulturo;
7. standarde, navodila in modele, ki jih organizacija uporablja; ter
8. oblikovanje in razširitev pogodbenih odnosov.

Vzpostavitev politike upravljanja tveganj

Politika upravljanja tveganj mora jasno opredeliti cilje organizacije in njeno zavezanost k politiki upravljanja tveganj, ki običajno vključuje:

1. organizacijsko utemeljitev glede obvladovanja tveganj;
2. povezave med organizacijskimi cilji in politiko ter politiko upravljanja tveganj;
3. obveznosti in odgovornosti glede upravljanja tveganj;
4. način, ki ga organizacija uporablja pri reševanju navzkrižnih interesov;
5. prizadevanje za omogočanje potrebnih virov oziroma informacij tistim, ki so odgovorni za upravljanje tveganj;
6. definiranje načina, s katerim bo tveganje izmerjeno in sporočeno; ter
7. stremljenje k temu, da se bo politika upravljanja tveganj ves čas razvijala ter da bo ta politika vedno odgovorila na nek dogodek oziroma spremembo okoliščin.

Politiko obvladovanj tveganj je treba sporočati ustrezno.

Odgovornost

Organizacija mora zagotoviti odgovornost, potrebno avtoriteto in kompetence za upravljanje tveganj ter vzpostavitev in vzdrževanje procesa upravljanja tveganj. Vzpostavitev odgovornosti vključuje tudi ustrezne in učinkovite kontrole. Pri tem je med najpomembnejšimi:

1. identificiranje lastnikov tveganja, ki imajo odgovornost in ustrezno avtoriteto, potrebno pri obvladovanju tveganj;
2. identificiranje odgovornih za razvoj, izvedbo in trajnost okvira za upravljanje tveganj;
3. identificiranje vseh ostalih odgovornosti posameznikov v organizaciji, saj lahko to pomaga pri obvladovanju tveganj;
4. vzpostavitev meritev učinkovitosti ter zunanjih in/ali notranjih procesov poročanja; in
5. zagotavljanje ustrezne ravni priznavanja.

Integracija v vse procese organizacije

Integracija v procese organizacije mora biti izvedena tako, da je upravljanje tveganj ustrezno, učinkovito in uspešno. Upravljanje tveganj mora biti del posameznih procesov in ne sme biti od njih oddvojeno. Zlasti je treba upravljanje tveganj integrirati v razvoj politik, v poslovno in strateško načrtovanje in pregled, ter v postopke uvajanja sprememb.

Potreben je načrt za upravljanje tveganj celotne organizacije, da se zagotovi, da se politika upravljanja tveganj izvaja in je vgrajena v vse postopke in procese organizacije. Načrt za upravljanje tveganj se lahko vključi v druge organizacijske načrte podobno kot strateški načrt.

Sredstva

Organizacija mora zagotoviti potrebna sredstva za upravljanje tveganj. Med temi sredstvi so:

1. ljudje, znanje, veščine, izkušnje in kompetence;
2. sredstva, potrebna za vsak korak v procesu upravljanja tveganj;

3. postopki, orodja in metode organizacije, ki se uporabljajo za upravljanje tveganj;
4. dokumentirani procesi in postopki;
5. informacijski sistemi in sistemi za upravljanje znanja; ter
6. programi izobraževanj oziroma usposabljanj.

Vzpostavitev sistema notranje komunikacije in mehanizmov poročanja

Organizacija bi morala v podporo in povečanje odgovornosti ter lastništva tveganja vzpostaviti notranje komuniciranje in poročevalne mehanizme. Ti mehanizmi naj bi zagotavljali, da:

1. so glavne komponente okvira upravljanja tveganj in vse nadaljnje modifikacije tega okvira ustrezno posredovane;
2. obstaja ustrezno notranje poročanje glede okvira, predvsem glede njegove učinkovitosti in rezultatov;
3. so vse relevantne informacije, ki izhajajo iz upravljanja tevganj, na voljo na primernem nivoju in pravočasno; ter da
4. so vzpostavljeni procesi za posvetovanje z notranjimi deležniki.

Ti mehanizmi bi morali, kjer je to primerno, vključevati procese za utrditev informacij glede tveganj, ki prihajajo iz različnih virov, ter po potrebi obravnavati njihovo občutljivost.

Vzpostavitev sistema zunanje komunikacije in mehanizmov poročanja

Organizacija bi morala razviti in implementirati načrt, kako bo komunicirala z zunanjimi deležniki. To vključuje:

1. vključevanje primernih zunanjih deležnikov in zagotavljanje učinkovite izmenjave informacij;
2. zunanje poročanje v skladu z zakonskimi in regulativnimi zahtevami;
3. zagotavljanje povratnih informacij in poročanje o komunikaciji in posvetovanju;
4. uporabljanje komunikacije za izgradnjo zaupanja v organizaciji; in

5. komuniciranje z deležniki v primeru nepredvidene krize.

Ti mehanizmi bi morali, kjer je to primerno, vključevati procese za utrditev informacij glede tveganj, ki prihajajo iz različnih virov, ter po potrebi obravnavati njihovo občutljivost.

2.4.3 Implementacija upravljanja tveganj

Implementacija okvira upravljanja tveganj Implementacja okvira za upravljanje tveganj pomeni, da mora organizacija predvsem:

1. določiti pravilen rok in strategijo za izvedbo;
2. uporabjati politiko in proces upravljanja tveganj vzporedno s procesi organizacije;
3. izpolniti zakonske in regulativne zahteve;
4. zagotoviti, da so odločitve, vključno z razvojem in določanjem ciljev, usklajene z rezultati procesov upravljanja tveganj;
5. imeti informacije in zagotavljati izobraževanja in usposabljanja; ter
6. razpravljati in se posvetovati z deležniki, da ostane okvir upravljanja tveganj primeren.

Implementacija procesa upravljanja tveganj

Upravljanje tveganj je potrebno izvesti z zagotovilom, da se proces upravljanja tveganj uresničuje preko načrta za upravljanje tveganj na vseh ustreznih ravneh in funkcijah organizacije kot del njenih standardnih postopkov in procesov. Proces bo podrobneje opisan v naslednjem razdelku.

2.4.4 Spremljanje in pregled okvira

Za zagotavljanje učinkovitega upravljanja tveganj, ki vseskozi prispeva k učinkovitosti organizacije, je potrebno spremljanje in pregled okvira. V ta namen mora organizacija:

1. meriti prisotnost upravljanja tveganj s pomočjo kazalnikov ter redno pregledovati njihovo ustreznost;

2. redno meriti napredek v smislu približevanja ali odklona od načrta upravljanja tveganj;

3. redno pregledovati, ali so okvir upravljanja tveganj, politika in načrt še vedno ustrezni glede na zunanji in notranji kontekst organizacije;

4. poročati o tveganjih, napredku glede uresničevanja načrta upravljanja tveganj ter o tem, kako dosledno se politika upravljanja tveganj zpolnjuje; in

5. pregledati učinkovitost okvira upravljanja tveganj.

2.4.5 Nenehno izboljševanje okvira

Rezultat spremljanja in pregledovanja okvira je stalno izboljševanje okvira, politik in načrta upravljanja tveganj. Odločitve glede tega se izvajajo zato, da se upravljanje tveganj organizacije izboljšuje, prav tako pa tudi njena kultura upravljanja tveganj.

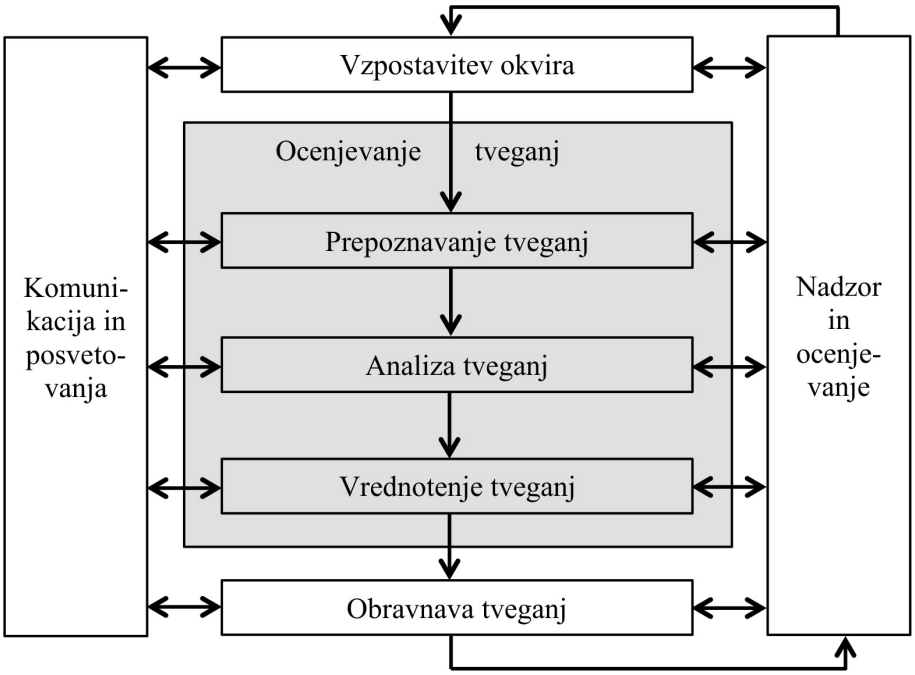
2.5 Proces

Proces sestavljajo aktivnosti, ki jih prikazuje slika 2.3. Za proces veljajo naslednje tri splošne usmeritve, ki jih moramo upoštevati pri vseh aktivnostih procesa. Te usmeritve so:

1. Upravljanje tveganj mora biti sestavni del upravljanja organizacije. To pomeni, da tveganja ne zahtevajo niti ne smejo biti posebni del upravljanja, s katerim se poslovodstvo ukvarja ob posebnih priložnostih (na primer enkrat letno).

2. Upravljanje tveganj mora biti del vsesplošne kulture v organizaciji in v praksah, ki se dnevno izvajajo. Seveda pa je prejšnja alineja predpogoj za doseganje te usmeritve.

3. Ker je vsaka organizacija posebna in unikatna, in ker se s časom vsaka organizacija tudi spreminja, je potrebno upravljanje tveganj prilagoditi posebnostim organizacije in ga s časom tudi dodatno dopolnjevati ali kako drugače spreminjati.



Slika 2.3: Aktivnosti procesa upravljanja tveganj in njihove medsebojne relacije

2.5.1 Komunikacija in posvetovanje

Ker sta komunikacija in posvetovanje z notranjimi in zunanjimi deležniki organizacije nujno potrebnI aktivnosti skozi celoten proces upravljanja tveganj, je potrebno razviti načrte za te aktivnosti in vzpostaviti mehanizme za delo v skladu s temi načrti že povsem na začetku. Posvetovalni timski pristop lahko pomaga:

1. vzpostaviti ustrezen okvir;
2. zagotoviti, da so interesi razumljeni in upoštevani;
3. pripeljati strokovnjake za analizo tveganj;
4. zagotoviti različne poglede, katere je potrebno ustrezno razumeti;
5. zagotoviti potrditev in podporo; ter
6. izboljšati ustrezno uvajanje sprememb v proces upravljanja tveganj.

Komunikacija je pomembna, saj se tako presojajo možnosti tveganj glede na njihovo percepcijo. Te zaznave pa so lahko različne in odvisne od vrednot, potreb, predpostavk,

konceptov itd. deležnikov. Ker imajo njihova stališča pomemben vpliv na odločitve, morajo biti vse te zaznave deležnikov prepoznane, evidentirane ter upoštevane pri procesu odločanja.

2.5.2 Vzpostavitev okvira

Z vzpostavitvijo okvira organizacija artikulira svoje cilje, definira notranje in zunanje parametre, ki jih je potrebno upoštevati med upravljanjem tveganj, ter definira obseg in kriterije za preostali del procesa upravljanja tveganj. Pri tem ločimo med vzpostavitvijo notranjega in zunanjega okvira ter vzpostavitvijo okvira za sam proces upravljanja tveganj.

Zunanji kontekst predstavlja zunanje okolje, v katerem organizacija skuša dosegati svoje cilje. Ta kontekst je pomemben zato, da lahko upoštevamo cilje zunanjih deležnikov pri razvoju kriterijev za tveganja. Temelji na kontekstu celotne organizacije, vendar s posebnimi podrobnostmi glede zakonskih in regulativnih zahtev, dojemanjem deležnikov in drugih vidikov tveganj, ki so značilna za področje procesa upravljanja tveganj. Vsebuje pa lahko:

1. socialno, kulturno, politično, finančno, tehnološko, ekonomsko in naravno okolje, bodisi internacionalno, nacionalno, regionalno ali lokalno okolje;
2. ključne dejavnike in trende, ki vplivajo na cilje organizacije; ter
3. odnose z zunanjimi deležniki, njihovo dojemanje ter vrednote.

Po drugi strani notranji kontekst predstavlja notranje okolje, v katerem organizacija skuša dosegati svoje cilje. Proces upravljanja tveganj mora biti skladen s kulturo organizacije, ostalimi procesi, strukturo in strategijo. Notranji kontekst je vse tisto znotraj organizacije, kar vpliva na način upravljanja tveganj. Vzpostaviti ga je potrebno ker:

1. upravljanje tveganja poteka v okviru ciljev organizacije;
2. je potrebno cilje in merila določenega projekta, procesa ali dejavnosti obravnavati v luči ciljev organizacije kot celote; in ker
3. nekatere organizacije ne morejo prepoznati priložnosti, da dosežejo svoje strateške, projektne ali poslovne cilje, kar vpliva na organizacijsko pripadnost, verodostojnost, zaupanje in vrednost.

Notranji kontekst je potrebno razumeti, to razumevanje pa lahko vključuje:

1. upravljanje, organizacijske strukture, vloge in odgovornosti;
2. usmeritve, cilje in strategije, ki so na voljo za njihovo doseganje;
3. zmogljivosti v smislu virov in znanja (npr. kapitala, časa, ljudi, procesov, sistemov in tehnologij);
4. odnos z notranjimi deležniki, njihovo dojemanje ter vrednote;
5. organizacijsko kulturo;
6. informacijske sisteme, informacijske tokove in odločitvene procese (formalne in neformalne);
7. standarde, navodila in modele, ki jih organizacija uporablja; ter
8. oblikovanje in razširitev pogodbenih odnosov.

Vzpostaviti oziroma določiti je potrebno cilje, strategije, področja uporabe in parametre dejavnosti organizacije, ali tiste dele organizacije, kjer se uporablja postopek upravljanja tveganja. Upravljanje tveganj je treba opraviti na način, da bi upravičili sredstva, ki so namenjena upravljanju tveganj. Prav tako je potrebno opredeliti sredstva, odgovornosti in pooblastila ter evidence, ki se vodijo.

Kontekst procesa upravljanja tveganj se lahko tudi spremeni glede na potrebe organizacije. Ta sprememba lahko vključuje:

1. opredelitev ciljev in dejavnosti upravljanja tveganj;
2. opredelitev odgovornosti v procesu upravljanja tveganj;
3. opredelitvi področja, kot tudi obseg aktivnosti za upravljanje tveganj, ki se izvajajo;
4. opredelitev dejavnosti, procesa, funkcije, projekta, izdelka, storitve ali sredstev v smislu časa in lokacije;
5. opredelitev odnosov med konkretnimi projekti, procesi ali dejavnostmi in drugimi projekti, procesi ali dejavnostmi organizacije;
6. opredelitev metodologij za oceno tveganja;
7. opredelitev načinov ocenjevanja uspešnosti in učinkovitosti znotraj upravljanja tveganja;

8. prepoznavanje in določanje odločitev, ki jih je potrebno sprejeti; ter
9. ugotavljanje potreb po študijah, določanje njihovega obsega in ciljev ter sredstev, potrebnih za takšne študije.

Organizacija mora definirati tudi kriterije, ki jih uporabljamo pri ovrednotenju pomembnosti posameznih tveganj. Ti kriteriji odsevajo vrednostne sisteme, cilje in vire neke organizacije. Nekateri od teh kriterijev so lahko pridobljeni na osnovi zakonskih, drugih regulativih in pogodbenih zahtev. Kriteriji tveganja bi morali biti v skladu s politiko upravljanja tveganj v organizaciji, opredeljeni na začetku vsakega procesa upravljanja tveganj ter jih je potrebno nenehno pregledovati. Pri določanju kriterijev tveganj, je treba upoštevati dejavnike, ki vključujejo:

1. naravo in vrsto vzrokov ter posledic, ki se lahko pojavijo, in način, kako se merijo;
2. inforamcijo, kako bo definirana verjetnost;
3. časovni(e) rok/e verjetnosti in/ali posledica(e);
4. informacijo, kako naj bo določena stopnja tveganja,
5. stališča deležnikov;
6. raven, do katere je tveganje sprejemljivo oziroma dopustno; ter
7. informacijo, ali je potrebno upoštevati kombinacije različnih tveganj, in če je tako, kako in katere kombinacije je potrebno upoštevati.

2.5.3 Ocenjevanje tveganj

Aktivnost ocenjevanja tveganj predstavlja srčiko upravljanja tveganj in predstavlja skupno ime za aktivnosti prepoznavanja, analizo in vrednotenje tveganj.

Pri ocenjevanju tveganj skušamo med drugim odgovoriti na naslednja temeljna vprašanja, ki se zastavljajo v zvezi tveganj:

1. Kaj se lahko zgodi in zakaj?
2. Kakšne so posledice?
3. Kakšna je verjetnost, da se tveganje pojavi v prihodnosti?
4. Ali obstajajo kakšni dejavniki, ki omogočajo, da se nekemu tveganju izognemo ali da zmanjšamo verjetnost, da se sploh pojavi?

