

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

**PODATKOVNI VIDIK UČINKOVITEGA OBVLADOVANJA
OPERATIVNEGA TVEGANJA**

Ljubljana, junij 2009

MATEJA MOZETIČ MERHAR

IZJAVA

Študentka Mateja Mozetič Merhar izjavljam, da sem avtorica tega magistrskega dela, ki sem ga napisal/a pod mentorstvom dr. Aleksandre Gregorič in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega/specialističnega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____

Podpis: _____

1	UVOD	1
2	NOVI KAPITALSKI SPORAZUM – BASEL II	4
2.1	OD BASLA I DO BASLA II.....	4
2.2	ZAHTEVE BASLA II V EU IN SLOVENIJI	6
2.3	OPERATIVNO TVEGANJE	6
2.3.1	<i>Zahteve glede zbiranja podatkov</i>	7
3	DEFINIRANJE OPERATIVNEGA TVEGANJA	9
3.1	DEFINICIJA PO BASLU II.....	9
4	IDENTIFIKACIJA RELEVANTNIH TVEGANJ	12
4.1	STANDARDIZACIJA KATEGORIJ PO BASLU II.....	13
4.1.1	<i>Poslovna področja</i>	13
4.1.2	<i>Kategorije škodnih dogodkov</i>	14
5	ZBIRANJE PODATKOV	14
5.1	UPRAVIČENOST ZBIRANJA PODATKOV	15
5.2	OBLIKOVANJE PODATKOVNEGA MODELA IN STANDARDI	16
5.2.1	<i>Standardi zbiranja podatkov</i>	17
5.2.1.1	Vrste škodnih dogodkov.....	17
5.2.1.2	Spodnja meja zbiranja podatkov	18
5.2.1.3	Podatki o škodnem dogodku	19
5.2.2	<i>Zaupnost podatkov</i>	24
5.3	KRITIČEN VIDIK KATEGORIZACIJE ŠKODNIH DOGODKOV	24
5.3.1	<i>Tridimenzionalna kategorizacija</i>	26
5.4	POLITIKA ZBIRANJA PODATKOV	28
5.5	PROCES ZBIRANJA PODATKOV	28
5.5.1	<i>Infrastruktura</i>	30
5.5.1.1	Vloge in odgovornosti	30
5.5.1.1.1	Vloge v okviru podatkovne baze.....	31
5.5.1.2	Podporna tehnologija.....	31
5.5.2	<i>Izvedba</i>	33
5.5.3	<i>Nadzor in kontrola</i>	34
5.5.3.1	Postopki validacije	35
5.6	IZZIVI ZBIRANJA PODATKOV V PRAKSI	36
5.6.1	<i>Redkost večjih škodnih dogodkov</i>	36
5.6.2	<i>Razmejevanje podatkov od kreditnega in tržnega tveganja</i>	38
5.6.3	<i>Odvisnost od danih razmer</i>	39
5.6.4	<i>Relevantnost prijavljenih škodnih dogodkov</i>	40
6	CELOVITOST PODATKOVNEGA MODELA	40

6.1	KLJUČNI INDIKATORJI TVEGANJA	41
6.2	SAMOOCENJEVANJE	45
6.2.1	<i>Točkovanje</i>	47
6.3	ZUNANJI PODATKI	48
6.3.1	<i>Viri zunanjih podatkov</i>	50
6.3.1.1	Baze na osnovi javnih podatkov	50
6.3.1.2	Baze konzorcijev bank	51
6.3.2	<i>Izzivi pri uporabi zunanjih podatkov v praksi</i>	52
6.4	PODATKI NA OSNOVI SCENARIJEV	54
7	ANALIZA PODATKOV IN POROČANJE	56
8	KULTURA IN OSTALI KLJUČNI POGOJI UČINKOVITEGA OBVLADOVANJA OPERATIVNEGA TVEGNJA	60
8.1	ZNAČILNOSTI KULTURE	62
8.2	IZZIVI PRI VZPOSTAVITVI KULTURE V PRAKSI.....	63
8.3	UKREPI ZA VZPOSTAVITEV USTREZNE KULTURE	64
8.4	VODSTVO IN ORGANIZACIJSKA STRUKTURA	66
8.4.1	<i>Organizacijska struktura</i>	66
9	SLOVENSKA BANČNA PRAKSA	69
9.1	PRIMERI ŠKODNIH DOGODKOV	69
9.2	UPRAVLJANJE Z OPERATIVNIM TVEGANJEM.....	70
9.3	UPRAVLJANJE S PODATKI O OPERATIVNEM TVEGANJU.....	71
9.4	PRAKTIČNI PRIMER APLIKACIJE ZA ZBIRANJE PODATKOV O ŠKODNIH DOGODKIH.....	73
9.4.1	<i>Zajem škodnih dogodkov</i>	73
9.4.2	<i>Izdelava poročil</i>	74
9.4.3	<i>Prednosti in slabosti rešitve</i>	74
10	SKLEP	75
	LITERATURA	78
	VIRI	83
	PRILOGE	
	SLOVARČEK SLOVENSКИH PREVODOV TUJIH IZRAZOV	

1 UVOD

Z letom 2007 je stopil v veljavo novi kapitalski sporazum, poimenovan Basel II.

Inovacije in razvoj kompleksnih produktov, strategij in e-bančništva so postali stalnica sodobnega bančnega poslovanja, specializirani poslovni procesi so vse bolj odvisni od informacijske tehnologije, število združenj in nakupov bank, zlasti na mednarodnem nivoju, narašča, zunanji dobavitelji predstavljajo pomemben dejavnik poslovanja. Te spremembe so v zadnjem desetletju narekovale vse večje kritike predhodnega kapitalskega sporazuma – Basla I. Ena izmed poglobitvenih pomanjkljivosti starega sporazuma je postala tudi eden največjih izzivov novega: vključitev kapitalske zahteve za zavarovanje pred operativnim tveganjem. S tem je operativno tveganje (v nadaljevanju: OT) postalo tveganje, ki ga je potrebno upravljati preudarno, skupaj s kreditnim in tržnim tveganjem, in se je tako znašlo v središču pozornosti bančne industrije.

Odgovor bančnih ustanov na nove regulatorne zahteve in predvsem na odmevne dogodke v zadnjem desetletju, ki so povzročali velike izgube in celo propade institucij, je v učinkovitem obvladovanju OT. S tem namenom je potrebno vzpostaviti ustrezen okvir upravljanja z OT, kar pomeni, da se morajo kot nepretrgan proces v smislu nenehnih izboljšav in prilagajanj novim oz. spremenjenim razmeram odvijati posamezne faze: od identifikacije tveganj, kjer je potrebno (če poenostavimo) poiskati odgovore na vprašanja »Kakšni škodni dogodki se lahko zgodijo, zakaj in kakšne so njihove možne posledice in učinki?«, ocenjevanja, kjer se iščejo odgovori na vprašanja »Kakšna je verjetnost, da se škodni dogodek zgodi in kakšna bo višina škode, če se zgodi?«, rednega spremljanja dejansko realiziranih škodnih dogodkov, njihove analize in ustreznega poročanja do faze, kjer se s pomočjo vprašanj »Kako se zoper ugotovljena tveganja in potencialne škodne dogodke braniti, jih preprečiti oziroma zmanjšati njihove vplive?« poskuša izbrati ustrezne inštrumente obvladovanja OT.

Področje OT je obsežno. S tem delom želim izpostaviti tiste kategorije, ki po mojem mnenju lahko služijo kot izhodišče oziroma so ključne pri samih začetkih vzpostavljanja ustreznega okvira upravljanja. Želim torej najti pot do zagotavljanja učinkovitega obvladovanja OT. V tem delu bo zato večkrat kot samo obvladovanje OT uporabljeno upravljanje z OT.

Smiselno je začeti s podatki, natančneje z zbiranjem podatkov o škodnih dogodkih iz OT. Ne glede na to, da je baza podatkov eksplicitna zahteva naprednejših pristopov¹ v okviru Basla II in da brez nje pravzaprav ni osnov za objektivno ocenjevanje OT banke, je to tudi pot za postopno uvajanje nove kulture v bančno poslovanje z ustreznim zavedanjem o pomembnosti OT.

¹ Tako imenovana standardizirani in napredni (AMA) pristop.

Če povzamem enega izmed najbolj priznanih strokovnjakov s tega področja, se mora banka ob ustreznem definiranju, zbiranju in interpretaciji podatkov soočiti z naslednjimi izzivi in nalogami (Cruz, 2002, str. 10): a) vzpostaviti dosledno definicijo vsake vrste OT, ki mu je izpostavljena, in identificirati podatke, ki so v zvezi s posamezno vrsto tveganja pomembni za banko; b) razviti in implementirati ustrezen mehanizem za zbiranje definiranih podatkov; c) razlagati izhodne informacije ter oceniti stopnjo posamezne vrste OT, ki mu je banka izpostavljena.

Predpogoj k temu je zagotavljanje skladnosti poslovanja in aktivnosti z regulatornimi zahtevami. S strani regulatorja je predpisana široka usmeritev, banka pa mora zase glede na svoje specifičnosti določiti podrobnosti in ustrezne postopke zbiranja. Ob temu se mora opredeliti do različnih vprašanj in jih v okviru politike zbiranja podatkov vgraditi v obliki standardov, med drugim glede vrste in kategorij škodnih dogodkov ter podrobnih podatkov v zvezi z najnižjo mejo zbiranja podatkov, varovanja zaupnosti ter vlogami in odgovornostmi zaposlenih. Zaradi raznolikosti in množice podatkov, povezanih z OT, je takšna standardizacija pomembna za konsistentnost nadaljnjih analiz podatkov.

Zbrane podatke je potrebno namreč tudi ustrezno analizirati in z njimi seznaniti predvsem različne ravni posloводства. V ta namen mora banka vzpostaviti takšne postopke, ki bodo zagotavljali iz zbranih podatkov pridobiti relevantne, zanesljive in pravočasne informacije o profilu OT. Ne glede na to, da naj bi s tem omogočili ustrezno prepoznavanje šibkih točk v poslovnih procesih in s tem možnosti za izboljšanje, pravilno oblikovali cene produktov in storitev ter postavili temelje za modeliranje ekonomskega kapitala pri naprednih pristopih (Kralj, 2005, str. 20), pa se zastavlja vprašanje, ali zgolj informacije na podlagi notranjih podatkov za pregled nad celovito izpostavljenostjo OT v praksi zadoščajo. Izkušnje namreč kažejo, da zbiranje podatkov spremlja vrsto dilem in težav.

Ključni problem, ki se pojavlja pri OT, je nepripravljenost govoriti javno in odkrito o škodnih dogodkih iz tega naslova. Malo jih je takšnih, ki pričakujejo, da bo trgovec v banki ustvarjal samo pozitivne prihodke ali da kreditni referent ne bo nikoli imel slabega kredita. Po drugi strani pa se težko pričakuje, da bo enako mišljenje tudi pri OT. Kako torej motivirati zaposlene, da bodo pripravljeni razkrivati svoje napake in zagotavljati konsistentne podatke iz OT? Odgovor, ki se skriva v ustrezni organizacijski kulturi, pa ni ravno enostaven, o čemer priča tudi dejstvo, da so v eni od raziskav kot največjo oviro pri vzpostavljanju okvira upravljanja z OT poleg težav z zbiranjem podatkov vprašani navedli prav slabo zavedanje o tej problematiki med zaposlenimi (Operational Risk Management in the Financial Service Industry, 2004).

Zato je eden izmed prvih izziv kompleksnega procesa vzpostavitve okvira upravljanja z OT tudi pridobitev popolne podpore uprave banke in višjega managementa. Z ustreznim delovanjem vodstva, z izobraževanjem in rednim obveščanjem ter različnimi motivacijskimi mehanizmi bodo zaposleni dobili ustrezne signale o pomenu področja OT v banki. Vsak zaposleni je namreč lahko vir OT, vsak zaposleni ga lahko prepozna oziroma

odkrije, zato je odločilnega pomena, da so vsi pripravljeni sodelovati v temu procesu. Le tako je zagotovljeno konsistentno zbiranje podatkov.

Namen magistrskega dela je torej podrobno in kritično proučiti ključne dejavnike, ki so potrebni za vzpostavitev učinkovitega okvira upravljanja z OT, oziroma tiste, ki so po mojem mnenju pomembni pri samih začetkih. Zagotovo se vsaka institucija srečuje s projekti, ki so propadli zaradi slabo »zgrajenih temeljev«. Zato menim, da je tem aktivnostim potrebno posvetiti največ pozornosti. Za področje OT nam to med drugim še posebej narekujejo njegova širina in kompleksnost, povsem nov vidik gledanja na to področje ter množica dilem in nejasnosti, ki so bile izpostavljene v številnih razpravah.

Magistrsko delo je razdeljeno na devet vsebinskih sklopov. Glede na pomen in vlogo, ki jo ima Basel II v celotnem procesu upravljanja z OT, se ne bom mogla izogniti njegovi osnovni predstavitvi v drugem poglavju, ki sledi uvodnemu besedilu. V okviru tega bom izpostavila nekatere konkretne zahteve predvsem z vidika zbiranja notranjih podatkov. Širši pregled teh zahtev bi presegal namen tega dela, bom pa v posameznih poglavjih poskušala vsebinske sklope povezati z eksplicitnimi regulatornimi zahtevami. Tretje in četrto poglavje bosta namenjeni vzpostavljanju enotnih smernic in posledično tudi zbiranja podatkov: kot prvo z definiranjem OT in kot drugo s standardizacijo ključnih kategorij OT, ki jo zagotovimo s pomočjo identifikacije za banko relevantnih tveganj.

Sklop naslednjih treh poglavij bo namenjen podatkovnemu modelu, ki je osnova za celovit pregled izpostavljenosti banke OT. V petem poglavju bom tako predstavila poglavitne faze vzpostavitve mehanizma za zbiranje podatkov, kjer bom izpostavila tudi ključne težave, zaradi katerih se zbiranje v praksi sooča s številnimi izzivi. Najboljša rešitev je zagotovitev celovitega podatkovnega modela, ki vključuje poleg notranjih podatkov še zunanje podatke, ključne dejavnike tveganj ter podatke na osnovi analize scenarijev in samoocenjevanja, ki so podrobneje opisani v šestem poglavju. S sedmim poglavjem bom še posebej opozorila na pomen ustrezne analize in poročanja na podlagi podatkov iz OT.

Zbiranje podatkov ne more biti učinkovito brez ustrezne integracije OT v splošno organizacijsko strukturo kot dela sistema za upravljanje s tveganji in brez ustrezne podpore najvišjih vodstvenih ravni. Prav ti so tudi odgovorni za vzpostavitev ustrezne kulture, ki vzpodbuja zaposlene, da govorijo odkrito o OT. Tej problematiki bom namenila osmo poglavje.

Magistrsko delo bom zaključila s pregledom slovenske bančne prakse na področju OT. V okviru tega bom kot prvo izpostavila nekaj bolj odmevnih škodnih dogodkov. V nadaljevanju bom predstavila ugotovitve, v kakšni fazi razvoja upravljanja z OT in konkretno osnovanja ustreznega podatkovnega modela so slovenske banke, in zaključila s konkretnim primerom aplikacije za zbiranje notranjih podatkov o škodnih dogodkih.

Metoda magistrskega dela je zasnovana tako, da vključuje strokovno poglobitev in znanstveno raziskovalni pristop k preučevani tematiki. Pri preučevanju literature sem

uporabljala predvsem metode analize vsebine, primerjave teoretičnih ugotovitev ter kritične presoje zaključkov. Ob temu sem poskušala preučiti in analizirati izkušnje dobre prakse naprednejših držav na področju OT in njihova spoznanja, ki so se pokazala kot uporabna, in jih prenesti v svoje delo. Slovenska bančna praksa (na področje bančništva se bom v magistrskem delu tudi omejila) je namreč na temu področju na začetku, strokovna literatura pa omejena na redke prispevke posameznih avtorjev s področja OT, ki praviloma tudi povzemajo izkušnje tujih strokovnjakov. Skladno s tem se bom opirala predvsem na strokovno literaturo tujih avtorjev, raziskav in razprav ter na različne vire, kot so članki, poročila, internetne strani.

2 NOVI KAPITALSKI SPORAZUM – BASEL II

Basel II je v bančnem okolju poznano poimenovanje za drugi kapitalni sporazum, ki ga je predlagal Baselski komite za bančni nadzor (v nadaljevanju: Baselski komite)² v okviru Banke za mednarodne poravnave. V veljavo je stopil 1.1.2007 kot nadgradnja Basla I.

2.1 Od Basla I do Basla II

S tako imenovanim Baslom I se je leta 1988 pričel spodbujati proces, ki je od bank zahteval rezervacije dela kapitala, namenjenega za povračilo morebitnih izgub, ki bi jih povzročilo kreditno in kasneje tržno tveganje.

V ta namen je tedaj Baselski komite izdal dokument »Mednarodno usklajevanje merjenja kapitala in kapitalnih standardov«, bolj znan kot Baselski kapitalni standardi oziroma Basel I, s katerim so želeli uvesti poenotena pravila za izračun tako imenovane minimalne kapitalne zahteve³ za banke v mednarodnem poslovanju. Na tej osnovi so regulatorji oz. centralne banke tudi kontrolirale poslovne banke. Kljub temu da je bil formalen dogovor držav G-10 o njegovi uporabi sprejet le za mednarodno aktivne banke, se je sporazum dejansko implementiral v izredno velikem številu bank po svetu, ne glede na raven njihove kompleksnosti oziroma velikosti. Zahteve Basla I so bile sprejete v skoraj 100 državah (Rotovnik, 2004a, str.43).

Leta 1999 pa je v skladu s številnimi spremembami, ki so jih narekovale inovacije in razvoj v bančni industriji (npr. elektronsko bančništvo in izvedeni finančni instrumenti) ter

² Baselski komite je mednarodna skupina centralnih bank in regulatorjev s sedežem v uradu Banke za mednarodne poravnave v švicarskem Baslu, ki so ga leta 1974 ustanovili guvernerji centralnih bank držav članic G-10, kamor spada deset najrazvitejših držav: Belgija, Francija, Japonska, Kanada, Luksemburg, Nemčija, Nizozemska, Švedska, Velika Britanija in ZDA, s ciljem zagotoviti kakovosten nadzor dejavnosti bank po vsem svetu (Zabavnik, 2003, str. 36).

³ Gre za najmanjšo količino denarja, ki jo poslovna banka potrebuje za varno poslovanje.

razkritje velikih operativnih izgub v preteklem desetletju⁴, Banka za mednarodne poravnave napovedala uvedbo popolnoma prenovljenega okvira kapitalske ustreznosti.

Po večletnih razpravah, pogajanjih ter strokovnih in političnih diskusijah je Basel II stopil v veljavo 1.1.2007 in izpopolnjuje strukturo kapitalske ustreznosti, tako da omogoča organizacijam večjo fleksibilnost v zameno za večjo kontrolo. Na eni strani se fleksibilnost odraža v različnih (bolj ali manj sofisticiranih) pristopih za izračun kapitalske ustreznosti, ki jih predlaga novi kapitalski sporazum in jih banke lahko ustrezno uporabijo glede na svoje potrebe in kompleksnost poslovanja, po drugi strani pa je nov okvir kapitalskih pravil prirejen tako, da bo lahko dovolj »odziven na tržne in nadzorniške inovacije, saj bo le tako vzdrževal optimalno učinkovitost in konkurenčnost sektorja finančnih storitev« (Zakaj nova evropska kapitalska ureditev).

