UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VZPOSTAVITEV SISTEMA NOTRANJIH KONTROL NA PODLAGI OPERATIVNIH TVEGANJ V IZBRANEM PODJETJU

Ljubljana, september 2017

KATICA SEVER

IZJAVA O AVTORSTVU

Podpisana Katica Sever, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Vzpostavitev sistema notranjih kontrol na podlagi operativnih tveganj v izbranem podjetju, pripravljenega v sodelovanju s svetovalko prof. dr. Darjo Peljhan,

IZJAVLJAM,

1. da sem predloženo delo pripravila samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;
7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 4.9.2017 Podpis študentke:_____

KAZALO

UVOD **1**

1 POSLOVNA TVEGANJA **4**
1.1 Opredelitev in vrste tveganj 4
1.1.1 Kreditno tveganje 6
1.1.2 Tržno in likvidnostno tveganje 8
1.1.3 Tveganje objekta 10
1.2 Ravni obvladovanja tveganj 11

2 NOTRANJE KONTROLE **12**
2.1 Sestavni deli notranjega kontroliranja 13
2.1.1 Kontrolno okolje 14
2.1.2 Ocena tveganj 14
2.1.3 Kontrolne aktivnosti 15
2.1.4 Informiranje in komuniciranje 16
2.1.5 Nadzor nad kontrolnimi aktivnostmi 16
2.2 Pomanjkljivosti notranjih kontrol 17
2.3 Načela ocenjevanja in izboljšanja notranjih kontrol 18
2.4 Prednosti in stroški notranjih kontrol 19

3 OBVLADOVANJE OPERATIVNEGA TVEGANJA **21**
3.1 Opredelitev operativnega tveganja 21
3.2 Pristopi merjenja operativnega tveganja z vidika regulatorja 23
3.2.1 Enostavni pristop 24
3.2.2 Standardizirani pristop 25
3.2.3 Napredni pristop 26
3.3 Identifikacija operativnih tveganj 27
3.4 Vrste ukrepov pri obvladovanju tveganj 29
3.5 Metode merjenja operativnega tveganja 32

4 VZPOSTAVITEV SISTEMA NOTRANJIH KONTROL NA PODLAGI OPERATIVNIH TVEGANJ V PODJETJU XY **33**
4.1 Predstavitev podjetja 33
4.2 Model celovitega obvladovanja operativnih tveganj 35
4.2.1 Vloge in odgovornosti 37
4.2.2 Postopek razvrščanja in zbiranja podatkov o izgubah 38
4.2.3 Pripravljenost za prevzemanje tveganj 39
4.2.4 Kvalitativno ocenjevanje operativnih tveganj 41
4.2.5 Poročanje 43
4.3 Proces vzpostavitve notranjih kontrol 44

4.3.1 Ozaveščanje o tveganjih ... 44
4.3.2 Računovodska matrika in predlog mejnega zneska ... 46
4.3.3 Identifikacija relevantnih procesov za obravnavo ... 48
4.3.4 Management poslovnih procesov v podjetju ... 49
4.3.5 Prepoznavanje ključnih in potencialnih tveganj ... 50
4.4 Ocena učinkovitosti notranjih kontrol v podjetju XY ... 53

SKLEP ... 56

LITERATURA IN VIRI ... 58

PRILOGE

KAZALO TABEL

Tabela 1: Prikaz izračuna mejnih zneskov na podlagi povprečne pomembnosti ... 48

KAZALO SLIK

Slika 1: Obvladovanje tveganj v podjetju XY ... 12
Slika 2: Okvir notranjih kontrol COSO ... 13
Slika 3: Krivulja porazdelitev operativnih izgub ... 31
Slika 4: Matrika frekvenc pojava in vpliva škodnih dogodkov ... 33
Slika 5: Proces obvladovanja tveganj v podjetju XY ... 36
Slika 6: Proces zbiranja podatkov o škodnih dogodkih in izgubah ... 38
Slika 7: Von Neumann-Morgensternova krivulja koristnosti ... 40
Slika 8: Zasnova scenarijev operativnih tveganj ... 42
Slika 9: Ozaveščanje zaposlenih o sistemu notranjih kontrol ... 45
Slika 10: Dejavniki za izračun povprečne pomembnosti po mednarodnih smernicah ... 46
Slika 11: Osnutek kataloga tveganj ... 51
Slika 12: Primer poslovnega procesa v finančnem podjetju ... 51
Slika 13: Diagram z vsemi obveznimi elementi ... 53
Slika 14: Model upravljanja modula »Governance Risk & Control« ... 54

UVOD

S pojavom finančnih škandalov v preteklih letih v velikih in uspešnih svetovnih in evropskih korporacijah (Enron, WorldCom, Parmalat), s procesom globalizacije in povečevanjem vloge ustvarjanja vrednosti za lastnike je ustrezno in učinkovito ravnanje s tveganji dobilo pomembno vlogo (Koletnik, 2002, str. 70).

Po mnenju Bertonclja (Gea College, 2015) podjetja o visokih tveganjih v večini primerov razmišljajo kot o negotovih dogodkih manjše verjetnosti. Problem predstavljata tudi podcenjevanje in precenjevanje tveganja ter pretirana prepričanost o pravilnosti lastne ocene tveganj. Meni, da sta se zavedanje o tveganjih in obvladovanje tveganj v zadnjih desetih letih v Sloveniji bistveno izboljšala, vendar še obstajajo možnosti za izboljšave, saj zavedanje o tveganjih ne bo nikoli popolno. Zaznava tveganj je namreč izrazito subjektivno pogojena, kar pa se lahko izboljša z ustreznim usposabljanjem, predvsem vodilnih delavcev. Temeljno znanje o tveganjih bi morali imeti vsi zaposleni, ne le vodstvo podjetij, vodje poslovnih in podpornih funkcij, zaposleni v reviziji, vodje projektov, zaposleni v obvladovanju kakovosti itd.

Po mnenju Berka, Peterlina in Ribariča (2005, str. 18) opredelitev načina obvladovanja tveganj v podjetju ni preprosta naloga. Eden od najboljših načinov izoblikovanja organizacijske kulture je v podjetjih, kjer zaposleni intuitivno razumejo razmišljanje vodstva o tveganju in ciljih, ki naj bi jih prineslo njegovo obvladovanje. Pomembno je, da vodstvo podjetja pripisuje obvladovanju tveganj velik pomen in skrbi za zadovoljivo komuniciranje glede sprejemljivih stopenj tveganja, vzpostavitev komunikacije, ki daje napotke za prepoznavo posameznih vrst tveganj, in sprejemanje primernih ukrepov, vzpostavitev centra odgovornosti za obvladovanje tveganja, zagotovitev ustreznega nadzora postopkov obvladovanja tveganja in možnosti za implementacijo nadzora aktivnosti prek interne (notranje) revizije.

Po navedbah internega gradiva izbranega podjetja (ki je predmet analize v magistrskem delu in ga poimenujem kot podjetje XY) podjetja prevzemajo nekatera tveganja, ki so kvantificirana z ustreznimi kazalniki in opredeljena skladno s strategijo tveganja. Da bi dosegli pravilno usmerjanje, je treba skupno omejitev podjetja razporediti na različne vrste tveganj in tudi na glavne segmente. Opredelitev ustrezne želje po tveganju je osnovni predpogoj za določanje stalnih omejitev, pri čemer je treba odgovoriti na naslednja vprašanja: koliko lahko podjetje tvega, koliko tveganj želi podjetje prevzeti, koliko kapitala je potrebnega za pokrivanje tveganj.

Harmantzis (2003, str. 2) meni, da je izmed vseh različnih vrst tveganj, ki lahko vplivajo na podjetja, operativno tveganje med najbolj uničujočimi in najtežje predvidljivimi. Kljub temu da sta kreditno in tržno tveganje dodobra razumljiva in obvladljiva, operativno tveganje še vedno ostaja uganka za obvladovanje tveganj. Harmantzis (2003) meni, da gre

za relativno pomanjkanje razumevanja tega, kar nas ogroža. Za razliko od kreditnega in tržnega tveganja, ki ju v praksi obravnavamo na posameznih področjih poslovanja, so operativna tveganja del vseh poslovnih procesov. Gre za širši koncept kot le za tveganja zalednih služb.

Koristi zaščite pred tveganji izhajajo iz manjše oziroma zmanjšane spremenljivosti vrednosti podjetja, kar zmanjša verjetnost, da podjetje prizadenejo stroški finančne stiske. Stroški so neposredni – stroški sodišč, pravni stroški ipd. ter tudi posredni, oportunitetni stroški – stroški izgubljenih priložnosti in stroški izgubljenega zaupanja (Berk et al., 2005, str. 31).

Eden od najboljših obvladovanj poslovnih neuspehov in pomemben dejavnik uspešnosti poslovanja je primeren sistem notranjih kontrol, ki zmanjšuje nastanek tveganj in pripomore k dodani vrednosti podjetja. Uspešna globalna podjetja obvladujejo tveganja v mnogih primerih skozi določene ključne notranje kontrole in s tem zagotovijo dolgoročno trajnostno delovanje. Nedvomno se je pomen ustreznega kontrolnega sistema zaradi finančne krize v zadnjih letih okrepil. Notranje kontrolno okolje je ključni vidik vodenja podjetja in obvladovanja tveganj ter je bistvenega pomena za podporo doseganja ciljev podjetja in zaščito sredstev lastnikov. Uvedba dodatnih pravil in zahtev, ki izhajajo iz organizacijskih napak, kot tudi strmenje k delovanju v skladu z veljavnimi zakoni, s predpisanimi zahtevami ter politikami, pripelje do spoznanja, da so ključne notranje kontrole osredotočene na priložnosti, ki lahko ogrozijo poslovanje podjetja in dejansko lahko prihranijo čas in denar ter spodbujajo k ohranjanju vrednosti. Na podlagi intervjujev, ki so bili izvedeni s strani podjetja International Federation of Accountants v letu 2011, avtorji povzemajo, da bi moral biti uveljavljen sistem notranjih kontrol ključen del poslovanja. Vrsta finančnih kriz v preteklih letih je dokazala, da so procesi obvladovanja tveganj v nekaterih podjetjih, predvsem finančnih inštitucijah, pomanjkljivi. Glede na rezultate intervjujev z lastniki ta podjetja niso v celoti razumela tveganja, ki so jim izpostavljena. Pred zadnjim nizom finančne krize so bila številna podjetja osredotočena predvsem na kontrolo finančnega poročanja. Pri tem se je izpostavilo dejstvo, da je večina tveganja, ki je prizadelo podjetja, izhajala iz zunanjih okoliščin. Obvladovanje tveganj in sistem notranjih kontrol morata vključevati širšo perspektivo, če upoštevamo, da na podjetja vplivajo številne spremenljivke, pogosto zunaj njihovega neposrednega nadzora, in nastopati kot ključni del celostnega nadzora na vseh ravneh podjetja in v vseh poslovnih procesih (International Federation of Accountants, 2011).

Smernice za operativno tveganje (Združenje bank Slovenije, 2013) opredeljujejo, da naj se v podjetju vzpostavi politika, po kateri morajo vsi zaposleni upoštevati splošna načela skrbnega, varnega in učinkovitega ravnanja, predvsem pa prepoznati dejanska in potencialna operativna tveganja ter jih sporočati enoti za obvladovanje tveganj. Podjetja naj zagotovijo, da so nosilci posameznih produktov in procesov v podjetju v celoti odgovorni za operativno tveganje, ki nastaja v okviru njihovega poslovanja oziroma

izvajanja aktivnosti, ter pozorno prepoznavajo, analizirajo in uravnavajo tveganja, ki so jim (lahko) izpostavljena zaradi uporabe zunanjih izvajalcev.

Kot projektni vodja sem sodelovala pri vzpostavitvi sistema notranjih kontrol v slovenskem podjetju, ki se ukvarja s financiranjem. V sodelovanju z različnimi oddelki sem spoznala, da se zaposleni v večini zavedajo pomembnosti izvajanja notranjih kontrol, vendar le tistih, kjer se je v preteklosti že pripetil škodni dogodek, ter tistih, ki so bile v času popisov delovnih procesov določene kot ključne kontrole. Procesni management v podjetju je bil delno vzpostavljen, vendar zaradi obširnih področij, števila delovnih procesov in pomanjkljivega števila zaposlenih vsa ključna tveganja niso bila primerno dokumentirana.

Predmet proučevanja magistrskega dela so poslovna tveganja, osredotočim pa se na operativna tveganja in ugotavljam, ali učinkovit sistem notranjih kontrol zmanjšuje možnost pojava operativnih tveganj. Zaradi dejavnosti analiziranega podjetja se osredotočam na obvladovanje tveganj, ki se nanaša na finančne inštitucije.

Namen magistrskega dela je dvigniti zavedanje o pomembnosti obvladovanja operativnih tveganj v podjetju XY in širše ter prikazati postopek vpeljave notranjih kontrol v poslovanje. S tem bi uspešno obvladali nepotrebne poslovne odhodke, ki vplivajo na slabši rezultat poslovanja izbranega podjetja, ter hkrati zagotovili zanesljivost, točnost in pravočasnost računovodskega poročanja in skladnost z zakonodajo, s predpisi in z notranjimi pravilniki. Predlogi izboljšav bodo vodstvu podjetja zagotovili obvladovanje pomembnih tveganj in doseganje zastavljenih ciljev.

Cilja magistrskega dela sta:

1. proučiti problematiko obvladovanja operativnega tveganja in sistema notranjih kontrol s pomočjo strokovne in znanstvene literature domačih in tujih avtorjev, poročil, spletnih strani in člankov,
2. z empirično analizo na primeru slovenskega podjetja ugotoviti, ali so postopki obvladovanja tveganj primerni, in na tej podlagi podati predloge izboljšav.

V delu poskušam odgovoriti na raziskovalno vprašanje, ki se pojavlja ob obravnavani temi, kako učinkovit sistem notranjih kontrol zmanjšuje možnost pojava operativnih tveganj. Osrednja raziskovalna teza je, da sodobno podjetje za uspešno obvladovanje operativnih tveganj potrebuje primeren sistem notranjih kontrol. Ta bo preprečeval oziroma zmanjševal možnost ponovitve ključnih škodnih dogodkov. To se bo najintenzivneje odražalo pri podjetjih, ki bodo celovit postopek notranjih kontrol vpeljala v poslovne procese.

Struktura magistrskega dela predvideva štiri v celoto smiselno zaokrožena poglavja, tematika pa bo dodatno razčlenjena v podpoglavjih. Metodologija raziskovanja pri pripravi dela je raznovrstna. Velik poudarek je na teoretično-analitičnem delu, kjer gre predvsem za pregled in povzetek izsledkov strokovne literature, raziskav, člankov in razprav predvsem tujih avtorjev na področju izbrane tematike.

Analiza tveganj, ki pretijo podjetjem, je predstavljena v prvem poglavju, kjer se osredotočim predvsem na predstavitev pojma tveganja in vrste tveganj. Opiram se predvsem na tujo strokovno literaturo, poročila, raziskave, strokovne članke in deloma tudi na prispevke in literaturo domačih strokovnjakov s področja obvladovanja tveganj. V drugem poglavju magistrskega dela je podrobneje predstavljen model obvladovanja tveganj »Committee of Sponsoring Organization« (v nadaljevanju COSO).

V tretjem poglavju z metodo klasifikacije uvrstim pojem operativnih tveganj v širši koncept ostalih tveganj. Na operativnih tveganjih temelji postopek vzpostavitve sistema notranjih kontrol. V opis umestim tudi metodo kompilacije, s katero združim ugotovitve in spoznanja avtorjev, ki proučujejo ali delujejo na področju obvladovanja operativnih tveganj.

Četrto poglavje je namenjeno empirični analizi modela celovitega obvladovanja operativnih tveganj v podjetju XY in postopku vpeljave kontrolnega sistema. V okviru predstavitve postopka uporabim predvsem pridobljene praktične izkušnje sodelovanja pri postopku vpeljave sistema notranjih kontrol v enem od slovenskih podjetij, pridobljeno znanje s podiplomskega študija, znanje s strokovnih certificiranj s področja obvladovanja tveganj in preprečevanja prevar. Ugotavljam, ali postopek kontroliranja uspešno oziroma pravočasno prepozna možnost nastanka tveganja. Pri tem podam svoje mnenje glede izboljšav postopka. Magistrsko delo zaključim s sklepnimi ugotovitvami.

1 POSLOVNA TVEGANJA

1.1 Opredelitev in vrste tveganj

Na poslovni rezultat posameznega podjetja vplivajo tako notranji kot zunanji dejavniki. COSO (2011, str. 38) opredeljuje tveganje kot možnost, da se bo zgodil nek dogodek, ki bo neugodno vplival na zastavljene cilje podjetja. Podjetja se premalo zavedajo, da med ključna tveganja sodi tudi neizkoriščanje priložnosti in nepripravljenosti za sprejemanje in ustrezno obvladovanje sprememb. Obdobja prebojnih tehnologij in druge spremembe se izredno hitro skrajšujejo. Podjetja, ki ne bodo sposobna pravočasno zaznavati priložnosti ali jih ne bodo dovolj hitro izkoristila, bodo izgubljala proti tistim, ki to zmorejo (Vezjak, b. l., str. 1).

Tveganja se pogosto opredeli kot možnosti nevarnosti, izgube, poškodb ali drugih škodljivih posledic. Pri računovodskem in finančnem tveganju je upoštevano v okviru drevesa odločanja, verjetnostne razporeditve, analize stroškov in dobička, diskontiranem denarnem toku, modelih oblikovanja cen osnovnih sredstev in tehnik obvladovanja (Collier, Berry, & Burke, 2006). Upravljanje tveganj (angl. *Risk Governance*) se nanaša na usmeritev in nadzor sistema za obvladovanje tveganj. Gre za povezavo med upravljanjem podjetij (angl. *Corporate Governance*) in obvladovanjem tveganj (angl. *Risk Management*). Zagotavlja strukturo sistema za obvladovanje tveganj in določa odgovornosti, pooblastila in odgovornost v sistemu upravljanja s tveganji ter pravila in postopke za sprejemanje odločitev pri upravljanju s tveganji (Lundqvist, 2015). V magistrskem delu je poudarek na obvladovanju tveganj v finančnih inštitucijah.

Berk et al. (2005, str. 27) pojem tveganje uporabljajo v različnih zvezah: tveganje kot priložnost, ki predpostavlja, da obstaja povezava med tveganjem in donosnostjo, tveganje kot nevarnost ali grožnja in tveganje kot porazdelitev negotovih prihodnjih rezultatov. Glede na mogoče izide in njihove posledice delijo tveganja na dve skupini: čista tveganja; tveganja, pri katerih obstaja možnost nastanka izgube brez koristi, in špekulativna tveganja; tveganja, pri katerih obstaja možnost nastanka izgube in koristi. Vodstvo podjetja najpogosteje dojema tveganje kot nevarnost ali grožnjo v smislu negativnih vplivov mogočih dogodkov, kot so zlorabe, kraje, finančna izguba, izguba ugleda podjetja, tožbe, odpovedi sistemov.

Veliko pozornosti zahtevajo tudi globalna tveganja, na katera se osredotoča World Economic Forum v zadnjem poročilu o globalnih tveganjih (Global Risk Report, 2016), saj ostajajo aktualna zaradi svojega kombiniranega vpliva na gospodarska tveganja, vključno z davčno krizo v ključnih gospodarstvih in visoko brezposelnostjo, ki ju dopolnjujejo kibernetski napadi[1] in izrazite družbene nestabilnosti. Njihova ocena odraža potencialno velik vpliv na četrto industrijsko revolucijo v gospodarstvu in družbi ter poudarja skrb za zagotavljanje prihodnjih koristi. Rezultati anketiranja zasebnega sektorja, ki ga je v letu 2016 izvedel World Economic Forum na podlagi 140 gospodarstev, razkrivajo brezposelnost ter pretrese zaradi sprememb cene energije kot največja tveganja v svetovnem merilu v naslednjih desetih letih. Gospodarska tveganja prevladujejo predvsem v Evropi, vključno z davčno krizo, nezaposlenostjo in napihnjenimi cenami nepremičnin in energije; slednje so med drugim tudi glavna skrb v Kanadi, medtem ko v Združenih

[1] Mrežni vandalizem: napadi, ki kazijo internetne strani, zanikanje državnih napadov. Ti napadi so po navadi izvedeni hitro in ne povzročijo veliko škode. Propaganda: politična sporočila se lahko razširijo do vsakega, in to predvsem s pomočjo interneta, do katerega dostopa že velika večina. Zbiranje podatkov: zaupne informacije, ki niso ustrezno zavarovane, so lahko prestrežene in celo modificirane z drugega dela sveta, to pa se omogoči predvsem z dobrim vohunstvom. Razdvojitev opreme: vojaške sile, ki uporabljajo računalnike in satelite za koordinacijo, so v nevarnosti pred takšno obliko napada. Povelja in sporočila so lahko prestrežena in spremenjena, kar vojake postavi v zelo nevaren položaj. Napad na pomembno infrastrukturo: elektrika, voda, nafta, komunikacije in logistika so vsi občutljivi na kibernetski napad. Ponarejena strojna oprema: običajna strojna oprema, uporabljena v računalnikih in medmrežju, ima slabonamerno programsko opremo skrito znotraj programske opreme ali morda celo v mikroprocesorju.

državah Amerike največje tveganje predstavljajo kibernetski napadi. Anketiranci iz srednje Azije in Rusije so zaskrbljeni zaradi javnofinančne krize in brezposelnosti, neobvladljive inflacije in meddržavnih konfliktov. Vzhodno Azijo in Pacifik pa poleg okoljskega tveganja ogrožajo tudi cene energije, napihnjene cene nepremičnin in kibernetski napadi. Iz narave dejavnosti podjetja izhaja več vrst tveganj, ki so po vsebini in obsegu različna. Obseg prevzemanja tveganj se razlikuje glede na dejavnost, organiziranost, velikost in poslovno kulturo podjetja. Pri poslovanju se to odraža v načinu pojavljanja na trgu (agresivnost, inovativnost), raznovrstnosti produktov, koncentraciji kreditnega portfelja ipd. Tveganja predstavljajo verjetnost, da bodo dogodki v prihodnosti vplivali na poslovanje in stabilnost podjetja, na njegove prihodke in kapital. Banka Slovenije ustrezno oceni tveganja finančnih institucij, ovrednoti in skladno s svojimi pooblastili ustrezno ukrepa (Banka Slovenije, 2007b, str. 11).

Tveganja, ki jih opredelim v nadaljevanju, so s strani Banke Slovenije primerna za ocenjevanje in smiselna za medsebojno razlikovanje zaradi kakovostnejšega razumevanja prevzemanja tveganj[2] in hkrati pomembna za izbrano podjetje. Poleg spodaj navedenih tveganj obstajajo še številna druga tveganja, kot so na primer strateško tveganje, kapitalsko tveganje, tveganje dobičkonosnosti.[3] Operativno tveganje podrobneje predstavljam v tretjem poglavju o obvladovanju operativnega tveganja.

1.1.1 Kreditno tveganje

Kreditno tveganje je tveganje izgube zaradi spremembe dejavnikov, ki vodijo kreditno kakovost sredstev. Ti vključujejo neželene učinke, ki izhajajo iz migracije bonitetnih razredov, vključno z neplačili in dinamiko stopenj izterjave (Crouhi, Galai, & Mark, 2006). Izraz kreditno tveganje je opredeljen kot možnost delne ali popolne izgube zaradi neizpolnjevanja pogodbenih obveznosti iz pogodb, sklenjenih v okviru kreditnih poslov zaradi poslabšanja kreditne sposobnosti pogodbenega partnerja. Izraz poslabšanje kreditne sposobnosti vključuje tako dogodke neplačil kot poslabšanje kreditne sposobnosti, ki ne vključuje nujno izgube terjatev (Podjetje XY, 2016a).

Banka Slovenije (2007b, str. 24) pod pojem kreditno tveganje vključuje vrsto podkategorij, ki so v strokovni literaturi mnogokrat ločeno navedene. Tveganje koncentracije je tveganje nastanka izgube v primeru prekomerne izpostavljenosti do posamezne osebe, skupine povezanih oseb in oseb, ki jih povezujejo skupni dejavniki tveganj, kot so: isti gospodarski sektor oziroma geografsko območje ali istovrstni posli. Listinjenje je posel, pri katerem se kreditno tveganje, povezano s posamezno osnovno izpostavljenostjo ali skupino osnovnih

---

[2] Banka Slovenije se je na podlagi dokumenta »The Application of the Supervisory Review Process under Pillar 2" (Committee of European Banking Supervisors – CEBS CP03, junij 2005) odločila za pomembna tveganja.

[3] Posamezna tveganja so opredeljena v dokumentu »Proces ocenjevanja tveganj« na spletni strani https://www.bsi.si/library/includes/datoteka.asp?DatotekaId=2437.

izpostavljenosti, razdeli na vsaj dva dela, ki odražata različno stopnjo kreditnega tveganja. Zanj je značilno, da so plačila investitorjem odvisna od izpolnjevanja obveznosti dolžnikov pri skupini osnovnih izpostavljenosti in kreditnih izboljšav ter podrejenosti delov posojil, ki so podlaga za določitev porazdelitve izgub med celotnim trajanjem tega posla. Deželno tveganje je tveganje nastanka izgube v primeru mednarodnega kreditiranja in je povezano z ekonomskim, socialnim in političnim okoljem dolžnikove države. Posebna oblika deželnega tveganja je transferno tveganje, ki obstaja, kadar dolžnikova obveznost ni nominirana v lokalni valuti.