2.5.4 Prepoznavanje/identificiranje tveganj

Organizacija mora opredeliti vire tveganj, področja vplivov, dogodke, ki so posledica nekega pojava ali spremembe določenega položaja, z vzroki in s potencialnimi posledicami, ki se lahko s časom tudi spreminjajo. Osnovni namen te aktivnosti (ali koraka v procesu) je ustvariti celovit seznam tveganj, ki bazira na tistih dogodkih, ki lahko ustvarijo, povečajo, onemogočijo, zmanjšajo, pospešijo ali upočasnijo doseganje ciljev. Celovito prepoznavanje je kritično, saj tveganje, ki ni identificirano v tem koraku, ne bo del nadaljnje analize. Zajeta morajo biti tudi tista tveganja, katerih vzrok ni nujno pod kontrolo organizacije, ali pa sploh ni znan. Upoštevati je potrebno tudi posebne učinke posledic (kumulativni učinki in kaskade) ter najrazličnejše možne vzroke in posledice, s pomočjo katerih se nato oblikujejo možni scenariji. Pri prepoznavanju tveganj si mora organizacija pomagati z različnimi orodji in tehnikami, vključene pa morajo biti tudi ustrezne podporne informacije ter ljudje z ustreznim znanjem.

2.5.5 Analiza tveganj

Pri analizi tveganj razvijemo razumevanje tveganja. Ta aktivnost je pogoj za vrednotenje tveganj in za odločitev o tem, ali naj se s tveganjem sploh ukvarjamo, in če se naj, katere najustreznejše strategije in metode bi bile primerne. Prav tako je ta aktivnost pogoj za odločanje o tem, kje v organizaciji se je potrebno posvetiti tveganjem in katere opcije (viri, področja vplivov, dogodki, posledice, itd.) vsebujejo različne vrste tveganj ter na kakšnem nivoju (poslovnem, tehničnem, itd.) je neko tveganje.

Pri analizi ugotavljamo vzroke in izvore tveganj, pozitivne in negativne posledice ter možnosti, da se zgodijo posledice (ponavadi predstavljene z verjetnostjo za dogodek). Iščemo faktorje, ki vplivajo na posledice, in možnosti za posledice. Upoštevamo, da lahko ima nek dogodek množico posledic, ki lahko vplivajo na množico ciljev organizacije. Upoštevamo pa tudi obstoječe kontrole in njihovo učinkovitost oziroma uspešnost.

S pomočjo načina, s katerim so posledice in verjetnosti izražene, in s pomočjo načina, ki določa stopnjo tveganja, se določi vrsta tveganja, informacije, ki so na voljo, ter namen, za katerega je rezultat ocenjevanja tveganja uporabljen. Vse pa mora biti v skladu s kriteriji tveganj.

Pri analizi tveganj je mogoče uporabiti različne stopnje podrobnosti, odvisno od tveganja, namena analize, ter informacij, podatkov in virov, ki so na voljo. Analiza je lahko kvalitativna, delno kvantitativna ali delno kvantitativna, ali pa kombinacija obeh načinov – odvisno od okoliščin.

Posledice in njihova verjetnost se lahko določijo z modeliranjem rezultatov dogodka ali niza dogodkov, z ekstrapolacijo iz eksperimentalnih študij, ali z analizo razpoložljivih podatkov. Posledice se lahko izrazi v smislu materialnih in nematerialnih učinkov. Lahko so izražene z večimi numeričnimi vrednostmi ali opisi, za različne čase, prostore, skupine in situacije.

2.5.6 Vrednotenje tveganj

Namen vrednotenja je pomoč pri sprejemanju odločitev. Temelji na analizi tveganj glede prioritet ravnanja s tveganji. Pri tem posamezno tveganje primerjamo s kriteriji sprejemljivosti, ki smo jih določili v aktivnosti vzpostavitve okvira, na podlagi rezultatov primerjave pa se nato določi način obravnave tveganja, ki mora biti v skladu z zakonskimi, regulativnimi in drugimi zahtevami.

V nekaterih primerih lahko ocena tveganja vodi v odločitev, da je potrebna dodatna analiza, ali pa v odločitev, da se tveganje obravnava samo zato, da se obdržijo obstoječe kontrole. Seveda pa je to odvisno od odnosa organizacije do tveganja ter kriterijev tveganj.

2.5.7 Obravnava tveganj

V okviru obravnave tveganj (v dobesednem prevodu bi lahko rekli tudi v „okviru zdravljenja tveganj") izbiramo eno ali več možnosti za spreminjanje tveganj in te možnosti tudi implementiramo. Po implementaciji obravnave tveganj zagotovimo ali spremenimo kontrole.

Sama aktivnost vsebuje manjši cikličen proces, ki zajema:

1. ocenjevanje tveganja;
2. odločanje o sprejemljivosti preostalega (residual risk) tveganja;
3. ponovno obravnavavo tveganja, če preostanek ni sprejemljiv; in
4. ocenjevanje uspešnosti te obravnave.

Možnosti obravnave tveganj niso nujno medsebojno izključujoče ali ustrezne v vseh okoliščinah. Možnosti so lahko:

1. izogibati se tveganjem tako, da se organizacija odloči, da ne začne ali ne nadaljuje aktivnosti, ki bi povečala to tveganje;

2. tveganje sprejeti ali celo povečati, da bi izkoristili priložnost;

3. odstraniti vzrok tveganja;

4. spremeniti verjetnost;

5. spremeniti posledice;

6. deliti tveganje s partnerjem/i (pogodbe, finančna tveganja); ter

7. ohranjati tveganje na premišljen način s premišljenimi odločitvami.

Pri izbiri najustreznejših možnosti za obravnavo tveganj tehtamo med vloženimi stroški in napori glede na koristi, upoštevaje zakonske in druge predpise, kot so družbena odgovornost in varstvo okolja. Odločitev je odvisna tudi od tega, ali je obravnava finančno upravičena, kot je to v primeru visoke stopnje negativne/ih posledic(e) z nizko verjetnostjo pojava dogodka.

Med obravnavo se osredotočimo tako na posamezno možnost, kakor tudi na kombinacijo različnih možnosti, pri čemer lahko ima organizacija veliko koristi.

Pri izbiri možnosti obravnave tveganja, mora organizacija upoštevati vrednote in dojemanje deležnikov in najprimernejše načine za komunikacijo z njimi. Tu gre predvsem za diskusijo glede tega, kako lahko možnosti obravnave tveganja vplivajo na druga tveganja v organizaciji ali z deležniki. Nekatere obravnave tveganj so namreč lahko bolj sprejemljive za nekatere deležnike kot za druge.

V načrtu obravnave je potrebno jasno opredeliti prednostni vrstni red, v katerem naj bi se izvajale posamezne obravnave tveganj.

Obravnava tveganj sama po sebi vsebuje tveganja. Eno najpomembnejših tveganj je tveganje, da sprejmemo neučinkovite ukrepe, ali da ti odpovedo. Zato je potrebno obravnavo tveganj stalno spremljati in pregledovati, da na ta način zagotavimo učinkovitost ukrepov.

Obravnava tveganj lahko privede do sekundarnih tveganj, ki jih je treba oceniti, obravnavati, spremljati in pregledovati. Ta sekundarna tveganja je treba vključiti v isti načrt obravnave kot primarno tveganje in se ne obravnavajo kot nova tveganja, pri tem pa mora biti povezava med primarnim in sekundarnim tveganjem jasna in trajna.

Namen načrtovanja obravnave tveganj je dokumentirati, kako bo posamezna izbrana možnost obravnave izvedena. Informacije, navedene v načrtu obravnave, morajo vsebovati:

1. razlog izbora možnosti, vključno s pričakovanimi koristmi, ki jih prinaša ta možnost;
2. imena odgovornih za odobritev načrta, in imena odgovornih za njegovo izvedbo;
3. predlagane ukrepe;
4. zahteve za potrebne vire, vključno z nepredvidenimi;
5. merila za učinkovitost ukrepov ter omejitve;
6. zahteve glede poročanja in spremljanja; ter
7. roke in urnik.

Načrte obravnave tveganj bi bilo potrebno vključiti v procese upravljanja organizacije in glede njih tudi razpravljati z ustreznimi deležniki.

Odločevalci in drugi deležniki pa morajo biti seznanjeni tudi z naravo in obsegom preostalega tveganja, ki ostane kljub obravnavi tveganja. Preostalo tveganje je treba dokumentirati in nadzorovati, pregledati in po potrebi ponovno obravnavati.

2.5.8 Spremljanje in pregledovanje

Oba, nadzor in pregled, morata biti del načrta upravljanja tveganj, ki mora vsebovati redne in naključne preglede ali spremljanje. Pri tem so zelo pomembne jasno določene odgovornosti.

Procesi spremljanja in pregledovanja bi morali vključevati vse vidike upravljanja tveganj zato, da:

1. se zagotovi, da so kontrole učinkovite in uspešne tako pri zasnovi kot v izvedbi;
2. pridobivanju dodatnih informacij za izboljšanje ocene tveganja;
3. organizacija analizira in pridobiva izkušnje na podlagi dogodkov (vključno s tistimi, ki so se skoraj zgodili), sprememb, trendov, uspehov in napak;
4. se zaznajo spremembe v notranjem in zunanjem kontekstu, vključno s spremembami kriterija tveganj in tveganja samega, kar lahko zahteva revizijo obravnave tveganj in zastavljenih prioritet; ter da
5. se ugotavijo nastajajoča tveganja.

Napredek pri izvajanju načrtov za obravnavo tveganj omogoča merjenje uspešnosti. Rezultate spremljanja in pregledovanja je potrebno zabeležiti/evidentirati, nato pa o njih poročati ustreznim notranjim in zunanjim javnostim, prav tako pa jih je potrebno uporabiti pri pregledu okvira upravljanja tveganj.

2.5.9 Evidentiranje v procesu upravljanja tveganj

Aktivnosti upravljanja tveganj morajo biti sledljive. V procesu upravljanja tveganj evidence zagotavljajo temelje za izboljšanje metod in orodij, kot tudi v celotnem procesu.

Odločitve glede oblikovanja evidenc so povezane s/z:

1. potrebami organizacije po nenehnem učenju;
2. ugodnostmi, ki jih ponuja ponovna uporaba informacij za namene upravljanja;
3. stroški in prizadevanji, nastalimi pri ustvarjanju in vzdrževanju evidenc;
4. zakonskimi, regulativnimi in operativnimi potrebami po evidencah;
5. načini dostopa, dostopnostjo in enostavnostjo medija za hrambo;
6. obdobjem hrambe; ter
7. občutljivostjo informacij.

Poglavje 3

Nekateri drugi standardi povezani z upravljanjem tveganj

3.1 ISO 31010:2009

ISO/IEC 31010:2009 [8] podpira standard ISO 31000 in daje napotke o izbiri in uporabi sistematičnih metod za oceno tveganja, postopek ocenjevanja tveganja in izbiro metode za oceno tveganja.

Nastal je kot plod sodelovanja med organizacijama ISO in IEC in podpira standard ISO 31000 v tistem delu, ko se le ta ukvarja z ocenjevanjem tveganj. Ocena tveganja je sestavni del upravljanja tveganj, ki zagotavlja organizacijam strukturiran proces za identifikacijo vplivov pri doseganju ciljev organizacije.

Ocenjevanje tveganja zagotavlja boljše razumevanje tveganj in omogoča boljše vedenje o ustreznosti in učinkovitosti obstoječega nadzora nad tveganji. Standard je podlaga za odločanje o najustreznejšem pristopu za obvladovanje posameznega tveganja. Je v pomoč pri implementaciji principov obvladovanja tveganj, ki jih podaja ISO 31000. Podrobno podaja:

1. koncepte ocenjevanja tveganj,
2. proces ocenjevanja tveganja in
3. izbiro tehnike za ocenjevanje tveganj.

S tem standard povzema obstoječe dobre prakse in odgovarja na naslednja vprašanja:

1. Kaj se lahko zgodi in zakaj?
2. Kakšne so posledice?
3. Kakšna je verjetnost njihovega nastanka v bodoče?
4. Ali obstajajo kakršni koli dejavniki, ki lahko ublažijo posledice tveganja ali zmanjšajo verjetnost za tveganje?

Standard sestavlja šest poglavij in dva izčrpna dodatka – vsega skupaj 90 strani.

Po uvodnih kratkih poglavjih, ki opisujejo dokument, obrazložijo povezave z drugimi dokumenti in definirajo v standardu uporabljene termine, sledijo tri osrednja poglavja, ki podrobno definirajo aktivnost ocenjevanja tveganja. Ta tri poglavja obravnavajo koncepte ocenjevanja, samo ocenjevanje in izbiro tehnike za ocenjevanje tveganj. Sledi prvi dodatek, ki vsebuje primerjave enaintridesetih različnih tehnik, ki jih lahko uporabimo pri ocenjevanju tveganj, in drugi dodatek, ki te tehnike tudi na kratko predstavi in podaja reference za nadaljnji študij le teh.

Četrto poglavje ISO 31010 podrobneje predstavlja koncepte, ki naj bi jih upoštevali pri obravnavi tveganj (kar ne smemo zamenjevati s principi, ki jih opisuje ISO 31000). Ti koncepti predstavljajo zelo poučen seznam dejstev, ki jih je pri ocenjevanju smiselno upoštevati. Zapisani so v podpoglavjih, ki govorijo o:

1. namenu in prednostih ocenjevanja,
2. vlogi in pomenu ocenjevanja glede na okvir za upravljanje tveganj, ter
3. vlogi in pomenu ocenjevanja v procesu upravljanja tveganj, kjer je ta pomen posebej izpostavljen v luči izmenjave mnenj in komuniciranja, vzpostavitve okvirja za upravljanje tveganj, samega procesa ocenjevanja tveganj, obravnave tveganj in seveda nadzora ter ocenjevanja.

Pri tem ISO 31010 ne ponavlja, temveč smiselno nadgrajuje zapisano v ISO 31000.

Peto poglavje podrobneje opisuje proces ocenjevanja. Pri tem ne samo, da podrobneje nadgrajuje vse zapisano o procesu v ISO 31000, temveč za vse aktivnosti tudi podaja predloge za uporabo posameznih tehnik iz nabora enaintridesetih, ki jih podajata oba dodatka.

Šesto poglavje opisuje, kako je mogoče izbrati ustrezno tehniko pri ocenjevanju tveganj. Pri tem opozarja, da je večkrat potrebno izbrati več teh tehnik ali metod, saj je posamezna namenjena ali pa je v danem primeru ustrezna samo eni ali več aktivnostim

procesa ocenjevanja, vendar ne vsem. Pri tem poglobljeno v posameznih podpoglavjih opisuje področja znanj, ki jih je potrebno pri uporabi tehnik upoštevati. Ta področja so: izbira tehnike, razpoložljivost virov, ki vplivajo na izbiro tehnike in kompleksnost tehnike. Obstajajo še tri podpoglavja, ki govorijo o naravi in lastnostih negotovosti, ki je sestavni del tveganj, o uporabi ocenjevanja tveganj v življenjskih procesih (predvsem projektov) ter o mogočih klasifikacijah tehnik za ocenjevanje tveganj. Kratki povzetki nekaterih podpoglavij sledijo v nadaljevanju.

V dodatku A so navedeni nekateri atributi posameznih metod, kot so zahtevana sredstva, stopnja negotovosti, kompleksnost in zmožnost podajanja kvantitativnega rezultata pri oceni tveganja.

3.1.1 Izbira tehnike

Ocenjevanje tveganj se lahko izvaja z različnimi zahtevnostmi glede podrobnosti ocenjevanja in tako uporablja eno ali več metod, ki se razlikujejo po svoji kompleksnosti. Rezultat ocenjevanja ima lahko različne oblike, ki morajo biti v skladu s kriteriji, ki smo jih postavili v aktivnosti „Vzpostavitev okvirja". Pri tem si pomagamo z vrednotenjem posameznih metod po kriterijih, ki jih prikazuje slika 3.1. Slika prikazuje izsek tabele iz dodatka A standarda ISO 31010, kjer so posamezne metode ovrednotene glede na uporabnost v posameznih aktivnostih procesa ocenjevanja tveganj.

3.1.2 Razpoložljivost virov

Viri in zmožnosti, ki lahko vplivajo na izbiro tehnike ocenjevanja, vsebujejo:

1. spretnosti, izkušnje in zmožnosti skupine, ki ocenjuje tveganje;
2. časovne in ostale omejitve, ki so pogojene s samo organizacijo, ki ocenjuje tveganja; ter
3. finančne okvire, ki so na voljo v primeru, da so potrebni zunanji viri.

3.1.3 Narava in stopnja negotovosti

Oboje, narava in stopnja negotovosti zahtevata razumevanje kvalitete, količine in celovitosti informacij o posameznih tveganjih. To vsebuje tudi zavedanje o pomanjkanju informacij o tveganjih samih, njihovih virih in vzrokih ter posledicah, ki jih imajo za

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13

Legenda slike:
SA - Zelo uporabno
A - Uporabno
NA - Neuporabno

Slika 3.1: Uporabnost posameznih metod pri ocenjevanju tveganj (izsek iz ISO 31010)

doseganje ciljev organizacije. Negotovost lahko izhaja iz slabih podatkov ali iz pomanjkanja pomembnih in zaupanja vrednih podatkov. Negotovost je lahko prisotna tudi v eksternem ali internem kontekstu organizacije. Nekateri podatki na osnovi zgodovine niso dosegljivi ali jih ni mogoče pravilno interpretirati. Vse to zahteva razumevanje tipa in narave negotovosti, kar je potrebno posredovati vsem odločevalcem v organizaciji.