Basel II ima tri glavne komponente ali stebre (International Convergence of Capital Measurement and Capital Standards, 2006):

- Steber I: Minimalne kapitalske zahteve

Prvi steber postavlja minimalne zahteve glede kapitalskih standardov in uresničuje kvalitativne in kvantitativne zahteve za upravljanje s tveganji. Vpeljuje del kapitala, namenjenega posebej za potrebe OT.

- Steber II: Regulativni nadzor

Z drugim stebrom je poudarjena vloga nadzornih institucij pri preverjanju, ali banke pravilno ocenjujejo tveganja, ki so jim izpostavljene, in posledično zagotavljajo primerno kapitalsko ustreznost. V ta namen morajo banke vzpostaviti proces ocenjevanja ustreznosti notranjega kapitala glede na svoj profil tveganosti. Naloga nadzornika je preveriti ta proces.

- Steber III: Tržna disciplina

Tretji steber zadeva naravo in obseg javnega razkritja podatkov banke s področja upravljanja s tveganji. Ta steber naj bi bil vzvod za varnost in preglednost celotnega sistema in naj bi predstavljal zaokrožitev kapitalskih zahtev (Steber I) in nadzornega procesa (Steber II) (Rotovnik, 2002, str. 18).

⁴ Svetovna javnost je največ pozornosti namenila tako imenovanemu primeru Barings, ko je leta 1995 nekdanja močna angleška banka zaradi neavtoriziranega trgovanja utrpela izgube v višini 1,3 milijarde dolarjev in čez noč propadla. Operativne izgube pa so bile tudi sicer močno razširjene. Nekatera poročila navajajo, da naj bi finančne institucije zaradi operativnih problemov utrpeli več kot 7 milijard dolarjev izgub v letu 1998 in da je tovrstna izguba največjih finančnih institucij tudi 100 milijonov dolarjev letno (Smithson, 2000, str. 58).

2.2 Zahteve Basla II v EU in Sloveniji

Čeprav Basel II ni zavezujoč, saj je pripravljen v obliki priporočil predvsem za mednarodno aktivne banke in jih morajo s tem namenom sprejeti posamezni nacionalni regulatorji ter jih prilagoditi svojim lokalnim posebnostim (Davidson, 2004), je v evropskih bančnih krogih sprejet v celoti. Evropska unija ga je uveljavila s sprejemom Direktive o kapitalski ustreznosti⁵ (v nadaljevanju: Direktiva), ki je zavezujoča tako za banke kot investicijska podjetja v skladu z načelom uveljavljanja enakih pogojev poslovanja na enotnem evropskem trgu⁶.

V okviru slovenske zakonodaje so zahteve vpeljane z novim Zakonom o bančništvu (Zban-1, 2006) in ustreznimi podzakonskimi akti:

- Sklep o izračunu kapitalne zahteve za operativno tveganje za banke in hranilnice,
- Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice in
- Sklep o poročanju o kapitalu in kapitalskih zahtevah bank in hranilnic.

To pomeni popolni vpliv Basla II in njegovih kapitalskih zahtev tudi za Slovenijo.

2.3 Operativno tveganje

Basel II predstavlja nadgradnjo kapitalskih zahtev za banke, s tem da razširja in izboljšuje osnovno idejo obvladovanja merljivih (kreditno in tržno tveganje) ter nemerljivih tveganj. Ta nemerljiva tveganja so po velikih dogodkih, izmed katerih je največkrat omenjeni primer Barings⁷, postala opazna nadzornikom, ki so jih označili kot OT - kategorija, ki je

⁵ Direktiva obsega:

- Direktivo 2006/49/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 14. junija 2006 o kapitalski ustreznosti investicijskih podjetij in kreditnih institucij (preoblikovano) in
- Direktivo 2006/48/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 14. junija 2006 o začetku opravljanja in opravljanju dejavnosti kreditnih institucij (preoblikovano).

⁶ V nasprotju z EU so oblasti v ZDA pristopile k sprejemanju priporočil bolj zadržano: med drugim je z letom 2008 obvezna uporaba pravil Basla II za določanje kapitalskih zahtev po naprednih pristopih predpisana samo za največje mednarodno aktivne banke. Skoraj 6500 bank v ZDA pa bo lahko še naprej uporabljalo pravila starega kapitalnega sporazuma - Basel I (Rubin, 2003, str.1) ali pa bodo pristopile k zahtevam prenovljenega Basla I, poimenovanega Basel IA. Pripravljen je bil namreč za manjše in manj kompleksne banke v ZDA, in sicer z namenom izboljšati občutljivost za tveganje starega sporazuma obenem pa ohraniti njegovo enostavnost in jasnost (Kroszner, 2007).

⁷ Primer iz leta 1995 je odprl vrata obdobju velikih škodnih dogodkov in zato ostaja nekakšen sinonim za OT v bankah. Celotna izguba je bila večja od kapitala in rezerv, ki jih je imela banka. Morala je razglasiti stečaj in marca 1995 jo je kupila nizozemska banka ING za 1 angleški funt. Dogodek je šokiral vso bančno javnost. Vso izgubo je povzročil Nick Leeson, 28-letni borzni posrednik pri Baringsovi poslovalnici v Singapuru. Julija 1992 je Leeson začel špekulirati z delniškim indeksom NIKKEI 225. Do konca leta 1992 je izgubil že 3 milijone dolarjev, ki jih je skrtil na posebnem kontu. Banka mu je dopuščala, da je sam trgoval z indeksom in obenem sam nadziral knjige. Tako ni imel nobene kontrole nad svojim početjem. Do leta 1994 je ustvaril 250

od leta 1998 postala predmet eksplicitne usmerjenosti regulatorjev (Power, 2003, str. 6), kar je tudi ena največjih novosti Basla II.

Basel II v okviru prvega stebra in minimalnih kapitalskih zahtev vpeljuje evolucionaren pristop k obravnavi OT, saj vzpodbuja banke, da za izračun kapitalskih zahtev postopno razvijajo vse bolj za tveganje občutljive metodologije: od najbolj preprostega enostavnega pristopa preko standardiziranega pristopa k ciljnim najbolj sofisticiranim naprednim pristopom (pristop temelječ na internem merjenju, pristop s statistično porazdelitvijo, točkovni pristop).

Pri enostavnem pristopu je kapitalska zahteva opredeljena kot 15% triletnega povprečja neto obrestnih in neto neobrestnih prihodkov. Pri standardiziranem pristopu je izračun podoben, le da banka svoje aktivnosti razdeli na 8 poslovnih področij. Odstotek za opredelitev kapitalskih zahtev je različen po področjih in znaša 12%, 15% ali 18%. Pri naprednem pristopu banka izračunava kapitalsko zahtevo na podlagi notranjih sistemov merjenja OT, vendar mora za to pridobiti mnenje nadzornika.

Potem ko se banka kvalificira oz. zadosti ustreznim kvalitativnim in kvantitativnim kriterijem za uporabo bolj naprednega pristopa, postane ta pristop zanjo obvezen (International Convergence of Capital Measurement and Capital Standards, 2006, str. 144-149).

2.3.1 Zahteve glede zbiranja podatkov

Basel II poudarja pomembnost zbiranja podatkov. Ustrezne baze podatkov so celo predmet eksplicitne zahteve Basla II, in sicer za standardizirani in napredni pristop (International Convergence of Capital Measurement and Capital Standards, 2006):

1. »Banke morajo sistematično spremljati ustrezne podatke o operativnem tveganju.« (standardizirani pristop⁸).
2. »Banke morajo spremljati notranje podatke o izgubah.« ... »Spremljanje notranjih podatkov je pogoj za razvoj in delovanje verodostojnega sistema za merjenje operativnega tveganja. Notranji podatki so bistveni za povezavo med ugotovitvijo bančnega tveganja in njeno dejansko izkušnjo z izgubami.« (napredni pristopi).

Basel II vzpodbuja banke, da pričnejo s procesom zbiranja podatkov čim prej, saj zahteva, da so notranje izračunane mere OT zasnovane na podlagi najmanj petletnega obdobja opazovanja. Ko banka prvič preide na napredni pristop za merjenje OT, je sprejemljivo triletno obdobje.

milijonov izgube. Vrhunec njegovih izgub je bil potres na Japonskem, takrat je v enem dnevu izgubil 75 milijonov dolarjev (Mishkin, 2001, str. 238).

Preostale regulatorne zahteve naprednih pristopov v zvezi z notranjimi podatki (International Convergence of Capital Measurement and Capital Standards, 2006, 152-153), ki jih je preko Direktive v Sklepu o izračunu kapitalne zahteve za operativno tveganje za banke in hranilnice povzela tudi slovenska zakonodaja:

- Banke morajo biti sposobne razporediti svoje pretekle notranje podatke o izgubi po poslovnih področjih (raven 1 iz priloge 1), po vrstah dogodkov (raven 1 iz priloge 2) ter te podatke na zahtevo zagotoviti pristojnim organom. Postopki in merila za razvrščanje morajo biti dokumentirani.
- Zahteva se celovitost podatkov v smislu, da zajemajo vse bistvene dejavnosti in izpostavljenosti iz vseh ustreznih podsistemov in geografskih lokacij. Banke morajo biti zmožne utemeljiti, da katerekoli izključene dejavnosti ali izpostavljenosti, tako posamezno kot v kombinaciji, nimajo bistvenega vpliva na celotno oceno tveganja.
- Opredeliti je treba ustrezne spodnje meje izgube za zbiranje podatkov (t. i. prag zbiranja podatkov), npr. 10.000 EUR.
- Poleg informacij o bruto zneskih izgube banke kot minimum zbirajo informacije o datumu dogodka, morebitnih povračilih od bruto zneskov izgube, kakor tudi določene opisne informacije o dejavnikih ali vzrokih škodnega dogodka.
- Oblikujejo se merila za razporejanje podatkov o izgubi, ki izhaja iz dogodka v centralizirani funkciji oz. dejavnosti (npr. informatika), ki vpliva na več kot eno poslovno področje, kakor tudi iz povezanih dogodkov skozi čas.
- Izgube iz OT, ki so povezane s kreditnim tveganjem in so bile v preteklosti vključene v notranjih zbirkah podatkov o kreditnem tveganju, morajo biti evidentirane v zbirkah podatkov o OT in ločeno označene. Takšne izgube ne bodo predmet kapitalni zahtevi za OT, temveč se bodo za namene izračuna minimalnih kapitalnih zahtev obravnavale v okviru kreditnega tveganja.
- Izgube iz OT, ki so povezane s tržnimi tveganji, se vključijo v obseg kapitalne zahteve za OT.
- Banka mora imeti dokumentirane postopke za ocenjevanje ustreznosti preteklih podatkov o izgubi vključno s situacijami, pri katerih se lahko uporabijo popravki teh podatkov zaradi spremenjenih pogojev za nastanek škode iz naslova OT. Določeno mora biti tudi, do katerega obsega se lahko zadevni popravki uporabijo in kdo je pooblaščen za sprejemanje takih odločitev.

⁸ Ta zahteva pri standardiziranem pristopu je sicer zavezujoča samo za mednarodno dejavne banke, vendar Basel II priporoča, da jo na podlagi nacionalnih pooblastil v posameznih državah uveljavijo kot obvezno za vse banke. EU je z Direktivo to priporočilo sprejela in zahtevo predpisala za vse banke.

3 DEFINIRANJE OPERATIVNEGA TVEGANJA

Definicije ključnih pojmov so osnovni del začetka vsake prakse, ki brez sistematičnosti lahko hitro postane neorganizirana, neproduktivna in vprašljive upravičenosti. Definicije so usmerjene v načrte in strategije, ki določajo cilje, skladne z vodstvenimi in regulatornimi interesi. Ker pa so cilji lahko že v osnovi nejasni in morda celo protislovni, je kot vsaka druga tudi definicija OT zato še toliko bolj pomembna. Vzpodbuja prakso, ki pomaga izoblikovati jasne cilje, kar je tudi v osnovi namen Basla II.

Osnovanje in izoblikovanje formalne definicije OT pa ni ravno lahka naloga, saj to tveganje zajema širok nabor raznolikih dogodkov (od težav z informacijsko tehnologijo in infrastrukturo, prevar in goljufij, do prekinitev poslovanja, tožb in celo nepredvidljivih katastrof, tudi takšnih, kot je na primer znameniti 11. september).

V prvih obravnavah je bilo OT pogosto opredeljeno kot kategorija, ki je zajemala »preostala tveganja« (t. i. posredna definicija, kjer je OT razumljeno kot vsako tveganje, ki ni kreditno in tržno). Na začetku je bil tak pristop zaradi enostavnosti dobrodošel, vendar so se kmalu pričele pojavljati težave tako pri teoretikih kot praktikih, saj je bilo pojmovanje preširoko za bolj natančno opredelitev in razmejitev ključnih pojmov. Diskusija se je zato razvijala v iskanju neposredne definicije: raziskave so pokazale, da se ob obravnavi OT najbolj pogosto pojavljajo pojmi, kot so npr. procesi in postopki, ljudje in človeške napake, notranja kontrola, notranji in zunanji dogodki, posredna in neposredna izguba, tehnologija in sistemi, neuspehi (Geiger, 2000, str. 4).

3.1 Definicija po Baslu II

Baselski komite je prav tako priznal težave zaradi pomanjkanja formalne definicije OT v svojih začetnih raziskavah (Operational Risk Management, 1998, str. 3). Z namenom, da se ustvari skupni jezik in določi parametre za identifikacijo, nadzor in merjenje OT v bankah, je komite po letih javne diskusije sprejel končno uradno definicijo tega tveganja kot **»tveganje izgube kot posledice neprimerne ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi ali delovanja sistemov oziroma zaradi zunanjih dejavnikov.«**

Definicija poudarja kot ključne štiri kategorije vzrokov: ljudje, sistemi, procesi in zunanji dejavniki oz. okolje. Podrobnejša opredelitev vseh je v prilogi 3.

Definicija vključuje pravno tveganje⁹ in izključuje strateško tveganje¹⁰ ter tveganje izgube ugleda¹¹.

»Tveganje izgube ugleda ni vključeno v definicijo OT zato, ker se ga ne da izmeriti s konkretnimi številkami oziroma ker ga ni mogoče kako drugače kvantificirati. S tega stališča gledamo tveganje izgube ugleda kot posledico tistega OT, ki se šteje v uradno definicijo.«¹² (Pregled tretjega posvetovalnega dokumenta »Novi kapitalski sporazum« v delu, ki govori o operativnem tveganju s poudarkom na spremembah – povzetki v slovenščini, 2003, str. 1.)

V strokovnih krogih je bila najbolj kritično obravnavana izključitev strateškega tveganja iz definicije OT glede na dejstvo, da imajo spremembe konkurenčnega in ekonomskega okolja ali spremembe v obnašanju strank lahko pomemben vpliv na banko (Barriga, 2004, str. 14). Zagovorniki na drugi strani poudarjajo, da se te izločitve ne sme razumeti tako absolutno, saj ima strateško tveganje toliko ločenih značilnosti, da se ga lahko obravnava in upravlja posebej (Dev, 2004).

Pomislek in kritikam je sledil tudi Basel II, ki je v svojih spremljajočih dokumentih oba tipa izključenih tveganj uvrstil v Steber II, kar pomeni pod področje regulatornega nadzora (Implementation of Basel II: Practical Considerations, 2004, str. 17). V slovenski zakonodaji je dilema obravnavana v 5. členu Sklepa o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice (2007), kjer je določeno, da mora biti banka v vsakem trenutku sposobna upravljati z vsemi drugimi pomembnimi tveganji, ki jih prevzema v svojem poslovanju.

Ne glede na vse kritike govori v prid Baslovi definiciji dejstvo, da se banke v svojih politikah rade sklicujejo na uradno definicijo Basla II, kljub temu da za svoje potrebe lahko sprejmejo okoliščinam prilagojeno lastno definicijo OT. V slovenski bančni praksi, kar ugotavljam v okviru preučevanj letnih poročil za 2007, je to pravzaprav kar pravilo. To

⁹ Pravno tveganje obsega, a ni omejeno, globe, kazni, kazenske odškodnine iz regulatornih ukrepov, kakor tudi privatne poravnave (International Convergence of Capital Measurement and Capital Standards, 2006, str.144).

¹⁰ Strateško tveganje je tveganje nastanka izgube zaradi nepravilnih poslovnih odločitev banke, neustreznega izvajanja sprejetih odločitev ter premajhne odzivnosti banke na spremembe poslovnega okolja (Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, 2007).

¹¹ Tveganje ugleda je tveganje nastanka izgube zaradi negativne podobe, ki jo imajo o banki njeni komitenti, poslovni partnerji, lastniki, investitorji in nadzorniki (Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, 2007).

¹² Kot primer lahko navedem kar banko NLB d.d.: pri prehodu na nov informacijski sistem Sigma leta 2003 so imeli veliko težav (odpoved bankomatov, napačni izpiski prometa, otežkočeno dvigovanje denarja v bankah, moteno elektronsko poslovanje ipd.), kar je močno načelo ugled banke. Vendar pa lahko izvor tega najdemo v napakah v informacijski tehnologiji, napakah pri vodenju internih procesov, odnosih s komitenti ipd., kar navedena definicija obsega.

seveda ni narobe, če je dovolj pozornosti usmerjene v ustrezno razlago posameznih kategorij te definicije in s tem zagotovljeno enotno razumevanje, kaj se razume pod pojmom OT.

4 IDENTIFIKACIJA RELEVANTNIH TVEGANJ

Definicija OT predstavlja širok pogled na potencialno izpostavljenost OT.

SLIKA 1: Predstavitev raznolikosti področja OT

transakcije	izvedba	kraja	goljuživ trgovec	nezadovoljiv nadzor
informacije	zaupnost podatkov	strategija	ugled	odnosi iz delovnih razmerij
prevara	ljudje	osnovna sredstva	komitenti	poslovanje
kriminal	tehnologija	regulativa	potres	interni predpisi
prekinitev poslovanja	neupoštevanje navodil	poravnave	stranke	slabo vodenje
pomanjkanje virov	ključni zaposleni	nezadostno izobraževanje	pomanjkanje izkušenj	
nepopolna dokumentacija	outsourcing	prevzemi	združitve	projekti
novi trgi	novi produkti	teroristični napadi	odpisi	
			

VIR: prilagojeno po Doering, 2001, str. 5.

Širino in kompleksnost problematike OT prikazuje tudi zgornja slika: množico pojmov (tveganj, vzrokov, dogodkov), ki jih lahko povežemo z OT. Takšna raznolikost povzroča zmedo. Če ne bomo iz te množice izločili kategorije, ki so relevantne za »našo« banko in jih sistematično uvrstili v kategorije, nam ob izvajanju nadaljnjih aktivnost, tudi pri procesu zbiranja podatkov o OT, raznolikost podatkov lahko povzroča precejšnje težave.

Zato je potreben postopek, s katerim pripravimo podrobnejši seznam za banko relevantnih tveganj. S tem postopkom lahko razširimo ali podrobneje opredelimo osnovno definicijo OT, če prepoznamo bolj specifična tveganja za posamezno poslovno področje, ki v definiciji niso jasno izražena (Dev, 2004).

V strokovni literaturi je faza identifikacije tveganj opredeljena kot ugotavljanje, definiranje in kategorizacija škodnih dogodkov, njihovih vzrokov ter njihovih posledic in učinkov. Z drugimi besedami bi lahko rekli, da iščemo odgovore na vprašanja (Kralj, 2005, str. 15):

- kaj se lahko zgodi,
- zakaj se lahko zgodi,
- kakšne so možne posledice in učinki.

