UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

MAGISTRSKO DELO

MANAGEMENT POSLOVNIH PROCESOV KOT POMOČ PRI MANAGEMENTU OPERATIVNIH TVEGANJ: PRIMER BANČNEGA PROCESA

Ljubljana, julij 2013 MAJA URH

IZJAVA O AVTORSTVU

Spodaj podpisana Maja Urh, študentka Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtorica magistrskega dela z naslovom Management poslovnih procesov kot pomoč pri managementu operativnih tveganj: primer bančnega procesa, pripravljenega v sodelovanju s svetovalcem, doc. dr. Petrom Trkmanom.

Izrecno izjavljam, da v skladu z določili Zakona o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo 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 v magistrskem delu, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal(-a);
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku (Ur. l. RS, št. 55/2008 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predloženega magistrskega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne 28. 6. 2013 Podpis avtorice:_____

KAZALO

KAZALO SLIK

UVOD

Neprestane spremembe v poslovnem okolju, gospodarska kriza in povečevanje konkurence silijo podjetja k iskanju novih priložnosti. Ker razmere na trgu za uspešnost poslovanja ne dopuščajo več zgolj zniževanja stroškov, je ključna prilagodljivost spremembam, zaradi česar pa postaja vedno bolj pomemben notranji pogled na podjetje – procesi (Becker, Kugeler & Rosemann, 2003). Podjetja, ki imajo dober pregled nad procesi, le-te lažje prilagajajo in lahko proaktivno iščejo nove rešitve, s katerimi povečujejo učinkovitost, kakovost in zadovoljstvo kupcev (Willaert, van den Bergh, Willems & Deschoolmeester, 2007). V zadnjih treh desetletjih je tako prišlo do nekaj ključnih sprememb v poslovanju (Sangeetha & Mahalingam, 2011): vertikalni funkcijski pristop so nadomestili vodoravni procesi, informacije so lažje dostopne in se hitreje širijo, večji poudarek je na organizaciji in fleksibilnosti procesov, pojavlja se potreba po koordinaciji procesov med organizacijskimi enotami. Povečuje se pomen procesne usmerjenosti, kar pomeni postavitev poslovnih procesov v središče organizacije (Van der Hoeven, 2009, str. 3–5; McCormack et al., 2009). Bolje, kot so definirani poslovni procesi, bolj učinkovito lahko podjetje deluje, saj razumevanje podrobnosti procesov omogoča prepoznavanje tveganja, ozka grla in pomaga procese narediti učinkovitejše, poleg tega pa tudi zmanjša obremenitev zaposlenih ter izrabo virov (Jurič & Pant, 2008, str. 7). Z vsem tem se ukvarja management poslovnih procesov (v nadaljevanju MPP), ki je ob poudarjanju procesne usmerjenosti močno pridobil na pomenu.

Ker pa se procesi izvajajo v negotovem okolju, se ne moremo izogniti morebitnim dogodkom, ki bi lahko imeli negativen vpliv na poslovanje. To so tveganja, ki pa jih lahko prepoznamo in zmanjšamo verjetnost njihovega nastanka (Alhawari, Thabtah, Karadsheh & Hadi, 2008). S tem se ukvarja disciplina, ki je prav tako v zadnjih letih postala zelo pomembna – to je management tveganj. Ta ponuja priložnost za boljše poslovanje na podlagi pridobljenih informacij o tveganjih, preko katerih se lahko odgovorni v podjetjih lažje in bolje odločajo (Trkman & McCormack, 2009; Jolly, 2003). Tveganja, ki se nanašajo na notranje okolje podjetja, na procese in aktivnosti, v skladu z definicijo Baselskega odbora za nadzor bank imenujemo »operativna tveganja« (Cheng, Gamarnik, Jengte, Min & Ramachandran, 2005).

MPP skrbi za to, da je proces uspešno izveden, v skladu s strateškimi cilji in izpolnjuje zahteve deležnikov, pri čemer se upošteva učinkovitost, varnost, zanesljivost, funkcionalnost itn. Ker pa potencialna operativna tveganja lahko ogrozijo izvajanje procesa, se procesom posveča tudi management operativnih tveganj (v nadaljevanju MOT) (Tepina, 2010). Cilj MOT je, da se sooča s tveganji, ki so del vsakega procesa, in proces načrtuje tako, da bo v njem čim manj možnosti za realizacijo tveganj (Tafri, Rahman & Omar, 2011). Iz tega sledi, da so procesi skupna točka obema disciplinama. Vedno več avtorjev poudarja pomen povezovanja obeh disciplin (zur Muehlen & Rosemann, 2005). Dober primer pomena managementa procesov in operativnih tveganj najdemo v bančnem sektorju, ki ga je v zadnjih desetletjih zaznamovalo veliko sprememb. Ob hudi konkurenci znotraj sektorja in soočanjem s finančno krizo se banke še posebej trudijo najti nove pristope. Ob tem veliko poudarka dajejo obvladovanju tveganj, saj so ta v preteklosti povzročila milijardne izgube uglednim bankam (Tafri et al., 2011). MPP je v

bankah pomemben, saj je veriga vrednosti razdeljena v neodvisne organizacijske enote in je zato potrebna koordinacija medfunkcijskih procesov. Management informacij je osrednja aktivnost bančništva in je vpliv tehnoloških inovacij v procesu večji kot v drugih industrijah. Za koordinacijo velikega obsega informacij banke kritično potrebujejo zanesljivo informacijsko tehnologijo (v nadaljevanju IT) (Trkman, 2010, str. 127). Iz tega sledi, da sta v bančništvu za doseganje strateških ciljev pomembna tako MPP kot tudi MOT ter tudi ustrezna informacijska podpora, ki omogoča njuno integracijo. Banke potrebujejo dober pregled nad procesi, saj jim realizacija tveganj lahko prinese tako finančne kot tudi nefinančne posledice. Zato je ključno, da se izognejo čim več tveganjem ali pa z ukrepi obvladovanja tveganj in managementa procesov omilijo njihove posledice. V magistrskem delu bom predstavila primer, kako lahko MPP pomaga pri MOT.

Namen magistrskega dela je s pomočjo domače in predvsem tuje znanstvene ter strokovne literature proučiti, kakšne prednosti lahko podjetjem prineseta dober management poslovnih procesov in operativnih tveganj, ter obenem poudariti pomen povezovanja elementov obeh disciplin. Ker je slednje v literaturi relativno nova tematika, želim k področju raziskovanja povezovanja med obema disciplinama prispevati s predstavitvijo literature, prispevkom k modeliranju tveganj v procesih in predvsem s konkretnim primerom. Bančnim strokovnjakom s področij MPP in MOT želim prikazati uporabno vrednost tega pristopa, da bi se ga v prihodnosti bolj posluževali.

Cilj magistrskega dela je na podlagi analize strokovne literature najprej predstaviti različne načine povezovanja managementa poslovnih procesov in operativnih tveganj, nato pa na primeru procesa izvršb v banki ugotoviti, kako lahko z elementi MPP-informatizacijo, modeliranjem, analiziranjem procesov in prenovo vplivamo na operativna tveganja v procesu. Ker proces izvršb v proučevani banki prej še ni bil podrobno modeliran, je moj cilj, da ga modeliram bolj podrobno. V tej banki so bila do sedaj operativna tveganja vrednotena po oddelkih, moj cilj pa jih je opredeliti po procesih oz. aktivnostih s pomočjo analize škodnih dogodkov. Operativna tveganja bom vizualizirala v procesnem modelu z notacijo BPMN, v katero bom dodala simbol za operativna tveganja. Na koncu želim podati predloge ukrepov, s katerimi bi ugotovljena tveganja omejili oz. zmanjšali.

Magistrsko delo je razdeljeno na šest poglavij. Začnem s pregledom literature, predvsem tuje, s področja managementa poslovnih procesov, operativnih tveganj in povezovanja obeh. Najprej bom predstavila, kaj je poslovni proces, v čem je dodana vrednost, da se podjetja osredotočajo na procese, kako k uspešnosti pripomoreta management poslovnih procesov in znotraj tega modeliranje procesov. V tretjem poglavju bom opisala management tveganj s poudarkom na operativnih tveganjih, ki se pojavljajo v procesih. Nato bom na podlagi preteklih raziskav s tega področja opredelila, kako se MPP in MOT med seboj povezujeta in s tem podjetjem pomagata k doseganju strateških ciljev.

V praktičnem delu bom na podlagi pridobljenih teoretičnih znanj poskušala predlagati, kako bi lahko uporabili povezovanje MOT in MPP na konkretnem primeru. Izbrala sem bančni proces,

ki je za to dovolj kompleksen. Podatki, uporabljeni v analizi, so resnični, je pa naziv banke zaradi varovanja zaupnih podatkov skrit in bom zato skozi celotno magistrsko delo uporabljala kar izraz »Dobra banka«. Najbolj proučevan bančni proces v literaturi je sicer proces kreditiranja, jaz pa sem se odločila za manj proučevanega, in sicer za proces izvrševanja izvršb. Na primeru tega procesa bom uporabila kombinacijo elementov managementa operativnih tveganj (določitev kritičnih točk, opredelitev operativnih tveganj po aktivnostih, vizualizacija tveganj, predlogi za obvladovanje tveganj) in managementa poslovnih procesov (analiza procesov, modeliranje, informatizacija, prenova).

Najprej bom predstavila ozadje izvršb, nato pa kako proces izvrševanja sklepov o izvršbi poteka znotraj ene izmed slovenskih bank. V drugem delu sem celotni proces izvršb z notacijo BPMN modelirala »kot je« ter znotraj tega vizualizirala operativna tveganja. Na podlagi lastnih ugotovitev bom predstavila glavne kritične točke z vidika tveganj ter predlagala, s katerimi ukrepi oz. kontrolami lahko zmanjšamo ali omejimo možnost nastanka teh tveganj, kar bo lahko služilo kot usmeritev za nadaljnje spremljanje in prenovo procesa. Podrobnosti o procesu in tveganjih bom pridobila preko intervjujev zaposlenih in z analizo sekundarnih virov podatkov – navodil za delo, pravilnikov za izvajanje aktivnosti v teh organizacijskih enotah, poročil o škodnih dogodkih (od leta 2008 dalje) ter druge dokumentacije, povezane s procesom. Izpise škodnih dogodkov bom pridobila iz baze škodnih dogodkov, ki jo v banki redno ažurirajo.

1 POSLOVNI PROCES

V preteklosti so se podjetja osredotočala na učinkovito izvajanje posameznih poslovnih funkcij in optimizacijo le-teh. Razvoj moderne informacijske in komunikacijske tehnologije je omogočil pomembno povečanje produktivnosti in kvalitete v posameznih funkcijah (proizvodnja, računovodstvo, logistika itn.). Na žalost pa so stroški koordinacije med posameznimi področji narasli s povečanjem avtonomije le-teh. Uporaba tehnologije ni odpravila strukturnih problemov, ampak le ublažila simptome oz. skrajšala proces koordinacije. Zaradi povečanega števila interakcij med oddelki ni bilo več enostavno izvajati prodajnih aktivnosti na stroškovno učinkovit način. Zato se je v 80. letih pričelo preusmerjati poudarek iz optimiziranja funkcij na optimiziranje medfunkcijskih procesov in povečevanje pomena procesne organiziranosti (van der Hoeven, 2009, str. 1–9).

1.1 Od funkcijske k procesni usmerjenosti

Zniževanje stroškov za pridobitev konkurenčne prednosti ni več zadostovalo. V spremenljivem okolju je postala najpomembnejša notranja prilagodljivost podjetij, za katero so ključni predvsem ustrezno managirani procesi (Stalk, Evans & Schulman, 1992, str. 62). Michael Porter je predstavil verigo vrednosti, koncept, kjer aktivnosti (razdeljene na temeljne in pomožne) ustvarjajo dodano vrednost in kot celota postanejo najpomembnejše za podjetje. Porter je tako namesto poslovnih funkcij v ospredje postavil poslovni proces. Ta se prične z vložki, ki se preko procesa pretvorijo v izložke. Ideja je še pridobila na pomenu s pojavom pristopov prenove poslovnih procesov (angl. *Business Process Reengineering*) in

managementa poslovnih procesov (angl. *Business Process Management*) (Becker et al., 2003, str. 2).

Procesna usmerjenost je organizacijski koncept, ki pomeni postavitev poslovnih procesov v središče organizacije. Uskladitev poslovnih aktivnosti z željami kupcev je bistvena razlika v pogledu procesne usmerjenosti v primerjavi s pogledom z vidika poslovnih funkcij (van der Hoeven, 2009, str. 4–5). Procesna usmerjenost podjetja pomeni stopnjo, do katere podjetje posveča pozornost svojim ključnim procesom. Pri tem procese spremlja od začetka do konca (angl. *end-to-end*), preko meja področij, organizacij in celo držav. Ljudje v podjetju pa so tisti, ki razvijejo procesno usmerjeno miselnost (McCormack & Johnson, 2001). Procesno usmerjena podjetja vidijo poslovanje kot skupek procesov, uporabljajo strateške plane za usmerjanje procesov, razumejo povezavo med procesi in ključnimi poslovnimi cilji ter rezultati, se osredotočajo na ključne procese, ki morajo biti osredotočeni na kupce, uporabljajo delovne time za implementacijo in izvajanje procesov, izvajajo meritve procesov za ugotavljanje njihovega stanja, managirajo podatke, pridobljene iz procesov, zahtevajo neprestano izboljševanje procesov skozi celotno poslovanje, uporabljajo enostavne, avtomatizirane in standardizirane procese, kjer je to mogoče (Harmon, 2007, str. 180). Imajo torej dober pregled nad procesi, kar jim omogoča večjo prilagodljivost spremembam.

Glavni namen ključnih poslovnih procesov je, da dodajajo vrednost za kupca, iz česar sledi, da management procesov izboljšuje zadovoljstvo kupcev, medtem ko funkcijske organizacijske strukture s svojo rigidnostjo to ovirajo. Študija McCormacka in Johnsona (2001) dokazuje, da so podjetja, ki so bila bolj procesno usmerjena, tudi na splošno bolje poslovala. Razvoj procesne usmerjenosti naj bi namreč pozitivno vplival na uspešnost, zmanjšal medfunkcijske konflikte in povečal medpodročno povezanost, sodelovanje in integracijo, kar pa prispeva k dolgoročni uspešnosti.

Podjetja so na različnih stopnjah razvitosti procesne usmerjenosti. V začetni stopnji procese sestavljajo nizi »ad hoc« aktivnosti in niso definirani, zato je uspeh procesov odvisen od truda posameznikov. Podjetja na zreli stopnji pa imajo zgrajeno razumljivo procesno arhitekturo, ki prikazuje, kako so med seboj procesi prepleteni. Vzpostavljene imajo sisteme za merjenje uspešnosti procesov. Vsak proces ima dodeljenega lastnika procesa, ki nosi odgovornost, da proces poteka nemoteno, se stalno izboljšuje na podlagi meritev, s pomočjo vpeljave inovacij ter novih tehnologij. V procesih so kontrole, ki preprečujejo napake, in zaznavajo, kdaj procesi ne dosegajo ciljev (Harmon, 2007).

1.2 Definicija poslovnega procesa

Osnovni element pri načrtovanju procesno usmerjene organizacije je poslovni proces. Medtem ko organizacijska struktura podjetje deli na ločene enote, kot so področja, divizije, oddelki, ki opravljajo dodeljene naloge, je poslovni proces povezano izvajanje teh nalog. Proces je določen tako časovno kot tudi iz drugih vidikov: npr., kdo izvaja posamezne aktivnosti, s čim in katere so te aktivnosti. Proces je tako zaključeno, časovno in logično zaporedje aktivnosti, ki so pogoj, da iz procesa nastane točno določen rezultat. Te aktivnosti delajo na točno določenem

procesno-usmerjenem objektu (npr. račun, naročilo) in morajo biti v skladu s poslovni cilji. Primera poslovnega procesa sta izvrševanje naročila v proizvodnji, odobritev kredita v banki (Becker et al., 2003, str. 4).

Nekaj podobnih definicij o procesu podajo še drugi avtorji. Harmon (2007, str. 198) meni, da je proces povezan niz zaporednih aktivnosti, ki se sprožijo zaradi nekega dogodka oz. ki prejmejo in preoblikujejo enega ali več vložkov, da ustvarijo enega ali več izložkov. Določitev zaporedja aktivnosti in alokacijo virov na te aktivnosti, z namenom ustvariti določen rezultat s poslovno vrednostjo, imenujemo poslovni proces (Jurič & Pant, 2008, str. 56). Van der Hoeven (2009, str. 4–9) opredeli proces kot zaporedje med seboj odvisnih aktivnosti, ki se pričnejo s »sprožilcem« (angl. *trigger*) in končajo z izročitvijo enega ali več produktov, storitev kupcu. Ob tem produkt predstavlja vrednost za kupca, ki je lahko zunanji ali notranji (npr. zaposleni, oddelek). Poslovni proces je sestavljen iz točno določenih aktivnosti, ki skupaj izpolnijo določen poslovni cilj. Zaporedje teh aktivnosti in učinkovitost tistih, ki jih izvajajo, določata uspešnost celotnega poslovnega procesa. V interesu vsakega podjetja je, da ima učinkovite poslovne procese s čim manj aktivnostmi brez dodane vrednosti. Poslovni proces torej definira zaporedje dela in je direktno povezan z učinkovitostjo in uspešnostjo podjetij. Poznamo več vrst procesov.

1.3 Vrste procesov

Vrste procesov lahko opredelimo glede na več različnih kriterijev:
Glede na vlogo v verigi vrednosti (Harmon, 2007, str. 86):

- Temeljni procesi (angl. *core processes*). Ti procesi (po Porterju) proizvajajo produkte oz. jim dodajajo vrednost.
- Podporni procesi (angl. support *processes*). To so procesi, ki neposredno ne dodajajo vrednosti, ampak so nujni, da ključni procesi nemoteno funkcionirajo.
- Managerski procesi (angl. *management processes*) so bili sprva opredeljeni kot podporni procesi, danes pa so svoja skupina in jo sestavljajo planiranje, organiziranje, komuniciranje, nadzor in kontrolne aktivnosti organizacije.

Glede na izvajalca (Jurič & Pant, 2008, str. 106):

- Procesi, ki jih izvajajo ljudje (angl. *human-centric processes*). To so procesi, ki za večino aktivnosti potrebujejo delo človeka, da se proces premakne za stopnjo naprej. Takšen primer je razvoj novih storitev, sistemov, raziskovalno delo itn.
- Avtomatizirani procesi so močno podprti s tehnologijo in zahtevajo minimalni obseg človeškega posredovanja.

Glede na kompleksnost. Procesi so lahko enostavni ali ekstremno zapleteni (Harmon, 2007, str. 198; vom Brocke & Rosemann, 2010a, str. 73):

- Preprosti procesi so procesi, ki ponavadi sledijo doslednemu, dobro definiranemu zaporedju korakov, z jasnimi pravili. Vsak korak ali naloga je lahko natančno definirana, v procesu ni veliko izjem in je malo odločitvenih točk. V njih delajo običajni zaposleni (angl. *ordinary workers*), procesi so lahko avtomatizirani. Primeri takšnih procesov so proizvodna linija, maloprodaja, izposoja knjige.
- Kompleksni procesi so razvejani, vsebujejo polno izjem, temeljijo na veliko pravilih in so zato ponavadi tudi slabše definirani. Ti procesi zahtevajo več človeškega posredovanja. Zaposleni v procesih so delavci z znanjem (angl. *knowledge workers*), primer procesa pa je popravilo orodja, prodaja na terenu, planiranje. Več znanja, kot je potrebnega za opravljanje procesnih aktivnosti, kompleksnejši je proces.
- Zelo kompleksni procesi zahtevajo veliko človeške kreativnosti in jih težje avtomatiziramo oz. jih sploh ne moremo. Za tovrstne aktivnosti podjetja zaposlenih ne izobražujejo, ampak najamejo strokovnjake, ki imajo že zahtevana strokovna znanja (angl. *experts*). Izvajalci takšnih procesov se soočajo z visoko stopnjo negotovosti v procesih. Določene naloge so lahko zelo težavne in vnaprej težko predvidljive, procesi se precej spreminjajo ter razvijajo skozi čas. Modeliranje teh procesov je kompleksno in velikokrat pride do tega, da v času modeliranja, še preden pride model v uporabo, podatki postanejo zastareli (ter Hofstede, Mecella, Sardina & Marrella, 2012). Primer takšnega procesa je razvoj novih produktov, razvoj aplikacij, svetovanje.

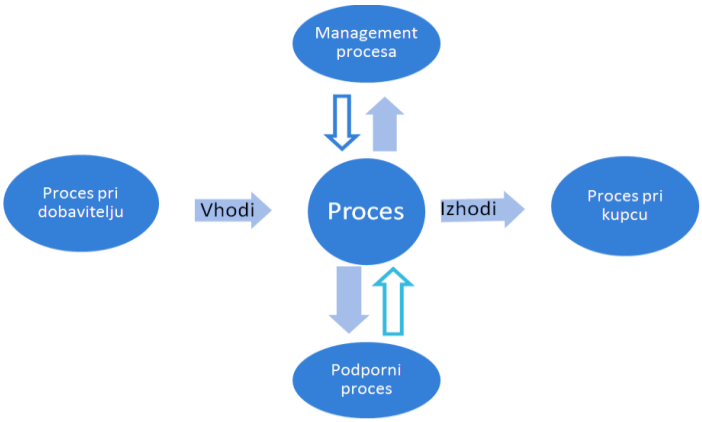
Glede na širino (Jurič & Pant, 2008, str. 107):

- Notranji oz. interni procesi potekajo znotraj podjetja (npr. obdelava naročila).
- Povezovalni (angl. *collaborative*) procesi. To so procesi, ki vključujejo povezovanje z zunanjimi deležniki (kupci, dobavitelji, partnerji itn). Takšen primer je npr., ko kupca vključimo v proces naročanja, kjer kupec sam izbere produkt in odda naročilo.

Glede na hierarhijo, raven. Procese lahko hierarhično organiziramo v ravni, pri tem pa moramo vedeti, ali bomo analizirali velik proces, kot je veriga vrednosti, srednje velik proces, kot je odobritev kredita, ali manjši proces, npr. vnos v kreditno aplikacijo. Poslovne procese, ki so procesi na višji ravni organizacije, lahko razdelimo v podprocese, nato pa še v nadaljnje podprocese. Tehnične omejitve, do kje lahko delimo procese, ni, največkrat pa so razdeljeni na 3 do 4 ravni. Na ravni podprocesov in aktivnosti postanejo vidni izvajalci (ljudje, informacijska podpora ali kombinacija obeh). Velikokrat za podprocese uporabljamo kar besedo »proces«, saj z vidika zaposlenega, ki opravlja podproces, le-ta predstavlja celoten proces (vom Brocke & Rosemann, 2010a, str. 87).

Različne vrste procesov se med seboj povezujejo. Na sliki 1 lahko vidimo, da izhodi enega procesa lahko predstavljajo vhod v drug proces (npr. v proces notranjega ali zunanjega kupca). Podporni procesi skrbijo, da izvajanje procesa poteka nemoteno. Da pa je proces uspešen,v skladu s strateškimi cilji, ter da so procesi med seboj usklajeni, skrbi management procesa.

Slika 1: Širši pogled na povezovanje procesov

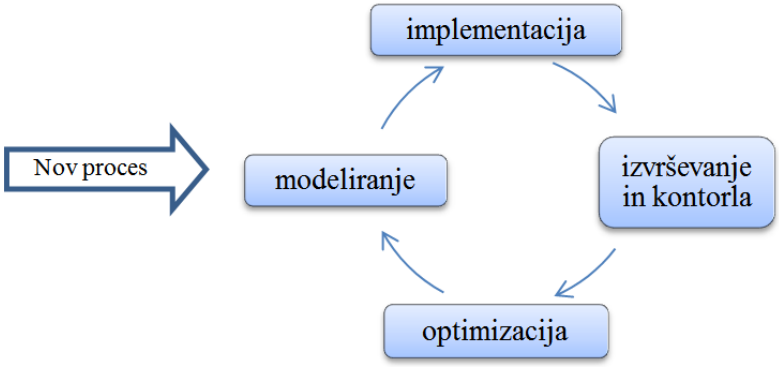


Vir: P. Harmon, Business Process Change, 2007, str. 115.

1.4 Življenjski cikel poslovnega procesa

Poslovni procesi so dinamični, kar lahko ponazorimo z življenjskim ciklom, ki vsebuje štiri faze, prikazane na sliki 2. V sklopu modeliranja procesa definiramo model procesa z uporabo izbrane metodologije in notacije. Implementacija procesa pomeni vpeljavo procesa, kot ga načrtujemo. Izvajanje in kontrola procesa se nanašata na dejanski potek procesa in kontrolo njegovega izvajanja, na podlagi česar sprejemamo določene korekcijske ukrepe. Zadnjo fazo pa predstavljata optimizacija in merjenje procesa, kjer zbiramo kvantitativne in ažurne podatke o izvajanju procesa ter jih interpretiramo za nadaljnjo optimizacijo (Jurič & Pant, 2008, str. 59).

Slika 2: Življenjski cikel poslovnega procesa



Vir: M. B. Jurič & K. Pant, Business Process Driven Soa Using Bpmn and Bpel, 2008, str. 59.

Da pa podjetja zagotovijo dolgoročno uspešnost procesov, morajo upoštevati pet kritičnih elementov oz. dejavnikov, ki jih izpostavita vom Brocke in Rosemann (2010a, str. 8–9):

- **Načrtovanje procesa**. To je zelo pomemben dejavnik, saj v tem delu nastane procesna specifikacija. V njej se definira, katere naloge morajo biti izvedene, kdo, kje in kako jih bo izvajal, s katerimi informacijami ter s kakšno stopnjo natančnosti. Brez tega je proces samo niz nekoordiniranih aktivnosti in organizacijski kaos.
- **Merjenje procesov**. Namesto meritev funkcijske uspešnosti podjetja potrebujejo merjenje procesov od začetka do konca, ki izhaja iz potreb kupcev in strateških ciljev. Zato morajo

biti le-ti vnaprej postavljeni, prav tako tudi uravnotežen niz kazalnikov (stroški, hitrost, kvaliteta).

- **Izvajalci procesov**. Ljudje, ki izvajajo procese, morajo imeti drugačne veščine in znanja kot zaposleni v običajnih funkcijskih organizacijskih enotah. Razumeti morajo potek celotnega procesa, procesne cilje, biti sposobni delovati v timih, saj le tako lahko opravijo delo v celoti.
- **Procesna infrastruktura**. Informacijska tehnologija mora biti prilagodljiva. V celoti mora podpirati procese ter biti podpora izvajalcem. Enako velja za kadrovske sisteme (izobraževanja, kariera, bonitete), ki morajo stremeti k napredovanju v znanju in učinkovitosti z vidika procesov.
- **Lastnik procesa**. V funkcijsko usmerjenih podjetjih ni nikogar, ki bi bil odgovoren za procese in bi vodil potek od začetka do konca (izpeljal cikel managementa procesa). Procesno usmerjena podjetja pa poskrbijo, da ima vsak proces dodeljenega lastnika.

Proces mora vsebovati vseh pet elementov, če želimo, da je uspešen. Dobro načrtovan proces, ciljno usmerjen in z dobrimi kazalniki ne more biti uspešen, če njegovi izvajalci nimajo potrebnih znanj ali če informacijski sistemi (v nadaljevanju IS) tega ne omogočajo. Vključitev vseh petih elementov je odvisna od vodenja podjetja, njegove kulture, nadzora in znanja. Podjetja, ki imajo dober pregled nad procesi, te lažje prilagajajo in tako lahko proaktivno iščejo nove možne rešitve problemov ter odpravo pomanjkljivosti v procesih. Vse te procesne vidike pa obvladujemo s pomočjo managementov poslovnih procesov (Willaert et al., 2007).

2 MANAGEMENT POSLOVNIH PROCESOV

Definicij managementa poslovnih procesov (angl. *BPM- Business Process Management*) najdemo več, so si pa med seboj podobne. *BPM Standard Group* (Business Performance Management Standards Group Formed, 2012) opiše MPP kot sistematičen niz analitičnih in managerskih procesov, ki jih podpira tehnologija. MPP sodeluje pri postavljanju strateških ciljev in se nato ukvarja z meritvami ter obvladovanjem procesov za doseganje teh ciljev in uresničevanjem strategije. Glavni MPP procesi vključujejo finančno in operativno planiranje, poročanje, analiziranje, modeliranje in spremljanje ključnih pokazateljev uspeha, povezanih s strategijo podjetja. Vom Brocke in Rosemann (2010a, str. 214) opredelita MPP kot integriran sistem za doseganje poslovne uspešnosti s pomočjo managiranja poslovnih procesov od začetka do konca (angl. *end-to-end*). MPP predstavita kot celosten, strukturiran, dosleden način dokumentiranja, modeliranja, analiziranja, simuliranja, izvajanja in neprestanega izboljševanja poslovnih procesov ter vpletenih virov z namenom prispevanja k poslovni uspešnosti. Osredotoča se na optimizacijo procesov in ne pomeni samo avtomatizacije ali reševanja poslovnih problemov. Ustvarja vrednost in konkurenčno prednost s pomočjo prilagajanja spremembam zahtev kupcev, trga in regulative hitreje od konkurence (vom Brocke & Rosemann, 2010b, str. 402).

Jurič in Pant (2008, str. 56) MPP obravnavata kot metodo, ki povezuje podjetje s potrebami njegovih kupcev, in s pomočjo inovativnosti, fleksibilnosti, integracije s tehnologijo pripomore

k poslovni učinkovitosti in uspešnosti. Kovačič in Bosilj Vukšić (2005, str. 15) pa definirata MPP kot sodoben sistem managementa sprememb pri prenavljanju poslovanja in poslovnih procesov, ki z ukrepi na področju organiziranosti, obvladovanja procesov in njihove informatizacije odpravlja nepovezanost med strateškim in operativnim managementom. MPP se je kot celovita disciplina sicer pojavil šele v zadnjih nekaj letih in se hitro ter neprestano razvija. Lahko trdimo, da gre za starejšo disciplino, sploh če upoštevamo še njegova predhodnika, to sta »celovito obvladovanje kakovosti« (angl. *Total Quality Management*) v 80. letih in »prenova poslovnih procesov« (angl. BPR- Business Process Reengineering) v zgodnjih 90. letih prejšnjega stoletja (vom Brocke & Rosemann, 2010b, str. 402).

Pri vpeljavi sprememb v podjetje so potrebna znanja z več različnih področij, zato so v MPP zajete različne discipline managementa, kar imenujemo celovito gledanje na MPP. Slednji vključuje management sprememb (angl. *Change management*), management informatike, projektni management, prav tako pa posega v odnose z deležniki, kupci, dobavitelji, zaposlenimi itn. Ko vpeljujemo ta celovit pristop, moramo upoštevati poslovno okolje podjetja, notranje okolje, strategijo, vrednote, kulturo podjetja, IT in se spopasti z notranjim upiranjem spremembam s strani zaposlenih (Willaert et al., 2007).

Na vprašanje, zakaj vpeljati management poslovnih procesov, Jurič in Pant (2008, str. 56, 226) odgovorita, da dober MPP lahko podjetju pomaga vzpostaviti visoko-učinkovite procese, ki pri izvajanju dosegajo nižje stroške, so hitrejši, natančnejši, bolj fleksibilni, potrebujejo manj virov in s pomočjo inovativnosti ter IT pripomorejo k poslovni učinkovitosti in uspešnosti. Z boljšo fleksibilnostjo omogočajo hitre spremembe in pridobivanje konkurenčne prednosti s povečanjem odzivnosti. Velikokrat pa podjetja ugotovijo, da so potrebne spremembe šele takrat, ko se to odraža v finančnem rezultatu, a je takrat že prepozno. Podjetja z dobrim MPP spremembe opazijo preko kazalnikov v procesih, izvajanja operativnih meritev in se tako lahko hitreje na njih odzovejo (vom Brocke & Rosemann, 2010a, str. 7).

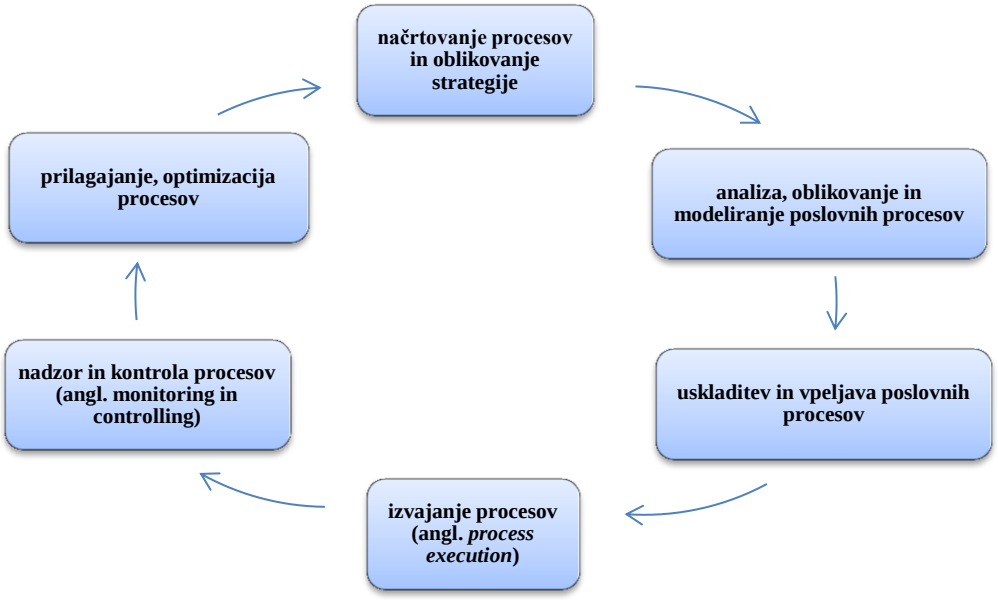
Ima pa MPP tudi nekaj slabosti, nanje opozarjajo različni avtorji. Poleg že prej predstavljenih pozitivnih učinkov uvedbe članki MPP opisujejo v smislu, kaj MPP pomeni, iz česa je sestavljen in kako se ga uporablja. Obenem pa ne podajajo dovolj jasnih smernic, kako MPP najbolje vpeljati v prakso. Poleg tega je še vedno razkorak med teoretično razlago in udejanjanjem v praksi, saj avtorji menijo, da je premalo povezovanj med teoretiki in praktiki (Škrinjar & Trkman, 2013). Raziskovanje MPP je še v začetni fazi, v izobraževalnih sistemih pa je premalo priložnosti za pridobitev znanja o tem področju. Posledično avtorji opozarjajo, da v praksi primanjkuje strokovnjakov, medtem ko se MPP hitro širi. Izziv pri izobraževanju je definirati meje tega področja, ki je zelo široko, ter slediti hitremu razvoju in trendom, saj gre za zelo dinamično disciplino (Delavari, Bandara, Marjanovic & Mathiesen, 2010).