3.1.4 Kompleksnost

Kompleksnost je naslednji izziv pri obravnavi tveganj. Nekatera tveganja so kompleksna sama po sebi, nekatera pa enostavna, vendar je medsebojna interakcija med posameznimi (lahko tudi zelo enostavnimi) tveganji zelo kompleksen pojav, ki ga nikakor ne smemo zanemariti, čeprav bi lahko rekli, da je vsako posamezno tveganje zanemarljivo.

3.2 ISO/IEC 27005:2011

Za izvedbo učinkovitega sistema upravljanja varnosti morajo organizacije poskrbeti za sistematično upravljanje tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem, v katerem organizacija deluje. Navsezadnje mora biti upravljanje posameznih (operativnih, IT, tečajnih, itd) tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje tveganj na področjih, kjer in kadar je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Standard ISO/IEC 27005:2011 (ISO/IEC 27005:2011; Information technology – Security techniques – Information security risk management, International organization for Standardization) [10] je standard, ki opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov. Za razliko od prejšnje različice, ki je nosila oznako ISO/IEC 27005:2008, opisani v članku [21], je standard v tej različici sinhroniziran z zgoraj opisanim standardom ISO 31000. Tako je najnovejši ISO/IEC 27005 primer uporabe ali impelmentacije ISO 31000.

Opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov, ki jih podaja ISO/IEC 27001:2013 [11]. ISO/IEC 27001:2013 sicer določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema vodenja varovanja informacij v okviru organizacije. To vključuje tudi zahteve za ocenjevanje in obravnavo informacijskih tveganj prilagojeno potrebam organizacije. Vendar ISO 27001 ni predmet te knjige, ker je področje tveganj,

ki ga opisuje, že pokrito s standadi ISO 31000, ISO 31010 in ISO 27005.

Proces upravljanja tveganj, ki jih predvideva ISO 27005, je mogoče uporabiti pri:

1. celotni organizaciji ali samo v enem od njenih delov (kot je oddelek, fizična lokacija ali celo storitev);
2. katerem koli informacijskem sistemu; in
3. pri obstoječih, planiranih ali pri posameznih vrstah kontrol v organizaciji (na primer pri načrtovanju neprekinjenega poslovanja).

Upravljanje informacijskih tveganj zajema opravila, ki med drugim zajemajo:

1. prepoznavanje tveganj;
2. ocenjevanje tveganj prek vplivov na poslovanje podjetja in morebitne verjetnosti, da se pojavijo;
3. komuniciranje in razumevanje verjetnosti za tveganja in posledice tveganj;
4. vzpostavitev prioritetnega vrstnega reda ukvarjanja s tveganji;
5. vzpostavitev vrstnega reda akcij za zmanjševanje tveganj;
6. vključevanje vseh deležnikov organizacije v odločanje o upravljanju tveganj in o stalnem informiranju o stanju glede tveganj;
7. učinkovit nadzor in spremljanje tveganj in samega upravljanja tveganj;
8. zajemanje informacij, s katerimi lahko upravljanje tveganj izboljšujemo;
9. izobraževanje zaposlenih - še posebej vodij - glede tveganj in načinov za izogibanje tveganjem.

Seveda ISO/IEC predstavlja samo enega od pristopov k reševanju problematike ocenjevanja tveganj. Podaja splošna priporočila za analizo in ocenjevanje informacijskih tveganj tako, da ne predpisuje posamezne metode ali orodja, ki bi bilo primerno za uporabo v neki organizaciji.

ISO/IEC 27005 podaja splošen pregled aktivnosti za obvladovanje informacijskih tveganj pri varovanju informacij. Pri vsaki aktivnosti so opisane dejavnosti, ki so porazdeljene v naslednja področja:

1. Prispevek (Input): Določa vse potrebne informacije za izvedbo aktivnosti.

2. Ukrep (Action): Dejavnost opiše.

3. Navodila za vpeljavo (Implementation guidance): Navede smernice za izvedbo ukrepa. Pri tem standard opozarja, da nekatere od teh smernic niso primerne v vseh primerih in da imamo opraviti z izbiro smernic ali načinov za izvedbo ukrepa.

4. Rezultat (Output): Določa vse informacije, ki nastajajo po izvedbi aktivnosti.

Nekateri dodatni izkustveni napotki za obvladovanje tveganja pri varovanju informacij so predstavljeni v prilogah:

1. Priloga A. Podaja izkustvene napotke o določanju konteksta upravljanja informacijskih tveganj.

2. Priloga B. Na osnovi dobre prakse priporoča prepoznavanje in ocenjevanje sredstev.

3. Priloga C. Predstavlja primere tipičnih groženj.

4. Priloga D. Našteti so primeri tipičnih ranljivosti.

5. Priloga E. Gre za prilogo, ki opisuje primere pristopov ocenjevanja informacijskih tveganj. V tej prilogi je podana jasna razmejitev med ocenjevanjem tveganj na splošnem, to je višjem nivoju in med ocenjevanjem na podrobnejšem nivoju. Ocenjevanje tveganj je osrednji izziv vsakega upravljanja tveganj.

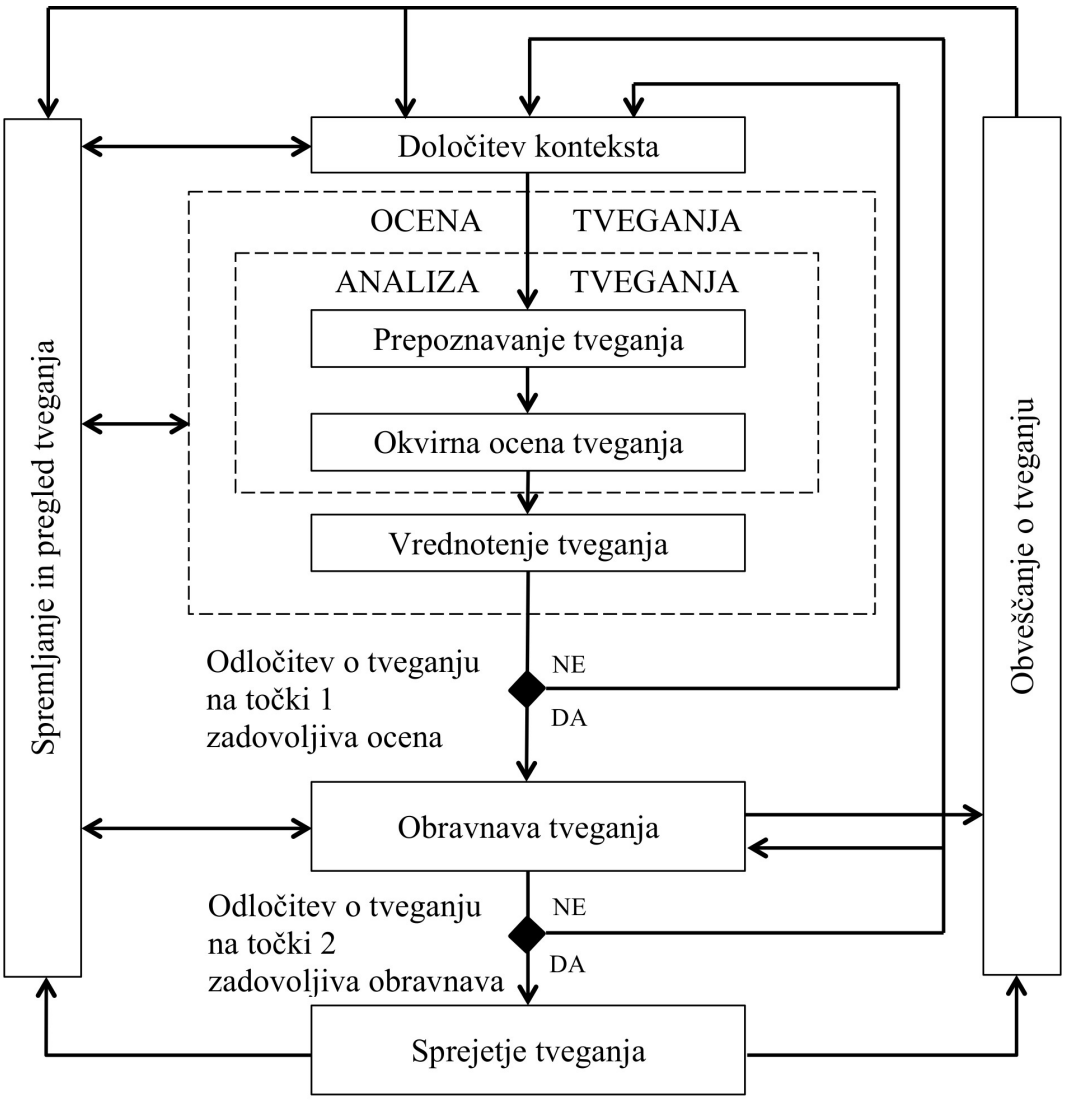
6. Priloga F. V tej prilogi je seznam splošnih omejitev za zmanjšanje tveganja, kot so časovne, tehnične, etične, okoljevarstvene in druge omejitve.

3.2.1 Proces upravljanja informacijskih tveganj

Proces je enak kot pri ISO 31000, ki je opisan zgoraj. Kljub temu, pa so tudi v najnovejši različici standarda ohranili bolj podrobno delitev procesa, kot ga prikazuje slika 3.2.

Pri sprejemanju tveganj moramo zagotoviti, da vodilni v organizaciji izrecno sprejmejo preostala tveganja. To pomeni, da sprejmejo vsa tveganja, ki niso bila predmet obravnave tveganj ali pa smo se pri obravnavi tveganj odločili, da jih v danem trenutku sprejmemo takšne, kot so.

Ker ISO 27001 predvideva cikel PDCA (Plan - Do - Check - Act) v okviru ISMS (Information Security Management System), je temu ciklu podvržen tudi ISO 27005. Spodnja tabela 3.1 povzema aktivnosti obvladovanja tveganja pri varovanju informacij.



Slika 3.2: Aktivnosti pri upravljanju informacijskih tveganj

Proces ISMS	Aktivnost pri procesu obvladovanja tveganja pri varovanju informacij
Načrtuj (Plan)	Določitev konteksta Ocena tveganja Razvoj načrta za obravnavo tveganja Sprejetje tveganja
Stori (Do)	Vpeljava načrta za obravnavo tveganja
Preveri (Check)	Stalno spremljanje in pregledovanje tveganj
Ukrepaj (Act)	Vzdrževanje in izboljševanje procesa obvladovanja tveganja pri varovanju informacij

Tabela 3.1: Prekrivanje ISMS po ISO 27001 (Information Security Management System) procesov z aktivnostmi procesa obvladovanja informacijskih tveganj

V nadaljevanju branja bo mogoče razbrati, da ISO/IEC 27005 sledi ISO 31000, vendar ni povsem identičen – gre za primer njegove uporabe. Prav tako v nadaljevanju ni v celoti opisan ISO/IEC 27005, temveč predvsem tisti, del, ki sledi ISO 31000.

3.2.2 Določitev konteksta

Pri določanju konteksta zberemo informacije o organizaciji, ki so relevantne za obvladovanje tveganj v okviru informacijske varnosti. Sem spada:

1. **Določanje osnovnih meril**, potrebnih za varnost pri upravljanju informacijskih tveganj. Izbrati je potrebno ustrezen pristop k obvladovanju tveganja ali ga razviti. Razviti in določiti je potrebno merila za vrednotenje:

   (a) tveganja, ki ogroža varnost informacij organizacije;

   (b) učinka v smislu stopnje škode ali stroškov za organizacijo, ki jih povzroči informacijski varnostni dogodek; ter

   (c) sprejetja tveganja, ki so pogosto odvisna od politike in ciljev organizacije ter interesov interesnih skupin.

   Merila za sprejetje tveganja se lahko razlikujejo glede na to, kako dolgo pričakujemo obstoj tveganja. Poleg tega mora organizacija oceniti, ali so na voljo ustrezna sredstva.

2. **Opredelitev področja uporabe in mej** vseh ustreznih sredstev, poslovnih ciljev, poslovnih procesov, strategij, pravnih in regulativnih zahtev, ki veljajo za organizacijo, ter vmesnikov. Področje uporabe procesa obvladovanja tveganja pri varovanju informacij mora biti opredeljeno za zagotovitev, da se pri oceni tveganja upoštevajo vsa sredstva. Poleg tega je treba določiti meje, da se lahko obravnavajo tveganja, ki lahko prestopijo meje. Informacije o organizaciji je treba zbrati za določitev okolja, v katerem deluje, in njegove pomembnosti pri procesih obvladovanja tveganja. Poleg tega mora organizacija utemeljiti vsako izključitev s področja uporabe.

3. **Organiziranje obvladovanja tveganja**, tj. vzpostavitev ustreznega delovanja zaposlenih v organizaciji na področju varnosti pri upravljanju informacijskih tveganj (vloge in odgovornosti). Takšno organiziranje mora odobriti vodstvo organizacije Bistveno je tudi, da določimo namen obvladovanja tveganja pri varovanju informacij, ker ta vpliva na celoten proces in zlasti na določitev konteksta.

3.2.3 Prepoznavanje tveganja

Namen prepoznavanje tveganja je, da določimo, kaj lahko povzroči potencialno izgubo ter kako, kje in zakaj lahko ta izguba nastane.

Sama aktivnost določa prepoznavanje sredstev, možnih groženj in šibkih točk, ki obstajajo (ali bi lahko obstajale) ter prepoznavanje že obstoječih kontrol, njihov vpliv na prepoznavanje tveganj in morebitne posledice. Prepoznavanje tveganja temelji na naslednjih opravilih:

1. **Prepoznavanje sredstev**. Prepoznavanje moramo izvesti tako podrobno, da zagotovimo dovolj informacij za oceno tveganja. Stopnja natančnosti vpliva na splošno količino informacij, zbranih med oceno tveganja. Stopnjo je mogoče v nadaljnjih ponovitvah ocene tveganja ponovno določiti kako drugače.

2. **Prepoznavanje groženj**. Opredeliti moramo splošne nevarnosti oz. grožnje in jih razvrstiti po tipu (npr. nedovoljene dejavnosti, materialna škoda in tehnične napake). Upoštevati je potrebno tudi interne izkušnje iz preteklih incidentov ter pretekle ocene nevarnosti. Pri obravnavi groženj moramo upoštevati še vidike okolja in kulture.

3. **Prepoznavanje obstoječih kontrol**. Znova moramo identificirati in preveriti obstoječe kontrole z namenom zagotavljanja njihovega pravilnega delovanja. Kon-

trole, katerih vpeljava se načrtuje v skladu z načrti za vpeljavo obravnave tveganja, je treba upoštevati na enak način kot že vpeljane kontrole. Za identifikacijo obstoječih oz. načrtovanih kontrol morajo biti zbrane informacije preverjene še pri osebah, odgovornih za varovanje informacij, in pri uporabnikih, da ugotovimo, katere kontrole so resnično vpeljane za informacijske procese ali informacijske sisteme. Opravimo še izvedbo fizičnih kontrol na mestu samem in pregled rezultatov internih presoj.

4. **Prepoznavanje ranljivosti**. Prepoznati moramo ranljivosti, ki jih lahko izkoristijo grožnje, da škodujejo sredstvom oziroma organizaciji. Sama prisotnost ranljivosti še ne povzroči škode, ker je potrebna grožnja, ki bi jo uresničila.

5. **Prepoznavanje posledic**. Ta dejavnost določa škodo ali posledice za organizacijo, ki jih lahko povzroči negativni scenarij (incident). Negativni scenarij opisuje grožnje, ki jim je organizacija izpostavljena zaradi pomanjkljivosti oziroma niza pomanjkljivosti v informacijskem varnostnem sistemu. Učinek negativnega scenarija moramo determinirati ob upoštevanju meril učinka, opredeljenih v procesu vzpostavitev vsebin in njihovih soodvisnosti.

3.2.4 Okvirna ocena tveganja

Ocenjevanje tveganja je aktivnost dodeljevanja vrednosti verjetnostim in posledicam vsakega identificiranega tveganja. Sestavljajo jo naslednja opravila:

1. **Izbira metodologije za okvirno oceno tveganja glede na specifičnost zahtev in specifičnost samega tveganja**: Tveganja lahko analiziramo različno natančno, odvisno od pomembnosti sredstva, obsega znanih ranljivosti in preteklih incidentov, ki so prizadeli organizacijo. Lahko je – odvisno od okoliščin – kvalitativna ali kvantitativna analiza ali kombinacija obeh. Kvalitativna okvirna ocena uporablja kvalifikacijske atribute za opis resnosti potencialnih posledic (npr. nizko, srednje, visoko) in verjetnost njihovega pojava. Prednost kvalitativne okvirne ocene je v preprostosti razumevanja, medtem ko je slaba lastnost odvisnost od subjektivne izbire ocene. Kvantitativna okvirna ocena uporablja ocenjevalno lestvico z numeričnimi vrednostmi (namesto opisnih ocenjevalnih lestvic) za posledice in verjetnost, pri čemer uporabljamo podatke iz različnih virov. Kvaliteta analize je odvisna od pravilnosti in popolnosti numeričnih vrednosti in veljavnosti uporabljenih modelov.

2. **Ocena posledic**: Oceniti moramo vpliv na poslovanje organizacije, ki ga lahko ima možen ali dejanski incident pri varovanju informacij. Pri tem moramo upoštevati kršitve varovanja informacij, kot so izguba zaupnosti, celovitosti ali razpoložljivosti sredstev. Vrednost vpliva na poslovanje se lahko izrazi v kvalitativni in kvantitativni obliki, vendar metoda določitve denarne vrednosti navadno zagotovi več informacij za odločanje in s tem olajša učinkovitejši proces odločanja.

