Kako obvladovati tveganja v organizacijah - vzpostavitev procesa obvladovanja tveganj po standardu ISO 31000

Borut Mozetič

e-pošta: borut.mozetic@letrika.com

Povzetek:

Čeprav ugotovitve raziskav kažejo, da je praksa celovitega obvladovanja tveganj v organizacijah tako v Sloveniji kot tudi tujini še vedno premalo prisotna, je celovito obvladovanje tveganj zagotovo dobra in koristna praksa. Dokazano pripomore h krepitvi stabilnosti pogojev za uspešnejše poslovanje organizacij, krepitvi njihovih konkurenčnih prednosti, ugleda in zaupanja vanje. Praksa celovitega obvladovanja tveganj se čedalje bolj uveljavlja kot sestavni del poslovnega načrtovanja, strategij, vodenja, politik in nadzora v organizacijah. Namen tega prispevka je opozoriti na pomen obvladovanja tveganj v organizaciji in prikazati pristop vzpostavitve sistema celovitega obvladovanja tveganj v organizaciji po standardu ISO 31000.

Ključne besede: tveganje, celovito obvladovanje tveganj v organizaciji, ISO 31000, register tveganj

1 Uvod

V poslovnem okolju smo priča veliki dinamiki dogajanj. Nenehne in hitre spremembe se pod vplivom globalizacije in informatizacije širijo na vsa poslovna področja. Bistveno se je razširil spekter poslovnih priložnosti, hkrati pa okrepila konkurenca in zahtevnost obvladovanja vse bolj kompleksnega poslovnega okolja. Podjetja poskušajo izkoristiti poslovne izzive s ciljem zagotavljanja lastnega razvoja, rasti in zadovoljitve drugih pričakovanj lastnikov. Izzivi pa prinašajo s seboj tudi tveganja. Tako se morajo podjetja kakor tudi druge organizacije nenehno prilagajati novim razmeram v poslovnem okolju in se izogibati nevarnostim, ki bi lahko ogrozile zastavljene cilje ali celo njihov obstoj.

Ali lahko vplivamo na izpostavljenost tveganju? Kako se izogniti tveganjem? Kako poskrbeti, da bo organizacija čim manj izpostavljena tveganjem? V skladu z navedbami v strokovni literaturi (Hopkin, 2010; Jorion, 2000; Norman & Jansson, 2004; March & Shapira, 1987; et al.) tveganja ne moremo ukiniti, lahko pa se mu izognemo, poskušamo zmanjšati njegov vpliv ali našo izpostavljenost tveganju. Sistematični pristop z usmerjenim izvajanjem aktivnosti za doseganje tovrstnih ciljev pojmujemo kot **obvladovanje tveganj**.

Tveganja so prisotna na vseh področjih organizacije. Vsako področje ima specifične značilnosti. Zato je poglavitno vprašanje pri obvladovanju tveganj: »Kako ustvariti povezovalno aktivnost, ki bo vodila k vzpostavitvi celovitega procesa obvladovanja tveganj na vseh področjih organizacije?« Mehr in Hedges (1982) sta v 60. letih prejšnjega stoletja kot prva osnovala in formalizirala usmeritve in priporočila za celovit sistem obvladovanja tveganj v organizaciji in ga poimenovala »Enterprise Risk Management« (skrajšano ERM). Skozi čas je ERM dobival različne dopolnitve in strukture. V letu 2009 je Mednarodna organizacija za standardizacijo objavila standard ISO 31000 »Risk Management - Principles and Guidelines« kot sintezo najboljših do tedaj razvitih usmeritev in dobrih praks na področju celovitega obvladovanja tveganj v organizacijah.

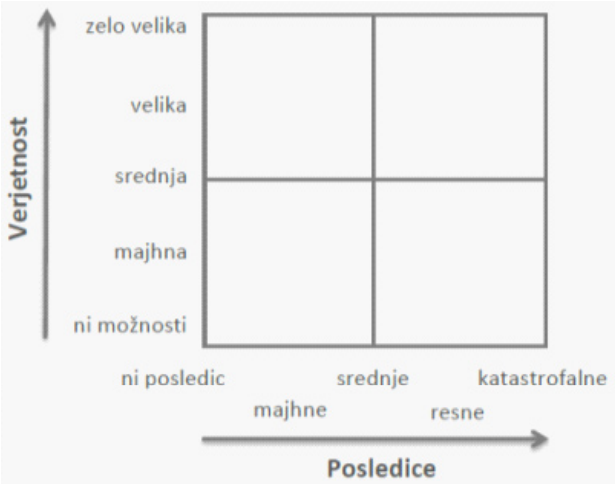
2 Opredelitev tveganja

Definicij tveganj je precej. Norrman in Jansson (2004, str. 436) opredeljujeta tveganje kot produkt

stopnje verjetnosti nastanka dogodka in stopnje prizadetosti posla. Slednja je rezultat razmerja med stopnjo verjetnosti uresničitve in nivojem učinka tveganja. Kvantitativna ocena tveganja je opredeljena v razmerju, kot prikazujeta enačba (1) in Slika 1: Matrika tveganja.

Tveganje = verjetnost nastanka dogodka X stopnja prizadetosti posla (1)

Slika 1: *Matrika tveganja*



Vir: A. Norrman & U. Jansson, Erricson's proactive supply chain risk management approach after a serious sub-supplier accident, 2004, str. 437.

Na prikazanem primeru matrike tveganja je **verjetnost** nastanka dogodka lahko:

- **Ničelna**: Dogodek se ne bo uresničil in se tudi v preteklosti ni uresničil.
- **Majhna**: Dogodek se verjetno ne bo uresničil. Čeprav se v preteklosti še ni uresničil, obstaja možnost uresničitve.
- **Srednja**: Obstaja enaka verjetnost, da se dogodek uresniči ali pa ne.
- **Velika**: Dogodek se bo verjetno uresničil. V preteklosti se je že uresničil ali se je uresničil drugim.
- **Zelo velika**: Dogodek se nam večkrat ponavlja ali se je večkrat ponovil drugim.