Kreditno tveganje se praviloma pojavlja v bankah, na vseh področjih bančnega poslovanja, kjer nastajajo tvegane aktivne bilančne postavke, ki obsegajo vse dospele in nedospele kredite vseh ročnosti, naložbe v vrednostne papirje in dolgoročne naložbe v kapital, terjatve iz finančnih najemov, terjatve iz izvedenih (izpeljanih) finančnih instrumentov, naložbe v naložbene nepremičnine, obračunane obresti, nadomestila in provizije ter terjatve za plačane garancije, vloge pri bankah ter druge postavke, ki jih je mogoče razporediti na posameznega dolžnika in so merjene po metodi odplačne vrednosti, nabavni vrednosti ali po pošteni vrednosti (Banka Slovenije, 2007b, str. 24). Spremljanje kreditnega tveganja je pomembno tudi za ostale finančne družbe. Glavni namen je analizirati denarne tokove in obvestiti vodstvo o vseh pomembnih premikih portfelja, ki vplivajo na poslovne odločitve.

Heffernan (2005, str. 156) opredeljuje pet načinov obvladovanja kreditnega tveganja: natančna določitev cen posojila, kreditno omejevanje, zavarovanje terjatev, razpršitev tveganj ter sredstva za listinjenje in/ali uporaba kreditnih izvedenih finančnih instrumentov. Uteži, ki se uporabljajo za vsako od metode, se razlikujejo glede na to, ali je posojilo namenjeno podjetjem ali fizičnim osebam.

Točka (d) člena 59(3) Uredbe (EU) št. 909/2014 določa, da mora izvajalec bančnih storitev za obvladovanje ustreznega kreditnega tveganja sprejeti visoko likvidno zavarovanje z minimalnim kreditnim in tržnim tveganjem. V isti točki je določeno, da se v specifičnih primerih lahko uporabijo druge vrste zavarovanja, ki niso visoko likvidno zavarovanje z minimalnim kreditnim in tržnim tveganjem, pri čemer se upošteva ustrezen odbitek. Da bi se to omogočilo, bi bilo treba določiti jasno hierarhijo kakovosti zavarovanj, da bi lahko razlikovali, katero zavarovanje je lahko sprejemljivo za popolno kritje izpostavljenosti zaradi kreditnega tveganja, katero zavarovanje je sprejemljivo kot likvidno sredstvo in za katero zavarovanje, ki je sicer še vedno sprejemljivo za zmanjšanje kreditnega tveganja, so potrebna primerna likvidna sredstva. Ponudniki zavarovanja se ne bi smeli ovirati pri prosti zamenjavi zavarovanja glede na razpoložljivost sredstev ali njihove strategije obvladovanja sredstev in obveznosti (Evropska komisija, 2016, str. 11).

Da pripomoremo k minimiziranju kreditnega tveganja, je treba poznati koncepta moralnega hazarda in napačne izbire. »Moralni hazard imenujejo ekonomisti okoliščine za

sprejemanje odločitev, v katerih se tisti, ki odločitve sprejema, zaveda, da ne bo nosil posledic svojih tveganih dejanj, ampak da lahko tveganja prevali na druge. Moralni hazard je ključni problem slovenske tranzicije« (Kovač, 2013). Asimetričnost informacij privede do problema napačne izbire, ki nastopi takrat, ko se proizvodi različne kakovosti prodajajo po enaki ceni. Z asimetričnimi informacijami blago slabše kakovosti izrine blago boljše kakovosti s trga, na trgu se ne vzpostavi vsestransko koristna menjava, na trgu je preveč proizvodov slabe kakovosti in premalo proizvodov dobre kakovosti, pojavi se napačna izbira; na trgu bodo ostali le proizvodi slabše kakovosti (Prašnikar, 2012). Nekateri so mnenja, da je moralni hazard del tveganja ugleda podjetja, kar je v nasprotju z mnenjem Chorafas (2002, str. 60), ki trdi, da so osnovni koncepti drugačni. Po drugi strani meni, da moralni hazard prispeva k povečanju tveganja ugleda, ker zavira etična načela in zaobide vrednote finančne odgovornosti.

1.1.2 Tržno in likvidnostno tveganje

Tržno tveganje je tveganje izgube zaradi sprememb tržnih dejavnikov. Lahko izhaja iz sprememb obrestnih mer, deviznih tečajev ali faktorjev kapitala in cen surovin (Crouhi et al., 2006, str. 14). Crouhi et al. (2006, str. 27) opredeljujejo štiri glavne vrste tržnega tveganja: obrestno tveganje[4], tveganje lastniških vrednostnih papirjev[5], valutno tveganje[6] in tveganje cen blaga[7]. Tržno tveganje se nanaša na tveganje, ki izhaja neposredno ali posredno iz nihanja ali nestabilnosti tržnih cen sredstev, obveznosti in finančnih instrumentov. Finančna teorija razume tveganje kot porazdelitev nepričakovanih rezultatov investiranja zaradi gibanja finančnih spremenljivk. Za neko finančno podjetje oziroma finančnega investitorja je pomembno gibanje rezultatov (dobičkov) iz trgovanja s finančnimi instrumenti, kar pomeni, da je potrebno spremljanje tako pozitivnih kot tudi negativnih odmikov − oboji odmiki so namreč viri tveganja. Finančnega investitorja zanima, kakšen rezultat bo dosegel na koncu obdobja investiranja. Ker vsak odmik od nekega pričakovanega rezultata prinaša tveganje, da bo rezultat na koncu obdobja različen od pričakovanega, je pomembno spremljanje tako pozitivnih kot negativnih odmikov. S tem se namreč poveča možnost uravnavanja rezultata oziroma se lahko z različnimi pristopi zmanjša tveganje in s tem poveča točnost pričakovanega rezultata v primerjavi z dejanskim oziroma doseženim (Banka Slovenije, 2006, str. 2).

Izbrano finančno podjetje, ki se ukvarja z upravljanjem s slabimi naložbami, s trgovanjem z lastnimi nepremičninami in z dajanjem lastnih nepremičnin v najem ter s podjetniškim in poslovnim izobraževanjem (podrobneje predstavljeno v 4. poglavju), definira tržno tveganje kot potencialno izgubo, ki lahko nastopi zaradi sprememb tržnih cen ali zaradi sprememb parametrov, ki povzročijo spremembe teh tržnih cen. Vključuje zlasti tveganje

---

[4] Tveganje, da bo vrednost fiksne zapadlosti padla zaradi povečanja tržnih obrestnih mer.
[5] Tveganje, povezano z nestanovitnostjo cen delnic.
[6] Tveganje izhaja iz odprtih ali nepopolno zavarovanih pozicij v določeni valuti.
[7] Koncentracija dobave v rokah nekaj dobaviteljev lahko poveča nestanovitnost cen surovin na trgih.

sprememb obrestne mere in valutno tveganje. Ugotovljena tržna tveganja so predmet merjenja, analiziranja in ocenjevanja. V ta namen je treba uporabljati in redno preverjati zlasti kvantitativne in kvalitativne metode s preizkušanjem na podlagi primerjav s preteklimi rezultati ter postopki za preverjanje in potrjevanje. Pri tem je treba upoštevati, analizirati in ovrednotiti medsebojno povezanost tržnih tveganj (Podjetje XY, 2016a).

Tržno tveganje se v prvi vrsti meri s tvegano vrednostjo (angl. *Value-at-Risk*; v nadaljevanju VaR). VaR je mogoče opredeliti kot najhujšo izgubo, ki bi jo lahko pričakovali pri posredovanju vrednostnega papirja ali portfelja v določenem časovnem obdobju (na primer en dan ali 10 dni za namene regulativnega poročanja o kapitalu) glede na določeno stopnjo verjetnosti (znano kot stopnja zaupanja). Večina modelov VaR je zasnovana za merjenje tveganja v kratkem časovnem obdobju, na primer en dan ali 10 dni v primeru merjenja tržnega tveganja, ki ga zahtevajo regulatorji za regulatorni kapital. VaR ima širok spekter uporabe, saj zagotavlja skupno, dosledno in integrirano mero tveganja med dejavniki tveganja, instrumenti in razredi sredstev; skupno merilo tveganja in tveganju prilagojeno spremljanje; pripomore k določitvi mejne vrednosti tveganja za poslovne linije ter zagotavlja merilo tveganja, ki je razumljivo vodstvu podjetij (Crouhi, et al., 2006).

Po navedbah Banke Slovenije (2006, str. 1) tvegana vrednost predstavlja mero tveganja, ki meri največjo izgubo, ki naj bi jo utrpel imetnik določenega portfelja ob nekem danem intervalu zaupanja v določenem investicijskem obdobju. Pri izračunu VaR nam rezultat pove, kolikšna je največja izguba, ki jo lahko pričakujemo v nekem časovnem obdobju ob dani stopnji zaupanja ($1-\alpha$). Armeanu, Vintila, Barbu in Nedelescu (2010) navajajo, da je tveganje ocenjeno s pomočjo statističnih in simulacijskih metod, ki merijo volatilnost[8] vrednostnega papirja v portfelju. Z drugimi besedami, VaR predstavlja α-odstotni centil določene porazdelitve dobičkov in izgub v nekem (investicijskem) obdobju (Torkar, 2005).

Po besedah Chorafasa (2002, str. 147) so mnogi dobro poznani finančni analitiki mnenja, da je tudi likvidnostno tveganje, čeprav v knjigah to ni zapisano, največja izpostavljenost finančnega podjetja, ker vpliva na rezerve in obveznosti podjetja v kratkoročnem, srednjeročnem in dolgoročnem obdobju. Likvidnosti ni treba izmeriti le v kvantitativnem, ampak tudi v kvalitativnem smislu. Kapital prvega reda finančnih inštitucij (angl. *Tier 1*) vzpostavlja likvidnostne limite na podlagi dveh referenčnih ravni: likvidnostno tveganje − glede na vrsto tveganja, dejavnike tveganja, valuto in trg; obseg likvidnosti − po odprtem položaju in posamezni varnosti v svojem portfelju ali v portfelju, za katerega so zainteresirani za prihodnje naložbe. Regulatorji ob proučitvi zmožnosti finančne inštitucije, da preživi, iščejo odgovore na naslednja vprašanja: ali so meje tveganja primerne za poslovanje finančne inštitucije, ali politike omejujejo notranje trgovanje in razmerje

[8] Volatilnost ali nihajnost je statistična mera za verjetnost, da cena (delnice ali točke sklada) v kratkem času močno zraste ali pade. Izražena je z varianco ali s standardno deviacijo. Merilo za relativno volatilnost delnice glede na celoten trg oziroma izbrani indeks se imenuje beta.

tveganja/dobička, ki ga pričakuje vodstvo, ali se transakcije spremljajo v realnem času ter v kakšni meri je najvišje vodstvo občutljivo na odstopanja in prekoračitev meja (Chorafas, 2002, str. 148).

Likvidnostno tveganje lahko izhaja iz katerekoli pomožne storitve, ki jo opravlja podjetje. V okviru za obvladovanje likvidnostnih tveganj bi morali opredeliti tveganja, ki izhajajo iz različnih pomožnih storitev, in ustrezno razlikovati njihovo obvladovanje. Za pokritje vseh likvidnostnih potreb, vključno z likvidnostnimi potrebami izvajalca storitev znotraj enega dne, bi se moralo z okvirom za obvladovanje likvidnostnih tveganj zagotoviti, da so izpolnjene obveznosti v zvezi s plačili in poravnavo v vseh valutah poravnave v okviru sistema poravnave vrednostnih papirjev, ko obveznosti zapadejo, tudi znotraj enega dne (Evropska komisija, 2016, str. 12). Po drugi strani Banks in Dunn (2003, str. 68) menita, da se likvidnostno tveganje lahko meri s pomočjo analitične formule in scenarijev. Kot primer navajata tudi poudarek in spremljanje likvidnostnega tveganja na bilančnih in zunajbilančnih postavkah. Gre za spremljanje morebitne neusklajenosti med sredstvi in obveznostmi.

Tveganje mora biti razvidno že v načrtu poslovanja in usklajenem načrtu financiranja. Neujemanje ročnosti sredstev in obveznosti mora ostati v središču pozornosti, nove ročnosti pa je treba uskladiti z možnostmi financiranja v prihodnosti. Zato mora obvladovanje likvidnosti znotraj podjetja zagotavljati, da lahko podjetje učinkovito zadosti tako pričakovanim kot nepričakovanim, trenutnim in prihodnjim denarnim tokovom ter potrebam zavarovanja, brez vpliva na njeno dnevno poslovanje ali finančno stanje. Dodatno mora obvladovanje likvidnosti nadzorovati strukturno likvidnost v statičnem in dinamičnem vidiku (Podjetje XY, 2016a).

1.1.3 Tveganje objekta

Tveganje objekta (angl. *Object Risk*) predstavlja potencialna izguba, ki je posledica nihanja tržne vrednosti sredstev v portfelju podjetja. Ta vključuje tudi portfelje hčerinskih družb, podjetij, ki imajo v lasti nepremičnine, podjetja s posebnim namenom itd. V podjetjih so ta vrsta sredstev lahko na primer vsa zasežena sredstva – premičnine (na primer vozila, stroji, oprema) in nepremičnine. Nihanja tržne vrednosti najbolj vplivajo na vrednost nepremičnin, ki so po navadi v portfelju tudi daljše časovno obdobje. Upoštevajo se tudi premičnine, čeprav niso v takšnem obsegu, da bi bistveno vplivale na uspešnost in rezultate podjetij. Tveganje objekta pomeni bistveno tveganje, ki se meri posamezno, ločeno od drugih tveganj, z namenom, da se prepozna tveganost tovrstnega premoženja v portfelju družbe in s tem pridobi informacije za notranje kapitalske zahteve. Zato je tveganje objekta del postopka razporejanja notranjega kapitala in merjenja uspešnosti, ki se lahko pojavi v treh oblikah. Kot prvo se lahko pojavi v finančnih inštitucijah (na primer bankah). Če dolžnik ne plača dolga, prevzame podjetje njegovo podjetje in obravnava njegova zastavljena sredstva (zavarovanja) kot svoja lastna sredstva (še posebno

nepremičnine in trajno blago večjih proizvajalcev). Lahko se pojavi pri financiranju: finančnem leasingu ali pri poslovnem najemu. Če lizingojemalec ne plača dolga, postane sredstvo, ki je predmet leasinške pogodbe, last leasinškega podjetja (zaseg) (Podjetje XY, 2014).

1.2 Ravni obvladovanja tveganj

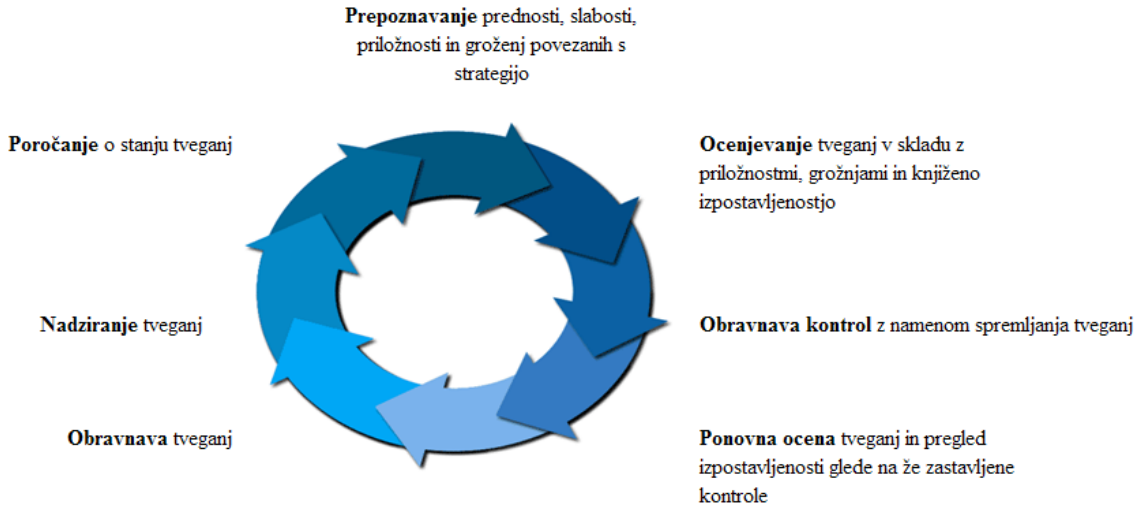
Obvladovanje tveganj v podjetju je postopek, ki ga izvajajo vodstvo podjetja, vodje področij ter zaposleni z namenom določitve strategij v celotnem podjetju in pravočasnem odkrivanju morebitnih dogodkov, ki bi lahko vplivali na podjetje (Arena, Arnaboldi, & Azzone, 2010, str. 1). Mnoga podjetja izvajajo postopke obvladovanja tveganj z namenom povečanja učinkovitosti svojih dejavnosti s končnim ciljem povečevanja vrednosti podjetja (Beasley, Clune, & Hermanson, 2005, str. 523). Gordon, Loeb in Tseng, (2009, str. 302) opredeljujejo obvladovanje tveganj kot disciplino, s katero podjetja v panogi ocenjujejo, nadzirajo, financirajo in spremljajo tveganja iz vseh virov z namenom povečanja kratkoročne in dolgoročne vrednosti podjetja.

Profili obvladovanja tveganj delijo vodstvene naloge na kontroliranje, spremljanje, smernice za izvajanje in učinkovito raven izvajanja. Odgovornost za kontrolo opredeljujejo strateški cilji v okviru strategije tveganja in vzpostavljajo lokalni okvir za izvajanje. Odgovornost spremljanja vključuje spremljanje skladnosti in izvajanja strateških zahtev v danem okviru izvajanja, opredeljuje spremembe in prilagajanje potrebam, nasprotja in ovire kot posledica pravnega vodenja ali lokalnih pravnih omejitev ter sproži ustrezne postopke za reševanje tovrstnih zadev. To pomeni, da se spremlja razvoj portfelja kot tudi procese neskladnosti poslovanja, spremljanje skladnosti z omejitvami, orodja in procese. Smernice za izvajanje vključujejo ključno podporo in operativno sodelovanje pri uresničevanju strateških ciljev v podjetju. Izražajo jasna navodila za vodenje in potrebno podporo za izvajanje in zagotovitev pomoči pri izvajanju ukrepov za izboljšanje in posledično odpravo ugotovljenih pomanjkljivosti v formalnem in materialnem smislu. Učinkovita raven izvajanja zahteva podporo za ustvarjanje optimalnih pogojev za izvajanje, daje povratne informacije o morebitnih ovirah in sproži ustrezne mehanizme za reševanje sporov. To pomeni, da podjetja za zagotavljanje obvladovanja tveganj razvijajo in vzdržujejo primerne sisteme, hkrati pa v svoje poslovanje vpeljejo lokalne politike, priročnike in delovna navodila, ki podpirajo njihovo delovanje (Podjetje XY, 2016a).

Slika 1 kot primer predstavlja cikličen proces obvladovanja tveganj v podjetju XY. Načrt poslovanja podjetja se upošteva kot izhodišče za ugotavljanje prednosti, pomanjkljivosti, priložnosti in groženj. V podjetju se upošteva vsako priložnost in grožnjo z vidika negotovosti in zmožnosti obvladovanja tveganja. V to so vključeni pričakovani učinek, verjetnost pojava ali izpostavljenost tveganjem. Obravnava kontrol z namenom spremljanja tveganj je namenjena nadzoru že vzpostavljenih kontrol in ukrepov, ki so že bili izvedeni in pripomorejo k zmanjšanju tveganj. Ponovno se oceni vpliv in verjetnost preostalega

tveganja. Takšna ocena vključuje naknadne kontrole. Na ravni ocenjevanja je treba navesti, katere priložnosti in grožnje bi bilo treba sprejeti z najvišjo prioriteto pri načrtovanju ukrepov. Obravnava tveganj se razlikuje glede na: oceno učinka in verjetnosti preostalega tveganja; odstopanja za posebna tveganja in možnosti nadzorovanja tveganja. Tveganja je treba spremljati in poročati z namenom, da se zaključijo ukrepi za reševanje, poročajo vse spremembe ocene učinka ter zagotovi, da so tveganja še vedno pomembna kljub spreminjajočemu se okolju.

Slika 1: Obvladovanje tveganj v podjetju XY



Vir: Podjetje XY, Politika tveganja, 2016, str.15.

Cilj obvladovanja tveganja je v sposobnosti objektivnega presojanja tveganja oziroma ocenjevanja nevarnosti z zdravo mero razuma in ne naivnega izkoriščanja priložnosti. Vodstvo mora najti ustrezno ravnotežje in hkrati nenehno imeti v mislih vzdržno konkurenčno sposobnost podjetja (Berk et al., 2005, str. 53).

2 NOTRANJE KONTROLE

Pooblaščeni revizor Perner (b. l., str. 2) meni, da so lastniki in poslovodstva podjetij že od nekdaj iskali poti in načine, kako bolje in učinkoviteje nadzirati podjetja. S tem namenom si organizirajo sistem notranjih kontrol, ki naj bi zagotavljal uresničevanje poslanstva in ciljev podjetja ter tako minimiziral pojav nepravilnosti v poslovnih procesih. Tako uspešen sistem notranjih kontrol omogoči obvladovanje poslovanja podjetja, ki ga zahtevajo hitro spreminjajoče se gospodarsko okolje, spremembe navad kupcev in oblikovanje prihodnje rasti podjetja. Hkrati organizacija COSO (2011, str. 1) opredeljuje notranje kontrole kot proces, ki je pod vplivom vodstva podjetja in ostalih zaposlenih, zasnovan z namenom razumnega zagotovila doseganja ciljev v naslednjih kategorijah: uspešnost in učinkovitost poslovanja, zanesljivost poročanja ter skladnost z veljavno zakonodajo in s predpisi.

Ta definicija poudarja, da je notranja kontrola: proces, ki vsebuje redne naloge in aktivnosti (kontrola je del delovnega procesa); izvedena s strani zaposlenih; ne gre samo za priročnike in sisteme, temveč za ljudi na vseh ravneh podjetja, ki imajo vpliv na notranje kontrole; zmožna prispevati določena zagotovila vodstvu podjetja; usmerjena k ciljem v eni ali več ločenih prekrivajočih se kategorijah in prilagodljiva strukturi podjetja.

Urad Republike Slovenije za nadzor proračuna (2004, str. 9) določa, da je notranje kontroliranje potrebno, ker postajajo podjetja večja in kompleksnejša in neposreden nadzor posameznikov ni več mogoč. Poleg tega se podjetja zaradi notranjih in zunanjih dejavnikov soočajo z različnimi tveganji, ki onemogočajo doseganje ciljev. Področje obvladovanja tveganj je še posebej podrobno opisano v poročilu COSO (2011) v Združenih državah Amerike in Turnbullovem poročilu (angl. *Turnbull report*)[9] v Veliki Britaniji. Poročilo COSO je v prvi obliki nastalo leta 1992 in podrobno opisuje metodologijo, s pomočjo katere lahko podjetje oceni uspešnost notranjih kontrol in prepozna možnosti njegovih izboljšav. To poročilo je postalo osnova standardov upravljanja podjetij in notranje revizije v številnih državah ter je močno vplivalo tudi na pripravo Sestavljenega kodeksa upravljanja[10] v Veliki Britaniji.

2.1 Sestavni deli notranjega kontroliranja

Organizacija COSO (2011, str. 10) opredeljuje pet komponent notranje kontrole in sedemnajst načel, ki predstavljajo temeljne koncepte komponent in zagotavljajo uporabniku jasno podlago za vzpostavitev in uveljavitev sistemov notranjega kontroliranja ter razumevanja zahtev za uspešno notranje kontroliranje.

Slika 2: Okvir notranjih kontrol COSO

Vir: A. Chambers, Tolley's Internal Auditor's Handbook, 2005, str. 337.

[9] Turnbullovo poročilo je podrobno predstavljeno na povezavi https://www.frc.org.uk/getattachment/5e4d12e4-a94f-4186-9d6f-19e17aeb5351/Turnbull-guidance-October-2005.aspx.

[10] Sestavljeni kodeks upravljanja (angl. UK *Corporate Governance code*) je podrobno predstavljen na povezavi https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance/UK-Corporate-Governance-Code.aspx

Prepoznamo jih lahko z opazovanjem načina vodenja organizacije in vključenosti v proces vodenja. Komponente notranjih kontrol se nanašajo na vsa podjetja, vendar jih manjša podjetja uporabijo drugače kot velika. Kontrole pri manjših podjetjih so lahko manj formalne in manj strukturirane, vendar je sistem notranjih kontrol še vedno lahko (zelo) uspešen. Komponente notranjih kontrol, navedene v Sliki 2, so nadzor, informacije in komunikacije, kontrolne aktivnosti, ocena tveganja in kontrolno okolje.

2.1.1 Kontrolno okolje

Kontrolno okolje je sestav standardov, procesov in struktur, ki predstavljajo osnovo za sistem notranjih kontrol v podjetju. Vodstvo podjetja in višji management vzpostavita smernice glede pomembnosti notranjih kontrol, vključno s pričakovanimi standardi ravnanja (COSO, 2011, str. 25).

Organizacija COSO (2011, str. 25) opredeljuje naslednja načela, ki so povezana s kontrolnim okoljem:

1. izkazovanje zavezanosti celovitosti: organizacija predstavlja obvezo skladnosti in etičnim vrednotam,
2. izvajanje nadzora: člani vodstva predstavljajo neodvisnost od vodij področij in izvajajo nadzor razvoja in izvajanja notranjih kontrol,
3. vzpostavitev strukture, pristojnosti in odgovornosti: vodje področij vključno z nadzornim odborom vzpostavijo strukturo, poročevalske linije, pristojnosti in odgovornosti pri uresničevanju ciljev,
4. izkazovanje zavezanosti kompetencam zaposlenih: podjetje stremi k zavezanosti in razvoju pobud za privabljanje, razvoj in zadržanje usposobljenih zaposlenih v skladu s cilji,
5. uveljavljanje odgovornosti: podjetje od posameznikov zahteva odgovorno spremljanje notranjih kontrol z namenom doseganja ciljev.