2.1 Življenjski cikel MPP

Kot sem že prej omenila, je potrebno procese neprestano prilagajati. Ker pa se s tem ukvarja MPP, lahko življenjski cikel managementa procesov (angl. *BPM practice lifecycle*) predstavimo podobno kot življenjski cikel procesa – v sklenjenem krogu, s podobnimi fazami,

le da razširjeno za management vseh procesov v podjetju. Vom Brocke in Rosemann (2010b, str. 425) predstavita 6 glavnih faz v ciklu. Za načrtovanjem strategije sledijo analiza, oblikovanje in modeliranje procesov ter uskladitev in vpeljava le-teh. Izvajanje procesov se nadzira preko kontrol in meritev, rezultati pa služijo kot podlaga za prilagoditev, optimizacijo procesov. To vpliva na strategijo, prenovo modela, vpeljavo sprememb itn. Življenjski cikel prikazuje slika 3.

Slika 3: Življenjski cikel managementa poslovnih procesov



Vir: J. vom Brocke & M. Rosemann, Handbook on Business Process Management 2, 2010b, str. 425.

Merjenje procesov je namenjeno ugotavljanju, ali so procesi v podjetju usklajeni s strategijo in dosegajo cilje. V ta namen je potrebno vzpostaviti sistem merjenja procesov (angl. *Process Performance Measurement System)*, npr. BSC- sistem uravnoteženih kazalnikov. Dobro je, da se zaposlene oceni in nagradi na podlagi ključnih kazalnikov poslovanja (angl. *KPI- Key Performance Indicators*), v katerih se morata odražati notranja učinkovitost in zadovoljstvo kupcev. Na podlagi teh kazalnikov lahko management ugotovi pomembne informacije za prenovo in izboljšavo procesov. Ne zadostuje le vzpostavitev merilnega sistema, ampak je pomembna tudi vzpostavitev sistema kontrol, ki dolgoročno uravnovesijo cilje organizacijskih enot in osebnih ciljev zaposlenih s strategijo podjetja. Meritve so pomembne za fazo optimizacije, saj brez tega težko opazimo, kje v procesu se skrivajo pravi problemi (vom Brocke & Rosemann, 2010a, str. 5–10, 100).

Faza optimizacije je ena najpomembnejših faz, saj ima lahko veliko pozitivnih učinkov in ponuja priložnost za pridobitev konkurenčne prednosti. Z optimizacijo procesov lahko izboljšamo storitve, skrajšamo odzivne čase, dosežemo hitrejšo, učinkovitejšo proizvodnjo, se bolj prilagodimo kupcem, to pa se lahko obrestuje v povečani prodaji in zadovoljstvu kupcev. Večja učinkovitost in zmanjševanje stroškov sta neposredno povezani s krajšimi časi izvajanja procesov ter boljšo izrabo virov. Optimiziranje in avtomatizacija omogočata tudi lažje obvladovanje tveganj v procesih. Tveganja so namreč najbolj nezaželena, saj motijo ali celo

ustavijo potek procesa, ter za odpravo vzamejo kar nekaj časa in virov, za podjetja pa je pomembno, da z optimizacijo ne samo odpravijo ozka grla in napake, temveč tudi vključijo inovacije in nove pristope. Prav tako ne smejo dati prevelikega poudarka IT. Ni dovolj, da le informatizirajo proces od začetka do konca, saj to ne reši vseh problemov. Spreminjanje poslovnih procesov posega v delo zaposlenih, ki ponavadi ne marajo sprememb. Zato je spremembe potrebno implementirati previdno in ob tem motivirati zaposlene. Organizacija mora razviti poslovno okolje, v katerem bodo poslovni procesi neprestano optimizirani, kar pa je za podjetja precej težko, saj to stalno posega v delo zaposlenih in IT (Jurič & Pant, 2008, str. 96–100).

Potrebno je vedeti, da se pri vpeljavi in izvajanju MPP ter njegovih faz lahko srečamo s težavami. Modeliranje procesov na primer lahko vzame preveč časa in ni dovolj podrobno, zato modeli pogosto niso dovolj natančni, ne vsebujejo scenarijev v primeru izjem ali pa so zastarani. Optimizacija je lahko narejena v glavah analitikov in kljub temu da dobro izgleda v modelu, ni nujno, da bo funkcionirala tudi v realnem svetu. Trenutna programska oprema morda ne omogoča predlaganih sprememb. Predstavitev novega, optimiziranega procesa skupaj s prilagojeno programsko opremo, predstavlja veliko spremembo v operativnih postopkih. To pa lahko sproži odpor zaposlenih in posledično ogrozi funkcioniranje novega modela (Jurič & Pant, 2008, str. 21). Kot razlog za neuspeh projektov MPP Chakravorty (2010) navaja še problem motiviranosti zaposlenih. Projekti se večinoma začnejo dobro, z navdušenjem zaposlenih, in hitro napredujejo. Nato pa se napredovanje v projektih upočasni. Zaposleni izgubijo motivacijo in ob zasedenosti z drugimi projekti projekte počasi opuščajo. Ker lahko tako vse dotedanje delo gre v nič, je potrebna konstantna motiviranost. Da pa se podjetja izognejo neuspešnemu MPP, je potrebno vedeti, katere dejavnike morajo upoštevati pri vpeljavi.

2.2 Omogočevalci managementa poslovnih procesov

Šest temeljnih, t.i. »omogočevalcev« *(angl. enablers)*, ki so obenem kritični dejavniki uspeha MPP in jih morajo organizacije ob vpeljavi upoštevati, predstavita vom Brocke in Rosemann (2010a, str. 112–120):

- **Usklajenost s strategijo** (angl. *strategy alignment*). MPP mora biti usklajen s strategijo podjetja, in sicer tako, da so procesi načrtovani, izvedeni, managirani in merjeni v skladu s strateškimi prioritetami. Ugotovljene prednosti procesov pa obenem lahko spodbudijo nadaljnje strateško načrtovanje v smeri procesno-usmerjenosti. Povezava med strategijo in poslovnim procesom mora biti torej vzajemna.
- **Obvladovanje procesov** (angl. *governance*) je namenjeno zagotovitvi skladnosti procesov s strategijo in doseganju uspešnosti. Vključuje primerno in transparentno dodeljevanje vlog ter odgovornosti za različne ravni MPP (lastnik procesa, analitik v procesu). Skrbi za kontrole v procesu (angl. *process management controls*), ohranjanje kakovosti in skladnosti procesov z regulativo (angl. *compliance*), vzpostavitev pravil in delno tudi za obvladovanje tveganj.

- **Metode** (angl. *methods*). Gre za uporabo primernih orodij in tehnik, ki podpirajo in omogočajo MPP aktivnosti. Pri načrtovanju in modeliranju procesov uporabljamo metode za analizo procesov ter tehnike modeliranja za prepoznavanje trenutnega stanja poslovnih procesov (angl. *As-Is*) in načrtovanje novih (angl. *To-Be*) procesov. Pri kontroli procesov in merjenju uporabljamo metode za zbiranje ter analizo podatkov pri izvajanju procesov. Ti podatki so lahko vezani na procesne kontrole (podatki o tveganjih) ali pa so splošne meritve procesa (čas, stroški, kakovost).
- **Informacijska tehnologija**. V to kategorijo spadata programska in strojna oprema, ter informacijski sistemi, ki omogočajo in podpirajo procesne aktivnosti. Tako, kot se med seboj razlikujejo metode, se tudi to področje razlikuje glede na faze MPP. Poznamo informacijske rešitve za podporo načrtovanju in modeliranju procesov, sisteme za management delovnih procesov (pri implementaciji in izvajanju procesov) ter sisteme za merjenje oz. spremljanje uspešnosti procesov in ugotavljanje napak.
- **Ljudje**. Za uspeh MPP so ključni ljudje, ki izvajajo, nadzirajo ali managirajo proces. Ključna so njihova znanja o procesu, managementu procesov, njihovo neprestano izobraževanje, motiviranje, sodelovanje v procesu in dodeljevanje odgovornosti.
- **Kultura**. Gre za vrednote in prepričanja podjetja, ki mora biti procesno usmerjeno in naklonjeno MPP. Velikokrat je razlog za neuspeh projektov MPP prav v neprimerni organizacijski kulturi, ki ni dovzetna za procesne spremembe. Uspešnost je odvisna od mišljenja, zaznavanja in naklonjenosti zaposlenih do želenih sprememb. Če bodo spremembe zaznavali kot nekaj pozitivnega, bodo svoje delo opravljali v podporo projektu, sicer je nevarnost, da bodo projekt ovirali. Zato Škerlavaj, Indihar Štemberger, Škrinjar in Dimovski (2007) menijo, da mora biti organizacijska kultura takšna, da omogoča učenje, kreativnost in inovacije.

2.3 Informatizacija poslovnih procesov

Pomemben element MPP je informacijska tehnologija, ki jo uporabljamo za avtomatizacijo, informatizacijo posameznih aktivnosti ali celotnih procesov, za različne faze MPP (modeliranje, merjenje itn.), za podporo prenovi proizvodov in poslovnih procesov. S pomočjo IT zmanjšujemo obremenjenost zaposlenih in zagotavljamo učinkovitejše izvajanje aktivnosti v primerjavi z ročnim izvajanjem. Kovačič in Bosilj Vukšić (2005, str. 239–242) menita, da uporaba lahko pozitivno vpliva na učinkovitost, prilagodljivost poslovanja, kakovost izvajanja poslovnih procesov in preglednost le-teh. Obenem pa opozarjata, da naložbe v IT neposredno ne vplivajo na dvig konkurenčnosti in poslovne uspešnosti organizacij. Podjetja, ki ne managirajo svojih procesov, so manj učinkovita od tistih, ki jih. Vom Brocke in Rosemann (2010a, str. 127–8) predstavita ugotovitve raziskave, in sicer, da so podjetja, ki so aktivno managirala svoje poslovne procese, a imela nizko raven IT, dosegla 8 % donosnost naložb (ROI). Ta podatek opozarja na dejstvo, da že samo management procesov privede do višjega ROI. Podjetja, ki pa so aktivno managirala procese in imela med drugim še visoko stopnjo tehnološke podpore, pa so dosegla kar 20 % donosnost. Iz tega lahko sledi, da so podjetja, ki dajejo večji poudarek na MPP in znotraj tega informatizaciji, uspešnejša.

V začetku so aplikacije pokrivale samo določene aktivnosti, dele procesov, kmalu pa so ugotovili da to ni vse, kar IT lahko zagotovi. Tako so se pojavili sistemi, ki so pokrivali širša področja poslovanja, npr. ERP sistemi (celovite informacijske rešitve), sistemi za management odnosov s strankami (angl. CRM- *Customer Relationship Management*) in podobni sistemi. Preko vpeljave teh sistemov so organizacije ugotovile, da je končni cilj informatizacija celotnih poslovnih procesov oz. razvoj aplikacij, ki bi zagotovile informacijsko podporo aktivnostim v procesu od začetka do konca (Jurič & Pant, 2008, str. 5, 13). IT je pridobila na pomenu sočasno z razvojem MPP in je danes obenem tudi glavni element, ki omogoča razvoj MPP (vom Brocke in Rosemann, 2010a, str. 383).

Willaert et al. (2007) ugotavljajo, da danes vedno več IT ponudnikov na trgu zagotavlja orodja, ki tako ali drugače podpirajo MPP. Nekatera orodja vsebujejo funkciji modeliranja in simuliranja, ki sta v pomoč pri dokumentiranju procesov, druga vsebujejo funkcije, ki omogočajo tudi merjenje procesov. Informacijske rešitve, ki podpirajo celotne procese, imenujemo PAIS sistemi (angl. *Process-aware Information Systems*). Glavni niz načel in zmožnosti PAIS vsebujejo sistemi za krmiljenje delovnih procesov (angl. *Workflow management systems,* v nadaljevanju WFMS), ki se posvečajo načrtovanju, izvajanju in kontroli vsaj pol-avtomatiziranih poslovnih procesov. Primeri PAIS pa so še ERP sistemi, help-desk sistemi, sistemi za management podatkov itn. (vom Brocke & Rosemann, 2010a, str. 313–314, 383).

Orodja za analizo poslovnih procesov, ki jih imenujemo tudi BPA orodja (angl. *Business Process Analysis tools*), omogočajo dokumentiranje organizacijskih delovnih nalog ter zagotavljajo podporo poslovnim zahtevam za izboljšavo, prenovo ali avtomatizacijo procesov. Ta orodja omogočajo dokumentiranje, oblikovanje in simulacijo poslovnih procesov. Celoviti sistemi BPMS (angl. *Business Process Management Suites*) pa so namenjeni več kot samo analizi in modeliranju procesov, in sicer vpeljavi in nadzoru procesov v realnem času (vom Brocke & Rosemann, 2010a, str. 342–343).

Sistemi za management delovnih procesov (angl. Workflow Management Systems- WFMS) so vrsta programske opreme, ki podpira delovne procese. Delovni proces je sestavni del poslovnega procesa in predstavlja vmesni člen med poslovnimi procesi ter programskimi rešitvami, ki podpirajo njihovo izvajanje. Sistem vsebuje vse potrebne informacije za izvršitev procesa (pogoji, pravila, sestavne aktivnosti, izvajalci). WFMS se ukvarjajo z logistiko informacij v procesu oz. zagotavljajo, da prava informacija doseže pravo osebo ob pravem času s pomočjo avtomatizacije (Kovačič & Bosilj Vukšić, 2005, str. 321–323).

Aplikacij in sistemov je torej pri MPP precej na izbiro, je pa potrebno vedeti, da ima vsako podjetje edinstvene procese. Aplikacije morajo biti zato prilagojene procesom in ne obratno. Jurič in Pant (2008, str. 5, 13) še dodajata, da se poslovni procesi spreminjajo, kar vpliva tudi na informacijsko podporo. Slednja mora biti zato zelo fleksibilna, da jo lahko hitro in učinkovito prilagajamo. Čas za prilagoditve aplikacij ter odpravljanje napak sta namreč z vidika poslovanja organizacij izgubljeni čas.

2.4 Modeliranje poslovnih procesov

Modeli poslovnih procesov omogočajo transparenten pregled nad aktivnostmi procesa in drugimi procesnimi elementi. Uporabljamo jih, da ustvarimo jasno sliko o procesni logiki in zaporedju aktivnosti, za opis vhodov in izhodov iz procesov, zahtevanih virov, podatkov ter vključenih organizacijskih enot (vom Brocke in Rosemann 2010a, str. 187). Modeliranje pa Kovačič in Bosilj Vukšić (2005, str. 177) definirata kot snovanje, izdelavo in uporabo teh modelov, ki služijo za pridobivanje spoznanj, širjenje znanja, preizkušanje brez tveganja za izvirnik in omogočajo lažje razumevanje problema. Pregled nad poslovnim procesom ustvarimo z izhodiščnim modeliranjem, modelom »kot je« (angl. *As-Is*), ki nam služi za nadaljnjo analizo in izboljšavo procesa. Prikaže nam grafično sliko realnega stanja, kar nam omogoča lažje razumevanje. Iz tega pa na podlagi izboljšav izpeljemo prenovljeni model »kot bo« (angl. *To-Be*) (Willaert et al., 2007).

2.4.1 Različni nameni modeliranja

Poslovne procese sicer modeliramo z različnimi nameni: za namene preučevanja, izvajanja, za osnovo prenovi ali optimiziranju procesov, vpeljavi avtomatiziranih sistemov, ureditvi dokumentacije v zvezi z organizacijskim delom itn. Procesni modeli nam lahko služijo za hitrejše odkrivanje procesnih pomanjkljivosti, boljše razumevanje in preglednost, celotni pogled na proces, deljenje znanja ali vizije, natančna navodila zaposlenim za izvrševanje poslovnih aktivnosti itn. (vom Brocke in Rosemann 2010a, str. 149–150, 340). Jurič in Pant (2008, str. 62, 63) v splošnem ugotavljata, da procese modeliramo z namenom, da:

- razumemo aktivnosti v procesu, vemo točno, katere naloge morajo biti dokončane, kdo je za njih odgovoren, kakšen je izložek iz procesa in kakšno poslovno vrednost ima;
- razumemo zaporedje aktivnosti, ki lahko potekajo vzporedno ali zaporedno. To nam lahko pomaga pri skrajšanju časa izvajanja procesa. Modele pa uporabljamo tudi za zaposlene, in sicer kot navodila za delo, da lažje razumejo proces in učinkoviteje opravijo svoje naloge;
- razumemo izrabo virov, uporabljenih v procesu, kar nam lahko pomaga izboljšati izkoriščenost virov in da razumemo povezavo ter komunikacijo med ljudmi v procesu, kar nam pomaga pri optimizaciji komuniciranja;
- razumemo tokove dokumentov, ki so lahko v fizični ali elektronski obliki, da vemo, od kod pridejo in kam gredo, ter tako ugotovimo, ali so sploh potrebni;
- identificiramo potencialna ozka grla in točke, kjer so možnosti za izboljšavo, kar nam prav pride v fazi optimizacije;
- ustvarimo podlago za razvoj informacijske podpore.

V skladu z različnimi nameni in drugimi dejavniki pa se razlikujejo tudi končni procesni modeli (ali gre za podrobno analizo za prenovo procesa ali zgolj za ureditev dokumentacije). Razlikujejo se glede na pogled uporabnika in analitika (administrativno-usmerjen, usmerjen v kupce), glede na vlogo tistega, ki proces modelira (lastnik procesa, izvajalec procesa, zunanji analitik), glede na zahteve modela (nizki stroški, polna izraba virov, minimalna stopnja napak)

in glede na kompleksnost oz. obseg abstrakcije (večje ali manjše število elementov v procesu) (vom Brocke in Rosemann 2010a, str. 302–303).

2.4.2 Potek modeliranja, problemi in načela

Ko pričnemo z modeliranjem procesov, moramo najprej določiti zadolžitve, saj pri projektu sodelujejo različni ljudje, z različnih oddelkov in podjetij. Ti morajo biti pripravljeni posvetiti projektu dovolj časa, za kar pa je ključna podpora vrhnjega managementa. Imeti morajo tudi točno določena znanja. Da poslovni analitik lahko pridobljene informacije pretvori v uporabne modele, mora imeti znanje o modeliranju in tehniki, ki jo uporablja, podrobno pa mora poznati proces in poslovno področje, ki ga analizira. V prvem koraku modeliranja najprej naredimo posnetek stanja. Na osnovi tega izdelamo izhodiščni model »kot-je«, ki prikazuje dejansko stanje procesa. Za pripravo tega modela je potrebno zbrati informacije, znanje o procesu. V ta namen z zaposlenimi izvedemo intervjuje in proučimo zbrano procesno dokumentacijo (Jurič & Pant, 2008, str. 62, 69, 86). Pri tem se moramo vprašati, kakšni so vhodi in izhodi procesa, katere so aktivnosti znotraj procesa, kakšno je njihovo zaporedje, kdo jih izvaja, ter kateri dokumenti se izmenjujejo tekom procesa. Ko odgovorimo na vprašanja, dobimo dober vpogled v to, kako proces poteka. Lahko definiramo tudi strukturne, organizacijske, tehnološke točke slabosti, ozka grla, ter ugotovimo možne izboljšave procesa (Kovačič & Bosilj Vukšić, 2005, str. 182). Iz tega izpeljemo optimizirane, prenovljene modele »kot-bo«.

Med modeliranjem pa lahko naletimo na različne probleme. Eden od njih je čas zaposlenih. Ti so ponavadi polno zasedeni, delajo na več procesih in projektih hkrati. To ovira delo tistih, ki procese analizirajo, saj si zaposleni za to ne vzamejo časa. Problem je lahko tudi njihova subjektivnost in bojazen, da bodo o svojem delu razkrili kaj preveč. Jurič in Pant (2008, str. 18) dodajata, da je modeliranje lahko precej dolgotrajno in so zato lahko, preden zaključimo projekt, nekatere specifikacije že zastarele. Velik problem pri modeliranju je tudi kompleksnost. Velikokrat analitiki posnamejo vsako izjemo, kar privede do kompleksnih modelov. Ob tem preveč podrobni elementi v procesu zakrijejo glavno procesno logiko. Da zadovoljimo različne zahteve, modeliramo v različnih nivojih podrobnosti z različno potrebno stopnjo abstrakcije (vom Brocke & Rosemann 2010a, str. 149–150). Abstrakcija je generalizacija, ki zmanjša število nezaželenih podrobnosti z namenom preglednosti in ohranjanja samo uporabnih informacij za tistega, ki mu je model namenjen. Na najvišji ravni abstrakcije pokažemo samo najpomembnejše aktivnosti (do 10). Vsaka od teh aktivnosti pa je potem naprej razčlenjena v podrobnejše tokove (Jurič & Pant, 2008, str. 69).

Da se izognemo problemom, moramo upoštevati nekaj osnovnih načel. Model mora biti semantično pravilen, kar pomeni, da smo vključili vse relevantne aktivnosti, točke odločitev, dogodke, dokumente in druge pomembne elemente. Ob tem Mendling, Reijers in van der Aalst (2010) poudarjajo, da mora biti teh elementov čim manj. Če ima model več kot 50 elementov, ga je potrebno razdeliti v več modelov. Večji, kot je model, težje je razumljiv in ima zato večjo verjetnost za napake. Za preglednost je dobro tudi, da ima model samo en začetek in konec. V model moramo vključiti samo procese, ki so za naš namen modeliranja relevantni. Procesi so namreč med seboj povezani, kar nas lahko velikokrat zavede, z nepotrebnim modeliranjem pa

izgubljamo čas. Paziti moramo, da stroški modeliranja ne presegajo koristi, ki jih bodo modeli prinesli. Modeli morajo biti uporabni, razumljivi. Ker so poslovni procesi kompleksni, jih moramo razčleniti v več različnih nivojev. Narediti moramo procesno shemo (angl. *pocess map*), ki je model na najvišji ravni in so v njem navedeni vsi procesi ter povezave med njimi (Jurič & Pant, 2008, str. 84–86). Modeliranje poslovnih procesov mora biti usklajeno s poslovno strategijo in cilji organizacije, sicer ni smiselno, da izgubljamo vire in čas na tem projektu.

2.4.3 Tehnike modeliranja procesov

Pri modeliranju poslovnih procesov imamo na izbiro veliko število različnih tehnik, ki se med seboj razlikujejo po kompleksnosti, uporabnosti, preglednosti. Po zmožnostih, ceni in prijaznosti do uporabnikov pa se razlikujejo tudi orodja, ki te tehnike omogočajo (Kovačič & Bosilj Vukšić, 2005, str. 185). Tehnike in orodja modeliranja se neprestano spreminjajo, zato se morajo tisti, ki modelirajo, temu stalno prilagajati. Nekatera orodja omogočajo zgolj grafično modeliranje, druga pa imajo tudi možnost simulacij modelov. Izbor orodja in tehnike moramo prilagoditi našemu namenu modeliranja, ravni abstrakcije in končnim uporabnikom, ki jim mora biti model razumljiv.

Vsem tehnikam pa je skupno, da vsebujejo nabor grafičnih simbolov in napredne vizualizacijske tehnike, s katerimi olajšajo razumevanje razmerij med različnimi procesnimi elementi. Simboli ponazarjajo koncepte poslovnega sistema, kot so poslovna aktivnost, začetek, konec procesa, dogodek, organizacijske enote, viri, dokumenti, sistemi, ki podpirajo proces/aktivnost, razvejišča in puščice, ki ponazarjajo potek izvajanja procesa oz. zaporedje aktivnosti. S pravimi orodji modele lahko obogatimo tako, da jim dodamo informacije o problemih, tveganjih, priložnostih, jih povežemo z drugimi modeli, kot na primer podatkovnimi modeli, organizacijsko strukturo (vom Brocke & Rosemann 2010a, str. 299, 340–342).

Tehnika procesnih diagramov poteka (angl. *flow chart)* je ena izmed predstavnikov prve generacije tehnik. Nato so se pojavile bolj sofisticirane in dodelane tehnike, kot so diagrami toka podatkov, petrijeve mreže, eEPC (angl. *extended Event Process Chain*), IDEF3, UML diagrami itn. Nekaj let nazaj je bila posebej za modeliranje poslovnih procesov razvita notacija, imenovana BPMN (angl. *Business Process Modeling Notation*, v nadaljevanju BPMN) (Jurič & Pant, 2008, str. 66). To tehniko bom uporabila tudi v praktičnem delu magistrske naloge.

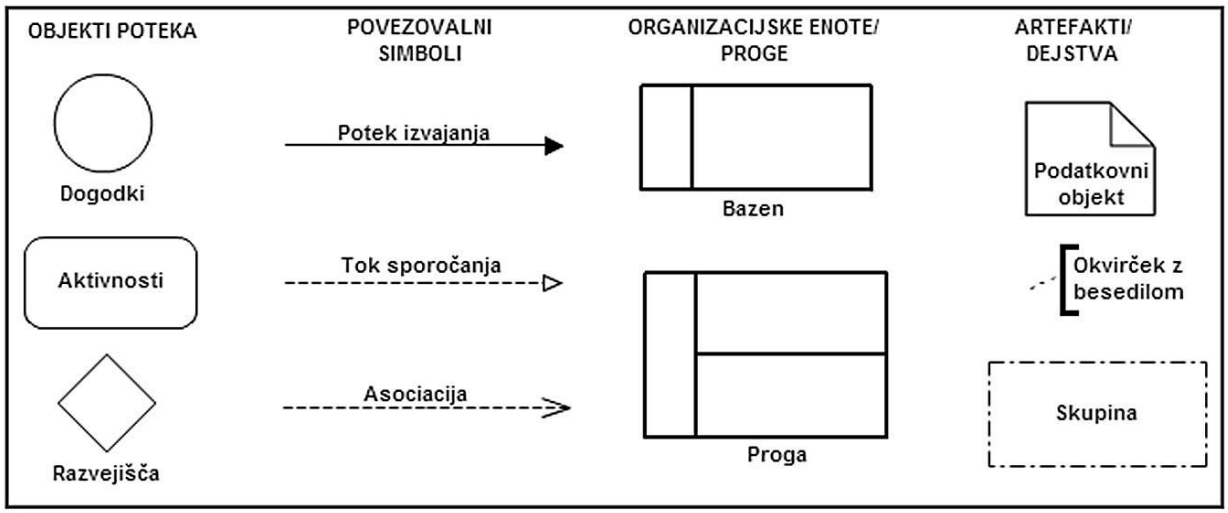
BPMN uporabljamo za risanje diagramov poslovnih procesov (angl. *Business process diagram*), ki predstavljajo aktivnosti v procesu in njihova razmerja. Tehnika uporablja koncept diagramov poteka (angl. *flow chart*), s katerim predstavlja procesno logiko. Gre za vizualni jezik, ki uporablja niz grafičnih elementov različnih geometrijskih oblik (Jurič & Pant 2008, str. 34). Harmon (2007, str. 513) pojasni, da je BPMN grafična notacija, ki se danes uporablja kot najbolj razširjen oz. »*de facto*« standard za modeliranje poslovnih procesov, medtem ko tehnika EPC izgublja na svojem pomenu. BPMN je razvila organizacija BPMI (angl. *Business Process Management Initiative),* danes pod okriljem OMG (angl. *Object Management Group*).

BPMN je bil ustvarjen z namenom vzpostavitve mostu med notacijami in jeziki za zapis poslovnih procesov. Modele se lahko namreč direktno aktivira oz. transformira v izvršljiv jezik BPEL (vom Brocke & Rosemann 2010a, str. 217).

BPMN je poslovno usmerjena tehnika modeliranja procesov, ki omogoča standardizacijo modeliranja in je pomembna tudi za razvoj MPP, saj zagotavlja skupen jezik za svetovalce, poslovne analitike, IT razvijalce, tehnologe (Business Performance Management Standards Group Formed, 2012). Prav zato ker so v modeliranje vključeni različni ljudje – od uporabnikov, analitikov, lastnikov procesov do razvijalcev in managerjev, je bil namen razviti grafično notacijo, ki bi bila razumljiva vsem. Ob tem pa je tudi dovolj zmogljiva, da omogoči modeliranje procesa na želeni stopnji podrobnosti. Drug namen pa je bil, kot sem že omenila, zagotoviti avtomatsko transformacijo v izvršljivo kodo in obratno (BPEL ali BPML). BPML in BPEL sta podobna jezika, nastala iz potrebe po standardiziranemu zapisu poslovnih procesov, za vzpostavitev komunikacije med aplikacijami in procesi. Razkorak med modelom poslovnih procesov in IT je bil vedno velik, zato je bila ta notacija oblikovana posebej za omogočanje takšnih transformacij (Jurič & Pant, 2008, str. 66).

Simboli BPMN (vom Brocke & Rosemann, 2010a, str. 216-217; Jurič & Pant, 2008, str. 109; Harmon, 2007, str. 514; Kovačič, 2008, str. 12-15) so združeni v štiri osnovne kategorije elementov (kot je prikazano na sliki 4): objekti poteka (angl. *flow objects*), povezovalni simboli (angl. *connecting objects*), organizacijske enote oz. proge (angl. *swimmlanes*) in artefakti oz. dejstva (angl. *artifacts*). Znotraj kategorij je notacija razdeljena v osnovni in razširjen niz elementov. Osnovni elementi so preprosti in razumljivi, zato se priporoča, da se modele, namenjene za širšo uporabo, modelira prav s tem nizom elementov.

Slika 4: Osnovni simboli notacije BPMN



Vir: M. B. Jurič & K. Pant, Business Process Driven Soa Using Bpmn and Bpel, 2008, str. 109.

Objekti poteka so dogodki (angl. *events*), aktivnosti (angl. *activities*) in razvejišča (angl. *gateways*). Dogodki so lahko začetek, konec, vmesni dogodki ali čakanje znotraj procesa. Aktivnosti so razdeljene na procese, podprocese, naloge in ponazarjajo opravljeno delo.

Razvejišča pa pomenijo razdelitev procesa na več različnih vej ali združitev teh vej, ki so lahko izključujoče (odločitev) ali sočasne.

Povezovalni simboli so namenjeni povezovanju elementov. Potek izvajanja (angl. *sequence flow*) definira zaporedje izvajanja aktivnosti znotraj procesa, medtem ko tok sporočanja (angl. *message flow*) ponazarja potek komuniciranja med poslovnimi entitetami, vloge pripravljanja ter prejemanja sporočil. Asociacija (angl. *association*) povezuje artefakte (npr. besedilo) z objekti poteka in povezovalnimi simboli.

Organizacijske enote oz. proge uporabljamo za organiziranje aktivnosti v vidne kategorije, s katerimi ponazorimo različne funkcije, odgovornosti, oddelke, udeležence. V to kategorijo spadajo bazeni (angl. *pools*), ki jih lahko naprej razdelimo v proge (angl. *lanes*). Bazeni ponavadi predstavljajo različne organizacije, ki sodelujejo v procesu, medtem ko s progami ponazorimo organizacijske enote znotraj njih. Lahko pa bazene uporabimo za organizacijske enote, ki jih nadalje razdelimo na različne odgovornosti oz. vloge znotraj njih.

Artefakte oz. opisne objekte uporabljamo za podajanje dodatnih informacij o poslovnem procesu, za boljšo razumljivost. Ti elementi so podatkovni objekti (angl. *data objects*), okvirčki z besedilom (angl. *text annotation*) in skupine (angl. *group*). Podatkovni objekti dajejo informacije o zahtevanih podatkovnih virih/produktih za posamezno aktivnost. Analitiki s tem zabeležijo uporabo oz. nastanek določenih podatkovnih elementov, npr. dokumentov, obrazcev, informacijskih virov. Skupina je vizualni pripomoček, s katerim za lažje razumevanje grupiramo določen niz elementov ali poudarimo določen del procesa. Z okvirčkom za besedilo pa dodajamo informacije za lažje razumevanje.

3 MANAGEMENT TVEGANJ

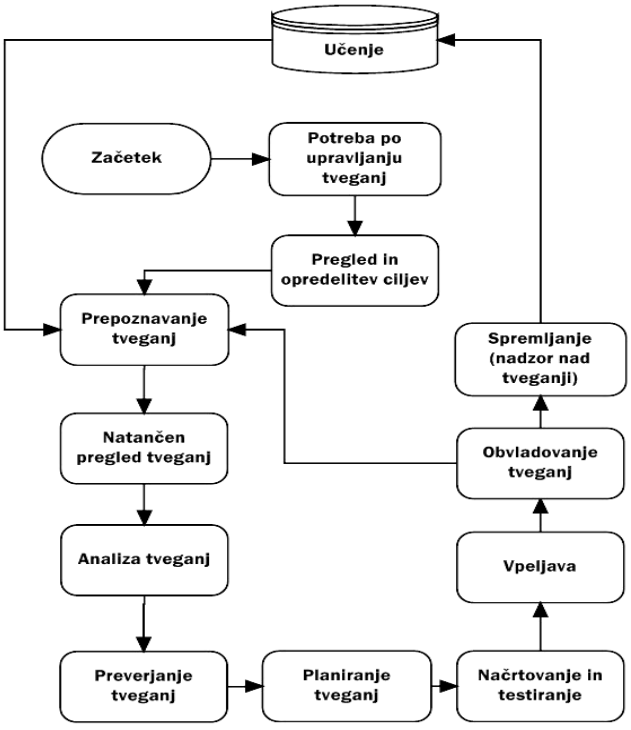
Kljub dobremu managementu poslovnih procesov se ne moremo izogniti izjemnim, nezaželenim dogodkom. Ti lahko preprečijo posamezniku ali podjetju uresničitev ciljev. To so tveganja, ki pa jih lahko prepoznamo in zmanjšamo verjetnost njihovega nastanka. V literaturi se pojavlja več različnih opredelitev tveganj. Alhawari et al. (2008) meni, da je tveganje vsaka sprememba v projektu ali procesu, ki lahko privede do neuspeha. Sestavljeno je iz dveh elementov: negotovosti in izgube. Panjer (2006, str. 3) pravi, da se tveganje nanaša na vse dogodke, pojave in dejavnosti, ki lahko preprečijo posamezniku ali organizaciji uresničitev ciljev. Pomeni verjetnost ali priložnost, da bo nekaj šlo narobe, ter možne posledice v primeru da se bo to uresničilo. Zato se mora podjetje vnaprej vprašati in si odgovoriti na tri vprašanja: "Kaj gre lahko narobe?", "Kaj bomo naredili?" in "Če se kaj pripeti – kako bomo to poplačali?" V praksi je to kompliciran in dolgotrajen postopek, saj podjetja morajo razmišljati in planirati o namišljenem. Pa vendar se jim to obrestuje, saj pravi odgovori na ta vprašanja lahko rešijo podjetje pred katastrofo (Jolly, 2003, str. 4–5). Informacije o tveganjih so bistvenega pomena za uspešno in učinkovito izvajanje poslovnih procesov ter so kritični dejavnik uspeha na konkurenčnem trgu. Na podlagi pridobljenih informacij se lahko odgovorni v podjetjih lažje in bolje odločajo pri pomembnih odločitvah. (Trkman & McCormack, 2009; Jolly, 2003, str. 32).