Posledice dogodka so glede na velikost povzročene škode lahko:

- **Ničelne**: Ni škode za organizacijo.
- **Majhne**: Škoda je majhna in nima pomembnejših posledic za organizacijo.
- **Srednje**: Nastala je škoda, ki bo zahtevala svoj čas za odpravo posledic, vendar pa ne ogroža poslovanja organizacije.
- **Resne**: Nastala je velika škoda, ki ogroža organizacijo in bo pustila posledice za organizacijo na daljši rok.
- **Katastrofalne**: Nastala je ogromna škoda, ki je za organizacijo pogubna.

Koristno je poznati tudi **časovno komponento posledice tveganja**, in sicer, kdaj se lahko zgodi ter koliko časa lahko traja.

3 Vrste tveganj v organizacijah

Pri razlikovanju tveganj je pomembno poznati njihovo naravo, izvor in možne posledice. Na osnovi teh lastnosti je priporočljivo izdelati **klasifikacijske ali razvrstitvene sisteme tveganj**, ki omogočajo prepoznavanje in razvrščanje tveganj po posameznih skupinah glede na sorodne lastnosti. Literatura navaja precej različic razvrstitev tveganj: neugodna, ugodna tveganja; zunanja, operativna, finančna tveganja; čista, kontrolna, špekulativna tveganja, idr. Organizacije, zlasti podjetja s proizvodno dejavnostjo (Skupina Letrika, 2014, str. 64-70; Gorenje d. d., 2014, str. 72-76; Helios d. d., 2014, str. 38-43), pogosto uporabljajo naslednjo klasifikacijo tveganj:

1. **poslovna tveganja**, kamor uvrščajo trženjska, nabavna, produktna tveganja, tveganja izgube premoženja in druge vrste tveganj;
2. **finančna tveganja**, kamor uvrščajo kreditna, valutna, obrestna tveganja in tveganja plačilne sposobnosti;
3. **tveganja delovanja**, ki zajemajo proizvodna, organizacijska, kadrovska, družbena, davčna, okoljska tveganja, tveganja informacijskega sistema in druga tveganja.

V literaturi in praksi najdemo še veliko drugih opredelitev kategorij in vrst tveganj kot na primer: strateška tveganja, naložbena tveganja, tveganja odgovornosti, zakonsko-pravna tveganja, varnostna tveganja, tveganja izgube dobrega imena in drugo. Čeprav je sistemov razvrstitev tveganj precej, so avtorji mnenja, da nobena različica ni splošno uporabna za vse vrste organizacij. Slednje morajo same ugotoviti, kateri sistem razvrstitve tveganj je zanje najbolj ustrezen in ga po potrebi dopolniti.

4 Značilnosti sistema celovitega obvladovanja tveganj

Namen tega sistema je učinkovito obvladovati tveganja po celotni organizaciji, ki bi lahko povzročila odstopanja od zastavljenih ciljev. Pri tem gre za uporabo različnih tehnik, ki s sistematičnim pristopom, celovito obravnavo tveganj po vsej organizaciji, usklajenimi in učinkovitimi ukrepi doprinesejo organizaciji koristi. Slednje se lahko odražajo kot zmanjšanje neželenih posledic ali pridobitev dodatnih koristi za organizacijo. Osnovna gradnika sistema celovitega obvladovanja tveganj sta:

- **ogrodje sistema** (angl. *risk management framework*), ki ga tvorijo načela in navodila kot podpora za vzpostavitev procesa obvladovanja tveganj;
- **proces obvladovanja tveganj** (angl. *risk management process*), kjer gre za strukturiran, skladen in neprekinjen proces spremljanja in prepoznavanja tveganj, ocenjevanja le-teh, sprejemanja ukrepov za obvladovanje tveganj ter poročanja o učinkovitosti obvladovanja tveganj, ki teče po celotni organizaciji.

Učinkovita orodja za sistematičen pristop obravnave posameznih področij problematik predstavljajo **standardi**. Ti so rezultat dobrih praks, kar med drugim pomeni, da so preverjeni. Obvladovanje tveganj v organizacijah obravnava precej standardov. V nekaterih primerih, kjer so standardi razviti za druge primarne namene (ISO 9001, ISO 14001, BS OHSAS 18001 idr.), obvladovanje tveganj ni izrecno omenjeno, zasledimo pa njegove elemente v usmeritvah in zahtevah, ki izhajajo iz standardov. Prvi objavljen standard za celovito obvladovanje tveganj v organizacijah je bil Australian Standard AS4360, prvič objavljen leta 1995 (Hopkin, 2010, str. 54). Predstavljal je dobro osnovo številnim kasneje objavljenim standardom, kot npr. COSO ERM Framework, British Standard BS 31100, IRM standard, ISO 31000, idr. Skupna značilnost standardov za celovito obvladovanje tveganj je sistematičen pristop pri vzpostavitvi ogrodja sistema, kakor tudi načrtovanja procesa celovitega obvladovanja tveganj. Gonilo vseh procesov je stalno izboljševanje stanja in sistema.

5 Pričakovane koristi od učinkovitega obvladovanja tveganj

Z učinkovitim obvladovanjem tveganj lahko pomembno vplivamo na verjetnost uresničitve dogodkov, kakor tudi na velikost njihovih posledic. To nam daje zelo pomemben vzvod pri usmerjanju organizacije na poti k cilju. Hopkin (2010, str. 4) opredeljuje tako imenovan sistem pričakovanih koristi CADE3, ki izhajajo iz učinkovitega obvladovanja tveganj. Po tem sistemu naj bi organizacija pridobila naslednje koristi:

- **skladnost delovanja** (angl. *Compliance*) kot skupni rezultat delovanja tistih aktivnosti obvladovanja tveganj, ki usmerjajo organizacijo k izpolnjevanju zakonskih, družbenih in okoljevarstvenih zahtev;
- **jamstvo** (angl. *Assurance*), da so ključna tveganja bila prepoznana in so bili sprejeti ustrezni ukrepi;
- **učinkovitejše odločanje** (angl. E*nhanced decision making*). Informacije, pridobljene na osnovi izvajanja procesa obvladovanja tveganj, so koristne za sprejemanje hitrih in učinkovitih odločitev. Proces obvladovanja tveganj je torej pomembna podpora pri odločanju in vodenju, zato ga mora organizacija podpirati;
- **večjo učinkovitost** (angl, *Efficiency*/*Effectiveness*/*Efficacy*) aktivnosti, procesov in strategij v organizaciji.