2.1.2 Ocena tveganj

Vsako podjetje se sooča z vrsto tveganj notranjih in zunanjih virov. Tveganje je opredeljeno kot možnost, da se pojavi nek dogodek, ki bo posledično vplival na dosežke zastavljenih ciljev. Ocenjevanje tveganj omogoča dinamičen in ponavljajoči se proces prepoznavanja in ocenjevanja tveganj za doseganje ciljev. Ocenjevanje tveganj nadalje tudi oblikuje osnovo za opredelitev, kako se bodo tveganja obvladovala. Pogoj za oceno tveganj je določitev ciljev, ki so povezani na različnih ravneh v podjetju. Vodstvo podjetja določa jasne cilje znotraj zalednih oddelkov ter glede poročanja in skladnosti poslovanja z namenom lažje opredelitve in analize tveganj. Ocenjevanje tveganj poleg tega od vodstva podjetij zahteva, da prouči in upošteva možne vplive sprememb v zunanjem okolju, ki

lahko vplivajo na poslovni model in izničijo delovanje notranjih kontrol (COSO, 2011, str. 51).

Organizacija COSO (2011, str. 51) opredeljuje naslednja načela, ki so povezana z ocenjevanjem tveganj:

1. določitev pomembnih ciljev: podjetje jasno določi cilje z namenom lažjega prepoznavanja in ocenjevanja tveganj.
2. ugotavljanje in analiziranje tveganj: podjetje prepoznava tveganja, ki vplivajo na poslovni rezultat podjetja in analizira tveganja kot podlago za določanje postopkov, ki bodo ta tveganja obvladovali.
3. ocenjevanje tveganja prevar in goljufij: podjetje preuči možnosti prevar in goljufij, tako notranjih kot zunanjih, ki bi lahko negativno vplivali na poslovni rezultat.
4. prepoznavanje in analiziranje pomembnih sprememb: podjetje prepoznava in ocenjuje spremembe, ki bi lahko pomembneje vplivale na sistem notranjih kontrol.

2.1.3 Kontrolne aktivnosti

Kontrolne aktivnosti so aktivnosti, ustanovljene s politikami in postopki, ki pripomorejo k temu, da se smernice, ki preprečujejo oziroma zmanjšujejo tveganja, redno izvajajo. Kontrolne aktivnosti se izvajajo na vseh področjih v podjetju na različnih stopnjah, v poslovnih procesih in informacijskem okolju (računalniške aplikacije in programi, ki podpirajo poslovanje podjetja). Kontrole so lahko preventivne (angl. *preventive control)* ali odkrivajoče (angl. *detective control)* ter lahko zajemajo vrsto ročnih in avtomatskih aktivnosti, kot so na primer dana pooblastila (angl. *authorizations*) ali dovoljenja, preverjanja, usklajevanja in pregledi uspešnosti poslovanja. Ločevanje nalog (angl. *segregation of duties*) je običajno vgrajeno v izbor in razvoj kontrolnih aktivnosti. V podjetjih, ki tega ne uporabljajo, vodstvo izbere in razvija druge kontrolne dejavnosti (COSO, 2011, str. 75).

Organizacija COSO (2011, str. 75) opredeljuje naslednja načela, ki so povezana s kontrolnimi aktivnostmi:

1. izbor in razvoj kontrolnih aktivnosti: podjetje si izbere in razvija kontrolne aktivnosti, ki pripomorejo k zmanjševanju oziroma preprečevanju ponovitve škodnega dogodka;
2. podjetje izbere in razvija ključne kontrolne aktivnosti v računalniških programih, ki podpirajo poslovanje podjetja;
3. vpeljava kontrolnih aktivnosti prek politik in delovnih postopkov: podjetje vpelje kontrolne aktivnosti, opredeljene v politikah, ki določajo, kaj se pričakuje, vključno z ustreznimi postopki za izvedbo.

2.1.4 Informiranje in komuniciranje

Podjetje za uspešno opravljene notranje kontrolne aktivnosti potrebuje vse potrebne informacije. Vodstvo podjetja pridobi ustrezne in kakovostne informacije iz notranjih in zunanjih virov za podporo delovanja ostalih komponent notranjih kontrol. Komuniciranje je nenehno ponavljajoč se proces zagotavljanja, izmenjave in pridobivanja potrebnih informacij. Interno komuniciranje je sredstvo, s katerim se širijo informacije v podjetju na vseh ravneh. Zaposleni na ta način prejmejo jasna sporočila s strani vodstva, da je kontrolne aktivnosti treba izvajati z veliko mero odgovornosti. Zunanje komuniciranje je dvojno: omogoča prejem ustreznih zunanjih informacij in zagotavlja informacije zunanjim strankam kot odgovor na zahteve in pričakovanja (COSO, 2011, str. 91).

Organizacija COSO (2011, str. 91) opredeljuje naslednja načela, ki so povezana z informiranjem in s komuniciranjem:

1. uporaba ustreznih informacij: organizacija pridobi oziroma ustvari ustrezne in kakovostne informacije za podporo delovanja drugih sestavin notranjega kontroliranja;
2. interno komuniciranje: znotraj podjetja se deli informacije, ki vključujejo cilje in odgovornosti za izvajanje notranjih kontrol, nujne za podporo delovanja drugih komponent notranjega kontroliranja;
3. zunanje komuniciranje: podjetje komunicira z zunanjimi strankami o zadevah, ki lahko vplivajo na delovanje komponent notranjih kontrol.

2.1.5 Nadzor nad kontrolnimi aktivnostmi

Stalno ocenjevanje (angl. *monitoring activities*) in posamezno ocenjevanje ali kombinacije obeh se uporablja za ugotavljanje, ali vsaka od petih komponent notranjega kontrolnega sistema vključuje kontrole, ki so prisotne in delujejo. Stalno ocenjevanje, ki je vključeno v poslovne procese na različnih področjih podjetja, zagotavlja pravočasne informacije. Redno izvedeno posamezno ocenjevanje se bo razlikovalo v obsegu in pogostosti, odvisno od ocenjevanja tveganja, uspešnosti stalnih ocenjevanj in drugih vidikov obvladovanja tveganj (COSO, 2011, str. 107).

Organizacija COSO (2011, str. 107) opredeljuje dve načeli, ki sta povezani z nadzornimi aktivnostmi. Gre za izvajanje stalnih in/ali posameznih ocenjevanj in ocenjevanje ter posredovanje pomanjkljivosti, kjer podjetje ocenjuje in pravočasno posreduje pomanjkljivosti notranjih kontrol odgovornim za sprejemanje ukrepov.

Kljub vsem podrobnim opredelitvam načel COSO po raziskavah Paape in Spekle (2012, str. 549) ni mogoče najti dokaza, da uporaba okvira COSO izboljšuje učinkovitost obvladovanja tveganj. V raziskavo sta bili vključeni dve temi, povezani z obvladovanjem tveganj v podjetjih. Najprej so bili proučeni obseg izvajanja obvladovanja tveganj in

dejavniki, ki bi lahko pripomogli k razjasnitvi različnih ravni sprejema. V drugem delu študije so bile proučene različne izbire obvladovanja tveganj in njihova povezava z zaznanim tveganjem in uspešnostjo obvladovanja. Prvi del raziskave temelji na ugotovitvah predhodnih raziskav o obsegu izvajanja.[11] Z uporabo dodatnih podatkov, prejetih s strani 825 podjetij, je študija precej razširila empirično osnovo. V raziskavo so bila vključena mala in srednje velika podjetja ter podjetja v javnem sektorju. Prišli so do ugotovitve, da imajo podjetja, ki zaposlujejo člana uprave, odgovornega za tveganja in revizijsko komisijo, bolj izpopolnjene sisteme obvladovanja tveganj. Podjetja, ki jih upravljajo lastniki, pa so manj nagnjena k temu, da bi vlagala v obvladovanje tveganj. Rezultati analize drugega dela študije so pokazali, da pogostost ocene tveganja, uporaba kvantitativnih metod ocenjevanja tveganja in pogostost poročanja o tveganju prispevajo k učinkovitemu obvladovanju tveganj. Nadaljnja ugotovitev, kljub temu da lahko ti podatki podcenjujejo pravi vpliv načel COSO, je, da le 43 % podjetij v sklopu analize dejansko uporablja omenjeni okvir. Poleg tega so ugotovili, da uporaba okvirja COSO ne prispeva k učinkovitemu obvladovanju tveganj. Omenjene ugotovitve lahko privedejo do dvomov v merodajnost okvirja COSO. Porajajo se vprašanja, ali je okvir dejansko dober in zakaj se tako veliko podjetij odloči, da ga ne bodo uporabljala. Končni rezultati študije so privedli do dejstva, da je obvladovanje tveganj še vedno v fazi razvoja, tako v praksi kot teoriji.

2.2 Pomanjkljivosti notranjih kontrol

Ne glede na to, kako uspešno so notranje kontrole zastavljene in izvedene, lahko vodstvu podjetja zagotovijo doseganje le določene mere zastavljenih ciljev. Verjetnost doseganja ciljev je pogojena z omejitvami, ki so značilne za vse kontrolne sisteme. Presoja pri odločanju je mnogokrat lahko napačna, posledično lahko pride do raznih škodnih dogodkov. Poleg tega se lahko zaposleni izognejo izvajanju kontrolnih aktivnosti z usklajevanji ali s skrivnim dogovarjanjem, lahko se zgodi tudi to, da vodstvo podjetja preglasi kontrolni sistem. Učinkovitost delovanja notranjih kontrol je omejena z realnostjo človeške krhkosti pri sprejemanju poslovnih odločitev, ki jih je treba sprejeti v primernem časovnem okviru na podlagi informacij v danem trenutku in pod težo pritiskov pri vodenju poslovanja. Za nekatere odločitve, ki temeljijo na osnovi odločitve posameznikov, se lahko naknadno ugotovi, da ne izkazujejo želenih rezultatov, in jih bo morda treba spremeniti (COSO, 2011, str. 121). Po drugi strani Vezjak (b.l., str. 4) navaja, da je pogosta pomanjkljivost tudi stroškovna neučinkovitost notranjih kontrol, ko se izvaja vrsta notranjih kontrol na manj tveganih področjih, pri tem pa se katera od pomembnih kontrol ne izvaja. Podjetja morajo paziti, da s prevelikim poudarjanjem tveganj ne zaidejo v pretirano previdnost, tako da se zaposleni bojijo sprejemati potrebne odločitve.

[11] Raziskave avtorjev Beasley (2005), Kleffner (2003) ter Liebenberg in Hoyt (2003).

Po mnenju Jiang, Rupley in Wu (2010) obstoj ključnih tveganj v kontrolnem okolju predstavlja višjo stopnjo tveganja pri nadzoru kontrol, kar vodi v revizijsko tveganje[12]. Pomanjkljiv sistem notranjih kontrol omogoča višjemu poslovodstvu namerno povečevanje zaslužkov, ki ne bodo zaznani zaradi slabih kontrolnih postopkov. Raziskava s strani Ashbaugh Skaife (2009) je odkrila, da podjetja, pri katerih so opazili pomanjkljiv sistem notranjih kontrol, izkazujejo bistveno večjo izpostavljenost tveganjem. Ključna tveganja povečujejo verjetnost pojava nepričakovanega poslovnega neuspeha ali dramatični padec cene delnice, kar lahko privede do skupinskih tožb delničarjev proti revizorjem. Po dodatni raziskavi v letu 2009 je Ashbaugh Skaife odkril, da so stroški kapitala podjetja pozitivno povezani s pomanjkljivostjo notranjih kontrol. Takšno podjetje bo verjetno imelo višje stroške za pridobitev dodatnega kapitala.

2.3 Načela ocenjevanja in izboljšanja notranjih kontrol

Urad Republike Slovenije za nadzor proračuna (2004, str. 11) opredeljuje naslednja temeljna načela, ki usmerjajo notranje kontrole:

1. Sistem notranjih kontrol lahko daje samo sprejemljivo, ne pa absolutnega zagotovila: sistemi notranjih kontrol so namenjeni obvladovanju tveganj pri doseganju ciljev podjetij, ne njihovemu odpravljanju. Zato lahko dajejo le sprejemljivo in ne popolno zagotovilo za uspešnost pri obvladovanju tveganj, nanje lahko vplivajo človeške napake in slaba presoja, povezanost več oseb z namenom, da se izognejo kontrolam, neupoštevanje postopkov s strani vodstva ter ocena stroškov in koristi v zvezi s kontrolami.
2. Predstojnik oziroma vodstvo podjetja za vzpostavitev in vzdrževanje ustreznega sistema notranjih kontrol: sistem notranjih kontrol se nenehno spreminja in izboljšuje na pobudo predstojnika oziroma vodstva podjetja, zaposlencev in na podlagi ugotovitev ter priporočil notranje ali zunanje revizije. Sistem notranjih kontrol je treba prilagajati tudi zaradi zunanjih dejavnikov, tveganj, sprememb prednostnih nalog, organizacijskih sprememb in zaradi tehnološkega razvoja. Predstojnik oziroma vodstvo podjetja mora redno preverjati ustreznost sistema notranjih kontrol, da zagotovi, da so vse ključne kontrole vedno ustrezne.
3. Notranja kontrola je pomemben, vendar ne edini element poslovanja: notranja kontrola ne predstavlja vseh elementov, ki so potrebni za poslovanje podjetja in obvladovanje tveganj. Notranja kontrola ne določa strategije ali ciljev in ne more preprečiti nepravilnih strateških ali poslovnih odločitev.
4. Notranja kontrola mora biti smotrna, upoštevati mora ocene tveganja in zagotavljati dodano vrednost: stroški izvajanja notranjih kontrol ne smejo presegati koristi. Predstojnik oziroma vodstvo podjetja mora oceniti stroške in koristi notranjih kontrol

[12] Revizijsko tveganje je tveganje, da revizor posreduje neprimerno mnenje o računovodskih izkazih. Tveganje je sestavljeno iz treh komponent: notranjega tveganja, tveganja pri nadzoru in tveganja pri odkrivanju pomanjkljivosti.

in izvajati le tiste kontrole, ki so potrebne za doseganje ciljev podjetja in za ohranjanje tveganja na še sprejemljivi stopnji. Obseg in uporaba notranjih kontrol morata temeljiti na celoviti oceni tveganja in biti sorazmerna z njo.

5. Notranje kontrole so učinkovite, če se dosledno uporabljajo: notranje kontrole morajo dosledno v polnosti upoštevati vsi zaposleni, kar velja tudi za predstojnika oziroma vodstvo podjetja.
6. Notranje kontrole je treba obravnavati kot celoto in ne vsake posebej: posamezna notranja kontrola se redko obravnava neodvisno, ampak glede na to, kako deluje v povezavi z drugimi obstoječimi ali načrtovanimi kontrolami.
7. Potrebe po notranjih kontrolah in njihova uporaba se lahko med podjetji razlikujejo: različni načini notranjega kontroliranja so lahko posledica razlik v stopnji centralizacije ali decentralizacije pri posameznem podjetju ali razlik v kadrovskih in drugih vplivnih dejavnikih. Lahko so tudi posledica razlik v naravi dela podjetij, njihovih ciljev, zunanjega okolja itn.
8. Za uspešnost notranjih kontrol je bistven odnos vodstva: za obstoj pozitivnega okolja do sistema notranjih kontrol je pomembno ravnanje predstojnika oziroma vodstva podjetja, ko z besedami in dejanji zaposlencem prenaša jasno sporočilo, da poštenost, vestnost, strokovnost in druge vrednote ne smejo biti ogrožene. Kontrolno okolje in odnos, ki ga predstojnik oziroma vodstvo podjetja vzpostavi do notranjih kontrol, najbolj vplivata na izvajanje kontrolnih usmeritev in postopkov.
9. Notranja revizija ni nadomestilo za notranjo kontrolo in vodstva ne razbremenjuje odgovornosti: notranja revizija je pomemben del sistema notranjega nadzora, ker ocenjuje ustreznost in učinkovitost notranjih kontrol, da lahko da predstojniku oziroma vodstvu podjetja zagotovilo, v kakšnem obsegu se je mogoče na njih zanašati. Ob tem pa obstoj notranje revizijske dejavnosti ne zmanjšuje odgovornosti vodstva za vzpostavljanje in vzdrževanje učinkovitih sistemov notranjih kontrol.

2.4 Prednosti in stroški notranjih kontrol

Z obvladovanjem tveganja niso povezane zgolj koristi, ampak tudi stroški. Koristi, ki so bile dosežene z obvladovanjem tveganj, je treba zmanjšati za dodatne stroške, ki so nastali zaradi obvladovanja tveganj. Za podjetje je smiselno samo takšno obvladovanje tveganj, ki zagotavlja, da bodo neto koristi od obvladovanja pozitivne. Na ta način podjetje povečuje svojo vrednost (Berk et al., 2005, str. 56). Sistem notranjih kontrol prinaša podjetju, področnim vodjem in vodstvu podjetja mnogo prednosti, med drugim dodano vrednost pri krepitvi zaupanja v doseganje zastavljenih poslovnih ciljev, zagotavlja povratno informacijo o pravilnosti delovanja podjetja in pomaga pri preprečevanju neželenih dogodkov. Za mnoga podjetja je najpomembnejša prednost učinkovitega kontrolnega sistema sposobnost, da izpolnjuje določene kriterije, potrebne za dostop do kapitalskih trgov, ki zagotavljajo kapitalsko usmerjene inovacije in gospodarsko rast. Tovrstni dostopi zahtevajo odgovornost za pravočasno izvedbo in zanesljivo poročanje delničarjem, upnikom, upravnim organom in drugim tretjim osebam, s katerimi ima podjetje neposredne

pogodbene odnose. Učinkovit kontrolni sistem omogoča zanesljivo zunanje finančno poročanje, kar krepi zaupanje vlagateljev pri zagotavljanju potrebnega kapitala. Ostale prednosti učinkovitega kontrolnega sistema po mnenju organizacije COSO (2011, str. 219) vključujejo:

- zanesljive in ustrezne informacije, ki podpirajo odločitve vodstva o zadevah, kot sta določanje cen izdelkov in kapitalskih naložb ter uporabe virov,
- skladne mehanizme za obdelavo transakcij, ki podpirajo kakovost informacij in komunikacij v celotnem podjetju, povečujejo hitrost in zanesljivost, pri kateri se začnejo in poravnajo transakcije, ter zagotavljajo zanesljivo hranjenje in celovitost podatkov,
- večjo učinkovitost med delovnimi funkcijami in procesi,
- ohranitev dejstev, obrazložitev in osnovo za odločitve, kjer je potrebna zelo subjektivna in znatna sodba,
- sposobnost in zaupanja vredno poslovanje s poslovnimi partnerji in strankami, kar omogoča uspešen poslovni odnos.

Podjetja pogosto omejijo porabo za človeške in kapitalske vire, zato pogosto obravnavajo stroške relativno na koristi alternativnih pristopov pri presoji možnosti notranje kontrole. Na splošno je lažje, da stroškovni vidik opredelimo z vidika stroškov in koristi, saj stroške lahko v večini primerov ocenimo dokaj natančno. Običajno so vsi neposredni in posredni stroški povezani z izvajanjem ukrepov in z odzivom notranjih kontrol. Nekatera podjetja vključujejo tudi stroške opuščene priložnosti (angl. *Opportunity costs*), povezane z uporabo virov.

Organizacija COSO (2011, str. 22) meni, da vodstvo podjetja upošteva številne stroškovne dejavnike v zvezi s pričakovanimi koristmi pri izbiri in razvoju notranjega kontrolnega sistema, ki lahko vključuje:

- kompromise pri zaposlovanju in motiviranju zaposlenih z višjo stopnjo usposobljenosti (s tem povezani višji stroški). Na primer manjše podjetje v zasebni lasti ne želi ali finančno ne zmore zaposliti finančnika z delovnimi izkušnjami v javnih delniških družbah;
- ocenjevanje vpliva dodane odvisnosti od tehnologije. Medtem ko sta prizadevanje za opravljanje nadzora in vpliv dodatnih tehnoloških kontrol na poslovni proces majhna, so stroški povezani z izbiro, razvojem, vzdrževanjem in s posodabljanjem tehnologije lahko visoki;
- razumevanje, kako spremembe v zahtevah po informacijah zahtevajo večjo zbiranje, obdelavo in shranjevanje podatkov, ki bi lahko sprožila eksponentno rast obsega podatkov. Kadar se podjetje sooča s prevelikimi količinami podatkov, mora zagotoviti pravočasen pretok pravih informacij v pravi obliki do pravih ljudi. Vzpostavitev

informacijskega sistema, ki uravnava stroške in koristi, je odvisna od premišljenega upoštevanja zahtev po podatkih.

Razmerje med stroški in koristmi notranjih kontrol pogosto vključuje subjektivno oceno. Koristi učinkovitih programov so na primer očitne, vendar težko merljive. Programi usposabljanja pogosto niso zasnovani za merjenje koristi ali zmožni zajeti vseh potrebnih podatkov za oceno programa. Odločitev, kako podjetje ocenjuje stroške v primerjavi s koristmi alternativnih pristopov k izvajanju sistema notranjih kontrol in končnih ukrepov, ki jih sprejme, je na strani vodstva. Na splošno stroški, ki nastanejo, ne bi smeli biti sprejemljiv razlog za izognitev vpeljavi kontrolnega sistema (COSO, 2011, str. 21). V naslednjem poglavju opredelim obvladovanje operativnega tveganja za finančne inštitucije, ki ga lahko v svoje poslovanje vpeljejo tudi nefinančna podjetja.

3 OBVLADOVANJE OPERATIVNEGA TVEGANJA

3.1 Opredelitev operativnega tveganja

Finančna industrija je prvotno razvila standardne metode za merjenje in upravljanje tržnega in kreditnega tveganja. Kasneje se kot pomemben vzrok za finančne izgube izkaže operativno tveganje, ki se mu izkazuje vse večjo pozornost. Dejansko je večina finančnih izgub povezanih z izpostavljenostjo tržnega ali kreditnega tveganja skupaj z neuspešnimi kontrolami, kar je ena izmed oblik operativnega tveganja. Operativno tveganje je veliko težje prepoznati kot tržno in kreditno tveganje. Že definicija operativnega tveganja je odprta za razpravo.

Walker (2001, str. 7) obravnava operativna tveganja kot vsakodnevna tveganja, s katerimi se sooča organizacija na področjih, kot so osebno tveganje, tveganje lastnine, tehnološko tveganje, pravno tveganje, regulatorno tveganje in tveganje ugleda. Stari grški pregovor pravi: »Bolje izgubiti oko kot svoje ime«, kar pomeni, da bi trpeli manj, če bi izgubili oko, kot če bi izgubili svoj dober ugled, ki je s strani Grkov zelo cenjena vrlina. Ta rek povzema bistvo tveganja izgube poslovnega ugleda, ki gre na vse ali nič.

Jorion (2003, str. 533) po krajši definiciji navaja, da je operativno tveganje omejeno na obdelavo transakcij. Druga, veliko širša definicija gleda na operativno tveganje kot na vsako finančno tveganje, ki ni tržno ali kreditno tveganje. Schroeck (2002, str. 196) je operativno tveganje opredelil kot tveganje nepričakovane finančne izgube zaradi človeških napak, napak v postopkih, sistemih ter njihovih notranjih kontrolah ali zunanjih dejavnikov in poslovnih strategij podjetja ali poslovnega okolja. Omenjena tveganja so skupna vsem podjetjem, ne samo finančnim inštitucijam. Schroeck (2002, str. 197) razdeli operativno tveganje na dve podkategoriji tveganja: tveganje dogodka (angl. *Event risk),* kjer gre za

redke dogodke[13] v finančnih inštitucijah, ki jih povzročijo večje napake v sistemih[14], procesih in napake v kontrolah[15], prevare[16], pravna tveganja[17] in zunanje motnje (požari in druge naravne katastrofe) ter poslovno tveganje (angl. *Business Risk)*; tveganje, da bo finančna inštitucija utrpela izgube zaradi nepričakovanih sprememb (bodisi prihodnjih prihodkov ali fiksnih stroškov, ki niso posledica kreditnega ali tržnega tveganja).

Operativno tveganje pridobiva na pomenu, saj se z njegovo problematiko ukvarja večina podjetij s področja bančne regulative, prav tako pa ga v svoje poslovanje vključujejo tudi nefinančna podjetja. Banka Slovenije operativno tveganje opredeljuje po definiciji Baselskega odbora za bančni nadzor kot tveganje izgube zaradi neustreznih ali neuspešnih notranjih postopkov, ljudi in sistemov ali zaradi zunanjih dogodkov. Definicija vključuje tudi pravna/zakonodajna tveganja, izključena pa so strateška in sistemska tveganja ter tveganja zaradi slabega imena organizacije. Opredelitev po Baselskem odboru temelji na vzrokih operativnih tveganj in ne toliko na izidih operativnega tveganja (Banka Slovenije, 2002, str. 2).