Rezultat te faze je izdelan zbirni seznam kategoriziranih identificiranih OT, katerim so bistveno izpostavljeni zaposleni, komitenti, produkti, dejavnosti, procesi in sistemi banke glede na vzroke, ki izhajajo iz definicije OT in/ali pripadajoče posledice glede na obstoječo organizacijsko in geografsko shemo. (Priporočila za vzpostavitev in izvajanje sistema upravljanja z operativnim tveganjem, 2005, str. 29)

Banka lahko za identifikacijo ključnih tveganj uporabi različne metode, med katerimi so najbolj uporabne (Cagan, 2001, str. 6):

- **Delavnice**, na katerih se zberejo posamezniki z namenom govoriti o tem, kaj po njihovem mnenju najbolj ogroža poslovanje. Takšen kvalitativni način zagotavlja relativno hiter začetek upravljanja z OT. Vključuje multidisciplinarni timski pristop, ki zbere skupaj zaposlene in vodstvo, izhaja pa iz predpostavke, da med sodelujočimi obstajajo znanje in izkušnje, ki jih bodo lahko učinkovito prenesli v okviru rezultatov takšnih delavnic. Prednost te metode je tudi povečevanje zavedanja o OT med zaposlenimi.
- **Samoocenjevanje** na podlagi posredovanih vprašalnikov. Prednost te metode je, da identifikacijo izvajajo ljudje, ki so zaposleni neposredno v poslovnih enotah in se srečujejo s težavami, ki se najvišjega vodstva ne »dotaknejo«. Po drugi strani pa analiziranje rezultatov takšnega pristopa zahteva precej spretnosti, kajti posamezniki imajo pri odkrivanju tveganj lahko nasprotujoče si interese.

Na osnovi rezultatov pridobimo seznam podatkov iz OT, ki so pomembni za banko. V nadaljevanju je potrebno te podatke ustrezno kategorizirati in jih v obliki standardov vključiti v ustrezen mehanizem za zbiranje definiranih podatkov.

4.1 Standardizacija kategorij po Baslu II

Standardizacija je pomemben vidik učinkovitega upravljanja z OT. S tem je zagotovljena enotna uporaba kategorij, s čimer se na področju OT ustvarja skupni jezik, omogoča primerjavo znotraj organizacije in navzven, pospešuje agregacijo tveganj in zagotavlja enotno poročanje (Dev, 2004).

Tega se je zavedal tudi Baselski komite in svoja prizadevanja usmeril v standardizacijo poslovnih področij in škodnih dogodkov¹³.

4.1.1 Poslovna področja

Vrsta poslovnega področja vpliva na raven OT. Na področju poslovanja s prebivalstvom se na primer izvajajo predvsem standardizirane transakcije - veliko število transakcij manjše

¹³ V svojih prvotnih dokumentih je Basel II prepoznaval tudi kategorije učinkov oziroma finančnih posledic škodnih dogodkov (Sound Practices for the Management and Supervision of Operational Risk. Basel, 2001, str. 15), kasneje so ta del v prenovljenem dokumentu izpustili. Kategorije učinkov so za namen te naloge podrobnejše predstavljene v prilogi 5.

vrednosti, kar posledično vodi v večje število škodnih dogodkov, ki pa so manjše vrednosti (npr. zlorabe pri kartičnih transakcijah). Drugačna slika je pri poslih trgovanja, kjer so nestandardizirane transakcije velikih vrednosti in ima en dogodek lahko velik negativen vpliv na poslovanje banke.

Posledično Basel II uveljavlja osem standardnih poslovnih področij, ki ustrezno zajemajo vsa glavna področja bančnega poslovanja¹⁴. S tem naj bi bila zagotovljena razumna začetna točka za prepoznavanje bistvenih kategorij OT znotraj teh področij. Tako standardizirana poslovna področja je prevzela tudi Direktiva, kar pomeni tudi za naše banke obvezno umestitev posamezne aktivnosti poslovanja.

Povzet seznam je v prilogi 1.

4.1.2 Kategorije škodnih dogodkov

Basel II je predpisal 7 primarnih kategorij škodnih dogodkov, ki jih je v 2. ravni razdelal v različne podkategorije, 3. raven pa je uporabil za konkretne primere dogodkov (Priloga 2). Direktiva se je v nasprotju z Baslom II omejila le na 7 primarnih kategorij. Definicija ostalih ravni je prepuščena institucijam.

Ne glede na to, da je obvezna zgolj uporaba kategorij prve ravni in se podkategorije lahko prilagodijo potrebam banke, je seznam v celoti dobro izhodišče za izvajanje identifikacije relevantnih tveganj. 3. raven lahko banka uporabi za nadaljnje drobljenje škodnih dogodkov (npr. pri izpadih sistemov jo bo morda zanimala ločitev med izpadi zaradi strojne opreme (hardwara), programske opreme (softwara) ali omrežja).

5 ZBIRANJE PODATKOV

Zbiranje podatkov iz OT v bankah ni novost, saj so bile izgube iz tega naslova od vedno na nek način evidentirane. V nekaterih primerih so odgovorni sprejemali ukrepe z namenom, da se v bodoče izognejo podobnim dogodkom. Vendar pa do nedavnega te izgube niso bile nikoli analizirane na sistematičen način, niti niso bile informacije zbrane na nekem centralnem mestu.

¹⁴ Če obstaja aktivnost, ki jo v banki ne morejo uvrstiti v eno standardno področje oziroma je ta aktivnost izven področja Basla (npr. posredovanje zavarovanj), se takšno aktivnost enostavno doda na seznam (Peccia, 2004, str. 403).

5.1 Upravičenost zbiranja podatkov

Vprašanje, ki bo na začetku vzpostavitve sistema za zbiranje podatkov verjetno pogosto izpostavljeno, je »Zakaj sploh oblikovati bazo podatkov o izgubah iz OT?«.

Če bo banka pristopila k uporabi standardiziranega ali naprednega pristopa za izračun kapitalske zahteve za OT, bo k zbiranju podatkov zavezana že zaradi regulatornih zahtev. Ta vzpodbuda je po mojem mnenju dobrodošla, saj bi verjetno sicer marsikatera banka z vidika stroškov odlašala z zbiranjem podatkov, kar bi bila z vidika koristi slaba odločitev.

Splošno gledano zbiranje podatkov pomaga pri doseganju cilja zmanjševanja števila in vrednosti izgub. S procesom kreiranja lastne baze podatkov o izgubah banka dosega določeno stopnjo poznavanja svoje zgodovine izgub, to znanje pa lahko s pridom uporabi pri vzorčnih analizah, boljšemu ocenjevanju, kontroli in zmanjševanju izgub, kot tudi pri učinkovitejšemu poročanju (Rotovnik, 2003, str. 56).

Gledano bolj podrobno pa se te koristi odražajo v (Haubenstock, 2004, str. 431, in Kühnert, 2001, str. 107):

- **povečanem zavedanju o OT**, ki izvira iz seznanjenosti z izpostavljenostjo OT in možnostjo škode, ki se lahko pripeti. Velikokrat se dogaja, da se zaposleni v banki ne zavedajo dejanske izpostavljenosti OT in se jih lahko prepriča šele s pomočjo konkretnih podatkov;
- **kvantifikaciji izpostavljenosti OT**. Eden izmed elementov zavedanja je tudi, koliko OT lahko stane institucijo. V večini primerov, potem ko zaključijo prvo fazo zbiranja in analize podatkov, banke ugotovijo, da so dejanske izgube veliko večje, kot so jih sprva predvidevali. Podatki služijo tudi za primerjavo med poslovnimi področji, kar vse pomaga usmerjati resurse v področja, kjer je zmanjševanje OT dejansko potrebno;
- **analizi ključnih vzrokov**. Poznavanje ključnih vzrokov za nastanek škodnih dogodkov pomaga pri odločitvenih procesih: pripomore k identifikaciji možnosti za boljšo kontrolo; lahko opozori na določen proces, funkcijo ali poslovno področje, ki ima pomanjkljivo kontrolo in predstavlja povečano grožnjo instituciji; ponavljajoči se škodni dogodki in trendi le-teh lahko opozorijo na nove možnosti izboljšav;
- **merjenju pričakovanih in nepričakovanih izgub**. Za namen določanja pravilne cene produktov oz. storitev je potrebna ocena pričakovanih izgub, za katero so podlaga ustrezni podatki. Izračun pričakovanih izgub namreč pomaga zagotoviti, da je povprečna izguba iz OT pravilno vgrajena v ceno produkta oz. storitve. Če gremo korak naprej, pa podrobnejši podatki omogočajo merjenje nepričakovanih izgub oz. spremenljivost izgub. Ta mera je dejansko tveganje, ki mu je banka izpostavljena;

- **preverjanju in usklajevanju s postopkom samoocenjevanja.** Prvič, dogodki zagotavljajo objektivni vir za določitev frekvence in resnosti pri samoocenjevalnem postopku. Drugič, dejanski dogodki delujejo kot kvalitativno preverjanje samoocenjevanj. Če pride do dogodkov brez pripadajočih kategorij tveganja (pri postopku samoocenjevanj niso bila identificirana kot relevantna), potem je postopek potrebno obnoviti. Če so tveganja identificirana in ni povezanih dogodkov, potem se preveri, ali je kategorija smiselna, ali pa se preveri kvaliteto kontrol, ki odkrivajo dogodke.

5.2 Oblikovanje podatkovnega modela in standardi

Celoten proces zbiranja podatkov temelji na vzpostavitvi ustreznih podatkovnih standardov, kar je pri oblikovanju podatkovnih baz sicer prvi, a velikokrat podcenjen korak. Najtežje in stroškovno drago se je vračati na začetek in ponovno obravnavati podatke, ko se ugotovi, da prvotno podatki niso bili ustrezno zbrani, npr. določen bistven podatek o škodnem dogodku manjka. Zbiranje podatkov glede na neoptimalno zastavljene standarde lahko vodi v neustrezne odločitvene procese in zavede organizacijo v napačne smeri (Cagan, 2001, str. 19-21).

Preden namenim poglavje konkretnim vprašanjem, do katerih se mora banka opredeliti in jih vgraditi v mehanizem zbiranja podatkov v obliki standardov, naj opozorim še na nekatere zahteve, ki pri tej aktivnosti lahko služijo kot vodilo (Anders, 2003):

- **Možnost združevanja in delitev izgub.** Pogosto lahko zaradi enega vzroka pride do več različnih škodnih dogodkov. V temu primeru bo vodstvo zanimala skupna vsota vseh izgub. Podatkovna baza mora omogočati grupiranje teh dogodkov. Po drugi strani pa se zahteva tudi možnost delitve izgub, na primer ko odgovornosti (in prevzem stroškov) za neko izgubo ne more prevzeti samo en lastnik procesa, temveč jo je potrebno razdeliti na več različnih. V temu primeru lastnik posameznega procesa zabeleži, kaj je šlo narobe na njegovem področju. Ta delni škodni dogodek se v podatkovni bazi lahko po potrebi pripiše skupnemu dogodku.
- **Fleksibilnost,** ki omogoča zbiranje specifičnih informacij. Posamezne poslovne enote bodo želele za svoje potrebe zbirati specifične podatke, npr. referenčna oznaka transakcije, številka depozita itd., zato mora podatkovna baza omogočati posebna, prilagodljiva obvezna ali opcijska polja.
- **Varnost.** Podatki iz naslova OT so zelo občutljivi. Ker se podatki zbirajo lokalno, hranijo pa centralno, mora biti zagotovljen tako varen prenos kot varna hramba.
- **Decentralizirana administracija.** Predvsem pri velikih bančnih sistemih so podatkovne baze povezane s širšimi in nehomogenimi skupinami uporabnikov, kar zahteva visoko stopnjo administracije (profili uporabnikov, pravice dostopov,

podpora uporabnikom, zahteve po specifičnih poslovnih informacijah). Če ni nujna centralizacija ali ločena in neodvisna podpora, se predlaga decentralizirana administracija.

- **Večjezičnost**, ki mora biti omogočena za velike, večnacionalne banke.

5.2.1 Standardi zbiranja podatkov

Ustrezni standardi, ki opredeljujejo posamezne in v nadaljevanju predstavljene segmente zbiranja podatkov, so zaradi raznolikosti in množice podatkov iz OT ključni predvsem pri zagotavljanju konsistentnosti in kvalitete nadaljnjih analiz.

5.2.1.1 Vrste škodnih dogodkov

Eno poglavitnih vprašanj je točna definicija, kaj dogodek je in v kakšnem obsegu zbirati podatke o dogodkih. Basel II predvideva samo zbiranje podatkov o:

- **škodnih dogodkih z neposrednimi izgubami**, npr. z odpisi, regulatornimi in davčnimi kaznimi, različnimi pravnimi stroški in poravnami, povračili strank, izgubami zaradi neplačil, izgubami ali poškodbami osnovnih sredstev (glej prilogo 4).

Korak naprej predstavlja vgraditev standardov v politiko zbiranja ostalih podatkov, ki jih narekuje dobra praksa in ki so lahko vir pomembnih informacij (Haubenstock, 2004, str.433):

- **»Skoraj izgube«**. »Skoraj izguba« je dogodek, ki se je zgodil, vendar ni povzročil finančne škode, kot na primer neuspeh poskus ropanja bančne enote, pravočasno odkritje napačne informacije z goljufivimi nameni še pred izvedbo transakcije ali posla. V drugačnih okoliščinah bi dogodek lahko privedel do izgub. Za analizo je dobro vedeti, ali je bila ničelna izguba posledica dobre kontrole ali zgolj srečno naključje, kar lahko predvidimo v vsebini podatkov o teh vrstah dogodkov.

Zbiranje podatkov o »skoraj izgubah« predstavlja v praksi pravi izziv (različne interpretacije takšnih dogodkov, diskrecijska pravica vodje, ali se bo poročalo o temu dogodku), ki se ga banke lahko lotijo različno. Kljub temu da se zato pri uporabi takšnih podatkov za naknadne analize in morebitno modeliranje svetuje posebna previdnost, pa so »skoraj izgube« lahko pomemben vir zgodnjega odkrivanja morebitnih lukenj v kontrolnih postopkih (Ramadurai, 2004b, str. 4).

- **Posredna izguba oziroma povezani stroški**. Zaradi okvare sistema v popoldanskih urah se na primer vrsta transakcij ne(pravilno) poravnava. To ima za posledico nastanek tveganja izgube dobrega imena banke, odškodninske zahtevke po zamudnih obrestih ipd., kar ima posreden učinek na finančni rezultat banke. Tovrstne izgube je težko kvantificirati, zato so jih iz uradne Baslove definicije

naknadno izločili. Kljub temu pa se lahko posamezna banka odloči, da bo vložila dodatne napore v zbiranje teh podatkov. Ob tem je potrebno predvideti, kako bodo posamezni učinki merjeni: npr. pri prekinitvah poslovanja se lahko uporabi standard stroška na uro prekinitve. Zadostna je lahko že tudi samo identifikacija takšnega posrednega učinka, ki ga povzroči posamezen dogodek.

- **Kreditne izgube.** Zajemanje kreditnih izgub z operativnim vzrokom (npr. goljufije pri najemanju kreditov (ponarejena poroštvena dokumentacija, napačno prikazan finančni položaj, goljufije v zvezi s kreditnimi karticami) lahko poveča vrednost podatkovne baze. V skladu z regulativo (poglavje 5.6.2) se tovrstni dogodki izključijo iz izračuna kapitalske zahteve za OT.
- **Strateški dogodki oziroma strateško tveganje.** Potrebna je jasna definicija za ustrezno razlikovanje operativnega od strateškega tveganja. Medtem ko je Basel II izločil to tveganje iz uradne definicije OT, meje pogosto niso jasne (npr. kako bi opredelili stroške, nastale zaradi umika poslovanja iz države, neuspelega poskusa uvedbe novega produkta).

V praksi so mnenja tudi deljena: veliko bank obravnava izgube zaradi neustreznih poslovnih odločitev kot izgube strateškega tveganja, veliko pa je tudi takšnih, ki jih uvršča med izgube OT (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 18).

- **Slučajni dobički.** Nekatere banke beležijo tudi dogodke, kot na primer, ko neustrezen postopek ob ugodnem tržnem dogajanju privede do nepredvidenega zaslužka.

5.2.1.2 Spodnja meja zbiranja podatkov

Naslednja temeljna odločitev pri oblikovanju podatkovne baze je glede postavitve spodnje meje, nad katero se podatki zbirajo (t. i. prag zbiranja podatkov), kar je tudi eksplicitna regulatorna zahteva. Na odločitev o višini vplivata predvsem namen podatkovne baze¹⁵ ter pričakovano razmerje med stroški in koristmi zbiranja podatkov (Thirlwell, 2001, str. 234). Previsoko postavljena meja lahko pomeni nezadostno število podatkov in izgubo pomembnega dela porazdelitve izgub, pri prenizki pa stroški zbiranja podatkov lahko presegajo koristi, ki jih takšno zbiranje prinaša.

Zbiranje majhnih dogodkov ima navkljub večjim stroškom svoje prednosti (Haubenstock, 2004, str. 436):

¹⁵ Na primer, člani skupne podatkovne baze angleškega bančnega združenja (BBA) GOLD so se strinjali, da je njen glavni namen zagotovitev podatkov o večjih in manj pričakovanih izgubah. Zato je postavljen relativno visok prag zbiranja podatkov: 50.000 USD za izgube, povzročene na področju poslovanja s prebivalstvom, in 100.000 USD na področju poslovanja s podjetji (Thirlwell, 2001, str. 234).

- Majhni dogodki so potrebni zaradi izvajanja trend analiz. Večji dogodki so redki in se lahko v svoji osnovi močno razlikujejo, kar oteži tovrstne analize.
- Brez majhnih dogodkov se lahko izpustijo pomembni vzroki OT. Osnovno vprašanje je: Se ta dogodek lahko pripeti ponovno? In: Ali so lahko v prihodnje še hujše posledice? Lahko so samo opozorilo za večji dogodek, ki se bo pripetil za njimi, ali pa niz ponavljajočih manjših dogodkov, katerih vsota lahko sčasoma postane znatna.
- Majhni dogodki lahko pomagajo pri določanju pričakovanih izgub. To je pomembno za določitev pravilne cene produktov oz. storitev.

Dosedanja tuja bančna praksa je pokazala, da si je večina bank postavila to mejo med 0 in 25.000 USD, najbolj pogosto 10.000 USD (oziroma EUR na evropskem finančnem področju), kar pa je precej višji znesek kot praviloma velja za naše banke, kar bo predstavljeno v poglavju 9.

Res pa je, da so tuje izkušnje prav tako pokazale, da v nekaterih bankah sčasoma, ko prepoznajo koristi od zbiranja podatkov, začetno mejo počasi znižujejo ali pa ne glede na postavljeno mejo zbirajo podatke tudi pod njo in te podatke uporabljajo za analizo pričakovanih izgub (Kennett, 2001, str. 75).

Nekatere banke glede na postavljeni prag oz. višino izgube diferencirano pristopajo k zbiranju informacij: več podrobnosti zahtevajo pri izgubah nad postavljeno mejo, zgolj osnovne podatke pa za dogodke z manjšimi izgubami (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 19).

5.2.1.3 Podatki o škodnem dogodku

Regulator je določil minimalne zahteve glede potrebnih informacij o škodnih dogodkih (bruto znesek izgube, datum dogodka, morebitna povračila od bruto zneskov izgube, opisne informacije o dejavnikih ali vzrokih škodnega dogodka). V praksi so banke praviloma pristopile k zbiranju dodatnih informacij. Navajam nabor možnih podatkov v podatkovni bazi, ki so zbrani na osnovi različnih literatur in kot priporočila dobre bančne prakse¹⁶.

Z zbranimi podatki naj bi si odgovorili na štiri poglavitna vprašanja o dogodku (kje se je škodni dogodek zgodil, kaj se je zgodilo, kdaj in zakaj).