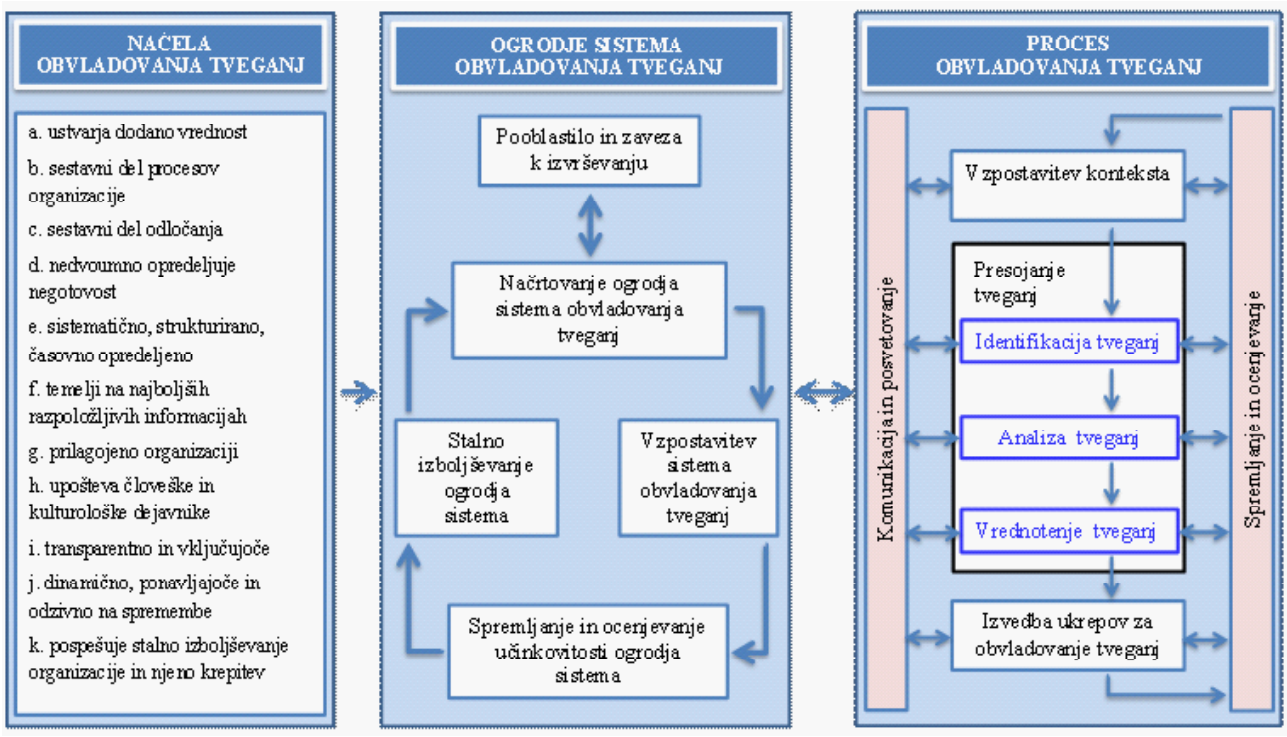
Literatura navaja še veliko drugih možnih koristi kot na primer: povečanje konkurenčnih prednosti, točnost finančnega poročanja, večjo transparentnost v organizaciji, proaktivno vodenje organizacije, hitrejšo odzivnost organizacije, povečan ugled organizacije, povečano zaupanje deležnikov in delničarjev v organizacijo, izboljševanje sposobnosti učenja organizacije, neprestano izboljševanje in drugo. Kot navaja Šušteršič (2013, str. 9), raziskave kažejo, da podjetja, ki sledijo razvitim metodologijam obvladovanja tveganj, dosegajo tudi višji EBITDA[1]. Obvladovanje tveganj pomaga tudi pri pridobivanju vlagateljev in delničarjev. Če podjetje obvladuje to področje, daje pozitivni signal tudi bankam. Slednje se bodo lažje odločile za odobritev posojila. Tudi okolje bo manj negotovo glede izgube delovnih mest. Koristi od obvladovanja tveganj je nedvomno precej.

1 EBITDA je kratica za angl. izraz Earnings Before Interests and Taxes, Depreciation and Amortization, kar predstavlja finančni kazalec, ki vključuje čisti dobiček, obresti, davke, odpise in amortizacijo.