Velik izziv pri operativnem tveganju je opredelitev (potencialne) izgube. Zgodovinski podatki, potrebni za finančno ovrednotenje tveganja, morajo biti veliko bolj podrobni kot v primeru tržnega ali kreditnega tveganja. Posledično se operativna tveganja pogosto merijo glede na visoko ali nizko prioriteto tveganja ocen (Walker, 2001, str. 12). Crouhi et al. (2006, str. 327), sodeč po svojih izkušnjah, menijo, da je za uspešno izvajanje okvira operativnega tveganja in pripadajočih modelov potrebnih osem ključnih elementov. Mednje uvrščajo: določitev politik in ugotavljanje tveganja na podlagi dogovorjene terminologije, modeliranje poslovnih procesov, priprava metodologije merjenja najboljše prakse, zagotavljanje upravljanja izpostavljenosti, namestitev pravočasne poročevalske zmogljivosti, izvajanje analize tveganja (vključno s testiranjem izjemnih situacij) in dodeljevanje kapitala kot funkcija operativnega tveganja.

Številna podjetja so začela razvijati postopke za ugotavljanje, merjenje, pregledovanje in poročanje notranjih dejavnikov kot kazalnikov operativnega tveganja. Ti postopki vključujejo revizijske ocene, notranje preglede, uporabo modelov za analizo notranjega obsega in izgub, izkušnje z neplačili in nestabilnostjo bilance stanja. Sistem obvladovanja operativnega tveganja se med podjetji in glede na industrijsko panogo razlikuje. Po navedbah Kaplan Schweser (2008, str. 4) naslednjih pet točk predstavlja okvir, na podlagi

---

[13] Podroben seznam opisov in definicij dogodkov v literaturi: Lam, J. & Cameron, G. (1999). *Measuring and Managing Operational Risk within an Integrated Risk Framework—Putting Theory into Practice in Operational Risk and Financial Institutions.* London: Risk Publications, str. 85, Tabela 2.

[14] Izgube zaradi nedelovanja informacijskih sistemov za upravljanje in komunikacije ali računalniških sistemov.

[15] Nepredvidene izgube zaradi človeške napake ali neskladnosti z uveljavljenimi poslovnimi smernicami.

[16] Izgube zaradi prevar/kraj zaposlenih ali zunanjih oseb.

[17] Pravni stroški, globe in izgubljene poravnave iz naslova pravnih dejanj in tožb. Lahko tudi oportunitetni stroški, ki izhajajo iz regulativnih ukrepov.

katerega se organizira in zgradi učinkovit sistem: vloga vodstva, merjenje in spremljanje tveganja, politike in postopki, notranje kontrole in nadzorne vloge.

Problematika opredelitve definicije operativnega tveganja je po mnenju Muermananna in Oktema (2002, str. 26) dvojna. Prvotno gre za to, da je operativno tveganje predvsem samosvoje, značilno, kar je nasprotno tržnemu in kreditnemu tveganju, ki imata veliko večjo sistemsko komponento. Zato je težko določiti definicijo, ki bo ustrezala in bila sprejeta s strani vseh panog v gospodarstvu. Kot drugo navajata, da bi bilo smiselno, da bi opredelitev operativnega tveganja temeljila na podlagi večjih incidentov, ki so sprožili razpravo o operativnem tveganju. Glede na raznolikost operativnega tveganja bi bilo tako najbolj smiselno, da podjetja sama opredelijo in kategorizirajo tveganja tako, da kar najbolje ustrezajo managementu njihovega podjetja. Kot primer navajata, da so banke dejansko pričele z notranjo opredelitvijo operativnega tveganja na podlagi vzrokov in učinkov, ki so povezani z njihovo izpostavljenostjo, kot so: operativno tveganje zaradi napak v transakcijah, goljufivega trgovanja, tveganja izgube ali poškodbe premoženja (na primer zgradbe ali računalniki), tveganje notranjih in zunanjih goljufij, prevar, pravna tveganja/tveganje odgovornosti zaradi praks zaposlovanja, varnosti na delovnem mestu ali sprememb v regulativnem okolju.

3.2 Pristopi merjenja operativnega tveganja z vidika regulatorja

V juniju 2011 je Baselski odbor objavil načela za obvladovanje operativnega tveganja z namenom zagotoviti smernice za operativno tveganje. Smernice so obvezne za finančne inštitucije, prav tako pa se načel lahko držijo tudi preostala podjetja s tem, da s strani regulatorja ne bodo kontrolirana. Enajst načel vključuje izkušnje, pridobljene iz finančne krize, in primere dobrega ravnanja z operativnim tveganjem. Po ugotovitvah odbora so finančne inštitucije dosegle zadosten napredek pri izvajanju prvotnih načel, izdanih v letu 2003, ki so bila revidirana v letu 2011. Kljub temu so mnoge finančne inštitucije še vedno v procesu izvajanja različnih načel. Sistemsko pomembne inštitucije izvajajo načela in način obvladovanja tveganj v različnem obsegu. Z zgodovinskega vidika je izvajanje načel močno povezano z okvirom Baselskih pristopov za izračun kapitalske zahteve za operativna tveganja; kot primera sta standardizirani pristop (angl. *Standardized Approach* – TSA) in napreden pristop (angl. *Advanced Measurement Approach* – AMA). Za finančne inštitucije, ki uporabljajo napredne pristope, se pričakuje, da imajo bolj napreden okvir obvladovanja operativnega tveganja, implementirajo naprednejša orodja, kar vključuje samoocenjevanje tveganj (angl. *Risk and control self-assessment),* zbiranje notranjih podatkov, analizo scenarijev, zunanje zbiranje podatkov, ključne indikatorje tveganj (angl. *Key Risk Indicators),* management sprememb in primerjalne analize (Bank for international settlements, 2014a, str. 1).

Kuritzkes (2002, str. 51) opredeljuje več razlogov, zakaj je v praksi izračun za kapitalsko zahtevo operativnega tveganja zelo težko oceniti:

- pomanjkljivi podatki: škodni dogodki z nizko frekvenco pojava in velikim tveganjem izgube se po navadi redko pojavijo v posamezni finančni inštituciji. Kljub temu da obstajajo znani primeri obsežnih operativnih izgub, večina finančnih inštitucij ne pridobi zadostnih podatkov, ki so najpomembnejši za ocenjevanje kapitala za izračun zahteve. Iz tega razloga Baselski odbor zahteva, da finančne inštitucije, ki uporabljajo napreden sistem za izračun kapitalske zahteve, dopolnijo notranje vire podatkov z zunanjimi podatki ekstremnih škodnih dogodkov;
- primerljivost podatkov: zunanji podatki pogosto niso primerljivi z lastnimi možnostmi izgub, saj so operativne izgube v veliki meri endogene (specifične za posamezno podjetje). Težava pri uporabi zunanjih podatkov je presoja, kako pomembni so ekstremni primeri izgub za lastno uporabo;
- zavarovanja: izgube iz naslova operativnega tveganja podjetja pogosto ne morejo omiliti ali preprečiti z notranjimi procesi in kontrolami. S tem namenom se jih pogosto zavaruje, predvsem ko so prisotni zunanji škodni dogodki;
- težave pri opredelitvi operativnega tveganja: operativnega tveganja pogosto ne moremo umestiti v eno kategorijo. Ne samo, da lahko imajo vpliv notranji in zunanji dejavniki, operativna tveganja se lahko prekrivajo tudi s kreditnim ali tržnim tveganjem. Eden od takšnih primerov je napaka v dokumentaciji, ki vodi do neplačila posojila. Delno gre za kreditno tveganje in delno za operativno tveganje. Ločevanje vzrokov nastanka je še posebej oteženo, ko se preiskuje zgodovinske podatke.

Po sklepu o izračunu kapitalske zahteve za operativno tveganje za finančne inštitucije Banka Slovenija (2007a) opredeljuje izračun kapitalske zahteve za operativno tveganje, izračunan po enostavnem, standardiziranem in naprednem pristopu. Finančna inštitucija mora uporabljati enostavni pristop, če ne uporablja ali ne sme uporabljati drugega pristopa za izračun kapitalske zahteve. Pred začetkom uporabe naprednega pristopa mora pridobiti dovoljenje Banke Slovenije. Finančna inštitucija lahko, če pridobi ustrezno dovoljenje Banke Slovenije, tudi kombinira uporabo različnih pristopov: naprednega in standardiziranega ali naprednega in enostavnega pristopa, izjemoma pa tudi standardiziranega in enostavnega pristopa. Posamezne pristope podrobneje opisujem v nadaljevanju.

3.2.1 Enostavni pristop

Bank for international settlements (2014b, str. 5) navaja, da enostavni pristop za izračun kapitalske zahteve temelji na predpostavki, da finančne inštitucije izpostavljenost iz operativnega tveganja povečajo linearno sorazmerno s prihodki. Banka Slovenije (2007a, str. 3) opredeljuje, da je kapitalska zahteva za operativno tveganje, izračunana po enostavnem pristopu, enaka 15 % osnove za izračun kapitalske zahteve za operativno tveganje. Osnova za izračun kapitalske zahteve za operativno tveganje, izračunana po enostavnem pristopu, je triletno povprečje vsote čistih obrestnih in neobrestnih prihodkov. Triletno povprečje se izračuna na podlagi zadnjih treh let pred letom, za katero se izračuna

kapitalska zahteva za operativno tveganje. Če revidirani podatki o čistih prihodkih niso na voljo, se uporabijo nerevidirani podatki. Če je v danem obdobju opazovanja vsota čistih obrestnih in neobrestnih prihodkov negativna ali enaka nič, se mora ta podatek pri izračunu triletnega povprečja izvzeti. Osnova za izračun kapitalske zahteve za operativno tveganje se izračuna kot vsota pozitivnih rezultatov vsote čistih obrestnih in neobrestnih prihodkov po posameznih letih, deljeno s številom pozitivnih opazovanj.

3.2.2 Standardizirani pristop

Strategija in kultura tveganja v podjetju sta ključna dejavnika pri določanju učinkovitosti strukture obvladovanja tveganj, kot je neposredna in aktivna podpora uprave in višjega vodstva, ki želi vpeljati standardizirani pristop za izračun kapitalske zahteve (Financial Services Authority, 2011).

Kapitalska zahteva za operativno tveganje, izračunana po standardiziranem pristopu, je povprečje letnih kapitalskih zahtev za zadnja tri poslovna leta pred letom, za katero se izračuna kapitalska zahteva za operativno tveganje. Če je posamezna letna kapitalska zahteva negativna, se ji za namene izračuna triletnega povprečja dodeli vrednost nič. Letna kapitalska zahteva se izračuna kot vsota kapitalskih zahtev za vsa poslovna področja, našteta v četrtem odstavku tega člena. Kapitalska zahteva za posamezno poslovno področje se v vsoto (letno kapitalsko zahtevo) vključuje s svojim pozitivnim in negativnim predznakom. Kapitalska zahteva za posamezno poslovno področje je enaka zmnožku odstotka, določenega za to poslovno področje in njegove osnove za izračun kapitalske zahteve za operativno tveganje (Banka Slovenije, 2007a, str. 3). Metodologija za izračun osnove kapitalske zahteve za operativno tveganje, izračunana po standardiziranem pristopu, se izračuna za vsako poslovno področje posebej in za vsako leto, ki se upošteva pri izračunu povprečja letnih kapitalskih zahtev posebej. Osnova za izračun kapitalske zahteve za operativno tveganje, za posamezno poslovno področje, izračunana po standardiziranem pristopu, je vsota čistih obrestnih in neobrestnih prihodkov. Če revidirani podatki o čistih prihodkih niso na voljo, se uporabijo nerevidirani podatki (Banka Slovenije, 2007a, str. 6). Finančna inštitucija mora poleg splošnih standardov upravljanja z operativnim tveganjem v skladu s sklepom o upravljanju s tveganji izpolnjevati tudi naslednje kvalifikacijske kriterije (Banka Slovenije, 2007a, str. 6):

- imeti mora dobro dokumentiran sistem upravljanja z operativnim tveganjem in jasno določene odgovornosti v okviru tega sistema. S sistemom se ugotovijo izpostavljenosti banke operativnemu tveganju in sledijo ustrezni podatki o operativnem tveganju, vključno s podatki o pomembni izgubi;
- sistem upravljanja z operativnim tveganjem mora biti predmet rednih in neodvisnih pregledov, ki jih izvaja služba notranje revizije in/ali zunanja revizijska družba;

- sistem ocenjevanja operativnega tveganja mora biti tesno vključen v procese upravljanja s tveganji. Njegov rezultat mora biti sestavni del procesa spremljanja in kontroliranja profila operativne tveganosti finančne inštitucije;
- vzpostaviti mora sistem vodstvenega poročanja, s katerim se ustreznim strukturam v finančni inštituciji zagotavljajo poročila o operativnem tveganju. Vzpostavljeni morajo biti postopki za ustrezno ukrepanje glede na informacije, vsebovane v teh poročilih.

Financial Services Authority (2011) ugotavljajo pomanjkanje navodil o ustreznih sestavnih delih in obliki sprejemljivega okvira standardiziranega/naprednega pristopa, kar je nekaterim podjetjem in nadzornikom otežilo prepoznavanje slabosti v sprejetih okvirih. Ključno sporočilo je, da zaradi splošnih standardov za obvladovanje tveganja, ki jih vsebujejo višji upravni dogovori, sistemi in kontrole (angl. *Senior Management Arrangements, Systems and Controls)*, ne bi smelo biti pomembne razlike med kakovostnimi standardi, ki jih uporabljajo večja podjetja s standardiziranim pristopom in tista podjetja, ki uporabljajo napredni pristop. Izkušnje pa kažejo, da lahko nekatera podjetja s standardiziranim pristopom naletijo na težave, če bi želela pridobiti odobritev agencije za napredni pristop.

3.2.3 Napredni pristop

Kapitalska zahteva za operativno tveganje po naprednem pristopu temelji na lastnem sistemu merjenja operativnega tveganja. Finančna inštitucija mora poleg splošnih standardov upravljanja z operativnim tveganjem v skladu s sklepom o upravljanju s tveganji izpolnjevati tudi naslednje kvalitativne kvalifikacijske kriterije (Banka Slovenije, 2007a, str. 8):

- sistem merjenja operativnega tveganja mora tesno vključiti v vsakodnevne procese upravljanja s tveganji;
- imeti mora neodvisno funkcijo upravljanja z operativnim tveganjem;
- vzpostaviti mora redno poročanje vodstvenim strukturam o izpostavljenostih operativnemu tveganju in o preteklih izgubah. Vzpostavljeni morajo biti postopki za sprejemanje ustreznih korektivnih ukrepov;
- imeti mora dobro dokumentiran sistem upravljanja s tveganji. Finančna inštitucija mora imeti vzpostavljene tudi redne postopke za zagotavljanje skladnosti s tem sistemom in izdelane politike za obravnavo neskladnosti;
- procesi upravljanja z operativnim tveganjem in sistem merjenja operativnega tveganja morajo biti predmet rednih pregledov, ki jih izvaja služba notranje revizije in/ali zunanja revizijska družba;
- pri potrditvi primernosti (validaciji) sistema merjenja operativnega tveganja se ugotavlja, ali je finančna inštitucija sama zadovoljivo potrdila primernost sistema

merjenja operativnega tveganja, sta zagotovljeni preglednost in dostopnost podatkovnih tokov in procesov, povezanih s sistemom merjenja operativnega tveganja.

Finančna inštitucija mora pri izračunu kapitalske zahteve za operativno tveganje upoštevati pričakovane in nepričakovane izgube, razen če lahko dokaže, da je pričakovana izguba obvladovana na drug ustrezen način. Merjenje operativnega tveganja mora zajeti vse potencialno resne dogodke z repa statistične distribucije izgube, pri čemer mora doseči standard stabilnosti, primerljiv z 99,9-odstotnim intervalom zaupanja skozi obdobje enega leta. Sistem merjenja operativnega tveganja mora imeti nekatere ključne elemente, da izpolni standard stabilnosti iz prvega odstavka tega člena. Ti elementi so: notranji podatki, zunanji podatki, analize scenarijev in dejavniki, ki odražajo poslovno okolje in notranje kontrolne sisteme (Banka Slovenije, 2007a, str. 8).

Po pregledu letnih poročil trinajstih bank za leto 2015, ki imajo po Zakonu o bančništvu (Uradni list RS, št. 25/15) dovoljenje Banke Slovenije za opravljanje bančnih, vzajemno priznanih in dodatnih finančnih storitev, sem prišla do ugotovitve, da v Sloveniji kar devet od trinajstih bank uporablja enostavni pristop za izračun kapitalske zahteve operativnega tveganja (Abanka, d.d., Addiko, d.d., Banka Koper, d.d., Banka Sparkasse, d.d., Deželna banka Slovenije, d.d., Gorenjska banka, d.d., Nova Ljubljanska Banka, d.d., SID – Slovenska izvozna in razvojna banka, d.d., in Nova Kreditna Banka Maribor, d.d.). Dve banki uporabljata standardiziran pristop (KBS banka, d.d., in Sberbank banka, d.d.) in dve banki sta že pričeli uporabljati napreden pristop za izračun kapitalske zahteve (Unicredit banka, d.d., in SKB banka, d.d.). Iz teh podatkov lahko razberemo, da so s postopkom ocenjevanja tveganj najbolj zadovoljne banke, ki so izbrale enostaven pristop, saj ga je možno prilagoditi različnim organizacijskih enotam, kjer s kombinacijo poznavanja poslovnih procesov in poslovnega znanja, potrebnega za analize, sodelujejo posamezni strokovnjaki.

Podobni rezultati so bili prikazani tudi v raziskavi Ushe Janakiraman iz leta 2008 o indijskih bankah ob začetkih oblikovanja procesa operativnega tveganja. Indijske banke so imele zelo dobro definirane organizacijske strukture in potrjene politike za obvladovanje operativnega tveganja. Banke so pričele uporabljati enostaven pristop za izračun kapitalske zahteve, večina od njih pa je imela željo preiti na uporabo naprednega pristopa, za kar so morale banke posvetiti več časa in sredstev (Janakiraman, 2008). Standardiziran pristop za izračunavanje kapitalske zahteve je bolj natančen kot enostaven pristop, saj je treba upoštevati tudi dejstvo, da so nekatera poslovna področja bolj tvegana od drugih, posledično je treba za njih rezervirati večji delež kapitala.

3.3 Identifikacija operativnih tveganj

Podjetja morajo zagotoviti, da postopek obvladovanja tveganj zajema odkrivanje, ocenjevanje, spremljanje in kontroliranje operativnega tveganja za vse produkte,

aktivnosti, procese in sisteme. Vse pomembnejše spremembe v podjetju, infrastrukturi in v operativnem sistemu bi morale biti ocenjene in kontrolirane skozi celoten proces s primernimi sistemi in kontrolnimi točkami. Operativno tveganje lahko nastane tudi pri vpeljavi novega produkta ali aktivnosti, z vstopom na nepoznane trge ali s prevzemom poslovanja na trgih, ki so geografsko oddaljeni od glavnih pisarn. Posledično morajo podjetja v takšnih okoliščinah še posebno paziti, da primerno ocenijo tveganja in kontrole. Identifikacija vrst operativnega tveganja, ki so jim podjetja izpostavljena, pogosto vključuje naravo strank, produktov in aktivnosti, načrtovanje, izvajanje in delovanje procesov, ki se uporabljajo za proizvode in dejavnosti, in splošno zavest, odnos in vedenje zaposlenih v podjetju za tveganja in obvladovanje tveganja v podjetju. Mnoga podjetja sledijo najrazličnejšim podatkom o operativnem tveganju, zato je pomembno, da podjetja razumejo odnos med spremljanjem kazalcev tveganja, operativnimi izgubami in izpostavljenostjo tveganjem. Podjetja si morajo prizadevati za razvoj ključnih kazalnikov tveganja, ki zagotavljajo zgodnje opozarjanje na povečano tveganje, ter znati razlikovati med kazalniki tveganj in izpostavljenostjo, ki jo redno merijo. Prav tako morajo razmisliti o tem, kako bi lahko podatki, pridobljeni prek spremljanja operativnega tveganja, pripomogli k finančnemu izboljšanju poslovanja (Sheen, 2005, str. 319).

Sheen (2005, str. 319) zajema naslednje ključne kazalnike operativnih tveganj:

- kazalnike tveganja zaposlenih (nadure, bolezni, fluktuacija zaposlenih),
- kazalnike procesov ali sistemskih tveganj (novi produkti, postopki, plačila nadomestil, napake v dokumentaciji, pritožbe kupcev, ročne obdelave transakcij),
- kazalnike tveganj IT-sistemov (procesne ali sistemske napake, tehnični zahtevki).

Mainelli (2002, str. 31) meni, da gospodarstvo postavlja tehnike obvladovanja s tveganji v sam vrh poslovanja podjetij prek:

- strateškega vrednotenja tveganj: spodbujanje podjetij, da imajo nadzor nad vsemi tveganji, ne le finančnimi, kot tudi oblikovanjem ustreznih mehanizmov za obvladovanje tveganj, vključno z odpravo tveganj, obvladovanjem učinkov, zavarovanj,
- notranjega obvladovanja »premij« in »terjatev«: prikaz finančnih rezultatov in posledic, za katere se je podjetje odločilo, da jih je treba imeti pod nadzorom, kakor tudi razvoja notranjega trga za tveganje,
- obveščanja in preiskovanja: aktivno poročanje in preiskovanje potencialnih incidentov ter uporaba rezultatov za prilagoditev internih finančnih mehanizmov,
- izmenjave najboljših praks: z uporabo informacij o tveganosti, pridobljenih iz obvestil, preiskav iz zunanjih virov in najboljših virov iz prakse. S tem se zagotovi bazo podatkov, poročila, primerjave in ukrepe, ki omogočajo nadrejenim, da se učijo drug od drugega,

- zunanjih primerjav: zagotavljanje primerjalnih podatkov o obvladovanju tveganj iz zunanjih virov, na primer: zavarovalnic, tečajev obveznic, primerjalne analize.

Poznamo škodne dogodke, ki nam povzročijo finančno izgubo, ter dogodke, ki nam trenutno ne prinesejo ne izgube ne dobička, temveč le potencialno grožnjo prihodnje realizacije škodnega dogodka. Maurmann in Oktem (2002, str. 30) definirata te potencialne škodne dogodke izgub (angl. *Near miss*) kot dogodek, zaporedje dogodkov ali opazovanje nenavadnih pojavov, ki lahko potencialno vplivajo na delovanje poslovanja podjetja in sčasoma lahko povzročijo resne finančne posledice. Potencialne škodne dogodke lahko razumemo kot opozorila, da se lahko pojavi dogodek, ki bo podjetju v prihodnosti lahko povzročil večjo škodo. Pri pregledu zabeleženih incidentov v bančni panogi v letu 2002 je bilo ugotovljeno, da je za vsak večji škodni dogodek že bila zabeležena manjša nepravilnost, ki ni prinesla finančnih izgub. Kljub njihovim omejenim vplivom potencialni škodni dogodki zagotovijo vpogled v morebitne večje neugodne poslovne razmere in poslovne motnje. Zato je pravočasno in ustrezno spremljanje tovrstnih dogodkov smiselno, saj pripomore k pravočasnemu odkritju morebitnih večjih zapletov. Kljub temu je treba poudariti, da prav vsi manjši škodni dogodki ne povzročijo večjih izgub (Muermann & Oktem, 2002).

3.4 Vrste ukrepov pri obvladovanju tveganj

Berk et al. (2005, str. 177) ukrepe na področju obvladovanja tveganj razvrščajo v tri skupine, in sicer v skupino ukrepov izogibanja tveganju, skupino ukrepov zmanjševanja tveganja in skupino zavarovanja tveganj. Crouhi et al. (2006, str. 88) ločijo štiri osnovne izbire pri obvladovanju tveganj: izognitev tveganju z neizvajanjem določenih aktivnosti, prenos tveganja na tretje osebe prek zavarovanj in zunanjih izvajalcev, zmanjšati pojavnost tveganj – kot na primer operativno tveganje s preventivnimi in detektivnimi nadzornimi ukrepi in sprejem tveganja, ki se ga podjetje že vnaprej zaveda.

Walker (2001, str. 88) poleg zgoraj omenjenih skupin povzema še druge ukrepe za obvladovanje tveganj: zmanjšanje vrednosti tveganja, izvajanje zaščitnih ukrepov proti ugotovljenim grožnjam, prenos tveganj na tretje osebe, izoliranje tveganj, izravnava tveganj, izogibanje tveganjem, prevzem tveganja in razpršitev tveganja. Vrste ukrepov pri obvladovanju tveganj so pogosto medsebojno povezane. Značilni primer zmanjšanja vrednosti tveganja je viden v bančnem okolju. Banke imajo v svojih blagajnah določene denarne zneske. Da zmanjšajo vrednost tveganja v primeru bančnega ropa, zmanjšajo vrednost gotovine, ki jo hranijo v blagajni. Berk et al. (2005, str. 177) v skupino ukrepov zmanjševanja tveganja uvrščajo postopke zmanjševanja pogostosti izgub in postopke nadzorovanja višine izgub. Izvajanje zaščitnih ukrepov proti ugotovljenim grožnjam je predvsem preprosta, hitra in stroškovno učinkovita metoda. Tako na primer požarni alarm svari pred požarom, varnostna oprema brani delavce pred nesrečo in podobno.

Prenos tveganj na tretje osebe bo tako zmanjšal vrednost tveganja, saj se bo podjetje tveganju izognilo. Tipičen primer prenosa tveganj so zavarovalne police ali podizvajalci. S pomočjo zavarovanja tveganj lahko podjetja zmanjšajo vpliv tveganj na spremenljivost dobička, sredstev, likvidnosti ali denarnega toka podjetja. Pri izpolnjevanju navedenih ciljev pogosto pride do nesporazumov med zavarovalnico in podjetjem, saj zavarovalnice zavarovalnemu zahtevku na področju zavarovanja tveganja delovanja le redko ugodijo brez dodanih pogojev. Iz tega razloga zavarovalni zahtevki pogosto niso izplačani v obračunskem obdobju, v katerem je bila knjižena izguba, kar povzroči, da cilj varovanja računovodskega dobička in sredstev pogosto ni dosežen. Podjetje ne more zavarovati vseh negativnih vplivov izgub, predvsem tistih, ki vplivajo na ugled podjetja. Dolžnost podjetja je načrtovati program zavarovanja, s katerim določi obseg kritja, delitev tveganja in odgovornost vodstva.