¹⁶ Seznam podatkov je nastal na osnovi različne literature:

- An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk., 2003, str. 7
- Haubenstock, 2004, str. 452-454 ,
- Implementation of the Capital Accord for Operational Risk , 2002, str. 53-54,
- Thirlwell, 2001, str. 235-236.

□ KJE?

- Poslovni proces/produkt

Nekatere banke bo zanimalo ločevanje izgube glede na poslovni proces ali tip produkta. Tip produkta (npr. kredit) oz. tip poslovnega procesa (odobranje kreditov) je bolj relevanten za analizo izgub kot tip poslovne enote (čeprav sta potrebna oba podatka). Organizacijske strukture se med bankami razlikujejo, v osnovi pa vse ponujajo enake produkte in izvajajo enake poslovne procese, ki v sebi skrivajo podobna OT¹⁷ (Cagan, 2001, str. 21).

- Poslovna enota

- enota glede na organizacijsko shemo, kjer se je dogodek zgodil.

- Poslovno področje

- uvrstitev v eno izmed kategorij, kot so predlagane s strani regulatorja (7 poslovnih področij, priloga 1).

Potrebno je najti način ustrezne delitve odgovornosti za izgubo med poslovnimi področji, saj je to predmet regulatorne zahteve. Praksa na temu področju se razvija v dve smeri: a) alokacija celotne izgube področju, kjer je njen vpliv oziroma delež največji, ali b) alokacija izgube pro-rata na vsa vpletena poslovna področja (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 14). Drugo vprašanje pa je delitev izgub, ki so nastale v centralni oziroma podporni službi: tudi za te je potrebno razviti kriterije, po katerih se dodeljuje izguba.

- Regija oz. država

Različne regije oziroma države lahko prispevajo k razlikam v OT, zato je za analize zanimiv tudi ta podatek.

□ KAJ?

- Kategorija dogodka

- uvrstitev v eno izmed kategorij, kot so predlagane s strani regulatorja (3 nivojski seznam, priloga 2).

Za nadaljnjo uporabnost podatkov je ustrezna kategorizacija verjetno eden večjih izzivov (podrobneje je problematika predstavljena v poglavju 5.3). V zvezi s tem je pomembno izobraževanje zaposlenih. Nekatere banke z

¹⁷ Pri kreditih oziroma odobritvi kredita lahko pride do izgub zaradi nepopolne dokumentacije, spora z nasprotno stranko ne glede na to, kje je prijavljena izguba.

decentraliziranim zbiranjem podatkov so razvile različne oblike pomoči, na primer t. i. odločitvena drevesa (primer v prilogi 5) in spletno pomoč v obliki »čarovnika«, ki klasificira dogodek odvisno od odgovorov uporabnika na serijo različnih vprašanj (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk, 2003, str. 10).

- **Tip dogodka**

Uporabnikom podatkovne baze se lahko ponudi možnost različnih tipov dogodka, na primer:

- škodni dogodek
- skoraj izguba
- posredna izguba
- agregirani dogodki
- nezaključen dogodek.

Večina dogodkov bo tipa »škodni dogodek« (škodni dogodek z neposrednimi izgubami). Dogodka, poimenovana »skoraj izguba« in »posredna izguba« sta bila pojasnjena v poglavju 5.2.1.1. »Nezaključen dogodek« pomeni, da je dogodek vnesen v bazo, vendar ker vnos še ni zaključen, se izključi iz poročanj. Tip dogodka »agregirani dogodki« pa je ena izmed možnosti, da zajamemo dogodke »visoka frekvenca/majhna izguba«, kjer je posamezen dogodek pod spodnjo mejo zbiranja podatkov (npr. določen tip kartične prevare), skupni vpliv istovrstnih dogodkov pa je velik.

- **Opis dogodka**

Za večjo konsistentnost podatkov, kar omogoča lažjo primerljivost podatkov med poslovnimi področji, je priporočljivo, da se vnese tudi opis okoliščin in ostalih podatkov. Takšen opis je tudi v pomoč pri preverjanju ustreznosti klasifikacije. Glede na obsežen seznam dogodkov je namreč možno, da različne enote oziroma področja podobnih dogodkov ne klasificirajo enako.

- **Indikator, ali je izguba povezana z večjim dogodkom**

V praksi lahko pride do povezanih škodnih dogodkov, ki se odvijajo daljše obdobje, ali do dogodkov, ki imajo več različnih negativnih učinkov. Primer prvega je dogodek, kjer je zaposleni kradel večkrat v zaporedju več mesecev ali celo let. V temu primeru se posamezne izgube lahko ugotovijo različno, medtem ko preiskava še poteka. Primer drugega dogodka: potres uniči različne zgradbe, pride do daljšega izpada informacijskega sistema ipd. Zato je potrebno predvideti, da se lahko poveže vse povezane izgube.

- **Indikator, ali je izguba povezana s kreditnim oziroma tržnim tveganjem**

V skladu s poglavjem 5.6.2 Ločevanje podatkov nasproti tržnemu in kreditnemu tveganju je potrebno tovrstne izgube v bazi podatkov posebej označiti.

- **Kategorija učinka**

Poslovna praksa praviloma uporablja 6 kategorij učinkov oziroma finančnih posledic, ki so relativno lahko merljivi neposredni stroški (Priporočila za vzpostavitev in izvajanje sistema upravljanja z operativnim tveganjem, 2005, str. 58):

- pravna odgovornost
- regulatorna in davčna kazen
- povračilo
- izguba iz naslova neplačil
- odpisi
- izguba ali poškodba osnovnih sredstev.

Nekatere organizacije pa zbirajo še dodatne učinke OT:

- stroški poplačila, povrnitve
- izgubljen prihodek
- prekinitev poslovanja.

Podrobnejša opredelitev, vključno s primeri, je navedena v prilogi 4.

- **Znesek izgub(e)**

- Bruto izguba: primarna izguba ne glede na delno ali celotno povrnitev.
- Neto izguba: dejanski znesek izgube (bruto znesek zmanjšan za znesek povrnitve).

Čeprav se bruto izguba lahko praviloma določi brez težav, pa v nekaterih primerih to ne drži. Na primer, pri vrednotenju poškodovanih osnovnih sredstev se lahko ugotovijo precej različne vrednosti glede na to, ali za vrednotenje uporabimo knjigovodsko vrednost, tržno vrednost ali stroške nadomestila. Praksa nobene izmed vseh treh možnosti za vrednotenje ne izključuje. Zaradi možnih razlik pa je potreben poudarek na validaciji teh izgub (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 13).

Druga težava lahko nastopi pri ugotavljanju neto izgube, saj do povrnitev izgub lahko pride tudi po nekaj mesecih in letih. Ne glede na to, da je zmanjšanje bruto vrednosti upravičeno v vseh primerih, ko obstaja zagotovilo glede zneska povrnitve, dobra praksa predlaga opredelitev obdobja, v katerem je ugotavljanje neto vrednosti izgub še sprejemljivo (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 15). V

primeru popolne povrnitve izgube banke praviloma dogodek prijavijo kot »skoraj izgubo«.

Če se originalni zneski s časom spremenijo (npr. izguba je bila izrazito premalo ocenjena) in je sprememba bistvena, se predlaga možnost revizije predhodnih vnosov in ustrezna prilagoditev zneskov izgub (Thirlwell, 2001, str. 235).

- **Povrnitve z opisom**

- npr. povrnitve od zavarovanj, tožb, stečajne mase.

□ **KDAJ?**

- **Datum dogodka**

- začetek dogodka
- datum odkritja dogodka
- datum zaključka obravnave dogodka.

Pomen podatka o datumu dogodka je lahko velik, saj pri velikih izgubah močno vpliva na oceno profila tveganja v določenem obdobju in izračun kapitalske zahteve.

Ker datum dogodka v veliko primerih ni samoumeven, je v nasprotju z regulatorno zahtevo po enem datumu praksa pokazala, da je potrebnih več datumov. V primeru dolgotrajnih sodnih postopkov je namesto datuma začetka dogodka za izračun kapitalske zahteve bolj ustrezen datum knjiženja oziroma datum poravnave (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 12).

□ **ZAKAJ?**

- **Povod dogodka (neposredni vzrok)**

Informacija, kaj je povzročilo izgubo, je nujna za kvalitativno analizo dogodka in za identifikacijo indikatorjev tveganja. Povod za škodne dogodke je lahko npr. človeška napaka, diskriminacija pri zaposlovanju.

- **Spremljajoči dejavniki nastanka dogodka**

Zbrani podatki morajo vsebovati tudi informacijo o spremljajočih dejavnikih, ki morda neposredno ne povzročijo neke izgube, a bistveno pripomorejo k njeni resnosti. Ob ustreznih notranjih kontrolah, razmejitvi odgovornosti (funkcije poslovanja s strankami z zalednimi funkcijami) in učinkovitejšemu nadzoru primer Barrings verjetno ne bi zašel v takšne razsežnosti, kakršne poznamo danes.

5.2.2 Zaupnost podatkov

Podatki o dogodkih iz OT so praviloma obravnavani kot zelo občutljive informacije. Posebnih standardov glede razkritij ni. Obstaja pa splošna bojazen, da informacije postanejo javno razkrite oziroma dostopne posameznikom, ki bi jih lahko izkoristili proti organizaciji. Zato mora vsaka institucija osnovati svojo lastno politiko varovanja in zaupnosti podatkov. Ob temu mora pretehtati na eni strani želeni nivo varnosti, na drugi strani pa, v kolikšni meri želi preglednost nad OT in možnost učenja na podlagi izkušenj, ki se skrivajo v podatkih (Haubenstock, 2004, str. 447).

Podatki morajo biti varni pred morebitnimi zunanjimi in notranjimi vdori, kar lahko vodi v odločitve o kodiranju podatkov. Vsekakor pa bo banka morala omejiti dostope z oblikovanjem pravic dostopa z možnostjo branja in/ali vnosa oz. spreminjanja podatkov. Veliko institucij omeji dostope pooblaščenim osebam samo do podatkov z njihovega poslovnega področja oz. organizacijske enote. Nekateri bolj občutljivi podatki, na primer v zvezi s človeškimi viri in pravnimi dogodki, so lahko še bolj zaščiteni. Do vseh podatkov ima dostop le peščica zaposlenih v okviru funkcije upravljanja z OT. Širši krog zaposlenih ima lahko pregled nad različnimi izvlečki in informacijami glede skupnih vrednosti, odstotkov, relativnih primerjav ipd., brez podrobnejših podatkov o posameznih dogodkih.

5.3 Kritičen vidik kategorizacije škodnih dogodkov

Ustrezna kategorizacija škodnih dogodkov je z vidika uporabnosti podatkov zelo pomembna. Po McLenaghenu navajam naslednja področja (2007, str. 25):

- ❑ **Modeliranje OT.** Če so dogodki klasificirani napačno in uvrščeni v neustrezno kategorijo, to ustvarja anomalije v distribuciji porazdelitve frekvence in vpliva, kar lahko povzroči izkrivljeno oceno kapitala.
- ❑ **Primerjava z zunanjimi podatki** v okviru konzorcijev bank ali iz drugih virov. Že tako problematično primerjavo z zunanjimi podatki iz različnih virov bi neustrezna klasifikacija še poslabšala.
- ❑ **Analiza podatkov.** Vodstvene ravni banke za razumevanje velikosti in širine različnih problemov potrebujejo zanesljive podatke, kar napačna klasifikacija ne zagotavlja.

V ta namen je že regulator identificiral in uvrstil v svoje dokumente 7 standardiziranih kategorij škodnih dogodkov¹⁸ (poglavje 4.1.2). Na predlagano kategorizacijo se je razvila širša polemična razprava, katere kategorije naj se v praksi dejansko uporabljajo. Večina se jih sicer strinja, da je seznam celovit, a da so kljub temu potrebne dopolnitve. Nekatere

¹⁸ Za te kategorije obstaja prepričanje, da se lahko odrazijo v znatnih izgubah iz naslova OT (Komljenovič, 2007, str. 3).

organizacije so že zahtevale revizijo 7-ih kategorij OT. Kot primer dodatnih kategorij, ki so bile doslej izpuščene, navajajo projektno tveganje (Haubenstock, 2004, str. 438).

Ne glede na različne kritike menim, da dejansko nobena kategorizacija ne bi mogla ustrezati vsem organizacijam in da Basel II omogoča dobro izhodišče pri prizadevanjih za zagotavljanje konsistentnosti podatkov. So pa bolj kot sama kategorizacija pomembna jasna, logična in konsistentna pravila, ki postavljajo mejo med dvema tipoma kategorij.

V praksi so se namreč pri kategorizaciji nekaterih škodnih dogodkov pokazale težave zaradi nejasnih in nepopolnih definicij posameznih kategorij in možnosti prekrivanja njihovih področij (Samad-Khan, 2002, str. 1).

V nadaljevanju izpostavljam nekatera takšna področja, kjer je Basel II nejasen, skupaj z možnimi pravili za bolj nedvoumno razvrščanje dogodkov (Haubenstock, 2004, 438-440).

□ **Sistemske proti izvedbenim napakam**

Če zaradi napačnega vnosa pride do programske napake in posledično do izgube, je to izvedbena napaka ali sistemska napaka? Eno od možnih pravil bi lahko bilo, če je za odpravo napake potrebna pomoč IT področja, je to sistemska napaka, sicer pa izvedbena.

□ **Dogodki, ki se zgodijo v specifičnih računalniških programih**

Ali kot »izpad sistema« lahko opredelimo dogodek na podlagi težav z aplikacijami, ki jih upravljajo poslovna področja (razni interni programi, razpredelnice, makroji, ipd.)? Pravilo je lahko, če se aplikacija upravlja izven IT področja, se ne kategorizira kot »izpad sistema«.

□ **Napake v postopkih odobravanja kreditov**

Operativna napaka v postopku odobravanja kredita je nekako na mejnem področju med kategorijama »stranke, produkti in poslovna praksa« in »izvedba, dostava in upravljanje procesov«. Nobena opredelitev ne pokriva omenjenega procesa. Zato se lahko postavi pravilo, da se napake v kreditnih modelih uvršča v kategorijo »stranke, produkti in poslovna praksa«, kar je po eni strani logično glede na to, da ta kategorija vsebuje večinoma tveganja v povezavi s strankami, npr. zadeve, ki se zgodijo, preden se izvrši transakcija.

□ **Nenamerna napaka v pogodbenih določbah, splošnih pogojih ali sporočilih strankam**

Tudi ta napaka je na meji med kategorijama »stranke, produkti in poslovna praksa« in »izvedba, dostava in upravljanje procesov«. Možno pravilo je, da je to izvedbena napaka.

□ **Vprašanja v zvezi s prodajalci, ki imajo za posledico povečanje stroškov**

Kaj se zgodi, če na podlagi odnosov s prodajalci nastanejo nepričakovani stroški?

V primeru »outsourcinga« vse goljufije ali IT napake lahko uvrstimo po enakem principu, kot če bi se zgodile znotraj organizacije, s predpostavko, da so vsi procesi podobni in lahko združimo negativne izkušnje na osnovi obeh virov. Po drugi strani pa lahko težave z zunanjim okoljem ločimo in jih uvrstimo v posebno podkategorijo »prodajalci in dobavitelji«. To nam kasneje lahko pomaga združiti težave s prodajalci in identificirati najbolj problematične.

□ **Poslovna odločitev, ki povzroči neposredne stroške**

Lahko se zgodi, da na podlagi strateške odločitve uvedemo produkt ali storitev ne glede na to, da je znana napaka v produktu ali da obstaja možnost za napako. Ko pride dejansko do izgub, ali jih opredelimo kot strateške ali so to izgube iz OT¹⁹? Na splošno je lažje določiti, da se vse napake, ki povzročijo izgube, uvrstijo v OT.

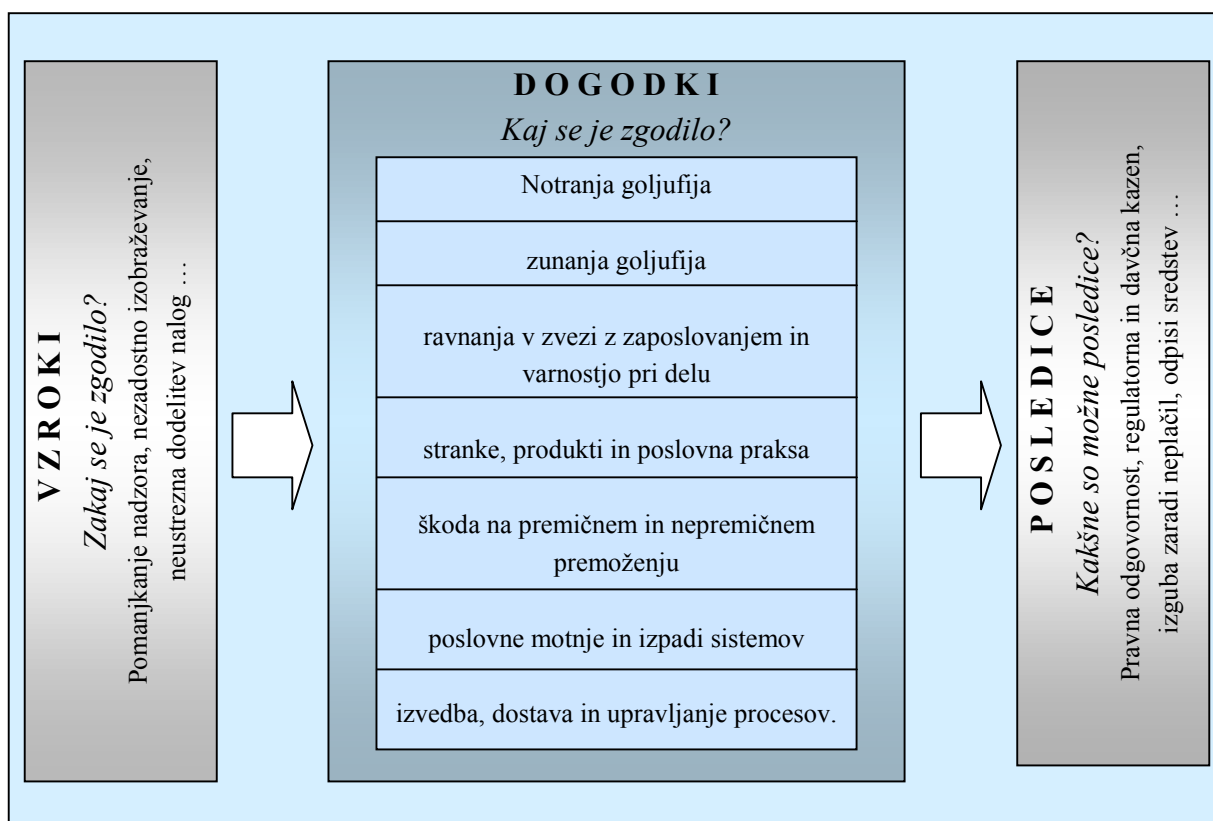
To so sicer samo nekatere iz izkušenj ugotovljene dileme. Skozi proces zbiranja podatkov se bo posamezna banka gotovo srečala z novimi izzivi. Ob ustreznem soočenju z njimi in dokumentiranju dogovorjenih pravil lahko razvije dobro prakso, ki bo v pomoč zaposlenim pri izvajanju procesa zbiranja podatkov.

5.3.1 Tridimenzionalna kategorizacija

Večina avtorjev poudarja pomembnost tridimenzionalne kategorizacije škodnih dogodkov, kar pomeni upoštevanje in hkratno obravnavo vzrokov, dogodkov in učinkov oz. posledic OT. Vzemimo kot primer nepravočasno poravnava obresti po računih, kar opredelimo kot dogodek. Vzrok za to je lahko človeška napaka, izpad računalniškega sistema ali težave s podatki. Možne posledice so povračila, pravna odgovornost ali regulatorna kazen.