6 Razlogi za vpeljavo standarda ISO 31000

ISO 31000 sodi med najnovejše standarde celovitega obvladovanja tveganj v organizacijah in temelji na dosedanjih najboljših spoznanjih in dobrih praksah na tem področju. Po trditvah stroke (Hopkin, 2010, str. 56; ISO 31000 Risk Management, 2012) je učinkovit in spada med najbolj uporabljane pristope obvladovanja tveganj v zadnjih letih. Je univerzalen, uporaben za obvladovanje vseh vrst tveganj za kakršenkoli tip organizacije. Omogoča obravnavo in obvladovanje tveganj na slehernem organizacijskem področju, procesu, projektu, izdelku ali storitvi, odločitvi in drugih aktivnostih organizacije. Pomembne odlike ISO 31000 so njegova celovitost, sistematičnost in natančnost pristopa pri obravnavi tveganj. Standard namreč predvideva nedvoumno oznako - naslov vsakega identificiranega tveganja, določitev njegovega skrbnika in časovni načrt aktivnosti obvladovanja posameznega tveganja oz. njegovo spremljanje. Je konkreten, kratek in jedrnat ter usmerjen k rezultatom. Z namenom nedvoumnega razumevanja terminoloških izrazov standarda je izdelan slovar **ISO Guide 73**, ki je sestavni del obravnavanega standarda. V lanskem letu je Mednarodna organizacija za standardizacijo objavila ISO/TR 31004:2013, Risk Management – Guidance, ki predstavlja vodilo za lažjo povezavo dobrih praks obvladovanja tveganj v organizacijah s standardom ISO 31000. Ta standard predvideva obravnavo celovitega spektra dejavnikov tveganja, tako z vidika notranjega kot tudi zunanjega okolja organizacije. Njegov koncept ima jasno in trdno strukturo. Vzpostavitev ogrodja daje konceptu čvrsto zasnovo z vidika sistematičnosti gradnje sistema za kasnejše izvajanje procesa. Največji poudarek je namreč na samem procesu obvladovanja tveganj. ISO 31000 ima status mednarodnega standarda, kar je z vidika uporabe koristno za organizacije z mednarodnim poslovanjem. Ker je kot standard podvržen reviziji na vsaka štiri leta, je ISO 31000 izpostavljen nadgraditvam in izboljševanju v skladu z najnovejšimi spoznanji in dobrimi praksami. Vsebuje soroden pristop z ostalimi, že uvedenimi ISO standardi kot npr. ISO 9001, ISO/TS 16949, ISO 14001. Ta standard ni predmet certificiranja, kar je nedvomno stroškovna korist za organizacijo. Poraja pa se vprašanje, ali bo organizacija zmogla dovolj samodiscipline pri doslednem izvajanju vseh potrebnih aktivnosti za učinkovito obvladovanje tveganj.

Slika 2: *Razmerja med gradniki ISO 31000*



Vir: International Organization for Standardization, International Standard ISO/FDIS 31000:2009(E), Risk management - Principles and guidelines, 2009b, str. VII.

ISO 31000 opredeljuje tri področja – gradnike sistema (Slika 2), ki omogočajo celovito obvladovanje tveganj v organizaciji, in sicer:

1. **načela** pri obvladovanju tveganj,
2. **ogrodje** sistema obvladovanja tveganj in
3. **proces** obvladovanja tveganj.

7 Gradniki sistema ISO 31000

7.1 Načela pri obvladovanju tveganj

Za vzpostavitev učinkovitega sistema obvladovanja tveganj standard ISO 31000 priporoča organizacijam, da zasledujejo in izpolnjujejo naslednja načela (angl. Principles), kot navaja International Organization for Standardization (2009b, str. 7-8):

- Obvladovanje tveganj **pomaga podjetju varovati in ustvarjati dodano vrednost.**
- Obvladovanje tveganj **je integrirano v vse procese organizacije** in je sestavni del odgovornosti vodstva.
- Obvladovanje tveganj **je pomembna podpora odločanju.**
- **Tveganja so opredeljena nedvoumno in imajo svoj naslov.**
- **Pristop pri obvladovanju tveganj je sistematičen, strukturiran, aktivnosti pa časovno opredeljene.**
- Obvladovanje tveganj **temelji na najboljših informacijah**, ki so v danem trenutku dostopne. Te so rezultat ažurne podatkovne baze, mreže informacijskih virov, statistike, izkušenj, strokovnih ocen in predvidevanj idr.
- Obvladovanje tveganj **je prilagojeno konkretni organizaciji.**
- Pri obravnavi tveganj je potrebno upoštevati **človeške in kulturološke dejavnike**.
- Obvladovanje tveganj je **transparentno in vključujoče**. Z vključevanjem mnenj čim širšega kroga deležnikov, še posebno odločevalcev, po celotni organizaciji poskuša izpopolniti sistem do najboljše možne mere.
- Obvladovanje tveganj je **dinamično, ponavljajoče in odzivno na spremembe.**
- Obvladovanje tveganj **pospešuje proces stalnega izboljševanja organizacije in jo krepi.**

7.2 Ogrodje sistema obvladovanja tveganj

Ogrodje sistema je povezovalni mehanizem med elementi procesa obvladovanja tveganj v organizaciji. Proces celovitega obvladovanja tveganj v organizaciji je običajno zelo kompleksen, saj obravnava številna tveganja na različnih področjih in nivojih organizacije, omogoča usklajevanje, izvajanje ter nadzor aktivnosti za njihovo obvladovanje. Ogrodje v skladu z ISO 31000 vzpostavlja potrebne temelje za uvajanje dobrih praks v proces celovitega obvladovanja tveganj. Zasnovano je na konceptu **PDCA**[2] cikla kot prikazano na Sliki 2. To daje dobro osnovo za nenehno izboljševanje učinkovitosti procesa.

Standard poudarja pomen integracije obvladovanja tveganj v samo kulturo organizacije. To zahteva **zavezo najvišjega vodstva organizacije k podpori**, spodbujanju in izvrševanju vseh potrebnih aktivnosti za učinkovito obvladovanje tveganj na vseh področjih in nivojih organizacije. Zelo pomembno je pred načrtovanjem sistema oceniti in razumeti **notranji in zunanji kontekst** podjetja oziroma notranje in zunanje dejavnike okolja, ki vplivajo na organizacijo. Načrtovanje ogrodja sistema zahteva poznavanje organizacije, njenega delovanja, posebnosti, šibkosti in nevarnosti. Potrebno je predvideti in oblikovati **politiko obvladovanja tveganj** v organizaciji. Predvideti in zagotoviti je potrebno **vire** za izvajanje procesa obvladovanja tveganj. Učinkovitost procesa zahteva uvedbo ustreznih organizacijskih pristopov in metod pri načrtovanju aktivnosti, izvajanju, spremljanju, ocenjevanju rezultatov in izboljševanju sistema. Nepogrešljivo orodje v izvajanju procesov so ljudje – nosilci aktivnosti s svojim znanjem, izkušnjami in seveda angažiranostjo. Učinkovito komuniciranje je nujno tako znotraj organizacije kot tudi navzven. Priporočljivo je predvideti izdelavo **komunikacijskega načrta in eskalacijskega procesa**. V okviru področja **vzpostavitve sistema** obvladovanja tveganj standard predvideva:

- oblikovanje strategije za vzpostavitev ogrodja sistema obvladovanja tveganj v organizaciji, v naslednjem koraku pa njeno izvršitev;
- pripravo načrta za uvedbo procesa obvladovanja tveganj v organizaciji in kasneje njegovo aktiviranje.