S prepoznavanjem tveganj, razumevanjem le-teh in pripravo načrtov za zmanjšanje njihovega vpliva na poslovanje, se ukvarja disciplina, ki je, tako kot management procesov, v zadnjih letih pridobila na pomenu, to je management tveganj (Trkman & McCormack, 2009). Management tveganj je skupek strategij, metod, orodij za prepoznavanje in nadzor tveganj ter ohranjanje teh na sprejemljivi ravni. Poleg prepoznavanja tveganj tveganja ovrednotimo glede na njihovo pomembnost, pogostost pojavljanja, stopnjo vpliva in na podlagi tega vzpostavimo aktivnosti za nadzor nad temi tveganji (Alhawari et al., 2008). Namen managementa tveganj je torej sprejem ukrepov, ki preprečujejo tveganja ali ublažijo njihove posledice. Skok, Peterlin in Ribarič (2005, str. 167) na kratko opredelijo management tveganj kot zmanjševanje spremenljivosti bodočega poslovanja podjetja. Predstavijo ga kot niz korakov, ki omogočajo razumevati in obvladovati negotovosti. Ta niz korakov pa lahko tvori proces managementa tveganj.

3.1 Proces managementa tveganj

Kombinacijo različnih aktivnosti managementa tveganj lahko obravnavamo kot svoj proces, ki ga v splošnem lahko razdelimo na štiri faze (Alhawari et al., 2008, str. 890). Prva faza je prepoznavanje tveganj, ki prouči in locira potencialne grožnje. V drugi fazi analiziramo tveganja, jih razvrstimo ter ugotovimo njihov pomen. Tretja faza vključuje planiranje kontrol nad tveganji s poudarkom na najpomembnejših tveganjih. Zadnja faza pa predstavlja nadaljnje spremljanje tveganj, opazovanje stanja. Avtorji (Alhawari et al., 2008, str. 890–892) so na podlagi združitev opredelitev več različnih avtorjev ta proces predstavili bolj podrobno, v razširjenem okviru managementa tveganj, ki je razviden na sliki 5.

Slika 5: Okvir managementa tveganj



Vir: S. Alhawari et al., A Risk Management Model for Project Execution, 2008, str. 890.

- **Potreba po managementu tveganj** *(*angl. *need for risk management)* se nanaša na prepoznavanje prednosti, ki bi jih podjetju lahko prinesel management tveganja v vsakdanjem poslovanju (pri izvajanju projektov in procesov). V dinamičnem in tveganem okolju morajo management tveganj videti kot priložnost za uspeh. Pomena tega procesa pa se morajo zavedati tudi zaposleni, da so pripravljeni sodelovati pri obvladovanju tveganj.
- **Pregled in opredelitev ciljev** *(*angl. *goal definition review).* Podjetje pregleda svoje cilje, na podlagi tega opredeli poslanstvo in vizijo ter začrta pot za doseganje ciljev, oblikuje svojo strategijo.
- **Prepoznavanje, ugotavljanje tveganj** *(*angl. *risk identification).* V tem koraku podjetje ugotovi, katera tveganja lahko vplivajo na doseganje postavljenih ciljev. Prepoznavanje tveganj je prvi korak za preprečitev realizacije le-teh. V tej fazi moramo izpostaviti vsa možna tveganja in narediti seznam potencialnih tveganj, vsakemu ugotovljenemu tveganju pa pripisati vzrok in možne posledice. Vzroki so lahko v tehnologiji, zaposlenih, stiku z okoljem itn. Glavne informacije o potencialnih tveganjih pridobimo preko vprašalnikov, intervjujev zaposlenih, pregleda revizijskih poročil, poročil o napakah, pritožb kupcev itn.
- **Natančen pregled tveganj** (angl. *risk scrutiny).* Namen te faze je, da podjetje poglobljeno preuči in oceni vsa prepoznana potencialna tveganja in nato izloči tista, ki niso povezana oz. nimajo vpliva na proučevan projekt/proces. V tej fazi se v seznam doda še verjetnost nastanka posameznega tveganja. Rezultat te faze je torej opredelitev relevantnih tveganj in določitev verjetnosti njihovega nastanka.
- **Analiza tveganj** (angl. *risk analysis).* Ta korak omogoča pretvorbo pridobljenih podatkov o tveganjih v uporabne informacije za sprejemanje odločitev. Tveganja se razporedi glede na verjetnost nastanka in vpliv ter tako ugotovi njihovo resnost. Na podlagi tega podjetje v skladu s cilji postavi prioritete med tveganji. To služi kot osnova za vzpostavitev potrebnih ukrepov za zmanjševanje posledic tveganj na sprejemljivo raven. Najprej je npr. potrebno ukrepati pri tveganjih z veliko verjetnostjo nastanka in velikim vplivom, nato pa sledijo tveganja z veliko verjetnostjo nastanka in majhnim vplivom, ter tveganja, ki imajo velik vpliv in majhno verjetnost nastanka.
- **Preverjanje tveganja** (angl. *risk verification).* V tej fazi proučimo rezultate analize tveganja in ugotovimo, ali so navedena tveganja relevantna za podjetje oz. ali mu predstavljajo resne grožnje. Pri tem sodelujejo različni ljudje iz podjetja, ki niso sodelovali v predhodni fazi. Namen je iz seznama še dodatno izločiti tveganja, za katera menijo, da niso relevantna.
- **Planiranje tveganja** (angl. *risk planning*). S tem korakom pretvorimo informacije o tveganjih v dejanja in razvijemo aktivnosti za obvladovanje vsakega od tveganj. Ustvarijo se plani, strategije in aktivnosti za zmanjševanje verjetnosti nastanka in posledic tveganj. Rezultat te faze so predlogi, kako v kasnejših fazah kontrolirati tveganja in vzpostaviti določene procesne varnostne kontrole.
- **Načrtovanje in eksperimentiranje** (angl. *planning and experimentation).* Gre za preizkus, ali je bilo planiranje tveganj v prejšnjem koraku natančno in celovito. Glavni namen te faze je preprečiti zapravljanje virov za implementacijo nepravih ukrepov s pomočjo tehnik, kot so strukturirano testiranje za odkrivanje napak, simulacija, kontrolni seznami itn.

- **Vpeljava** (angl. *risk implementation).* V tej fazi se izvedejo planirane aktivnosti iz prejšnje faze in vpeljejo varnostne kontrole. Postavi se časovni okvir in dodeli odgovornosti članom tima. Potreben je tudi celovit nadzor v času implementacije. Možnosti vpeljanih ukrepov je več: izogibanje tveganju, zmanjšanje tveganja, prenos tveganja itn.
- **Obvladovanje, kontrola tveganj** (angl. *risk control).* Gre za fazo ocenjevanja procesa vpeljave in odkrivanja novih tveganj. S tem se posodablja celoten življenjski cikel managementa tveganj. Rezultat faze je poročilo o napredku/nazadovanju izvajanja oz. ugotovitvi, ali se tveganja dejansko zmanjšujejo.
- **Spremljanje (nadzor) tveganja** (angl. *risk monitoring).* Faza vsebuje sprotno spremljanje stanja tveganj in ukrepov. Ob tem se prilagaja izvajanje procesa in dopolnjuje, posodablja seznam tveganj. Podjetja delujejo v spreminjajočem okolju, kar lahko prinese nova tveganja, ki prej še niso bila poznana. Ta faza pripomore k razvoju sistema tveganj, s katerim nabiramo znanje za nadaljnji managament tveganj in se s tem vrnemo v prejšnje faze, nov cikel za dopolnitve.
- **Učenje** (angl. *education).* To je zadnji korak, v katerem so zajete vse izkušnje iz prejšnjih ciklov in se shranjujejo v arhiv. Gre za znanje, ki ga podjetje uporabi ob naslednjih podobnih situacijah. Z akumuliranim znanjem bo ob naslednjem pojavu podobnega tveganja podjetje lahko pogledalo, kako je reševalo tveganje v preteklem primeru in bo s tem precej skrajšalo čas za prepoznavanje in obvladovanje tveganj.

3.2 Razdelitev tveganj

Med poslovanjem se podjetja soočajo z različnimi vrstami tveganj, ki jih povzročata notranje in zunanje okolje. V splošnem Jolly (2003, str. 7) razdeli tveganja na finančna, operativna in strateška. Glavni tveganji, ki jih povezujemo z zunanjim okoljem in obenem uvrščamo med finančna, sta kreditno in tržno tveganje. Strateška tveganja pa se delijo na tveganja poslovnega okolja (tehnologija, konkurenca), transakcijska (investicije, združevanje podjetij) in odnose do investitorjev. Tveganja, ki jih povzroča notranje okolje, so večinoma operativna tveganja. Pod operativna tveganja uvrščamo procesna tveganja, ki so kombinacija virov (ljudje, veščine, metode, oprema, materiali) in delovnega okolja, ter tveganja inovacij. Le-ta pa pomenijo tveganja, ki jih predstavlja vpeljava novosti v poslovanje (Norimarna, 2010; Jolly, 2003, str. 7).

Če za primer pogledamo verigo vrednosti, poslovni proces v najširšem pomenu, se v njem srečujemo s petimi glavnimi tveganji, ki jih izpostavi Christopher (v Jolly, 2003, str. 47):

- **Tveganje dobave**, ki je lahko rezultat prevelikega zanašanja na glavnega dobavitelja oz. slabega managementa dobaviteljev.
- **Tveganje povpraševanja**, ki nastane zaradi napačnega predvidevanja, neuspeha promocije ali nenadnega vstopa novega uspešnega konkurenta na trg.
- **Procesno tveganje** je rezultat variabilnosti proizvajanja, nedefiniranih ozkih grl, slabosti v procesu in neprimernih IT sistemov.
- **Tveganje kontrol** nastane, ko imajo notranji sistem kontrol, pravila in politike lahko negativni vpliv na produktivnost ali dajejo irelevantne rezultate.

- **Tveganje okolja** pa so zunanje katastrofe, kot so poplava, požar, vojna.

Tveganja, ki vplivajo na procese, so relevantna tudi za MPP, saj lahko ogrozijo njihovo izvajanje. Ker so to v splošnem operativna tveganja, jih bom obravnavala v naslednjem poglavju.

3.3 Opredelitev operativnih tveganj

Operativna tveganja (v nadaljevanju OT) so že od nekdaj del poslovanja, na pomenu pa pridobivajo šele v zadnjih letih. Podjetja so jim namreč vse bolj izpostavljena zaradi večje kompleksnosti, pritiska konkurence, razvoja tehnologije, naraščajočega števila tožb, spreminjanja zakonodaje, večjega števila naravnih nesreč, medsebojne odvisnosti poslovnih procesov itn. (Skok et al., 2005, str. 164). Nastajajo zaradi zunanjih in notranjih dejavnikov, kot so človeške, sistemske napake, kažejo pa se lahko v obliki neuspešno izvedenih procesov in imajo nefinančne ali finančne negativne vplive na podjetje (Norimarna, 2010).

V skladu z definicijo Baselskega odbora za nadzor bank se OT nanašajo na notranje okolje podjetja, na procese in aktivnosti (Cheng et al., 2005). Ta odbor definira OT kot »tveganja neposredne oz. posredne izgube zaradi neprimernih ali neuspešno izvedenih notranjih procesov, dejanj ljudi, delovanja sistemov ali zaradi zunanjih dogodkov« (Basel Committee on Banking Supervision, 2001, str. 2). Pri tem so notranji dogodki rezultat napak v procesih ali sistemih, zunanji dogodki pa tisti, katerih pojav ne more biti kontroliran s strani podjetij (npr. naravne nesreče). Podjetja lahko zunanje vplive le omilijo, medtem ko so notranji dogodki direktno pod vplivom podjetij (Panjer, 2006, str. 3–6). Druga opredelitev v splošnem pravi, da so OT tista tveganja, ki so povezana s poslovanjem podjetja in različnimi funkcijami v podjetju. Z vidika bank pa poenostavljeno definirajo OT kot vsa tveganja, ki niso kreditna ali tržna (Balestra, b.l.). Primer OT v bančništvu je npr. nedovoljena avtorizacija posojila s strani zaposlenega ali prekinjeno bančno poslovanje zaradi napak v IT sistemu, nesreč.

3.3.1 Razvrščanje operativnih tveganj

OT lahko razlikujemo glede na njihov vzrok (dejavnik tveganja) in posledice, ki jih prinašajo (Skok et al., 2005, str. 181). Vzrok je dogodek ali splet okoliščin, ki povzroči tveganje, posledica pa je finančna ali nefinančna izguba. Glede na dejavnik tveganja pa Skok et al. (2005, str. 181–190) razdelijo OT v štiri skupine:

- **Tveganja zaposlenih** nastanejo zaradi dejanj zaposlenih oz. opustitve dejanj v podjetju. Gre za notranje organizacijske težave podjetja, kot so napake zaposlenih, zlorabe, nerazpoložljivost zaposlenih in postopki obravnave zaposlenih. Pod napake zaposlenih štejemo nenamerna dejanja, zaradi katerih nastanejo motnje v procesu (npr. napačni vnos podatkov). Zlorabe pa so namerne napake zaposlenih, ko zavestno prikrivajo dejansko stanje nadrejenim ali namerno izvedejo določena dejanja (kraja, prevara, prikrivanje dejstev, povzročanje škode, podkupovanje, prekoračitev pooblastil, ponarejanje). Te vrste tveganj podjetje obvladuje preko politik obravnavanja zlorab, poseben poudarek pa mora biti na

nadzoru procesov, kjer je možnost zlorab večja (nabava, gotovinsko poslovanje). Poslovni proces lahko ovira tudi nerazpoložljivost zaposlenih (začasna delovna nezmožnost, prekinitev delovnega razmerja, stavka). Postopki obravnave zaposlenih pa se lahko nanašajo na kršenje pravic zaposlenih (diskriminacija zaposlenih zaradi spola, narodnosti, nadlegovanje, protizakoniti postopki prekinitev delovnega razmerja itn.).

- **Tveganja razmerij** se nanašajo na odnose s strankami, državnimi organi, tretjimi osebami in vključujejo tveganja obeh strani v razmerju. So posledica neizpolnjevanja obveznosti podjetja do deležnikov (stranke, delničarji, država), ki so lahko finančne narave (odškodnine). Zato je že v fazi načrtovanja izdelka pomembno preveriti skladnost z zakonodajo, pripraviti natančna navodila za uporabo, v fazi izdelave spremljati kakovost in skrbno pripraviti varnostni načrt umika izdelka v primeru bistvenih napak na izdelku. Podjetje lahko tožijo tudi delničarji (tveganje razmerij z delničarji) zaradi zavajajočih napovedi bodočih dobičkov podjetja, neustrezno prikazanih finančnih rezultatov ali spornih naložb. Tveganje razmerij z državo so kršitve davčne ali okoljske zakonodaje.
- **Tveganja poslovnih procesov in tehnologije** so posledica izvajanja poslovnih aktivnosti in tehnologije. Gre za tveganje v primeru neuspešne izvedbe poslovnih procesov, nepravilno izvedenih postopkov (nepravilna izvedba naročila zaradi nesporazuma pri zapisu naročila). Tveganje tehnologije pa opišemo kot tveganje izgub zaradi nepravilnega delovanja ali zaustavitve sistemov, posledično celotnega procesa. Sem štejemo tudi tveganja kraje podatkov, zunanje sistemske motnje (izpad plačilnih sistemov zunaj družbe), notranje sistemske motnje (programske napake, zastareli sistemi, virusi). Zato je pomembna ustrezna sistemska arhitektura, vlaganja v nove, bolj zmogljive sisteme, in razvoj v skladu s procesi.
- **Zunanja tveganja** so povezana z dogodki, povzročenimi s strani tretjih oseb, katerih aktivnosti ni mogoče nadzirati. Gre za finančne izgube zaradi zunanjih dejavnikov – vplivov narave, zlorab tretjih oseb in sprememb zakonodaje. Premoženjsko tveganje je tveganje zaradi poškodb ali izgube premoženja podjetja, zlorabe tretjih oseb pa so načrtna dejanja v obliki odtujitve premoženja, ponarejanja, napada na računalniški sistem, terorizma.

Glede na to, da so OT povezana s procesi, ljudmi, sistemi in zunanjimi dogodki, lahko ogrožajo vsako izmed organizacijskih enot znotraj podjetja. Zato si podjetja prizadevajo razviti pristope za merjenje, ovrednotenje, spremljanje in obvladovanje operativnih tveganj, kar pa širše imenujemo management operativnih tveganj (v nadaljevanju MOT) (Cheng et al., 2005). MOT ob podpori vodstva lahko pomaga zmanjšati verjetnost nastanka nepričakovanih izgub, izboljšati učinkovitost poslovanja, slediti zakonskim predpisom, obenem pa s tem povečuje kakovost poslovnih procesov (Skok et al., 2005, str. 167). Kot management tveganj pa lahko tudi MOT predstavimo v več fazah.

3.4 Faze managementa operativnih tveganj

V splošnem Norimarna (2010) MOT deli na štiri faze: identificiranje, ocenjevanje (verjetnosti in vpliva), obvladovanje tveganj (s poudarkom na tistih z visoko verjetnostjo in velikim vplivom) in določitev kritičnih kazalnikov tveganj, ki v prihodnje služijo kot zgodnje opozorilo

o tveganjih. Skok et al. (2005, str. 167) pa združijo te faze v dve, in sicer: faza prepoznave in merjenja tveganja ter faza ukrepanja.

3.4.1 Faza prepoznave in merjenja

Prepoznava tveganj in njihovih vzrokov je ključna podlaga za nadaljnje ukrepanje. Prepoznavamo jih lahko na različne načine: na podlagi analize preteklih škodnih dogodkov, s tehniko soočanja idej »Viharjenje možganov« (angl. *Brainstorming*), s pomočjo predhodnih raziskav na podlagi meritev in statističnih analiz, z raziskovanjem povezave problemov in vzrokov v poslovnih procesih. Ko prepoznamo vzroke, tudi lažje ocenimo izpostavljenost tveganju. Poleg glavnih vzrokov (napake pri izvajanju, prevare, zlorabe pooblastil) je pomembno najti tudi stranske vzroke, ki posredno vplivajo na višino izgube (npr. pomanjkljiv nadzor nad zaposlenimi, pomanjkljive kontrole, brez dvojnega preverjanja) (Norimarna, 2010).

Ko tveganja identificiramo, jih je potrebno ovrednotiti in ugotoviti, katera izmed njih so nesprejemljiva ter potrebna ukrepov. Ob tem upoštevamo verjetnost za realizacijo tveganja in ocenimo vpliv. Ko ocenjujemo izpostavljenost, upoštevamo podatke o preteklih izgubah. Če poznamo razmere, v katerih so se v preteklosti realizirala podobna tveganja, ocenimo njihovo relevantnost za trenutno tveganje. Višino izgub pa moramo ovrednotiti v celoti. Ni dovolj, da ocenimo samo stroške, ki nastanejo v času nezgode, ampak tudi kasnejše (denimo stroške sodnih postopkov) (Skok et al., 2005, str. 168–170; Utratnik & Grasselli, b.l.). To je kompleksen proces, še posebej v primeru da gre za tveganje zaposlenih. Ne moremo npr. točno predvideti, kako verjetno je, da bo zaposleni zlorabil pooblastila, koliko denarja bo izgubilo podjetje, če zaposleni ne bo izpolnjeval pravil in bo grdo ravnal s strankami itn. (Mora Campos, 2008).

Ob tem Fehér (2009) poudarja, da OT težko merimo, napovedujemo in prepoznavamo njihove vzroke. Razlog je med drugim ta, da pogoste izgube manjše vrednosti v podjetjih velikokrat niso zabeležene, izgube visokih vrednosti pa se zgodijo zelo redko in tako težje sklepamo verjetnost nastanka izgub v prihodnosti. Izziv merjenja OT je, da so vnaprej težko vidni, skriti, kompleksni, med seboj odvisni in imajo lahko velik vpliv. Za odkrivanje in lažje merjenje OT je podjetjem v pomoč, da vnaprej oblikujejo sistem kazalnikov tveganj.

Merljive pokazatelje, ki opozarjajo na možnost izpostavljenosti operativnim tveganjem, imenujemo kazalniki tveganja. Tiste, ki pa kažejo na zelo pomembno izpostavljenost, pa imenujemo ključni kazalniki tveganja (angl. *key risk indicators- KRI*). Med nadzorom tekočega poslovanja s pomočjo teh kazalnikov ocenimo bodoča tveganja ter kakovost notranjih kontrol. Gre za mere, s katerimi se na podlagi opazovanja in ocenjevanja poskušamo izogniti oz. omiliti sedanje in bodoče finančne ali nefinančne negativne vplive (ugled), saj lahko pravočasno odpravimo težave (Davies, Finlay, McLenaghen & Wilson, 2006). Nekateri KRI opominjajo na izpostavljenost tveganjem na ravni organizacije (delež odpovedi v številu zaposlenih), drugi pa so značilni za posamezne procese in funkcije (Skok et al., 2005, str. 168). Primer KRI je število pritožb kupcev. Ko te narastejo, je precej verjetno, da za tem lahko stoji neka sistemska ali

širša napaka. Povedano v splošnem, večje spremembe vrednosti tega kazalnika signalizirajo večjo izpostavljenost OT (Davies et al., 2006).

Operativna tveganja se lahko kažejo v treh stopnjah: pojav težav, nezgod in nastanek večjih izgub. Pokazatelji tveganj so lahko že majhne težave, ki ob neukrepanju privedejo do nezgod. Za slednje ni nujno, da imajo finančne posledice. Ob nadaljnjem neukrepanju pa se ti dogodki lahko razširijo v neposredne ali posredne izgube, ki so merljive in se odražajo v finančnih izkazih. Kot nezgodo lahko opredelimo kratkotrajno prekinitev v delovanju računalniških sistemov. Če pa to prezremo, lahko privede do motenj sistema, ki pa se že odražajo v večjih izgubah (pritožbe, reklamacije strank, prekinitev pogodb). Nezgoda ali incident (Skok et al., 2005, str. 169–170) je torej dogodek, zaporedje dogodkov ali nenavadnih pojavov, ki odstopajo od normalnega delovanja in signalizirajo potrebo po izboljšanju procesov. Zaradi svojih lastnosti so dober kazalnik tveganj. Največje število nezgod je brez gmotnih izgub, nekaj manj jih je z manjšimi gmotnimi izgubami, redkejše pa so nesreče z velikimi gmotnimi izgubami in človeškimi poškodbami. Incidenti, ki nastanejo zaradi napak v notranjih procesih, sistemih, zaradi ljudi ali zunanjih dejavnikov in imajo posreden ali neposreden vpliv na izkaz poslovanja, pa imenujemo škodni dogodki (Dobra banka, 2010a). Da se slednjim izognimo v čim večjem številu, je ključna naslednja faza – faza ukrepanja.

3.4.2 Faza ukrepanja

Za tveganja, ki smo jih prepoznali in ocenili v prejšnji fazi, se v tej fazi moramo odločiti, s katerimi ukrepi bomo ta tveganja obvladovali. Z ukrepi vplivamo na zmanjšanje izpostavljenosti tveganjem, pogostosti in vpliva. Od slednjih dejavnikov pa je tudi odvisno, za kakšen ukrep se bomo odločili. Pri tem moramo presoditi, ali se predlagani ukrepi izplačajo (da stroški ukrepanja ne presegajo posledic tveganj, proti katerim ukrepamo). Poleg tega moramo biti pozorni na to, da vpeljani ukrepi zares zmanjšujejo tveganja in ne le prenesejo tveganja na kakšno drugo organizacijsko enoto (Basel, 2001, str. 15). Za ukrepe MOT ne poznamo standardnih postopkov, saj se tveganja med seboj razlikujejo. V splošnem pa so na voljo štiri skupine različnih ukrepov oz. strategij MOT, ki jih podjetje lahko izbere (zur Muehlen & Rosemann, 2005; Helquist, Deokar, Cox & Walker, 2012; Skok et al., 2005, str. 176–179):

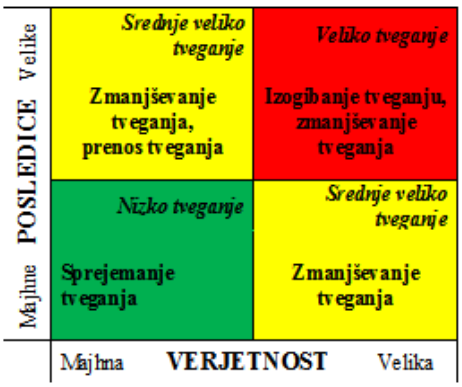
- **Izogibanje tveganju** (angl. *avoidance*). Nesprejemljivim tveganjem se podjetje hoče izogniti, če njihovi negativni učinki lahko presežejo pozitivne učinke izvajanja poslovnega procesa (npr. če proizvajamo izdelek, ki lahko povzroči poškodbe uporabnikov in kasnejše tožbe). Zato v tem primeru izberemo ukrepe, ki preprečujejo nastajanje kazalnikov tveganja oz. izločijo verjetnost nastanka določenega tveganja, preden se ta pojavi. To lahko dosežemo s prenovo poslovnih procesov oz. izločitvijo aktivnosti, ki tveganje povzročajo. Velikokrat gre tudi za preobrazbo v druga tveganja, ki so manj nevarna in jih lažje obvladujemo. Pa vendar ukrep izogibanja ni vedno uporaben, saj s preobsežno uporabo te metode podjetje težje doseže cilje poslovanja. Ukrep je primeren za tveganja, ki povzročijo katastrofalne izgube, imajo visoko stopnjo verjetnosti nastanka, ne moremo pa jih zmanjšati.
- **zmanjševanje tveganja** (angl. *mitigation*). Tveganja omejimo s pomočjo meritev in vpeljavo kontrol, ki zmanjšajo pogostost nastanka in vpliva na sprejemljivo raven, ne

izločijo pa tveganja. Ukrepi so lahko na ravni procesa ali širše in jih delimo na organizacijske, tehnološke in izobraževalne. Primer širših ukrepov na ravni podjetja so npr. požarna varnost, reševanje ob naravnih katastrofah, notranja revizija, nagrajevanje zaposlenih. Na ravni procesov pa lahko postavimo kontrolne aktivnosti znotraj procesov. Cilj ukrepov je maksimirati preostanek vrednosti premoženja po nastalem škodnem dogodku.

- **Prenos tveganja** (angl. *transfer*). Prenos tveganja pomeni izognitev posledicam s prenosom tveganja na tretjo osebo (zunanje izvajalce, zavarovalnice). Primer tega sta zunanje izvajanje določenega procesa in zavarovanje pred potencialno izgubo. S pomočjo zavarovanja podjetja zmanjšajo vpliv tveganja na spremenljivost svojega dobička, sredstev, likvidnosti, denarnega toka. Zavarovati je smiselno tiste dele, ki so izpostavljeni velikim izgubam in lahko dosežejo sprejemljivo soudeležbo kritja izgube. Potrebno je najti ravnotežje med prevzemom in prenosom tveganja. Zaradi stroškov zavarovanja je potrebno preučiti, kolikšen del tveganja se nam izplača prevzeti, višina soudeležbe pa mora biti v finančnih zmožnostih podjetja za sprejemanje tveganja. Tveganja z visoko višino izgube in nizko pogostostjo zavarujemo, tista z nizko višino izgube in večjo pogostnostjo pa so tveganja, ki jih prevzamemo v breme tekočega poslovanja ter jih z ukrepi poskušamo zmanjšati. Ukrep torej ni smiseln, če stroški zavarovanja oz. prenosa tveganja presegajo višino pričakovanih izgub v primeru realizacije ali če npr. zunanje izvajanje procesa prinese še večja tveganja.
- **Sprejemanje tveganja** (angl. *acceptance*). V tem primeru sprejmemo posledice realizacije tveganj. Povedano z drugimi besedami – o identificiranem tveganju ne sprejmemo nobenih ukrepov. To se zgodi, ko podjetje oceni, da je majhna verjetnost, da se tveganje realizira, v primeru realizacije pa bi bila majhna tudi izguba. Zato ukrep ni potreben oz. niti ni ekonomsko upravičen.

V katerih primerih se odločiti za posamezno skupino ukrepov pa prikazuje slika 6.

Slika 6: Matrika stopenj tveganja in predlaganih ukrepov (iz okvira COSO-ERM)



Vir: H. E. Mora Campos, Desarrollo de aplicacion para gestion de riesgo operacional en procesos, 2008, str. 26.

3.5 Notranje kontrole

Podatkovna, IT in organizacijska tveganja se nanašajo na tveganja zaradi netočnih podatkov, razpoložljivosti sistemov, uspešnosti zaposlenih. Tovrstnih tveganj pa ne moremo povsem

izločiti, saj so povezana s samim izvajanjem procesov (zur Muehlen & Rosemann, 2005). Moramo jih omejiti, konkreten ukrep za to pa je vpeljava notranjih kontrol (npr. ločevanje odgovornosti, varnostno kopiranje, preverjanje pravilnosti podatkov) (vom Brocke & Rosemann, 2010b, str. 165). Notranje kontrole so vedno služile za pomoč doseganju ciljev, v zadnjem času pa se pojavljajo tudi kot ukrep managementa tveganj in za zagotavljanje skladnosti poslovanja (Weiß & Winkelmann, 2011). S pomočjo kontrol spremljamo pojav tveganj v vsakdanjem izvajanju procesov in zmanjšamo možnost realizacije le-teh s proaktivnim managementom. Notranje kontrole so v povezavi s tveganji vključene v kar nekaj okvirov, kot sta npr. ERM (COSO) in COBIT (Panjer, 2006, str. 5).

Poznamo dve vrsti kontrolnih mehanizmov: procesne kontrole, ki se izvajajo znotraj procesov kot aktivnosti, in notranje revizijske procese. Slednji so ločeni poslovni procesi, ki so na manjšem vzorcu izvedeni naknadno za preverjanje pravilnosti izvedbe. Notranje kontrole so različne: kontrole obnašanja, informacijske kontrole, operativne kontrole, splošne kontrole itn. Lahko so ročne ali avtomatizirane, preventivne ali naknadne. Podjetja stremijo k bolj preventivnim in avtomatiziranim kontrolam (Panjer, 2006, str. 5).

Kontrolne aktivnosti znotraj procesov so namenjene zmanjševanju tveganj in s tem posredno dodajajo vrednost, jih pa lahko ločimo od procesnih aktivnosti, ki dodajajo vrednost neposredno (so v procesu nujne, da nastane nek produkt). Število notranjih kontrol v procesih odraža, koliko je podjetje pripravljeno tvegati (vom Brocke & Rosemann, 2010b, str. 164–165). Na podlagi tega pa zur Muehlen (2008, str. 26–27) loči dve vrsti procesov: 1. "vitki" (angl. *lean*) procesi, v katerih večina aktivnosti neposredno dodaja vrednost, malo, če sploh kaj, pa je kontrol. Takšni procesi so z vidika tveganj zelo ranljivi. 2. "debeli" (angl. *fat*) procesi pa imajo veliko kontrolnih aktivnosti in so zato bolj kompleksni ter imajo manj aktivnosti, ki neposredno dodajajo vrednost. Zato je potrebno najti pravo razmerje med obema vrstama aktivnosti, v skladu s proračunom in poslovnimi cilji. Nesmiselno bi bilo, da bi npr. za nabavo pisarniškega materiala v vrednosti 20 EUR potrebovali 5 ljudi, katerih čas je vreden 100 EUR. Tudi kontrole je potrebno kontrolirati, testirati, dokumentirati in spremljati, da dosegajo svoj namen, ter jih čim bolj avtomatizirati, kjer je to možno.

Kontrole znotraj procesov so tesno povezane z razvojem procesov. Načrtovanje kontrol vpliva na potek aktivnosti v poslovnem procesu. Podatki za oblikovanje kontrol izhajajo iz rezultatov spremljanja izvajanja procesa. Po drugi strani prenova poslovnega procesa povzroči spremembo tveganj, kar pa lahko privede do novih, posodobljenih kontrol (vom Brocke & Rosemann, 2010b, str. 164–165). Nadzor poslovnega procesa kaže, ali postavljene notranje kontrole funkcionirajo pravilno. Vsak proces je sestavljen iz več aktivnosti in v vsakem procesu so tveganja, zaradi katerih potrebujemo notranje kontrole. Na eno aktivnost lahko v modelu procesa apliciramo več različnih kontrol, prav tako pa lahko ena kontrola vpliva na več različnih aktivnosti (Rikhardsson et al., 2006, str. 5).

Konkretni primer kontrol sta načelo štirih oči, ločitev dolžnosti (en posameznik ne more sodelovati v več kot eni ključni funkciji v procesu). Na tem primeru lahko ponazorimo oblikovanje kontrole na podlagi tveganja (vom Brocke & Rosemann, 2010b, str. 164–165):

- Tveganje: neavtorizirano kreiranje naročila in plačila neobstoječim dobaviteljem.
- Cilj kontrole: preprečiti neavtorizirano naročanje.
- Notranja kontrola: izvrševanje naročil in odobritev morata opraviti dva različna nabavna referenta.

Naslednji primer so bančne kontrole, ki so lahko kombinacija avtomatskih in ročnih preverjanj. Npr. izpolnjen obrazec se najprej preveri računalniško. Če kakšen podatek manjka, aplikacija pošlje bančnemu osebju obrazec v ponovni pregled, dopolnitev. Ko pa so vse informacije na voljo, so izvedena še preverjanja veljavnosti podatkov (Majič, 2002).

3.6 Management operativnih tveganj v bankah

Posebno velik interes za ugotavljanje izgub, povezanih z operativnimi tveganji, so izkazale finančne institucije. V zadnjih desetletjih je namreč njihov sektor zaznamovalo veliko sprememb, kot so finančna kriza, huda konkurenca, zahtevni uporabniki. Banke so bile zato prisiljene hitro prilagajati tako produkte kot tudi notranje procese, kar je povečalo izpostavljenost OT (Di Renzo et al., 2007; Jallow et al., 2007). Ker pa jim niso posvetile dovolj pozornosti, so ugledne finančne institucije, kot so Barings Bank, Societe Generale na račun operativnih tveganj utrpele milijardne izgube (Tafri et al., 2011; Di Renzo et al., 2007). Societe Generale je npr. v letu 2008 zaradi pomanjkljivega MOT izgubila okrog 4,9 milijard EUR (Dahen & Dionne, 2010). Danes tako OT sodijo med najpomembnejša tveganja. Panjer (2006, str. 6–8) pojasni, da OT v bančnem sektorju zavzemajo 30 % vseh tveganj, 60 % predstavljajo kreditna, 5 % tržna in 5 % ostala tveganja. Zato bančna regulativa in banke posvečajo precej časa in sredstev za management teh tveganj.