3. **Ocena verjetnosti incidenta**: Oceniti moramo verjetnost uresničitve negativnih scenarijev (scenarijev incidenta). Po določitvi scenarijev incidenta je potrebno oceniti verjetnost pojava posameznega scenarija in vpliva, za kar ponovno uporabimo kvalitativne in kvantitativne ocenjevalne tehnike. Pri tem je potrebno upoštevati, kako pogosto se grožnje uresničijo in kako lahko je izkoristiti ranljivost.

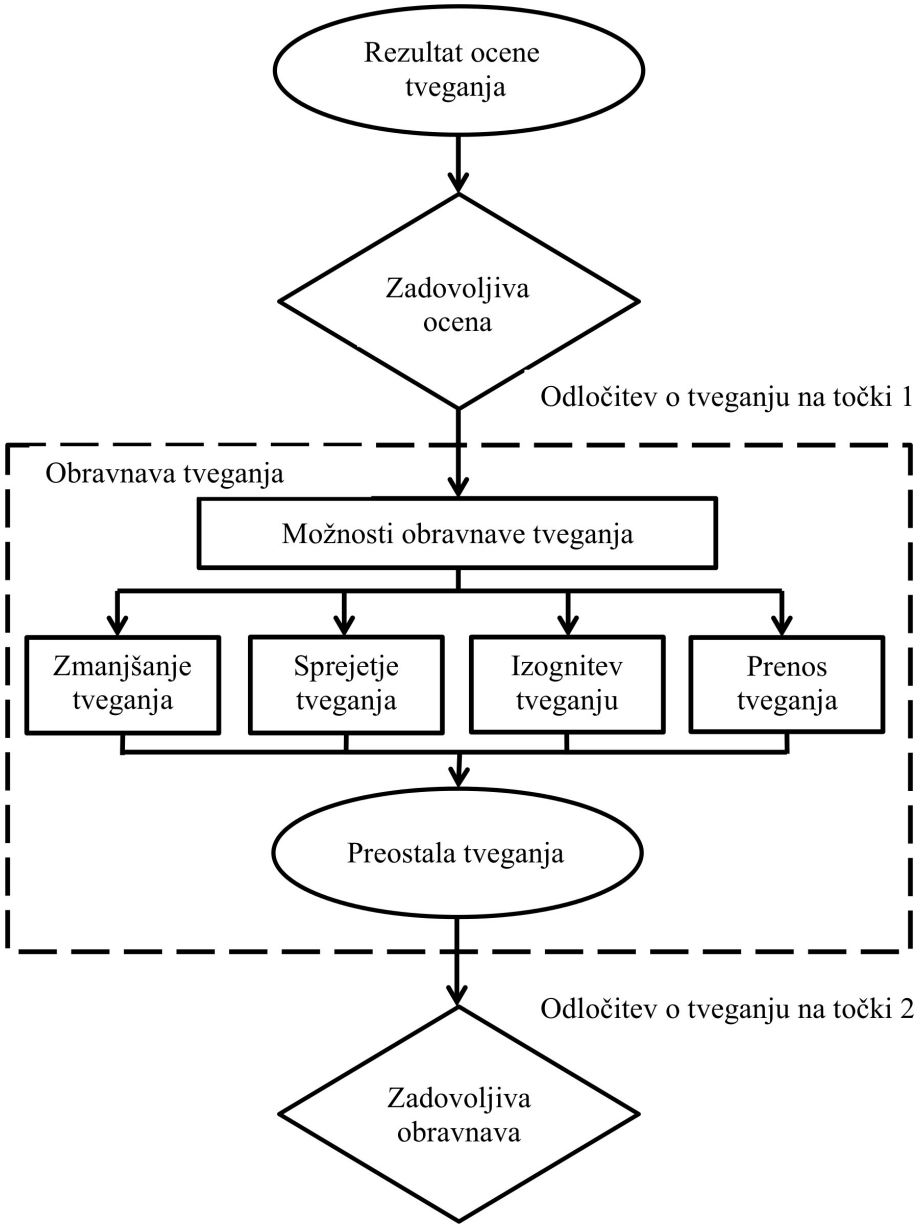
4. **Raven ocene tveganja**: Z okvirno oceno tveganja določimo vrednosti verjetnosti in posledic tveganja (kvantitativne ali kvalitativne vrednosti). Okvirna ocena tveganja temelji na ocenjenih posledicah verjetnosti. Poleg tega pri tem lahko upoštevamo stroškovne koristi, skrbi interesnih skupin in druge spremenljivke, primerne za vrednotenje tveganja.

3.2.5 Vrednotenje tveganja

Pri aktivnosti vrednotenja tveganj primerjamo nivo tveganja z merili za oceno tveganja ter merili sprejemljivosti (opredeljenih v procesu vzpostavitve vsebin in njihovih soodvisnosti). Merila za vrednotenje tveganja, ki se uporabijo za sprejemanje odločitev, morajo biti skladna z opredeljenim eksternim in internim kontekstom obvladovanja tveganj pri varovanju informacij. Upoštevamo cilje organizacije, pomen poslovnega procesa oziroma z določenimi sredstvi podprte dejavnosti ali niz sredstev, stališča interesnih skupin itn. Odločitve, sprejete med vrednotenjem tveganja, večinoma temeljijo na sprejemljivi ravni tveganja. Vendar moramo upoštevati tudi posledice, verjetnost in stopnjo zaupanja v določitev tveganja in analizo. Združitev več nizkih ali srednjih tveganj lahko povzroči precej višja skupna tveganja, zato jih obravnavamo v skladu s tem spoznanjem.

3.2.6 Obravnava tveganja

Pri ravnanju s tveganji zagotovimo seznam prednostnih tveganj z negativnimi scenariji glede na merila tveganj. Slika 3.3 kaže zgoraj naštete štiri dejavnosti pri obravnavi tveganja.



Slika 3.3: Obravnava tveganj

Kot je razvidno iz slike, standard definira štiri načine soočenja s tveganji:

1. **Zmanjšanje tveganja**: Raven tveganja je treba zmanjšati z izborom kontrol, tako da je preostala tveganja mogoče ponovno oceniti kot sprejemljiva. Izbrati je treba ustrezne in utemeljene kontrole, da se izpolnijo zahteve, ugotovljene med oceno tveganja in obravnavo tveganja. Na splošno lahko kontrole zagotovijo eno ali več naslednjih vrst zaščite: popravilo, odprava, preprečevanje, zmanjšanje vpliva, odvračanje, odkrivanje, obnova, spremljanje in ozaveščanje.

2. **Zavestno in objektivno sprejetje tveganja**: Odločitev brez nadaljnjih ukrepov mora biti odvisna od vrednotenja tveganja. Povsem mora ustrezati politikam organizacije in kriterijem za sprejem tveganj. Tveganja sprejmemo takšna, kot so.

3. **Tveganju se izognemo**: Dejavnosti ali pogoju, ki sproža določeno tveganje, se je treba izogniti.

4. **Prenos tveganja**: Tveganje je treba prenesti na drugo stranko, ki bo najučinkoviteje obvladala določeno tveganje glede na vrednotenje tveganja (na zavarovalnico na primer). Prenos tveganja lahko ustvari nova tveganja ali spremeni obstoječa, prepoznana tveganja.

Možnosti za obravnavo tveganja izberemo na podlagi rezultata ocene tveganja, pričakovanih stroškov za vpeljavo teh možnosti in pričakovanih koristi teh možnosti.

3.2.7 Sprejetje tveganj

Pri tej aktivnosti se odločimo, da tveganje sprejmemo, določimo odgovornost za to določitev in jo uradno zabeležimo. Načrti za obravnavo tveganj morajo opisati, kako obravnavamo ocenjena tveganja za izpolnitev meril za sprejetje tveganja. Pomembno je, da odgovorni pregledajo in odobrijo predlagane načrte za obravnavo tveganja in nastala preostala tveganja ter zabeležijo vse pogoje, ki so povezani s takšno odobritvijo.

3.2.8 Obveščanje o tveganju

Obveščanje o tveganju je dejavnost za sklenitev sporazuma o tem, kako obvladovati tveganja. Slednje storimo z izmenjavo in/ali delitvijo informacij o tveganju med osebami, ki sprejemajo odločitve, in drugimi interesnimi skupinami. Takšne informacije vključujejo obstoj, naravo, obliko, verjetnost, resnost, obravnavo, sprejemljivost tveganj in ostalo.

Oseba, ki sprejema odločitve, in zainteresirane javnosti, si morajo izmenjavati informacije o tveganju. Uspešna komunikacija med zainteresiranimi stranmi je pomembna, ker lahko odločilno vpliva na odločitve, ki jih je treba sprejeti. Sporočanje bo zagotovilo, da osebe, odgovorne za vpeljavo obvladovanja tveganja, in osebe, zainteresirane zanj, razumejo podlago, na kateri sprejememo odločitve in določene ukrepe. Komunikacija je dvosmerna.

3.2.9 Nadzor in ocenjevanje tveganja

Ocena tveganja določa vrednost informacijskih sredstev, prepoznava obstoječe grožnje in ranljivosti (ali ki bi lahko obstajale), prepoznava obstoječe kontrole in njihov vpliv na obstoječa tveganja, določa možne posledice in prednostni vrstni red ugotovljenih tveganj in jih razporedi v skladu z merili za vrednotenje tveganja, opredeljenimi pri določanju konteksta. Stalno spremljanje in pregledovanje sta nujna koraka, s katerima zagotovimo, da kontekst, rezultat ocene tveganja in obravnave tveganja ter načrti za obvladovanje ostanejo ustrezni glede na okoliščine. Organizacija se mora prepričati, da proces obvladovanja tveganj pri varovanju informacij in z njimi povezane dejavnosti ostanejo ustrezne glede na obstoječe okoliščine in se upoštevajo. Vsako dogovorjeno izboljšavo procesa ali ukrepov, ki so potrebni za izboljšanje skladnosti s procesom, moramo sporočiti vodstvu, da bi zagotovili, da nobenega tveganja ali elementa tveganja ne spregledamo ali podcenimo, da ustrezno ukrepamo, tveganje razumemo in smo se sposobni nanj odzvati.

Poleg tega mora organizacija redno preverjati, da so ukrepi, ki se uporabljajo za merjenje tveganja in njegovih elementov, še vedno veljavni in v skladu s poslovnimi cilji, strategijami in politikami ter da se med obvladovanjem tveganja pri varovanju informacij ustrezno upoštevajo spremembe poslovnega okolja.

3.3 ISO 28000:2007

Ta standard se uporablja za izvajanje sistemov za upravljanje varnosti oskrbovalne verige v organizacijah. Osnovni namen standarda je, da „se lahko neposredno in formalno pristopi k upravljanju varnosti organizacij tako, da se zagotovi poslovna uspešnost in verodostojnost organizacije" [6]. ISO 31000 je splošni standard za upravljanje tveganj, ISO 28000 pa specifična uporaba varnosti pri oskrbovalnih verigah. Pri tem upravljanje varnosti opredeljuje kot „uporabo sistematičnih in usklajenih dejavnosti in praks, prek katerih organizacija optimalno upravlja tveganj povezanimi z oskrbovalnimi verigami ter

s tem povezanimi potencialnimi nevarnostmi in vplivi njih" [6].

ISO 28000:2007 določa zahteve za sistem upravljanja varnosti, vključno s tistimi vidiki, kritičnih za varnostne zanesljivosti dobavne verige.

ISO 28000: 2007 se uporablja za vse velikosti organizacij v kateri koli fazi proizvodnje ali oskrbovalne verige, ki želi:

1. vzpostaviti, izvajati, vzdrževati ali izboljšati sistem upravljanja varnosti;
2. zagotoviti skladnost z vzpostavljeno politiko upravljanja varnosti;
3. drugim dokazati takšno skladnost;
4. si prizadeva certificirati svoj sistem upravljanja varnosti tako, da je akreditiran s strani certifikacijskega organa; ali
5. da zase doseže skladnost s standardom ISO 28000.

Poleg tega lahko obstaja zakonodaja ali kakšne druge pogodbene obveznosti, ki vključujejo nekatere zahteve iz standarda.

Organizacije, ki se odločijo za certificiranja s strani tretje osebe (certifikacijskega organa na primer) dokazujejo, da pomembno prispevajo k varnosti dobavne verige.

Področja kot jih definira ISO 28000, kjer se tveganja lahko pojavljajo so:

1. Tveganja fizičnih odpovedi, kot so na primer funkcionalne odpovedi opreme, naključne odpovedi, zlonamerne poškodbe, teroristična ali kriminalna dejanja.
2. Operativna tveganja, ki vključujejo nadzor varnosti, človeškega faktorja in ostale aktivnosti, ki vplivajo na uspešnost, stanje in varnost organizacije.
3. Naravni okoljski dogodki (nevihte, poplave itd.), zaradi katerih lahko varnostni ukrepi in oprema postanejo manj učinkoviti.
4. Faktorji, ki niso pod nadzorom organizacije, kot na primer odpoved opreme ali storitev, ki jih izvajajo zunanji ponudniki.
5. Tveganja vseh zainteresiranih udeležencev organizacije, kot na primer nedoseganje regulativnih zahtev ali zmanjšan ugled blagovne znamke.
6. Načrtovanje in instalacija varnostne opreme, vključujoč menjavo, vzdrževanje itd.
7. Upravljanje informacij in podatkov ter komunikacije.
8. Grožnje za kontinuiteto delovanja.

Poglavje 4

Princip modeliranja tveganj s segmentacijo javnosti

V literaturi in v praksi govorimo o tveganjih, ki jih nosijo nežive stvari, pa čeprav imajo samo ljudje sposobnost zaznavanja samega sebe [4]. Če je res, da nosijo tveganja samo ljudje, se lahko vprašamo: „Čigava tveganja upravljamo? [4]" Potemtakem potrebujemo samo modele tveganj, ki bi upoštevali specifičnosti posameznih javnosti, če velja, da tveganja zadevajo samo ljudi?

Sedanji modeli tveganj v večini primerov ne upoštevajo stanja okolja, ki ga zaznavajo, in kjer so akumulirana pretekla dejstva, lastna opazovanemu sistemu in imajo svoj vpliv na trenutno stanje. Modeli, ki se danes v literaturi in v praksi pretežno uporabljajo, so posledica precejšnjih poenostavitev in posplošitev. Takšno stanje je seveda pričakovano, saj bi bili brez poenostavitev in posplošitev verjetno še vedno brez uporabnih modelov. Gre za razvoj, ki se, če je uspešen, vedno začne s poenostavitvami.

Obstoječi modeli prav tako ne upoštevajo in ne vključujejo hkrati „negotovosti" in „izpostavljenosti", ki sta lastni ljudem. Vsaka oseba ali vsaka javnost ima specifična tveganja in s tem ima vsaka javnost svojo lastno negotovost in izpostavljenost.

V nadaljevanju je dopolnjen aktualen pogled na temeljne pojme, s katerimi se ukvarjamo pri tveganjih, saj je od širšega ali ožjega pojmovanja tveganj v veliki meri odvisna kompleksnost modelov upravljanja modela procesov ob upoštevanju tveganja in segmentacije javnosti.

Predlagan bo splošni princip za model tveganj, ki temelji na sistemskem pristopu. Pri tem modelu so pomembni predvsem [13]:

1. Vhodi in izhodi posameznega poslovnega procesa.
2. Tveganja („risks") in vplivi („impacts") kot nasprotje splošnih (podatkovnih) vhodov in izhodov.
3. Interno in eksterno okolje opazovanega sistema poslovnih procesov tako, da se vhodi, izhodi, tveganja in vplivi delijo na interne (na katere imamo načeloma večji vpliv) in eksterne.

Za vse vhode in izhode opazovanega sistema je potrebno določiti posamezne (zainteresirane) javnosti.

Morebitne dodatno definirane dimenzije modela so odvisne od potreb posameznega primera.

V nadaljevanju sledi podpoglavje o problemu definicije tveganj, ki je ključnega pomena za razumevanje predlaganega modela upravljanja tveganj. V tretjem poglavju bo po korakih opisan predlagani model tako, da bo v vsakem koraku opisana ena lastnost ali dimenzija modela. Celotno poglavje pa sledi objavam predlaganega modela v [16, 17, 20].

4.1 Definicija tveganja

V nadaljevanju bom upošteval Holtonovo definicijo, ki pripisuje tveganja le ljudem in zato v temeljih spreminja obstoječi pogled na tveganja in njihovo obravnavo. Holtonov [3] pogled na tveganje pravi, da je videti, da sta:

1. *izpostavljenost* in
2. *negotovost*

edini ključni komponenti tveganj. Najtežje jih je določiti in upoštevati. Oglejmo si ilustrativen primer. Most kot zgradba nima nobenega tveganja, četudi je zgrajen še tako slabo. Tveganja nosijo samo deležniki (ljudje), ki so na takšen ali drugačen način povezani s tem mostom. Most sam po sebi nima dimenzije izpostavljenosti, kot bo ta definirana in opisana v nadaljevanju. Prav tako je vprašljiva interpretacija negotovosti, ki jo ima most.