Standard poudarja pomen **spremljanja in ocenjevanja učinkovitosti ogrodja sistema**. V ta namen priporoča izdelavo in uporabo meril za ocenjevanje njegove učinkovitosti, evidentiranje

2 PDCA je kratica za angl. izraz Plan (planiraj) – Do (naredi) - Control (preveri) - Act (ukrepaj oz. popravi), kar poznamo kot Demingov krog nenehnega izboljševanja.

rezultatov in vzpostavitev sistema poročanja. Na osnovi presoje rezultatov učinkovitosti ogrodja sistema organizacija sprejme odločitve o potrebnih ukrepih za dopolnitev oziroma **izboljšanje ogrodja sistema**. Izboljševanje se izvaja kontinuirano v obliki cikličnega procesa.

7.3 Proces obvladovanja tveganj

Proces obvladovanja tveganj po ISO 31000 sistematično usklajuje izvajanje različnih politik, strategij in postopkov v organizaciji s širokim spektrom koordiniranih aktivnosti, ki se nanašajo na obvladovanje vplivov notranjih in zunanjih dejavnikov organizacije, posvetovanje in učinkovito komuniciranje z deležniki, identifikacijo tveganj, njihovo analizo, vrednotenje, obdelavo, spremljanje ter ponovno oceno tveganj. Deluje po sistemu cikla PDCA. Standard poudarja pomen **komuniciranja in posvetovanja z deležniki** v vseh fazah procesa obvladovanja tveganj. Ker je pomembno, da vzpostavimo možnost komunikacije s čim širšim krogom deležnikov, tako notranjih kot tudi zunanjih, je priporočljivo izdelati komunikacijski načrt in eskalacijski proces. Standard daje pomembno težo obravnavi **konteksta sistema** (angl. *context*), kjer gre za poudarek na opredelitvi:

- dejavnikov, ki imajo potencialni vpliv na tveganja v organizaciji,
- parametrov, ki omogočajo spremljanje uspešnosti izvajanja procesa obvladovanja tveganj.

Pri njihovem opredeljevanju moramo imeti v mislih vprašanje, v kolikšni meri lahko ti vplivajo na doseganje ciljev organizacije, kakor tudi obvladovanje tveganj v organizaciji. Standard strukturira opredelitev dejavnikov okolja, ki imajo potencialni vpliv na delovanje organizacije, na zunanje in notranje dejavnike. Med **zunanje dejavnike okolja** šteje ključne dejavnike in trende na področjih zakonodaje, ekonomije, tehnologije, konkurence, financ, politike, sociale, kulture in drugih področjih, ki imajo vpliv na doseganje ciljev organizacije. Ti dejavniki lahko izhajajo iz mednarodnega, nacionalnega, regionalnega in lokalnega okolja. Med najpomembnejše elemente obravnave sodijo odnosi z zunanjimi deležniki, njihove percepcije in vrednote. Pod **notranje dejavnike okolja** standarda navaja:

- vrednote, politike, cilje in strategije organizacije,
- sistem vodenja, organizacijsko strukturo, vloge in odgovornosti notranjih deležnikov,
- vire, kar predstavljajo zaposleni s svojim znanjem, kapital, razpoložljive tehnologije, procesi, sistemi in druga orodja, ki jih organizacija poseduje,
- odnose in percepcije notranjih deležnikov ter organizacijsko kulturo,
- formalne in neformalne komunikacijske sisteme ter tokove informacij,
- procese sprejemanja odločitev,
- standarde in sprejete modele v organizaciji,
- druge notranje dejavnike in specifičnosti, ki imajo vpliv na doseganje ciljev organizacije.

ISO 31000 poudarja pomembnost vzpostavitve edinstvenega konteksta obvladovanja tveganj v organizaciji. S tem mislimo na upoštevanje specifičnosti okolja konkretne organizacije, njenega delovanja in obnašanja. Cilj je doseči usklajenost in umeščenost procesa obvladovanja tveganj v organizacijsko kulturo konkretne organizacije, s čimer mislimo na umeščenost v njene procese, politike, strategije, vodenje in miselnost njenih deležnikov.

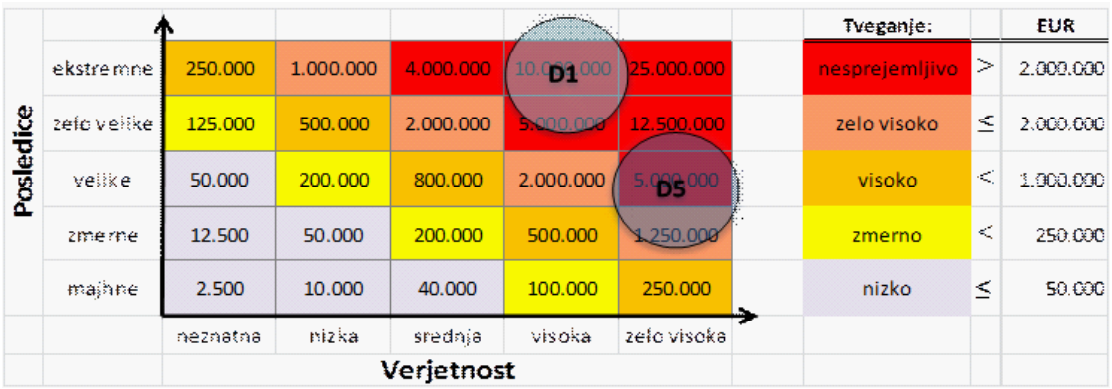
Zelo pomembno področje procesa obvladovanja tveganj predstavlja določitev **kriterijev ocenjevanja tveganj**. V okviru te aktivnosti opredelimo:

- naravo, tip vzroka in posledice potencialnih tveganj,
- definicijo verjetnosti,
- časovni okvir in verjetnost nastanka posledic.