Ključen je dober pregled nad procesi, na podlagi katerega se lahko banke čim več tveganjem izognejo oz. z ukrepi obvladovanja tveganj in managementa procesov omilijo njihove posledice. Vpeljujejo sisteme za merjenje tveganj in pridobivanje podatkov o že realiziranih tveganjih, na podlagi teh pa razvijajo sisteme za poročanje in nadaljnje obvladovanje OT. Način obvladovanja izbere banka sama in je odvisen od njene velikosti, tehnološke razvitosti in kompleksnosti (Majič, 2002).

Glavni motiv za vpeljavo MOT pa kot pravi Jolly (2003, str. 32) niso prednosti tega pristopa, ampak skladnost z regulativo panoge. Tudi v bančništvu je bila regulativa tista, ki je spodbudila odgovorne v podjetjih, da so OT pričeli identificirati, meriti in dokumentirati. Na OT v bančništvu se danes navezujejo različna priporočila, zakoni in standardi. Na področju ZDA je v veljavi zakon Sarbanes-Oxley (SOX), ki ga je država uvedla kot zaščito pred škandali in prevarami, kot so se npr. v preteklosti zgodile v podjetjih Enron, WorldCom in Tyco. Zakon je sicer specifičen za tveganje iz naslova finančnega poročanja (angl. *Financial Reporting Risk*) in tehnologije ter ne pokriva vseh vrst operativnih tveganj. SOX je v splošnem povezan z ameriškim standardom okvira notranjih kontrol (angl. *Internal Control framework*) s strani komiteja COSO (*Committee of Sponsoring Organizations of the Treadway Commission)* (Fionda, 2009).

COSO je leta 2004 predstavil celovit okvir managementa tveganj (angl. *Enterprise Risk Management – ERM*), ki naj bi zagotavljal ravnotežje med rastjo, donosnostjo, negotovostmi, tveganji in priložnostmi. ERM je proces, ki ga izvaja vodstvo podjetja in drugi udeleženi v načrtovanju strategije podjetja. Zasnovan je z namenom prepoznavanja potencialnih dogodkov, ki bi lahko ogrozili poslovanje, ter skrbi za to, da se obvladovanje tveganj izvaja v želenem obsegu in zagotavlja doseganje ciljev podjetja (Fionda, 2009). Gre za strukturo, ki omogoča kombiniranje vseh aktivnosti managementa tveganj v en sam, integriran okvir. To podjetju v nasprotju z nekoordiniranim managementom tveganj po oddelkih omogoča bolj učinkovit management tveganj z manjšimi stroški (Hoyt & Liebenberg, 2012). Ob tem pa avtorji Gordon, Loeb in Tseng (2009) opozarjajo, da ERM okvir lahko podjetju prinaša vrednost le, če ga pri uvedbi uskladijo in prilagodijo dejavnikom, ki vplivajo na njihovo podjetje, to so: negotovost okolja, konkurenca, velikost in kompleksnost podjetja ter nadzor.

Razširjen po celem svetu in aktualen tudi za naše banke pa je novi kapitalski sporazum Basel II (angl. *New Capital Accord*), ki ga je pripravil Baselski odbor za nadzor bank (angl. *Basel Committee on Banking Supervision*) (Fionda, 2009).

3.6.1 Basel II (Nov kapitalski sporazum)

Leta 2006 je bil sprejet Basel II, v katerem je Baselski odbor podal priporočila glede managementa tveganj (Basel Committee on Banking Supervision, 2006). Njegov namen je bil okrepiti stabilnost mednarodnega bančnega sistema. Z izboljšanjem managementa tveganj v bankah in z zahtevami po minimalnem kapitalu, ki ga banke morajo zadržati za kritje tveganj, so banke bolj stabilne (Di Renzo et al., 2007). Sporazum je zastavljen tako, da bolj kot napredne politike obvladovanja tveganj prevzame banka, manj kapitala mora imeti na razpolago za kritje tveganj. Z ekonomskega vidika pa je cilj bank doseči čim nižji nivo tega regulatornega kapitala (angl. *regulatory capital*). Obenem želijo banke pokazati investitorjem in bonitetnim agencijam, da imajo uvedene politike managementa tveganj. Zato je cilj Basla II stimulirati razvoj naprednih metod managmenta tveganj (Operational losses, much more than a tail only, 2009).

Sporazum je samo priporočilo, ki pa ga v svojo zakonodajo vključijo države same. Regulatorne oblasti so zelo fleksibilne glede vprašanja, katere metode naj banke izberejo, le da uporabljajo primerno kombinacijo kvalitativnih in kvantitativnih kriterijev (relevantni notranji in zunanji podatki, analiza scenarijev, dejavniki v poslovnem okolju in notranje kontrole). Izbrana metoda mora odsevati raven izpostavljenosti OT in čim bolj točno meriti izgube zaradi tveganj (Dahen & Dionne, 2010). Sporazum se nanaša na več vrst tveganj, jaz pa se bom osredotočila na OT. Za slednje je pri pregledovanju stanja v bančništvu Baselski odbor ugotovil, da sta merjenje in modeliranje še v povojih. Zato je to s svojim delovanjem in kapitalskim okvirom skušal zavarovati institucije pred direktnimi in posrednimi izgubami zaradi OT (Basel Committee on Banking Supervision, 2001).

Okvir za opredelitev minimalnih kapitalskih zahtev bank je razdeljen na tri stebre (angl. *Pillars*). V vsakem od teh stebrov pa najdemo zahteve tudi glede izboljšanja MOT. Minimalne

zahteve so določene v prvem od treh stebrov, ostala dva stebra se nanašata na nadzorni proces in obnašanje trga (Panjer, 2006, str. 6–8).

- Prvi steber predlaga kalkulacije minimalnih kapitalskih zahtev. V tem stebru je definiran regulatorni kapital, tveganja pa so razdeljena v pet kategorij: kreditno, tržno, operativno, likvidnostno in pravno tveganje. V sklopu tega so bile eksplicitno in posebej dodane minimalne kapitalske zahteve za operativna tveganja.
- Drugi steber naslovi regulativni nadzor, s ciljem zagotavljati primerno raven kapitala v banki in spodbuditi boljšo prakso managementa tveganj. Glede OT ta steber posredno določa, da morajo banke spremljati vse dogodke v zvezi z OT ter imeti notranje kontrole v procesih. Te morajo biti dokumentirane in s tem na razpolago bančnim nadzornikom. Boljše razumevanje OT pa pomaga prepoznati potencialna področja izgub, kjer lahko banke zmanjšajo pogostost in posledice škodnih dogodkov.
- Tretji steber se nanaša na tržno disciplino. Ob javnem razkritju določenih podatkov bank glede njihove izpostavljenosti tveganjem, sistemov merjenja in drugih podatkov lahko primerjamo udeležence trga in tako spodbudimo tržno disciplino (Di Renzo, 2007).

V sklopu prvega stebra lahko banke izbirajo med tremi različnimi pristopi za izračun minimalnih kapitalskih zahtev za OT. Te zahteve naraščajo glede na sofisticiranost in občutljivost na tveganja: enostavni pristop (angl. *the Basic Indicator Approach*), standardiziran pristop (angl. *the Standardized Approach*) in napredni pristop (angl. *the Advanced Measurement Approach- AMA*) (Di Renzo, 2007; Panjer, 2006, str. 8). Ko so bili izvršni direktorji v raziskavi (Ryan & Hida, 2007) vprašani, kateri pristop uporabljajo za doseganje zahtev po Baslu II, jih je največ (44 %) izbralo standardiziran pristop, 41 % pa enostavni pristop.

Enostavni pristop določa kapital OT z uporabo enega samega kazalnika kot pokazatelja za splošno bančno izpostavljenost operativnim tveganjem. Ta kazalnik so bruto prihodki. Vsaka banka zadrži kot kapital določen odstotek od bruto prihodkov. Npr., banke naj za OT zadržijo 15 % bruto prihodkov preko zadnjih treh let. Ta pristop je lahek za vpeljavo in ga lahko apliciramo na vse banke. Problem pristopa pa je omejena odzivnost na specifične potrebe in karakteristike bank. Zato je bolj primeren za manjše banke z manj raznolikimi storitvami. Od večjih bank, z večjo izpostavljenostjo OT, komite pričakuje uporabo bolj sofisticiranega pristopa (Panjer, 2006, str. 8; Basel, 2001, str. 6–8).

Standardiziran pristop se od enostavnega razlikuje v tem, da so bančne aktivnosti pri njem razdeljene na več standardiziranih poslovnih področij (npr. korporativne finance, prodaja, bančno poslovanje s prebivalstvom, komercialno bančništvo, plačila in poravnava, agencijske storitve, borzno posredništvo). Ta področja dosledno zbirajo podatke o notranjih izgubah. Določen odstotek (12–18 %) povprečnega bruto dohodka za tri leta se dodeli vsakemu od področij. Tako ta pristop natančneje odraža različne profile tveganj preko banke, povezane z njihovimi poslovnimi aktivnostmi (Panjer, 2006, str. 8; Basel, 2001, str. 6–8).

Napredni pristop AMA pa zahteva večji vložek sredstev, vendar omogoča bankam, da razvijejo bolj sofisticirane notranje politike MOT. V ta pristop mora biti vključeno zadostno število virov, vključno z upravo, nadzornim svetom, zaposlenimi v področjih kontrole ter revizije in glavnih poslovnih področjih. AMA pristop vključuje strukturirano analizo podatkov notranjih in zunanjih izgub, analiz scenarijev in notranjih kontrol. Potrebno je beleženje zgodovinskih podatkov o izgubah po kategorijah tveganj ter podrobno modeliranje OT. Za doseganje tega pristopa mora banka razdeliti poslovanje na poslovna področja in znotraj njih opredeliti tveganja ter določiti kritične kazalnike OT. To omogočajo meritve preteklih podatkov o izgubah z vidika velikosti in pogostosti. Na podlagi teh se izračuna pričakovana izguba v prihodnosti in zahtevan minimalni kapital. Banke o uporabi podatkov o izgubah odločajo same, medtem ko metodo za kalkulacijo zahtevanega kapitala določijo nadzorniki, ki določijo kvalitativne in kvantitativne standarde za zagotovitev integritete tega pristopa, kvalitete podatkov in ustreznosti notranjih kontrol. Ta pristop natančneje razjasni profil banke in zniža višino zahtevanega kapitala (Panjer, 2006, str. 8; Basel, 2001, str. 6–8).

4 MANAGEMENT POSLOVNIH PROCESOV IN MANAGEMENT OPERATIVNIH TVEGANJ

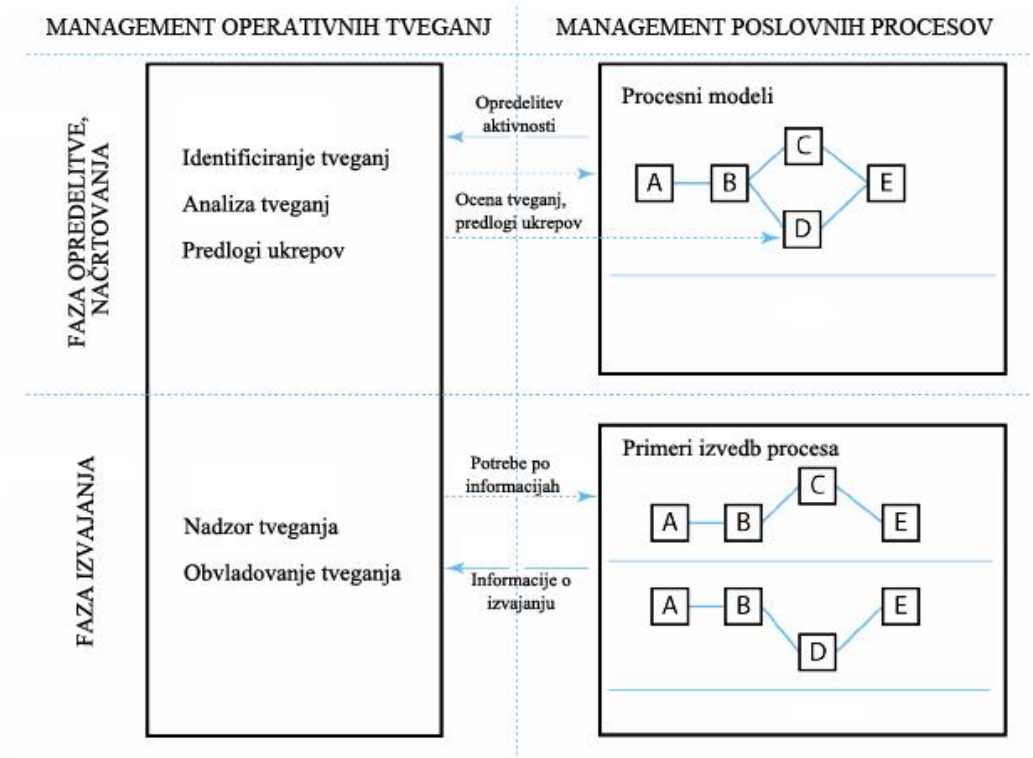
Če povzamem – MPP predstavlja niz aktivnosti, s pomočjo katerih podjetje lahko optimizira poslovne procese in jih prilagaja svojim ciljem. Skrbi za to, da so procesi uspešno izvedeni, v skladu s strateškimi cilji, in izpolnjujejo zahteve deležnikov, pri čemer se upošteva učinkovitost, varnost, zanesljivost, funkcionalnost itn. Procesi morajo ustvarjati vrednost, ključno je dobro načrtovanje procesov. Uspešnost procesov kažejo kritični kazalniki poslovanja (angl. *key performance indicators*) (zur Muehlen, 2007, str. 12). Ker pa večina procesov poteka v okolju, kjer je veliko potencialnih nevarnosti, ki lahko ogrozijo izvajanje procesa, se procesom posveča tudi MOT (Tepina, 2010). Slednji se osredotoča na zagotavljanje vrednosti za deležnike s tem, da se sooča s tveganji, ki so del vsakega procesa. Proces načrtuje tako, da je v njem čim manj možnosti za realizacijo tveganj, povratne informacije iz procesov pa pridobiva s pomočjo kritičnih kazalnikov tveganj (KRI) (Tafri et al., 2011). MPP in MOT sta si torej v osnovi različna po namenu, aktivnostih. Tako je večinoma tudi v podjetjih, saj zaposleni v MPP in MOT delujejo v ločenih organizacijskih enotah, imajo različne cilje in uporabljajo druge metodologije (zur Muehlen & Rosemann, 2005).

Kljub razlikam pa imata disciplini pomembno skupno točko, to so procesi. Zato vedno več avtorjev zagovarja, da se morata povezovati, saj ob pravilni kombinaciji prinašata dodano vrednost podjetjem. Še več, povezovanje MOT z osnovnimi tehnikami MPP v zadnjem času vedno več avtorjev vidi kot učinkovit način obvladovanja OT (Nota & Di Georgio, 2010). Ob finančni krizi je koncept zaradi svojih prednosti še pridobil na pomenu. Pa vendar do leta 2005 še ni bilo nobenega utrjenega pristopa, ki bi oba okvira popolnoma integriral. Zur Muehlen in Rosemann (2005) naredita prvi korak k povezovanju disciplin, predvsem na področju modeliranja tveganj v procesih.

4.1 Povezovanje managementa procesov in operativnih tveganj

Povezovanje obeh disciplin se kaže v več različnih pogledih. MOT je sam po sebi lahko poslovni proces, saj različne stopnje življenjskega cikla MOT sestavljajo proces. Zato ga v sklopu MPP lahko obravnavamo kot ostale poslovne procese. Po drugi strani pa je tveganje pomemben poslovni fenomen, ki ga moramo upoštevati pri vsakem načrtovanju ali prenovi procesov (zur Muehlen & Rosemann 2005; Rikhardsson, Best, Green & Rosemann, 2006, str. 5). V praksi se povezovanje npr. kaže, ko postavljanje notranjih kontrol v procesu,z namenom zmanjšanja tveganj vpliva na potek in razvoj poslovnih procesov. S pomočjo informatizacije, ki je element MPP, se lahko v procesu izognemo tveganjem napak zaradi ročne obdelave, po drugi strani pa prav to lahko prinese dodatna tveganja, kot so odpovedi sistemov, sistemske napake (Majič, 2002). Naslednji dokaz povezovanja je, da je eden izmed pomembnih pokazateljev uspešnosti neprekinjenost poslovanja (angl. *operational continuity*). Da to dosežemo, je potrebno v procesih spremljati notranje dejavnike, ki lahko to preprečujejo. Te smo lahko spregledali pri načrtovanju procesa ali pa so se pojavili šele pri izvajanju in jih je zato potrebno obravnavati kot potencialna tveganja za poslovni proces – operativna tveganja. Napačni vnosi, odpovedi sistemov lahko proces ustavijo in prekinejo tok podatkov, zamude pri izvajanju procesov pa lahko sprožijo verižno reakcijo in pride do zaostanka vseh aktivnosti. Vse to pa preprečuje uspešnost procesa. Zato je mesta v procesu, kjer se takšna tveganja lahko realizirajo, potrebno zmanjšati, izločiti, kar pa je v interesu tako MOT kot tudi MPP (Jallow et al., 2007).

Slika 7: Povezovanje managementa operativnih tveganj in managementa poslovnih procesov



Vir: G. Nota & M. P. Di Georgio, A model for process oriented risk management, 2010, str. 21.

Primer, kako se MPP in MOT povezujeta, je prikazan na sliki 7. V fazi načrtovanja procesov le-te modeliramo, podatke iz teh modelov pa v MOT uporabimo za opredelitev tveganj. Na podlagi teh se vzpostavi pravila ravnanja, kontrole za zmanjšanje tveganj, to pa vpliva tudi na posodobitev modelov procesov. Ko se proces izvaja, MPP nadzoruje uspešnost procesa, MOT pa realizacijo tveganj. Na podlagi merjenja procesov in tveganj zaznavamo napake in škodne dogodke. Pridobljene informacije o izvajanju služijo MOT kot osnova za sprejem ukrepov proti tveganjem, MPP pa prenovi poslovni proces, če se to s poslovnega vidika splača. Odločitev o prenovi mora temeljiti na trenutnem in pričakovanem finančnem vplivu tveganj ter višini stroškov za obvladovanje tveganj (Nota & Di Georgio, 2010; Dickstein & Flast, 2009, str. 157).

Povezovanje obeh disciplin se prične s poslovno strategijo. Da podjetje uspešno sledi tej strategiji, so v skladu z načeli in vrednotami podjetja postavljeni poslovni cilji, pri čemer morata sodelovati tudi MPP in MOT. V ciljih mora biti namreč opredeljeno dopuščanje operativnih tveganj in politike MOT. MPP pa sodeluje pri postavljanju ciljev in skrbi za to, da poslovni procesi potekajo v skladu z njimi (Dickstein & Flast, 2009, str. 99).

Oba življenjska cikla sta torej tesno povezana. Življenjski cikel MOT lahko predstavimo kot niz sledečih aktivnosti: vzpostavitev primernega okolja za management tveganj, identificiranje potencialnih tveganj, spremljanje aktualnih tveganj, aktivni MOT in poročanje. MPP pa sestavljajo aktivnosti: sodelovanje pri postavitvi in pregledu poslovnih ciljev, oblikovanje in prenova poslovnih procesov, modeliranje in simuliranje, vpeljava, izvajanje, nadzor, merjenje procesov ter analiza rezultatov (Dickstein & Flast, 2009, str. 75–76). Aktivnosti obeh ciklov so med seboj močno prepletene. Vzpostavljanje okolja tveganj mora potekati hkrati s postavljanjem poslovnih ciljev in zasnovo poslovnih procesov. Simuliranje modelov procesov je idealni čas za prepoznavo potencialnih tveganj. Prepoznavanje potencialnih možnosti za izboljšavo poslovnega procesa je priložnost, da hkrati najdemo še načine za zmanjšanje potencialnih tveganj v procesu. Med izvajanjem procesa moramo spremljati njegovo uspešnost, spremembe v poslovnem okolju, pomanjkljivosti v kontrolah in morebitne napake. Gre za sočasen nadzor (angl. *ongoing monitoring*), ki je komponenta obeh disciplin. Povežemo pa lahko tudi aktivno obvladovanje tveganj in analizo procesa. Rezultati analize so namreč podlaga za sprejemanje ukrepov za obvladovanje tveganj. Glede na izkušnje iz procesa se krepi in posodablja tudi okolje za obvladovanje tveganj in cilji/strategija (Dickstein & Flast, 2009, str. 75–76).

MOT in MPP se povezujeta tudi posredno, in sicer preko aktivnosti oz. disciplin, ki so povezane z obema. Takšen primer je povezovanje preko zagotavljanja skladnosti (angl. *compliance*) (Rikhardsson et al., 2006, str. 5). Skladnost je osnova poslovanja, saj mora biti podjetje še prej kot vse ostalo skladno z zakonodajo. Potrebno je vzpostaviti procese v skladu z regulativo, pravili, zagotoviti izpolnjevanje pogodbenih obveznosti, doseči dogovorjeno kakovost storitev itn. (Rikhardsson et al., 2006). Vom Brocke in Rosemann (2010b, str. 271–276) nalogo zagotavljanja skladnosti procesov pripisujeta kar MPP (nadzor odstopanj v procesu, zagotavljanje revizijske sledi). Slednji mora torej poskrbeti ne samo za učinkovitost,

ampak tudi za skladnost procesov in temu prilagoditi MPP metode, orodja in tehnike. Skladnost je lahko zahtevana (npr. Basel II, SOX) ali želena (ISO standardi, ITIL) (zur Muehlen, 2007, str. 5). Drugi avtorji (Rikhardsson et al., 2006) pa vidijo skladnost kot del nalog MOT. Le-ta se mora osredotočati na tveganja v primeru neskladnosti in oblikovati kontrole za zagotovitev skladnosti. V kolikor slednje ne zagotovimo, lahko to prinese dodatne stroške, denarne kazni ali pa manj prihodkov zaradi izgube ugleda, kupcev, investitorjev. Po drugi strani pa je ravno zunanja regulativa tista, ki določa, da morajo podjetja meriti tveganja in sezname tveganj, politike obvladovanj pa posodabljati za namene poročanja. Tako lahko ugotovimo, da se MOT in MPP povezujeta tudi preko zagotavljanja skladnosti.

Z vidika povezovanja obeh disciplin v literaturi avtorji omenjajo dva pristopa: procesno usmerjen management tveganj (angl. *Process-oriented Risk Management*) in management poslovnih procesov, usmerjen na tveganja (angl. *Risk-oriented Process Management*). Namen procesno usmerjenega managementa tveganj je, da tveganja obvladujemo na ravni procesov in aktivnosti, ki jih povzročajo. Tveganja obravnavamo kot neločljivi del procesa, pristopi managementa poslovnih procesov pa služijo kot pomoč pri obvladovanju tveganj. Pri managementu poslovnih procesov, ki je usmerjen na tveganja, pa je znotraj nalog in ciljev MPP tudi obvladovanje tveganj, predvsem v povezavi s projekti prenove procesov. Ob prenovi je potrebno analizirati in upoštevati trenutna tveganja, tista, ki jih prenova prinaša, in tveganja, ki bi lahko ogrozila projekte (zur Muehlen & Rosemann, 2005).

4.2 Procesno usmerjen management tveganj

V poslovnih procesih se ustvarja vrednost za kupce, nastajajo produkti in informacije. Proces je uspešno izveden, če izpolnjuje postavljene cilje, je učinkovit, varen in zanesljiv. Uspešno izvedbo pa lahko preprečujejo neželeni dogodki, kot je realizacija operativnih tveganj. Prav odsotnost MOT je zato v precejšnji meri razlog za neuspešne procese (Alhawari, 2008). Operativna tveganja so lahko povezana z aktivnostmi procesov ali s procesnimi elementi (materialom, ljudmi, sistemi). Nastajajo v vseh fazah poslovnih procesov – od stikov z dobavitelji, ustvarjanja dodane vrednosti do prodaje produktov (Skok et al., 2005). Ker pa so "prirojeni del" procesov in lahko preprečujejo doseganje ciljev, kar nekaj avtorjev vidi rešitev v procesno usmerjenemu managementu tveganj (zur Muellen & Rosemann 2005; Rikhardsson et al. 2006). Slednji pomeni, da je potrebno OT opredeliti po posameznih aktivnostih, procesih, oceniti izpostavljenost, vpliv tveganj in v procese dodati kontrolne aktivnosti za zmanjšanje teh tveganj. Da podjetje v kontekstu procesov pravilno uporablja okvir MOT, ga mora "operacionalizirati" (angl. *operationalize*), kot to poimenujeta avtorja Dickstein in Flast (2009, str. 75–76). To pomeni, da ga morajo popolnoma vgraditi v okvir poslovnih procesov in uporabljati pri vsakdanjem poslovanju**.**

Prednost procesno usmerjenega managementa tveganj Fehér (2009, str. 3) vidi v tem, da imajo podjetja boljši pregled nad višino izgub, ki jih je povzročil posamezen proces. S tem pristopom podjetja lažje odkrijejo tudi skrita tveganja. Da jih opazijo, jim ni potrebno čakati na realizacijo teh, ampak jih lahko predvidijo in ukrepajo vnaprej (Interfacing Technologies Corporation, 2011). S povezavo tveganj in poslovnih aktivnosti se lažje osredotočijo na preventivni

management tveganj ter porabijo manj časa za okrevanje po škodnih dogodkih. Tveganja se tako iz groženj spremenijo v planirane aktivnosti poslovnih procesov. V primeru več zaporednih procesov izhodi enega procesa predstavljajo vhode v naslednji proces, kar pomeni, da če se pojavi napaka v enem izmed njih, to vpliva še na vse nadaljnje procese. Zato s pomočjo procesno usmerjenega MOT lahko vzdržujemo tudi neprekinjenost poslovanja (Norimarna, 2010). Dodano vrednost pristopu prinesejo še vzdrževanje baze tveganj in kontrol ter njihovih povezav s poslovnimi procesi, dimenzijami časa in lastništva. S tem podjetja dosegajo tudi skladnost z zakonodajo (Interfacing Technologies Corporation, 2011). Kako pa naj bi procesno usmerjen management tveganj potekal, predlaga več avtorjev.

4.2.1 Faze procesno usmerjenega managementa tveganj

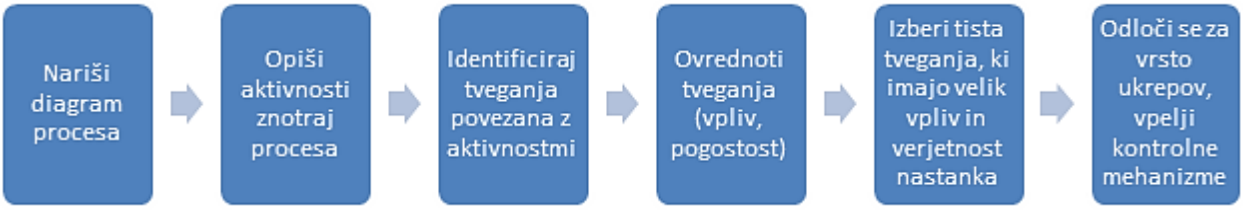
Različni avtorji podajo različno število faz procesno usmerjenega managementa tveganj. Te faze so si med seboj podobne in so sestavljene iz vseh faz okvira MOT (od prepoznave do obvladovanja tveganj). Fehér (2009, str. 14) v svojem okviru predlaga štiri osnovne korake:

- Identificirati procese in jih modelirati, da postanejo pregledni (kdo, kaj, kdaj, kako, s katerimi viri).
- Identificirati tveganja v vseh delih procesa in jih oceniti (kaj lahko prepreči izvajanje aktivnosti, kakšne so zahteve po doseganju kakovosti).
- Planirati kontrole in jih namestiti v proces (za tista tveganja, ki jih ne moremo izločiti).
- Razvijati proces (v smeri zmanjševanja tveganj in izboljšanja procesne učinkovitosti).

Groznik in Vičič (2007) model opišeta v podobnih korakih. Najprej je potrebno identificirati poslovne procese, pri tem pa izbrati samo ključne, da se podjetje deloma izogni kompleksnosti projekta. Sledi modeliranje obstoječega stanja (angl. *As-Is*), pri katerem morajo paziti, da vsi, ki popisujejo, uporabljajo enotno metodologijo z vnaprej določeno ravnjo podrobnosti modeliranja. Na podlagi modelov obstoječega stanja strokovnjaki iz poslovnih področij, procesni analitiki in strokovnjaki za OT skupaj pripravijo predloge izboljšav. Na podlagi informacij o tveganjih izberejo najboljše rešitve ter potrdijo nove modele procesov (angl. *To-Be*). Po sprejetju in vpeljavi prenovljenih procesov v poslovanje sledi spremljava procesov, v katero so vključeni vsi odgovorni za posamezna področja. Na podlagi tega se lahko pokažejo nove zahteve po spremembah. Kot zadnji korak pa avtorja predlagata identifikacijo in vzpostavitev kataloga tveganj. S pomočjo modela poslovnih procesov lahko sistematično prepoznamo operativna tveganja, ki jih ovrednotimo glede na to, ali so potrebna ukrepanja. Ker pa vsa tveganja ne izhajajo iz modela, ampak tudi iz sredstev podjetja, zaposlenih in IS, avtorja za boljšo preglednost predlagata vzpostavitev kataloga tveganj.

Svoj model (slika 8) predstavijo tudi Champagne et al., (2008, str. 45). Za model je značilno to, da prve tri aktivnosti lahko opravijo zaposleni v procesih tudi sami oz. pomagajo strokovnjakom pri tem. Te faze služijo npr. za dokumentiranje procesov ali izdelavo izobraževalnih vsebin o procesih. Zadnje tri aktivnosti pa so v pristojnosti predvsem specializiranih oddelkov in oseb, ki se ukvarjajo z managementom tveganj (notranja revizija, management tveganj).

Slika 8: Potek procesno usmerjenega managementa tveganj



Vir: P. Champagne et al., A Toolkit For Process Mapping for MFIs, 2008, Str.45.

V svojem okviru procesno usmerjenega managementa tveganj Jallow et al. (2007) dodajajo tri pomembne dimenzije uspešnosti procesov, to so stroški, čas in kvaliteta produktov. Analiza stroškov pove, kakšen vpliv na stroške ima lahko tveganje, povezano z določeno aktivnostjo. S tem prepoznamo tveganja, ki jih moramo najprej obravnavati v primeru da je naš cilj znižati stroške procesa. S časovno analizo ugotavljamo, kako tveganje vpliva na čas izvajanja aktivnosti. To omogoča preprečiti zamude v procesih. Analiza kakovosti/uspešnosti se osredotoča na vpliv tveganj na kakovost izhodov iz procesov. Z meritvami ugotovimo, katera tveganja povzročijo, da je odstopanje produkta izven dopustnih meja. Ob tem avtorji v kontekst poslovnih procesov vpeljejo okvir managementa tveganj, ki ga je predstavila organizacija »Committee of Sponsoring Organizations of the Treadway Commission« (v nadaljevanju COSO). COSO okvir je celovit okvir procesa managementa tveganj, ki gleda na tveganja s perspektive celotnega podjetja in je precej razširjen, še posebej v finančnem sektorju. Vsebuje sledeče korake:

- **Modeliranje aktivnosti** v poslovnem procesu. V tem koraku natančno opredelimo, iz katerih aktivnosti je sestavljen proces. To omogoča, da kasneje tveganja ne opredelimo za celotni proces, ampak bolj podrobno, na ravni aktivnosti.
- **Določitev ciljev**. Poslovne procese lahko ocenimo glede na tri dimenzije, to so stroški, čas in uspešnost. Če proces razdelimo na aktivnosti, lahko po njih razdelimo tudi stroške in čas (uspešnost težje) ter glede na to ocenimo tveganja. Zato je ključno, da določimo cilje v zvezi s tveganji oz. na katera tveganja se bomo osredotočili – tista, ki preprečujejo, da bi bil proces izveden v času, v mejah proračuna, ali tista, ki se kažejo preko vnaprej definiranih KRI, itn.
- **Identificiranje dejavnikov tveganj, verjetnosti nastanka in vpliv**. V tem koraku identificiramo notranje in zunanje dejavnike tveganja za vsako posamezno aktivnost procesa, vzroke za nastanek tveganj in posledice. Ko so tveganja identificirana, moramo ugotoviti še verjetnost njihovega nastanka in obseg vpliva.
- **Izračun tveganja.** Avtor predlaga, da za vsak prepoznani dejavnik tveganja izračunamo velikost tveganja, in sicer tako, da pomnožimo verjetnosti nastanka z obsegom vpliva.
- **Izračun napovedi.** Okvir predlaga dve različni napovedi tveganj, eno za vsako posamezno aktivnost, drugo pa skupno za celotni poslovni proces. Napoved upošteva kumulativno vrednost vseh tveganj, ki so bili identificirani za posamezno aktivnost. Napoved za poslovni proces pa je vsota tveganj vseh aktivnosti. To služi kot signal, v katerih procesih je potrebno ukrepati.

Tem korakom pa v svojem okviru procesno usmerjenega MOT zur Muehlen (2007) doda še, da nato s pomočjo različnih strategij managementa tveganj izberemo najprimernejše kontrolne aktivnosti. Sledi neprestano spremljanje tveganja, kar pomaga aktivno obvladovati tveganja in jih zmanjševati na dopustno raven. Kot pa je predlagal že Feher (2009), je hkrati z razvojem procesa potrebno posodabljati tudi seznam KRI. Ti morajo biti povezani s procesno uspešnostjo in za podjetje predstavljati zgodnji opozorilni sistem, da v procesih nekaj odstopa od normalnega stanja. Pri vsem tem pa moramo upoštevati, da se podjetjem ne splača obvladovati vseh OT. Da ne bi potrošili preveč virov, morajo v podjetju presoditi, katera tveganja so relevantna.

Vičič in Groznik (2007) ob vpeljavi povezovanja MPP in MOT opozarjata, da mora biti podjetje procesno usmerjeno. Uvedba tega področja je lahko zahtevna in pogojena z organizacijskimi in tehnološkimi spremembami ter zahteva izvedbo številnih dolgoročnih projektov z visoko stopnjo tveganja. Zato morajo pri uvedbi sodelovati strokovnjaki z omenjenih področjih, cilji uvedbe pa morajo biti vnaprej jasno opredeljeni in v skladu s strategijo podjetja.

4.2.2 Informacijska podpora in procesno usmerjen management tveganj

Vloga novodobne informacijske podpore ni samo podpora procesom, ampak tudi managementu tveganj v procesih, torej procesno usmerjenem managementu tveganj. Določeni sistemi omogočajo modeliranje, simuliranje procesov, kar je osnova za ugotavljanje tveganj (primer uporabe simulacij za ocenjevanje tveganj je prikazan v Trkman in McCormack (2010)). Drugi celoviti sistemi so podpora procesom. Z njimi zmanjšujemo tveganja, v procesih so postavljene avtomatizirane kontrole. Sistemi, ki omogočajo spremljanje procesov v izvajanju, hkrati služijo tudi za pridobivanje podatkov o tveganjih. Zato Weiß & Winkelmann (2011) vidita potencial v nadaljnjem razvoju celovitih sistemov, ki bi še bolj temeljili na povezavi MPP in MOT, še posebej na področju analize poslovnih procesov in OT znotraj njih.