¹⁹ Strateško tveganje je izključeno iz uradne definicije OT.

SLIKA 2: Povezava vzrokov, dogodkov in posledic



VIR: Prilagojeno po Kaishan, 2007.

Strokovnjaka za OT mora primarno zanimati, kako zmanjšati izpostavljenost tveganju, kar zahteva razčlenitev posameznih dogodkov z ustreznimi posledicami na vzroke njihovega nastanka. S tem svoja prizadevanja usmerijo na področja, kjer bodo ukrepi dosegli zelene rezultate. To pomeni izogibanje vzrokom ali zmanjševanje njihovih vplivov na frekvenco ali resnost dogodka.

Škodni dogodek ima lahko več vzrokov. Prav tako ima lahko več posledic, ki se odražajo v finančnem računu. Analize morajo potekati tako, da se identificira vse vzroke in posledice. Kar pa ni enostavno in to je eden izmed razlogov, zakaj je bila v okviru Basla II razvita klasifikacija na osnovi dogodkov (Hübner et.al., 2002, str. 17).

Nekateri avtorji kritično obravnavajo to klasifikacijo tudi z vidika omenjene trodimenzionalnosti in sicer da kategorizacija v posameznih sklopih ni enoznačna, saj so nekatere kategorije mešanica vzrokov, dogodkov in učinkov. Na primer, aktivnost »Računovodska napaka/napačni pripisi« lahko opredelimo kot vzrok, »Neizpolnitev obveznega poročanja« pa kot dogodek. Oba primera sta iz kategorije »Izvedba, dostava in upravljanje procesov«. Vse to naj bi zmanjšalo kakovost informacij in povečalo zmedo pri uporabi posameznih kategorij (Ali Samad-Khan, 2002, str.1).

Da omilim kritičnost zgornje trditve, bi jaz konkretni primer »računovodske napake« raje opredelila kot povod za škodni dogodek neustreznega poročanja regulatorju. Namreč, sama »napaka« nam dejansko še ne poda prave informacije o osnovnem vzroku dogodka. V ta namen si moramo zastaviti vprašanje: Ali je vzrok te napake v neustreznih kontrolah, morda neizobraženem ali neustreznem kadru?

5.4 Politika zbiranja podatkov

Ko so določeni vsi elementi procesa zbiranja podatkov, mora institucija poskrbeti, da se dogovorjena pravila oziroma standardi formalizirajo v t. i. politiki zbiranja podatkov (lahko kot del splošne politike upravljanja z OT), ki jo odobri in sprejme odgovorna oseba, praviloma najvišje vodstvo.

Celovita politika naj bi vsebovala (Haubenstock, 2004, str. 448):

- **definicijo** OT;
- **izjavo** o zbiranju podatkov;
- **spodnjo mejo zbiranja podatkov**, nad katero se bodo podatki sporočali in vključevali v podatkovno bazo, **opise posameznih kategorij** škodnih dogodkov in učinkov, kriterij za **rok prijave** podatka o škodnem dogodku (npr. najkasneje 48 ur po odkritju);
- **odgovornosti** poslovnih področij, funkcije upravljanja z OT ter ostalih zaposlenih.

Kot takšna mora politika biti (Operational Risk Regulatory Approach, 2001, str. 22):

- razumljena s strani zaposlenih, ki so odgovorni za upravljanje z obravnavanimi tveganji;
- posredovana oziroma predstavljena vsem zaposlenim, s čemer se zagotavlja zavedanje o problematiki in njeno konsistentno izvajanje;
- predmet rednega pregleda in ažuriranja, da se zagotovi ustrezno skladnost s spremembami okolja, v katerem organizacija deluje.

Za operativno izvajanje politike vseh zaposlenih je pomembno, da je opredelitev in razvrstitev vseh relevantnih vrst OT ter ostalih ključnih področij popolnoma zajeta tudi v podpornih pisnih dokumentih (navodilih, usmeritvah, postopkih ...).

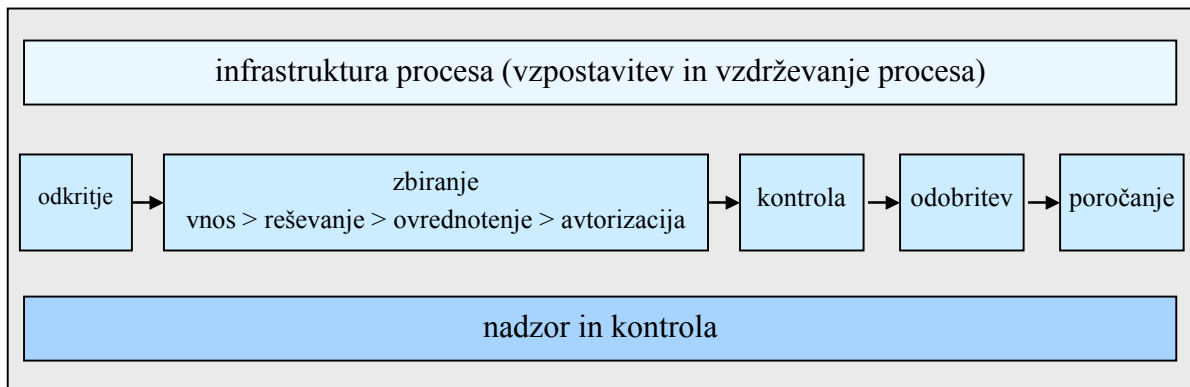
5.5 Proces zbiranja podatkov

Proces zbiranja podatkov sestoji iz treh primarnih faz (Haubenstock, 2004, str. 448):

1. vzpostavitev infrastrukture, s katero se vzpostavi in vzdržuje proces;
2. izvajanje procesa;
3. nadzor in kontrola, ki zagotavlja, da je proces zbiranja pravočasen, temeljit in ustrezen.

Navedene faze ponazarjam s sliko 3.

SLIKA 3: Faze procesa zbiranja podatkov



VIR: Prilagojeno po Haubenstocku, 2004, str. 449.

Pri procesu zbiranja podatkov se praksa srečuje s številnimi izzivi, ki izvirajo iz (Kühnert in Stubbs, 2001, str. 112):

- ❑ **različnih virov oziroma sistemov**
Podatki lahko pridejo v bazo iz različnih virov, če na primer poslovna področja uporabljajo različne postopke in sisteme za zbiranje podatkov o škodnih dogodkih.
- ❑ **različnih zahtev za različne tipe izgub**
Različni tipi izgub zahtevajo različne podatke (npr. izgube na podlagi transakcije, izgube, osnovane brez transakcij).
- ❑ **pomanjkanja konsistentnosti**
Poslovna področja s škodnimi dogodki pogosto upravljajo različno; nekatera bistveno bolj dovršeno kot druga.
- ❑ **(ne)razpoložljivosti podatkov o dogodku**
Pri nekaterih dogodkih določeni podatki niso razpoložljivi (npr. datum nastanka dogodka je lahko potrebno določiti kot približek na podlagi drugih razpoložljivih podatkov).
- ❑ **ročnega zbiranja podatkov**
Kjer ni avtomatiziranih procesov, je potrebno uvesti ročne rešitve. Ta način je lahko stroškovno in časovno intenziven in ne zagotavlja zanesljivih in konsistentnih podatkov.
- ❑ **večjih stroškov, kot so koristi**
Zbiranje podatkov lahko ni stroškovno učinkovito, kar pomeni, da stroški presegajo nepričakovane izgube.

Nekateri odgovori se skrivajo v uresničevanju napisanega v tem delu, med drugim v standardizaciji procesa zbiranja podatkov, razumljivem in celovitem izobraževalnem

programu za zaposlene, zagotavljanju podpore uporabnikom v obliki takojšnje pomoči oziroma dostopnosti do jasnih vodil in popolne dokumentacije.

5.5.1 Infrastruktura

Cilj vzpostavitve prve faze procesa zbiranja podatkov je zagotoviti okolje za nenehno odkrivanje in poročanje o dogodkih iz OT, ki bo ugotovitve vključevalo v proces upravljanja z OT. V ta namen je potrebno urediti organizacijske odgovornosti in lastništvo nad podatki ter sprejeti odločitev o podporni tehnologiji.

5.5.1.1 Vloge in odgovornosti

Glede na razdelitev vlog pri izvajanju procesa zbiranja podatkov sta možna dva osnovna modela odgovornosti: centraliziran in decentraliziran model (Haubenstock, 2004, str. 449). Prvi je enostaven, ločuje pa proces zbiranja od dejanskega nastanka dogodkov, kar lahko povzroča težave pri zagotavljanju celovitosti podatkov. Ta model prav tako predstavlja najmanjšo mero zavzetosti poslovnih področij. Drugi ponuja več različic, odvisno od tega, kako so porazdeljene odgovornosti med poslovnim področjem in centralno funkcijo.

Odločitev, za kakšen način se bomo odločili, je odvisna od okoliščin poslovanja.

Veliko bank v praksi dejansko kombinira obe možnosti: za nekatere izgube centralizirano zbiranje (npr. področje varnosti in zdravja zaposlenih, pravne zadeve), za druge pa decentralizirano zbiranje (npr. izgube, ki nastanejo pri posameznih opravilih).

Centralno zbiranje je smiselno v primerih, kjer so izgube iz OT procesirane centralno. Nekateri se za to odločajo tudi pri geografsko ločenem in zaokroženem sklopu enot. Morda je tak način uporaben v uvajalnih fazah zbiranja podatkov. Kjer izgube iz OT niso procesirane centralno, decentralizirano zbiranje vodi v boljše informacije o izgubah, pravočasnejše poročanje z manjšo možnostjo napak, do katerih lahko pride zaradi dodatne izmenjave informacij med centralno funkcijo in poslovnim področjem (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk, 2003, str. 9).

Pri decentraliziranem modelu so osnovne vloge zaposlenih na poslovnem področju, ki so vključena v proces zbiranja podatkov, praviloma odkrivanje in zbiranje podatkov, vrednotenje izgub in odobritev celotnega vnosa. Vodje poslovnih področij so odgovorni za pravočasno in ustrezno izvajanje tega procesa. Centralni oddelek za upravljanje z OT pa je odgovoren za zagotavljanje orodij in metodologij, ki jih poslovna področja potrebujejo pri zbiranju podatkov, ter poročanje o ugotovitvah na podlagi zbranih podatkov (Haubenstock, 2004, str. 459-460).

5.5.1.1.1 Vloge v okviru podatkovne baze

Osnovne vloge oziroma pravice v okviru podatkovne baze so lahko naslednje (Anders, 2003):

- **vnašalec**, ki vnaša podatke;
- **potrjevalec**, ki vnesene podatke pregleda in potrdi;
- **administrator**, ki vzdržuje pravice do sistema in morebitne šifrante;
- **bralec**, ki ima samo možnost pregleda podatkov.

Priporočljivo je, da se v okviru poslovnega področja določi ključne zaposlene za vnos v podatkovno bazo. To naj bodo posamezniki, povezani v nekakšne skupine za identifikacijo tveganj, ki imajo izkušnje pri poslovanju in poznajo področja upravljanja s tveganji. Tovrstno dodeljevanje nalog pomeni bolj obvladljivo število zaposlenih, ki jih je potrebno izobraziti za to področje (Muzzy, 2003, str. 60).

5.5.1.2 Podporna tehnologija

Izkušnje kažejo, da praktično noben obstoječi sistem v poslovnih procesih ni primerno orodje za zbiranje podatkov o OT; niti glavna knjiga, kjer ima računovodska služba lahko posamezne račune nastavljene tako, da izkazujejo posamezne vrste tveganja (npr. goljufije, napake iz trgovanja). Upravljanje z OT zahteva bistveno več podrobnosti, poročanj in analiz, kot jih lahko nudi sistem glavne knjige. Posledično je oblikovana praviloma ločena podatkovna baza, v kateri se zbirajo podatki o škodnih dogodkih iz OT (Newberry, 2002, str. 41).

Viri podatkov

Baza se lahko oskrbuje s podatki iz obstoječih produkcijskih sistemov ali z ročnim vnosom podatkov.

Bolj učinkovit je prvi način: prenos iz obstoječih produkcijskih sistemov. S tem se izognemo dodatnim postopkom in napakam. Razpoložljivost podatkov v teh sistemih je različna. Npr. sistem za odobravanje in vodenje kreditnih poslov lahko beleži odpise (npr. za goljufije pri kreditnih karticah), zavarovanja (npr. za zneske poplačil iz tega naslova), pravne zadeve (npr. za tožbe). Ponavadi vseh zahtevanih podatkov iz obstoječih sistemov brez dodatnih raziskav ni možno dobiti.

Tehnologija za zajem podatkov

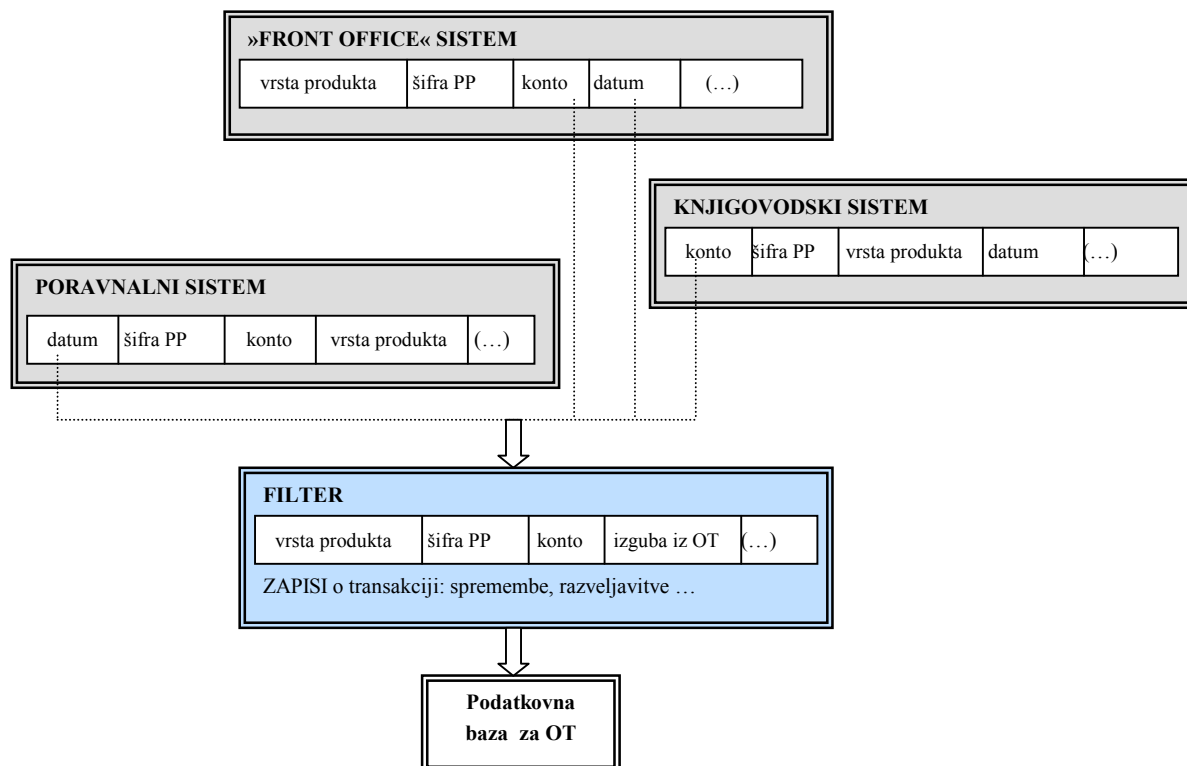
Potrebno je načrtovati tudi tehnologijo za zajem dogodkov. Vodilna praksa je, da ima banka deloma avtomatiziran zajem podatkov z možnostjo, da poslovna področja ročno beležijo dogodke, ko do njih pride (Haubenstein, 2004, str. 452).

Banka lahko za namen avtomatskega zbiranja podatkov razvije t. i. filtre, ki delujejo po principu vezne poti med sistemi oz. aplikacijami, tako da zbirajo vse podatke, ki se

nanašajo na posamezno transakcijo (razveljavitev, sprememba, razlike med parametri v različnih aplikacijah ...) (Rotovnik, 2003a, str.8).

Primer modela filtra prikazuje naslednja slika.

SLIKA 4: Filtriranje podatkov iz OT



VIR: Rotovnik, 2003a, str. 8

Slika prikazuje pot transakcije od njenega aktiviranja in registriranja v sistemu za podporo produkciji (npr. bančno okence) do posledične izvedbe ustreznih zapisov v zalednih sistemih (poravnave, knjigovodstvo, poročanje itd.). Vse razlike, spremembe ali razveljavitve transakcije se morajo registrirati prek filtra za OT, ki mora označiti tudi neobičajne vnose. Filter bo v množici podatkov prepoznal škodni dogodek ter morebitne vplive na organizacijo in ga zabeležil v podatkovno bazo za OT.

Pravzaprav ni pravega odgovora na to, do kolikšne mere avtomatizirati zbiranje. Veliko je odvisno od velikosti in kompleksnosti organizacije in obstoječe infrastrukture. Morda se bodo izplačale investicije v obsežen sistem, ki bo odkrival in beležil OT, npr. pranje denarja. Kakorkoli, težava v povezovanju teh sistemov in omejenemu številu virov OT omejuje možnost, da se tovrstne sisteme uporablja učinkovito (Muzzy, 2003, str 60).

Verjetno je smiselno, da banke vsaj na začetku usmerijo napore v zagotovitev sistema za ročni zajem podatkov. Tudi ob avtomatizaciji zbiranja bodo namreč še vedno takšni

dogodki, ki niso zajeti v nobenemu produkcijskemu sistemu ali jih ni možno odkriti v okviru kontrolnih točk in posebnih filtrov.

Praksa je pokazala, da ročni vnos v razpredelnice, na papir in preko elektronske pošte ne zagotavljajo dolgoročne podpore. Potrebna je bolj dodelana podpora za zbiranje in sporočanje podatkov o OT. Najbolj primerna je spletna rešitev, s čimer lahko dobijo dostop praktično vsi zaposleni. Razvita je lahko z lastnimi resursi ali kupljena kot že izdelana rešitev. Odločitev je odvisna tudi od tega, koliko želimo prilagojenosti na naše okoliščine oziroma kako hitro želimo dobiti program.

V obeh primerih se priporoča pilotsko uvajanje v okviru enega poslovnega področja ali produkta (Newberry, 2002, str. 41).

5.5.2 Izvedba

Izvedba procesa zbiranja podatkov²⁰ sestoji iz odkritja, zbiranja, ki vključuje vnos, reševanje, ovrednotenje in avtorizacijo podatkov, ter kontrole, odobritve in poročanja o škodnih dogodkih (Haubenstock, 2004, str. 455-456).

Proces se prične s krajem in načinom **odkritja škodnega dogodka**, na primer napake v procesu, izpada sistema, tožbe. Ta dogodek **zabeležimo**, se pravi, da v bazo vnesemo zahtevane podatke. Verjetno vnos ne bo vedno enostaven in enoznačen, potrebne bodo dodatne raziskave in analize (npr. o ustreznosti kategorizacije). Lahko sledi že faza **reševanja**, s katero se popravijo napake v postopkih, sistemih, nadomesti oprema oziroma izvedejo druge ustrezne korektivne akcije in povračila izgub. Dogodek mora biti nato **ovrednoten** z vidika izgub. Pred zaključkom dogodka se lahko vključi še **avtorizacijo**, kjer podatke o dogodku preveri še vodstvo poslovnega področja ali odgovorni za OT. Hierarhija za avtorizacijo se lahko določi glede na velikost izgub.