Pri opredeljevanju kriterijev moramo imeti v mislih sprejeto politiko obvladovanja tveganj organizacije, način in specifike delovanja organizacije, interese in pričakovanja deležnikov, opredelitev narave in možnih izvorov tveganja, način opredelitve verjetnosti, kakor tudi posledic v primeru uresničitve tveganja. Vzpostavljen mora biti tudi sistem za spremljanje ustreznosti kriterijev in njihovo nadgrajevanje.

Zelo pomemben poudarek je na vzpostavitvi **registra tveganj**, ki je ključno orodje za obvladovanje tveganj, katerega je potrebno vzpostaviti na ravni celotne organizacije. Vsebuje specifikacijo prepoznanih tveganj, njihove opise in ocene, lastnike, akcijski načrt ukrepov in podatke, iz katerih je razvidno, da je obravnavano tveganje spremljano in se izvaja aktivnosti za njegovo obvladovanje. Zaradi dinamike dopolnjevanja in posodabljanja je register tveganj proces in ne zgolj dokument. Je odraz proaktivnega delovanja deležnikov in vodstva. Običajno je obravnavan na mesečnih sestankih posamezne organizacijske enote in kvartalnih kolegijih skrbnikov tveganj. Zapisniki

Slika 3: *Matrika tveganj - vrednostne ocene tveganj in nivoji tveganj*



Legenda: *Identificirani viri tveganj:*
D1 = dobavitelj, rast cen materialov;
D5 = dobavitelj, zamude dobav oz. pomanjkljiva logistična podpora dobavitelja

sestankov služijo kot dokazilo o njegovi uporabi in posodabljanju.

Pomemben del sistema obvladovanja tveganj je **informacijska podpora**. Ta omogoča razširitev **mreže vključenosti deležnikov** pri identificiranju tveganj, olajša komuniciranje, izboljša pretok informacij, obdelavo podatkov, spremljanje in nadzor nad ukrepi za obvladovanje tveganj. Večina organizacij v začetnih fazah implementacije sistema obvladovanja tveganj nima vzpostavljenega namenskega informacijskega sistema, temveč si pri tem pomaga z razpoložljivimi informacijskimi sistemi, programskimi orodji oz. jih sama dograjujejo glede na potrebe (poslovni informacijski sistem, excellove tabele, intranet mreža idr.). Izsledki literature (Compliance Software, 2012; Fraser & Simkins, 2010; Hopkin, 2010; et al.) kažejo, da je prednosti od vpeljave namenskega informacijskega sistema oz. namenske programske opreme za obvladovanje tveganj precej. Trg ponuja številne verzije informacijskih sistemov in programskih paketov za obvladovanje tveganj, kot so npr.: SAP Risk Management, MKinsight ERM, Active Risk Manager – ARM, Counter Measures, Riskware idr.

V okviru **presojanja tveganj** kot sklopa procesa standard opredeljuje naslednje faze:

- V fazi **identifikacije ali prepoznavanja tveganj** poskušamo ugotoviti: »Kaj lahko gre narobe, na kakšen način, v kolikšni meri in s kakšno verjetnostjo?« Za identificirano tveganje je potrebno zbrati in evidentirati bazo podatkov, ki omogočajo sistematičen opis ali tako imenovano **profiliranje tveganja**[3]. Pristopov prepoznavanja tveganj je več. Najbolj razširjeno je prepoznavanje tveganj z obveščanjem oziroma zbiranjem informacij - prijav s strani deležnikov. Pogost pristop je tudi t.i. **mapiranje** (angl. *mapping*) organizacij, področij ali procesov z namenom ugotavljanja njihovih kritičnih elementov. Za prepoznavanje tveganj je potrebno angažirati kompetentne ljudi, ki z ustreznimi znanji, pristopi in orodji vzpostavijo in ažurno vodijo preglednico s podatki o prepoznanih tveganjih ali tako imenovani **register tveganj**.
- V okviru **analize tveganj** podatke o prepoznanem tveganju pretvorimo v uporabno vrednost informacij. Bistvo analize je čim bolje opredeliti in razumeti posamezno tveganje ter dejavnike, povezane z njim. Na podlagi pridobljenih podatkov ugotavljamo lastnosti posameznega tveganja, razloge za nastanek in vire tveganja, velikost učinkov in možne posledice ter verjetnost njihove uresničitve. Pri tem imamo na voljo uporabo kvantitativne analize, kvalitativne analize ali kombinacije obeh. Ključni komponenti analize tveganj sta **opredelitev posledic posameznega tveganja in opredelitev verjetnosti njihove uresničitve**. Njun zmnožek odraža vrednostno oceno tveganja, kot prikazuje enačba (2).

Tveganje = posledice uresničitve tveganja X verjetnost uresničitve tveganja (2)

Na podlagi medsebojne primerjave izračunanih vrednosti ocen tveganja razporedimo po stopnjah ali nivojih tveganj, kot prikazuje Slika 3.

3 Profiliranje ali opredelitev tveganja je izvedena z njegovo klasifikacijo v ustrezni skupini tveganj, ki imajo sorodne lastnosti.

Rezultati odražajo naravno stopnjo posameznega tveganja oziroma ali stopnjo tveganja pred uvedbo ukrepov za njihovo obvladovanje.

- Sledi **vrednotenje tveganj**, katerega namen je pripraviti kakovostne informacije za sprejemanje odločitev v organizaciji. Cilj te faze je:
  - določiti tveganja, za katera je potrebno izvesti ustrezne ukrepe za njihovo obvladovanje (angl. *risk treatment*[4]). Določimo jih na podlagi primerjave rezultatov nivojev posameznih tveganj, ki smo jih ugotovili v fazi analize;
  - določiti prioritete tveganj, za katere je potrebno izvesti ustrezne ukrepe. To vprašanje je koristno obravnavati v širšem smislu in navzočnosti širšega kroga deležnikov.