Rotovnik (b.l., str. 2) meni, da so zavarovalni produkti, ki pokrivajo operativna tveganja, v zadnjih letih doživeli velik razvoj. Že tradicionalno se posamezna zavarovanja nanašajo na posamezne vrste kategorij operativnega tveganja. Med drugim navaja, da so trenutno v finančnih inštitucijah najpogostejše naslednje zavarovalne police:

- zavarovanje proti goljufiji zagotavlja pokritje izgub iz naslova nepoštenih dejanj zaposlenih, kot so prevare in poneverbe;
- zavarovanje proti računalniški zlorabi zagotavlja pokritje izgub iz naslova računalniških virusov, težav pri prenosu podatkov ipd.;
- poslovno odškodninsko zavarovanje je namenjeno pokrivanju izgub iz naslova obveznosti do komitentov zaradi malomarnosti ali neprofesionalnosti zaposlenih (napačni nasveti vplivnim komitentom o investicijah ipd.);
- zavarovanje obveznosti vodstvenega kadra, ki izhajajo iz tožb zaradi njihovih poslovnih potez;
- zavarovanje obveznosti uslužbencev;
- zavarovanje nefinančne lastnine, kot so na primer zgradbe in poslovne stavbe;
- zavarovanje proti nepooblaščenemu trgovanju, ki je relativno nov zavarovalniški produkt, posledica dogodkov v Baringsu[18];
- splošna zavarovanja, namenjena pokrivanju ostalih izgub.

Po raziskavah Rotovnika (b.l., str. 3) zavarovalnice neutrudno razvijajo nove produkte za zavarovanje različnih vrst operativnega tveganja, čeprav pri tem ne smemo spregledati dejstva, da so nekatere police zaradi svoje cene namenjene samo največjim finančnim inštitucijam (na primer polica »Financial Institutions Operational Risk Insurance« mednarodne korporacije Swiss Re[19]).

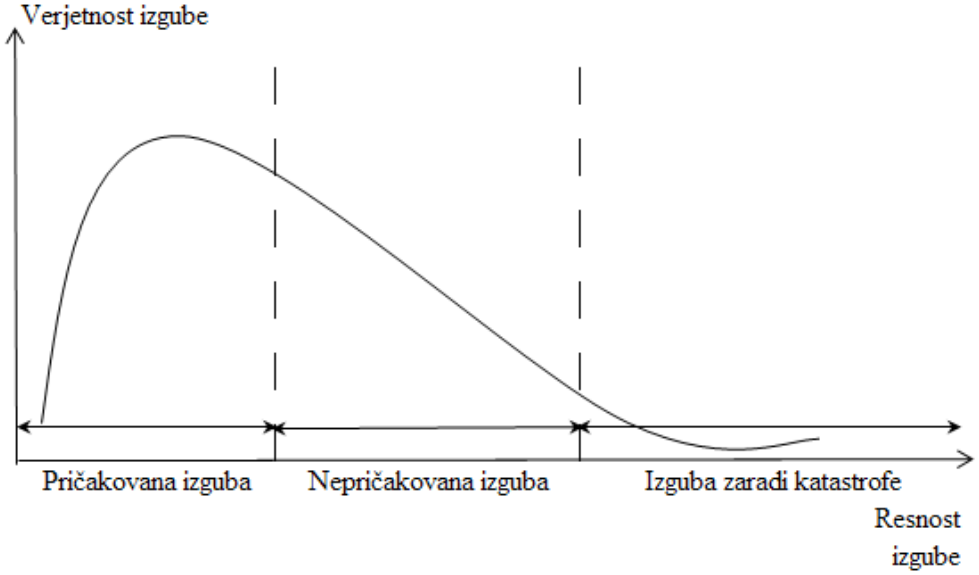
---

[18] Propad banke Baring's v letu 1995, London, zaradi goljufivega trgovanja zaposlenega.

[19] Zavarovalna polica pokriva odgovornost, zvestobo, nedovoljene dejavnosti, tehnološko tveganje, zaščito sredstev in zunanje goljufije.

Slika 3 prikazuje krivuljo porazdelitev operativnih izgub. Operativna tveganja bi pred dokončno odločitvijo o tem, katere vrste se lahko krijejo s pomočjo kapitala in katere z zavarovanjem, morali razdelili glede na statistično pričakovanje dogodka in velikost izgube. Majhne, a zelo pogoste izgube, ki se zaradi napak zaposlenih ali še nestabilnih aplikacij dogajajo vsak dan, se običajno krijejo iz postavk operativnih stroškov. Te izgube so predvidljive oziroma pričakovane, podjetja pa se jim zaradi svoje narave poslovanja zelo težko izognejo. Drugače je z izgubami, ki sicer nastajajo manj pogosto, a spadajo v kategorijo srednjih in visokih izgub. Ker niso popolnoma predvidljive oziroma nepričakovane in so za podjetja veliko bolj resnega značaja, je nujno, da se pred njimi zavarujejo s pomočjo kapitala ali primernih zavarovalnih polic. Poleg tega so tu tudi redke, a izjemno visoke izgube iz naslova operativnega tveganja, ki nastanejo kot posledica naravnih katastrof ali podobnih dogodkov. Ti predstavljajo spodnji del porazdelitvene krivulje, za natančnejšo oceno tovrstne izgube pa je treba zbrati podatke večjega števila podjetij.

Slika 3: Krivulja porazdelitev operativnih izgub



Vir: P. Jorion, Financial Risk Management – Handbook, 2003, str. 546.

Izoliranje tveganj je metoda, ki je lahko zelo učinkovita, kadar mora organizacija sodelovati pri dejavnostih z visokim tveganjem. Najpogostejša metoda, ki se uporablja za izolacijo tveganja, je ustanovitev ločene družbe z omejenimi obveznostmi za izvajanje dejavnosti z visokim tveganjem. Na ta način lahko podjetje izkoristi vse velike potencialne dobičke, ki jih lahko ponujajo dejavnosti z visokim tveganjem, medtem ko je izpostavljeno le omejeni odgovornosti. Izravnava tveganj je tehnika, s katero se potencialne izgube izravnavajo s potencialnimi dobički na drugih področjih. Izravnava se lahko uporabi za dejavnosti podjetja. Programska družba bi se lahko soočala s tveganjem velike izgube

zaradi napačnih lastnosti izdelka. Morebitne izgube zaradi stroškov popravila in izgubo ugleda bi lahko izravnali z izboljšanimi proizvodi, ki bi se prodali novim strankam. Izogibanje tveganj je učinkovita metoda obvladovanja tveganj in zmanjšanja potencialnih izgub. Metoda je primerna, kadar potencialne izgube presegajo potencialne dobičke, povezane z dejavnostjo. Kot primer je lahko verižna trgovina, ki ima svojo poslovalnico odprto na področju, kjer ji grozi večja izguba zaradi večjega števila poskusov vloma kot na drugih lokacijah. Trgovina se lahko izogne tveganju in svojo dejavnost preseli na drugo lokacijo. Prevzem tveganja je metoda, ki je primerna, kadar so potencialni dobički višji od potencialnih izgub in so največje možne izgube trajnostne. Na splošno se strategijo uporabi, kadar so potencialne izgube majhne ali so stroški izvajanja drugih strategij za obvladovanje tveganj previsoki. Ko se tveganje prevzame zaradi pomanjkanja alternativnih strategij za obvladovanje tveganj, je pomembno, da podjetje, ki obdrži tveganja, upraviči potrebo po sodelovanju na teh področjih tveganja. Pri tem je treba pretehtati potencialne dobičke tveganja glede na morebitne izgube. Razpršitev tveganj je lahko učinkovit način obvladovanja prevzetih tveganj. Primer tovrstne metode je shranjevanje dokumentacije podjetja na različnih lokacijah. V tem primeru ob morebitnem uničenju ene arhivske baze ohranimo preostale na drugih lokacijah (Walker, 2001, str. 89).

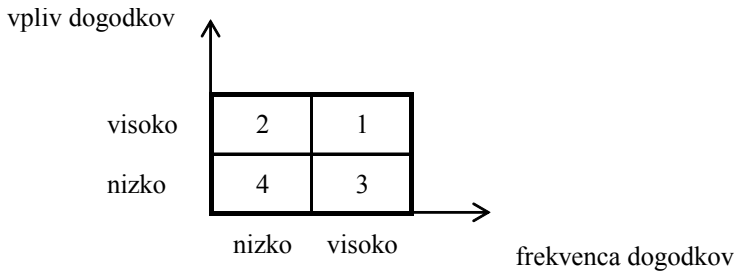
3.5 Metode merjenja operativnega tveganja

Za mnoga podjetja je prvi korak pri merjenju operativnega tveganja razvrstitev potencialnih izgub v skupine glede na velikost izgube in pogostost pojava. Ena od metod je razdelitev potencialne izgube v dve skupini: pogosto nastale manjše izgube, ki jih povzročajo človeške napake, in redko nastale velike izgube, ki jih povzročajo napake v operativnih sistemih podjetja ali mednarodne kriminalne dejavnosti. Notranji podatki so po navadi zadostni za razvoj natančnih ukrepov za tveganje visokofrekvenčnih dogodkov z manjšimi izgubami, vendar pomanjkanje podatkov o nizkofrekvenčnih in visokih stroškovnih dogodkih zahteva izmenjavo podatkov med podjetji (Kaplan Schweser, 2008, str. 5).

Operativno tveganje zajema škodne dogodke z zelo različnimi vzorci frekvenc pojava in težnosti vplivov dogodkov na poslovanje, kar prikazuje Slika 4. Kot prvi korak pri ugotavljanju uporabnosti statistične analize se zdi primerno, da se kategorizira potencialne incidente v matriki frekvenc pojava/vplivov škodnih dogodkov, ki temelji na izkušnjah in mnenju strokovnjakov. Matrika zagotavlja prve smernice za določanje pomembnih škodnih dogodkov. Za uspešno obvladovanje tveganja je treba največjo pozornost posvetiti dogodkom, ki se pojavljajo s pogosto frekvenco in z visokim vplivom na finančne izkaze (polje 1), in relativno manjšo pozornost dogodkom, ki se redko pojavijo in imajo relativno nizek vpliv na finančne izkaze (polje 4). Po znanih primerih goljufivih trgovanj (primer Baring's) in zlasti po terorističnih napadih 11. septembra leta 2001 v Združenih državah Amerike se je sprožilo veliko razprav po vseh korporacijah, vladnih organih in raziskovalnih inštitucijah s poudarkom na tem, kako obvladovati škodne dogodke z nizko

frekvenco pojava in zelo velikim vplivom na poslovanje (polje 2) in relativno malo na obvladovanje dogodkov z visoko frekvenco in majhnim vplivom na poslovanje (polje 3). Mnenje avtorjev je, da z dobrim poznavanjem in osredotočenjem na škodne dogodke, ki imajo majhen vpliv in visoko frekvenco pojava (polje 3), lahko izboljšamo sposobnost prepoznavanja dogodkov z velikim vplivom in manjšo pojavno frekvenco (polje 2), saj ti dogodki signalizirajo možnost redkega, a velikega škodnega dogodka (Muermann & Oktem, 2002, str. 26).

Slika 4: Matrika frekvenc pojava in vpliva škodnih dogodkov



Vir: A. Muermann & U. Oktem, The Near-Miss Management of Operational Risk, 2002, str. 27.

4 VZPOSTAVITEV SISTEMA NOTRANJIH KONTROL NA PODLAGI OPERATIVNIH TVEGANJ V PODJETJU XY

V predstavitvi izbranega podjetja so zbrani podatki iz zadnjega letnega finančnega poročila in interne dokumentacije. V nadaljevanju podrobno predstavim model celovitega obvladovanja operativnih tveganj v podjetju in postopek vzpostavitve notranjih kontrol, kjer sem sodelovala kot vodja projekta. Notranje kontrole podjetja temeljijo na operativnih tveganjih, kar pomeni, da se podjetje prvotno osredotoči na njihovo odkrivanje in na podlagi zbranih informacij vzpostavi notranje kontrole.

4.1 Predstavitev podjetja

Izbrano podjetje je del skupine, ki se ukvarja z upravljanjem s slabimi naložbami, trgovanjem z lastnimi nepremičninami in z dajanjem lastnih nepremičnin v najem ter s podjetniškim in poslovnim izobraževanjem. Podjetje prodaja portfelj naložb na pravilen, najboljši in najhitrejši možen način. Uvršča se med velike družbe; izpolnjuje tako pogoj glede vrednosti aktive kot višine čistih prihodkov od prodaje. V podjetju je okoli 160 zaposlenih. Strokovna izobrazba zaposlenih je na visoki ravni. Delež zaposlenih z visoko izobrazbo v zadnjih letih narašča in se približuje polovici vseh zaposlenih. Podjetje verjame v dejstvo, da lahko samo usposobljeni sodelavci sledijo potrebam slovenskega nepremičninskega in finančnega trga, zato v podjetju skrbijo za neprestano in celovito strokovno izobraževanje svojih zaposlenih. Za doseganje poslovnih ciljev so si zastavili ključna izobraževalna področja za razvoj poslovanja, ki izhajajo iz strateških zahtev. V letu

2015 so se osredotočili na izobraževanja za pridobitev licenc za cenilce vrednosti nepremičnin, revizorje, opravljanje poslov nepremičninskih posrednikov, prodajna, računalniška in jezikovna izobraževanja (Podjetje XY, 2015b). V podjetju se osredotočajo predvsem na naslednja tveganja (Podjetje XY, 2015b):

- kreditno tveganje; kjer gre za skrbno upravljanje s tveganjem, ki vključuje preudarno upravljanje razmerja med tveganjem in donosom ter nadzor in znižanje kreditnega tveganja prek različnih vidikov, kot so kakovost, koncentracija, valuta, rok, dospelosti, zavarovanja in vrsta produkta,
- valutno tveganje; podjetje ga obvladuje z izravnavo valute črpanja posojila na strani virov s terjatvami do strank na strani sredstev. Mesečno se spremlja in izravnava stanja različnih valut, tako da je valutna vrzel zanemarljiva,
- obrestno tveganje; podjetje skrbi za usklajenost obrestnih mer na strani sredstev in virov,
- likvidnostno tveganje; v podjetju so razviti ustrezni nadzorni postopki in informacijski sistem za učinkovito upravljanje in nadzor likvidnostnega tveganja. Oblikovane so tudi ustrezne likvidnostne rezerve, ki podjetju omogočajo dnevno izpolnjevanje vseh obveznosti.

V podjetju XY se je projekt vpeljave sistema notranjih kontrol pričel v letu 2011. Strategija, ki ureja omenjeno področje, opredeljuje ustreznost postavitve sistema notranjih kontrol, če se zagotovi izvajanje poslovne strategije podjetja in njegove strategije upravljanja s tveganji na vseh področjih poslovanja; poveča kakovost izvajanja poslovanja z vidika učinkovitosti in uspešnosti; zagotovi skladnost z zakonodajo in poveča kakovost računovodskih informacij in skladnost z veljavnimi računovodskimi standardi.

Sistem notranjih kontrol deluje, če sta postavljena delovanje in medsebojno sodelovanje internega kontrolnega sistema, sistema zagotavljanja usklajenosti poslovanja s predpisi (angl. *Compliance*) in z notranjim revidiranjem. Za učinkovit sistem notranjih kontrol so potrebni zavedanje in informiranje zaposlenih, zapis politik in postopkov, imeti in uporabljati je treba ustrezna orodja in avtomatizacijo procesa, imeti in uporabljati izkušnje in znanja zaposlenih, oceniti odgovornost zaposlenih in postaviti merila za posamezne notranje kontrole. Pri sistemu notranjih kontrol gre za vsakodnevne kontrole, ki omogočajo pravilno uporabo politik, procesov dela, delovnih navodil in orodij. Vsakodnevne kontrole so preprečevalne, usmerjevalne in popravljalne, vključujoč nadzorne dnevne kontrole. So stalen spreminjajoč se proces, ki ga oblikujejo vodstvo podjetja, lastniki posameznih aktivnosti in vsi drugi zaposleni. Vgrajene so v aplikacije, obrazce, navodila, procese in politike. Odgovornost za vzpostavitev dnevnih kontrol je na lastnikih posameznih aktivnosti. Lastniki posameznih aktivnosti so vodje področij in služb (Podjetje XY, 2013b).

Glavni namen sistema notranjih kontrol v podjetju XY je vzpostaviti uspešne kontrole na vseh področjih poslovanja podjetja, zagotoviti jasno odgovornost za izvajanje opredeljenih kontrol, zagotoviti ustrezno dokumentiranost – cilje in načine izvajanja vzpostavljenih notranjih kontrol ter ustrezno sledljivost izvajanja vzpostavljenih notranjih kontrol. Notranje kontrole temeljijo na sistemu organiziranosti dela, sistemu nadzorovanja, ločenosti izvajanja postopkov dela, razmejitvi odgovornosti, postopkih upravljanja z zaposlenimi, sistemu pooblastil, informacijskem sistemu podjetja in razmejitvi konflikta interesov. Izhodišča za vzpostavitev in oceno primernosti postavljenih kontrol so poslovni načrt podjetja oziroma področja, prepoznava in ocena tveganj, zahteve zakonodajalca, kodeks obnašanja in vrednote podjetja. Osnovno načelo sistema notranjih kontrol v podjetju XY je, da morajo lastniki aktivnosti ob vsaki spremembi izhodišč (strateški in poslovni načrt podjetja, identifikacija in sprejem tveganj, zakonske zahteve, kodeksi obnašanja in vrednostno okolje) za vzpostavitev postavljenih kontrol presoditi, ovrednotiti in prilagoditi sistem notranjih kontrol. Cilj delovanja sistema notranjih kontrol v podjetju je v največji možni meri zmanjšati pojavnost, število in možnosti namernih in nenamernih napak in tako zagotoviti stalen trend njihovega upadanja (Podjetje XY, 2013b).

Dokumenti, ki opredeljujejo postopek postavitve sistema notranjih kontrol, so opredeljeni s strani področja kontrolinga tveganj in se navezujejo na projektno delo, pripravo politik, procesov, poslovnikov in delovnih navodil. Podlaga za postavitev okvirja so politike skupine na področju operativnega tveganja in sistema notranjih kontrol. Četrtletno se v podjetju organizira Odbor za upravljanje z operativnimi tveganji, s sistemom notranjih kontrol (v nadaljevanju Oprisk Committee), katerega člani so zaposleni v kontrolingu tveganj, notranji reviziji, računovodstvu in pravni službi. Predmet Oprisk Committeeja so med drugim tudi poročila o rezultatih delovanja ključnih kontrol na vseh področjih dela podjetja; na primer komercialne aktivnosti, priprava dokumentacije, vknjižbe v zalednih in podpornih organizacijskih enotah, izvajanje poravnav. Poročila obsegajo tudi kvalitativne kot kvantitativne podatke. Gre za poročili imenovani KPI (angl. *Key Performance Indicators)* in KRI (angl. *Key Risk Indicators*), ki vsebujeta na primer obseg vseh izvedenih transakcij, obseg vseh stornacij, obseg knjižb za nazaj, število in vsebino pritožb, analize neusklajenosti s standardi, delež hipotek s plombami, prevzeme sredstev in podobno (Podjetje XY, 2013b).

4.2 Model celovitega obvladovanja operativnih tveganj

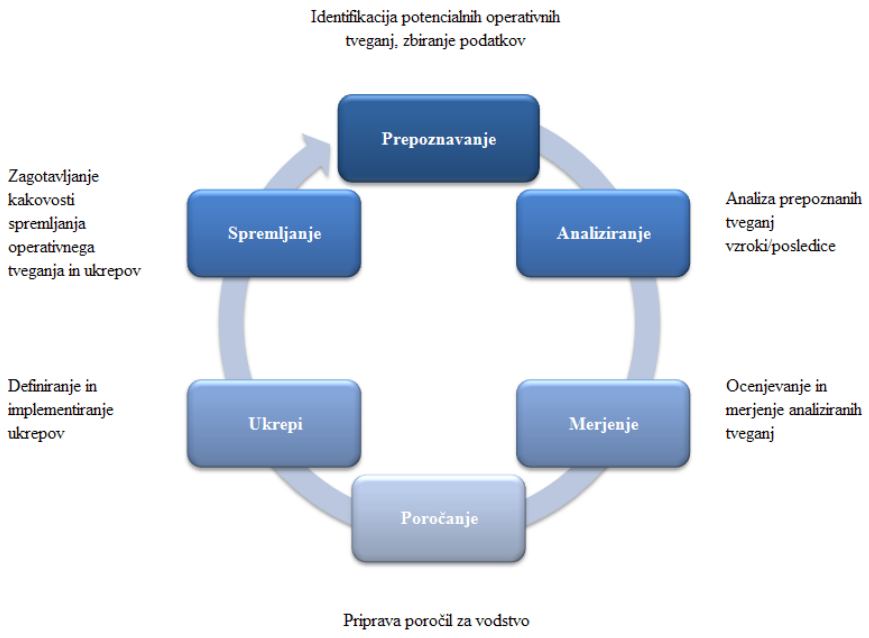
Po mnenju Berka et al. (2005, str. 59) ima podjetje pri vzpostavitvi sistema obvladovanja tveganja več možnosti. Najpogostejši možnosti sta najem svetovalca za razvoj primernega sistema obvladovanja tveganj in izobraževanje znotraj podjetja pod nadzorom zaposlenega, ki se specializira za področje obvladovanja tveganj. Kdaj je torej smiselna uvedba sistema za obvladovanje tveganj v podjetju? Organizacija International Federation of Accountants (2002, str. 16) podpira uvedbo sistema v primeru stroškovne učinkovitosti v širšem

pomenu. To pomeni, da morajo biti splošne koristi obvladovanja tveganj, ki upoštevajo gospodarske, okoljske in socialne vidike ter ureditve, večje od stroškov.

Nadzor nad izpostavljenostjo tveganjem je treba redno izvajati in ga sproti prilagajati spremembam v zunanjem okolju podjetja. Izboljšanje poslovanja in zmanjšanje poslovnih tveganj podjetje doseže s pridobivanjem povratnih informacij o delovanju notranjega kontrolnega sistema. Sistem notranjih kontrol je ustrezen, če zagotovi izvajanje poslovne strategije in strategije obvladovanja tveganj na vseh področjih poslovanja, poveča kakovost izvajanja poslovanja z vidika učinkovitosti in uspešnosti, zagotovi skladnost z zakonodajo in poveča kakovost računovodskih informacij in skladnost z računovodskimi standardi (Podjetje XY, 2013b). V podjetju XY se je notranje kontroliranje izvajalo že pred uvedbo sistema notranjih kontrol. Kontrole so se izvajale med potekom procesa, njihovo učinkovitost pa je periodično preverjala notranja revizija. Pomanjkljivost starega sistema vidim predvsem v tem, da ni bilo vzpostavljenega primernega procesnega managementa. Delovni procesi niso bili primerno modelirani, kar je posledično privedlo do nepoznavanja vseh aktivnosti znotraj procesov in nepoznavanja morebitnih groženj/tveganj, ki bi se lahko oziroma so se že pojavila.

V podjetju XY obvladovanje tveganj sledi procesu po Basel II in ga lahko opišemo kot cikel, ki ga prikazuje Slika 5. Gre za identifikacijo potencialnih tveganj in zbiranje podatkov. Sledijo analiza odkritih tveganj in vzrokov ter posledic, ocenjevanje in merjenje analiziranih tveganj, priprava poročil za vodstvo, definiranje in implementiranje ukrepov ter zagotavljanje kakovosti spremljanja operativnih tveganj.

Slika 5: Proces obvladovanja tveganj v podjetju XY



Vir: Podjetje XY, Priročnik o upravljanju z operativnim tveganje, 2015, str.9.

V nadaljevanju predstavim vloge in odgovornosti posameznih udeležencev procesa glede na organizacijsko strukturo podjetja.

4.2.1 Vloge in odgovornosti

Na osnovi obstoječe organizacijske strukture so za operativna tveganja opredeljene odgovornosti na štirih glavnih ravneh (Podjetje XY, 2015a):

- član vodstva, odgovoren za upravljanje s tveganji (angl. *Chief Risk Officer*), je odgovoren za izvedbo politike tveganj, ki jo sprejme celotna uprava in zato potrjuje temeljne odločitve o operativnih tveganjih ter podpira (kot »nosilec«) projekte in izvedbo metod upravljanja z operativnimi tveganji;
- zaposleni, odgovoren za obvladovanje operativnih tveganj na ravni skupine (angl. *Group Operational Risk Officer*), je odgovoren za usmerjanje odvisnih družb in zagotavljanje podpore;
- zaposleni, odgovoren za obvladovanje operativnih tveganj (angl. *Operational Risk Officer,* v nadaljevanju ORO), je odgovoren za lokalno izvedbo operativnih tveganj in poročanje skupini;
- zaposleni za obvladovanje operativnih tveganj v posameznem oddelku (angl. *Decentralized Operational Risk Officer,* v nadaljevanju DORO) so odgovorni za spremljanje in izvedbo standardov in metod znotraj posameznih oddelkov;
- za poročanje o vsakem škodnem dogodku so odgovorni vsi zaposleni, ki poročajo zaposlenemu, ki obvladuje operativna tveganja znotraj oddelka.