Basel II spodbuja podjetja, da razvijajo metodologije in tehnike za zbiranje podatkov, merjenje in spremljanje OT (Rikhardsson et al., 2006). Temu gredo naproti tudi novodobni sistemi. Sistemi za krmiljenje delovnih tokov (WfMS) omogočajo npr. avtomatično zbiranje podatkov iz izvajanj poslovnih procesov, ki služijo za namene nadzornih mehanizmov, orodij za podporo odločanju itn. (Jallow et al., 2007). Aplikacije za simulacijo poslovnih procesov omogočajo lažje vnaprejšnjo ugotavljanje kritičnih točk in OT. S pomočjo meritev in hranjenja podatkov o preteklih izgubah lahko podjetja že vnaprej ocenijo tudi tveganja v podobnih procesih (Dickstein & Flast, 2009, str. 75–76).

Zaradi deregulacije, globalizacije finančnih storitev in napredka tehnologije na področju finančnega poslovanja postajajo dejavnosti bank vse bolj zapletene, z njimi pa tudi oblike tveganj. Vpeljava IT je lahko eden izmed ukrepov za zmanjšanje teh tveganj, po drugi strani pa je prav IT lahko tudi vir tveganj oz. ima povečanje avtomatizacije lahko negativni vpliv (Majič, 2002). Z vpeljavo informacijskih sistemov npr. zmanjšamo tveganja napak pri ročni obdelavi, s tem pa pridobimo nova. Če je sistem nezanesljiv, se tveganja napak pri vnašanju spremenijo v

tveganja sistemskih napak. Preko povečanega obsega e-poslovanja se podjetja soočajo z vprašanji varnosti sistemov in tveganja prevar od zunaj. Tako se lahko tveganja, ki so bila prej pogosta, a so imela majhen vpliv, spremenijo v redka, a z velikim vplivom (Sackmann, 2008). Povečana odvisnost poslovnih procesov od IT lahko posredno vpliva tudi na izgubo v podjetju zaradi nedelovanja sistemov. Bančni revizorji, managerji tveganj in lastniki procesov sicer stremijo k optimiziranim, standardiziranim in avtomatiziranim procesom, vendar želijo, da imajo le-ti dobro (informacijsko podprto) revizijsko sled (Cernauskas & Tarantino, 2009).

4.2.3 Modeliranje tveganj v procesih

Eppler in Aeschimann (2009) poudarjata, da je vizualizacija tveganj pomembna za MOT. Poleg kognitivnih prednosti ima vizualizacija pomembno vlogo tako pri ocenjevanju kot tudi pri sporočanju in razumevanju tveganj. Rikhardsson et al. (2006) menijo, da je potrebno obravnavati tveganja kot elemente vsakega procesa in je zato procesne modele smotrno povezati z OT. S pomočjo modeliranja tveganj znotraj procesov (angl. *risk-aware process modeling*) izboljšamo vidnost tveganj, saj modeli, razširjeni s tveganji, pokažejo bolj točno sliko, kako procesi potekajo ter kje so nevarnosti znotraj njih (Rotaru et al., 2011). V modele procesov poleg tveganj lahko dodamo tudi procesne kontrole za obvladovanje teh tveganj. Da pa lahko čim bolj točno identificiramo tveganja znotraj modela, je potrebna dekompozicija procesa na nižje ravni (zur Muehlen & Rosemann, 2005). Potencialna tveganja lahko dodelimo točno določenim aktivnostim in jih povežemo z zato namenjenimi kontrolami (Interfacing Technologies Corporation, 2011). To daje zaposlenim možnost, da bolje razumejo, s kakšnimi tveganji se lahko srečajo med izvajanjem njihovih aktivnosti in kako morajo ukrepati, da tveganja ne bodo imela širšega vpliva (Majič, 2002). Problem pa je, da velikokrat ni popolnoma jasne povezave med tveganji in elementi procesa, saj je tveganje rezultat kompleksnih interakcij med več elementi procesa. Bankam modeliranje pomaga pri dokumentiranju tveganj, boljša dokumentacija pa se jim obrestuje v nižjem zahtevanem vezanem kapitalu za kritje morebitnih OT (Weiß & Winkelmann, 2011).

Modeliranje procesno usmerjenega managementa tveganj je še vedno v začetnih fazah. Rikhardsson et al. (2006) pravijo, da je v uporabi malo metod in orodij, s katerimi bi lahko dosledno modelirali tveganja po procesih. Metoda za modeliranje in opis tveganj bi morala biti integrirana v jezike za modeliranje poslovnih procesov (Interfacing Technologies Corporation, 2011). Večina avtorjev, ki so to poskušali vpeljati, je uporabila razširjeno tehniko EPC, ki počasi izgublja svojo vrednost, saj »de facto« standard modeliranja procesov postaja BPMN (vom Brocke & Rosemann, 2010b, str. 171). Slednji pa modeliranja tveganj znotraj modelov še ne omogoča. Pomanjkljivost simbolov v BPMN je izpostavil tudi Recker (2010), saj notacija npr. ne vsebuje simbola za »poslovno pravilo«. Med drugim je tudi mnenja, da so dodatni grafični simboli pomembni za boljše razumevanje modelov s strani uporabnikov. Korak naprej sta poskušala narediti Weiß in Winkelmann (2011) s pomočjo novega semantičnega pristopa modeliranja SBPML (angl. *Semantic business process modeling*), ki omogoča modeliranje poslovnih procesov in tudi njihovo analizo za različne namene: šibkosti v procesih, odločitve o

IT investicijah, omogoča pa tudi modeliranje OT. Problem je, da ta notacija še ni razširjena in je večina orodij za modeliranje ne podpira.

Zato sem se odločila, da bom v svoji magistrski nalogi sicer uporabila notacijo BPMN, a jo bom razširila s simbolom za operativna tveganja. Tega bom vzela in priredila iz notacije SBPML. Gre za opozorilni trikotni simbol, znotraj katerega je oznaka »OT« – operativna tveganja, kot je razvidno na sliki 9 (v originalu angl. *OR- operational risk*).

Slika 9: Simbol za operativna tveganja

Vir: B. Weiß & A. Winkelmann, Developing a Process-oriented Notation for Modeling Operational Risks, 2011, str. 6.

4.3 MPP in MOT v bankah

Vsako izvajanje posameznega procesa ima vpliv na doseganje ciljev poslovnega procesa in s tem strateških ciljev. Zato lahko sklepamo, da banke, ki OT merijo in obvladujejo na ravni procesov, s tem pripomorejo k doseganju strateških ciljev (Jallow, 2007). MPP je v bankah pomemben, saj je veriga vrednosti razdeljena v neodvisne organizacijske enote in je zato potrebna koordinacija medfunkcijskih procesov. Management informacij je osrednja aktivnost bančništva, zato je vpliv tehnoloških inovacij v procesu lahko še večji kot v drugih panogah (Trkman, 2010, str. 127). Za banke so značilni procesi, ki temeljijo na informacijah in znanju, v angleščini jih imenujemo "*knowledge intensive*". Tovrstni procesi so redko popolnoma avtomatizirani in rutinski, saj so večinoma kompleksni, vzamejo precej časa in zahtevajo delitev informacij. Ti procesi so tudi velik vir OT. Zaposleni uporabljajo svoje specialno znanje za izvajanje procesov in po eni strani predstavljajo določena tveganja za banko (slab pregled kreditne dokumentacije), po drugi strani pa hkrati obvladujejo tveganja (zavrnejo slabe kreditne vloge) (Weiß & Winkelmann, 2011). Iz tega sledi, da sta v bančništvu za doseganje strateških ciljev in poslovni uspeh bank pomembna tako MPP kot tudi MOT. Banke potrebujejo dober pregled nad procesi, saj jim realizacija tveganj lahko prinese tako finančne kot tudi nefinančne posledice. Zato je ključno, da se čim več tveganjem izognejo ali z ukrepi obvladovanja tveganj in managementa procesov omilijo njihove posledice (Norimarna, 2010).

Študijo primera finančnega podjetja, kjer se je povezovanje MOT in MPP obrestovalo, predstavi Tozer-Pennington (2009). Gre za podjetje *Capital One Financial Corporation*, kjer so s pomočjo tehnik MPP pri obvladovanju tveganj dosegli boljšo kakovost MOT in istočasno izboljšali poslovno uspešnost in donosnost naložb (ROI). Podjetje je vpeljalo okvir procesno usmerjenega managementa tveganj. Za MPP in MOT so postavili standard, v katerem so določili osnovni nivo zahtev glede procesov in tveganj. Za doseganje tega standarda so morale organizacijske enote narediti procesno arhitekturo in vsako poslovno aktivnost prikazati znotraj enega izmed poslovnih procesov. Med temi so prepoznali kritične procese, ki bi lahko imeli resen vpliv na poslovanje. Postavili so prioritete za obravnavanje tistih procesov, kjer je bilo tveganje visoko in bi z njihovim obvladovanjem pridobili največ. Razvili so orodje, ki pomaga

lastnikom kritičnih procesov dosegati osnovne procesne zahteve. Procesi morajo imeti jasne cilje, dobre kontrole, ocenjena tveganja in planirane ukrepe v primeru realizacij tveganj. Sproti pa morajo ažurirati tudi seznam kritičnih procesov. Ob spremembi okolja tudi procesi, ki prej niso bili kritični, lahko to postanejo.

MOT se pri Capital One prične z identificiranjem kritičnih procesov, modeliranjem OT znotraj njih in na koncu z oblikovanjem kontrol za obvladovanje teh tveganj. Po modeliranju in spremljanju procesov preko kazalnikov zaposleni točno vidijo, kaj se s procesi dogaja. Tako lahko tudi sami identificirajo dele procesov, kjer je možnost za tveganja, in hitreje ukrepajo. Z boljšo kontrolo in zagotavljanjem revizijske sledi so v podjetju izboljšali uspešnost managementa tveganj in zagotovili skladnost poslovanja. Obenem se je izkazalo, da so tiste poslovne enote, ki svoje procese stalno izboljšujejo z intenzivnim MPP, tudi precej bolj uspešne pri zmanjševanju tveganj.

Pri Capital One opozarjajo, da takšen pristop za veliko podjetje lahko pomeni precej porabljenega časa in denarja. Najtežja je vzpostavitev primernega okolja. Potreben je intenziven management sprememb in naklonjenost vodstva. Če se podjetje tega loti na pravi način, sama vpeljava ni nujno draga. Ogromne investicije v tehnologijo niso potrebne, saj sta sprememba kulture podjetja in pridobitev realnega vpogleda v obstoječe procese lahko izvedena že z osnovnimi, obstoječimi IT rešitvami. V Capital One so presodili, da se jim bolj izplača, da (namesto da najamejo zunanje izvajalce za modeliranje procesov), izobrazijo zaposlene, ki to naredijo sami. Obenem so jih spodbudili k temu, da tudi sami nadzirajo in obvladujejo tveganja v procesih, ki jih izvajajo. Če je management tveganj del vsakdanje službe nekoga, se ta trudi stalno nadzorovati spremembe v procesu, produktih ali poslovnem okolju. S tem se sicer zvišajo stroški dela zaposlenih, vendar gre precej manj denarja za odpravo posledic realiziranih tveganj. V Capital One zagovarjajo, da če bi banke bolje razumele in dokumentirale svoje procese, omogočale vpogled v njih, vpeljale politike MPP, vzpostavile kontrole, avtomatizirale procese, bi se lahko izognile mnogim problemom in morda tudi finančni krizi (Tozer-Pennington, 2009).

5 PRIMER UPRABE MANAGEMENTA POSLOVNIH PROCESOV IN MANAGEMENTA OPERATIVNIH TVEGANJ NA PROCESU IZVRŠEVANJA IZVRŠB V SLOVENSKI BANKI

V praktičnem delu bom na podlagi pridobljenih teoretičnih znanj poskušala predlagati, kako bi lahko uporabili MPP kot pomoč MOT na konkretnem primeru. Želim predstaviti primer, ki bo lahko služil kot podlaga za nadaljnje razvijanje proučevanega procesa v smeri zmanjševanja tveganj. V splošnem pa lahko primer služi kot predlog za obvladovanje tveganj na podobnih procesih v podjetjih, kjer je MOT zelo pomemben.

5.1 Metodologija in uvod v praktični del

Analizo procesa bom izvedla po korakih procesno usmerjenega managementa tveganj, ki sem ga predstavila v teoretičnem delu (slika 8). Pri tem bom prikazala uporabo MPP (analiziranje,

modeliranje procesov, prenova, informatizacija) in MOT (določitev kritičnih točk, opredelitev OT po aktivnostih, vizualizacija tveganj, predlogi za obvladovanje tveganj). S spremljanjem in vizualizacijo tveganj po podprocesih bom pridobila bolj jasno sliko o tem, s tem pa tudi boljšo podlago za ukrepanje. Za primer sem izbrala eno izmed slovenskih bank, znotraj nje pa proces izvršb. Podatki, uporabljeni v analizi, so resnični, je pa naziv banke zaradi varovanja zaupnih podatkov skrit in bom zato uporabljala kar izraz » Dobra banka«.

Dobra banka je ena večjih slovenskih bank, ki se v zadnjem obdobju še posebej trudi iskati nove pristope, veliko investira v informatizacijo in obvladovanje tveganj ter v procesni usmerjenosti podjetja vidi dolgoročno priložnost za konkurenčnost in boljšo prilagodljivost spremembam v okolju. V sklopu vseh aktivnosti, ki jih zaposleni izvajajo za doseganje procesno usmerjenega podjetja, si želijo OT povezati s procesi, saj v tem vidijo lažji način obvladovanja tveganj. Tveganja so bila namreč do sedaj opredeljena po organizacijskih enotah in je bilo slabše razvidno, katere aktivnosti v procesih so predstavljale tveganja. Zato bi rada s prikazom procesa in primera banki predstavila okvir, kako opredeliti tveganja po procesih, jih s pomočjo modeliranja vizualizirati in s tem lažje obvladovati. Najbolj pogost bančni proces v literaturi je sicer proces kreditiranja, jaz pa sem se odločila za manj proučevanega, proces izvrševanja izvršb.

Da predstavim ozadje, bom najprej opisala izvršbe na splošno, celoten potek uvedbe izvršb, potem pa se bom osredotočila na izvršilni del postopka v primeru izvršb na sredstva pri organizaciji za plačilni promet. Konkretno, predstavila bom, kako proces izvrševanja sklepov o izvršbi poteka znotraj Dobre banke. Ker proces izvršb v tej banki prej še ni bil podrobno modeliran, bom v drugem delu naredila podrobne modele celotnega procesa in ga s tem naredila preglednejšega. Najprej bom predstavila krovni proces, potem pa še njegove podprocese. V Dobri banki so bila do sedaj OT vrednotena po oddelkih, sedaj pa bom tveganja opredelila po procesu in aktivnostih. Znotraj modelov bom zato vizualizirala operativna tveganja, ki jih bom identificirala na podlagi lastne analize poročil o realiziranih in potencialnih škodnih dogodkih. Ker notacija BPMN, s katero bom proces modelirala, ne omogoča modeliranja tveganj, bom v notacijo dodala simbol za OT. Na podlagi lastnih ugotovitev bom predstavila glavne kritične točke z vidika tveganj, ter za nekaj izmed njih predlagala, s katerimi ukrepi oz. kontrolami jih lahko zmanjšamo ali omejimo možnost njihovega nastanka. Na primeru prvega podprocesa pa bom prikazala, kako se lahko proces razvija v smeri optimizacije in zmanjševanja tveganj s pomočjo MPP (prenove in informatizacije).

Podatke o procesu izvršb sem pridobila iz različnih organizacijskih enot Dobre banke: Oddelka za management tveganj, Oddelka za management procesov in Oddelka podpore plačilnemu prometu (v nadaljevanju OPPP). Vse tri enote so za svoje potrebe ločeno ustvarile dokumentacijo o procesu izvršb. Proces je bil modeliran samo na višji ravni abstrakcije, podatki o OT pa niso bili določeni po procesu oz. aktivnostih, ampak po oddelkih.

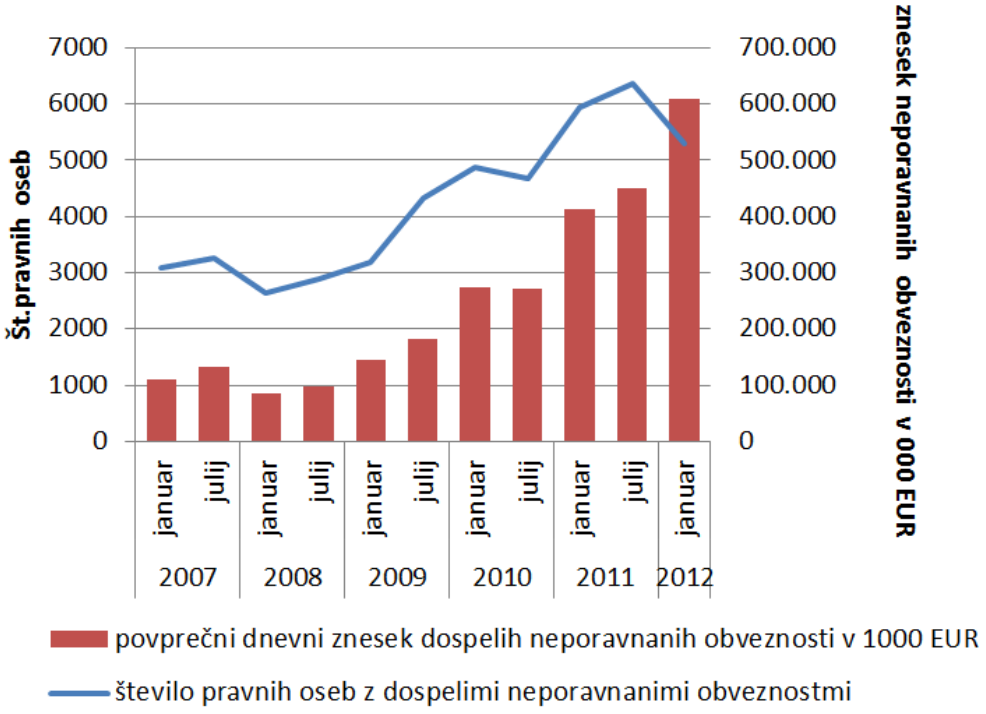
Podrobnosti o procesu in tveganjih sem pridobila preko intervjujev zaposlenih in z analizo sekundarnih virov podatkov. Intervjuje sem izvedla posamično, z več različnimi zaposlenimi: z

izvajalcem procesa, programerjem aplikacije Izvršbe, procesnim analitikom, dvakrat z vodjo procesa in trikrat z managerjem operativnih tveganj. S slednjima sem vzpostavila stik že pri načrtovanju magistrske naloge in na koncu pri pregledovanju točnosti podatkov, z ostalimi pa med pisanjem magistrske naloge (ko sem potrebovala določene informacije). Druge podatke sem pridobila s pregledom navodil za delo, pravilnikov za izvajanje aktivnosti v omenjenih organizacijskih enotah, navodil za izvrševanje sklepov o izvršbah s strani Združenja bank Slovenije, z analizo poročil o škodnih dogodkih (od leta 2008 do 2012) ter s pregledom zakonodaje na področju izvršb, bančništva in plačilnih storitev. Izpise škodnih dogodkov sem pridobila iz baze škodnih dogodkov, ki jo v banki v okviru managementa tveganj redno ažurirajo in v katero organizacijske enote sproti poročajo o realiziranih škodnih dogodkih. Omenjeno zbiranje podatkov sem izvedla med marcem 2012 in februarjem 2013, rezultate pa so v banki pregledali v maju 2013.

5.2 Ozadje izvršb

Vzrok za vedno večje število izvršb je plačilna nedisciplina. Ta se po mnenju Gospodarske zbornice Slovenije (2010) v našem sistemu pojavlja že več desetletij. Z nastopom gospodarske krize se je še precej povečala in zastoji plačil okrepili. Na to kažejo tudi statistični podatki o dospelih neporavnanih obveznostih v evidenci AJPES (Poslovni subjekti z dospelimi neporavnanimi obveznostmi po mesecih in dnevih, 2011; Poslovni subjekti z dospelimi neporavnanimi obveznostmi nad 5 dni neprekinjeno, 2012). Ker pa omenjena evidenca ne vsebuje vseh neporavnanih obveznosti iz naslova neplačanih računov med dolžniki in upniki, pomeni, da je dejanski obseg neplačevanja še precej večji.

Slika 10: Pravne osebe z dospelimi neporavnanimi obveznostmi od 2007 do 2012



Vir: Poslovni subjekti z dospelimi neporavnanimi obveznostmi po mesecih in dnevih, 2011.

Če primerjamo mesec januar 2007 in januar 2012, lahko s slike 10 razberemo, da se je število pravnih oseb z dospelimi neporavnanimi obveznostmi povečalo s 3086 na 5283 (za 71 %), medtem ko se je povprečni dnevni znesek neporavnanih obveznosti povečal za kar 5,47 krat, in sicer s 111.124.408 na 608.278.000 EUR. Povečuje se število sodnih in davčnih izvršb in posledično tudi sklepov, ki jih prejmejo banke v izvrševanje. V januarju 2012 je bilo npr. 68.489 zadev v blokadah (posamičnih zadev, ki se nanašajo na neporavnane obveznosti), od tega je bil povprečni dnevni znesek dospelih neporavnanih obveznosti iz naslova sodnih sklepov o izvršbi 497.190.000 EUR (80 % celotnega zneska) in iz naslova davčnega dolga ter stroškov davčne izvršbe 110.759.000 EUR (Poslovni subjekti z dospelimi neporavnanimi obveznostmi po mesecih in dnevih, 2011). Število izvršb sicer ne narašča sorazmerno z rastjo plačilne discipline. Razlog za to je med drugim ta, da je vedno več uvedb stečaja in prisilne poravnave, ti pa prekinejo postopek izvršbe (Križnik, 2012).

5.2.1 Pravna izterjava dolgov

Medtem ko plačilna disciplina narašča in posledično z njo tudi nevarnost propada podjetij, je ključna učinkovita izterjava dolgov. Izterjava združuje vsa poslovna pravila, procese in deležnike, ki vplivajo na čim boljše razmerje med prihodki (terjatvami) in ustreznimi prilivi (Lampret & Mislej, 2011, str. 12). Podjetja se v ta namen poslužujejo različnih načinov izterjave terjatev. Najprej pričnejo z opominjanjem, telefonskimi izterjavami, možnostjo kompenzacije itn. V kolikor pa dolžniki še vedno ne poravnajo dolgov in upniki ugotovijo, da dogovor ne bo mogoč, je terjatve možno izterjati po sodni poti, in sicer preko izvršb. Lampret in Mislej (2011, str. 12) znotraj tega ločita »mehke« in »trde« pristope k izterjavi. Mehki pristop je uporabljen predvsem v zgodnjih fazah dolžniškega razmerja. Gre za aktivnosti opominjanja preko telefonskih klicev in pošiljanja dopisov o neplačanih zapadlih terjatvah. Trdi pristop pa predstavlja uporabo vseh pravnih možnosti, da upniki dobijo povrnjene svoje terjatve (izvršbe).

5.2.2 Definicija izvršb in izvršilni postopki

Infranca (2009) izvršbo definira kot zaseg premoženja dolžnika ali prodajo njegovega premoženja, s čimer se ugodi razsodbi v korist upnika in se poplača njegove terjatve**.** Izvršba so procesna in materialna dejanja, ki nevestnega dolžnika prisilijo k izpolnitvi obveznosti (Križnik, 2012). Če dolžnik ne povrne dolga, imajo upniki zakonsko pravico zaseči dolžnikovo premoženje in zaslužke v vrednosti njihovih terjatev. Sodna izvršba je zato pravni proces, v katerem sodišče na zahtevo upnika odredi prenos ali prodajo določenega dolžnikovega premoženja v dobro upnika (Chatterjee & Gordon, 2011).

Izvršba na denarno terjatev dolžnika (angl. *garnishment*) je sodni postopek, v katerem upnik (ali potencialni upnik) zahteva sodišču, da odredi tretji osebi, ki dolguje ali hrani sredstva dolžniku, naj preda upniku premoženje dolžnika (npr. plača, sredstva na bančnih računih). S tem ima dolžnikov dolžnik prepoved predati ta sredstva dolžniku oz. ima dolžnik prepoved ta sredstva izterjati (Chatterjee & Gordon, 2011). Podobno definicijo poda Infranca (2009), ki za izvršbo na osebni dohodek (angl. *attachment of earnings*) smatra proces, v katerem upnik

izterja denarne terjatve dolžnika ali dolžnikovega delodajalca. Gre za rubež plače in njen prenos k upniku. Proces vključuje tri različne osebe: poleg dolžnika in upnika je tu še tretja oseba, to je dolžnik dolžnika (angl. *garnishee*), do katere ima dolžnik terjatve oz. zanj hrani premoženje.

Izvršilne postopke ureja več zakonov, eden najpomembnejših je Zakon o izvršbi in zavarovanju (Ur.l. RS, št. 3/2007-UPB4, 93/2007, 6/2008 Skl.US: U-I-354/07-6, 37/2008-ZST-1, 45/2008-Zarbit, 113/2008 Odl.US: U-I-344/06-11, 28/2009, 47/2009 Odl.US: U-I-54/06-32 (48/2009 popr.), 57/2009 Skl.US: Up-1801/08-10, U-I-237/08-10, 51/2010, 26/2011, 14/2012, v nadaljevanju ZIZ). V 16. členu ZIZ sta opredeljeni obe stranki v postopku: upnik je oseba, na zahtevo katere se vodi postopek izvršbe, dolžnik pa oseba, proti kateri se uveljavlja ali zavaruje terjatev. Dida Volk (2004, str 25) loči izvršilni postopek na dovolilni in izvršilni del. Prvi se prične, ko upnik predlaga izvršbo, in zaključi, ko je sklep o izvršbi pravnomočen. Po izdaji sklepa se prične izvršilni del in konča, ko je izvršba opravljena ali ustavljena. Če gre za izvršilni naslov, se lahko ta del prične že pred pravnomočnostjo, vendar upnik do pravnomočnosti ne more biti poplačan.

Sodna izvršba je v skladu z ZIZ (17. in 23. člen) možna na podlagi verodostojne listine ali izvršilnega naslova. Izvršilni naslovi so lahko izvršljiva sodna odločba in sodna poravnava, izvršljiva odločba v upravnem postopku, izvršljiv notarski zapis ali druga listina, za katero zakon določa, da je izvršilni naslov. Verodostojna listina je lahko faktura, obračun obresti, menica, ček s protestom in povratnim računom, javna listina, izpisek iz poslovnih knjig, overjen s strani odgovorne osebe, po zakonu overjena zasebna listina in listina, ki ima po posebnih predpisih naravo javne listine.

5.2.3 Izvršba na podlagi verodostojne listine

Postopek za izvršbo na podlagi verodostojne listine (v nadaljevanju VL) lahko upniki sprožijo sami ali pa s pomočjo pravnih podjetij. Eden izmed vzrokov za veliko povečanje števila izvršb v zadnjih letih je tudi ta, da je postopek leta 2008 postal preprostejši za stranke, saj je bil pri okrajnem sodišču v Ljubljani ustanovljen Centralni oddelek za izvršbo na podlagi verodostojne listine (v nadaljevanju COVL), na katerega imajo upniki možnost sami elektronsko vlagati izvršilne predloge preko portala (Mihajlović, 2012). Do ustanovitve COVL leta 2008 je izvršbo na podlagi verodostojne listine vodilo vsako izmed 44 okrajnih sodišč. Postopki za izdajo sklepa so lahko trajali več kot pol leta, kar je bilo veliko breme gospodarstvu. Danes pa se predloge vlaga centralizirano na COVL in kar 84 % zadev je odločenih v roku petih delovnih dni. S tem so se bistveno zmanjšali zaostanki na sodiščih, izboljšala se je učinkovitost sodišč v izvršilnih postopkih. To je omogočila avtomatizacija in informatizacija postopka izvršb na podlagi VL. Informacijski sistem omogoča preprosto in hitro vlaganje predlogov v elektronski obliki, vlaganje predlogov po klasični poti pa izumira, saj upniki v papirnati obliki vložijo le še 2,4 % predlogov. Že v prvem letu delovanja so prejeli 130.771 predlogov za elektronsko izvršbo na podlagi VL, v letu 2011 pa je število naraslo na 218.789. Po vzoru izvršbe na podlagi VL od marca 2012 omogoča odvetnikom elektronsko vlaganje predlogov za izvršbo tudi na podlagi pravnomočne sodbe (izvršilnega naslova) (Mihajlović, 2012).

Postopek za uvedbo izvršbe na podlagi ZIZ določa Pravilnik o obrazcih, vrstah izvršb in poteku avtomatiziranega izvršilnega postopka (Ur.l. RS, št. 104/2011). Upnik na podlagi dokaza, da njegova terjatev obstaja (izvršilni naslov ali verodostojna listina) izpolni predpisan obrazec v fizični obliki ali elektronsko preko spletne strani COVL. V predlogu mora navesti točne podatke o sebi, dolžniku (v kolikor z njimi razpolaga), verodostojni listini (vrsta, datum, zapadlost, znesek, valuta itn.) oz. izvršilnem naslovu, predlaganih sredstvih izvršbe in druge podatke: pogodbene, zamudne obresti, podatki o izvršitelju. Pomemben del obrazca so sredstva izvršbe. Upnik sam predlaga na katera sredstva dolžnika želi, da se izvrši izterjava terjatve. Če ima točne podatke o sredstvih, s katerimi dolžnik razpolaga, jih navede v predlog, lahko pa izbira med sledečimi izvršilnimi sredstvi (ZIZ, 30. člen): premičnine, nepremičnine, stavbna pravica, delež družbenika v družbi, vrednostni papirji in denarna sredstva, terjatve dolžnika (plača in drugi stalni denarni prejemki, denarna sredstva pri organizaciji za plačilni promet, druge denarne terjatve). Upnik nato plača sodno takso, po plačilu pa sodišče izda sklep o izvršbi, ki ga posreduje obema strankama v postopku.

5.2.4 Izvršba na denarna sredstva pri organizaciji za plačilni promet

Organizacija za plačilni promet je po ZIZ (v 14. in 140. členu) banka ali hranilnica, pri kateri ima dolžnik denarna sredstva na osebnem računu. Sodišče sklep o izvršbi na denarna sredstva vroči banki in ji naloži, naj blokira dolžnikova sredstva v višini obveznosti in po pravnomočnosti sklepa ta znesek izplača upniku. Izvršba na banki se torej prične z "zamrznitvijo" premoženja oz. z omejitvijo, s katero se blokira sredstva na računu imetnika do zaključka poplačila. Ko je sklep pravnomočen, banka opravi rubež sredstev in jih prenese na transakcijski račun upnika (ZIZ, 45., 136. in 138. člen). Terjatve banka poravna po zakonsko določenem vrstnem redu. Če ob prejemu sklepa na računu ni dovolj sredstev, se zadrži sklep in se nadaljuje s poplačilom ob naslednjem prilivu sredstev, če le-ta niso izvzeta iz poplačila. Izvršbo na podlagi davčnega ali sodnega sklepa lahko torej opredelimo kot poseg na transakcijski račun komitenta (v nadaljevanju TRR) brez pooblastila imetnika računa. Za ostale posege na TRR mora namreč banka pridobiti pisno soglasje, pogodbo, plačilni nalog komitenta itn. (Nadzorni svet Združenja bank Slovenije, 2007).

Banka prejema v izvršitev sklepe različnih izdajateljev. Sodni sklep o izvršbi izda sodišče, in sicer na podlagi ugoditve ali zavrnitve predloga za izvršbo. Sklep o davčni izvršbi izda Davčna uprava Republike Slovenije (DURS) ali drugi zakonsko upravičeni izdajatelji, ki želijo izterjati obveznosti: Carinska uprava Republike Slovenije (CURS), Kmetijsko gozdarska zbornica Slovenije (KGZS) in Radiotelevizija Slovenije. Davčni sklepi so izvršljivi takoj ob prejemu, sodni pa so lahko pravnomočni ali nepravnomočni. Banka je v tem primeru v vlogi izvrševalca sklepov, torej izvršitelj. Ob tem ne presoja, ali je izvršba pravilna in dopustna, ampak le izvršuje navodila, kot jih je v sklepu izdal izdajatelj, oz. je dolžna sklepe izvrševati, kot se glasijo. Zato banka v primeru da se dolžnik ne strinja z izvrševanjem, teh zadev ne rešuje sama, ampak predlaga, da dolžnik pošlje ugovor izdajatelju. Prav tako banka izvršuje samo sklepe, ki jih prejme s strani izdajatelja in ne neposredno s strani upnika (Nadzorni svet Združenja bank

Slovenije, 2007; Dobra banka, 2010b). Banka mora sklepe izvrševati dosledno, saj za izvrševanje nosi odškodninsko odgovornost.

Banka mora biti zelo pazljiva, da sklepe izvršuje v skladu z zakonom, saj je za izvedbo odškodninsko odgovorna. Sodišče lahko na željo upnika od banke zahteva, da poravna vse zneske sredstev, ki neupravičeno niso bili zarubljeni in izplačani upniku. Banka mora na zahtevo sodišča posredovati tudi vso dokumentacijo, ki dokazuje, kako je banka izvršila sklep. Če banka ne bi ravnala v skladu z zakonom in odredbo v sklepu, lahko upnik od banke zahteva povrnitev nastale škode, enako velja za dolžnika. Če bi npr. referent po pomoti pri vnosu zneska vnesel samo eno "0" preveč, s tem ne bi upošteval obsega in načina plačila obveznosti iz sklepa. Dolžnik bi bil oškodovan, upnik ne bi hotel vrniti denarja, škodo pa bi krila banka. Škodni dogodek bi nastal tudi, če banka ne bi upoštevala zakonskih določb o vrstnem redu poplačevanja in bi določene sklepe neupravičeno reševala prioritetno. Banka torej odgovarja za vso škodo, ki bi nastala zaradi nepravilne izvršitve sklepa o izvršbi (Nadzorni svet Združenja bank Slovenije, 2007; Dobra banka, 2010b).