- V okviru faze **priprave in izvedbe ukrepov** za obvladovanje tveganj opredelimo ustrezne rešitve/ukrepe za ublažitev določenega tveganja in jih izvedemo. **Iskanje ustreznih ukrepov** je cikličen proces, kjer presojamo različne rešitve/možne ukrepe, potrebne vire za izvedbo ukrepa, koristi od uvedenega ukrepa, učinkovitost in izvedljivost ukrepa. Ker se okoliščine spreminjajo, ni nujno, da je določena rešitev trajna. ISO 31000 (2009b, str. 19) opredeljuje več možnih **pristopov oz. strategij** iskanja ustreznih rešitev, in sicer:
  - **izogibanje tveganju**, ko aktivnost, ki je izpostavljena tveganju, ustavimo ali je sploh ne izvršimo;
  - **spodbujanje tveganja**, ko uresničitev le-tega prinaša korist;
  - **izključitev vira** tveganja in s tem izognitev tveganju;
  - **sprememba verjetnosti nastanka** tveganja;
  - **sprememba posledic** delovanja tveganja;
  - **prenos tveganja na drugo stranko** ali delitev tveganja z njo;
  - **sprejetje tveganja** na podlagi utemeljene odločitve. Izvede se priprava na tveganje in vzpostavitev stanja pripravljenosti še pred njeno uresničitvijo.

  Kriteriji pri izbiri ustrezne rešitve so običajno **učinkovitost**, ki nam jo ta rešitev prinaša, in **potrebni viri** za njeno izvršitev. Seveda mora organizacija pri tem upoštevati percepcije deležnikov, zakonodajo, odgovornost do družbe in okolja ter ostale pomembne dejavnike. Rešitev lahko zahteva enega ali več ukrepov, njihovi učinki pa se lahko odražajo na različnih področjih organizacije.

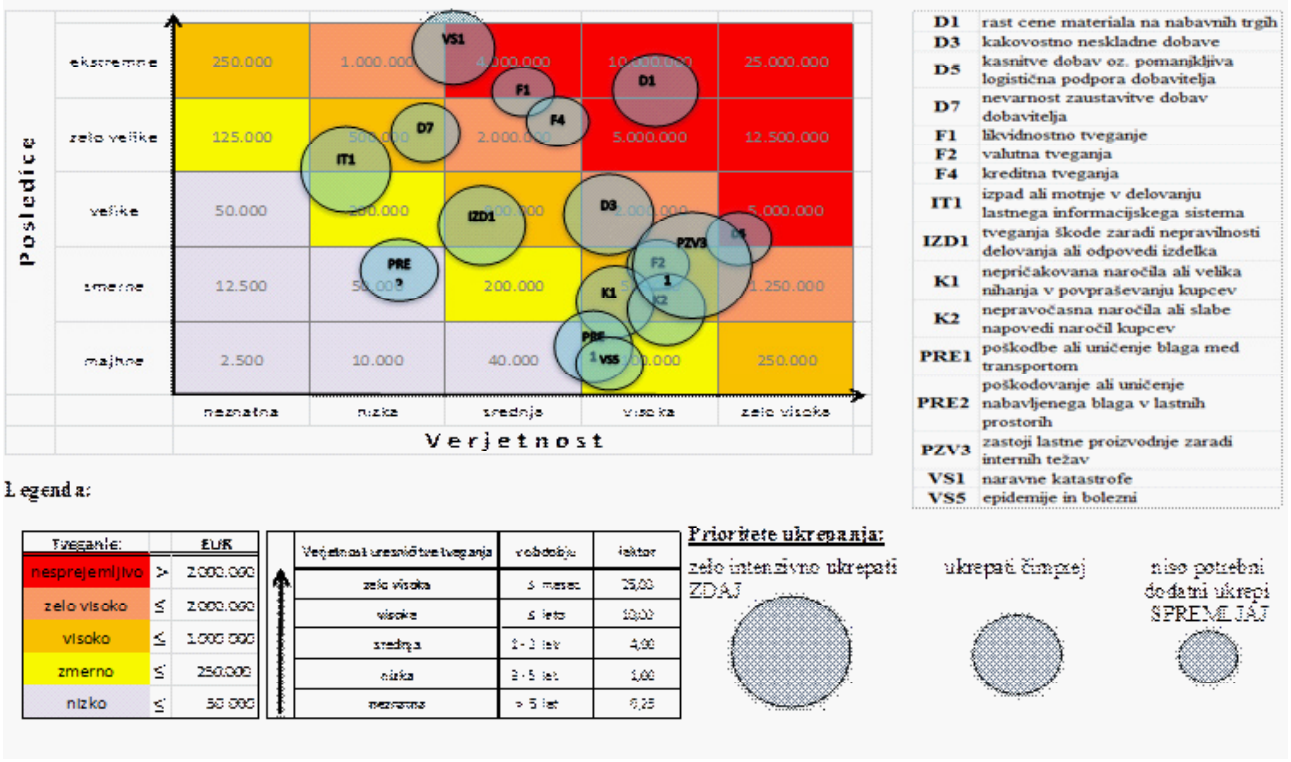
  Standard predvideva **izdelavo načrtov ukrepov za obvladovanje tveganj**, katerih namen je dokumentirati ukrepe in njihov način uvedbe oz. izvajanja. Koristno je namreč, da imamo za identificirana potencialna tveganja pripravljen seznam ukrepov, katerih uvedba in izvajanje sta predhodno preučena, preverjena in ovrednotena z vidika stroškov ter koristi. Načrt običajno vsebuje opredelitev ukrepov in prioritet njihove izvedbe, ocene pričakovanih stroškov in koristi zaradi izvedbe ukrepa, predvidena merila za spremljanje učinkovitosti ukrepa, roke in nosilce izvedbe ter zahteve glede poročanja. Standard priporoča seznanitev deležnikov z načrtom ukrepov obvladovanja tveganj, izvrševanje načrta pa naj postane sestavni del procesa vodenja organizacije.

- V skladu s priporočili standarda naj bi bilo **spremljanje in ocenjevanje učinkovitosti procesa** obvladovanja tveganj načrtovan in nadziran proces. V ta namen organizacija opredeli in pripravi kontrolni mehanizem, na podlagi katerega se bo preverjalo izvajanje in učinkovitost procesa. Osnova za spremljanje bo skupna matrika tveganj organizacije, kot je prikazano na Sliki 4. Frekvenca preverjanj je različna in je odvisna od odločitve organizacije. Kontrola doslednosti spremljanja tveganj in ocenjevanja učinkovitosti sprejetih ukrepov se lahko vrši stalno, preko periodičnih ali naključnih preverjanj.