Naslednji korak je predložitev dogodkov enoti za upravljanje z OT, ki izvaja **kontrolno** kvalitete podatkov o vseh dogodkih, ustreznost kategorizacije dogodkov, opisov in ovrednotenja izgub. Periodično lahko ta služba v **odobritev** posreduje poslovnim področjem seznam z njihovimi škodnimi dogodki. Ta korak služi kot preverjanje, da so bili vsi dogodki zabeleženi. Enota za upravljanje z OT lahko nato **poroča** o skupnih rezultatih vodstvu poslovnih področij in o agregiranih podatkih najvišjemu vodstvu.

Z organizacijskega vidika mora proces zadostiti različnim kriterijem (Anders, 2003):

- Ker so posamezne faze razdeljene med različne zaposlene, je pomembno zagotoviti preglednost. V vsaki fazi mora biti možnost prepoznati status prijave in odgovorne osebe.

²⁰ V nadaljevanju poglavja se proces nanaša na ročni vnos podatkov. Tako lahko tudi celovito opišemo vse izvedbene faze v procesu.

- Zagotovljeno mora biti, da je znesek izgube pripisan »pravemu« mestu, kar pa se ne sme izvesti brez potrditve s strani lastnika izgube.
- Proces mora omogočati, da se vneseni dogodek lahko zavrne ali posreduje naprej. To je smotno za primere, ko se škodni dogodek odkrije v enoti, ki ni niti odgovorna za škodo niti nima vseh ustreznih informacij, da bi lahko ustrezno poročala o dogodku.
- Obstajati mora možnost delitve zneska izgube med dve ali več organizacijskih enot.

5.5.3 Nadzor in kontrola

Zadnjo fazo zbiranja podatkov predstavljajo postopki kontrole in nadzora, ki zagotavljajo celovitost in popolnost podatkov ter popolnost procesa zbiranja podatkov. V strokovni literaturi se v ta namen uporablja izraz validacija²¹ podatkov o notranjih izgubah.

Ob poudarjanju popolnosti podatkov si velja zastaviti vprašanje: Ali se popolnost podatkov sploh dejansko zahteva? Odgovor lahko poiščemo v dveh smereh (Internal Loss Data Issues, 2005, str. 3):

- Če uporabljamo podatke iz OT za namen **upravljanja z OT**, mora biti sklop podatkov popoln v takšni meri, da so zagotovljene pravilne upravljske odločitve. Analize podatkov, ki ugotavljajo trende v povezavi z OT, so lahko narejene tudi na podlagi 80% celotnega dejanskega števila škodnih dogodkov. Trend bo še vedno opazen oziroma bo smer prepoznavna in se bomo nanj lahko zanesli ob določanju ukrepov in postavitvi strategije upravljanja z OT. Zatorej visoka stopnja popolnosti podatkov iz OT za namen upravljanja ni nujna.
- Lahko pa se podatki uporabljajo za namen **izračuna regulatornega kapitala**. Doslej so modeli naprednih pristopov za izračun kapitala, ki so jih razvile nekatere institucije, pokazali, da se izračunan kapital bistveno ne spremeni v primeru pomanjkanja podatkov o izgubah v spodnjem delu verjetnostne porazdelitve²². Modeli namreč izkazujejo občutljivost na velike in resne škodne dogodke.

Kadar torej govorimo o popolnosti podatkov, mora biti poudarek na zajemu podatkov velikih oziroma bistvenih izgub. Nadzor je potrebno primarno usmeriti v zagotavljanje, da tovrstni škodni dogodki niso izpuščeni, ob temu pa z vidika celovitosti izračunov in analiz zagotoviti primerno popolnost podatkov o dogodkih z manjšimi izgubami.

Poleg obravnavanja popolnosti podatkov in iskanja odgovora na vprašanje »Ali so vsa ključna tveganja v banki zajeta?« pa z validacijo odgovarjamo na vprašanja naslednjih področij (Data Integrity and Validation Issues, 2005, str. 2):

- točnost podatkov: Ali so podatki zbrani dosledno in odražajo pravi nivo tveganja?
- ustreznost podatkov: Ali se podatki nanašajo na tveganje banke?

²¹ Validacija: priznanje ali potrditev veljavnosti.

²² Na spodnjem delu verjetnostne porazdelitve izgub (glej sliko 7) so izgube manjših vrednosti.

- uporabnost podatkov: Ali so podatki v podporo pri odločanju?

5.5.3.1 Postopki validacije

Periodična validacija notranjih podatkov je bistvena za ustrezne odločitve pri upravljanju z OT in zagotavlja, da so rezultati postopkov kvantifikacije OT zanesljivi. Glede na to, da so banke z zbiranjem podatkov šele v začetnih fazah, so tudi metodologije za validacijo podatkov šele v povojih in je dobra praksa šele v nastajanju (Observed range of practice in key elements of Advanced Measurement Approaches, 2006, str. 20).

Banke izvajajo validacijo na različne načine:

□ **analiza podatkov s strani funkcije za upravljanje z OT**

Analiziranje podatkov po kategorijah dogodkov in učinkih, po času in vrednosti lahko zagotovi vpogled v temeljitost procesa. Z dobro komunikacijo znotraj organizacije se lahko poveča raven zaupanja v rezultate. Nekaj primerov vprašanj, ki bi nas lahko zanimala in na katera lahko odgovorimo s pomočjo tovrstnih analiz (Haubenstock, 2004, str. 457) :

- Kako se število prijavljenih dogodkov po poslovnih področjih in kategorijah tveganj spreminja skozi čas?
- Kakšen je profil dogodkov glede na vrednost po poslovnih področjih in kategorijah tveganj? Je porazdelitev v pričakovanih okvirih in če kakšen razpon vrednosti manjka?
- Kakšno je število in vrednost škodnih dogodkov po poslovnih področjih? Ali je proporcionalno z velikostjo poslovnega področja?
- Kako je profil dejanskih dogodkov primerljiv s samoocenjevanjem? So kakšna tveganja, ki so bila identificirana v postopku samoocenjevanj, pa nimajo dejanskih dogodkov? Če ne, ali zaupamo v proces odkrivanja in poročanja o teh dogodkih, ali se dejansko le-ti niso zgodili?

□ **kontrola notranje revizije kot popolnoma neodvisne funkcije**

Notranja revizija mora preverjati, ali se proces zbiranja podatkov izvaja in ali so dogodki sporočeni pravočasno in izgube konsistentno ovrednotene. V okviru svojih rednih pregledov organizacijskih enot preverjajo postopke, povezane z zajemom, zbiranjem in poročanjem o škodnih dogodkih. Osnovo za zagotavljanje kvalitativnih pregledov predstavljajo ustrezno postavljeni standardi in postopki v okviru politike zbiranja podatkov o OT.

□ **notranji benchmarking**

Stopnje izgub po posameznih kategorijah se lahko primerjajo med poslovnimi področji in poiščejo pojasnila za morebitne odklone. Z razvojem konzorcijev²³ je možnih tudi čedalje več zunanjih benchmarkingov.

□ uskladitev z glavno knjigo

Med največkrat omenjenimi načini za izvajanje validacije je zagotovo usklajenost podatkov z glavno knjigo. Teoretično je ta način tudi najboljši pri zagotavljanju celovitosti podatkov, vendar se v praksi izkazujejo velike težave.

Glavna knjiga praviloma vsebuje zapise o izgubah, pri katerih je izkazan dejanski odtok denarja oziroma ko je škodni dogodek imel dejanski vpliv. To pa verjetno ne drži za vse ostale okoliščine, kjer ni fizičnega toka denarja, kot na primer pri oportunitetnih stroških.

Še večje težave pri usklajevanju predstavlja škodni dogodek, ki ima vpliv na številne postavke oziroma račune v glavni knjigi. Razčlenitev vplivov in usklajevanje teh z glavno knjigo ali obratno (združevanje vplivov na ravni glavne knjige in povezovanje le-teh s škodnim dogodkom v bazi OT) ne da je samo težko ali celo nemogoče izvesti, ampak verjetno tudi ne bi imelo koristi za namen upravljanja z OT (Data Integrity and Validation, 2005, str. 4).

Lahko pa banka oceni, da so njeni notranji podatki nezadostni za namen merjenja OT. V temu primeru jih mora dopolniti z zunanjimi podatki in analizami scenarijev. Oboje seveda prav tako potrebuje dodatne validacijske postopke.

5.6 Izzivi zbiranja podatkov v praksi

Z ustrezno vzpostavitev mehanizma za zbiranje notranjih podatkov o škodnih dogodkih banka pridobi najbolj objektivni vir, s katerimi razpolaga in ki odraža pomemben profil njenega tveganja (Ramadurai, 2004a, str. 3).

Kritičen pogled in izkušnje s tega področja pa kažejo na številne težave, s katerimi se banke soočajo pri zbiranju podatkov. Glede na to strokovnjaki opozarjajo na slabost, da banka uporablja samo te podatke kot osnovo za merjenje OT.

5.6.1 Redkost večjih škodnih dogodkov

Medtem ko so škodni dogodki dobro dokumentirani v primeru tržnega in kreditnega tveganja, so podatki o škodnih dogodkih iz OT še vedno redki, saj se ti dogodki do nedavnega niso beležili z nekim standardiziranim postopkom. Ko se takšen postopek vzpostavi, tekom zbiranja postajajo podatki vse bolj kvalitetni in napredujejo v bolj učinkovite indikatorje izpostavljenosti OT, vendar predvsem ko gre za ocenjevanje

²³ Glej poglavje 6.3.1.2.

dogodkov »visoka frekvenca/majhna izguba« (t. i. manjši dogodki, npr. prevare na področju kartičnega poslovanja, napake pri poravnava na računih).

Na večje težave naletimo pri zbiranju podatkov za dogodke tipa »nizka frekvenca/velika izguba« (t. i. večji dogodki, npr. velike prevare na področju trgovanja, večje tožbe, naravne katastrofe), saj je majhna verjetnost, da se v obdobju opazovanja sploh zgodijo. Zaradi pomanjkanja tovrstnih podatkov se lahko banka v svojih analizah in modeliranjih prične zanašati na podatkovne baze manjših dogodkov, kar povzroča probleme vsaj v dveh smereh (Kin Ying Alvis, 2004, str. 79):

- Osnovni namen naprednih modelov ocenjevanja OT je obravnava večjih škodnih dogodkov, ker lahko ogrozijo kapital ali celo solventnost banke, kot se je zgodilo v primeru Barings. Manjši dogodki so s tega vidika sekundarnega pomena. Analize in rezultati modelov, ki temeljijo zgolj na manjših dogodkih, lahko preusmerijo pozornost vodstva od resnih in velikih potencialnih nevarnosti, ki grozijo poslovanju in celo obstoju banke.
- Tudi povzemanje kakršnihkoli zaključkov o nevarnosti velikih dogodkov na podlagi baze manjših dogodkov je problematično. Vzroki večjih dogodkov so namreč bolj kompleksni, saj lahko vključujejo človeške in organizacijske dejavnike, številne zunanje dejavnike in njihove kombinacije. Po drugi strani pa ta raznolikost zmanjšuje tudi uporabno vrednost podatkov o večjih dogodkih, saj zbrani podatki običajno niso relevantni za drugo vrsto tveganja (Rotovnik, 2004b, str. 39). Če banka, na primer, realizira znatne izgube zaradi večjih dogodkov na področju procesiranja podatkov, to samo po sebi še ne pomeni, da je hkrati izpostavljena tudi tveganju zaradi večje prevare svojega trgovalca oziroma da je njen požarni zid neučinkovit.

Zaradi teh pomanjkljivosti notranjih podatkovnih baz postajajo vse bolj aktualne tudi zunanje baze, ki zagotavljajo širši nabor oz. dodatni vir podatkov in s tem nevtralizirajo omenjene težave. V svetu že obstajajo različne tržne pobude za delitev podatkov, vključno z Multinational Operational Risk Exchange (MORE), Global Operational Loss Database (GOLD) in Operational Risk data eXchange (ORX).

Neposredna uporaba zunanjih podatkov pa lahko postane vprašljiva, če se ustrezno ne lotimo problema primerljivosti in relevantnosti teh podatkov za našo banko. Izgube iz OT so praviloma odvisne od organizacijskih struktur (Doering, 2003, str. 85). Velikost in verjetnost za izgubo se namreč močno razlikujeta med posameznimi organizacijami. Težko najdemo dve instituciji, ki bi imeli enako stopnjo izpostavljenosti OT. Celotakšne, ki poslujejo na enakih poslovnih področjih, imajo različno organizacijsko kulturo, vodstvene izkušnje, sposobnosti in znanja zaposlenih, primarna področja, sistem poročanja ipd. (Kin Ying Alvis, 2004, str. 80).

Več o zunanjih podatkih in med drugim tudi o načinih prilagajanja zunanjih podatkov lastnim okoliščinam poslovanja je napisano v poglavju 6.3.

5.6.2 Razmejevanje podatkov od kreditnega in tržnega tveganja

Naslednji problem je pravilno razvrščanje dogodkov iz OT – predvsem v smislu ločevanja izgub iz tržnega in kreditnega tveganja od izgub iz OT. Velikokrat je težko potegniti ločnico med vsemi tremi tveganji. Ko se, na primer, banka kljub jasnim opozorilnim signalom odloči odobriti kredit že preveč zadolženemu kreditojemalcu ali vlagatelju v sumljiv nepremičninski projekt ali stranki iz tveganega področja, je to znak neustreznih notranjih sistemov in napačnega ravnanja zaposlenih kot del OT.

Težavnosti sta se zavedala tudi Baselski komite in Evropska komisija, saj sta oba v svojih dokumentih poskušala razčistiti ta mejna področja. Obe instituciji sta zavzeli stališče, da izgube iz OT, ki so povezane s kreditnim tveganjem in so bile v preteklosti vključene v notranjih zbirkah podatkov o kreditnem tveganju, morajo biti evidentirane v zbirkah podatkov o OT in ločeno označene. Takšne izgube ne bodo predmet kapitalske zahteve za OT, dokler se bodo za namene izračuna minimalnih kapitalskih zahtev obravnavale v okviru kreditnega tveganja. Izgube iz OT, ki so povezane s tržnimi tveganji, pa se vključijo v obseg kapitalske zahteve za OT.

Kljub temu pa razmejevanje izgub, ki so nastale zaradi OT, ostaja problem, za katerega verjetno težko dobimo splošno sprejeto rešitev (ORIAG, 2003, str. 15), saj posameznik lahko različno interpretira dogodek in ga uvrsti med različne tipe tveganja. Pomembna je vloga presoje, kar lahko privede do nekonsistentnosti in manipulacije.

Že prej omenjen primer odobritve kredita v določenih okoliščinah (npr. preveč zadolženemu kreditojemalcu) nam lahko predstavlja vir razmišljanja tudi v smer, ki kaže, da je v bančnem poslovanju obseg kreditnega tveganja nasproti obsegu OT danes močno precenjen. Vprašanje namreč je, ali banke obravnavajo tovrstne primere, potem ko pride do izgub zaradi nezmožnosti odplačila kredita, tudi z vidika OT.

Regulativa dopušča možnosti za različne interpretacije tudi zaradi nedorečenosti, kako obravnavati izgube iz OT, ki so povezane s kreditnim tveganjem, pa v preteklosti niso bile vključene v notranje zbirke podatkov o kreditnem tveganju.

Ker so možni različni pristopi za izračun kapitalskih zahtev za posamezne tipe tveganj, lahko odvisno od umestitve škodnega dogodka izračun kapitala privede do različnih rezultatov (npr. banka pri kreditnem tveganju uporablja napredni pristop, ki naj bi rezultiral v manjši kapitalski zahtevi, pri OT pa enostavnejši pristop, kjer je kapitalska zahteva praviloma višja). To ustvarja možnost za kapitalsko arbitražo²⁴ in napeljuje banke, da klasifikacijo izgub prilagajajo glede na najbolj ugoden izid (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 17).

²⁴ Banke z izkoriščanjem pravil znižujejo zahtevo po regulatornem kapitalu, ne da bi zmanjšale dejansko tveganje (Kin Ying Alvis, 2004, str. 54).

V praksi se je izkazalo, da so banke pravzaprav osvojile koncept razmejevanja izgub iz posameznih vrst tveganj na način, kakor ga je regulator predvidel, ne glede na to, ali pri kreditnem tveganju obstaja zgodovina podatkov. V ta namen so nekatere banke razvile t. i. odločitvena drevesa, nekatere pa so zvišale prag zbiranja podatkov o izgubah, da bi se s tem zmanjšalo število mejnih primerov. Najbolj deljeno mnenje je na področju kartičnih prevar: na eni strani so banke, ki obravnavajo vse tipe kartičnih prevar kot OT, na drugi strani pa so banke, ki obravnavajo s strani tretje osebe povzročeno prevaro kot OT, vse ostale načine prevar pa kot kreditno tveganje (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 18).

V prilogi 6 je navedenih nekaj praktičnih primerov v zvezi s problematiko razmejevanja operativnega od kreditnega in tržnega tveganja. Takšni konkretni primeri so lahko osnova za nadaljnje aktivnosti v banki v smislu dogovarjanja in uveljavljanja dobre poslovne prakse pri načinih razmejevanja tveganj z namenom povečati transparentnost okvira OT.

Če kljub vsemu pri zbiranju podatkov pride do morebitnih nesoglasij, se o obravnavi določenega tveganja lahko odločitev prepusti neodvisni funkciji (npr. službi notranje revizije).

5.6.3 Odvisnost od danih razmer

Odvisnost od danih razmer pomeni, da se velikost in verjetnost dogodka spreminja v različnih situacijah. Glede na to, da se je način poslovanja v 10-ih letih bistveno spremenil (npr. veliko bank se je združilo, spremenilo svoje procese in sisteme) in so različne tudi nevarnosti, ki poslovanje ogrožajo (Ali so, na primer, pred leti banke tako skrbele za varnost pred računalniškimi virusi?), to pomeni, da je OT močno odvisno od danih razmer - v nasprotju s tržnim in kreditnim tveganjem, ki vzdržujeta zmerno odvisnost uporabnosti podatkov od danih razmer. Gibanje cen vrednostnih papirjev na borzi izkazuje podobne statistične značilnosti tudi v daljših obdobjih. Situacija na Wall Streetu leta 1929, na primer, je prepoznavna tudi sodobnemu trgovalcu z vrednostnimi papirji. Kreditno sposobnost kreditojemalcev in izgube zaradi neplačil banke prav tako spremljajo že desetletja, rezultati teh merjenj pa izkazujejo določeno stopnjo podobnosti tudi med različnimi časovnimi obdobji.

Višja kot je tovrstna odvisnost, slabše lahko preteklost napoveduje prihodnost (Holmes, 2003a, str. 86). Zunaj in znotraj organizacije se nenehno odvijajo spremembe, tehnologija napreduje, pojavljajo se novi produkti – z vsem tem postanejo podatki omejene vrednosti, saj ne odražajo več dejanskih nevarnosti (Kin Ying Alvis, 2004, str. 81).

Za vsaj delno rešitev teh problemov tako Baselski komite kot Evropska komisija predlagata, da se v preučevanje vključi tudi dejavnike, ki odražajo poslovno okolje in

notranje kontrolne sisteme, kar naj bi dalo področju in ocenam tveganja tudi večjo mero usmerjenosti v prihodnost.

V ta namen lahko banka poleg notranjih podatkov uporabi še ostala orodja za upravljanje in obvladovanje OT, med njimi samoocenjevanje npr. izkušenih borznih posrednikov o ustreznosti obstoječega kontrolnega sistema ali ključne indikatorje tveganja, kot na primer število neizvršenih poravnjav.