Zaradi poenostavitev lahko v posameznih primerih jemljemo za osebe tako fizične kot pravne osebe, čeprav ni težko prevesti pravne osebe v specifično javnost fizičnih oseb. Prav tako velja, da s tovrstno posplošitvijo kaj kmalu zaidemo v slepo ulico. Namreč v zelo malem številu primerov tvegajo samo deležniki v podjetjih in organizacijah. V

ozadju so zaposleni, lastniki, investitorji, lokalna skupnost, itd. Vsak od teh deležnikov (ali skupina) pa ima svojo negotovost in izpostavljenost. [3]

Oglejmo si še problematiko verjetnosti, saj je verjetnost sestavni del tveganj. Po Knightu [22] tveganja razdelimo na:

1. *prava* ali *objektivna* tveganja, kjer imamo opraviti z logiko, verjetnostmi in statističnimi metodami, in na

2. *negotovosti* ali *subjektivna* tveganja, ko si z verjetnostmi ne moremo ali ne znamo kaj veliko pomagati – ko jo določijo posamezniki glede na to koliko v kaj verjamejo ali si določijo vrednostni sistem na osnovi mnenj in tako opišejo svojo negotovost.

Torej lahko pri tveganjih sklepamo, da verjetnost sicer lahko uporabljamo kot metriko za mero tveganja, vendar je njena uporaba omejena in pomanjkljiva. Manjka vsaj še mera za negotovost [22].

4.1.1 Negotovost

Negotovost je stanje, ko ne vemo, ali neka predpostavka ali trditev drži ali ne (je pravilna ali nepravilna). Verjetnost je tista metrika, s katero največkrat izražamo negotovost, vendar je njena uporaba omejena. Največ, kar je mogoče oceniti, je tista negotovost, ki smo jo sposobni „zaznati".

Pri oblikovanju modela predlagam uporabo negotovosti tako, kot jo uporablja Holton, vendar jo delim naprej tako kot to pravi Knight za tveganja. Tako uporabljam:

1. *objektivno negotovost* in

2. *subjektivno negotovost*.

4.1.2 Izpostavljenost

Osnovno vprašanje pri testiranju izpostavljenosti je naslednje: Ali nam je mar? [3] Z drugimi besedami: izpostavljeni smo takrat, kadar ima neki dogodek za nas neke materialne ali nematerialne posledice. Ljudje smo torej izpostavljeni, če nas skrbi, ali predpostavka drži ali ne. Lahko smo izpostavljeni tveganju in se tega povsem zavedamo (v primeru, če prisebni hodimo po ograji visokega mostu) ali pa se tveganja sploh ne zavedamo (če nas „nosi luna" in hodimo po ograji visokega mostu). Tveganje lahko jemljemo zelo resno (na primer, če imamo opraviti z omejitvijo hitrosti v naselju, kjer je vedno policijska

patrulja) ali pa nam tveganja ni mar (kot v primeru vožnje s prekomerno hitrostjo v naselju, kjer vemo, da ni policijske kontrole, ura je pozna in cesta je prazna). Torej izpostavljenost vnaša dodatno nedoločljivost, ki je odvisna predvsem od posameznika ali neke javnosti in njene percepcije glede izpostavljenosti in posledično tudi tveganja. Tako nismo soočeni samo s problemom metrike negotovosti, temveč tudi s problemom metrike izpostavljenosti.

4.1.3 Tveganje

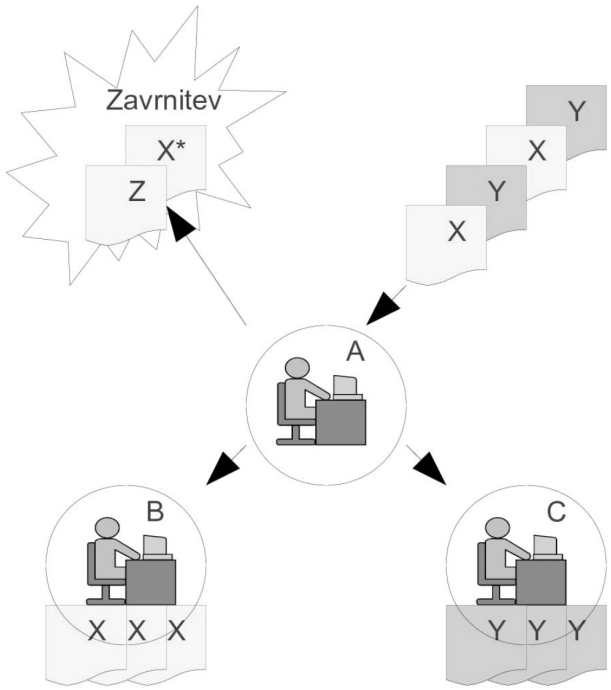
Upoštevaje zgornje opise negotovosti in izpostavljenosti, lahko zaključimo: **tveganje je izpostavljenost negotovosti**.

Ker je oboje, tako negotovost kot izpostavljenost, težko določiti, je tudi tveganje težko opredeliti. Torej je tveganja težko modelirati in simulirati. Po drugi strani s poenostavljenimi modeli, kadar poenostavimo tveganje, v splošnem ne moremo biti verodostojni. Največkrat modeli poenostavijo problematiko tveganj kar na zmnožek verjetnosti za pojav tveganja z velikostjo predvidene škode, ki ob tem nastane. Takšni modeli so seveda uporabni v zelo omejenem obsegu.

Zaradi dimenzije negotovosti in izpostavljenosti, je tveganje pojem, ki vključuje posameznika ali javnost kot nujno definiran parameter.

4.2 Principi oblikovanja modela

Pri opisanem principu sem sledil želji, da bi bil model dovolj splošen za uporabo v različnih situacijah in na različnih področjih, kjer se soočamo s tveganji kot na primer: prodajo in distribucijo naravnega plina, zagon nove poslovne priložnosti, vojaško avanturo, ... in tudi ljubezensko razmerje. Kljub temu, da je v tem prispevku opisani model mogoče uporabiti na širokem spektru področij življenja, je kot za primer v nadaljevanju obrazložen model poslovnih procesov. Glede na posamezno obravnavano področje, ki ga želimo modelirati, je pomen posameznega segmenta modela (različne javnosti, interno vs. eksterno, itd.) lahko različen, vendar verjetno ne moremo govoriti o tem, da je na nekem področju določen segment modela povsem zanemarljiv.



Slika 4.1: Poenostavljen poslovni proces, pri katerem uradnik A pregleduje in usmerja prispele dokumente v poslovna procesa B (k uradniku B) in C (k uradniku C)

4.2.1 Predstavitev procesov

Pri modeliranju je sistem poslovnih procesov predstavljen z grafom, ki je matematična struktura, v kateri vozlišča predstavljajo posamezen proces, usmerjene povezave med vozlišči pa njihove medsebojne odvisnosti.

Primer Poglejmo si primer sistema poslovnih procesov, pri katerem uradnik A (poslovni proces A) sprejema dva tipa dokumenta. To sta dokumenta tipa X in Y. Ko prejme dokument, ga pregleda in oceni korektnost ter ga po potrebi zavrne. Zavrnjen dokument je tipa Z. Dokumente tipa X pošlje naprej v postopek obravnave uradniku B (poslovni proces B) in dokumente tipa Y uradniku C (poslovni proces C). Slika 4.1 prikazuje pravkar opisan poenostavljen primer poslovnih procesov in njihove medsebojne odvisnosti.

4.2.2 Opis stanja procesa s parametri in časovna dimenzija modela

Vsakemu procesu lahko pripišemo poljubno število parametrov, ki simbolizirajo in opisujejo njegova notranja stanja. Primeri takšnih parametrov so lahko: predviden čas za izvajanje; funkcija odstopanja od predvidenega časa; senzibilnost na posamezne tipe tveganj; obdobje v letu, ko je pomen procesa v okviru celotnega sistema procesov visok ali nizek; stopnja zrelosti (t.i. „maturity level"); stopnja sprejemljivosti posameznih tveganj; stopnja sprejemljivosti posameznih vplivov; ...

Največji pomen parametrov je v tem, da omogočajo, da se s časom v njih „akumulira" pretekli življenjski cikel posameznega poslovnega procesa, ki ga upoštevamo pri izračunavanju vplivov in novih vrednosti parametrov. Na ta način pri modeliranju zajamemo „zgodovino" modeliranega sistema. V teh parametrih je akumulirana zgodovina preteklih trenutkov in s tem preteklih kombinacij tveganj in ostalih vplivov na poslovni proces.

Primer V primeru pregledovanja prispelih dokumentov je parameter procesa A lahko število zamud, ki nastanejo, ker uradnik A dokumenta ni v predpisanem roku poslal naprej v reševanje ali pa ga zavrnil zaradi neustreznosti. Vsaka posamezna zamuda, ki jo model sicer lahko upošteva, je v našem primeru nepomembna. Večje število posameznih zamud, pa ima lahko škodljive posledice. Torej je potrebno v model vnesti ne le posamezne zamude, temveč tudi „zgodovino" vseh zamud, ki jo je skozi čas potrebno spreminjati in upoštevati.

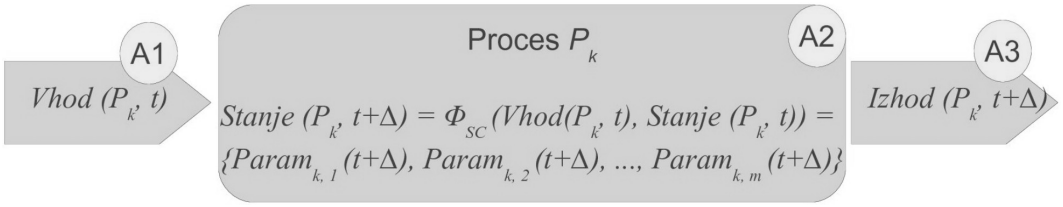
Pri modelu tveganja velja, da po vsakem diskretnem časovnem intervalu dobimo nov izračun opazovanih vrednosti. Pri tem opazujemo predvsem:

1. parametre, ki opisujejo notranja stanja,
2. tveganja in
3. vplive

posameznega procesa sistema opravil. Izračun lahko v vsakem časovnem segmentu spremeni opazovano vrednost ali pa ta ostane enaka.

Slika 4.2 prikazuje izračun izhoda $Izhod(P_k, t+\Delta)$ in parametre $Param_k, x(t)$ v času $t + \Delta$ procesa P_k, ki se glede na:

1. vhod $Vhod(P_k, t)$,
2. stanje procesa $Stanje(P_k, t)$ v času t in



Slika 4.2: Proces P_k s splošnimi vhodi in izhodi ter parametri, ki opisujejo njegova notranja stanja

3. funkcijo Φ_{SC}, s katero izračunavamo notranje stanje procesa v naslednjem časovnem obdobju,

spremenijo.

Primer V zgoraj opisanem primeru poenostavljenega poslovnega procesa, kjer uradniki A, B in C opravljajo svoje delo, lahko simuliramo njihovo poslovanje tako, da vsako uro simuliramo morebitno prispetje enega ali večjega števila dokumentov do uradnika A in nato na osnovi statistično poznanih dejstev simuliramo čase (in zamude) pri pregledovanju, preusmerjanju in zavračanju dokumentov. Seveda se vsako uro, to je v tistem diskretnem časovnem trenutku, ko pregledamo morebitne spremembe v sistemu procesov in ustrezno ažuriramo posamezne vrednosti parametrov modela, vrednosti parametrov procesa lahko spremenijo ali pa tudi ne, skladno s funkcijo $\Phi_S C$.

4.2.3 Vhodi in izhodi procesa ter segmentacija na tveganja in vplive

Tveganja so del vhoda v proces, ki lahko predstavljajo negativno (to je škodo) ali pozitivno pričakovanje. Največkrat gre za poslovna tveganja. Pomen ali velikost tveganja merimo na izhodni strani z vplivi, ki predstavljajo posebno vrsto izhoda.

Tako vhod segmentiramo na:

1. splošen vhod in na
2. tveganja,

izhod pa na:

1. splošen izhod in na

2. vplive (ki so posledica tveganj).

To pomeni, da moramo izluščiti tiste vhode, ki imajo za nas poseben pomen – to so tveganja, ki vplivajo skupaj s splošnim vhodom na stanje procesa in na vplive. Določitev tveganj je, kot je opisano zgoraj, težaven proces, vendar samo iskanje in določanje tveganj ni predmet tega prispevka. V nadaljevanju si oglejmo primer tveganja in vpliva.

Primer Primer tveganja je prispetje dokumenta, ki predstavlja slabo kopijo (slabo „sliko") nekega dokumenta in kot tak lahko predstavlja tveganje za njegovo ustrezno obravnavo. Uradnik A lahko takšen dokument potrdi kot ustreznega in ga pošlje v nadaljnjo obravnavo, vendar se lahko kasneje izkaže, da je ključni del takšnega dokumenta nečitljiv. Posledično nastane škoda. Predpostavimo, da so dokumenti tipa X takšni, da njihovo neustrezno obravnavanje v procesu sprejema povzroči večjo škodo, medtem ko napačno obravnavanje dokumentov tipa Y praktično nima negativnih posledic.

Vplive izračunamo podobno kot stanje procesa, vendar je tukaj funkcija seveda drugačna. Odvisni so od splošnega vhoda, tveganj in od stanja procesa.

Slika 4.5 prikazuje izračun splošnega izhoda $SploenIzhod(P_k, t + \Delta)$ in vplivov $Vplivi(P_k, t + \Delta)$ procesa P_k v času$t + \Delta$. Vplivi se glede na:

1. splošen vhod $SploenVhod(P_k, t)$ in tveganja $Tveganja(P_k, t)$, ki skupaj predstavljata $Vhod(P_k, t)$,
2. stanje procesa $Stanje(P_k, t)$ v času t in
3. funkcijo $\Phi_I C$

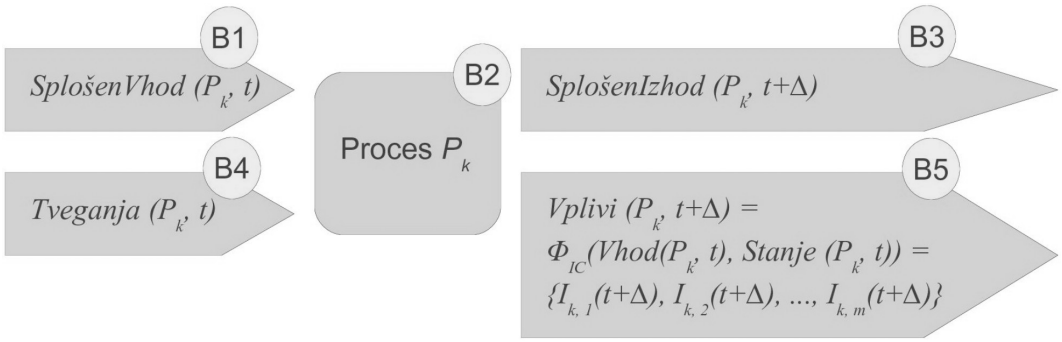
spremenijo. Posamezni vplivi v času t so $I_k, x(t)$.

Obe prejšnji sliki (4.2 in 4.3) je mogoče zliti v eno tako, da vhod in izhod na sliki 4.2 zamenjamo s segmentiranim vhodom (splošen vhod, tveganje) in izhodom (splošen izhod, vplivi), kot je prikazano na sliki 4.4.

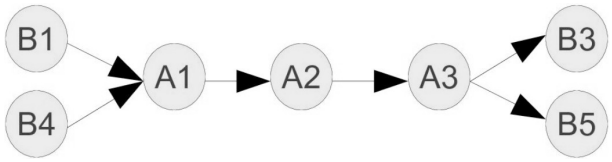
Tudi splošen izhod je izračunan po neki funkciji, vendar ta funkcija ni predmet tega prispevka. Pri modeliranju in simulacijah jo je potrebno upoštevati, saj je splošen izhod procesa P_k lahko splošen vhod v enega ali več ostalih procesov.