5.3 Proces izvrševanja izvršb v Dobri banki

Proces izvrševanja izvršb sem izbrala za primer, saj je dovolj kompleksen, poteka v vseh bankah in je eden tistih procesov, pri katerem je v zadnjem času prišlo do kar nekaj sprememb. Kot sem na to že opozorila zgoraj, se je v zadnjih letih precej povečal obseg prejetih sklepov o izvršbah zaradi povečanja plačilne nedisciplline. To je neposredno vplivalo tudi na organizacijo dela in zaostankov v organizacijski enoti, kjer omenjen proces izvajajo. Povedano drugače se gospodarska situacija neposredno odraža na obsegu dela v tem oddelku. Z enakim problemom se soočajo tudi druge banke. Ker pa banke odgovarjajo za izvrševanje vsakega sklepa, ki ga prejmejo, je to proces, ki ob nepravilnem izvajanju lahko predstavlja veliko tveganje. Banke morajo vse sklepe obdelati še v istem dnevu, kot jih prejmejo, zato je še kako pomembno, da proces poteka tekoče, brez ozkih grl in s čim manj možnostmi za realizacijo OT.

V Dobri banki v Oddelku podpore plačilnemu prometu (OPPP) centralizirano izvršujejo sklepe o izvršbi v breme transakcijskih računov dolžnikov (pravne osebe, samostojni podjetniki in fizične osebe). Proces so pred nekaj leti informatizirali ter delno avtomatizirali, kar je precej zmanjšalo možnost pojavljanja napak. Pa vendar se ob prisotnosti človeškega faktorja in tehničnih napak še vedno pojavljajo škodni dogodki, ti pa za banko lahko predstavljajo neposredne in posredne negativne finančne učinke. Tako sem se odločila proces in njegove podprocese analizirati ter ugotoviti, kje so kritične točke. Te bom ugotovila na podlagi realiziranih tveganj oz. škodnih dogodkov. V naslednjem poglavju bom prikazala, kako v Dobri banki zbirajo podatke, kako pri njih poteka proces MOT in kateri škodni dogodki v splošnem se nanašajo na proces izvršb.

5.3.1 Management operativnih tveganj in škodni dogodki

V Sloveniji so banke morale implementirati Basel II do leta 2007 (Rotovnik, 2003). To je bila dolžna storiti tudi banka, ki jo proučujem. Zato je na področju OT danes zaposlen manager OT,

ki je odgovoren za načrtovanje in vpeljavo okvira MOT, za ugotavljanje, ocenjevanje, spremljanje, obvladovanje tveganj, poročanje o potencialnih in realiziranih OT vsem ravnem managementa, organizacijo sestankov odbora za OT, v katerega sta vključena tudi uprava in srednji management itn. V banki danes potekajo vse faze cikla MOT (Dobra banka, 2011).

Identificiranje in ocenjevanje potencialnih tveganj poteka na več načinov: preko razgovorov z vodstvom, zaposlenimi, z izpolnjevanjem obrazcev za popis potencialnih škodnih dogodkov. Pri tem se zbira podatke o vzrokih za nastanek, možnih posledicah, vzpostavljenih kontrolah, predlaganih načrtih za preprečitev nastanka in možnih ukrepih. Dogodke zaposleni kategorizirajo s pomočjo kataloga potencialnih škodnih dogodkov, za že realizirane incidente in škodne dogodke pa imajo v banki izdelan sistem poročanja. Vsi zaposleni so dolžni poročati o kakršnemkoli opaženem odstopanju od normalnega stanja, delovanja, tudi če ta nima finančnih posledic. Prijavljanje škodnih dogodkov z osnovnimi informacijami poteka preko temu namenjene aplikacije HelpDesk (modul Škodni dogodki). Pri nadaljnjem popisu škodnega dogodka pa je potrebno pridobiti vse dodatne informacije tega dogodka, ki pa jih zabeležijo točno določeni poročevalci preko aplikacije ali sporočijo direktno skrbniku škodnih dogodkov. Na podlagi zbiranja informacij, ki se shranjujejo, lahko odgovorni pravočasno prepoznajo OT in ukrepajo v smeri preprečevanja njihovega nastanka oz. zmanjševanja verjetnosti njihove ponovitve. Dobra banka nastale škodne dogodke analizira z vidika vzrokov, višine izgub, statistike ponavljanja, nato pa se na podlagi stopnje tveganja odloči, kateri ukrep bo sprejela (sprejemanje, izogibanje, prenos ali zmanjševanje tveganja). S temi aktivnostmi banka ščiti sebe pred večjimi finančnimi in tudi nefinančnimi posledicami (izguba ugleda, odhajanje komitentov itn.) ter tako vpliva na svojo konkurenčnost (Dobra banka, 2011). Tako banka zbira tudi škodne dogodke v oddelku OPPP.

Pri opredelitvi OT so mi bili v pomoč škodni dogodki, ki so nastali od leta 2008 do 2012 in so bili prijavljeni Oddelku za MOT. Škodnih dogodkov iz oddelka OPPP je v bazi podatkov relativno malo (22), je pa število zadostovalo za mojo analizo tveganj v procesu. Razlog je ta, da so po navodilih banke v začetku popisovanja zaposleni poročali samo o škodnih dogodkih, ki so imeli neposredni finančni vpliv in ne tudi o manjših nezgodah. Nato se je z razvojem MOT pričelo dosledno poročati o vsakršnih odstopanjih in število ŠD se je povečalo. V zadnjih dveh letih pa je število spet upadlo, kar menim, da je znak dobrega sprotnega prilagajanja procesa.

Primeri škodnih dogodkov so bili npr. neupoštevanje izvzetij na dolžnikovem računu, neupoštevanje vrstnega reda poplačevanja, slabo preverjanje istovetnosti dolžnika in s tem prenakazilo iz napačnega računa, tehnične napake itn. Posledice nastalih škodnih dogodkov so bile tako finančne (v povezavi z odškodninsko odgovornostjo) kot tudi nefinančne. Dogodki, ki sicer niso imeli neposrednih negativnih finančnih učinkov, so lahko vplivali na ugled banke, izgubo komitentov, povzročili dodatno delo zaposlenih v OPPP ter tudi drugih oddelkih (IT, pravna služba- dodatno delo s pridobivanjem povračila sredstev). Vse škodne dogodke sem lahko razporedila v štiri različne kategorije OT, kot jih je definiral že Qureshi (2010). Ob tem

sem nekatere škodne dogodke uvrstila v dve kategoriji (npr. po napaki zaposlenega se je zaustavila aplikacija):

- **Tveganja zaposlenih** (54,5 %): Tveganja izgub, ki jih namerno ali nenamerno povzročijo zaposleni – npr. napaka zaposlenega, neupoštevanje pravil, neizvedba korakov, napačna komunikacija, kriminalna dejanja itn.
- **Procesna tveganja** (36 %): Tveganja, povezana z izvajanjem in vzdrževanjem transakcij. Gre za tveganja v primeru nepravilno zasnovanega ali neuspešno izvedenega poslovnega procesa, aktivnosti ter z njimi povezanimi različnimi vidiki poslovanja, vključno s produkti in storitvami (npr. tveganje, ki nastane zaradi ozkega grla v procesu).
- **Sistemska tveganja** (32 %): Gre za tveganja izgub, ki jih povzročijo prekinitve delovanja IS, napake v aplikacijah, vdori, kraja podatkov in vpeljava tehnologij, ki niso v skladu s poslovnimi potrebami.
- **Zunanja tveganja** (4,5 %): To so tveganja izgub zaradi poškodovanja fizične lastnine (iz naravnih ali nenaravnih vzrokov). Ta kategorija vključuje tudi dejanja zunanjih oseb, kot so kriminalna dejanja, prevare, sprememba regulative, ki bi ogrozila delovanje podjetja na določenem trgu, itn.

Izvrševanje izvršb je proces, ki je predpisan s strani več različnih zakonov, zato je še kako pomembna skladnost procesa in poznavanje zakonodaje s strani zaposlenih. Ker je proces kompleksen in samo delno avtomatiziran, imajo v procesu največjo vlogo za pravilno izvedbo zaposleni. To je tudi razlog za to, da je škodnih dogodkov v povezavi s tveganji zaposlenih največ (kar 54,5 %). Ker pa je gospodarska situacija pripomogla k povečanemu številu sklepov o izvršbi, je močno vplivala na obseg dela v OPPP na tem procesu. Zato je v zadnjih letih prihajalo do tega, da sklepi niso bili izvršeni dosledno in pravočasno zaradi ozkih grl, zaostankov. To so procesna tveganja (36 %).

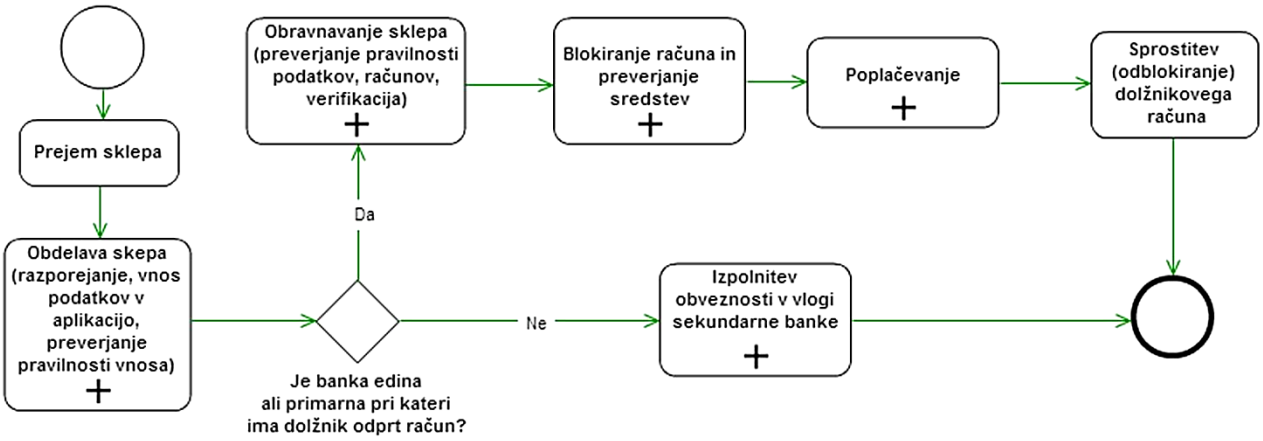
Podrobneje bom OT procesa predstavila na ravni podprocesov. V vsakem izmed njih bom izbrala ključna tveganja, tista, za katera menim, da je največja možnost njihove realizacije. Na ravni podprocesov bodo ti bolje vidni, saj bo proces razčlenjen na aktivnosti, na katere se vežejo posamezna tveganja. To bodo t.i. "kritične točke". Za boljše razumevanje in preglednost povezovanja podprocesov pa bom najprej predstavila krovni proces.

5.3.2 Krovni proces

Krovni proces izvršb je poslovni proces z zaporedjem aktivnosti, ki jih izvajajo različni zaposleni (poštar, referent, verifikator). Vhod v proces je sklep o izvršbi, končni rezultat procesa pa je poplačilo terjatev upnika. Proces je delno avtomatiziran, informacijsko podprt z aplikacijo Izvršbe, ki so jo v Dobri Banki razvili sami. Zaradi kompleksnosti pa so pri večini aktivnosti še vedno zaposleni tisti, ki s svojim delom in odločitvami premaknejo proces iz ene aktivnosti na drugo. Proces namreč temelji na precej pravilih, zaposleni morajo imeti znanje iz zakonodaje in izvršb na splošno. Z vidika obvladovanja tveganj bom proces obravnavala kot notranji proces, lahko pa na ta proces gledamo širše, kot povezovalni proces in ga umestimo v širši proces izvrševanja izvršb, ki vključuje še druga podjetja ter njihove procese (npr. postopke

na sodiščih). Proces izvrševanja izvršb se v tem primeru prične pri izdajatelju sklepa, poleg Dobre banke pa vključuje tudi morebitne druge banke, dolžnika, upnika. Krovni proces, ki je modeliran na sliki 11, bom glede na hierarhijo razdelila v pet podprocesov.

Slika 11: Model krovnega procesa



Izdajatelj sklepa pošlje Dobri banki sklep o izvršbi. Ko ga banka sprejme, sledi razporejanje prejetih sklepov, prenos podatkov iz sklepov v digitalno obliko in preverjanje pravilnosti vnosa. Te aktivnosti sem skupaj poimenovala "Obdelava sklepa". Naprej se proces loči glede na to, ali je Dobra banka primarna ali sekundarna. V sklepu so namreč navedene vse banke, pri katerih ima dolžnik sredstva. Primarna banka je tista, ki je v sklepu navedena prva (to določi izdajatelj) in je v vlogi izvršitelja, sekundarne banke pa so tiste, ki imajo druge, vnaprej določene obveznosti (prenakazilo sredstev iz dolžnikovih računov na račun primarne banke). Če ima torej Dobra banka primarno vlogo, izvede glavni postopek izvrševanja. Obveznost sekundarnih bank pa je, da primarni banki nakažejo manjkajoči znesek denarja, če na dolžnikovem računu pri primarni banki ni dovolj sredstev za poplačilo. Na primarni banki najprej sledi preverjanje pravilnosti, skladnosti podatkov, verifikacija. To sem združila v svoj podproces, ki sem ga poimenovala "Obravnavanje sklepa". Sledi podproces "Blokiranje računa in preverjanje sredstev". Preveriti je namreč potrebno, ali ima dolžnik dovolj sredstev za poplačilo, ter blokirati račun, dokler sklep ni poplačan. Za to je potreben naslednji podproces, ki sem ga poimenovala "Poplačevanje". Ko je upnik poplačan, se dolžnikov račun odblokira oz. sprosti in s tem proces zaključi.

Poleg zgoraj omenjenih dolžnosti v zvezi z izvršbami je naloga bank tudi poročanje različnim osebam. O stanju izvrševanja sproti obveščajo izdajatelje sklepov, dnevno pa morajo primarne banke o izvršbah poročati tudi v skupne evidence vseh slovenskih bank (sistem NODURS za pravne in SISBON za fizične osebe). O dokončanem poplačilu obvestijo upnika, banke in izdajatelje, ter sproti odgovarjajo na razne poizvedbe. Vsak dan naredijo izpis dopisov za prejšnji delovni dan (kateri sklepi so bili vneseni, kateri delno ali v celoti poplačani). Vendar pa se posebej na poročanja ne bom osredotočala, v modele sem vključila samo tista, ki se nanašajo neposredno na opisan proces. Prav tako ne bom podrobneje obravnavala vloge sekundarne banke. Njen model poslovnih procesov in opis, ki se ga naredila, je v prilogi 1.

Glavna tema obravnave bo namreč potek procesa, ko banka sklep izvršuje v vlogi primarne banke, in operativna tveganja, ki se na ta del procesa nanašajo.

5.4 Podproces Obdelava sklepa

Na tem delu procesa bom prikazala primer, kako se podproces lahko optimizira in razvija v smeri zmanjševanja tveganj, napak, krajšega izvajalnega časa s pomočjo MPP (prenove poslovnega procesa, informatizacije). Prikazala bom tri modele, in sicer podproces "Kot je bil", "Kot je" in "Kot bo". Ob tem bom ugotovila, kako se s prenovo spreminjajo tveganja – kakšno je bilo stanje tveganj na začetku, katera nova tveganja so se pojavila po prenovi oz. informatizaciji in katerim se ne da popolnoma izogniti. Ta del procesa je pomemben, saj je veliko škodnih dogodkov, ki so se zgodili sicer v drugi fazi procesa, izhajalo prav iz tega dela (npr. zaradi napačnega vnosa podatkov).

5.4.1 "Kot je bilo"

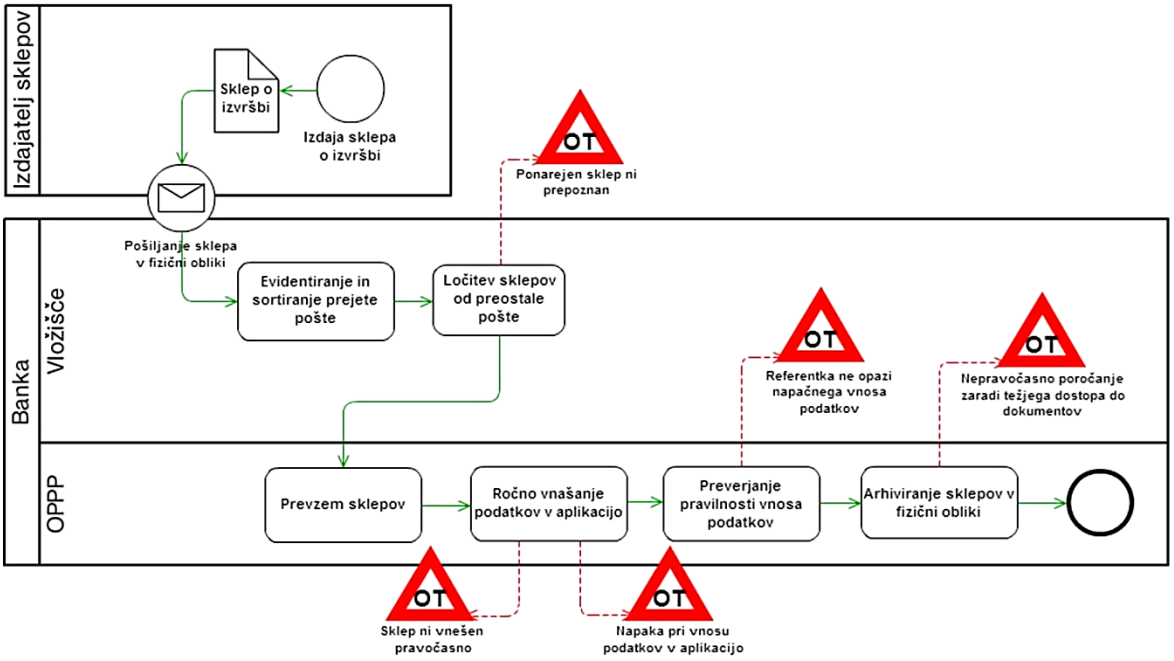
Podproces se je pričel, ko je banka s strani izdajatelja po pošti prejela sklep o izvršbi. V vložišču so zgodaj zjutraj sortirali prejeto pošto in posebej ločili sklepe o izvršbi ter jih posredovali OPPP. Referent je sklepe prevzel, iz njih razbral vse potrebne podatke in jih ročno vnesel v aplikacijo (vrsta sklepa, izdajatelj sklepa, datum, primarna banka, pravnomočnost, višina glavnice, TRR upnika itn.). Po vnosu je referent najprej preveril, ali je pravilno vnesel podatke, ki jih je nato preko aplikacije poslal verifikatorju, sklep v fizični obliki pa je pospravil v arhiv za morebitne naknadne poizvedbe. Podproces je prikazan na sliki 12. Na podlagi takratnih škodnih dogodkov sem identificirala pet glavnih operativnih tveganj:

Razporejevalec pošte ne opazi ponarejenega sklepa. Gre za tveganje kriminalnega dejanja, ki se je v preteklosti že realiziralo. Storilci so ustanovili podjetje, odprli račun na banki, ponaredili sklep o izvršbi in ga posredovali Dobri banki. Med pošiljkami se je tako pojavil ponarejen sklep, vendar ga pri razporejanju niso opazili. K sreči je banka, preden je nakazala denar, o tem obvestila navedenega dolžnika (česar sicer ni dolžna). Ta upnika ni poznal, zato je ukrepal na sodišču. Ko so ugotovili, da je sklep ponarejen, so tudi na banki opazili malenkostna odstopanja v barvi tiska, kuverti. Realizacija tega tveganja je sicer redka, vendar bi ob nerazkritju ponarejenega dokumenta lahko novica prišla v medije in s tem vplivala na zaupanje sedanjih in potencialnih komitentov banke v prihodnosti. V teh primerih je kot ukrep potrebno dobro izobraziti zaposlene, ki odpirajo sklepe, kako naj prepoznajo značilnosti ponarejene pošiljke. Ovojnice sklepov imajo tipični izgled (pošiljke s sodišč), zato jih mora zaposleni, ki razporeja pošto, pazljivo pregledati. Tveganje kljub temu ostaja, saj so včasih ponaredki tako dobri, da jih je težko prepoznati.

Zaradi prevelikega števila sklepov le-ti niso vneseni pravočasno. Zaradi velikega obsega ročnega vnašanja podatkov iz sklepov v sistem je ob precejšnjem povečanju števila sklepov prihajalo do težav z ohranjanjem postopkov v časovnem okviru. Po zakonu mora banka, ko podpiše, da je sklep prejela, še isti dan pričeti z izvršitvijo. Strokovno usposobljeni bančni uslužbenci so morali ročno vnašati veliko količino sklepov in tako so se povečali tudi stroški

dela. Veliko število izvršb tako predstavlja tveganje za banko. Zelo je pomembno, da ne pride do zaostankov, da ukrepajo pravočasno, sicer ima dolžnik vmes čas preusmeriti denar na drug račun, upnik pa bi ta denar lahko zahteval od banke. Ta tveganja so zmanjšali s prenovo procesa, in sicer tako, kot je prikazano v naslednjem poglavju »Kot je«.

Slika 12: Model podprocesa »Kot je bil«



Referentka ne opazi napačnega vnosa podatkov. Referentka pregleda podatke, ki jih je vnesla o sklepu, vendar pa lahko kakšno napako spregleda. Rešitev v tem primeru predstavlja kontrola, zasnovana na principu "štirih oči" (dvojno preverjanje).

Arhiviranje sklepov v fizični obliki ne omogoča pravočasnega poročanja. Naloga banke je, da odgovarja na poizvedbe drugih oseb (upniki, izdajatelji, banke). Ker so se dokumenti hranili v fizični obliki, so bili težje dostopni, banka pa s tem manj odzivna na poizvedbe. Zaradi velike količine sklepov se je lahko kakšen tudi izgubil, banka pa je dolžna o tem dosledno poročati. Posledično so narasli še stroški dela. S prenovo in informatizacijo so to izboljšali tako, da se sklepi arhivirajo v elektronski obliki.

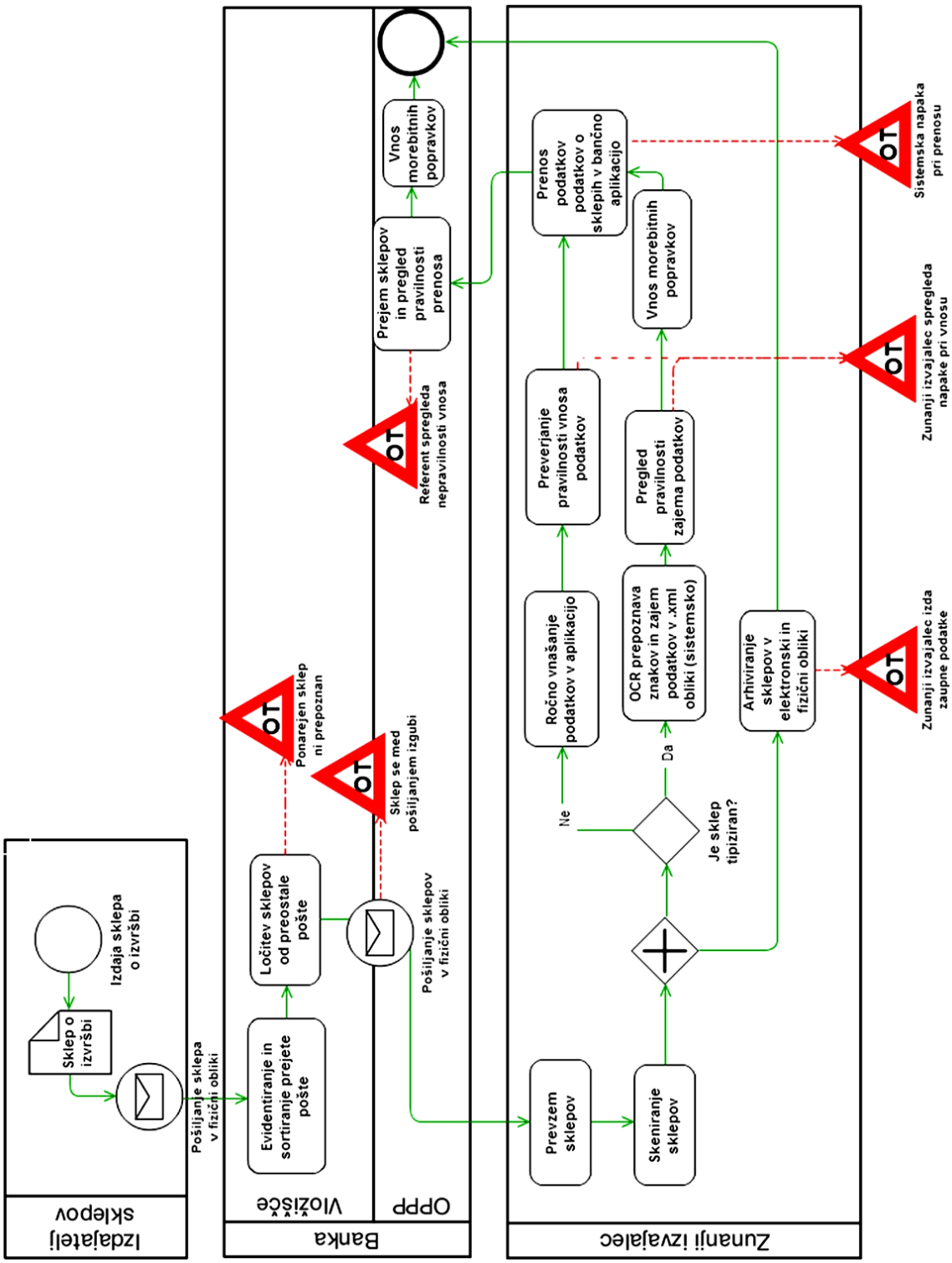
Zaradi zgoraj omenjenih težav in tveganj so se odločili prenoviti podproces. Z ročnim vnašanjem bi namreč potrebovali več zaposlenih, ki bi svoj čas posvetili samo temu delu procesa, saj v Dobri banki na dan prejmejo od 600 do 1000 sklepov o izvršbah, ki jih morajo obdelati. Število sklepov je sicer odvisno tudi od velikosti banke, so pa v precej bankah na tem področju morali povečati število zaposlenih, da so rešili zaostanke. V Dobri banki so se odločili za drugo pot zmanjšanja zamud, in sicer za digitalizacijo sklepov o izvršbi s pomočjo zunanjega izvajalca in elektronsko izmenjavo podatkov o sklepih med banko in zunanjim izvajalcem.

5.4.2 "Kot je"

Prenovljeni del procesa (na sliki 13) vključuje prejem sklepa, skeniranje sklepa, vnos v aplikacijo in že prvi pregled pravilnosti vnosa. Izdajatelj pošlje sklep o izvršbi v fizični obliki. Prejmejo ga v vložišču banke, kjer zjutraj evidentirajo in sortirajo prejeto pošto. Sklepe ločijo od preostale pošte, jih odprejo, ustrezno opremijo in že zgodaj zjutraj pošljejo zunanjemu izvajalcu v fizični obliki. Slednji sklepe skenira, digitalizira in z optično prepoznavo znakov (angl. *OCR – Optical character recognition*) iz sklepov v svojo aplikacijo zajame zahtevane metapodatke, ki jih banka potrebuje, da lahko izvrši sklep (podatki o dolžniku, upniku, izdajatelju, ostalih bankah, transakcijskih računih, višini glavnice itn.). Zunanji izvajalec nato že prvič preveri pravilnost vnosa, in sicer tako, da preveri skladnost meta podatkov s podatki iz sklepa v fizični obliki. Nato vnese morebitne manjkajoče podatke, dokumente v fizični obliki pa arhivira, prav tako tudi digitalno verzijo. Slednjo shrani v spletno aplikacijo, ki kasneje služi za pregled in preverjanje. Metapodatki se nato preko strežnika in posebnega vmesnika prenesejo v IS banke. V banki referent v spletni aplikaciji sprejme vsak sklep posebej, ga pregleda in prenese v bančno aplikacijo Izvršbe. V spletni aplikaciji je slika sklepa, da lahko referent metapodatke primerja z originalom. Če pa sklep ni tipiziran (takšni so sklepi na podlagi izvršilnega naslova), pomeni, da sistem ob OCR prepoznavi ne more ugotoviti, na katerem mestu najde določen podatek. Te sklepe je potrebno vnesti ročno, tudi to izvede zunanji izvajalec. S prenovo procesa so določena tveganja ostala, nekaj so jih izločili ali pa so zmanjšali možnost za njihovo realizacijo, druge so zmanjšali s prenosom storitev na zunanjega izvajalca, pojavilo pa se je tudi nekaj novih.

5.4.2.1 Tveganja

Tveganja, ki so jih zmanjšali/izločili: Kot sem prikazala v prejšnjem modelu, so bila prej tveganja povezana z napačnim vnosom, pomanjkljivim pregledom podatkov in posledično kasneje z napačnim izplačilom. Ta tveganja so sedaj redka zaradi avtomatiziranega vnosa podatkov in ustreznih kontrol, pristopa "štirih oči". Gre za trojni pregled pravilnosti vnosa podatkov. Ujemanje vseh metapodatkov takoj po skeniranju z originalom primerja že zunanji izvajalec. Nato enako preverjanje opravi referent v Dobri banki, kot zadnji pa sklep preveri še verifikator, preden dokončno verificira sklep o izvršbi (v naslednjem delu procesa izvršb). Boljši je tudi pregled nad opravljenim delom. Z elektronskim arhivom je dostop do dokumentov hitrejši, kar omogoča hitrejše iskanje in pravočasno poročanje, manjši so tudi stroški hrambe. Kljub velikemu številu sklepov je prenova omogočila hitrejše izvrševanje sklepov s pomočjo elektronske izmenjave podatkov in s tem zmanjšala tveganja zaradi zamud pri vnosu. Celotna obdelava sklepov je tako hitrejša in cenejša. Zaposleni v banki podatke samo še preverijo in validirajo ter se posvetijo strokovnemu delu, kar zmanjša stroške dela. Ker so večinoma že dopoldan podatki vneseni v aplikacijo, ima dolžnik manj časa, da denar z računa prenese drugam.



Slika 13: Model podprocesa »Kot je«

Tveganja, ki ostajajo: Še vedno ostaja tveganje, da v vložišče prispe ponarejen sklep in tega ne bi opazili. Prav tako obstaja možnost, da referent, ko bi sprejel sklep v aplikaciji, ne bi opazil morebitnih napak oz. odstopanj metapodatkov od "slike" dokumenta, do katere ima dostop preko spletne aplikacije. Vendar je slednja možnost zaradi dobrih kontrol v obliki preverjanj majhna.

Tveganja, ki ostajajo, le da so prenesena na zunanjega izvajalca: Netipizirani sklepi se vnašajo ročno in pri tem ostajajo enaka tveganja kot prej (napačni vnos, slabo preverjanje), vendar s to razliko, da je odgovornost za izvajanje te aktivnosti prenešena na zunanjega izvajalca. Slednji je tudi odgovoren za skeniranje in prvo preverjanje pri tipiziranih sklepih. Tako ostaja majhno tveganje, da bi spregledal napake pri vnosu. Ob tem je potrebno poudariti sledeče: zunanji izvajalec sicer v skladu s pogodbo nosi finančno odgovornost in krije nastalo škodo. Vendar pa banka kljub temu nosi del tveganja napak izvajalca, saj lahko to vpliva na njen ugled. Bančnih strank namreč ne zanima, na čigavi strani je krivda. Zato lahko rečem, da se tveganja ne prenesejo na zunanjega izvajalca v celoti.

Novonastala tveganja: Nova tveganja so predvsem tveganja, ki jih prinaša zunanji izvajalec. To so tveganja, da prekine pogodbo ali da namerno oz. nenamerno (vdor v njihov sistem) izda zaupne podatke, saj ima dostop do zaupnih bančnih podatkov itn. Ta tveganja zmanjšuje dejstvo, da Dobra banka z njim že dlje časa sodeluje tudi na drugih projektih in se je zunanji izvajalec z leti izkazal kot zanesljiv poslovni partner. Zaradi informatizacije postopka pa se pojavi tudi tveganje sistemskih napak. Če bi prišlo do prekinitve sistema, napačnega delovanja pri prenosu podatkov, banka ne bi mogla sklepov pravočasno obdelati. Obstaja pa tudi tveganje, da se pri razporejanju in prenosu sklepov v fizični obliki med banko in zunanjim izvajalcem kakšen sklep izgubi.

Če pogledamo model procesa na hitro, se morda zdi, da je prenovljen proces še bolj kompleksen in ni prihranka z vidika časa, saj so tri preverjanja pravilnosti podatkov. Pa vendar to ne drži, saj je bistven prihranek v prvem delu – pri računalniškem zajemu podatkov namesto ročnega vnašanja s strani zaposlenih, ki se tako lahko posvetijo strokovnemu delu. Poleg tega zadnje preverjanje s strani zaposlenih zaradi dveh predhodnih preverjanj ni tako temeljito in s tem dolgotrajno.

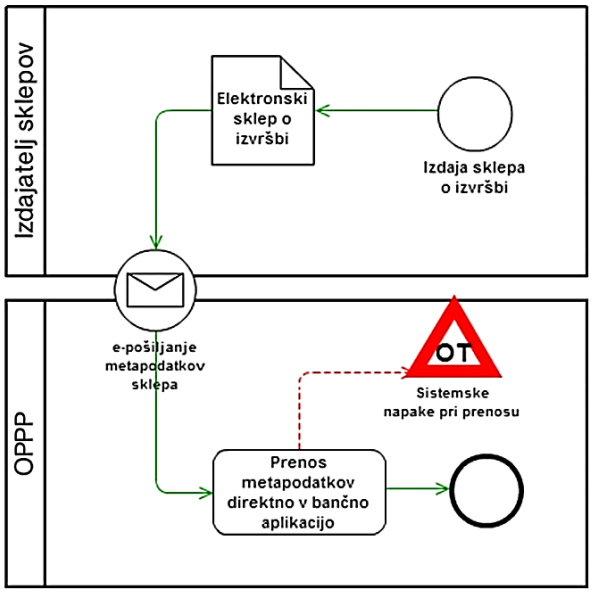
S pomočjo prenove lahko torej rečem, da je prišlo do zmanjšanja OT zaradi napak pri ročnem vnašanju, zaostankov itn. so se pa pojavila nova tveganja (tveganja sistemskih napak, ker se bolj zanašamo na sisteme in tveganja, ki jih prinaša zunanje izvajanje dela procesa). Gledano po samem številu tveganj torej ni manj, imajo pa manjšo možnost nastanka in manjši vpliv. Rešitev v smeri nadaljnjega zmanjševanja tveganj je v procesu »Kot-bo«.