5.6.4 Relevantnost prijavljenih škodnih dogodkov

Eno izmed ključnih vprašanj je »Kako motivirati ljudi, da bodo prijavljali podatke pravilno in v želeni obliki?«. Nekateri podatki, predvsem povezani z goljufijami zaposlenih, so bili doslej redko ustrezno in sistematično zabeleženi. Izgube, povezane z goljufanjem, praviloma kažejo na napake vodstva, kar lahko vodi v prikrivanje pravega razloga in kolikor je le mogoče prikrivanje dejanske velikosti in obsega izgub (Theodore, 2002, str. 6). Pravilno prijavljanje teh dogodkov zahteva od banke temeljito spremembo njenih nazorov oziroma ustrezno organizacijsko kulturo, ki ji je v tej nalogi namenjeno posebno poglavje 8.

6 CELOVITOST PODATKOVNEGA MODELA

Predstavljene pomanjkljivosti notranjih podatkov kažejo na dejstvo, da za ugotavljanje celovite izpostavljenosti banke OT v praksi samo zbiranje notranjih podatkov o vplivu škodnih dogodkov iz realiziranega OT ne zadošča.

Praviloma bo banka s strogo notranjo kontrolo v stabilnem poslovnem okolju ob ostalih nespremenjenih okoliščinah manj izpostavljena OT kot banka s slabostmi v kontrolnih sistemih, hitro stopnjo rasti in ob uvajanju novih produktov. Zato mora banka v svoj profil OT vključiti dejavnike poslovnega okolja in notranje kontrole, s čimer postanejo ocene bolj usmerjene tudi v prihodnost in odražajo hitro spreminjajoče se okolje, kar je tudi odgovor na eno izmed kritik uporabe v preteklost usmerjenih podatkov o izgubah iz OT. Ti dejavniki so tudi eden izmed štirih elementov upravljanja z OT, ki jih za napredne pristope zahtevata tako Basel II kot Direktiva²⁵.

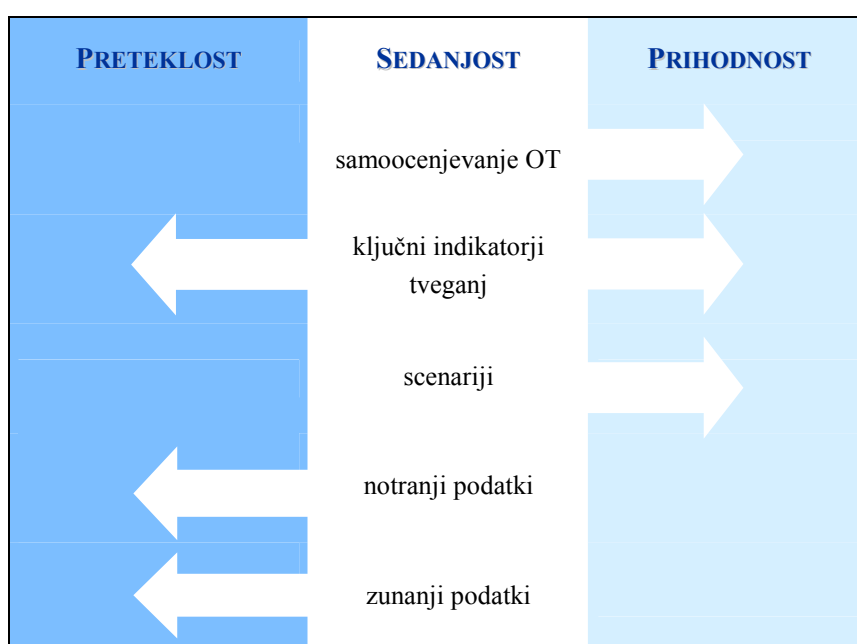
Banke so razvile predvsem dva pristopa za obravnavo omenjenih dejavnikov, in sicer samoocenjevanje tveganj ter ključne indikatorje tveganj. V razvoju pa je tudi uporaba t. i. točkovanj kot specifična različica samoocenjevanj (Observed range of practice in key elements of Advanced Measurement Approaches, 2006, str. 11).

²⁵ Poleg dejavnikov, ki odražajo poslovno okolje in notranje kontrolne sisteme, so navedeni še notranji podatki, zunanji podatki in analize scenarijev.

Celovitost podatkovnega modela zagotavljajo tudi zunanji podatki o izgubah iz OT in analiziranje različnih scenarijev nastanka škodnih dogodkov, s katerimi se dopolnjuje pomanjkanje notranjih podatkov v določenih kategorijah tveganj ter predvsem škodnih dogodkov vrste »nizka frekvenca/velika izguba« in pri katastrofalnih izgubah.

Ključna orodja za upravljanje z OT, s katerimi pridobimo celovit podatkovni model, ponazarjam z naslednjo sliko. Iz slike je razvidno, kako s širšo paleto orodij pridobimo tudi ustrezen pregled nad preteklimi izkušnjami in predvidevanji za prihodnje razmere, kar vse vpliva na dejansko izpostavljenost zaradi OT.

SLIKA 5: Ključna orodja za upravljanje z OT in njihova usmerjenost



VIR: Algo OpRisk Case Study, str. 2

6.1 Ključni indikatorji tveganja

Ključni indikatorji tveganja (v nadaljevanju: indikatorji) so eden izmed načinov za pridobivanje podatkov o dejavnikih, ki odražajo poslovno okolje in notranje kontrolne sisteme. Gre za postopek iskanja anomalij, ki za razliko od merjenja realiziranih finančnih posledic škodnih dogodkov označujejo potencialno izgubo oziroma možnost nastanka izgube.

Indikatorji opozarjajo vodstvo na spremembe v organizaciji, ki lahko predstavljajo zaskrbljujoče OT. Najbolj uporabni so indikatorji, ki kažejo na spremembe v poslovnem okolju in kontrolnih sistemih, še preden pride do izgub (Beck, 2005, str. 6). S tem ima vodstvo čas za ustrezno ukrepanje. Opozorilni signal se sproži, ko indikator preseže mejno

vrednost. V ta namen morajo biti določene tolerančne meje, ki vzpostavljajo evidenčno omejitev še sprejemljive realizacije spremljajočih pojavnih oblik OT. V primeru prekoračitve tolerančne meje je potrebno pozornejše spremljanje dogajanja na pripadajočem področju ter morebitno ukrepanje (Kavšek, 2005, str. 68). Npr. indikator »izraba kapacitet informacijskega sistema« je uporabljen za oceno faktorja tveganja informacijske tehnologije v zvezi s stabilnostjo izvrševanja procesov. Če je npr. presežen prag 85% kapacitet, se generira zgodnje opozorilo, ki zahteva odgovor.

Po drugi strani pa indikatorji pomagajo odkriti slabosti posameznega procesa ali sistema. Primer takšnega indikatorja na področju procesiranja transakcij je število napak pri mednarodnih prenosih med računi. Njihovo število lahko narašča zaradi napačnega delovanja nekega procesa oziroma procedure, ki je povezana s samo transakcijo prenosa. Pri izvedbi transakcije se izvedejo tudi ustrezna knjiženja v glavno knjigo posamezne banke. Praviloma se bodo istovrstne knjižbe skladale, lahko pa tudi ne. Razlike so lahko rezultat različnih računovodskih sistemov, napak v programu, površnosti pri ročnem knjiženju, ali pa so posledica kakšnih drugih začasnih vzrokov, ki pa običajno ne zahtevajo nadaljnje intervencije. Možno je tudi, da je takšna napaka pokazatelj tipične situacije, ki pod določenimi pogoji (npr.časna odsotnost strokovnjaka, ki edini zna v banki odkriti in programsko popraviti nastalo napako) kasneje izzove izgubo.

Indikator je lahko torej tudi pokazatelj stabilnosti posameznega procesa ali sistema in predmet analize pri vsakem konkretnem primeru za pridobitev ustreznega pregleda nad situacijo ter za izboljšanje upravljanja s pripadajočim OT (Rotovnik, 2003a, str. 13).

Za ponazoritev navajam nekaj možnih indikatorjev po različnih kategorijah škodnih dogodkov.

Notranja goljufija

tveganje notranje goljufije - število nadpovprečnih zaslužkov

Ravnanja v zvezi z zaposlovanjem in varnostjo pri delu

fluktuacija delovne sile - razmerje med mlado (<6 mesecev) in staro (> 5 let) delovno silo

- odstotek zaposlenih, ki so odšli v preteklih 12-ih mesecih

- število zaposlenih po pogodbi nasproti številu redno zaposlenih

tveganje iz nadurnega dela - število nadur kot odstotek vseh delovnih ur

Stranke, produkti in poslovna praksa

odprte sodne zadeve/tožbe - število odprtih sodnih zadev/tožb

reklamacijski postopki - število utemeljenih pritožb strank

Poslovne motnje in izpadi sistemov

tveganje izpada sistemov - povprečna starost strojne opreme

stabilnost programske opreme - število potrebnih sprememb v programu

Izvedba, dostava in upravljanje procesov

napačna izvedba prenosa v tujino - število napak pri prenosih na računih

tveganje izvajanja plačilnega prometa - zamudne obresti zaradi prepoznih plačil v % od celotnega prihodka plačilnega prometa

Velikokrat so najbolj nenavadni indikatorji najbolj primerni pokazatelj za določeno vrsto tveganja. Tako je tudi v primeru števila nadpovprečnih zaslužkov posameznega borznega posrednika, ki so na eni strani lahko osnova za nagrajevanje uspešnosti zaposlenih, na drugi strani pa ob dodatnih analizah ključni pri ugotavljanju notranje goljufije.

Zanimiva je primerjava uporabne vrednosti posameznega indikatorja, npr. neuspešna poravnava transakcije. Čeprav nam absolutna vrednost indikatorja sama po sebi ne pove veliko (npr. 5 neuspešnih poravnav na leto), so lahko veliko bolj uporabne relativne številke – med enotami ali v okviru ene enote spremljanja skozi časovno obdobje. Pri interpretaciji pomagajo dodatne analize: npr. relativne številke se združijo v indeks – dnevni porast posredniških transakcij pomnožen s spremembo v številu zaposlenih v okviru področja (obe številki izraženi v %).

Pri indikatorjih lahko nastane težava zaradi velikega števila različnih indikatorjev²⁶. Zato predstavlja glavni izziv za banko izbrati najbolj pomembne statistične podatke in jih uporabiti za ključne indikatorje (Jameson, 2004).

Po nekaterih mnenjih naj bi bili vsaj trije indikatorji pri vsaki izmed 7-ih kategorij tveganja, verjetno več v kategorijah, kjer je ocenjeno tveganje med večjimi²⁷. V uporabi naj ne bi bilo več kot 25 indikatorjev. V nasprotnem primeru bo število podatkov prekomerno (Kennett, 2001, str. 79).

Nekateri indikatorji se lahko postavljajo na previsoki ravni. Npr. stopnja fluktuacije zaposlenih v okviru celotne banke ne more pokazati pravzaprav na nobeno posebno OT.

Vprašanje je, ali uporabljati enake podatke o indikatorjih v vseh delih banke. Odgovor je ne, ker sta npr. investicijsko bančništvo in poslovanje s prebivalstvom zelo različni področji, ki potrebuje različne indikatorje. Potrebno je dopustiti področjem, da spremljajo, kar mislijo, da dejansko odraža njihovo OT. Seveda pa morajo obstajati splošne usmeritve in kontrola, ki zagotavlja konsistentne definicije vsakega indikatorja, ki se uporablja v banki (Kennett, 2001, str. 78). Lahko pa se na nivoju celotne banke sprejme niz univerzalnih in standardiziranih indikatorjev in jih poslovna področja kot takšna nato sprejmejo (ali pa ne). S tem je omogočena agregacija in možnost primerjave podatkov (Algo OpRisk Case Study, str. 2). Nekateri indikatorji bodo uporabni povsod, kot na primer sprememba števila zaposlenih.

Določanje indikatorjev mora postati v banki nenehen proces. Spremembo indikatorjev bodo zahtevale številne spremembe v okolju in organizaciji in posledično nastajanje novih tveganj ter spreminjanje obstoječih. Že s samim razvojem indikatorjev bodo nastajali novi, ki bodo vedno bolj natančni.

Ko so indikatorji enkrat določeni, je potrebno začeti zbirati dejanske podatke, iz katerih se bodo indikatorji izpeljali. Najprej je verjetno najbolje uporabiti podatke, ki že obstajajo, kar ne pomeni kreiranja indikatorjev na osnovi obstoječih podatkov. Nekateri vidijo problem v dejstvu, da nekatere podatke zagotavljajo poslovna področja sama, kar naj bi zmanjševalo objektivnost indikatorjev (Beck, 2005, str. 6).

²⁶ Glede na nekatere raziskave se giblje število možnih ključnih indikatorjev tveganja okoli 1500 (Jameson, 2004).

²⁷ Na to temo so bile izvedene različne raziskave. V eni izmed takšnih sta najvišje rangirani tveganji v povezavi z izpadom informacijskega sistema (60,8% vseh vprašanih je to kategorijo uvrstilo med 5 najbolj tveganih kategorij) in neuspešno izvedbo transakcij (48,6% vseh vprašanih je to kategorijo uvrstilo med 5 najbolj tveganih kategorij) (The broadening scope of op risk management, 2006). Tudi po drugi raziskavi je kategorija »izvedba, dostava in upravljanje procesov«, in še posebej upravljanje s transakcijami in podatki, označena kot visoko tvegana. Slaba tehnologija in postopki ter nepravi podatki sicer povzročajo manjše izgube, njihov seštevek pa lahko v zelo kratkem času predstavlja bistvene zneske, kar to kategorijo tudi uvršča med bolj tvegane (Taylor, 2003, str. 60).

Čeprav številni vidijo v uporabi indikatorjev pomemben vir učinkovitega upravljanje z OT, tuje izkušnje kažejo, da navkljub številnim pobudam večina institucij še ni dobila pomembnejših koristi iz svojih ogroditelj za uporabo indikatorjev (Capital Requirements Directive Implementatio, 2006, str. 8).

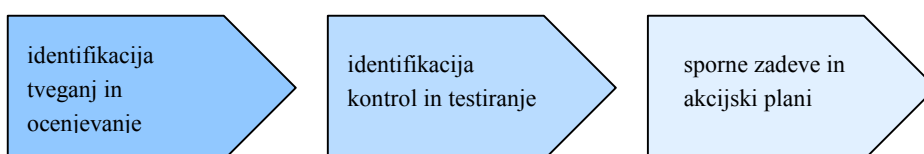
6.2 Samoocenjevanje

Samoocenjevanje tveganj in sistema kontrol (v nadaljevanju: samoocenjevanje) se je v zadnjih 20-ih letih razvilo iz metodologije, ki jo je uporabljala predvsem notranja revizija, v pristop za upravljanje z OT (Kaishan, 2007). Je sistematična metoda poročanja in dokumentiranja tveganj, kontrol in akcijskih planov in je njen glavni cilj pospeševati identifikacijo, ocenjevanje in zmanjševanje OT (Geiger, 2001, str. 69).

Veliko bank bo uporabilo samoocenjevanje kot osnovo za identifikacijo in ocenjevanje njihove izpostavljenosti OT, kar je ponavadi prvi korak v procesu upravljanja z OT in osnova za zbiranje podatkov o škodnih dogodkih. Pristop sicer zahteva nekaj spretnosti in izkušenj pri analizi zbranih informacij, je pa lahko zelo uporaben, poleg tega so stroški takšnega zbiranja podatkov relativno nizki (Andersen, 1998, str. 84).

Osnovni princip pri samoocenjevanju je, da ljudje z dobrim poznavanjem poslovanja – praviloma vodje poslovnih enot – identificirajo potencialen vir OT. Na ta način so vodje tudi prisiljeni, da mislijo na OT, s katerimi se srečujejo, kar izboljšuje zavedanje in upravljanje s temi tveganji in povečuje njihovo odgovornost (Beck, 2005, str. 4).

SLIKA 6: Prikaz postopka samoocenjevanj



VIR: Kaishan, 2007

Kot prikazuje zgornja slika se samoocenjevanje prične z **identifikacijo in ocenjevanjem tveganj**, njihovim rangiranjem in izdelavo profilov tveganj. Učinkovito se lahko uporablja za razumevanje, kakšen vpliv bo imel nek škodni dogodek na zmožnost, da banka posluje.

Izvajanje samoocenjevanj se ponavadi izvaja kot pristop »od spodaj navzgor«, kar pomeni, da vodje poslovnih linij zagotavljajo informacije, ki so potrebne za ogroditelj upravljanja z OT. Z namenom pridobiti najvišji pogled na OT banke pa se lahko izvaja najprej pristop »od zgoraj navzdol«, tako da se angažira najvišje vodstvo (Beck, 2005, str. 4).

Za izvajanje metode sta največkrat uporabljeni orodji sestanki oziroma delavnice »brainstorming«, s katerimi se poskuša pridobiti strokovne ocene in mnenja, in vprašalniki, ki se jih pošlje vodjem organizacijskih enot.

Bolj napredne banke pri zbiranju informacij uporabljajo intranet tehnologijo, ki informacije prenese neposredno v podatkovno bazo za analizo. To banki prihrani čas, informacije pa so bolj sveže in uporabne (Andersen, 1998, str. 84).

Vodje vsak za svojo enoto subjektivno, s pomočjo vprašalnika oz. vprašanj, ocenijo, katera OT so v njihovem okolju prisotna. Pri tem lahko izhajajo iz konkretnih dogodkov v preteklosti in nastalih posledic. Na podlagi ugotovljenega vzroka se definira posamezni dogodek, predvidi verjetnost dogodka ter možne posledice. Vprašalniki lahko temeljijo tudi na scenarijih, npr. izpad pomembnega (točno določenega) informacijskega sistema v (točno določenem) kritičnem času. Za vsak scenarij strokovnjak poda oceno verjetnosti (ponavadi od 1 do 5), s katero bi se dogodek lahko zgodil, ter možne posledice (npr. od 1 - brez posledic do 5 - katastrofalne posledice).

Oblikovanje vprašalnikov predstavlja poseben izziv, saj morajo biti ti dovolj splošni za vsa poslovna področja, hkrati pa dovolj specifični, da lahko zberemo pomembne informacije. Pri tem je pomembno, da povprašujemo le po tistih informacijah, ki jih resnično potrebujemo (Andersen, 1998, str. 83). Potrebno je zajeti kar največ področij poslovanja, za kar mora biti nabor vprašanj dovolj obširen. Vključevati mora področja od načrtovanja, vodenja, prepoznavanja tveganj, organizacije, postopkov dela, zaposlenih, informacijskih sistemov, varnosti podatkov, materialnega premoženja do zunanjega okolja (Slak, 2007, str. 26).

Na podlagi identificiranih in ocenjenih dogodkov se sestavi ocenjeni profil OT, ki se lahko prikaže v obliki matrike 5 x 5 polj (matrika verjetnosti/resnosti) oziroma razsevnega grafikona, iz katerega se vidi največja koncentracija tveganj (glej sliko 8).

Zaradi dinamičnosti profila tveganj je potrebno samoocenjevanje izvajati redno – periodično.

Ko je enkrat ocenjevanje tveganj na osnovi verjetnosti in vpliva na poslovanje končano, se **identificira relevantne kontrole** (vzpostavljenost in učinkovitost kontrol, ki naj bi zmanjševale obravnavano tveganje), ki se jih **validira** skozi periodična testiranja.

Na koncu se od zaposlenih pričakuje, da razvijejo **akcijski plan** (npr. plan reševanja neposredno po škodnem dogodku, plan neprekinjenega poslovanja, komunikacijski plan) za obravnavo tveganj in pomanjkljivosti kontrol.

Slabost te metode je v njeni subjektivnosti oziroma uveljavljanju lastnih interesov. Udeleženi v procesu samoocenjevanja imajo lahko razloge, namerne ali nenamerne, da niso povsem odkriti pri razkrivanju tveganj.