4.2.4 Segmentiranje glede na izvor in ponor vhodov in izhodov opazovanega sistema opravil

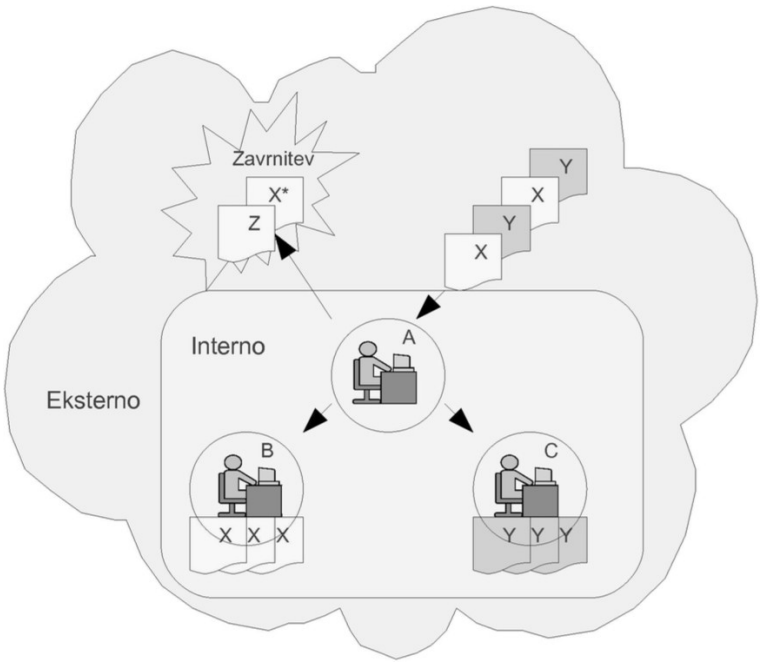
Naslednja segmentacija zahteva, da delimo vhode in izhode tako, da opazujemo posebej vhode, ki imajo izvor in ponor znotraj zaključenega in opazovanega sistema procesov,



Slika 4.3: Proces P_k z vhodom, ki ga sestavljajo splošen vhod in tveganja, in z izhodom, ki ga sestavljajo splošen izhod in vplivi



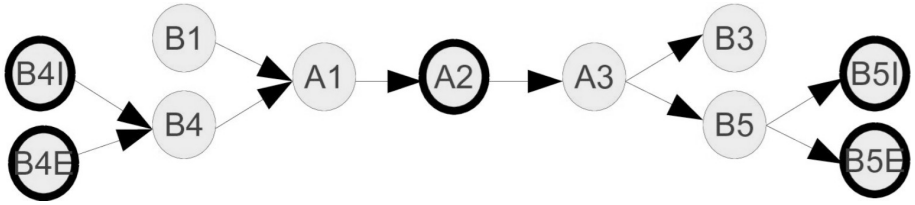
Slika 4.4: Zlitje slik 4.2 in 4.3, kjer imamo opravka s segmentiranim vhodom in izhodom ter z notranjimi stanji



Slika 4.5: Segmentacija vhodov in izhodov sistema procesov glede na to, ali gre za interne ali eksterne izvore in ponore

ter na tiste, ki imajo svoj izvor in ponor zunaj – to je eksterno glede na opazovan sistem opravil. Celoten sistem opravil naj predstavlja naš „model sveta". Glede na ta „model sveta", lahko govorimo o internih in eksternih vhodih in izhodih. Za interne izhode je značilno, da so v naslednjem diskretnem časovnem trenutku interni vhodi v nek drug proces znotraj opazovanega sistema procesov. Interni izhodi so v praksi posebej pomembni zato, ker imamo nanje večji vpliv (na primer interno glede na podjetje, oddelek, neko skupnost, državo, itd.). V praksi to pomeni, da lahko z internimi dogovori (predpisi, poslovnimi običaji, prakso, itd.), na katere imamo vpliv, spremenimo marsikateri interni izhod (torej tudi interni vpliv), ki določa obnašanje sistema procesov v naslednjem časovnem intervalu. Slika 5 grafično prikazuje sistem opravil, v katerem se zavedamo internosti in eksternosti.

Primer Pri delu uradnikov lahko vplivamo na zmanjšanje tveganja povezanega z napačno usmerjenimi dokumenti tipa X in Y uradnikoma B in C in s tem na zmanjšanje vplivov napačno usmerjenih dokumentov – gre za interne procese in njihove medsebojne povezave (glej sliko 4.1 ali 4.5). Nimamo pa nikakršnega vpliva na kakovost „slike" prispe-



Slika 4.6: Segmentacija tveganj in vplivov na množico internih in eksternih

lih dokumentov od „zunaj" in zato v tem primeru kakovost „slike" predstavlja eksterno tveganje. Pri modeliranju to pomeni, da sliko 4.4 dopolnimo tako, da B4 (tveganja) segmentiramo na B4I in B4E, kar predstavlja interna in eksterna tveganja. B5 (vplivi) pa segmentiramo na B5I in B5E, ki predstavljata interne in eksterne vplive. Rezultat takšne transformacije je na sliki 4.6.

Predmet posebne pozornosti pri oblikovanju modela in simulacijah so tako:

1. interna tveganja (B4I),
2. eksterna tveganja (B4E),
3. stanje procesa, ki ga opisujejo njegovi parametri (A2),
4. interni vplivi (B5I) in
5. eksterni vplivi (B5E).

Splošne vhode in izhode ne segmentiramo glede na interno ali eksterno, ker jih pri obravnavanem principu oblikovanja modela sicer predvidimo in pri simulacijah modela tudi upoštevamo, vendar nimajo posebnega pomena pri upravljanju tveganj. Torej niso predmet naše pozornosti.

4.2.5 Segmentiranje glede na različne javnosti

Ob predpostavki, da smo ljudje v različnem odnosu do nekega tveganja, ki se pojavlja v neki situaciji, največkrat problema ne delimo na posameznike, temveč na množice ljudi, oziroma posamezne javnosti, ki imajo skupen odnos do določenega tveganja. Zato je potrebno opraviti tudi segmentacijo javnosti in izvesti simulacijo za vsako javnost posebej. Enačbi s slike 4.2 in 4.3 upoštevata dimenzijo časa, ne upoštevata pa dimenzije, ki jo prinese segmentacija javnosti.

Glede na pristop, ki ga pojasnjujem v tem gradivu, moramo izračunati tveganje glede na posamezno javnost. Tveganja se lahko spreminjajo tudi glede na čas. Enačba (4.1) prikazuje izračunana tveganja $R_{k,x}$ za proces P_k in segment javnosti $SegmentJavnosti_l$ v času t.

$$\begin{gathered} Tveganje(P_k, SegmentJavnosti_l, t) = \\ \Phi_{RC}\begin{pmatrix} Negotovost(P_k, SegmentJavnosti_l, t) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\ \Phi_{RC}\begin{pmatrix} ObjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ SubjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\ \{(R_{k,l,1}(t), (R_{k,l,2}(t), \ldots, (R_{k,l,m}(t)\} \end{gathered} \tag{4.1}$$

kjer pomenijo:

1. P_k je proces k.
2. $Negotovost(P_k, SegmentJavnosti_l, t)$ je negotovost pri procesu P_k glede na segment javnosti $SegmentJavnosti_l$ v času t, ki se v drugem koraku deli na objektivno ($ObjektivnaNegotovost$) in subjektivno ($SubjektivnaNegotovost$) negotovost.
3. $Izpostavljenost(P_k, SegmentJavnosti_l, t)$ je izpostavljenost pri procesu P_k glede na segment javnosti $SegmentJavnosti_l$ v času t.
4. Posamezna tveganja za proces P_k predstavlja množica m-tih tveganj $\{(R_{k,l,1}(t), (R_{k,l,2}(t), \ldots, (R_{k,l,m}(t)\}$ glede na segment javnosti $SegmentJavnosti_l$ v času t.
5. Funkcija Φ_{RC} izračunava tveganja.

Enačba (4.2) predstavlja izračun stanja procesov v naslednjem časovnem intervalu. Izračunavamo s funkcijo Φ_{SC}, izračunavanje pa temelji na:

1. vrednosti vhoda v proces, ki je sestavljena iz (glej sliko 4.2 in 4.3):
   (a) tveganja, ki ga izračunamo na osnovi informacij o (glej enačbo (4.1)):
      i. objektivni in
      ii. subjektivni negotovosti ter

iii. izpostavljenosti;

(b) splošnega vhoda, ki ne vsebuje tveganj;

2. in trenutni vednosti parametrov s katerimi opisujemo stanje procesa.

$$
\begin{gathered}
Stanje(P_k, SegmentJavnosti_l, t+\Delta) = \\
\Phi_{SC}\begin{pmatrix} Vhod(P_k, SegmentJavnosti_l, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\
\Phi_{SC}\begin{pmatrix} Tveganje(P_k, SegmentJavnosti_l, t) \\ SplosenVhod(P_k, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\
\Phi_{SC}\left(\begin{array}{c} \Phi_{RC}\begin{pmatrix} ObjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ SubjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t) \end{pmatrix} \\ SplosenVhod(P_k, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{array}\right) = \\
\{Param_{k,l,1}(t+\Delta), Param_{k,l,2}(t+\Delta), \ldots, Param_{k,l,m}(t+\Delta)\}
\end{gathered}
\tag{4.2}
$$

Z enačbo (4.3) izračunamo vplive na podoben način, kot smo z enačbo (4.2) izračunali stanja procesa.

$$
\begin{gathered}
Vpliv(P_k, SegmentJavnosti_l, t+\Delta) = \\
\Phi_{IC}\begin{pmatrix} Vhod(P_k, SegmentJavnosti_l, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\
\Phi_{IC}\begin{pmatrix} Tveganje(P_k, SegmentJavnosti_l, t) \\ SplosenVhod(P_k, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\
\Phi_{IC}\left(\begin{array}{c} \Phi_{RC}\begin{pmatrix} ObjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ SubjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t) \end{pmatrix} \\ SplosenVhod(P_k, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{array}\right) = \\
\{I_{k,l,1}(t+\Delta), I_{k,l,2}(t+\Delta), \ldots, I_{k,l,m}(t+\Delta)\}
\end{gathered}
\tag{4.3}
$$

Z upoštevanjem enačb (4.2) in (4.3) lahko vplive izrazimo tudi z enačbo (4.4).

$$
\begin{aligned}
&Vpliv(P_k, SegmentJavnosti_l, t+\Delta) = \\
&\Phi_{IC}\begin{pmatrix} Vhod(P_k, SegmentJavnosti_l, t) \\ Stanje(P_k, SegmentJavnosti_l, t) \end{pmatrix} = \\
&\Phi_{IC}\left(\begin{array}{c} Vhod(P_k, SegmentJavnosti_l, t) \\ \Phi_{SC}\begin{pmatrix} Tveganje(P_k, SegmentJavnosti_l, t-1) \\ SplosenVhod(P_k, t-1) \\ Stanje(P_k, SegmentJavnosti_l, t-1) \end{pmatrix} = \end{array}\right) = \\
&\Phi_{IC}\left(\begin{array}{c} SplosenVhod(P_k, t) \\ \Phi_{RC}\begin{pmatrix} ObjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ SubjektivnaNegotovost(P_k, SegmentJavnosti_l, t) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t) \end{pmatrix} \\ \Phi_{SC}\left(\begin{array}{c} \Phi_{RC}\begin{pmatrix} ObjektivnaNegotovost(P_k, SegmentJavnosti_l, t-1) \\ SubjektivnaNegotovost(P_k, SegmentJavnosti_l, t-1) \\ Izpostavljenost(P_k, SegmentJavnosti_l, t-1) \end{pmatrix} \\ SplosenVhod(P_k, t-1) \\ Stanje(P_k, SegmentJavnosti_l, t-1) \end{array}\right) \\ \{I_{k,l,1}(t+\Delta), I_{k,l,2}(t+\Delta), \ldots, I_{k,l,m}(t+\Delta)\} \end{array}\right) = \\
&\qquad (4.4)
\end{aligned}
$$

Tako smo z enačbami od (4.1) do (4.4) dodali še zadnji napotek, kako izračunati vrednosti, ki so za upravljanje tveganj posebnega pomena. Z drugimi besedami: predlagan princip za oblikovanje modelov upravljanja procesov ob upoštevanju tveganj in segmentiranja javnosti predvideva, da so v model vgrajeni izračuni enačb (4.1), (4.2) in (4.3) ali (4.1), (4.2) in (4.4).

4.2.6 Meje sprejemljivosti

Na koncu moramo v modelu določiti še meje sprejemljivosti za tveganja, vplive in stanja procesov ter glede na tako določene meje določiti sprejemljiva in nesprejemljiva tveganja, vplive in stanja procesov. To lahko določimo z enačbami od (4.5) do (4.13).

Pri tveganjih so meje sprejemljivosti tveganja RAB izračunane v enačbi (4.5) s funkcijo Φ_{RAB}, meje sprejemljivosti vplivov IAB v enačbi (4.6)6 s funkcijo Φ_{IAB} in meje sprejemljivosti vrednosti stanj procesov SAB v enačbi (4.7) s funkcijo Φ_{SAB}.

$$\begin{gathered} MejaSprejemljivostiTveganja(P_k, SegmentJavnosti_l, t) = \\ \Phi_{RAB}\left(Tveganje(P_k, SegmentJavnosti_l, t)\right) \\ \{RAB_{k,l,1}(t), RAB_{k,l,2}(t), \ldots, RAB_{k,l,m}(t)\} \end{gathered} \tag{4.5}$$

$$\begin{gathered} MejaSprejemljivostiVpliva(P_k, SegmentJavnosti_l, t) = \\ \Phi_{IAB}\left(Vpliv(P_k, SegmentJavnosti_l, t)\right) \\ \{IAB_{k,l,1}(t), IAB_{k,l,2}(t), \ldots, IAB_{k,l,m}(t)\} \end{gathered} \tag{4.6}$$

$$\begin{gathered} MejaSprejemljivostiStanja(P_k, SegmentJavnosti_l, t) = \\ \Phi_{RAB}\left(Stanje(P_k, SegmentJavnosti_l, t)\right) \\ \{SAB_{k,l,1}(t), SAB_{k,l,2}(t), \ldots, SAB_{k,l,m}(t)\} \end{gathered} \tag{4.7}$$

V enačbah (4.8), (4.9) in (4.10) so napisane sprejemljive vrednosti za tveganje, vplive in vrednosti stanj procesa glede na dane meje sprejemljivosti.

$$\begin{gathered} SprejemljivaTveganja(P_k, SegmentJavnosti_l, t) = \\ \{R_{k,l,x}(t); x = 1, 2, \ldots, m \wedge R_{k,l,x}(t) < RAB_{k,l,x}(t)\} \end{gathered} \tag{4.8}$$

$$\begin{gathered} SprejemljiviVplivi(P_k, SegmentJavnosti_l, t) = \\ \{I_{k,l,x}(t); x = 1, 2, \ldots, m \wedge I_{k,l,x}(t) < IAB_{k,l,x}(t)\} \end{gathered} \tag{4.9}$$

$$\begin{gathered} SprejemljivaTveganja(P_k, SegmentJavnosti_l, t) = \\ \{Param_{k,l,x}(t); x = 1, 2, \ldots, m \wedge Param_{k,l,x}(t) < SAB_{k,l,x}(t)\} \end{gathered} \tag{4.10}$$

V enačbah (4.11), (4.12) in (4.13) so napisane nesprejemljive vrednosti, ki seveda predstavljajo množico vrednosti, ki je enaka množici vseh vrednosti, zmanjšana za množico vrednosti, ki so sprejemljive.

$$\begin{gathered} NesprejemljivaTveganja(P_k, SegmentJavnosti_l, t) = \\ Tveganje(P_k, SegmentJavnosti_l, t) - SprejemljivaTveganja(P_k, SegmentJavnosti_l, t) \end{gathered} \tag{4.11}$$

$$\begin{gathered} NesprejemljiviVplivi(P_k, SegmentJavnosti_l, t) = \\ Vpliv(P_k, SegmentJavnosti_l, t) - SprejemljiviVplivi(P_k, SegmentJavnosti_l, t) \end{gathered} \tag{4.12}$$

Tabela 4.1: Objektivne negotovosti glede na posamezna tveganja in javnosti

	SJ_1	SJ_2	SJ_3
R_1	M	M	Ø
R_2	S	S	Ø
R_3	M	M	Ø

$$NesprejemljivaStanja(P_k, SegmentJavnosti_l, t) = Stanje(P_k, SegmentJavnosti_l, t) - SprejemljivaStanja(P_k, SegmentJavnosti_l, t) \tag{4.13}$$

Primer Za poslovni proces A (glej sliko 4.1) naj za vse opazovane javnosti velja, da se tveganja in meje sprejemljivosti tveganj skozi čas ne spreminjajo. Tveganja, ki jih spremljajo, naj bodo:

1. R_1 – Prispeli dokument ima slabo kakovost.
2. R_2 – Zamuda pri pregledovanju, preusmerjanju in zavračanju dokumentov.
3. R_3 – Napačno usmerjen dokument.

Posamezne opazovane javnosti so:

1. SJ_1 – Zaposleni, ki izvajajo poslovni proces A.
2. SJ_2 – Lastniki poslovnega procesa A.
3. SJ_3 – Uporabniki poslovnega procesa A.

Objektivna in subjektivna negotovost, izpostavljenost ter tveganja naj imajo zalogo štirih vrednosti: Ø – ni vrednosti, M – relativno male vrednosti, S – srednje vrednosti, V – relativno velike vrednosti. Kljub temu, da so oznake enake, imajo različen pomen za negotovosti, izpostavljenost in tveganje. V tabelah od 4.1 do 4.3 so primeri vrednosti, ki jih v primeru modeliranja spreminjamo.

Z enačbo (4.1) računamo tveganja, ki jih za dani primer prikazuje tabela 4.4. Funkcija Φ_{RC} je v tem primeru poenostavljena tako, da izračuna tveganje kot najslabšo možnost v kartezičnem produktu med objektivno in subjektivno negotovostjo ter med izpostavljenostjo.

Tabela 4.2: Subjektivne negotovosti glede na posamezna tveganja in javnosti

	SJ_1	SJ_2	SJ_3
R_1	Ø	M	M
R_2	Ø	V	V
R_3	Ø	S	V

Tabela 4.3: Izpostavljenost glede na posamezna tveganja in javnosti

	SJ_1	SJ_2	SJ_3
R_1	M	S	M
R_2	M	S	V
R_3	S	V	V

Tabela 4.4: Izračunana tveganja glede na posamezne javnosti

	SJ_1	SJ_2	SJ_3
R_1	M	S	M
R_2	S	V	V
R_3	S	V	V

Tabela 4.5: Sprejemljiva tveganja za posamezne javnosti

	SJ_1	SJ_2	SJ_3
R_1	M,S	M,S	M,S
R_2	M,S	M,S	M,S,V
R_3	M	M	M,S

Če bi bila meja sprejemljivosti takšna, da bi bila sprejemljiva tveganja, kot jih opisuje tabela 4.5, bi bilo tveganje R_3 nesprejemljivo za vse javnosti, medtem ko bi bila ostala tveganja sprejemljiva, tveganje R_2 pa za javnost SJ_2.

V praksi bi se morali odločiti, kaj s temi tveganji storiti. V primeru, da bi jih želeli zmanjšati, bi bilo potrebno izvesti ukrepe za zmanjšanje negotovosti in/ali izpostavljenosti.