5.4.3 "Kot bo"

Rešitev, ki bi banke rešila vnašanja podatkov o sklepih in izločila vsa s tem povezana tveganja, je v prenovi in informatizaciji celotnega prvega dela procesa, gledano širše – prenova že pri

izdajatelju sklepa. Gre za skupno idejo bank, katere malce prirejen model prikazujem na sliki 14. Izdajatelj bi svoje sklepe izdajal v elektronski obliki in bi sam pošiljal metapodatke direktno v bančni sistem. Banka tako ne bi bila odgovorna za napačno izvrševanje sklepov zaradi napak pri vnosu v sistem. Ne bi prišlo do ponarejanj sklepov, odgovornost za pravilnost podatkov bi nosil izdajatelj, izognili bi se tveganju zunanjega izvajalca (varovanje podatkov, zanesljivost) in ročnemu vnašanju netipiziranih sklepov. Tako bi za banko od vseh zgoraj omenjenih tveganj ostala le tveganja sistemskih napak. V naslednjem podprocesu pa bi še vedno morala ostati kontrola – pregled podatkov (npr. istovetnost dolžnika), da bi se s tem izognili izvrševanju izvršb, pri katerih bi prišlo do morebitnih napak s strani izdajatelja.

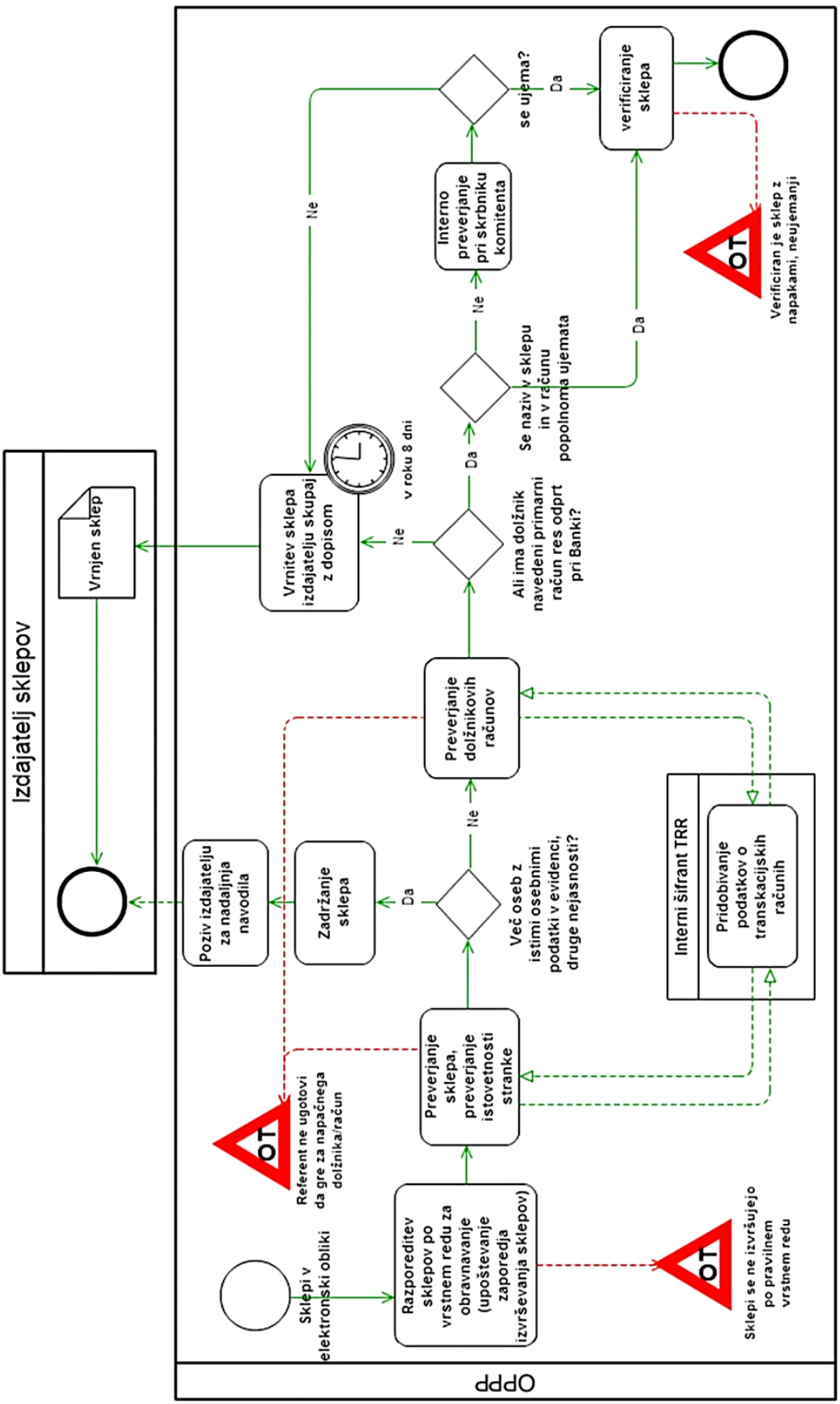
Slika 14: Model podprocesa »Kot bo«



S takšno prenovo bi se precej skrajšal proces, banke pa bi imele manjše stroške, saj ne bi bilo potrebno imeti dodatnih zaposlenih pri vnašanju podatkov ali plačilu zunanjih izvajalcev, zaposleni bi se posvetili strokovnemu delu. Krajši proces z manj tveganji pa je v skladu s cilji tako MPP kot tudi MOT. Za podobno rešitev se banke torej že zavzemajo, vendar je do njene uresničitve lahko še daleč, saj bi bilo potrebno informatizirati proces v širšem pomenu. Vključiti bi se morali vsi izdajatelji sklepov, ki jih je kar nekaj. Informatizacija bi predstavljala dodaten strošek predvsem pri izdajateljih, medtem ko je interes za to večji na strani bank.

5.5 Podproces Obravnavanje sklepa

Preverjanje pravilnosti podatkov in verifikacijo, ki sledita prejšnjemu podprocesu, sem poimenovala Obravnavanje sklepa (podproces je prikazan v sliki 15). Vhod v ta podproces je sklep v elektronski obliki, s preverjeno pravilnostjo metapodatkov s strani referenta. V tem delu pa sledi vsebinsko preverjanje podatkov iz sklepa. To pomeni, da verifikator preveri, ali se dolžnikovi podatki iz sklepa ujemajo s podatki, ki jih ima Dobra banka v svojem šifrantu računov. To je pomembno, saj je banka objektivno odgovorna za izvršitev sklepa. Če se vsi podatki ujemajo, verifikator sklep dokončno potrdi in ta lahko gre v izvrševanje. Verificiran sklep je izhod iz tega podprocesa.



Slika 15: Model podprocesa Obravnavanje sklepa

Sklepi se pričnejo izvrševati po zakonsko določenem vrstnem redu. Zato jih je potrebno najprej razporediti po pravilnem vrstnem redu za obravnavanje in ob tem upoštevati predpisano zaporedje izvrševanja sklepov. Nato sledi preverjanje istovetnosti stranke v sklepu. Najprej se preverijo osnovni podatki (naziv, EMŠO, davčna številka), nato pa še ujemanje podatkov o dolžnikovem transakcijskem računu. Če se kakšen izmed podatkov ne bi ujemal, bi to preverili še pri internem skrbniku stranke (v bančnih poslovalnicah). Ob nejasnostih (npr. če je v bančni evidenci več oseb z enakimi podatki, kot so navedeni v sklepu, če v sklepu ni navedena višina obrestne mere, druge nejasnosti), bi sklep zadržali in za nadaljnja navodila pozvali izdajatelja (Nadzorni svet ZBS, 2007). Če pa bi ugotovili, da navedeni dolžnik sploh nima odprtega računa pri Dobri banki, bi sklep vrnili izdajatelju v roku osmih dni. Če se vsi podatki ujemajo, verifikator sklep verificira. Tako se prične naslednji podproces z blokado računa.

5.5.1 Tveganja

Neupoštevanje vrstnega reda izvrševanja. Banka razvršča sklepe glede na dva kriterija: datum prejetja sklepa in vrsta sklepa. Če banka prejme v izvrševanje samo sodne sklepe o izvršbi, jih mora izvršiti po vrstnem redu, kot jih je prejela. Če jih je prejela več hkrati, upnike poplača sorazmerno (glede na delež od vseh terjatev). Po časovnem vrstnem redu banka izvršuje tudi davčne sklepe, če razpolaga samo z njimi. Če pa razpolaga tako z davčnimi kot s sodnimi sklepi, pa najprej izvrši prednostne sodne sklepe (iz naslova preživnine, odškodnine zaradi prizadetega zdravja, izgube delovne zmožnosti itn.), nato davčne sklepe in na koncu še ostale sodne sklepe, in sicer po vrstnem redu, kot jih je banka prejela. To pomeni, da se vrstni red ob naknadno prejetem sklepu lahko popolnoma spremeni. Pri tem pa ne morejo uporabiti že predhodno blokiranih sredstev na podlagi nepravnomočnega sklepa. Sklepi carinske uprave se pri določanju vrstnega reda obravnavajo enako kot davčni sklepi (Nadzorni svet ZBS, 2007; Dobra banka, 2010b). Prvo tveganje se tako nanaša na neizpolnjevanje tega zakonskega vrstnega reda izvrševanja. Če banka ne bi izvršila sklepov v pravem vrstnem redu, bi pri nekem dolžniku, ki ima več različnih upnikov, lahko neupravičeno prioritetno poplačala kakšnega od upnikov. Ostali "oškodovani upniki", ki bi morali biti poplačani prej, pa bi denar zahtevali od banke. Dobra banka bi morala nato zahtevati vrnitev denarja od že poplačanih upnikov, ki lahko denarja ne bi vrnili in bi tako celotni znesek morala kriti banka sama.

Tveganja pri preverjanju. Ta tveganja so povezana s preverjanjem istovetnosti stranke in njenih računov (zaposleni slabo preveri podatke o stranki, spregleda neujemanja, verifikator sklep z neujemanji verificira). Preverjanje istovetnosti dolžnika in njegovih računov je tudi zelo pomemben del procesa, saj ob slabem preverjanju iz tega lahko izhajajo napake v naslednjih delih procesa. Prvo tveganje je, da zaposleni slabo preveri podatke o stranki (dolžniku), ki so navedeni v sklepu, in spregleda neujemanja. Drugo tveganje, ki se nanaša na prvega, pa je, da verifikator tak sklep verificira. V preteklosti se je na tem delu realiziralo kar nekaj tveganj. Škodni dogodki so nastali predvsem zaradi napak zaposlenih pri izvajanju transakcij, zaradi pomanjkanja znanja in izkušenj za izvajanje aktivnosti ali nepozornosti.

Večina posledic s tem povezanih škodnih dogodkov je bilo nefinančnih, a so vseeno vplivale na ugled banke in ji povzročile dodatno delo.

Do takšnega primera je prišlo, ko je izdajatelj navedel napačno številko TRR dolžnika. V bančni evidenci so bile tri stranke z enakim nazivom, kot je bil naziv dolžnika v sklepu (a vsaka s svojo davčno številko). Ker referentka pri verificiranju ni opravila dodatnega preverjanja istovetnosti in ni bila pozorna na neujemanje, je sklep verificirala. To je povzročilo, da je v naslednjih fazah procesa blokirala račun napačnemu in prenesla sredstva na drug račun. Drugi primer se je zgodil, ko je izdajatelj navedel napačni naziv in se ta zaradi dolžine v aplikaciji referentu ni izpisal v celoti, davčna številka pa se je ujemala. Ker referentka ni popolnoma preverila ujemanja in ni podvomila v pravilnost podatkov, je sklep verificirala. Kasneje so ugotovili, da je Dobra banka imela zavedeno napačno davčno številko pod omenjeno osebo, ki je pripadala drugi stranki. Tako je zopet blokirala napačen račun in zarubila sredstva. V teh dogodkih je Dobra banka imela samo nefinančne posledice, ker so vpleteni po opozorilu vrnili denar. Imela je dodatno delo (obvestilo strankam, naj vrnejo denar, dodatno delo glede neupravičeno zaračunane provizije –ureditev dobropisa komitentu ter stornacijo nadomestila za nalog za prenos sredstev). Realizacija tega tveganja bi lahko poleg slabega vpliva na ugled banke imela tudi velike finančne posledice.

5.5.2 Ukrepi

O tveganjih v zvezi s preverjanjem podatkov je najprej pomembno dobro opozoriti zaposlene. Že sami škodni dogodki so v preteklosti služili kot svarilo zaposlenim o pomenu tega dela procesa, da je potrebno pred vsako blokado računa dobro preveriti istovetnost in ob vsakem minimalnem odstopanju narediti dodatna preverjanja. Tako je teh tveganj danes vedno manj. Kontrola štirih oči je tu ustrezna, ni pa avtomatizirana. Zato v tem primeru kot nadaljnji ukrep, s katerim bi tveganja še zmanjšali, predlagam delno avtomatizacijo kontrole – in sicer, da bi aplikacija Izvršbe omogočala, da bi se ujemanja že predhodno sistemsko preverila. Program bi opomnil na to, kateri podatki se ne ujemajo popolnoma in bi jih referent moral še posebej preveriti. Da bi bilo to mogoče, bi bilo potrebno interni šifrant TRR povezati z aplikacijo Izvršbe. Prav tako bi pri določanju vrstnega reda izvrševanja izvršb lahko aplikacijo zasnovali tako, da bi sama predlagala pravo zaporedje, referent pa bi na določenem številu sklepov nato še ročno preveril pravilnost zaporedja. Za obe vrsti tveganj bi tako uporabili kontrole, ki so kombinacija avtomatskih in ročnih preverjanj. Popolna avtomatizacija pa glede na pomen tega dela procesa ne bi bila mogoča. Moj predlog bi lahko služil zgolj kot pomoč referentu pri preverjanju, saj ta še vedno mora sam potrditi in odgovarjati za pravilnost podatkov.

5.6 Podproces Blokada računa in preverjanje sredstev

Vhod v ta podproces (prikazan je na sliki 16) je verificiran sklep, ki gre naprej v izvrševanje. Najprej sledi blokada dolžnikovih računov. Račun se takoj blokira pri pravnomočnih sklepih, nepravnomočnih, ki imajo posebno oznako "Ig" (sklepi na podlagi izvršilnega naslova v primeru t.i. "gospodarskih sporov") in če ima dolžnik za poplačilo izrecno željo. Za ostale nepravnomočne sklepe je potrebno počakati na pravnomočnost, medtem pa se blokira

dolžnikova sredstva v višini obveznosti iz sklepa in za vsak dan čakanja zaračuna še zamudne obresti (Dobra banka, 2010b). Dolžnikovi računi so blokirani, dokler ni terjatev iz sklepa v celoti poplačana. V internem šifrantu računov se blokada zabeleži tako, da se na dolžnikovem računu vzpostavi status "IZV" (aktivne izterjave, račun pod izvršbo). Dnevno se ti statusi (za pravne osebe) avtomatsko poročajo tudi v AJPES-ov register transakcijskih računov eRTR, kjer so javno objavljeni. Ko so računi blokirani, sledi preverjanje sredstev na računih. Referent pregleda, ali sredstva na dolžnikovih računih zadostujejo za poplačilo. Ob tem mora pri fizičnih osebah upoštevati določena izvzetja – denar, ki ga banka po zakonu ne sme zarubiti. Pravne osebe teh izvzetij nimajo.

Če je na primarnem računu dovolj sredstev, banka obvesti morebitne sekundarne banke, da ne potrebujejo nakazovati dodatnih sredstev. Če ima dolžnik pri Dobri banki več računov, iz drugih računov prenakaže denar na primarnega. V kolikor ta sredstva ne zadostujejo in ima dolžnik račune še pri sekundarnih bankah, le-te nakažejo sredstva v višini obveznosti iz sklepa. Dolžnik lahko tudi sam predlaga s katerih računov naj se izvršba izvrši. Če sredstva še vedno ne zadostujejo, se prenesejo v poplačilo trenutna sredstva in banka čaka na naslednji priliv, medtem pa je račun blokiran. Ta del podprocesa se zaključi s prenosom sredstev v poplačilo (t.i. avtorizirana sredstva na računu).

Register transakcijskih računov (v nadaljevanju *eRTR*), ki ga upravlja AJPES, je baza o transakcijskih računih in njihovih imetnikih, katere namen je centraliziran dostop do podatkov o transakcijskih računih (Register transakcijskih računov, splošno, 2013). V njem imajo računi poslovnih subjektov, ki so blokirani, oznako "R", to pa jim dnevno sporočajo banke. V primeru napak oz. neupravičene blokade računov in s tem napačnega poročanja so oškodovane stranke, ki zaradi tega lahko izgubijo ugled. Podatki so namreč javni in na dosegu tudi kupcem bančnih strank. Poleg tega podjetja, ki nudijo poslovne in bonitetne informacije, tovrstne informacije hitro razširijo svojim naročnikom.

5.6.1 Tveganja

Tveganja so predvsem, da bi referent blokiral napačen račun (to izhaja še iz napak v prejšnjem podprocesu), nepravilno zaračunavanje obresti ali da bi prišlo (kot se je to že nekajkrat realiziralo) do tehničnih napak, zaradi katerih bi bil neopravičeno dodeljen status "IZV" (blokiran račun). Posledično pride do napačnega poročanja naprej v eRTR in škoduje ugledu bančnih strank in banke.

Škodni dogodki, ki so nastali v tem delu procesa, so bili predvsem posledica človeških napak in nedelovanja aplikacije. Iz naslova napačnega poročanja v eRTR je bilo škodnih dogodkov kar nekaj. Pri vsakodnevnem obračunavanju zamudnih obresti za nepravnomočne sklepe je postopek takšen, da se v aplikaciji sproži procedura, v kateri se najprej za kratek čas vzpostavi status IZV, nato pa aplikacija preveri, ali imajo dolžniki na računu dovolj sredstev. Če jih imajo, se status ukine in zaračunajo obresti. To se izvede avtomatsko. Ko pa na takšen transakcijski račun pride priliv, korake v aplikaciji ročno sproži referent ob obdelavi prilivov. Primeri škodnih dogodkov so bili tako pri ročnem kot avtomatskem zaračunavanju. Npr. ker

zaposleni ni pozorno izvedel vseh potrebnih procedur pri obdelavi prilivov, se status IZV ni ugasnil. V drugem primeru se zaradi aplikacijske napake nista izvedla oba koraka pri avtomatski proceduri in se je na računu podjetja neupravičeno aktiviral status IZV. Tveganje tovrstnih napak ostaja.

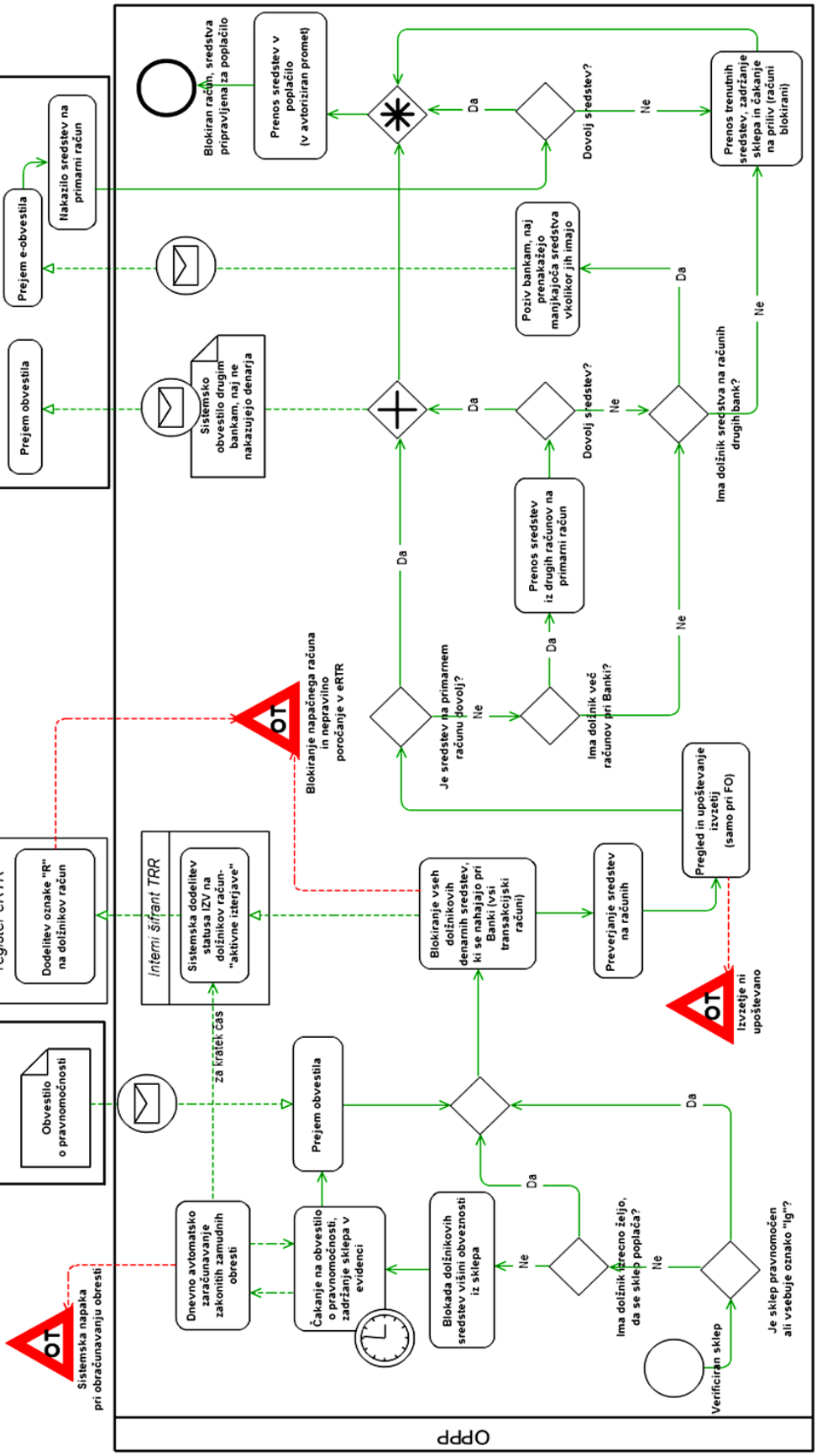
Drugo možno tveganje je, da bi zaposleni blokiral napačen račun na podlagi tveganj iz prejšnjega podprocesa (zaradi slabega pregleda podatkov). Transakcijski računi s statusi IZV se dnevno poročajo v eRTR in tam dobijo oznako »R«. Tveganje je torej, da bi banka na podlagi zgoraj omenjenih napak napačno poročala in bi na transakcijske račune neupravičeno dodelili oznako "R". Po teh škodnih dogodkih so zaposleni imeli dodatno delo, saj so naknadno morali odpraviti napake (ročno sprožiti obdelave, da je podjetjem izginil status IZV), nezadovoljnim strankam pa so izstavili potrdila o poravnanih obveznostih. V njih so navedli, da niso imeli blokiranega transakcijskega računa in so ob tem obrazložili, da je poročanje v eRTR zgolj informativne narave in se iz njega ne more dokončno sklepati, da je podjetje plačilno nesposobno.

Naslednje tveganje je pri pregledu sredstev, in sicer, da zaposleni spregleda izvzetja oz. sredstva, ki jih ne sme upoštevati za poplačilo. To pomeni, da ne upošteva dosledno, koliko lahko banka dolžniku zarubi od trenutnega stanja glede na zakonske omejitve in izvzetja ter njegovo pravno obliko. Ta tveganja bom podrobneje obravnavala v naslednjem podprocesu.

5.6.2 Ukrepi

Tveganja, da referent blokira napačen račun, je potrebno omejiti s kontrolami in ukrepi v prejšnjih fazah procesa (pravilni vnos, pregled sklepa). Škodnih dogodkov v zvezi s tehničnimi napakami pa je vedno manj, saj so bile napake sproti odpravljene in je aplikacija vedno bolj izpopolnjena. Ker pa možnost za realizacijo zgoraj omenjenih tveganj ostaja, bi lahko uvedli dodatno kontrolo zaposlenih pri tistih dolžnikih, katerih sklepi so nepravnomočni in imajo dovolj sredstev (pri teh je namreč prihajalo do škodnih dogodkov). Predlagam, da bi ob koncu delovnega dne preverili, ali so tako avtomatsko kot ročno sprožene procedure strankam ustrezno opredelile status IZV in obračunale obresti. To bi preveril referent na podlagi nekaj vzorčnih transakcijskih računov. V kolikor bi se izkazalo, da je prišlo do napak, bi bilo potrebno ponovno sprožiti obdelave, da bi se podjetjem izbrisal status IZV in pregledati še druge račune. Šele po izvedbi te dodatne kontrole bi se podatke ob točno določeni uri pošiljalo v eRTR, v tistem času pa se postopkov obračunavanja obresti ne bi smelo izvajati.

Slika 16: Model podprocesa Blokada računa in preverjanje sredstev



5.7 Podproces Poplačevanje

Zadnji del procesa predstavlja »poplačevanje« oz. prenos sredstev iz dolžnikovega na upnikov transakcijski račun. Vsi prilivi na blokiran račun (z oznako IZV) se samodejno preusmerijo v "avtoriziran promet" v aplikaciji Izvršbe. Od tam referent razporeja naloge in v aplikaciji ročno sproži vsakega od posameznih odlivnih nalogov. Ob tem upošteva vrstni red poplačevanja obveznosti in izvzetja. Pri poplačevanju se obračunajo tudi obresti in drugi stroški (ob prvem poplačilu sklepa se dolžniku pravni osebi sistemsko zaračuna provizija za prvi odliv, prav tako se mu sistemsko zaračuna provizija za toliko nalogov, kolikor jih je bilo potrebno izvršiti do dokončnega poplačila sklepa o izvršbi). Obveznosti se poplačujejo po točno določenem vrstnem redu, kot je to prikazano v modelu podprocesa na sliki 17 v črtkanem okviru. Če sredstev za poplačilo ni dovolj, je potrebno čakati na naslednji priliv. V kolikor na dolžnikov račun več kot leto dni ni priliva, se o tem obvesti izdajatelja in sekundarne banke ter se preneha z izvršitvijo.

Ko so poplačane vse obveznosti iz sklepa in se vsi nalogi dokončno izvršijo v breme dolžnika, se podatki o dolžniku izbrišejo s seznama blokiranih oseb. To pomeni, da se račun sprosti oz. odblokira, iz internega šifranta se izbriše oznaka "IZV" in iz eRTR oznaka "R". Na koncu sledi še kratek pregled, ali je bil sklep izvršen v skladu z navodili, o zaključenem poplačilu se obvesti tudi izdajatelja in sekundarne banke. Sklep in podatki o izvrševanju ostanejo v arhivu za morebitne naknadne poizvedbe. S tem se proces, z izjemo naknadnega poročanja, zaključi.

5.7.1 Tveganja

Ta del procesa je tisti, v katerem se dejansko izvrši poplačilo upnika, zato je še posebej potrebna natančnost in upoštevanje pravil. Tu se tudi odražajo napake iz prejšnjih podprocesov, zato se je v preteklosti kar nekaj tveganj realiziralo prav v tem podprocesu.

Izvzetja. V rokah dolžnika je nekaj pravnih mehanizmov, ki omogočajo preprečitev prenosa premoženja k upniku, to so pravno določena izvzetja iz izvršb (npr. socialna podpora, preživnina), razglasitev stečaja itn. Tako zakonodaja z omejevanjem izvršb do določene mere varuje dolžnika pred pravicam upnika (Chatterjee & Gordon, 2011). Izvzetja so pri fizičnih osebah, pri pravnih jih ni. Se pa lahko tudi ta izvzetja porabi oz. zarubi (če so na računu več kot mesec), saj se štejejo kot privarčevana sredstva. Poleg zakonsko določenih prilivov, ki so iz izvršbe izvzeti (prejemki iz naslova zakonite preživnine, denarna socialna pomoč, starševski dodatek, štipendije, nadomestilo za invalidnost itn.), so tudi druga sredstva, ki jih banka ne sme porabiti za poplačevanje izvršb – npr. sredstva, ki so namenjena kritju negativnega stanja na računu (limita), sredstva podjetja v stečajnem postopku itn. (Nadzorni svet ZBS, 2007). V preteklosti so se dogodili škodni dogodki iz naslova porabljenih nedovoljenih sredstev za poplačilo, ker referenti niso upoštevali izvzetij. Večina teh dogodkov je nastala zaradi napak zaposlenih pri izvajanju aktivnosti, neupoštevanja pravil ter napačne komunikacije. Škodni dogodki so imeli tako finančne kot nefinančne posledice, predvsem pa dodatno delo zaposlenih zaradi zahteve povračila sredstev od upnika ter pritožbe in reklamacije strank.

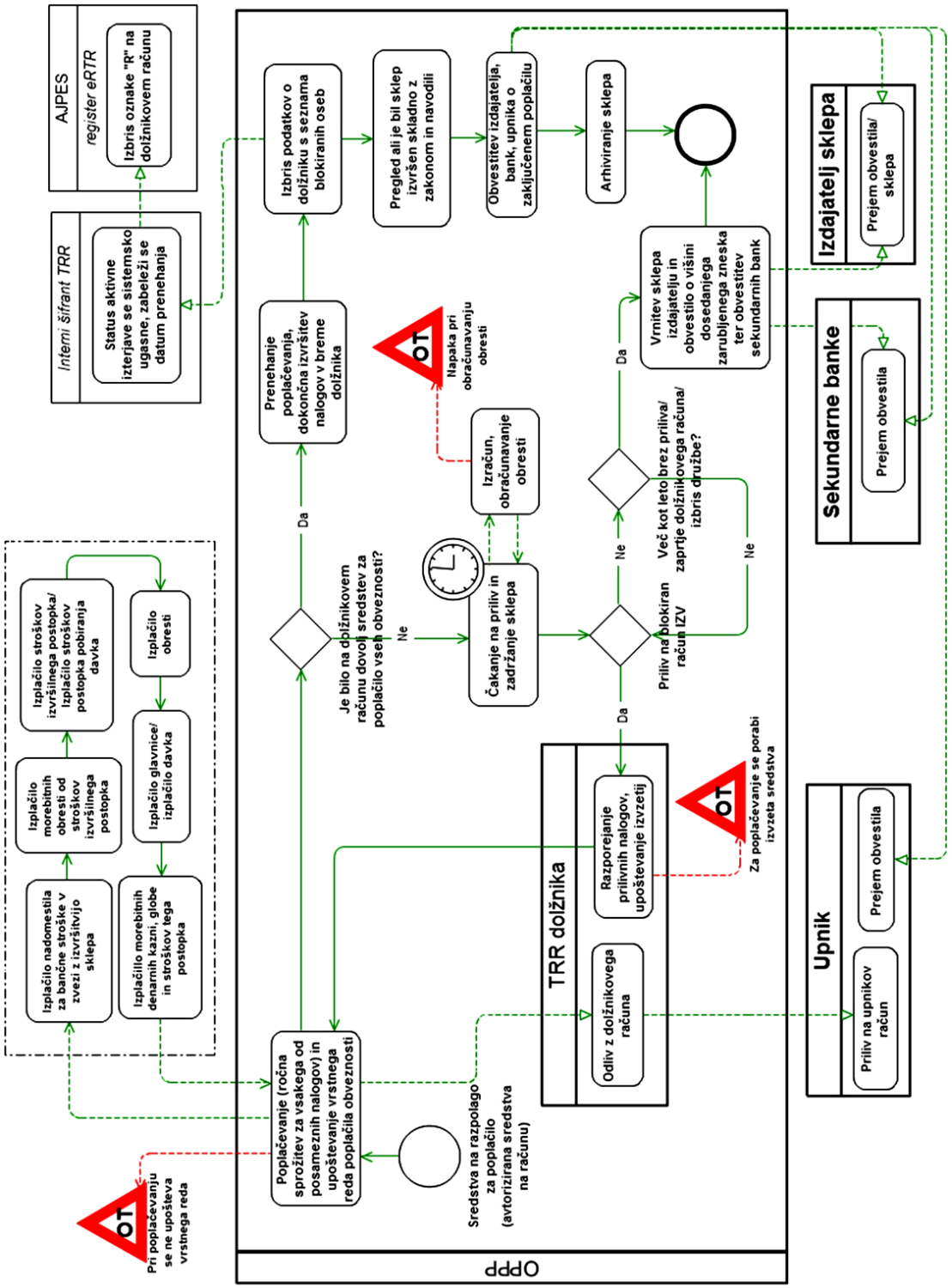
Tipičen primer škodnega dogodka je bil, ko je zaposlena storila napako in zarubila del pokojnine, ki je po zakonu ne bi smela (dodatek za invalidnost in dodatek za pomoč ter postrežbo). V drugem primeru zaradi pomanjkanja komunikacije med oddelki OPPP ni bil obveščen, da je komitentu z blokiranim računom potekel limit in je bilo potrebno priliv zadržati za pokrivanje limita. Tako so denar porabili za poplačilo izvršbe. Prav tako je bil problem v komunikaciji, ko se je sklep poplačeval skladno s prispelimi prilivi na račun dolžnika, tik pred zadnjim poplačilom pa je bil nad dolžnikom uveden stečajni postopek. Oddelek, ki to spremlja, je OPPP prepozno obvestil, znesek poplačila sklepa pa so nakazali upniku. V naslednjem primeru, ko je šlo za osebni stečaj fizične osebe, pa je zaposlena prejeti sklep o prekinitvi izvršilnega postopka le arhivirala, ni pa prekinila izvrševanja.

Tovrstni dogodki so povzročili dodatno delo zaposlenih s tem, da so morali obvestiti upnike, naj denar vrnejo. Če upnik denarja ni vrnil, se je morala vključiti še pravna služba, kar je bil dodaten strošek poleg stroškov bančnih transakcij (npr. nadomestila za nalog za prenos sredstev). Primer neposredne finančne škode je bil, ko denarja niso dobili povrnjenega, pravna služba pa je odsvetovala vložitev tožbe, saj bi bili sodni stroški višji kot znesek vračila.

Ozko grlo pri poplačevanju. To tveganje se delno navezuje na prejšnje tveganje, pregledovanje izvzetij. Pri dolžnikih, ki ob prvem poplačilu nimajo dovolj sredstev in se njihova izvršba poplačuje v več delih, je potrebno čakati, da na njihov blokiran račun pride naslednji priliv. Vsak priliv in nato odlivni nalog morajo referenti ročno sprožiti v aplikaciji. Iz tega sledi, da na dneve, ko pridejo prilivi na veliko računov hkrati (npr. dan za izplačilo pokojnin, plač), je to velika obremenitev in na tem delu nastane ozko grlo. Ko je dan izplačila pokojnin, je na račune fizičnih oseb preusmerjenih več kot 1000 prilivov. Vsakega od teh prilivov morajo zaposleni posebej opredeliti glede izvzetij, ko delajo obdelave. Zato se ti postopki lahko precej zavlečejo, dolžniki pa lahko z denarjem, ki jim zakonsko pripada (izvzetja), razpolagajo šele, ko se postopki zaključijo. Zaposleni morajo torej primere hitro reševati, poleg tega pa so na takšne dneve še dodatno obremenjeni s telefonskimi klici strank. To za zaposlene predstavlja pritisk, zaradi česar delajo napake. Ta ozka grla tako predstavljajo tveganje – nezadovoljstvo dolžnikov, če zaradi gneče ne morejo dovolj hitro razpolagati s sredstvi in možnost napak zaposlenih pri opredelitvi izvzetij.