Pomemben člen pri obvladovanju operativnega tveganja je tudi notranja revizija, ki bi morala prilagoditi načrtovanje, cilje in postopke z namenom zagotovitve ustreznega nadzora. Po mnenju Fernandeza (2007, str. 144) mora letni revizijski načrt vključevati poseben pregled politik in postopkov za obvladovanje operativnega tveganja z naslednjimi cilji:

- potrditev obstoja in ravni izvajanja politik in postopkov v zvezi z operativnim tveganjem, ki ga je odobrilo vodstvo podjetja;
- pregled celovitosti procesa identifikacije operativnega tveganja;
- vrednotenje učinkovitosti orodij, ki se uporabljajo za ocenjevanje operativnega tveganja, kot tudi metodologije in načine merjenja;
- sprejetje pristopa, ki temelji na tveganju, za redno spremljanje ocene operativnega tveganja na različnih področjih poslovanja podjetja;
- potrditev pristopa, ki se uporablja za kvalitativno oceno tveganja in regulativen izračun kapitala v primeru naprednega pristopa za merjenje oziroma pregled podatkov za izračun kapitala in odbitkov v preostalih pristopih;

- pregled ustreznosti postopkov, ki jih podjetje uporablja za dokumentiranje procesov obvladovanja operativnega tveganja;
- preverjanje obstoja ukrepov, ki jih zaposleni, odgovorni za posamezna področja, predlagajo z namenom, da se ublažijo prepoznana operativna tveganja, kot tudi potrditev o njihovi učinkovitosti;
- notranja revizija spremlja, ali se informacije iz sistemov za obvladovanje tveganj vključujejo in upoštevajo v procesu odločanja.

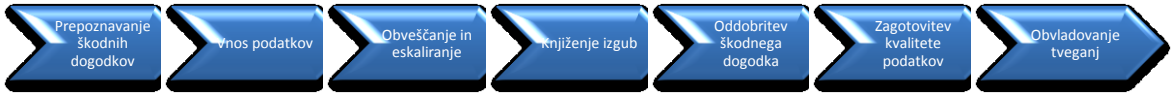
V nadaljevanju predstavim postopek razvrščanja in zbiranja podatkov o izgubah v podjetju XY, ki med drugim opredeljuje tudi vloge zaposlenih in postopek poročanja.

4.2.2 Postopek razvrščanja in zbiranja podatkov o izgubah

Zbiranje in poročanje o izgubah, povezanih z operativnimi tveganji, je ključni proces obvladovanja operativnih tveganj. Glavni cilji ustreznega zbiranja podatkov o izgubah (angl. *Loss Data Collection*) in procesa poročanja so analizirati, kje se pojavljajo škodni dogodki, in primerjava z rezultati ocen; analizirati vzroke za pojav škodnih dogodkov in nalog preprečevanja pojava škodnih dogodkov v prihodnje.

Podatkovna baza škodnih dogodkov se uporablja za zbiranje podatkov o izgubah zaradi operativnih tveganj. Meja, ki v podjetju XY velja za poročanje o izgubah zaradi operativnih tveganj, znaša 5.000 EUR, sume prevar in tatvin pa se poroča od zneska izgube 1.000 EUR. Škodne dogodke, nastale zaradi operativnih tveganj, je treba v podatkovno bazo škodnih dogodkov v vsakem primeru vnesti v petih dneh po njihovem odkritju. Predlogi ali ukrepi za zmanjšanje verjetnosti pojavnosti operativnih tveganj so obvezni pri izgubah, ki presegajo 100.000 EUR. Sporočiti jih je treba s pomočjo podatkovne baze škodnih dogodkov. Meja za stopnjevanje sporočanja izgub skupini znaša 100.000 EUR. Izvede se tako, da se izpolni obrazec Ad-Hoc poročilo v podatkovni bazi škodnih dogodkov. Vsak zaposleni ima pomembno vlogo pri odkrivanju in prepoznavanju izgub zaradi operativnih tveganj. Za zagotovitev najboljše podpore pri obvladovanju tveganj in zbiranju/vnašanju izgub v centralni informacijski sistem za zbiranje škodnih dogodkov se je treba držati postopka, ki ga predstavlja Slika 6 (Podjetje XY, 2015a).

Slika 6: Proces zbiranja podatkov o škodnih dogodkih in izgubah



Vir: Podjetje XY, Priročnik o upravljanju z operativnim tveganjem, 2015, str.12.

Slika 6 predstavlja interni postopek poročanja o škodnih dogodkih iz naslova operativnega tveganja. Vodstvo se zaveda dejstva, da lahko vsakdo dela napake. Zaradi tega ni naklonjeno temu, da bi s postopkom zbiranja podatkov o izgubah zaradi operativnih

tveganj iskala krivce med zaposlenimi ali drugimi osebami, temveč skuša zbrati stvarne podatke o izgubah, povezanih z operativnimi tveganji, in o njihovih vzrokih. Vsi zaposleni so zato zaprošeni, naj po svojem najboljšem védenju prijavljajo škodne dogodke na poslovnih področjih. Oddelki, ki sodelujejo v odločilnih poslovnih procesih ter poslovno pomembnih produktih in storitvah, morajo imeti prednost pri vključevanju v proces zbiranja podatkov o izgubah in poročanje o izgubah.

Struktura za podatkovni nabor podatkov o izgubah (katere podatke je potrebno dokumentirati za vsak škodni dogodek) je opredeljena z vsakokratno različico podatkovne baze škodnih dogodkov. Poročajo se ključni podatki: opis škodnega dogodka, predvideni datum nastanka dogodka, ocena potencialnega zneska izgube in predlogi/ukrepi za odpravo tveganja v prihodnje. Pri poročanju škodnih dogodkov bi podjetju priporočila, da v opise vključi še naslednje podatke: naziv in številko stranke, na katero se navezuje tveganje, poleg ukrepov naj se določi še zapadle roke in odgovorne osebe za ukrep. Vse te informacije bodo koristne, ko se bo iskalo zgodovinske podatke. Aplikacija za zbiranje škodnih dogodkov bi z nadgradnjo pridobila na dodani vrednosti, če bi se dodalo obvezno polje za vpis statusov reševanja dogodkov v določenem intervalu (na primer četrtletje). S tem bi se zagotovilo spremljanje dogodkov in reševanje.

Vsi zaposleni poročajo odkrite škodne dogodke prek telefona ali e-pošte odgovornemu za obvladovanje operativnega tveganja v posameznem oddelku. Kljub dejstvu, da vodstvo zagovarja kulturo neobsojanja zaposlenih pri poročanju škodnih dogodkov zaradi človeških napak, se pogosto dogaja, da mnogi škodni primeri ostanejo prikriti. Eden od načinov, kako izboljšati odstotek poročanih dogodkov, bi bil ta, da DORO v nekem časovnem intervalu potrdijo popolnost in pravilnost podatkov o izgubah tako, da pošljejo podpisane izjave s potrditvijo, da so vsi zaznani škodni dogodki bili poročani zaposlenemu za obvladovanje operativnih tveganj − ORO. Za DORO so imenovani izkušeni zaposleni, ki so s tem odgovorni za ugotavljanje in zbiranje podatkov o izgubah ter poročanje o njih. Prav tako so tudi podpora pri izvajanju kontrol pri posameznih procesih v sklopu sistema notranjih kontrol. Zaposleni mora biti izbran s soglasjem vodje področja in zaposlenega za obvladovanje operativnih tveganj in mora delovati v imenu vodje. Imeti mora zadostne izkušnje, da lahko ustrezno izpolni svoje naloge v skladu s potrebami operativnih tveganj. Ukrepe za zmanjšanje/odpravo škodnega dogodka opredeli in izvede področje, kjer se je škodni dogodek realiziral, v soglasju z ORO. Vzpostavi se tudi postopek spremljanja ukrepov (angl. *Mitigation Tracking*). O aktualnem statusu ukrepov se na mesečni ravni poroča vodstvu podjetja.

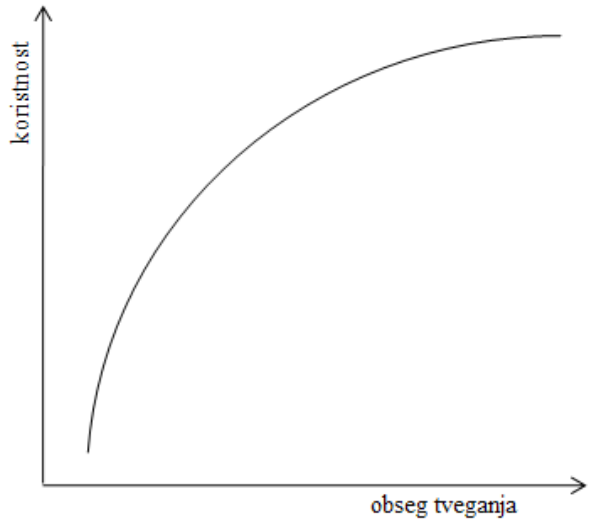
4.2.3 Pripravljenost za prevzemanje tveganj

Berk et al. (2005, str. 36) menijo, da je naklonjenost tveganju odvisna od načina njegovega nagrajevanja, od tega pa je odvisen tudi obseg zaščite pred tveganjem v podjetju. Če se delež nagrade vodstvu glede na vrednost premoženja podjetja zmanjšuje z večanjem

vrednosti premoženja, je vodstvo tveganju bolj naklonjeno. Vodstvo je manj naklonjeno odločitvam, ki povečujejo spremenljivost denarnih tokov.
Pripravljenost za prevzemanje tveganj (angl. *Risk Appetite*) je strateška naravnanost vodstva glede tega, kakšno stopnjo izpostavljenosti tveganjem je pripravljeno sprejeti. Cilj obvladovanja operativnih tveganj v podjetju XY je čim bolj zmanjšati izgube ter doseči skladnost z dodeljenimi viri in s proračunom. Z vidika pripravljenosti za prevzemanje operativnih tveganj so v priročniku o upravljanju z operativnim tveganjem (Podjetje XY, 2015a) določena osnovna pravila. Ta opredeljujejo, da je treba ugotovljena bistvena (visoka) tveganja obravnavati lokalno, v smislu njihovega razumevanja in ublažitve.

Temelj za proučevanje posameznikove nagnjenosti k tveganju je posameznikova krivulja koristnosti, ki jo prikazuje Slika 7. Von Neuman in Morgenstern sta v domnevi krivulje koristnosti razvila von Neumann-Morgensternovo funkcijo koristnosti. Funkcija temelji na razmišljanju in ugotovitvah Daniela Bernoullija, profesorja matematike na Ruski akademiji v St. Peterburgu. Profesor je prišel do ugotovitve, da se ljudje nikoli ne izpostavljajo tveganjem, če to ni potrebno. Von Neumann-Morgensternova funkcija koristnosti prikazuje razmerja med stopnjo tveganja ter višjo donosnostjo in koristnostjo posameznika. Razmerje ni linearno. Z naraščanjem tveganja oziroma donosnostjo se povečuje koristnost posameznika, vendar ne za enak prirastek. Prirastek koristnosti je pri prirastku donosnosti istega obsega čedalje manjši. Funkcija koristnosti je s tem razlogom konveksne oblike (Berk et al., 2005, str. 40).

Slika 7: Von Neumann-Morgensternova krivulja koristnosti



Vir: A. Berk, J. Peterlin, & P. Ribarič, Obvladovanje tveganj: skrivnosti celovitega pristopa, 2005, str. 40.

Kriteriji tveganj so določene meje, s katerimi podjetje lažje razmeji tveganja, ki jih je mogoče sprejeti, od tveganj, ki jih je treba obravnavati. Podjetje je odgovorno za opredelitev kazalnikov, ki jih bo uporabilo kot kriterije tveganj za instrumente ali metode

upravljanja z operativnimi tveganji. Hkrati lahko sprejme različne sisteme in meje, s katerimi opredeli kriterije tveganj. Obravnava tveganj (angl. *Risk Treatment*) je proces izbora in izvedbe ukrepov za spreminjanje tveganj. Pri tem izbrano podjetje XY uporablja naslednje možnosti, ki jih opredeljuje Priročnik o upravljanju z operativnim tveganjem (Podjetje XY, 2015a):

- sprejem tveganj (angl. *Risk Acceptance*) – strategija: gre za namerno sprejemanje določenih tveganj na ciljno usmerjen način, kar zajema odločitev uprave, da sprejme tveganja brez nadaljnje ublažitve ali prenosa za določeno obdobje;
- prenos tveganj (angl. *Risk Transfer*) – strategija: gre za inteligentni prenos tveganj na tretje osebe, s katerimi se poskuša doseči delitev tveganj z drugimi osebami – večinoma zavarovalnicami ali zunanjimi izvajalci;
- zmanjševanje tveganj (angl. *Risk Reduction)* – strategija: inteligentno zmanjševanje tveganj pri njihovem razvoju, s katerimi se poskuša zmanjšati preostala tveganja z uporabo zaščitnih ukrepov, namenjenih odpravi ali zmanjšanju verjetnosti zaporedja dogodkov, ki bi lahko povzročili resne negativne posledice;
- izogib tveganjem (angl. *Risk Avoidance)* – strategija: tveganj ne prevzemamo; kot poslovna strategija, da se določenih vrst dejavnosti ali poslovnih procesov ne izvaja, ker so tveganja previsoka, da bi lahko upravičila donos na naložbo.

4.2.4 Kvalitativno ocenjevanje operativnih tveganj

V podjetju XY se uporabljata dva pristopa ugotavljanja in vrednotenja operativnih tveganj, opredeljena v Priročniku o kvalitativnem ocenjevanju operativnih tveganj (Podjetje XY, 2016b). Gre za pristop na podlagi posameznih dogodkov (ocene tveganj) in redne ocene (analiza scenarijev). Analiza, izhajajoča iz posameznih dogodkov, se izvaja za predmete tveganj, kadar se ocenjevanje tveganj uporablja za presojo nujnosti v okviru začetnega hitrega pregleda (angl. *Initial fast screening*). Če je tveganje nizko (»nebistveno«), nadaljnji koraki niso potrebni. Če se v oceni tveganj ugotovi ključno tveganje, je treba izvesti podrobnejšo analizo. Analiza scenarijev uporablja isti pristop, vendar se v okviru istega področja/oddelka izvaja vsaj vsako leto. Postopki poročanja, obdelave in pregleda se sprožijo na osnovi izpostavljenosti tveganjem: na primer o vseh velikih tveganjih je treba poročati vodstvu podjetja, ublažitvene ukrepe pa je treba načrtovati, izvesti in jim slediti takoj. V nadaljevanju sta podrobno opredeljena oba pristopa ugotavljanja in vrednotenja operativnih tveganj.

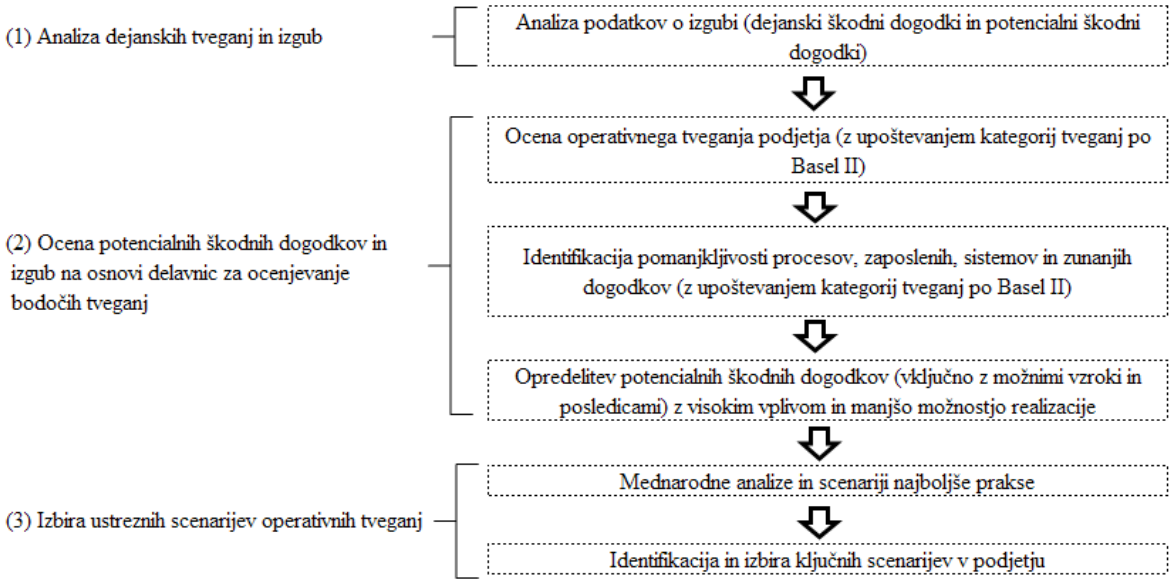
1. Ocena tveganj: osnovni cilj ocene tveganj je izvedba podrobne ocene tveganj in ugotavljanje dejanskega tveganja, povezanega s predmetom tveganj. DORO mora zagotoviti, da bodo vsi »bistveni« (angl. *Essential*) ali »delno bistveni« (angl. *Partly essential*) predmeti tveganj (angl. *Risk Objects*) analizirani v okviru ocenjevanja tveganj v sodelovanju z vodjem področja (razvoj izvedbenega načrta). Tveganja, ki bi lahko/povzročajo veliko finančno škodo, mora vodja področja takoj poročati vodstvu

podjetja, odgovornemu za zadevno področje. Takoj po ugotovitvi takšnih tveganj mora DORO v dotičnem oddelku poročati ugotovljene predmete tveganj in s tem povezane rezultate. Z uporabo kategorij tveganj iz sporazuma Basel II se ugotavljajo in analizirajo posamezna tveganja, povezana s predmetom tveganj, z vidika potencialne škode/zneska izgube, ter potencialna verjetnost njihovega pojava v okviru podatkovne baze za zbiranje škodnih dogodkov. Pogostost pregledov je odvisna od pomembnosti tveganj. ORO je odgovoren za vodenje pregleda nad izdelanimi popisi tveganj (angl. *Risk Inventories*).

2. Scenariji operativnih tveganj: analiza scenarijev je eno od orodij, ki se uporablja za obvladovanje operativnih tveganj. Namen te analize je določiti scenarije potencialne škode/izgub, ki se po navadi pojavljajo z nizko pogostostjo in lahko imajo velik negativen finančni učinek. Scenariji so skupina dogodkov z operativnimi tveganji, tj. vsota incidentov, ki povzročijo, da se dejanski izidi poslovnega procesa razlikujejo od pričakovanih izidov zaradi neustreznih ali neuspešnih procesov, ljudi in sistemov ali zaradi zunanjih dogodkov, ki povzročijo vsoto negativnih vplivov na dobiček ali kapitalsko vrednost podjetja. Scenariji predstavljajo »verjetno« prihodnost in morajo biti zato zasnovani na verjetnih dogodkih s tveganji. Možni dogodki s tveganji so lahko bodisi interno ali zunanje pogojeni ter lahko upoštevajo makroekonomske in/ali zunanje dejavnike.

Zasnova scenarijev v podjetju XY sledi tristopenjskemu pristopu, ki ga prikazuje Slika 8. Posamezni koraki (stopnje) so opisani v nadaljevanju.

Slika 8: Zasnova scenarijev operativnih tveganj



Vir: Podjetje XY, Priročnik o kvalitativnem ocenjevanju operativnih tveganj, 2016, str.5.

1. korak: Analiza dejanskih tveganj in izgub: gre za poglobljeno analizo interne podatkovne baze izgub (vključno z zbranimi dejanskimi škodnimi dogodki in s skorajšnjimi škodnimi dogodki (angl. *Near misses*)) v zadnjih petih letih.

2. korak: Ocena potencialnih škodnih dogodkov in izgub na osnovi delavnic za ocenjevanje prihodnjih tveganj: V naslednjem koraku se oceni profil operativnih tveganj posameznega področja/oddelka v podjetju in ugotavljanje potencialnih tveganih dogodkov (vključno z možnimi vzroki in posledicami) na osnovi strukturiranih delavnic za ocenjevanje prihodnjih tveganj z vnaprej izbranimi vodjami področij. Delavnice za oceno tveganj so namenjene prepoznavanju pomanjkljivosti in vrzeli v okviru posameznega oddelka glede procesov, produktov, sistemov in ljudi ter tudi zunanjih dogodkov (v skladu s kategorijami tveganj po Baslu II), kar lahko vodi do nastanka velikih potencialnih izgub ali v najslabšem primeru povzroči, da podjetje preneha poslovati ali je njegov ugled za več let načet.

3. korak: Izbira ustreznih scenarijev operativnih tveganj: sledita ugotavljanje in izbira scenarijev na podlagi mednarodnih in nacionalnih primerjav ter scenarijev najboljše prakse (ali zunanjih podatkov, če so na voljo).

Opisani pristop, ki ga uporablja izbrano podjetje, upošteva (pod)kategorije tveganj po Baslu II20. Strateško tveganje (na primer dogodki z operativnimi tveganji, ki izhajajo iz strateškega odločanja na ravni vodstva) je izrecno izključeno. Scenariji operativnega tveganja izbranega podjetja so opredeljeni na podlagi zbranih podatkov o izgubah in strokovne presoje vodij področja v skladu s kategorijami tveganj po Baslu II oziroma podkategorijami tveganj. Zajemajo materialna operativna tveganja, s katerimi se srečuje podjetje (Podjetje XY, 2016b).

4.2.5 Poročanje

Izbrano podjetje redno poroča skupini v skladu z določenimi standardi in opredelitvami poročanja. Na ravni skupine se zbirajo naslednje vrste poročil, ki so opredeljene v Priročniku o obvladovanju operativnega tveganja (Podjetje XY, 2016b):

- ad-hoc poročila o bistvenih izgubah (bruto izguba > 100.000 €);
- redno poročilo o stanju (angl. *Status Report*) in gibanjih, vključno s predstavitvijo podatkov o izgubah in skupinskih scenarijev;
- operativna tveganja naložb s popravki vrednosti.

[20] Kategorije tveganj po Baslu II: 1. notranja goljufija; 2. zunanja goljufija; 3. ravnanje v zvezi z zaposlovanjem in varnostjo pri delu; 4. stranke, produkti in poslovna praksa; 5. škoda na premičnem in nepremičnem premoženju; 6. prekinitve poslovanja in izpadi sistemov; 7. izvedba, dostava in upravljanje procesov.

Ad-hoc poročila je treba izvesti v primeru, ko je bruto izguba zaradi operativnih tveganj večja od 100.000 EUR. Ad-hoc poročilo mora odgovorni ORO nemudoma po odkritju poslati zaposlenemu za obvladovanje operativnih tveganj na raven skupine, v vsakem primeru pa najkasneje v petih delovnih dneh po tem, ko se vnese škodni dogodek v podatkovno bazo škodnih dogodkov. Izgube zaradi operativnih tveganj se na ravni skupine zbirajo in poročajo vsako četrtletje. Poročanje poteka v okviru poročila o tveganjih, ki je skupno poročilo o kreditnih, tržnih in operativnih tveganjih. Četrtletno poročilo o izgubah vsebuje podatke o pomembnih škodnih dogodkih z enkratno izgubo, vključno z opisom (na primer organizacije, vzroke, izgube); grafične predstavitve izgub po poslovnih področjih in kategorijah tveganj; pravne postopke in primere goljufij, povezane z operativnimi tveganji; skorajšnje škodne dogodke; kvantificiranje ocen (opis ugotovljenih operativnih tveganj); splošne komentarje in ključne kazalnike uspešnosti.

4.3 Proces vzpostavitve notranjih kontrol

Sistem notranjih kontrol v podjetju XY se prvovrstno gradi na že odkritih škodnih dogodkih z vidika operativnega tveganja, predstavljeno v preteklih točkah. V nadaljevanju so po sklopih navedeni proces uvedbe sistema notranjih kontrol, ki je bil vpeljan v podjetje XY, predlogi, ki bi lahko izboljšali postopek, in predlogi, s pomočjo katerih bi lahko dvignili pomembnost in zavest pri zaposlenih, da poznavanje in spremljanje ključnih tveganj pripomore k učinkovitosti poslovanja.

4.3.1 Ozaveščanje o tveganjih

Notranje kontrole temeljijo na sistemu organiziranosti dela, sistemu nadzorovanja, ločenosti izvajanja postopkov dela, razmejitvi odgovornosti, postopkih upravljanja z zaposlenimi, sistemu pooblastil, informacijskem sistemu finančne inštitucije, razmejitvi konflikta interesov itd. Menim, da je ozaveščanje o tveganjih eden izmed prvih najbolj pomembnih korakov v procesu organizacije sistema notranjih kontrol v podjetju XY. Ozavestiti zaposlene, da tveganja obstajajo, da se jih zavedajo in naučijo prepoznavati. V podjetju XY k ozaveščanju zaposlenih o operativnem tveganju[21] pristopajo po naslednjem postopku. Najprej se v vsakem oddelku določi zaposleni, ki je seznanjen s celotnim delovnim procesom v oddelku, poimenovan decentralizirani upravljavec operativnega tveganja – DORO. Za vse omenjene se pripravi individualno izobraževanje na temo prepoznavanja operativnega tveganja in beleženja škodnih dogodkov v lokalno aplikacijo za zbiranje škodnih dogodkov. Glede na dejstvo, da se škodni dogodki ne pojavljajo z enakomerno časovno frekvenco, zaposleni mnogokrat pozabijo oziroma niso pozorni na to, da bi ob nekem primeru zaznali škodo in jo neposredno povezali z operativnim tveganjem.

[21] Operativno tveganje v podjetju (če upoštevamo raven odločanja managementa) je povezano tudi s kreditnim tveganjem, tržnim in likvidnostnim tveganjem, saj so škodni dogodki pogosto povezani tudi s temi področji.