Na podoben način bi izračunali tudi notranja stanja in vplive ter jih ocenili glede na njihovo mejo sprejemljivosti.

Poglavje 5

Katalog tveganj v oskrbovalni verigi

Organizacije v današnjem času ne morejo delovati v izolirano varnem okolju brez tveganj, ki izhajajo iz oskrbovalnih verig. Še posebej lahko to trdimo zaradi trendov globalizacije in globalnega oskrbovanja, ki se pojavljajo v zadnjih letih in postajajo vedno bolj aktualni. Tveganja, ki izhajajo iz logistike in oskrbovalnih verig, postajajo glavna skrb v današnjih logističnih in oskrbovalnih procesih v vseh organizacijah. Posledično lahko trdimo, da je proces upravljanja tveganj ključnega pomena za neprekinjeno delovanje organizacij na vseh področjih delovanja. Najverjetneje je tveganja najlažje razumeti, če si jih predstavljamo v luči koncepta investicij. Te so baza vsake poslovne aktivnosti – omogočajo vzdrževanje, povečujejo obseg poslovanja ali omogočajo spremembe v poslovnih aktivnostih [5, 14, 15, 19, 20] – in hkrati vključujejo tveganja in njihovo upravljanje kot ključni faktor v operacijskih aktivnostih; praktično ni investicij brez tveganj.

Tveganja so integrirana v naša življenja, zdi se, kot da ljudje nikoli prej nismo posvečali toliko pozornosti izzivom, ki jih prinašajo tveganja, kot to počnemo danes. Veliko člankov, prispevkov in pogovorov se vrti okoli tematike tveganj, posledično obstaja veliko idej in predstav o tem, kaj tveganje sploh je in kaj predstavlja, kar kaže na kompleksnost problema, ki se pojavi, ko se nekdo loti obsežnega upravljanja tveganj.

Če se naslonimo na model upravljanja tveganj, kot nam ga nudi ISO 31000, vidimo, da so procesi, ki so vključeni v ocenjevanje tveganj, še posebej prepoznavanje in analiza tveganj, najbolj ključni v celotnem procesu upravljanja tveganj. Zavedati se je potrebno, da tveganja, ki niso zaznana v procesu prepoznavanja tveganj, tudi kasneje niso obravnavana in vključena v upravljanje tveganj, torej so spregledana in se nanje ne moremo pripraviti. Prav zaradi tega smo na Fakulteti za logistiko razvili model za učinkovito ocenjevanje tveganj v organizacijah. Pilotno testiranje modela je potekalo v sodelova-

nju s podjetjem, ki deluje pretežno na področju skladiščenja, nadaljnja testirana pa še na dodatnih organizacijah in oskrbovalnih verigah iz prakse. Rezultat teh testiranj je obsežen katalog prepoznanih tveganj, kjer je vsako tveganje uvrščeno v kategorije po različnih dimenzijah, ki jih bomo podrobneje razložili v nadaljevanju. Ker je bilo testiranje v organizacijah zelo dobro sprejeto, lahko sklepamo, da smo na pravi poti za dosego našega cilja, ki je razviti široko uporaben model za upravljanje tveganj v oskrbovalnih verigah. Dodaten cilj predstavlja tudi dopolnjevanje spletnega kataloga tveganj, ki je objavljen pod Creative Commons licenco, kar dovoljuje vsem uporabnikom kataloga, da ga prosto uporabljajo pri svojem delu ter z idejami, predlogi in dopolnitvami sodelujejo pri njegovem nastajanju.

5.1 Model za ocenjevanje tveganj

Prvi korak pri procesu ocenjevanja tveganj je vedno prepoznavanje le-teh. Ta proces mora biti izpeljan zelo pazljivo ter biti čim bolj obsežen, da s tem zagotovimo prepoznanje čim več tveganj in se izognemo spregledu pomembnih tveganj. V modelu je proces prepoznavanja tveganj podprt s tremi metodami, ki jih priporoča tudi standard ISO 31010, to so odprt intervju, strukturiran intervju in vodeno viharjenje možganov (brainstorming). Usposobljeni strokovnjaki vodijo srečanja z zaposlenimi v določeni organizaciji, kjer je poudarek na prepoznavanju tveganj. Ta tveganja so kasneje umeščena v model preko kategorizacije po različnih dimenzijah ter opisana.

Ker verjamemo, da sta prepoznavanje in analiza tveganj ključna procesa pri upravljanju tveganj, smo v model uvrstili več dimenzij, ki pomagajo pri opisovanju in definiranju tveganj in posledično omogočajo informiran pristop k upravljanju tveganj. Ko je posamično tveganje prepoznano, ga z uvrstitvijo v posamezne dimenzije definiramo po temeljnih dimenzijah, ki so vključene v model. Kasneje v procesu je potrebno uvesti še dodatne dimenzije, ki so specifične za vsako organizacijo, torej jih v katalog tveganj, ki ga izdelujemo, nismo uvrstili. Takšne kompleksnejše dimenzije opisa tveganj so na primer odnosi in medsebojni vplivi med tveganji, specifične posledice, ki jih lahko organizaciji prinese uresničitev posameznega tveganja in podobno.

5.1.1 Segmentiranje tveganj po ISO 28000

Model, ki smo ga ustvarili, in tudi katalog, ki iz njega izvira, sta strukturirana tako, da sta komplementarna standardu za zagotavljanje varnosti v oskrbovalnih verigah ISO

28000 in je opisan v tretjem poglavju. V tem standardu je definiranih več področij, kjer se lahko tveganja pojavljajo v organizaciji ali znotraj njene oskrbovalne verige. V prvem koraku procesa ocenjevanja tveganj, kot smo ga zastavili v našem modelu, se tveganja razvrstijo v skupine po ISO 28000, ki so:

1. Tveganja fizičnih odpovedi, kot npr. funkcionalne odpovedi opreme, naključne odpovedi, zlonamerne poškodbe, teroristična ali kriminalna dejanja.
2. Operativna tveganja, ki vključujejo nadzor varnosti, človeškega faktorja in ostale aktivnosti, ki vplivajo na uspešnost, stanje in varnost organizacije.
3. Naravni okoljski dogodki (nevihte, poplave itd.), zaradi katerih lahko varnostni ukrepi in prema postanejo manj učinkoviti.
4. Faktorji, ki niso pod nadzorom organizacije, kot npr. odpoved opreme ali storitev, ki jih izvajajo zunanji ponudniki.
5. Tveganja vseh zainteresiranih udeležencev organizacije, npr. nedoseganje regulatornih zahtev ali zmanjšan ugled blagovne znamke.
6. Načrtovanje in instalacija varnostne opreme, vključujoč menjavo, vzdrževanje itd.
7. Upravljanje informacij, podatkov in komunikacije.
8. Grožnje kontinuiteti delovanja.

Opis nekega tveganja po dimenziji skupin ISO 28000 predstavlja prvo skupino opisov, ki jih zajema spletni katalog tveganj. Ker so nekatera tveganja bolj kompleksna, jih ne moremo uvrstiti v samo eno skupino, zato so nekatera tveganja uvrščena v dve skupini – primarno in sekundarno.

5.1.2 Segmentiranje tveganj glede na vpliv na sredstva logistike

Pri analiziranju logističnih tveganj se moramo zavedati, da znotraj logističnih procesov in procesov v oskrbovalnih verigah obstaja več sredstev oziroma virov, ki so ključni za izvajanje logistike. Na podlagi raziskav ter posvetovanj s strokovnjaki s področja logistike smo za potrebe modela in kataloga sestavili seznam štirih primarnih virov, brez katerih logistični procesi ne morejo potekati. Ti so:

1. Tok blaga in/ali storitev mora biti upravljan od izvorne točke do porabne točke z namenom doseganja pričakovanj kupcev in potrošnikov.

2. Informacije so podatki (v vseh oblikah), ki predstavljajo vnos v informacijski sistem, ki jih obdela in tvori izhodne informacije, kot jih potrebuje organizacija [12].

3. Logistični infrastruktura in suprastruktura kot osnovne fizične in organizacijske strukture, ki so potrebne za logistične operacije.

4. Ljudje so osebje, ki je potrebno za načrtovanje, organiziranje, pridobivanje, uvajanje, dostavljanje, podporo, nadzorovanje in ocenjevanje logističnih sistemov in storitev. Lahko so notranji, zunanji ali pogodbeni, odvisno od potreb organizacije.

Vsaka posledica tveganj, ki se pojavljajo v oskrbovalnih verigah, lahko vpliva na enega ali več sredstev logistike. Če želimo učinkovito upravljati tveganja, se je potrebno zavedati, na katere vire ima posamezno tveganje vpliv. Ravno zato smo v model uvrstili kategorijo, ki te vplive definira. Prav tako kot s kategorijami po ISO 28000 tudi v tej kategoriji velja, da lahko posamezno tveganje vpliva na več kot eno sredstvo logistike, zato smo tudi pri tej kategoriji uvedli še kategorijo sekundarnega vpliva na sredstva logistike.

5.1.3 Segmentacija tveganj glede na nosilce tveganj – javnosti

Segmenti javnosti so skupine ljudi, ki jih lahko identificiramo na podlagi njihovega zanimanja za, odnosa do, ali trenutnega obnašanja glede na neko vprašanje. Kot takšne lahko ljudi (razdeljene na posamične javnosti) razumemo kot najpomembnejši del okolja, ki ga obravnavamo v procesu upravljanja tveganj. Pristop, kjer segmenti javnosti igrajo ključno vlogo pri upravljanju tveganj, je nov v znanstveni tehnično orientirani literaturi.

Ker je vsak človek edinstven in drugačen od ostalih, se lahko tudi posameznikov odnos do nekega tveganja, s katerim se srečuje, zelo razlikuje od odnosov ostalih do istega tveganja. Ravno zaradi tega imajo ljudje različne odnose in poglede na enako tveganje, kar je lahko rezultat različnih izpostavljenosti kot tudi različnih ocenjenih stopenj negotovosti. Ta problem najpogosteje gledamo ne na primeru posameznika, temveč na primeru posameznih skupkov ljudi, ki si delijo podobne značilnosti oziroma odnose do nekega tveganja, to so segmenti javnosti.

Naš pristop temelji na predpostavki, da je tveganje sestavljeno kot je opisano v prejšnjih poglavjih. S takšnim pristopom v modelu, in to v realnem primeru, opisujemo in

ocenjujemo tveganja in njihove vplive drugače kot večina današnje literature. Temeljimo na že opisaneni predspostavki, da lahko samo živa bitja čutijo in razumevajo sama sebe, medtem ko neživa bitja tega niso sposobna. Ugotovimo lahko , da v končni fazi tveganja prizadenejo samo ljudi, katerih značilnost je dojemljivost za razumevanje. V skladu s to teorijo v modelu vse ljudi, ki so deležniki v oskrbovalni verigi ali njenem okolju, segmentiramo na javnosti, to je na skupine ljudi s skupnimi interesi ali funkcijami, seveda z ozirom na določeno tveganje. Ko opisujemo tveganja v našem modelu, ena dimenzija predstavlja natančno to – opis, katere javnosti določeno tveganje prizadene. Ta teorija je v skladu z ISO 31000, kjer je kot eden izmed ključnih načel pri upravljanju tveganj opisano načelo: 'upravljanje tveganj upošteva človeške in kulturne faktorje. Prepoznava sposobnosti, razumevanje in namere zunanjih in notranjih ljudi, ki lahko pripomorejo ali zavirajo doseganje ciljev organizacije' [7]. Prav tako standard definira pomembnost komuniciranja in posvetovanja z deležniki organizacije, kar naš model dosega prav z segmentiranjem javnosti. ISO 31000 to pomembnost opisuje: 'Komunikacija in posvetovanja z deležniki je pomembna, saj le-ti ocenjujejo tveganja glede na svoje percepcije tveganja. Te percepcije se lahko razlikujejo zaradi različnih vrednot, potreb, domnev, konceptov in skrbi deležnikov. Ker lahko imajo njihovi pogledi ključen vpliv na sprejemanje odločitev, morajo biti deležnikove percepcije prepoznane, zapisane in upoštevane v procesu odločanja.' [7]

5.1.4 Segmentiranje tveganj glede na izvor

Oskrbovalna veriga je kompleksen sistem več organizacij, ki skupaj delujejo v določenem okolju, kjer se 'srečujejo z zunanjimi in notranjimi vplivi in faktorji, ki vplivajo na negotovost glede doseganja ciljev organizacije' [7]. Na podlagi obsega izvora posameznega tveganja lahko tveganja razdelimo po naslednji dimenziji, to je glede na izvor. V tej dimenziji tveganja delimo na skupine, ki izhajajo iz:

1. Opazovane organizacije, ki je vključena v oskrbovalno verigo;
2. Celotne opazovane oskrbovalne verige (ampak ne samo iz določene organizacije); ali
3. Iz zunanjega okolja, v kateri deluje oskrbovalna veriga.

Vsaka organizacija je odvisna od več tretjih oseb oziroma zunanjih organizacij. Kot del oskrbovalne verige je organizacija navadno tesno povezana in odvisna od drugih organizacij v določeni oskrbovalni verigi, manj pa z organizacijami zunaj nje. Zatorej mora

vsaka organizacija razumeti, da imajo nanjo organizacije, ki so povezane v oskrbno verigo, določen vpliv, prav tako je opazovana organizacija vpliva na ostale organizacije v verigi. Zavedati se je potrebno, kot pravi tudi Andrew Steward, da odvisnosti same tudi pomenijo tveganje, saj po definiciji drži, da če smo odvisni od nekoga, lahko ta deluje tako, da bodo posledice tega delovanja imele negativni učinek na nas [25]. Isti avtor prepoznava tudi dejstvo, da odvisnosti pogosto niso prepoznane kot tveganja in jih ne upoštevamo v procesu ocenjevanja tveganj ali jih ignoriramo zaradi političnih razlogov; ta tveganja so hkrati bolj subtilna in se pojavljajo samo pri analizi poslovnih procesov, ne pa pri analizi tehnoloških komponent ali infrastrukture.

5.1.5 Segmentiranje tveganj glede na poslovno ali tehnološko dejavnost

Vse dejavnosti znotraj organizacije lahko opišemo kot pretežno tehnološke ali pretežno poslovne. V skladu s tem lahko tudi tveganja opišemo kot pretežno poslovna ali pretežno tehnološka, neizogibno pa se pojavijo tudi nekatera tveganja, ki imajo značilnosti obeh, torej jih opišemo kot univerzalna. Ta opis predstavlja še dodatno dimenzijo v našem modelu.

Seznam prepoznanih tveganj, njihove definicije po dimenzijah in dodatni opisi skupaj tvorijo bazo za katalog tveganj v oskrbovalnih verigah, ki je prosto dostopen in objavljen na internetu. Katalog je podrobneje opisan v nadaljevanju.

5.1.6 Nadaljnje definicije, ki so potrebne pri procesu ocenjevanja tveganj

Kot smo že omenili, so v procesu prepoznavanja, analize in ocenjevanja tveganj v specifični organizaciji potrebne še dodatne dimenzije, ki jih moramo uvesti, da dosežemo popolno razumevanje tveganj, njihovih povezav in vplivov. Te dimenzije so kratko opisane v nadaljevanju, v domeni vsake posamezne organizacije, ki se loteva ocenjevanja tveganj s pomočjo našega modela pa je, da jih implementira.

Zavedati se je potrebno, da so oskrbovalne verige prav tako raznolike kot današnji trg potrošnih dobrin. Na podlagi tipa dobrin ali storitev, ki jih dobavlja oskrbna veriga, lahko tveganja definiramo po dodatni dimenziji. Nekatera tveganja se pojavljajo univerzalno v vseh oskrbovalnih verigah, nekatere oskrbovalne verige pa imajo svoja specifična tveganja, na primer hladne verige, proizvodnja in prodaja nevarnih snovi in podobno.

Pri vrednotenju tveganj moramo med drugim definirati tudi njihov vpliv na specifične javnosti. Zavedati se je potrebno, da vsako tveganje na svoj način vpliva na neko javnosti ter da ta vpliv vsaka javnost drugače sprejema. Z analizo vplivov z ozirom na javnosti dosežemo boljši vpogled v posledice tveganja. Tu ne gre za isto dimenzijo ali isti postopek kot pri sami segmentaciji javnosti – ta dimenzija je poglobljena in išče tudi vplive in učinke tveganja na javnosti.

V realnih situacijah so tveganja in njihovi vplivi velikokrat odvisni od časa, v katerem se pojavijo. Zato mora model za ocenjevanje tveganj vključevati tudi dimenzijo časa, ki v proces prinaša nedeterminizem. V nekaterih časovnih okvirjih je lahko tveganje neznatno, medtem ko je isto tveganje v drugem časovnem okvirju ključno za uspešno poslovanje organizacije. V kolikor so takšni časovni okvirji prisotni, morajo biti v fazi ocenjevanja tveganj definirani, da pridobimo pregled nad spreminjanjem tveganja skozi čas.

Za vsako tveganje je potrebno določiti mejo sprejemljivosti. Pri tem moramo upoštevati tudi časovno komponento, kjer je prisotna, da polno zajamemo vse nivoje potencialnega vpliva in znotraj njih pravilno določimo mejo sprejemljivosti.

Prepoznati moramo, da noben proces v organizaciji ne more potekati neodvisno od ostalih procesov. Enako velja za katero koli tveganje – nikoli ne obstaja tveganje, ki je izolirano in nima vpliva na procese znotraj organizacije in tudi znotraj oskrbovalne verige. Zato je potrebno definirati medsebojne odvisnosti med tveganji, kar predstavlja naslednjo dimenzijo organizacijsko specifičnega definiranja tveganj.