- Pomembno je zagotavljati sledljivost dogajanja, povezanega z izvajanjem ukrepov za obvladovanje tveganj in njihovih učinkov. Na tem področju standard poudarja pomen spremljanja in **evidentiranja** rezultatov ter drugih relevantnih podatkov. Dobre evidence so lahko zelo pomemben vir informacij in idej za dodatno izboljšanje procesa, kakor tudi ogrodja sistema. Seveda moramo pri tem imeti v mislih tudi potrebna sredstva in vire za vzpostavljanje in vzdrževanje podatkovne baze, občutljivost narave podatkov, zakonodajo in druge relevantne dejavnike.

4 V angleški literaturi je ta faza procesa opredeljena kot **risk treatment**, kar bi v slovenskem prevodu pomenilo **ukrepe za obvladovanje tveganj**.

Slika 4: *Matrika tveganj – stanje tveganj po zadnjem ocenjevanju dne 31. 3. 2014*



8 Sklep

Kot je razvidno iz prispevka, je vzpostavitev sistema celovitega obvladovanja tveganj v organizaciji kompleksna naloga. Zahteva celovit in sistematičen pristop, precej virov, podporo in angažiranje deležnikov, zlasti najvišjega vodstva. Izzivov je precej, zato traja načrtovanje in vzpostavitev sistema običajno nekaj let. Ker je sistem tudi po aktiviranju izpostavljen spremembam v dinamičnem okolju, ga je potrebno nenehno spremljati, dopolnjevati, izboljševati s ciljem zagotavljanja njegove učinkovitosti. Še tako dober sistem je zgolj orodje brez prave vrednosti, če ni sprejet pri deležnikih in izvajan v praksi. Prav ta del je običajno najtežji. Deležnike je potrebno prepričati o koristih obvladovanja tveganj, uporabni vrednosti sistema in jih motivirati za dosledno izvajanje aktivnosti v okviru vzpostavljenega procesa obvladovanja tveganj.

Praktični prikaz vzpostavitve sistema celovitega obvladovanja tveganj po ISO 31000 na konkretnem primeru organizacije najdete pod avtorjevo objavo »Vzpostavitev procesa obvladovanja tveganj po standardu ISO 31000 za področje nabave: primer Letrika«. Zanimanja in izzivov na tem področju je veliko, zato lahko pričakujemo intenzivni razvoj novih, učinkovitejših pristopov, orodij in standardov za celovito obvladovanje tveganj v organizacijah.

9 Viri in literatura

1. Mozetič, B. (2014). *Vzpostavitev procesa obvladovanja tveganj po standardu ISO 31000 za področje nabave: primer Letrika* (magistrsko delo). Ljubljana: Ekonomska fakulteta.
2. Compliance Software. Najdeno 12. aprila 2012 na spletnem naslovu http://www.best-practice.com/best-practice-software/compliance-software/
3. Fraser, J., & Simkins, B. (2010). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. New Jersey: John Wiley & Sons, Inc.
4. Gorenje d. d. (2014). Letno poročilo skupine Gorenje 2009. Najdeno 22. marca 2013 na spletnem naslovu http://lp2009.gorenjegroup.com/jart/GOAR09/html/sl/download/Letna_Porocila_2009_Skupina_Gorenje.pdf
5. Helios d. d. (2014). Letno poročilo skupine Helios 2011. Najdeno 22. marca 2013 na spletnem naslovu http://www.helios-group.eu/slo/informacije-za-delnicarje/financni-kazalci-in-poslovna-porocila

6. Hopkin, P. (2010). *Fundamentals of Risk Management; Understanding, evaluationg and implementing effective Risk Management* – Second edition. London, Kogan Page Limited.
7. International Organization for Standardization (2009a). ISO Guide 73:2009. *Risk Management – Vocabulary.* Geneva: International Organization for Standardization.
8. International Organization for Standardization (2009b). *International Standard ISO/FDIS 31000:2009(E), Risk Management – Principles and Guidelines*. Geneva: International Organization for Standardization.
9. *ISO 31000 Risk Management*. Najdeno 12. aprila 2012 na spletnem naslovu http://www.best-practice.com/risk-management-best-practices/risk-management-standards/iso-31000-risk-management/
10. Jorion, P. (2000). *Value at Risk: The new benchmark for Managing Financial Risk*. New York: The McGraw-Hill Companies Inc.
11. March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404-1418.
12. Mehr, R. I., & Hedges, B. A. (1982). Risk Management in the Busines Enterprise. Najdeno 11. aprila 2013 na spletnem naslovu http://www.genevaassociation.org/PDF/Geneva_papers_on_Risk_and_Insurance/GA1982GP7(23)_Head.pdf
13. Norrman, A., & Jansson, U. (2004). Erricson's proactive supply risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management, 34*(5), 434-456.
14. Skupina Letrika (2014). Letno poročilo 2012 - Skupina Letrika, družba Letrika, d. d. Najdeno 15. aprila 2014 na spletnem naslovu http://www.letrika.com/media/att/13/04/26/Letno_porocilo_2012_4.pdf
15. Šušteršič, M. (2013, 21. avgust). Pri upravljanju tveganj nismo računali na pohlep. *Delo*, str. 9.

Borut Mozetič, mag. posl. ved, je po zaključenem univerzitetnem študiju na Ekonomski fakulteti Univerze v Ljubljani (1997) opravljal različne naloge na področju globalne prodaje in nabave v avtomobilski industriji (Iskra Avtoelektrika d. d.) in na področju trženja sistemov avtomatizacije (Goap d. o. o.). Od leta 2010 opravlja naloge direktorja nabave v podjetju Letrika d.d. V letu 2014 je na Ekonomski fakulteti v Ljubljani magistriral na področju managementa, na tematiko obvladovanje tveganj v organizacijah.