Kot drugo, zaposleni se lahko poskušajo izogniti dodatnemu delu, ki ga imajo s poročanjem o škodnih dogodkih. Na tem mestu bi podjetju predlagala, da se zaposlene enkrat mesečno prek e-pošte opomni in naprosi k poročanju morebitnih odkritih tveganj. Na ta način se zagotovi ažurno zbiranje škodnih dogodkov. Kljub temu da so za beleženje škodnih dogodkov odgovorni določeni posamezniki, v podjetju stremijo k temu, da vse zaposlene podučijo o prepoznavanju in odkrivanju škodnih primerov in hkrati dolžnosti o poročanju odkritih dogodkov odgovornemu DORO v oddelku. Eden od načinov komunikacije, ki ga uporabljajo, je obveščanje zaposlenih prek interne spletne strani, kjer je na kratko predstavljeno, kaj je operativno tveganje ter kakšne so dolžnosti vseh zaposlenih, namen, cilji in nadaljnji postopki pri realizaciji projekta. Isti pristop so namenili obveščanju zaposlenih o projektu internega kontrolnega sistema, kar prikazuje Slika 9.

Kljub internim izobraževanjem ter splošni predstavitvi iz prakse ugotavljam nespretnost zaposlenih pri prenosu teoretičnega znanja v prakso in svoj delovni proces. S tega vidika je še kako treba vpeljati sistem notranjih kontrol v podjetje. Najprej bi bilo smotrno, da se organizirajo individualne delavnice v oddelkih, poišče čim več primerov iz prakse ter pripravi priročnik oziroma katalog vseh zbranih predlogov, ki bi bil na voljo vsem zaposlenim v podjetju. Izmenjava znanja bi lahko pripomogla k preprečitvi nastanka morebitnih nepravilnosti.

Slika 9: Ozaveščanje zaposlenih o sistemu notranjih kontrol

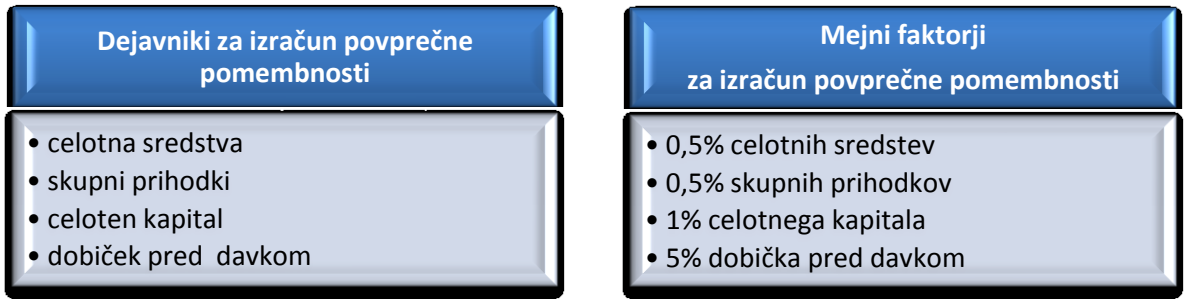
Vir: Podjetje XY, Področja in službe>Kontroling tveganj, 2016.

4.3.2 Računovodska matrika in predlog mejnega zneska

Zbrani škodni dogodki iz preteklosti so nekakšna predpriprava za nadaljevanje vpeljave procesa sistema notranjih kontrol. Enkrat letno se v podjetju pripravi seznam relevantnih procesov, ki jim je treba določiti ključna tveganja in jih testirati (ko so tveganja enkrat popisana, se jih samo še testira oziroma ažurira, če je potrebno). Da pridemo do seznama procesov, pripravimo računovodsko matriko. Računovodska matrika (angl. *Account matrix*) je dokument, na podlagi katerega se pripravi seznam procesov, ki so na prednostni listi za obravnavo z vidika notranjega kontrolnega sistema. Matriko uporabimo za izračun celotne pomembnosti (angl. *Overall Materiality*) in vsebuje osnovne informacije o kontih glavne knjige, ki jih poroča oddelek računovodstva, ter vse potrjene podatke iz zadnjega letnega finančnega poročila. Na podlagi teh podatkov določimo mejni znesek (angl. *Haircut*), ki razvrsti relevantne konte in z njimi povezane delovne procese.

Celotna pomembnost predstavlja stopnjo splošno sprejemljive napake (ali več napak) v konsolidiranem finančnem izkazu, medtem ko dopustna stopnja napake (angl. *Tolerable error*) predstavlja najvišjo stopnjo napake (ali več napak), ki se nanaša na posamezen konto v finančnem izkazu. Da omejimo obseg sistema notranjih kontrol na ustrezne konte in procese, konte selekcioniramo na podlagi njihovega stanja z uporabo dopustne stopnje napake kot merilo selekcije. V skladu z mednarodnimi smernicami lahko povprečno pomembnost (angl. *Average Overall Materiality)* določimo na podlagi: sredstev, prihodka, kapitala in dobička pred davkom (Tabela 1, prikazano v vrstici a), z uporabo predhodno določenih mejnih faktorjev s strani skupine, ki so prikazani v Sliki 10 (v Tabeli 1 prikazano v vrstici b).

Slika 10: Dejavniki za izračun povprečne pomembnosti po mednarodnih smernicah



Vir: Podjetje XY, Account Matrix manual, 2011, str. 6.

Tabela 1 prikazuje primer izračuna mejne vrednosti. Kot splošno pravilo je s strani skupine priporočljivo, da se upošteva dopustno stopnjo napake pri 50 %, vendar kljub temu posamezno podjetje znotraj skupine predlaga višino mejne vrednosti, ki se nato odobri na ravni skupine. Podatki so prirejeni kot primer in ne izkazujejo dejanskega stanja v podjetju XY. Na letni ravni se pripravi predlog mejnega zneska, sprejetega na ravni lokalnega vodstva, ter pošlje v potrditev na ravni skupine. Primer predloga se nahaja v Prilogi 1.

Povprečna pomembnost za leto 2016 predstavlja 1,13 mio EUR (glej Tabelo 1), kar predstavlja povprečje sredstev, prihodkov, kapitala in dobička pred davkom. Povprečne vrednosti izračunamo tako, da najprej seštejemo vse vrednosti dejavnikov (po upoštevanem mejnem faktorju – glej Sliko 10) in dobljen rezultat delimo s številom vrednosti. Izračun je po enačbi (1).

$$\textit{Povprečna pomembnost}_{2016} = \frac{\textit{sredstva + prihodek + kapital + dobiček pred davkom}}{4} \quad (1)$$

Pri tem smo pozorni, da se upošteva mejne faktorje za izračun podatkov. Zneske celotnih sredstev, prihodkov, kapitala in dobička pred davkom, ki so enaki podatkom v bilanci stanja (stolpec a), pomnožimo z mejnimi faktorji (stolpec b v Tabeli 1 ali kriteriji iz Slike 10). V našem primeru je podatek za dobiček pred davkom z negativnim predznakom (-11,28 mio EUR – glej Tabela 1, stolpec (6)); to pomeni, da je podjetje v letu 2016 zabeležilo izgubo. Izračun je po enačbah (2), (3), (4) in (5), rezultati so prikazani v Tabeli 1, vrstica c, stolpci od (3) do (6).

$$\textit{Celotna sredstva (po upoštevanem faktorju)} = 0{,}5\ \% * \textit{celotna sredstva} \quad (2)$$

$$\textit{Prihodek (po upoštevanem faktorju)} = 0{,}5\ \% * \textit{prihodek} \quad (3)$$

$$\textit{Kapital (po upoštevanem faktorju)} = 1\ \% * \textit{kapital} \quad (4)$$

$$\textit{Dobiček pred davkom (po upoštevanem faktorju)} = 5\ \% * \textit{dobiček pred davkom} \quad (5)$$

Podatki za zgoraj omenjena povprečja so pridobljeni iz letnega finančnega poročila. Priporočljivo je, da se pri izračunu uporabi povprečje posameznega dejavnika, ki odraža gospodarski položaj podjetja, in posledično izračuna tudi povprečno pomembnost. Mejni znesek predstavlja odstotek dopustne napake, ki se ga izračuna na podlagi celotne povprečne pomembnosti. V Tabeli 1 stolpec (2) prikazuje izračune mejnih zneskov v višini 25 % (282.286 EUR), 40 % (451.657 EUR) in 75 % (846.858 EUR). Izračune se opravi po enačbah (6), (7) in (8).

$$\textit{Mejni znesek 1} = 75\ \% * \textit{povprečna pomembnost} \quad (6)$$

$$\textit{Mejni znesek 2} = 40\ \% * \textit{povprečna pomembnost} \quad (7)$$

$$\textit{Mejni znesek 3} = 25\ \% * \textit{povprečna pomembnost} \quad (8)$$

Na podoben način se izračuna zneske za celotna sredstva, prihodke, kapital in dobiček pred davkom za posamezni odstotek mejnega zneska. Primer izračuna celotnih sredstev pri vseh treh mejnih vrednosti je prikazan v enačbah (9), (10) in (11).

$$\textit{Celotna sredstva za Mejni znesek 1} = 75\ \% * \textit{celotna sredstva (po upoštevanem faktorju)} \quad (9)$$

$$= 75\ \% * 3{,}29\ \textit{mio EUR}$$

*Celotna sredstva za Mejni znesek 2 = 40 % * celotna sredstva (po upoštevanem faktorju)* (10)

*= 40 % * 3,29 mio EUR*

*Celotna sredstva za Mejni znesek 2 = 25 % * celotna sredstva (po upoštevanem faktorju)* (11)

*= 25 % * 3,29 mio EUR*

Izbere se tisto mejno vrednost, ki pokrije čim več pomembnih kontov. V naslednjem primeru je končna mejna vrednost v podjetju XY privzeta pri 40 % povprečne pomembnosti. Mejni znesek znaša 451.657 EUR. To pomeni, da so vsi konti, katerih vrednost na presečni dan 31. 12. presega ta znesek, relevantni in pomembni za sistem notranjih kontrol.

Tabela 1: Prikaz izračuna mejnih zneskov na podlagi povprečne pomembnosti

Podatki 2016 v EUR

		(1) Dopustna stopnja napake	(2) Povprečna pomembnost	(3) Celotna sredstva	(4) Prihodek	(5) Kapital	(6) Dobiček pred davkom
a				659.211.324,16	15.269.136,52	58.012.293,85	- 11.280.979,81
b	Mejni faktorji			0,5%	0,5%	1,0%	5,0%
c	Povprečna pomembnost		1.129.143,56	3.296.056,62	76.345,68	580.122,94	564.048,99
d	Mejni znesek 1 (angl. Haircut)	75%	846.857,67	2.472.042,47	57.259,26	435.092,20	423.036,74
e	Mejni znesek 2 (angl. Haircut)	40%	451.657,42	1.318.422,65	30.538,27	232.049,18	225.619,60
f	Mejni znesek 3 (angl. Haircut)	25%	282.285,89	824.014,16	19.086,42	145.030,73	141.012,25
→ Mejni znesek (Haircut)		40%	€ 451.657				

Vir: Podjetje XY, Account Matrix manual, 2011, str. 7.

4.3.3 Identifikacija relevantnih procesov za obravnavo

Ko je mejni znesek določen, lahko pričnemo z nadaljnjim postopkom za pridobitev relevantnih procesov. Procesi, ki so pomembni za obravnavo z vidika sistema notranjih kontrol, se navezujejo na lokalne konsolidirane računovodske konte iz bilance stanja in izkaza poslovnega izida, katerih končno letno stanje je večje od ugotovljenega mejnega zneska (v našem primeru 451.657 EUR). Omenjenim kontom se določi lastnike, ki so odgovorni za knjiženje ter podatke o usklajevanjih (ročno, avtomatično) in frekvence knjiženj ter se jih poveže z delovnimi procesi, na katere vplivajo. Gre za enega izmed najpomembnejših in tudi najtežjih delov v postopku.

Določitev procesov, ki jim pripadajo določeni konti, poteka v sodelovanju z več področji hkrati, saj bo končni rezultat le tako optimalen. Glavni cilj pri identifikaciji relevantnih procesov je povečati pokritost bilance stanja z minimalnim številom procesov, ki jih je treba analizirati. Trenutno najpomembnejši procesi, ki so na prednostni listi obravnave z vidika sistema notranjih kontrol v podjetju XY, so pregled prejetih plačil in prevzetih predmetov, procesi, povezani s pravnimi primeri, ter prodajni procesi. Za posamezen

delovni proces je potrebna procesna dokumentacija, ki vključuje informacije o poteku, tveganjih in kontrolah.

Za uspešno oceno tveganj je procese treba modelirati v orodju za izris delovnih procesov. Glede na dejstvo, da vsi procesi niso modelirani v sistemu ali pa so zastareli, delovni proces pa mora biti pred popisom tveganj in kontrol potrjen s strani odgovornih, bi podjetju predlagala, da se pričnejo popisi na procesih, ki bodo potrjeni s strani odgovornih in objavljeni v ARIS aplikaciji »Business Publisher«. S tem bi zaposlenim, ki se ukvarjajo z modeliranjem procesov, pripravili tudi prioritetni plan za manjkajoče procese.

4.3.4 Management poslovnih procesov v podjetju

Management poslovnih procesov podpira vse zaposlene pri njihovih dnevnih aktivnostih na različnih področjih, s čimer izboljšuje transparentnost dela ter vmesnike do drugih področij in hkrati pomaga razviti postopke na vsakem področju z namenom doseganja najvišje učinkovitosti (odkrivanje, kje se pojavljajo ozka grla, in izdelava optimiziranega poteka). Omogoča boljše odločanje in pomaga pri izpolnjevanju zakonskih zahtev.

Glavni cilj managementa poslovnih procesov v podjetju XY je organizirati vse aktivnosti z namenom zadovoljitve želja in pričakovanj pri poslovanju s strankami. Princip odnosa stranke-podjetje velja tako za zunanji odnos na trgu kot tudi za odnos med sodelavci znotraj podjetja. Management poslovnih procesov je po sebi proces, ki zagotavlja nenehne izboljšave pri uspešnosti podjetja. Kot vsak proces zahteva vodenje in usmerjanje. Lahko ga definiramo kot področje znanja o križišču med vodenjem in informacijsko tehnologijo, pri čemer se uporabljajo metode, tehnike in orodja za oblikovanje, analizo in kontrolo procesov, vključujoč ljudi, podjetje, aplikacije, dokumente in ostale vire informacij.

Oblikovanje procesov vključuje modeliranje in zajem obstoječih procesov kot tudi simulacijo novih. Spremljanje procesov sledi posameznim procesom, tako da je informacije o njihovem stanju zlahka videti in zagotavljajo statistične podatke o uspešnosti enega ali več procesov. Sledenje omogoča definiranje stanja strankine zahteve (na primer prejeta zahteva, čakanje na dostavo, plačan račun), tako da so problemi pri izvedbi posameznega procesa lahko identificirani in odpravljeni. Primeri statističnih podatkov so izdelava meril, kako hitro je zahteva stranke procesirana, koliko zahtev je bilo procesiranih v zadnjem mesecu itd. Stopnja spremljave je odvisna od tega, katere informacije želi podjetje oceniti in analizirati ter kako jih želi spremljati, sproti ali ad-hoc (Podjetje XY, 2013a).

Izbrano podjetje obvladuje poslovne procese z uporabo aplikacije ARIS (angl. *Architecture of integrated Information Systems*) kot odgovor na naraščajočo konkurenco, višja pričakovanja strank, globalizacijo in hitrejši razvoj novih tehnologij, s katerimi se podjetje danes sooča. Za prilagoditev hitro spreminjajočemu se okolju je treba biti boljši v lastnem

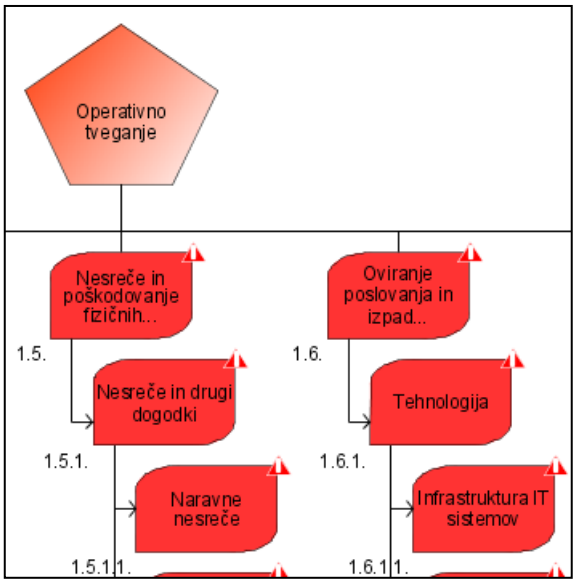
poslu od ostalih in pravočasno obvladovati spremembe. Management poslovnih procesov omogoča merljivost procesov z uvedbo ključnih dejavnikov, ki so ključnega pomena za podjetja za doseganje dveh glavnih ciljev − zagotoviti opredeljen rezultat z namenom zadovoljitve stranke (uspešnost) ter zagotoviti opredeljen rezultat z najnižjimi možnimi stroški (učinkovitost). Management poslovnih procesov hkrati podjetju omogoča izboljšati transparentnost procesov in stroškov, dokumentirati in standardizirati procese, natančno opredeliti odgovornosti, vizualizirati zahteve stranke, jasno definirati organizacijske prehode, identificirati in zmanjšati operativna tveganja, povečati produktivnost s postopkom nenehnih izboljšav, meriti in kontrolirati uspešnost procesa ter povečati motivacijo zaposlenih z možnostjo sodelovanja pri ustvarjanju procesa (Podjetje XY, 2013a).

4.3.5 Prepoznavanje ključnih in potencialnih tveganj

Fraser in Simkins (2016) podjetjem, ki se odločijo za izvajanje sistema notranjih kontrol, priporočata, da svoje zaposlene primerno izobrazijo. Zaposlenim naj poleg predstavitve in teoretičnega prikaza uprizorijo tudi praktično delavnico na realnih primerih. Ta način je veliko bolj praktičen za usposabljanje, saj se hkrati učijo metod in meril tveganj, ki se nanašajo na reševanje lastnih problemov v vsakodnevnem delovnem procesu. Prav tako ugotavljata, da podjetja sestavijo preobsežne sezname tveganj, ki lahko zaposlene preobremenijo in hkrati ne prinašajo dodane vrednosti, kar potrjuje tudi organizacija IFAC (International Federation of Accountants, 2011). Ta meni, da morajo biti notranje kontrole izbrane, implementirane in delujoče kot odziv na specifična tveganja in njihove možne interakcije.

Izbrano podjetje za vodenje sistema notranjih kontrol, kot že omenjeno, uporablja aplikacijo ARIS ter modul za obvladovanje tveganj in skladnosti, imenovan GRC-modul (angl. *Governance, Risk and Compliance*, v nadaljevanju GRC-modul), kjer se testira delovanje kontrol. Pred popisom tveganj in kontrol morajo biti delovni procesi modelirani in ažurirani v aplikaciji ARIS. Za ustrezno ugotavljanje in merjenje tveganj ter njihovo obvladovanje je treba razviti jasno prepoznavne kategorije tveganj, ki se medsebojno ne prekrivajo. Slika 11 prikazuje osnutek kataloga tveganj, kjer so s strani skupine definirane ključne kategorije tveganj, ki se uporabljajo pri popisu. Glavni dejavniki razvrščanja so vzroki za nastanek izgub in način, kako se lahko izgube pokažejo. Podjetju predlagam, da katalog tveganj redno ažurirajo na lokalni ravni, saj bi s tem optimizirali čas popisovanja tveganj. Aplikacija za modeliranje ARIS namreč omogoča, da se že definirana tveganja uporabi na več procesih.

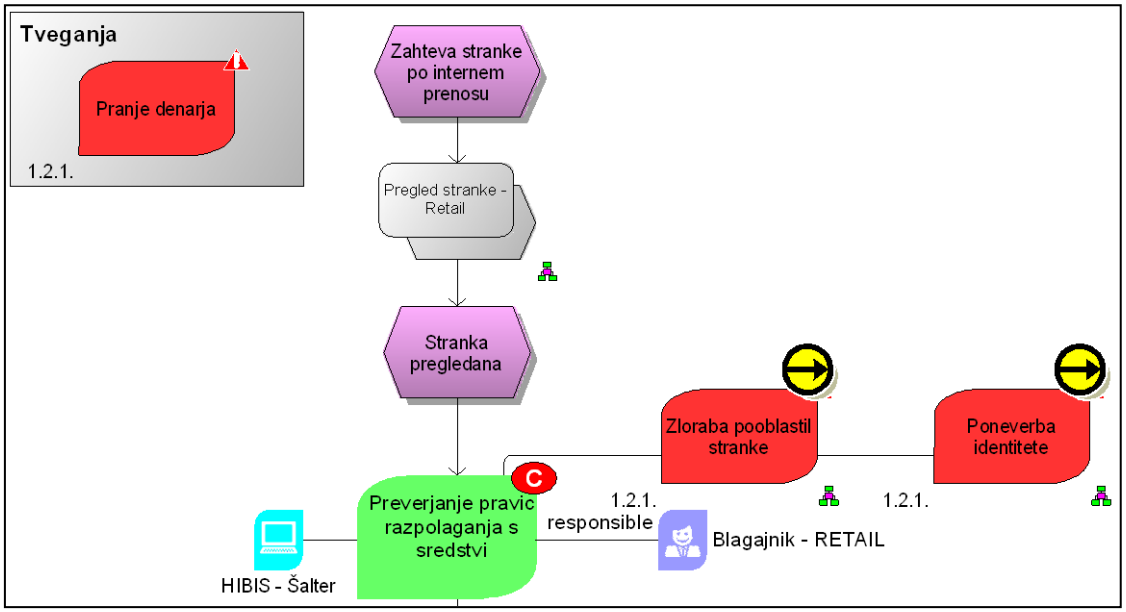
Slika 11: Osnutek kataloga tveganj



Vir: Podjetje XY, Katalog tveganj, 2012.

Slika 12 prikazuje primer poslovnega procesa v finančnem podjetju, izrisan v aplikaciji za modeliranje poslovnih procesov ARIS. Tveganja se na posameznem procesu definira na dva načina. Tveganja so lahko vezana na celoten proces; gre za splošna tveganja, ki se lahko zgodijo kadarkoli pri izvajanju procesa, neodvisno od izvajanja aktivnosti (na sliki Pranje denarja), ali pa so tveganja vezana na posamezno aktivnost in se lahko zgodijo izključno pri njenem izvajanju (na sliki Zloraba pooblastil stranke in Poneverba identitete).

Slika 12: Primer poslovnega procesa v finančnem podjetju



Vir: Podjetje XY, Navodilo za vnos tveganj, kontrol in testov, 2012, str.5.

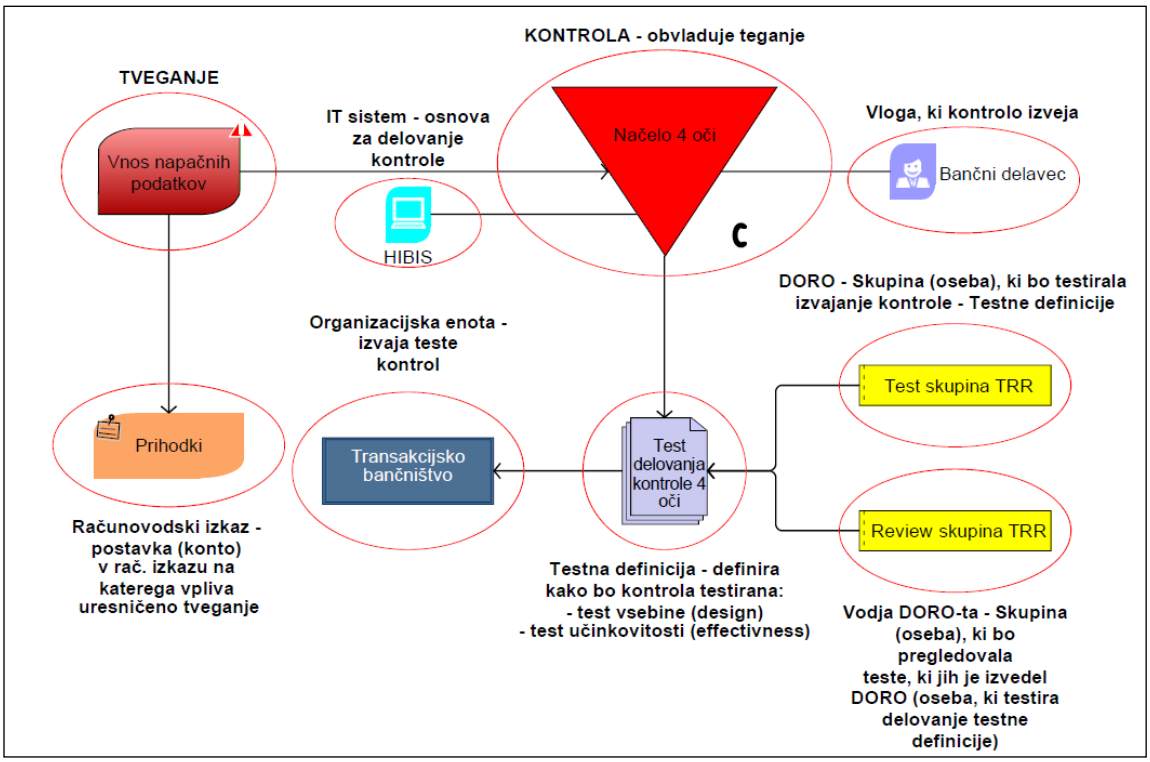
V aplikaciji ARIS se modeliranim tveganjem kreira diagram (angl. *Business Control Diagram*, v nadaljevanju BCD), kjer se definira podrobnosti tveganj, kontrol, testnih definicij za kontrole in odgovorne organizacijske enote za testiranje kontrol posameznega tveganja. Na podlagi izpolnjenega BCD se lastnosti tveganja, kontrol in testnih definicij prenese v aplikacijo za testiranje tveganj GRC-modul, kjer se vzpostavijo testni primeri, s katerimi odgovorne osebe (angl. *Tester in Test Reviewer*) ugotavljajo ustreznost delovanja kontrol.