Splošna ideja upravljanja tveganj je, da mora imeti vsako prepoznano tveganje dodeljeno osebo ali skupino ljudi, ki so zadolženi za njegovo upravljanje in jih po navadi imenujemo lastniki tveganja. ISO 31000 definira lastnika tveganja kot „osebo ali entiteto z odgovornostjo in avtoriteto za upravljanje tveganja". Hkrati definira, da „mora organizacija zagotoviti, da obstajajo odgovornost, avtoriteta in primerne kompetence za upravljanje tveganj, ki omogočajo uvajanje in vzdrževanje kontrol za upravljanje tveganj in zagotavljajo primernost, učinkovitost in uspešnost teh kontrol." [7]. Z določitvijo specifične osebe, ki je odgovorna za določeno tveganje, dosežemo višjo stopnjo zavedanja pri tistih, ki morajo biti vključeni v proces upravljanja tveganj znotraj organizacije ali oskrbovalne verige.

5.2 Katalog tveganj v oskrbovalnih verigah

Končni produkt konvencionalnega prepoznavanja in ocenjevanja tveganj je katalog tveganj v oskrbovalnih verigah [18], ki vsebuje vsa prepoznana in opisana tveganja v določeni

organizaciji. Težimo k temu, da vsa ta tveganja zberemo v katalog, ki je razširjen na raven celotne oskrbovalne verige oziroma na raven več oskrbovalnihih verig in je hkrati javno dosegljiv preko objavljenega spletnega kataloga tveganj v oskrbovalnih verigah, s čimer postane pomembno in uporabno orodje pri upravljanju tveganj. Proces upravljanja tveganj je velikokrat počasen in ne dovolj natančen, naša ideja prosto dostopnega kataloga vseh do sedaj prepoznanih tveganj pa organizacijam nudi možnost, da pri procesu uporabijo tudi zunanja znanja, ko se lotevajo upravljanja tveganj. Katalog tveganj vsebuje logistična tveganja, ki so bila prepoznana v organizacijah z različnih področij delovanja, ravno zato je lahko odličen vir informacij za širok spekter organizacij, ki pristopajo k upravljanju tveganj, saj ga lahko uporabljajo kot smernice za prepoznavanje tveganj in kot kontrolni seznam ali odkljuknico, s katero ugotovijo, katera od že identificiranih tveganj lahko prepoznajo tudi znotraj svoje organizacije. Uporabo odkljuknice kot pripomočka pri ocenjevanju tveganj priporoča tudi standard ISO 31010, ki jo definira kot „seznam nevarnosti, tveganj ali napak pri kontrolah , ki je navadno sestavljen na podlagi izkušenj, najsi bo kot rezultat prejšnjih procesov upravljanja tveganj ali kot rezultat preteklih napak ali škodnih dogodkov" [8]. Na podlagi tega lahko ugotovimo, da je katalog, ki ga uvajamo, v skladu z načeli ISO 31010 in s celotno družino ISO 31000 standardov.

Potreba po takšnem katalogu logističnih tveganj je lahko vidna iz različnih perspektiv. Tudi ISO 31000 definira končni rezultat procesa prepoznavanja tveganj kot „obsežen seznam tveganj, ki vključuje dogodke, ki lahko povzročijo, povečajo, preprečijo, poslabšajo, pospešijo ali povzročijo zamudo pri doseganju ciljev organizacije" [7]. Organizacija lahko pristopi k procesu upravljanja tveganj samostojno, vendar velikokrat zaradi prevelikega obsega potrebnih aktivnosti k njemu ne pristopijo in se odločijo, da bodo obstoj tveganj in njihovo upravljanje spregledali. S pomočjo kataloga kot vira izkušenj in odkljuknice je velik korak v procesu ocenjevanja tveganj že narejen, kar omogoča organizaciji pristop k celovitemu upravljanju tveganj z manj preprekami in z več znanja. Vidimo lahko, da katalog, ki je trenutno edinstven v svetu, predstavlja ključen napredek pri upravljanju tveganj v logistiki na svetovnem nivoju.

Ker verjamemo, da mora biti vir s takšno pomembnostjo prosto dostopen vsem potencialnim uporabnikom, je objavljen pod licenco Creative Commons, ki uporabnikom dovoljuje, da katalog prosto gledajo, nalagajo in delijo, ne smejo pa ga spreminjati brez odobritve in uporabljati za pridobitne namene, seveda pa morajo pri tem primerno navesti avtorja kataloga. Licenca, pod katero je objavljen, se imenuje 'Attribution – NonCommercial – NoDerivs. Ker je naša filozofija za katalogom takšna, da je to publikacija, ki

iz dneva v dan raste in se spreminja, verjamemo, da je potrebno omogočiti vsem uporabnikom, da h katalogu prispevajo, ga komentirajo ali predlagajo dodatke. Zato vse uporabnike spodbujamo, da svoje predloge posredujejo uredniškemu odboru, ki predloge oceni in jih nato vnese v katalog, če so primerni. Pripombe se sprejemajo preko elektronskega naslova SC.RiskCatalog@gmail.com. Upamo, da bomo s tem dosegli širok interes za uporabo kataloga med strokovnjaki s področja oskrbovalnih verig, hkrati pa dodatno povečali njegovo kakovost in obseg. Vsak vodilni v oskrbovalnih verigah se mora zavedati pomembnosti sodelovanja med organizacijami. Ena sama organizacija nikoli ne more prepoznati toliko tveganj, kot jih lahko skupina organizacij, še posebej kadar govorimo o tveganjih v oskrbovalnih verigah. Naš cilj je zato povezati strokovnjake s celega sveta in vzpostaviti skupnost z enotnim ciljem – zagotavljati nova znanja na področju ocenjevanja logističnih tveganj in izpolnjevati katalog tveganj.

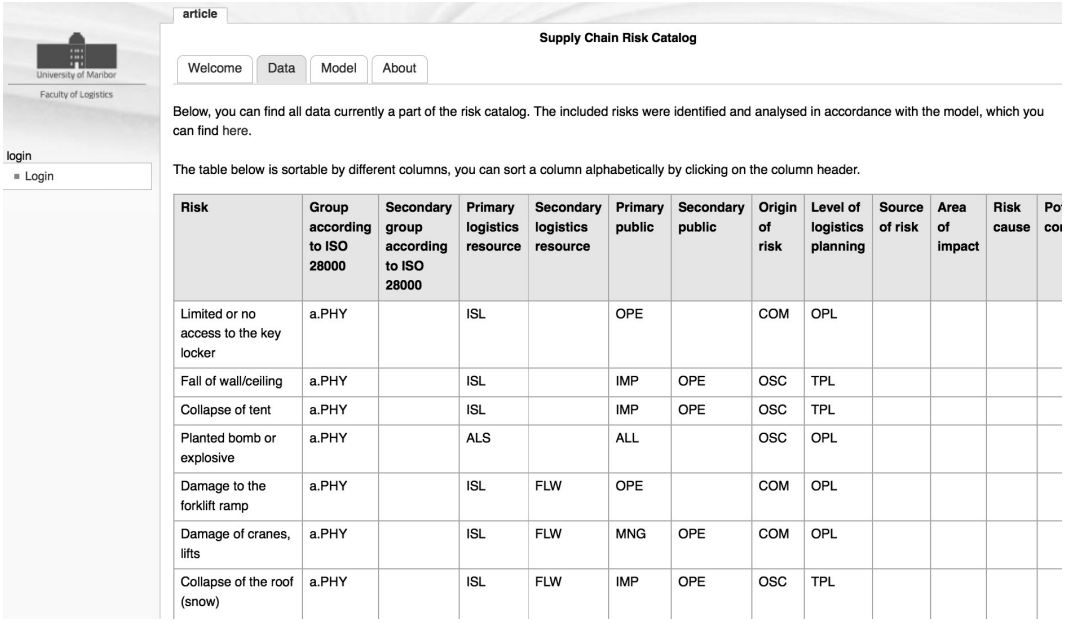
Katalog je dosegljiv na spletnem naslovu http://labinf.fl.uni-mb.si/risk-catalog. Tu je podan obsežen seznam do sedaj prepoznanih tveganj, ki so opisana po zgoraj definiranih dimenzijah. Dodatno so podani opisi dimenzij in šifranti kategorizacije. Pri vsaki šifri kategorije znotraj dimenzije so podana tudi vsa tveganja, ki se uvrščajo v to kategorijo, da je katalog lažje pregleden tudi po posameznih kategorijah.

Spletna stran kataloga vsebuje štiri zavihke. Prvi je pozdravni (Welcome) z osnovnimi informacijami o katalogu. Drugi predstavlja podatke (Data), kjer so navedena vsa zaznana tveganja. Seznam teh tveganj se sproti dopolnjuje. Tveganja je mogoče sortirati po vseh kategorijah. Sledi zavihek z opisom modela (Model). Zadnji vsebuje vse ključne informacije o samem katalogu – to je kolofon kataloga, o Creative Commons License in s povabilom za sodelovanje pri dopolnjevanju kataloga s podatki in razvijanjem modela.

Slika 5.1 prikazuje del zavihka s podatki o tveganjih, medtem ko slika 5.2 prikazuje del strani, kjer je opsian sam model, na katerem je katalog izdelan.

5.3 Zaključna diskusija o Katalogu

Na podlagi današnjih negotovih tržnih pogojev, zahtev globalizacije in vedno večjih zunanjih groženj lahko zaključimo, da lahko samo z učinkovitim upravljanjem tveganj v oskrbovalnih verigah zagotovimo kontinuiteto poslovanja organizacije. Upravljanje tveganj mora predstavljati prioriteto v vsaki organizaciji in mora biti vključeno v vse vidike poslovanja, če želimo zagotoviti njegovo uspešnost in učinkovitost. Vodilni se morajo zavedati groženj, ki pretijo organizaciji, prav tako pa morajo poznati in implementirati orodja, s katerimi jih lahko upravljamo in obvladujemo.



Risk	Group according to ISO 28000	Secondary group according to ISO 28000	Primary logistics resource	Secondary logistics resource	Primary public	Secondary public	Origin of risk	Level of logistics planning	Source of risk	Area of impact	Risk cause	Po co
Limited or no access to the key locker	a.PHY		ISL		OPE		COM	OPL				
Fall of wall/ceiling	a.PHY		ISL		IMP	OPE	OSC	TPL				
Collapse of tent	a.PHY		ISL		IMP	OPE	OSC	TPL				
Planted bomb or explosive	a.PHY		ALS		ALL		OSC	OPL				
Damage to the forklift ramp	a.PHY		ISL	FLW	OPE		COM	OPL				
Damage of cranes, lifts	a.PHY		ISL	FLW	MNG	OPE	COM	OPL				
Collapse of the roof (snow)	a.PHY		ISL	FLW	IMP	OPE	OSC	TPL				

Slika 5.1: Izsek strani na zavihku s podatki v Katalogu tveganj oskrbovalnih verig

Naš model za ocenjevanje tveganj dovoljuje vodilnim, da k upravljanju tveganj pristopijo na poenostavljen način, kjer so vsi potrebni koraki opisani, hkrati pa že imajo tudi razdelan osnovni seznam potencialnih tveganj. Spletni katalog tveganj v oskrbovalnih verigah, ki je prosto dostopen vsem, uporabnikom nudi enostavno odkljuknico s tveganji, kot so jih prepoznali in definirali strokovnjaki s področja logistike. Med ocenjevanjem tveganj v specifični organizaciji je potrebno dodati še nekaj dimenzij, ki jih ni mogoče posplošiti in zatorej niso v obsegu kataloga. S tem dosežemo dodatno razumevanje tveganj in boljši izhodiščni vhod v procese upravljanja tveganj. Verjamemo, da razvit model in posledični katalog, še posebej z uvedbo težišča na ljudi in javnosti, predstavljata izjemen vir za upravljanje tveganj v vseh organizacijah in oskrbovalnih verigah.

Ker verjamemo, da lahko skupina strokovnjakov v večjem obsegu zagotovi potrebna znanja in izkušnje, na podlagi katerih lahko izpopolnimo model in katalog, je spletni katalog z opisom modela prosto dostopen preko spleta. Managerje in ostale strokovnjake s področja logistike in upravljanja tveganj spodbujamo, naj pri svojem delu uporabljajo katalog, v zameno pa nam sporočijo svoje pripombe, ideje in dopolnitve, da bomo skupaj dosegli vedno boljši in popolnejši spletni katalog tveganj v oskrbovalnih verigah.

Risk analysis is the second step in risk assessment, where the risk catalog also represents a valuable resource for organizations. ISO 31000 defines the purpose of risk analysis as developing an understanding of the risk. In our model, risks are described by different dimensions which define their attributes and provide information about general risk properties. We also propose some organization specific dimensions of definig risks during risk analysis, which every organization has to define in the frame of its specific external and internal context.

Risk evaluation as the final step of risk assessment as defined in ISO 31000 is the process of deciding about which risks need treatment and the priority for treatment implementation. This step can not be generalized and is therefore not in the scope of this risk catalog, but is entirely dependant on specific organizations.

Risk catalog

With our model we developed a tool for companies that are prepared to combine internal and external knowledge for identifying and defining risks.

The Risk catalog that represents the final product of this process, can be a permanent and valuable tool for a company's and supply chain's risk management processes. The catalog has to be examined and complemented on a regular basis to ensure actuality. It provides a base for risk management processes throughout the chain.

The current catalog with its identified risks is accessible here.

Dimensions of risk definition

List of groups by ISO 28000

This model is structured so that it complements an international standard on security in supply chains, ISO 28000. In this standard, several fields from where risks to a company or a supply chain can originate are defined. Each identified risk is placed in one of these groups.

Code	Description
PHY	Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action.
OPT	Operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety.
NAT	Natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective.

Slika 5.2: Izsek strani na zavihku z opisom modela v Katalogu tveganj oskrbovalnih verig

Literatura

[1] BusinessDictionary.com. Risk. `http://www.businessdictionary.com/definition/risk.html`, nov 2014. [Online; accessed 21. november 2014].

[2] Adam Greene. A process approach to project risk management. *Department of Civil and Building Engineering, Loughborough University*, 2009. [Online; accessed 21. november 2014].

[3] Glyn A. Holton. Defining risk. *Financial Analyst Journal*, 60(6), 2004.

[4] InvestorWords.com. Risk. `http://www.investorwords.com/4292/risk.html`, nov 2014. [Online; accessed 21. november 2014].

[5] *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0.* IT Governance Institute, 2008.

[6] ISO. *ISO 28000:2007; Specification for security management systems for the supply chain.* ISO, 2007.

[7] ISO. *ISO 31000:2009; Risk management – Principles and guidelines.* ISO, 2009.

[8] ISO. *ISO 31010:2009; Risk management – Risk assessment techniques.* ISO, 2009.

[9] ISO. *ISO Guide 73:2009; Risk management – Vocabulary.* ISO, 2009.

[10] ISO. *ISO/IEC 27005:2011; Information technology – Security techniques – Information security risk management.* ISO, 2011.

[11] ISO. *ISO/IEC 27001:2013; Information technology – Security techniques – Information security management systems – Requirements.* ISO, 2013.

[12] Borut Jereb. Zadolževanje informacijskih virov. pages 237–24. Ljubljana: Slovenski inštitut za revizijo, 2002. 10. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[13] Borut Jereb. Segmenting risks in risk management. pages 465–475. Ljubljana: Slovenian Society Informatika, Section for Operational Research, 2008. Celje; Krško: Faculty of Logistics, 2008.

[14] Borut Jereb. Upravljanje it investicij. pages 7–22. Ljubljana: Slovenski inštitut za revizijo, 2008. 16. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[15] Borut Jereb. Upravljanje it investicij s pomočjo val it. Ljubljana: Slovensko društvo Informatika, 2008. Dnevi slovenske informatike 2008 - DSI, Portorož, Slovenija, 09.-11. april.

[16] Borut Jereb. Princip modeliranja tveganj s segmentacijo javnosti pri upravljanju procesov. *Uporabna informatika*, 18(2):90 – 100, 2010.

[17] Borut Jereb. Risk assessment model respecting segments of the public. *Montenegrin journal of economics*, 9(3):75–94, 2013.

[18] Borut Jereb and Tina Cvahte. Risk catalog. `http://labinf.fl.uni-mb.si/risk-catalog`, 2012. [Online; accessed 25. november 2014].

[19] Borut Jereb, Tina Cvahte, and Bojan Rosi. Val it v logistiki = val it in logistics. *Economics & economy*, 1(2):91–109, 2013.

[20] Borut Jereb, Teodora Ivanuša, and Bojan Rosi. Systemic thinking and requisite holism in mastering logistics risks : the model for identifying risks in organisations and supply chain. *Amfiteatru economic*, 15(33):56–73, 2013.

[21] Borut Jereb and Mateja Škornik. Upravljanje informacijskih tveganj po iso/iec 27005:2008. pages 9–28. Ljubljana: Slovenski inštitut za revizijo, 2009. 17. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[22] Frank Knight. *Risk, Uncertainty, and Profit.* New York: Hart Schafner, and Marx, 1921.

[23] Johnathan Mun. *Modeling Risk: Applying Monte Carlo Simulation, Real Options Analysis, Forecasting, and Optimization Techniques.* Wiley - Finance, 2006.

[24] Steven J. Ross. Four little words. *ISACA Journal*, 1, 2009.

[25] Andrew Steward. On risk: Perception and direction. *Computers & Security*, 23:362–370, 2004.

[26] Risk. `https://en.wikipedia.org/wiki/Risk`, nov 2014. [Online; accessed 21. november 2014].