V tem podprocesu lahko izpostavim še druga, a manjša tveganja. Podobno tveganje kot v prejšnjem podprocesu je pri obračunavanju obresti. Tako kot pri nepravnomočnih sklepih v prejšnjem podprocesu se obračunavajo dnevno, dokler ni sklep poplačan. Zaračunajo se tudi drugi stroški, kot je prikazano v modelu podprocesa. Ker pa se postopki izvedejo avtomatsko, ostaja tveganje tehničnih napak in s tem napačnega obračunavanja.

Slika 17: Model podprocesa Poplačevanje



5.7.2 Ukrepi

Zaposleni se morajo še naprej stalno izobraževati in spremljati zakonodajo, da bodo dosledni in bolj pozorni pri obdelavi prilivov ter bodo dobro preverili vsa sredstva, preden jih bodo uporabili za poplačilo. Poleg upoštevanja zakonodaje glede izvzetij pa morajo vsaj enkrat dnevno preveriti tudi druga dejstva, zaradi katerih ne smejo prenakazovati denarja – npr. katera podjetja in fizične osebe so v stečajnem postopku, da se postopek izvrševanja lahko pravočasno prekine. Temeljita mora biti tudi kontrola izvrševanja sklepa, preden gre sklep dokončno v arhiviranje. Podobno kot v prejšnjem podprocesu tudi v tem predlagam na določenem vzorčnem številu transakcijskih računov narejeno dodatno kontrolo preverjanja, ali so se obresti pravilno obračunale (ob koncu delovnega dne). Da pa bi bilo tudi zadnje pregledovanje izvrševanja procesa temeljito, menim, da bi bilo potrebno izboljšati tudi revizijsko sled. Trenutno je možen le vpogled o zaporednih dogodkih pri obravnavanju določenega sklepa, ter osebah, ki so sklep vršile (kdo je kaj naredil). Če bi bilo razvidno še, kdo je kaj pregledoval, bi lahko ugotovili, ali so referenti preverili ujemanje podatkov, ustreznost zaporedja izvzetij ali ne. To bi omogočalo tudi lažji pregled za kasnejše vpoglede in revizijo.

Večji problem je tveganje glede neupoštevanja izvzetij in z njimi povezano ozko grlo pri poplačevanju na dneve, ko pride večje število prilivov. Ker ta del še ni avtomatiziran, predlagam, da bi to rešili na podlagi kod namena. V sklopu uvedbe enotnega območja plačevanja v evrih (angl. *SEPA- Single Euro Payments Area*) so v bančni sistem prišle novosti, med njimi tudi univerzalni plačilni nalog (UPN), ki je nadomestil stare papirne obrazce (položnice in naloge). V UPN naloge so vpeljali t.i. kode namena (Kode namena plačila – NLB, 2013), ki podrobneje opisujejo namen plačila (Kaj je SEPA, 2013). S pomočjo teh kod bi bilo mogoče delno avtomatizirati postopek preverjanja izvzetij.

Banka bi lahko izvzetja prepoznala avtomatično preko kod namena in nato določena izvzetja preverila še ročno. Pri vsakem prilivu bi program prepoznal kodo namena in tako ugotovil, ali gre za izvzetje. Na podlagi kod bi aplikacija ločila prilive v tri dele: 1. tiste, ki nesporno niso izvzeti (npr. DIVD dividenda, vsi prilivi na račune pravnih oseb), 2. tiste, ki so nesporno izvzeti (npr. SSBE- socialna podpora, ALMY- preživnina, BECH- otroški dodatek) in tiste, pri katerih je potrebno dodatno preverjanje (npr. PENS- pokojnina, OTHR- drugo). Najprej bi se izvršba poplačala iz 1. skupine, v kolikor bi bilo sredstev premalo, pa bi se ročno preverilo še tretjo skupino. Sredstva iz 2. skupine, bi se avtomatično izločila.

Trenutno v banki med preverjanjem izvzetij sicer že upoštevajo kode namena, vendar se na njih ne zanašajo popolnoma, prav tako to preverjanje ni informatizirano. Omenjeni predlog ima namreč omejitev. Kljub temu da bi sistem prepoznal plačnika in namen plačila, je problem v tem, da lahko tisti, ki plačuje, namerno ali nenamerno navede napačno kodo namena. Če bi vzpostavili disciplino, da bi vsi prilivi, ki bi morali biti izvzeti, imeli točno določeno oznako, bi bilo preverjanje lažje in bolj avtomatizirano. Proces bi potekal bolj tekoče ob dneh, ko je povečano število prilivov in nastane ozko grlo pri poplačevanju.

SKLEP

S pomočjo literature in konkretnega primera sem analizirala pomen MPP in MOT, predvsem pa njunega povezovanja preko procesov. MPP procese prenavlja v smeri boljše učinkovitosti in uspešnosti, uspešno izvedbo procesa pa lahko preprečijo OT, ki so del procesov. Zato morajo biti procesi prenovljeni tudi v smeri manjših možnosti za realizacijo tveganj, za kar se zavzema MOT. Povezovanje MOT z osnovnimi tehnikami MPP lahko predstavlja učinkovit način obvladovanja operativnih tveganj. S pomočjo analize in modeliranja procese podrobneje definiramo in tako lažje odkrijemo OT. Nato tveganja ocenimo in na podlagi tega planiramo kontrole, ki jih namestimo v proces, ki ga neprestano izboljšujemo. Te korake skupaj imenujemo procesno usmerjen MOT. Tveganja torej obravnavamo kot neločljivi del procesov, s katerimi imamo boljši pregled nad tem, katere aktivnosti povzročajo tveganja. Sočasna kontrola procesov in tveganj omogoča lažje odkrivanje skritih tveganj, boljšo podlago za odločanje o ukrepih in nadaljnji razvoj procesa. S pomočjo modeliranja, vizualiziranja in ukrepov (prenove, informatizacije, kontrol) lahko zmanjšamo tveganja v procesih.

Povezovanje obeh področij je še posebej uporabno za podjetja, kot so banke, saj so njihovi procesi zahtevni, temeljijo na informacijah in znanju, ter jim realizacija tveganj lahko prinese velike negativne posledice. Zato sem za prikaz, kako lahko MPP uporabimo pri MOT, izbrala proces izvršb v Dobri banki. Proces je kompleksen, zaposleni morajo dobro poznati zakonodajo in morajo biti natančni. V zadnjem času se je zaradi plačilne nedisciplineprecej povečalo število prejetih sklepov o izvršbah, kar je privedlo do velikih zaostankov. Ker je banka odškodninsko odgovorna za izvrševanje vsakega sklepa in dolžna sklepe obdelati še v istem dnevu od prejetja, mora proces potekati tekoče, brez ozkih grl in s čim manj možnostmi za realizacijo operativnih tveganj. V Dobri banki so bila do sedaj OT vrednotena po organizacijskih enotah in je bilo slabše razvidno, katere aktivnosti v procesih so predstavljale tveganja, proces je bil modeliran samo na višji ravni abstrakcije. Zato sem naredila podrobne modele podprocesov in izpostavila nekaj ključnih tveganj, predstavila modeliranje tveganj, predlagala določene ukrepe ter prikazala kako prenova in informatizacija vplivata na OT. S pomočjo modeliranja tveganj znotraj procesov sem prikazala bolj točno sliko, kako procesi potekajo in kje so nevarnosti znotraj njih. Na primeru prvega podprocesa pa sem prikazala kako se lahko proces razvija v smeri optimizacije in zmanjševanja tveganj s pomočjo MPP.

Tveganja sem identificirala na podlagi poročil o škodnih dogodkih. Največ tveganj je bilo v povezavi z zaposlenimi. Razlog za to je v tem, da je proces le delno avtomatiziran in so še vedno zaposleni tisti, ki s svojim znanjem in odločitvami izvršujejo proces. Tem OT pa sledijo procesna tveganja, ki so posledica ozkih grl, zaradi katerih sklepi niso bili izvršeni dosledno in pravočasno. Škodni dogodki so povzročili tako finančno kot nefinančno škodo (dodatno delo zaposlenih, stroški pravne službe, kritje nepovrnjenih sredstev itn.). Se pa število škodnih dogodkov zmanjšuje, iz česar lahko sklepam, da se proces prenavlja v smeri zmanjševanja tveganj. Kljub temu ostaja nekaj ključnih tveganj, ki sem jih izpostavila. Zelo pomemben del procesa je preverjanje vnešenih podatkov istovetnosti dolžnika in njegovih računov. Obstaja tveganje, da zaposleni te podatke slabo preverijo, spregledajo napake in takšen sklep

verificirajo. Dodatno tveganje je, da banka sklepe ne bi izvrševala v pravem vrstnem redu in bi določene sklepe neupravičeno obravnavala prioritetno. Referent bi lahko blokiral napačen račun ali pa bi prišlo do tehničnih napak, zaradi katerih bi bil stranki neopravičeno dodeljen status "IZV". Posledično bi se napačno poročalo v eRTR, kar bi škodovalo ugledu bančnih strank in banke. V zadnjem delu procesa pa se dejansko izvrši poplačilo upnika, zato je v tem delu še posebej potrebna natančnost in upoštevanje pravil. Tu se tudi odražajo napake iz prejšnjih podprocesov. Tveganje je, da bi referenti za poplačilo porabili nedovoljena sredstva, ker ne bi upoštevali izvzetij.

Za ugotovljena OT sem po podprocesih podala predloge ukrepov, s katerimi bi jih omejili oz. zmanjšali. Primer ukrepa je kombinacija ročne in avtomatizirane kontrole pri upoštevanju izvzetij, preverjanju istovetnosti in pravega zaporedja izvrševanja. Drugi ukrepi so naknadne kontrole (ob koncu dneva), ki preverijo pravilnost obračuna obresti, in dodatna preverjanja, kontrola štirih oči. Še vedno pa so za obvladovanje teh tveganj ključni izvajalci tega procesa, zato se morajo še naprej stalno izobraževati in spremljati zakonodajo, da bodo dosledni, pazljivi, bolj pozorni pri obdelavi prilivov, ter bodo dobro preverili vsa sredstva pred poplačilom. Omenjeni predlogi se zdijo zanimivi tudi odgovornim v procesu izvršb v Dobri banki. Ob tem so opozorili na omejitve pri avtomatizaciji kontrol v procesu. Menijo, da bi prevelika avtomatizacija lahko predstavljala celo večje tveganje, kot ga predstavljajo zaposleni. Določene omejitve sem izpostavila tudi sama: npr. kontrola na podlagi kod namena bo težko zanesljiva, dokler ne bodo plačniki dosledno navajali namena plačila.

Kot ukrep zmanjševanja tveganj lahko prenovimo proces ali del procesa. Kako se OT spreminjajo tekom prenavljanja procesa, sem prikazala na prvem podprocesu. Po prenovi so določena tveganja ostala, nekaj so jih izločili, zmanjšali možnost za njihovo realizacijo, druge pa so prenesli na zunanjega izvajalca, pojavilo se je tudi nekaj novih. Velikokrat prenova procesa namreč ne zmanjša števila tveganj, saj se pojavijo nova. Tveganja napak pri ročnem vnašanju se ob vpeljavi nezanesljivega informacijskega sistema lahko spremenijo v tveganja sistemskih napak. Tveganja, ki so bila prej pogosta, a so imela majhen vpliv, se spremenijo v redka, a z velikim vplivom. Tudi tveganja, ki jih sicer formalno prenesemo na zunanjega izvajalca, se ne prenesejo v celoti, saj če pride do napake, na ugledu izgubi predvsem banka. Zato je tako pri kontrolah kot tudi pri prenovi ključno, da smo pozorni na to, da se tveganja dejansko zmanjšujejo oz. da imajo nova tveganja manjšo možnost nastanka in manjši vpliv. Pri prenovi procesa se je tako potrebno osredotočiti na oboje – da bo proces imel manj možnosti za nastanek tveganj in bo obenem bolj učinkovit. Kontrole morajo biti takšne, da se lahko izognemo čim več škodnim dogodkom in zaradi tega proces ne bo še daljši ter bolj kompleksen od prvotnega. Potrebno je torej najti pravo razmerje med tem, da je proces čim bolj učinkovit in obenem čim bolj "odporen" na tveganja.

Moj prispevek je v razširjeni predstavitvi literature na področju MPP in MOT ter povezovanja, prispevek k modeliranju tveganj v procesih in predstavitvi konkretnega primera. Prikazala sem uporabno vrednost tega pristopa, da bi se ga v prihodnosti bolj posluževali za obvladovanje tveganj na podobnih procesih. S podrobnejšim modeliranjem procesa in prikazom tveganj

znotraj njih sem predstavila banki okvir, kako opredeliti tveganja po procesih in jih s tem lažje obvladovati. V ta namen sem v notacijo BPMN dodala nov grafični simbol za OT. Z uporabnostjo takšnega modeliranja se strinja tudi manager OT v Dobri banki. Prednost je boljše dokumentiranje tveganj, boljša dokumentacija pa se lahko bankam obrestuje v nižjem zahtevanem vezanem kapitalu za kritje OT.

Ima pa takšen pristop tudi omejitve. Operativna tveganja je težko meriti in napovedovati z vidika vpliva in pogostosti, ter prepoznati njihove vzroke, saj so vnaprej težko vidni, kompleksni, med seboj odvisni. Zato tudi sama tveganj nisem ocenila kvantitativno, ampak sem samo izpostavila nekaj ključnih OT na podlagi že realiziranih škodnih dogodkov. Ob tem se pojavlja naslednji problem, in sicer ta, da je bilo v začetku poročanja škodnih dogodkov manj, saj škodni dogodki z manjšimi izgubami niso bili zabeleženi, izgube visokih vrednosti pa se zgodijo zelo redko. Posledično težje ocenimo verjetnost, da se bodo tveganja ponovno realizirala (škodni dogodki se večinoma niso ponavljali). Poleg tega je tveganja težko povezati s točno določenimi aktivnostmi, saj velikokrat ni popolnoma jasne povezave med njimi. OT so lahko rezultat kompleksnih interakcij med več elementi procesa. Do realizacije tveganj lahko pride šele v zadnjem delu procesa, povzročijo pa jih napake iz prejšnjih delov procesa. To je tudi eden izmed problemov pri modeliranju tveganj. Nastane namreč dilema, kako označiti ali kam vrisati tveganja, ki se realizirajo v določeni aktivnosti, so pa posledica napake v neki predhodni aktivnosti. Tveganja se razlikujejo tudi po vplivu in verjetnosti nastanka. V modelih procesa sem za vsa OT uporabila enak simbol in so tako na prvi pogled tveganja enakovredna, kar pa ne drži. Vprašanje je, kako torej označevati, vizualizirati tveganja, da se bodo med seboj ločila – npr. z različnimi barvami, velikostmi simbolov.

Vsa ta vprašanja ostajajo predmet za nadaljnje raziskovanje – kako izboljšati procesno usmerjen MOT in znotraj tega tudi modeliranje tveganj v procesih. Modeliranje procesno usmerjenega MOT bi bilo potrebno bolje razviti ter integrirati simbole za tveganja v notacijo BPMN. To bi pomenilo tudi boljše razumevanje modelov s strani uporabnikov in zavedanje, kje v procesih morajo biti še posebej pozorni na tveganja. V praksi je še vedno razkorak med MOT in MPP. Da sta si v osnovi različna, se kaže v podjetjih, kjer se po večini z MPP in MOT še vedno ukvarjajo različne organizacijske enote z različnimi cilji in uporabljajo druge metodologije. Tako je tudi v Dobri banki, kjer sta oba oddelka za svoje potrebe ločeno ustvarila dokumentacijo o procesu izvršb. Če bi med seboj sodelovali, bi pripomogli k bolj učinkovitemu obvladovanju tveganj. Sočasni nadzor tveganj in procesov ter skupno ustvarjanje dokumentacije o procesu bi bilo cenejše tudi z vidika dela, saj procesa ni potrebno spremljati in dokumentirati dvojno. Zato je pomembno, da se v Dobri banki MOT naprej razvija, saj je spremljanje tveganj po procesih še vedno v začetni fazi. Vzpostaviti je potrebno disciplino med zaposlenimi, da bodo dosledno poročali o vsakršnih odstopanjih in tudi sami poskrbeli, da je v procesih možnosti za realizacijo tveganj čim manj. V tesnem sodelovanju z MPP pa morajo pridobljene podatke o tveganjih sproti analizirati in na podlagi ugotovitev proces neprestano prenavljati. Menim, da se zato v prihodnosti v podjetjih lahko še precej naredi na izboljšanju sodelovanja in razvoju skupnih metodologij za izboljševanje procesov in zmanjševanja tveganj.

LITERATURA IN VIRI

1. Alhawari, S., Thabtah, F., Karadsheh, L., & Hadi, W. M. (2008). A Risk Management Model for Project Execution. *Proceedings of the 9th International Business Information Management Association Conference (IBIMA), Conference on Information Management in Modern Organizations: Trends & Challenges* (str. 887–893). Marrakech: IBIMA.
2. Balestra, A. (b.l.). Quantification of Operational Risk. *Global risk guard.* Najdeno 15. maja 2012 na spletnem naslovu http://www.globalriskguard.com/virtual-library/operational-risk/
3. Basel Committee on Banking Supervision. (2001). *Consultative Document: Operational Risk*. Basel: Bank for International Settlements.
4. Basel Committee on Banking Supervision. (2006). *A Revised Framework Comprehensive Version: International Convergence of Capital Measurement and Capital Standards*. Basel: Bank for International Settlements.
5. Becker, J., Kugeler, M., & Rosemann, M. (2003). *Process management: a guide for the design of business processes.* Berlin: Springer.
6. *Business Performance Management Standards Group Formed.* Najdeno 5. novembra 2012 na spletnem naslovu http://www.bptrends.com/news_items.cfm?newsTypeID=79C2F33A-2B3B-46FF-98CAF151E1D09360#0614DDA9-3048-2905-E660C1C0D07FB5F8
7. Cernauskas, D., & Tarantino, A. (2009). Operational risk management with process control and business process modeling. *The Journal of Operational Risk, 4*(2), 3–17.
8. Chakravorty, S. S. (2010, 25. januar). Where Process-Improvement Projects Go Wrong. *Wall Street Journal.* Najdeno 5. januarja 2012 na spletnem naslovu http://online.wsj.com/article/SB10001424052748703298004574457471313938130.html
9. Champagne, P., Ramesh, A., Baron, C., Sempangi, H., Cracknell, D., & Wright, G. (2008). A Toolkit For Process Mapping for MFIs. Najdeno 15. maja 2012 na spletnem naslovu http://www.microsave.org/toolkit/process-mapping-and-risk-analysis-toolkit
10. Chatterjee, S., & Gordon, G. (2011). Dealing with Consumer Default: Bankruptcy vs Garnishment. *Working papers*, (11–35). Najdeno 5. aprila 2012 na spletnem naslovu www.philadelphiafed.org/research-and-data/publications/working-papers/
11. Cheng, F., Gamarnik, D., Jengte, N., Min, W., & Ramachandran, B. (2005). IBM Research report: Modeling Operational Risks in Business Processes. *RC23672*. Najdeno 22. oktobra 2012 na spletnem naslovu http://domino.watson.ibm.com/
12. Dahen, H., & Dionne, G. (2010). Scaling models for the severity and frequency of external operational loss data. *Journal of Banking and Finance, 34*(7), 1484–1496.
13. Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key Risk Indicators – Their Role in Operational Risk Management and Measurement. *RiskBusiness International Limited.*
14. Delavari, H., Wasana, B., Marjanovic, O., & Mathiesen, P. (2010). Business Process Management (BPM) Education in Australia: A Critical Review Based on Content Analysis. *21st Australasian Conference on Information Systems Proceedings*. Brisbane: Queensland University of Technology, Brisbane, Qld.

15. Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., & Reinard, D. (2007). Operational risk management in financial institutions: Process assessment in concordance with Basel II. *Journal Software Process: Improvement and Practice - Special Issue using ISO-IEC 15504*, *12*(4), 321–330.
16. Dickstein, D. I., & Flast, R. H. (2009). *No Excuses: A Business Process Approach to Managing Operational Risk*. Hoboken: Wiley.
17. Dobra banka (2010a). *Navodila za prijavo škodnih dogodkov* (interno gradivo). Ljubljana: Dobra banka.
18. Dobra banka. (2010b). *Navodila za delo v oddelku OPPP* (interno gradivo). Ljubljana: Dobra banka.
19. Dobra banka. (2011). *Pravilnik o operativnih tveganjih* (interno gradivo). Ljubljana: Dobra banka.
20. Dobra banka. (2012). *Poročila o škodnih dogodkih* (interno gradivo). Ljubljana: Dobra banka.
21. Eppler, M. J., & Aeschimann, M. (2009). A systematic framework for risk visualization in risk management and communication. *Risk Management, 11*, 67–89.
22. Fehér, P. (2009). Process-based Risk Management. *Bacee coference on operational risk in banks, Budapest*. Najdeno 15. septembra 2012 na spletnem naslovu http://www.slideshare.net/pethich/process-based-risk-management
23. Fionda, S. (2009). The synergies and overlaps of Sarbanes- Oxley and Operational Risk. *IRM: SIG Financial Services.* Najdeno 5. novembra 2012 na spletnem naslovu http://www.theirm.org/events/financial_services_erm.htm
24. Gospodarska zbornica Slovenije. (2010). Plačilna nedisciplina – razlogi in predlogi, stališče GZS. Najdeno 10. aprila 2012 na spletnem naslovu http://www.gzs.si/slo/skupne_naloge/stalisca/vsa_stalisca/placilna_nedisciplina/49250
25. Groznik, A., & Vičič, D. (2007). Menedžment poslovnih procesov in operativnih tveganj. *Uporabna informatika, 15*(2), 65–69.
26. Harmon, P. (2007). *Business Process Change: A Guide for Business Managers and BPM and Six Sigma Professionals*. Amsterdam: Elsevier.
27. Helquist, J. H., Deokar, A., Cox, J. J., & Walker, A. (2012). Analyzing process uncertainty through virtual process simulation. *Business Process Management Journal, 18*(1), 4–19.
28. Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *Journal of Risk and Insurance, 78*(4), 795–822.
29. Huang, S. M., Yen, D. C., Hung, Y. C., Zhou, Y. J., & Hua, J. S. (2009). A business process gap detecting mechanism between information system process flow and internal control flow. *Decision Support Systems, 47*(4), 436–454.
30. Infranca, J. (2009). Safer than the Mattress? Protecting Social Security Benefits from Bank Freezes and Garnishments. *St. John's Law Review, 12*(4), 1127–1192.
31. Interfacing Technologies Corporation. (2011). Risk Management: Asses your risks to ensure an effective governance. Najdeno 10. septembra 2012 na spletnem naslovu http://interfacing.com/ComplianceSOX-ISO-BASEL-Six-Sigma-Risk/Risk
32. Jallow, A. K., Majeed, B., Vergidis, K., Tiwari, A., & Roy, R. (2007). Operational risk analysis in business processes. *BT Technology Journal, 25*(1), 168–177.

33. Jolly, A. (2003). *Managing Business Risk*. London: Kogan Page.
34. Jurič, M. B., & Pant, K. (2008). *Business Process Driven Soa Using Bpmn and Bpel*. Birmingham: Packt Publishing.
35. *Kaj je SEPA.* Najdeno 20. aprila 2013 na spletnem naslovu http://www.sepa.si/slo/Sepa/uvod.htm
36. *Kode namena plačila – NLB.* Najdeno 1. aprila 2013 na spletnem naslovu http://www.nlb.si/sepa-koda-namena
37. Kovačič, A. (2008). Informatizacija delovnih procesov WF, GW in ERP (prosojnice s predavanj). Najdeno 28. aprila 2013 na spletnem naslovu miha.ef.uni-lj.si/_dokumenti3plus2/190047/ISDP-WF-ERP-WF-08.PPT
38. Kovačič, A., & Bosilj Vukšić, V. (2005). *Management poslovnih procesov: prenova in informatizacija poslovanja s praktičnimi primeri*. Ljubljana: GV založba.
39. Križnik, B. (2012, 28. april). Zgodbe rubežnikov: tragedije, drame, kriminalke. *Delo,* (98), 9.
40. Lampret, A., & Mislej, S. (2011). Celovita informacijska podpora procesu izterjave. *infoSRC, 64*(1), 12–16.
41. Lawrence, A. G., Loeb, M. P., & Tsengb, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301–327.
42. Majič, M. (2002). Operativno tveganje: definicija, regulacija in merjenje. *Zbornik 8. strokovnega posvetovanja o bančništvu* (str. 47–60). Portorož: Zveza Ekonomistov Slovenije.
43. McCormack, K., & Johnson, W. C. (2001). *Business Process Orientation: Gaining the E-Business Competitive Advantage*. Boca Raton: St. Lucie Press.
44. McCormack, K., Willems, J., Van den Bergh, J., Deschoolmeester, D., Willaert, P., Indihar Štemberger, M., Škrinjar, R., Trkman, P., Ladeira, M. B., de Oliveira, M. P. V., Bosilj Vuksić, V., & Vlahović, N. (2009). A Global Investigation of Key Turning Points in Business Process Maturity. *Business Process Management Journal, 15*(5), 792–815.
45. Mendling, J., Reijers, H. A., & van der Aalst, W. M. P. (2010). Seven process modeling guidelines (7PMG). *Information and Software Technology, 52*(2), 127–136.
46. Mihajlović, N. (2012). E-izvršba postaja prijaznejša do upnikov. *Finance*, (42), 10.
47. Mora Campos, H. E. (2008). *Desarrollo de aplicacion para gestion de riesgo operacional en procesos.* Santiago de Chile: Facultad de Ciencias Fisicas y Matematicas.
48. Nadzorni svet Združenja bank Slovenije. (2007). Navodilo o izvrševanju sklepov o izvršbi pri bankah. Najdeno 1. februarja 2013 na spletnem naslovu http://www.zbs-giz.si/zdruzenje-bank.asp?StructureId=887
49. Norimarna, S. (2010). Operational Risk Management Based on Business Process Approach. Najdeno 10. septembra 2012 na spletnem naslovu http://crmsindonesia.org/programs/research/operational-risk-management-based-business-process-approach
50. Nota, G., & Di Georgio, M. P. (2010). A model for process oriented risk management. *Intechopen.* Najdeno 15. maja 2012 na spletnem naslovu

http://www.intechopen.com/books/advances-in-risk-management/a-model-for-process-oriented-risk-managenent

51. *Operational losses, much more than a tail only*. Najdeno na 5. oktobra 2012 na spletnem naslovu http://riskfriends.wordpress.com/2009/04/12/operational-losses-much-more-than-a-tail-only/
52. Panjer, H. (2006). *Operational Risk: Modeling Analytics*. Hoboken: Wiley Interscience.
53. *Poslovni subjekti z dospelimi neporavnanimi obveznostmi nad 5 dni neprekinjeno, zadnje poročilo.* Najdeno 10. aprila 2012 na spletnem naslovu http://www.ajpes.si/Statistike/Statistike_placilnega_prometa/Neporavnane_obveznosti/Zadnje_porocilo?id=176
54. *Poslovni subjekti z dospelimi neporavnanimi obveznostmi po mesecih in dnevih, za leta 2003 do 2011*. Najdeno 10. aprila 2012 na spletnem naslovu http://www.ajpes.si/Statistike/Statistike_placilnega_prometa/Neporavnane_obveznosti/Arhiv
55. Pravilnik o obrazcih, vrstah izvršb in poteku avtomatiziranega izvršilnega postopka. *Uradni list* RS št. 104/2011.
56. Qureshi, A. A. (2010). Operational Risk & Basel II. Najdeno 1. februarja 2013 na spletnem naslovu http://www.slideshare.net/arsqureshi/operational-risk-management-3609474
57. Recker, J. C. (2010). Opportunities and constraints: the current struggle with BPMN. *Business Process Management Journal, 16*(1), 181–201.
58. *Register transakcijskih računov, splošno.* Najdeno 10. marca 2013 na spletnem naslovu http://www.ajpes.si/registri/transakcijski_racuni/splosno
59. Rikhardsson, P., Best, P., Green, P., & Rosemann, M. (2006). Business Process Risk Management, Compliance and Internal Control: A proposed Research Agenda in the context of Compliance and ERP systems. *Proceedings of the Second Asia/Pacific Research Symposium on Accounting Information Systems.* Melbourne: IJAIS.
60. Rotaru, K., Wilkin, C., Churilov, L., Neiger, D., & Ceglowski, A. (2011). Formalizing process-based risk with Value-Focused Process Engineering. *Information Systems and e-Business Management, 9*(4), 447–474.
61. Rotovnik, T. (2003). Operativno tveganje in Basel II- Pripravljenost bank v Sloveniji na zahteve novega kapitalskega sporazuma. *9. strokovno posvetovanju o bančništvu* (str. 1–14). Ljubljana: Zveza ekonomistov Slovenije.
62. Ryan, O., & Hida, E. (2007). Global Risk Management Survey: Fift Edition- Accelerating Risk Management Practices. *Delloite*. Najdeno 10. oktobra 2012 na spletnem naslovu www.deloitte.com
63. Sackmann, S. (2008). A reference model for process- oriented IT risk managemnet. *Proceedings of the 16th European Conference on Information Systems (ECIS'08).* Galway: National University of Ireland.
64. Sangeetha, J., & Mahalingam, S. (2011). Service quality models in banking: a review. *International Journal of Islamic and Middle Eastern Finance and Management, 4*(1), 83–103.

65. Skok, A. B., Peterlin, J., & Ribarič, P. (2005). *Obvladovanje tveganja: skrivnosti celovitega pristopa*. Ljubljana: GV založba.
66. Stalk, G., Evans, P., & Schulman, L. E. (1992). Competing on capabilities: the new rules of corporate strategy. *Harvard Business Review, 70*(2), 57–70.
67. Škrinjar, R., & Trkman, P. (2013). Increasing Process Orientation with Business Process Management: Critical Practices. *International Journal of Information Management, 33*(1), 48–60.
68. Škerlavaj, M., Indihar Štemberger, M., Škrinjar, R., & Dimovski, V. (2007). Organizational learning culture- the missing link between business process change and organizational performance. *International Journal of Production Economics 106*(2), 346–367.
69. Tafri, F. H., Rahman, R. A., & Omar, N. (2011). Empirical evidence on the risk management tools practised in Islamic and conventional banks. *Qualitative Research in Financial Markets, 3*(2), 86–104.
70. Tepina, N. (2010). *Obvladovanje operativnega tveganja z managementom poslovnih procesov.* Diplomsko delo. Ljubljana: Ekonomska fakulteta.
71. ter Hofstede, A. H. M., Mecella, M., & Sardina, S. (2012). Knowledge-Intensive Business Processes. *Proceedings of the 1st International Workshop on Knowledge-intensive Business Processes, 861*. Rome: CEUR.
72. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2009). *Internal Control — Integrated Framework: Guidance on Monitoring Internal Control Systems*. Durham: The Committee of Sponsoring Organizations of the Treadway Commission.
73. Tozer-Pennington, V. (2009). The benefits of alignment. *Operational Risk & Regulation*. Najdeno 30. septembra 2012 na spletnem naslovu http://www.risk.net/operational-risk-and-regulation/feature/1530778/the-benefits-alignment
74. Trkman, P. (2010). The critical success factors of business process management. *International Journal of Information Management, 30*(2), 125–134.
75. Trkman, P., & McCormack, K. (2009). Supply chain risk in turbulent environments- A conceptual model for managing supply chain network risk. *International Journal of Production Economics, 119*(2), 247–258.
76. Trkman, P., & McCormack, K. (2010). Estimating the benefits and risks of implementing e-procurement *IEEE Transactions on Engineering Management, 57*(2), 338–349.
77. Utratnik, J., & Grasselli, P. (b. l.). Upravljanje operativnih tveganj v finančnih inštitucijah. Najdeno 30. septembra 2012 na spletnem naslovu www.isaca.si
78. van der Hoeven, H. (2009). *Erp and Business Processes.* Coral Springs: Llumina Press.
79. vom Brocke, J., & Rosemann, M. (2010a). *Handbook on Business Process Management 1: Introduction, Methods, and Information Systems*. Berlin: Springer.
80. vom Brocke, J., & Rosemann, M. (2010b). *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture*. Berlin: Springer.
81. Weiß, B., & Winkelmann, A. (2011). Developing a Process-oriented Notation for Modeling Operational Risks – A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry.

HICSS '11 Proceedings of the 2011 44th Hawaii International Conference on System Sciences (str. 1–10). Kauai: Institute of Electrical and Electronics Engineers (IEEE).

82. Willaert, P., Van den Bergh, J., Willems, J., & Deschoolmeester, D. (2007). The Process-Oriented Organisation: A Holistic View Developing a framework for business process orientation maturity. *Business Process Management, Lecture Notes in Computer Science* (str. 1–15). Berlin: Springer.
83. Zakon o izvršbi in zavarovanju. *Uradni list* RS št. 3/2007-UPB4, 93/2007, 6/2008 Skl.US: U-I-354/07-6, 37/2008-ZST-1, 45/2008-Zarbit, 113/2008 Odl.US: U-I-344/06-11, 28/2009, 47/2009 Odl.US: U-I-54/06-32 (48/2009 popr.), 57/2009 Skl.US: Up-1801/08-10, U-I-237/08-10, 51/2010, 26/2011, 14/2012.
84. zur Muehlen, M. (2007). Operational Risk Management and BPM. *The Business Transformation Conference.* Washington: Stevens Institute of Technology.
85. zur Muehlen, M. (2008). Process Innovation vs. Governance, Risk and Compliance. *International BPM Standards Conference in Seoul, Korea, 2008.* Najdeno 10. septembra 2012 na spletnem naslovu http://www.slideshare.net/mzurmuehlen/process-innovation-vs-governance-risk-and-compliance-presentation-664426
86. zur Muehlen, M., & Rosemann, M. (2005). Integrating Risks in Business Process Models. *Proceedings of the 16th Australasian Conference on Information Systems.* Sydney: ACIS.

PRILOGE

Priloga 1: Podproces Obveznosti v vlogi sekundarne banke

Opis podprocesa

Ko sekundarna banka prejme sklep, ga prav tako mora vnesti v aplikacijo in nato preveriti podatke v sklepu (istovetnost imetnika). Če primarna banka že prej sama ne sporoči, jo sekundarna pozove, naj ji sporoči, koliko sredstev ji primanjkuje. Če pošljejo odgovor, se ravnajo po navodilih in prenesejo toliko, kot primarna banka zahteva. Če pa do 14. ure ne prejmejo obvestila, zarubijo sredstva v višini, kot je to navedeno v obvestilu, in jih prenesejo na račun primarne banke (v kolikor ta sredstva imajo). Če sekundarne banke nakažejo preveč sredstev, višek sredstev ostane na primarnem računu.

Slika: Model podprocesa Obveznosti v vlogi sekundarne banke