Slika 13 prikazuje primer modeliranja tveganja z vsemi pripadajočimi elementi. Zaradi tehničnih postopkov aplikacije ARIS si morajo elementi slediti, kot je prikazano. Neki aktivnosti v procesu se je določilo tveganje vnosa napačnih podatkov. Tveganju se najprej določi računovodski izkaz oziroma konto, na katerega vpliva realizirano tveganje. Sledi opredelitev vsaj ene primerne kontrole, ki omenjeno tveganje obvladuje/preprečuje.

Ugotovi se, da je najprimernejša kontrola načelo štirih oči, kar pomeni, da se tveganje minimizira/odpravi z dodatno kontrolo, ki jo opravi drugi zaposleni. Kontroli se dodeli naziv delovnega mesta (vloga zaposlenega), ki bo kontrolo izvajal. V našem primeru bo kontrolo štirih oči izvajal bančni delavec, pri tem pa bo uporabil sistem Hibis. Kontroli načelo štirih oči dodelimo testno definicijo. To pomeni, da določimo test, ki definira način, kako se bo v nekem določenem intervalu testiralo delovanje kontrole štirih oči. Opredelimo lahko dve vrsti testa.

Testiramo lahko primernost vsebine kontrole (angl. *Test of design*) ali učinkovitost kontrol (angl. *Test of effectiveness*). Testu se določi organizacijsko enoto (Transakcijsko bančništvo), ki bo odgovorna za testiranje, ter naziv testerja in kontrolorja. Testiranje delovanja kontrole predlagam, da se izvaja s strani DORO (Test skupina TRR), saj ima širši pregled in pozna postopke. Vodja oddelka, v katerem deluje DORO, prevzame vlogo kontrolorja testiranj (skupina kontrolorji TRR).

Slika 13: Diagram z vsemi obveznimi elementi



4.4 Ocena učinkovitosti notranjih kontrol v podjetju XY

Spremljanje sistema notranjih kontrol v podjetju XY je podprto s tako imenovanim GRC-modulom. Z njim se spremlja ukrepe, ki so se opredelili aktivnostim pri modeliranju kontrolnih točk, testira učinkovitost določenih ukrepov, prikaže, ali določene izboljšave delujejo, meri, spremlja in ocenjuje stopnjo tveganosti in učinkovitosti nadzora in spremlja revizijske dejavnosti in rezultate. Na ta način se pridobi seznam potencialnih predlogov za izboljšanje. Za učinkovitost GRC-modula so potrebne številne komponente, vključno z identifikacijo in klasifikacijo tveganj, s klasifikacijo kontrol, z določanjem lastnikov testov, odgovornega za potrditev opravljenih testov in odgovornega za odpravo pomanjkljivosti (angl. *Issue owner*), s celostnim pristopom, z vodenjem, s skladnostjo in z obvladovanjem tveganj. Učinkovit GRC-modul vključuje ljudi, procese, tehnologijo in organizacijske dejavnike, kot prikazuje Slika 14 (Podjetje XY, 2012).

Slika 14: Model upravljanja modula »Governance Risk & Control«

Vir: Podjetje XY, Testiranje v GRC modulu, 2012, str.6.

Celoten proces testiranja delovanja ključnih kontrol se izvede v štirih korakih. Najprej se določi kontrole za testiranje v povezavi s fazo dokumentiranja, sledi določitev zaposlenih, odgovornih za izvedbo testiranja, pripravi scenarije za testiranje in ovrednoti rezultate. Pri načrtovanju testiranja je treba določiti predmet testiranja, na kakšen način in kdaj se bo izvajalo testiranje. Načrt je treba pripraviti z mislijo na zadovoljivo raven zagotovila, ki jo bodo nudile kontrole, glede zaznavanja ali preprečevanja nepravilnosti. Na dan testiranja posamezne kontrolne točke tester prejme na svojo elektronsko pošto obvestilo, da je treba opraviti test. Na razpolago ima 14 dni, da opravi test delovanja kontrolne točke. Po preteku 75 % časa, določenega za testiranje, so tester, »test reviewer« in »GRC-administrator« prek elektronske pošte obveščeni o iztekajočem se testu. Ko preteče čas, v katerem bi tester moral opraviti test kontrole in te ne opravi, sistem avtomatsko obvesti testerja, »test reviewerja« ter »GRC administratorja«, da določen test kontrole ni bil opravljen. Glavna naloga testerja je opraviti test in ugotoviti, ali so postavljene kontrolne točke na posameznih aktivnostih učinkovite. Njegova naloga je, da pregleda opis tveganja in kontrole, da dobi občutek, kakšno je tveganje ter kako poteka kontrola za odpravljanje določenega tveganja. V skladu z navodili opravi test pravilnosti delovanja in svoje ugotovitve zapiše v sistem.

Ugotavljam, da je postopek sistema notranjih kontrol v podjetju teoretično primerno zastavljen in podprt z ustreznimi podrobnimi delovnimi navodili, notranjimi politikami in s pomožnimi aplikacijami. Nadalje ob pregledu izvedbe celotnega postopka ugotavljam, da se postopek primerno izvede do točke, ko se pričnejo popisi tveganj in kontrol s strani odgovornega zaposlenega. Kvaliteta in kvantiteta delovnih procesov v podjetju nista primerni. Ugotavljam, da modelirani delovni procesi niso ažurirani, tako z vidika pravilnosti sledečih si aktivnosti v delovnem procesu kot odgovornih oseb za opravljanje

aktivnosti. Veliko procesov, ki so pomembni za obravnavo z vidika notranjih kontrol, manjka. Na tem mestu predlagam, da se postavi prioritete na mesto funkcije odgovornega za modeliranje delovnih procesov. Predlagam, da se ažurira že obstoječe delovne procese in postopoma modelira še preostale, ki so pomembni.

Po nadaljnjih pregledih sem prišla do ugotovitev, da so se popisi tveganj pričeli kljub neažurnemu stanju podatkov v procesu. Na določenih procesih je bilo vključenih preveč tveganj, ni se popisovalo le ključnih. Z enega vidika se tako zavedamo vseh možnih nevarnosti, vendar naj se za testne namene testira le ključne kontrole. Podrobni popisi tveganj in kontrol sledijo metodi COSO. Med popisi se je večkrat izkazalo, da sta znotraj delovnega tima pomanjkljivo znanje in zmožnost opredelitve vseh ključnih podrobnosti tveganj in kontrol. Tu se kažejo nepopolno informiranje zaposlenih in neprenos znanja med sodelavci kot tudi prenos znanja na nove sodelavce. Podjetju bi svetovala, da svoje resurse usmeri v izobraževanje zaposlenih in vzpodbudi vodje področij, da organizirajo primeren prenos znanja ob fluktuaciji zaposlenih.

Ob končanih popisih tveganj in kontrol je sledil prenos podatkov iz aplikacije ARIS v aplikacijo GRC-modul. Pri tem je bilo zaznanih kar nekaj težav, saj morajo biti procesi pravilno tehnično modelirani, da se lahko prenesejo v GRC-modul. Postopek odprave anomalij je zamuden, zato bi na tem mestu predlagala, da se pripravi spisek vseh tehničnih napak, ki onemogočajo prenos, da se uredijo s strani odgovornih za aplikacijo GRC-modul.

Po nekaj uspešnih prenosih tveganj, kontrol in testnih definicij v sistem se je pričelo testiranje. Ugotavljam, da je aplikacija v nadaljevanju primerno delovala, hkrati je omogočala pripravo dodatnih poročil. Vsekakor pa na mestu odgovornega za popis tveganj in kontrol vidim osebo, ki je vztrajna in ciljno usmerjena, saj je v času vpeljave procesa kar nekaj pomanjkljivosti, ki jih je še treba izpopolniti.

SKLEP

Ustrezno in učinkovito ravnanje s tveganji je v zadnjem desetletju pridobilo pomembno vlogo, kar gre pripisati pojavom finančnih škandalov in želji po povečanju dobička lastnikov. V podjetju XY so osredotočeni predvsem na spremljanje kreditnega tveganja ter v malo manjšem obsegu tudi na obrestno, likvidnostno, valutno in operativno tveganje. V nalogi sem se osredotočila na obvladovanje operativnih tveganj in vpeljavo sistema notranjih kontrol v podjetju XY.

Za učinkovit sistem notranjih kontrol so potrebni zavedanje in informiranje zaposlenih ter zapis politik in postopkov, imeti in uporabljati je treba ustrezna orodja in avtomatizacije procesa, imeti in uporabljati je treba izkušnje in znanja zaposlenih, oceniti odgovornost zaposlenih in postaviti merila za posamezne notranje kontrole.

Menim, da se proučevano podjetje XY zaveda notranjih in zunanjih nevarnosti, saj je v preteklosti notranja revizija v določenih časovnih intervalih spremljala učinkovitost ključnih kontrolnih točk, ki so bile zavedene v delovnih navodilih, politikah ali modelirane v aplikaciji ARIS. Nepravilnosti so bile izpostavljene in predane v reševanje odgovornim.

Ugotavljam, da so postopki vpeljave primernega sistema notranjih kontrol še v začetni fazi. V podjetju so določili odgovornega zaposlenega za vodenje vpeljave sistema notranjih kontrol. Pripravila so se ustrezna delovna navodila za popis tveganj, navodila za uporabo aplikacije za testiranje učinkovitosti kontrol in politika, ki ureja področje. Na podlagi izpolnjenega dokumenta »Account Matrix« je podjetje določilo procese, ki so ključnega pomena za poslovanje.

Po nadaljnjih pregledih procesov ugotavljam, da je procesni management v podjetju pomanjkljiv. Delovni procesi v aplikaciji ARIS niso primerno modelirani, saj ne prikazujejo zadnjih veljavnih postopkov, kar je posledično že privedlo do nepoznavanja vseh aktivnosti znotraj procesov in nepoznavanja morebitnih tveganj, ki bi se lahko pripetili oziroma so se že zgodili. Poleg modeliranja v aplikaciji so delovni procesi opisani in sprejeti tudi prek interne dokumentacije kot procesna navodila. Mnogo dokumentov je nepopolnih, saj jih zaposleni ročno dopolnjujejo, kontrola zaključenih in potrjenih navodil se ne izvaja. Podjetju predlagam, da postavi prioritete pri pomembnosti popisov procesov, prične z urejanjem delovnih procesov in redno spremlja napredek.

V začetni fazi so v oddelku organizacije zagotovili popolnost podatkov za nekaj ključnih procesov, za katere so nato določili tveganja in kontrole. Popis podatkov temelji na metodi COSO. Ob popisu podatkov sem zaznala, da zaposlenim primanjkuje osnovno znanje poznavanja delovnih procesov. Podjetju XY svetujem, da svoje resurse usmeri v izobraževanje zaposlenih. Pomembno je predvsem to, da vodje področij ali oddelkov poskrbijo, da se znanje ustrezno prenese na vse zaposlene. Po popisu tveganj in kontrol na

določenih procesih je sledil prenos diagramov iz aplikacije ARIS v testno aplikacijo GRC-modul. Pri nekaterih prenosih so se odkrile tehnične težave, nastale zaradi neprimernega modeliranja procesa. Glede na dejstvo, da je bilo več različnih težav pri prenosu, bi podjetju na tem mestu predlagala, da odpravo nepravilnosti rešuje podjetje, ki podpira aplikacijo GRC-modul.

Diagrami, ki so bili uspešno preneseni v modul za testiranje GRC, so bili testno preverjeni s strani testerjev. Aplikacija je primerna za testiranje kontrol, prav tako je na voljo več vrst poročil. Testiranje delovanja ključnih kontrol se je izvedlo samo v testnem okolju. Podjetju XY svetujem, da motivira zaposlene za nadaljnje delo v produkcijskem okolju, saj se procesi redno spreminjajo, pojavljajo se nove nevarnosti. Uvedba aplikacije za testiranje je ena od prednosti za spremljavo, saj so zbrani vsi podatki na enem mestu. Glede na dejstvo, da sistem notranjih kontrol v podjetju XY še ni vzpostavljen daljše obdobje, ne morem trditi, da je učinkovit. Začetki popisov in testiranj v testnem okolju so pokazali uspešne zaključke, realni rezultati pa se bodo pokazali čez čas. Moje mnenje in sklepna ugotovitev magistrskega dela sta, da so operativna tveganja v podjetju XY lahko obvladljiva, če se jih zaposleni zavedajo, jih zabeležijo ter opredelijo ukrepe, ki jih izvajajo in redno spremljajo.

LITERATURA IN VIRI

1. Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society, 35*(7), 659−675.
2. Armeanu, D., Vintila, G., Barbu, T., & Nedelescu, D. M. (2010). Using the value at risk (VaR) method to analyze and assess risk. *DAAAM International*, *21*(1), 289−290.
3. Banka Slovenije. (2002). *Operativno tveganje: definicija, regulacija in merjenje*. Ljubljana: Banka Slovenije.
4. Banka Slovenije. (2007a). *Sklep o izračunu kapitalske zahteve za operativno tveganje za banke in hranilnic.* Ljubljana: Banka Slovenije.
5. Banka Slovenije. (2007b). *Proces ocenjevanja tveganj*. Ljubljana: Banka Slovenije.
6. Bank for international Settlements. (2014a). *Review of the Principles for the Sound Management of Operational Risk.* Basel: Basel Committee on Banking Supervision.
7. Bank for international Settlements. (2014b). *Consultative document − Operational risk Revisions to the simpler approaches.* Basel: Basel Committee on Banking Supervision.
8. Banks, E., & Dunn, R. (2003). *Practical Risk management*. West Sussex: John Wiley & Sons.
9. Beasley, S. M., Clune, R., & Hermanson, R. D. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24*(6), 521−531.
10. Berk, A., Peterlin J., & Ribarič, P. (2005). *Obvladovanje tveganj: skrivnosti celovitega pristopa*. Ljubljana: GV založba.
11. Chambers, A. (2005). *Tolley's Internal Auditor's Handbook*. London: LexisNexis Butterworths.
12. Chorafas, N. D. (2002). Liabilities Liquidity and Cash Management Balacing Financial Risks. *Reputational and Operational Risk* (str. 59−75). New York: John Wiley & Sons.
13. Collier, M. P., Berry, J. A., & Burke, T. G. (2006). *Risk and management accounting: best practice guidelines for enterprise-wide internal control procedures*. London: The Chartered Institute of Management Accountants.
14. COSO - Committee of Sponsoring Organization. (2011). *Internal Control – Integrated Framework*. Durham: Committee of Sponsoring Organizations of the Treadway Commission.
15. Crouhi, M., Galai, D., & Mark, R. (2006). *The essentials of Risk management*. ZDA: The McGraw Hill.
16. Evropska komisija. (2016, november). *Delegirana uredba komisije EU.* Najdeno 16. decembra 2016 na spletnem naslovu https://ec.europa.eu/transparency/regdoc/rep/3/2016/SL/C-2016-7158-F1-SL-MAIN.PDF
17. Fernandez, L. A. (2007). Internal audit function role in operational risk management. *Journal of Financial Regulation and Compliance*, *15*(2), 143−155.
18. Financial Services Authority (2011). *Enhancing frameworks in the standardized approach to operational risk – guidance note.* Najdeno 15. decembra 2016 na spletnem naslovu http://www.fsa.gov.uk/library/policy/guidance/2011/gn11.shtml

19. Fraser, R. S. J., & Simkins, J. B. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizonts, 59*(6), 689−698.
20. Gea College. (2015). *Kako zmanjšati tveganja v podjetju in preprečiti najhujše?* Najdeno 28. oktobra 2016 na spletnem naslovu http://gea-college.si/kako-zmanjsati-tveganja-v-podjetju-in-prepreciti-najhujse/
21. Gordon, A. L., Loeb, P. M., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301−327.
22. Harmantzis. C, F. (2003, februar). Operational Risk Management in Financial Services and the New Basel Accord. *Social Science Research Network (SSRN).* Najdeno 28. oktobra 2016 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=579321
23. Heffernan, S. (2005). *Modern banking.* West Sussex: John Wiley & Sons.
24. IFAC - International Federation of Accountants. (2011). *Evaluating and Improving Internal Control in Organizations*. New York: International federation of Accountants.
25. Janakiraman, U. (2008, 4. julij). *Operational Risk Management in Indian banks in the context of Basel II: A survey of the state of preparedness and challenges in developing the framework.* Najdeno 28. oktobra 2016 na spletnem naslovu https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1536041
26. Jiang, W., Rupley, H. K., & Wu, J. (2010). Internal control deficiencies and the issuance of going concern opinions. *Elsevier, 22*(1), 40-46.
27. Jorion, P. (2003). *Financial Risk Management – Handbook* (2nd ed.). New Jersey: John Wiley & Sons.
28. Kaplan Schweser (2008). Book 4: Operational and integrated Risk management, legal. *Operational Risk Management* (str. 3-70). DF inštitut: Kaplan Schweser.
29. Koletnik, F. (2002). Novi okviri strokovnega ravnanja v notranji reviziji. *Zbornik referatov 5. letne konference notranjih revizorjev* (str. 69–85). Otočec: Slovenski inštitut za revizijo.
30. Kovač, J. (2013, 22. september). Strošek moralnega hazarda. *Časnik.* Najdeno 19. junija 2017 na spletnem naslovu http://www.casnik.si/index.php/2013/09/22/m-kovac-druzina-strosek-moralnega-hazarda/
31. Kuritzkes, A. (2002). Operational Risk Capital: A problem of Definition. *The Journal of Risk Finance, 4*(1), 47−56.
32. Lundqvist, A. S. (2015). Why firms implement risk governance – Stepping beyond traditional risk managament to enterprise risk management. *Journal of Accounting Public Policy, 34*(5), 441−466.
33. Mainelli, M. (2002). Industrial strengths: operational risk and banks. *Balance Sheet*, *10*(3), 25–34.
34. Ministrstvo za finance. (2004, november). *Usmeritve za notranje kontrole.* Najdeno 30. novembra 2016 na spletnem naslovu http://www.unp.gov.si/fileadmin/unp.gov.si/pageuploads/zakonske_podlage/predpisi_slo/usmeritve_notr_kontr.pdf

35. Muermann, A., & Oktem, U. (2002). The Near-Miss Management of Operational Risk. *The Journal of Risk Finance*, *4*(1), 25−36.
36. Paape, L., & Spekle, F. R. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review, 21*(3), 533−564.
37. Perner, V. (b.l.). *Notranje kontrole in storitve svetovanja*. Najdeno 8. novembra 2016 na spletni strani http://www.cpa-perner.si/vedez.html
38. Podjetje XY. (2011). *Account Matrix manual.* Slovenija: Podjetje XY.
39. Podjetje XY. (2012). *Testiranje v GRC modulu.* Slovenija: Podjetje XY.
40. Podjetje XY. (2013a). *Okvir upravljanja poslovnih procesov.* Slovenija: Podjetje XY.
41. Podjetje XY. (2013b). *Strategija organizacije sistema notranjih kontrol.* Slovenija: Podjetje XY.
42. Podjetje XY (2014). *Politika tveganja objekta.* Slovenija: Podjetje XY.
43. Podjetje XY. (2015a). *Priročnik o upravljanju z operativnim tveganjem.* Slovenija: Podjetje XY.
44. Podjetje XY. (2015b). *Letno poročilo 2015.* Slovenija: Podjetje XY.
45. Podjetje XY. (2016a). *Politika tveganja.* Slovenija: Podjetje XY.
46. Podjetje XY. (2016b). *Priročnik o kvalitativnem ocenjevanju operativnih tveganj.* Slovenija: Podjetje XY.
47. Prašnikar, J. (2012). *Predavanje Organizacija podjetja*. Ljubljana: Ekonomska fakulteta Ljubljana.
48. Rotovnik, T. (b.l.a). *Operativno tveganje in Basel II – pripravljenost bank v Sloveniji na zahteve novega kapitalskega sporazuma.* Najdeno 16. decembra 2016 na spletnem naslovu https://www.bsi.si/library/includes/datoteka.asp?DatotekaId=513
49. Rotovnik, T. (b.l.b). *Zavarovanje operativnega tveganja in Basel II − vidik bančnega regulatorja.* Najdeno 16. decembra 2016 na spletnem naslovu https://www.bsi.si/library/ includes/datoteka.asp?DatotekaId=513
50. Schroeck, G. (2002). *Risk Management and value creation in financial institutions.* New Jersey: John Wiley & Sons.
51. Sheen, A. (2005). Implementing the EU Capital Requirement Directive – key operational risk elements. *Journal of Financial Regulation and Compliance*, *13*(4), 313–323.
52. Torkar, G. (2005). Tveganje in mera tveganja. *Bančni vestnik, 5*(11), 34.
53. Vezjak, B. (b.l.). *Tveganja, letno poročilo in sodelovanje nadzornega sveta z revizorji.* Najdeno 10. decembra 2016 na spletni strani http://www.zdruzenje-ns.si/db/doc/upl/ vezjak___tveganja__letno_porocilo_in_sodelovanje_nadzornega_sveta_z_revizorji.pdf
54. Walker, M. S. (2001). *Operational Risk Management – Controlling, opportunities and threats*. Avstralija: Connley Walker Pty Ltd.
55. World Economic Forum. (2016). *The global Risk Report 2016* (11th ed.) Najdeno 29. novembra 2016 na spletnem naslovu http://www3.weforum.org/docs/Media/The GlobalRisksReport2016.pdf

56. Združenje bank Slovenije (2013). *Smernice upravljanja tveganj (UT). Priporočila Odbora za tveganja pri ZBS*. Najdeno 30. oktobra 2016 na spletnem naslovu http://www.zbs-giz.si/zdruzenje-bank.asp?StructureId=884

PRILOGE

KAZALO PRILOG

Priloga 1: Primer obrazca predloga mejnega zneska na ravni skupine 1
Priloga 2: Seznam kratic 2

Priloga 1: Primer obrazca predloga mejnega zneska na ravni skupine

Name of Entity:	**Podjetje XY**
Country:	**Slovenia**
Name of Local Internal Control System Officer, who proposes the Final Haircut of the Entity to the Group:	**Katica Sever**

YEAR of local Financial Statements: 2016

CURRENCY of local Financial Statements: EUR

A. Quantitative aspects to be considered for Haircut defining.

I. Position in Financial Statements	Local Currency	Amount in Local Currency	Amount in EUR
Total Assets	**EUR**	**€ 659.211.324**	**€ 659.211.324**
Total Equity	**EUR**	**€ 15.269.137**	**€ 15.269.137**
Total Revenues	**EUR**	**€58.012.293,85**	**€58.012.293,85**
Pre Tax Income	**EUR**	**€ -11.280.979,81**	**€ -11.280.979,81**

II. Financial Statements	Coverage of Financial Statements in %
Balance Sheet	**100 %**
Off Balance Sheet	**99,60%**
Profit and Loss	**41,29%**

III. Haircut Proposal	Haircut (%)	Haircut (amount in Local currency)	Haircut (amount in EUR Equiv.)
Haircut for Subsidiary	**40%**	**€ 451.657**	**€ 451.657**

B. Qualitative aspects to be considered for Haircut defining, if necessary.

I. Other significant aspects to be considered for Haircut	Explanation of reason
Significant aspects resulting from Management Board meetings, Internal Audit issues, Compliance issues, etc.	**Important accounts are considered as ICS relevant.**

II. Final Proposal of Haircut	Haircut (%)	Haircut (amount in Local currency)	Haircut (amount in EUR Equiv.)
Haircut for Subsidiary	**40%**	**€ 451.657**	**€ 451.657**

Proposed by:

LISCO of Entity _ Name:	Signature :	Date :
Employee 1		

Informed:

Head of Internal Audit	Signature :	Date :
Employee 2		

Informed:

Head of Accounting & Reporting:	Signature :	Date :
Employee 3		

Informed:

Head of Risk Controlling; LORO	Signature :	Date :
Employee 4		

Approved:

CRO:	Signature :	Date :
Employee 5		

Priloga 2: Seznam kratic

AMA	angl. *Advanced Measurement Approach;* napredni pristop izračuna kapitalske zahteve za operativna tveganja
ARIS	angl. *Architecture of integrated Information Systems*; aplikacija za modeliranje delovnih procesov
BCD	angl. *Business Control Diagram*; model za popis tveganj, kontrol in testov v programu
COSO	angl. *Committee of Sponsoring Organization;* celovit okvir notranjega kontroliranja
DORO	angl. *Decentralized operational risk officer*; decentralizirani sodelavec za upravljanje operativnega tveganja
EUR	evro – uradna denarna valuta držav Evropske unije, kratica EUR ali znak €.
GRC modul	angl. *Governance & Risk and Compliance*; modul za testiranje delovanja kontrol
KPI	angl. *Key Performance Indicator;* merljivi ukrepi, ki se uporabljajo za ocenjevanje uspešnosti podjetja
KRI	angl. *Key Risk Indicator;* ključni indikatorji za zaznavanje in merjenje tveganj
ORO	angl. *Operational risk officer*; sodelavec za upravljanje operativnega tveganja
TSA	angl. *Standardized Approach;* standardizirani pristop izračuna kapitalske zahteve za operativna tveganja
VaR	angl. *Value-at-risk*; mera tvegane vrednosti pri tržnem tveganju