Izkušnje so pokazale, da so posamezniki pri samoocenjevanju nagnjeni k izvajanju sistematičnih napak zaradi (Capital Requirements Directive Implementation, 2006, str. 4):

- pretiravanja pri oceni verjetnosti nastanka in vpliva škodnih dogodkov, ki se jih je najlažje spomniti (npr. dogodki, ki so se zgodili pred kratkim),
- podcenjevanja pri ocenah v zvezi z največjimi škodnimi dogodki,
- podcenjevanja ocen tveganj, ki obstajajo v majhnih enotah.

Uporabo podatkov na podlagi samoocenjevanj torej spremljajo novi problemi in tveganja. Temu se lahko izognemo, če se vzpostavi nepristranska kontrola tovrstnih kvalitativnih podatkov, npr. s strani notranjih revizorjev (Hiwatashi, 2002, str. 4). Prav tako je pomembna njihova validacija z notranjimi in zunanjimi podatki kot pokazatelji preteklih izkušenj (Beck, 2005, str. 4).

6.2.1 Točkovanje

Točkovanje je zelo podobna metoda kot samoocenjevanje. Razlike so v samem postopku. Pri samoocenjevanju vodje sami pregledujejo ključne procese in identificirajo z njimi povezana tveganja ter relevantne kontrole. Pri točkovanju pa vse te elemente identificirajo že v okviru centralne funkcije za OT in jih vodje nato ocenijo skozi odgovore na vprašanja s pripadajočimi točkami. Prednost metode je, da omogoča pretvorbo kvalitativnih ocen v kvantitativne mere, ki izkazujejo relativne range različnih tipov OT (Beck, 2005, str. 5).

Sam postopek se prične z razdelitvijo poslovnih aktivnosti v standardizirana poslovna področja. Vsakemu od teh področij se pripišejo specifične kategorije OT. Za te se identificirajo potencialni viri OT in kontrole, ki zmanjšujejo vsako vrsto OT. Vpliv teh dejavnikov in kontrol se nato oceni s pomočjo vodij.

Odgovori na vprašalnik imajo pripisane numerične vrednosti, s čimer se omogoči ovrednotenje nivoja OT.

Na primer, za ugotavljanje vpliva nekega dogodka se lahko uporabi rangiranje s točkami:

- 5 - zelo velik vpliv (poguben/katastrofalen)
- 4 - velik vpliv (bistven/pomemben)
- 3 - srednji vpliv (znosen/zmeren)
- 2 - majhen (zanemarljiv/manjši)
- 1 - zelo majhen (ni vpliva/nepomemben).

Vprašanja imajo različne ponderje, ki odražajo njihovo relativno pomembnost, npr. glede na velikost poslovanja.

Tveganja te metode izvirajo iz težav pri njeni implementaciji. Ponderiranje pomembno vpliva na končen rezultat in je subjektivne narave. Konsistentnost odgovorov je ključna in se jo v okviru celotne organizacije težko doseže. Izpolnjevanje vprašalnikov lahko postane papirnata vojna, če poslovne enote ne razumejo pomena točkovanja. Prav tako obstaja

tveganje, da po enem ali dveh izvedenih točkovanjih pride do izigravanja sistema z namenom, da je končni rezultat ugoden (Beck, str. 5).

6.3 Zunanji podatki

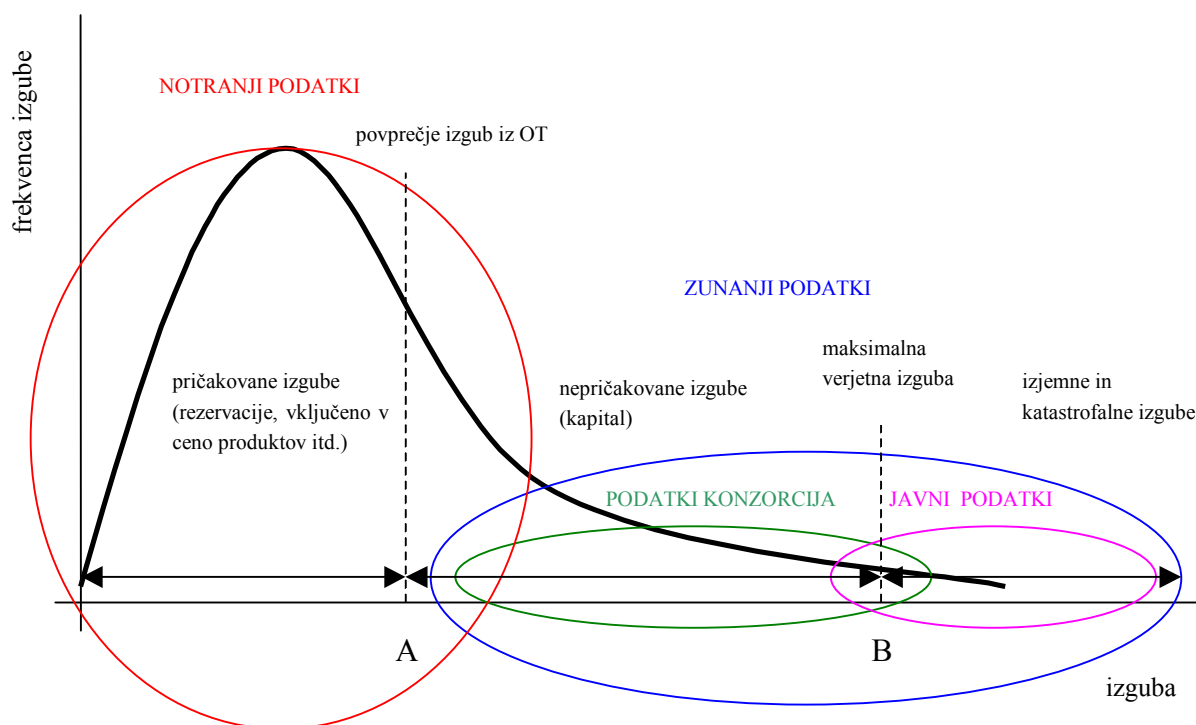
Zunanji podatki so uporabni na različne načine (Emerging Trends in Operational Risk within the Financial Services Industry, 2002, str.17):

- za primerjavo s primerljivo skupino:
Če ima banka veliko nižji nivo škodnih dogodkov od primerljivega, je to morda pokazatelj, da določen tip dogodkov ni bil odkrit, če pa je nivo višji, je to morda signal za pregled kontrolnih postopkov;
- kot izobrazbeno orodje,
s katerim banka usmeri dodatne napore na področja, kjer želi preprečiti podobne škodne dogodke. Npr. poznavanje primera Barings lahko usmeri pozornost na določene pomanjkljivosti internih kontrol.

Pri naprednih modelih so lahko zunanji podatki vključeni v izračune kapitala za pokrivanje OT. Nekatere banke uporabljajo zunanje podatke kot neposredni vložek (input) v modele (zunanji podatki lahko nadomestijo nezadostnost notranjih podatkov na področjih, kjer je banka izpostavljena OT, a še nima lastnih bistvenih izkušenj), druge kot posredni vložek (input) (na primer kot osnovo za konstruiranje scenarijev, za validacijo rezultatov, pridobljenih z notranjimi podatki, ali kot obliko primerjanja (benchmarking)) (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 28).

Za boljše razumevanje uporabnosti notranjih in zunanjih podatkov o škodnih dogodkih si pogledajmo njihovo vlogo pri naprednem pristopu s statistično obravnavo izgube iz OT. Spodnji graf prikazuje hipotetično krivuljo statistične distribucije izgub iz OT, na primer notranje goljufije v obdobju enega leta. Za takšno krivuljo mora banka razpolagati s tolikšno količino kvalitetnih podatkov, da bo z njimi zagotovila pravilno nastavitve parametrov in njihovih predpostavk v statističnem modelu.

SLIKA 7: Krivulja statistične distribucije izgub iz OT in vloga podatkov²⁸



VIR: Rotovnik, 2004b, str. 58

Notranji podatki so dober vir za ovrednotenje pričakovanih izgub banke (točka A) z opozorilom, da so osnovane na podlagi preteklih izkušenj. Težava nastane pri škodnih dogodkih tipa »nizka frekvenca/velika izguba« ter pri katastrofalnih škodnih dogodkih, ki so na repu zgornje krivulje (izgube nad točko A). Teh podatkov v banki načeloma ni oziroma jih ni toliko, da bi lahko na njihovi osnovi izračunali pravilno statistično distribucijo izgub iz OT ter posledično potrebno višino kapitala. To vrzel lahko zapolnijo zunanji podatki.

²⁸ Osnovna razlaga krivulje:

- točka A: srednja vrednost funkcije distribucije izgub. Za banko predstavlja pričakovano OT, ki je financirano z dobičkom oziroma so zanj oblikovane rezervacije.
- točka B: maksimalna verjetna izguba. Predvideva tako velik znesek izgube, da obstaja velika verjetnost (npr. 99%), da bodo dejanske izgube manjše ali enake temu znesku. Za izgube med A in B mora banka oblikovati zadostno višino kapitala, saj te izgube presegajo nivo dobička banke. Izgube nad točko B so večje od kapitala banke, zato v primeru teh postane nesolventna.

6.3.1 Viri zunanjih podatkov

Bankam se ponujajo različne možnosti pridobivanja podatkov o zunanjih škodnih dogodkih (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 22):

- z izgradnjo in vzdrževanjem lastne baze podatkov s pomočjo zbiranja relevantnih informacij iz javnih virov, kot na primer časopisi, revije, medmrežje ipd.,
- z nakupom zunanjih podatkov od komercialnih ponudnikov,
- s sodelovanjem v konzorcijih, katerih podatki pokrivajo najširši spekter škodnih dogodkov.

6.3.1.1 Baze na osnovi javnih podatkov

□ Lastne baze

Veliko bank začne zbiranje z lastnim angažiranjem, tako da nameni nekaj sredstev za pregledovanje javnih virov (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk, 2003, str.10). Velikokrat se ponujajo tudi možnosti pridobivanja koristnih informacij s sodelovanjem v različnih bančnih združenjih (na primer iz slovenske bančne prakse odbor za preprečevanje pranja denarja v okviru Združenja bank Slovenije).

Poglavitna prednost takšnega zbiranja zunanjih podatkov je, da ni drago.

Če pa želimo pridobiti celovite in podrobne podatke, postane zbiranje lahko časovno zelo zamudno, kljub temu v bazi zagotovo ostane veliko neizpoljenih polj. Takšni podatki so tudi predmet številnih pristranskosti: mediji so bolj usmerjeni k poročanju o senzacionalnih dogodkih, na primer goljufijah, tožbah in naravnih katastrofah (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk., 2003, str. 11).

Na ugotovljene izgube in stroške se ni možno zanašati. Pri tako občutljivih podatkih, kot so škodni dogodki iz OT, vedno obstaja nevarnost, da se javnosti ne razkrijejo vsi elementi škodnega dogodka, vključno z izgubo.

Podatki, zbrani na ta način, imajo drugorazredno obravnavo, saj jih je relativno težko preveriti in so zaradi tega tudi bolj nezanesljivi (Rotovnik, 2004, str 60). Glede na to so podatki v okviru omenjenih združenj morda bolj ustrezni, a so po drugi strani omejeni na določene tipe tveganj in poslovna področja.

□ Baze komercialnih ponudnikov

Nekateri komercialni ponudniki za podatke iz OT (npr. OpRisk Analytics, Fitch Inc.-IC²) so v tej dejavnosti očitno zaznali tržno priložnost. Ti ponudniki zbirajo podatke iz različnih javnih virov: tiska, poročil podjetij in sodišč, regulatornih

poročil, televizije in drugih medijev. Ekipe urednikov analizirajo javno dostopne podatke ter jih proti plačilu ter v določeni obliki posredujejo zainteresiranim finančnim institucijam.

Uporabniki bodo verjetno tako pridobili več podatkov, kot če se tega lotijo sami. Vendar pa so tudi ti podatki podvrženi nezanesljivosti in pristranskostim, ki izhajajo iz značilnosti medijev.

Zunanji podatki na osnovi javnih podatkov so zaradi navedenih značilnosti bolj primerni za namen upravljanja z OT kot pa za uporabo neposredno v naprednih modelih. Za banko lahko predstavljajo smernice za različne možne scenarije, poleg tega pripomorejo k pravočasni identifikaciji ukrepov za zmanjševanje verjetnosti realizacije teh škodnih dogodkov v njeni organizaciji (Rotovnik, 2004, str. 60).

6.3.1.2 Baze konzorcijev bank

Baze podatkov o OT od konzorcijev bank v svetu pridobivajo na pozornosti (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk., 2003, str. 11). Eden prvih iz leta 2000 pod okriljem British Bankers Association (BBA) je poznan pod imenom GOLD (Global Operational risk Loss Data). Konzorcij je pritegnil k sodelovanju predvsem banke s sedežem ali podružnico v Londonu, kar pa ne pomeni, da so škodni dogodki omejeni samo na to geografsko področje²⁹ (Hoffman, 2002, str. 227).

Trenutno je verjetno najbolj aktualen konzorcij ORX (Operational Risk data eXchange), ki je bil ustanovljen 2002 na pobudo 12-ih vodilnih severnoameriških in evropskih bank³⁰ in se trenutno ponaša s 35 člani in 63.500 zabeleženimi škodnimi dogodki v skupni vrednosti 21 milijard EUR (ORX Database and Report).

Številna bančna združenja razmišljajo o ustanovitvi konzorcijev na nacionalni ravni³¹.

Osnovna ideja teh konzorcijev je, da člani prispevajo svoje podatke o OT in imajo v zameno vpogled v celoten profil podatkov vseh članov. Temelj celotnega koncepta je anonimnost in zaupnost podatkov, kar je eden ključnih dejavnikov, zaradi katerega so banke sploh motivirane za posredovanje svojih podatkov o škodnih dogodkih v skupno zunanjo bazo. Takšna motivacija je zelo pomembna, saj natančnost izračuna funkcije

²⁹ Za sodelovanje z BBA naj bi se zanimala tudi nekatera druga evropska združenja bank (Hoffman, 2002, str. 227).

³⁰ ABN-AMRO (Amsterdam), Banco Bilbao Vizcaya Argentaria (Madrid), The Bank of Nova Scotia (Toronto), BNP Paribas (Pariz), Commerzbank AG (Frankfurt), Danske Bank A/S (Kobenhavn), Deutsche Bank AG (Frankfurt), Euroclear Bank (Brusel), Fortis (Brusel), ING (Amsterdam), JPMorganChase (New York), SanPaoloIMI SpA (Torino).

³¹ Na bolj neformalni osnovi so si nekatere banke že delile podatke iz OT, kot na primer britanske, kanadske, nemške in skandinavske banke (Hoffman, 2002, str. 227).

statistične distribucije izgube ter posledično alokacije kapitala narašča s količino posredovanih podatkov (Rotovnik, 2004, str. 59).

Glavna prednost teh podatkov je, da omogočajo dostop do večjega vzorca različnih vrst podatkov, potrebnih za natančnejše statistične analize. Vendar pa mora po drugi strani banka izpolnjevati vrsto zelo zahtevnih kriterijev za pridobitev članstva v konzorciju. Osnovni pogoj je kvalitetna interna baza podatkov ter urejen proces zbiranja podatkov o internih škodnih dogodkih, saj jih bo kot članica konzorcija v standardizirani obliki dolžna posredovati v skupno bazo podatkov konzorcija. V prid zagotavljanja kvalitete podatkov v skupni bazi konzorcija morajo imeti banke izdelano natančno pisno politiko internega zbiranja podatkov o škodnih dogodkih ter v ta namen vzpostavljeno učinkovito infrastrukturo tako z vidika informacijske tehnologije kot tudi z vidika celovitosti internih procedur. Standardiziran prenos podatkov iz interne v skupno bazo podatkov zahteva prilagoditev atributov internih podatkov lastnostim polj skupne baze podatkov ter trajno zagotavljanje konsistentnosti vrst podatkov, ki so predmet prenosa in potrebne kategorizacije. Politika zbiranja podatkov v skupne baze se sicer lahko razlikuje od konzorcija do konzorcija, vendar pa vse zahtevajo zlasti podatke, ki se v posamezni banki uporabljajo v interne namene upravljanja z OT (Rotovnik, 2004, str. 59).

Kljub očitnim prednostim in koristim skupnih baz podatkov konzorcijev bank pa se poleg težav, ki lahko izhajajo iz usklajevanja različnih interesov njihovih članic, le-te otepajo tudi z nekaterimi vsebinskimi slabostmi. Namreč, podobno kot pri internih bazah podatkov jim primanjkuje podatkov z repa statistične distribucije oziroma škodnih dogodkov, ki se odražajo v velikih in katastrofalnih izgubah (Rotovnik, 2004, str. 59).

6.3.2 Izzivi pri uporabi zunanjih podatkov v praksi

Vse omejitve in kritike notranjih podatkov (popolnost, konsistentnost, kvaliteta ...) veljajo tudi pri zunanjih podatkih in jih ne bom ponovno izpostavljala.

Že tako dovolj izzivov uporabnikom zunanjih podatkov prinaša glavno vprašanje, kako prilagoditi podatke za uporabo v heterogenih institucijah. Vsaka banka ima različno razvite kontrolne mehanizme in nivoje sprejemljivosti OT, kar nedvomno vpliva na naravo prijavljenih škodnih dogodkov. Razlike so v velikosti oziroma številu bančnih operacij, kar prav tako otežuje neposredno primerjavo.

Govorimo o relevantnosti zunanjih podatkov.

Beseda »relevanten« je izpostavljena že v samih regulatornih dokumentih, kjer je zapisano, da morajo banke pri uporabi naprednih modelov za interno merjenje OT uporabljati relevantne zunanje podatke, kar ne pomeni katerih koli zunanjih podatkov, ampak samo tiste, ki so glede na njeno situacijo ustrezni.

Ker sta poslovno in kontrolno okolje, v katerem banka posluje, med glavnimi dejavniki njene izpostavljenosti OT, izkušnje drugih bank, ki poslujejo v drugačnem okolju, ne morejo biti relevantne za našo banko. Na primer, če je delež poslovanja s prebivalstvom nepomemben za našo banko, medtem ko je za ostale banke to poglavitna dejavnost, bo ob uporabi zunanjih podatkov na temu področju OT previsoko ocenjeno. Enako je v primeru velikih razlik v kontrolnih sistemih. Na primer, obširni pregled s strani regulatorja v primeru večje izgube zaradi neavtoriziranega trgovanja odkrije resne slabosti in luknje v notranji kontroli. Vključevanje teh podatkov za izračun kapitala v banki z močno interno kontrolo bo rezultiralo v previsoki zahtevi po regulatornem kapitalu.

Prav tako je OT odvisno od velikosti banke oziroma števila njenih operacij. Večja banka je izpostavljena večjemu OT. Dejanski odnos je lahko močnejši ali šibkejši, odvisno od kategorije tveganja. Če banka ne upošteva različne velikosti ostalih bank, lahko ob uporabi zunanjih podatkov pride do popačenih ocen o OT banke.

Prilagajanje zunanjih podatkov njenim okoliščinam predstavlja za banko pravi izziv:

- Eden izmed načinov, kako vključiti samo relevantne podatke, je segmentacija zunanjih podatkov v primerljive skupine in uporaba tistih podatkov, ki so primerljivi banki (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk., 2003, str. 14). Podatek o škodnem dogodku iz OT, ki ga bo banka dala na razpolago zunanji bazi podatkov in s tem zainteresiranim bankam za potrebe njihovega internega merjenja OT, bo moral tako vsebovati številne podrobnosti, kot so vzroki in okoliščine realizacije dogodka, znesek izgube, poslovni proces oziroma enota, kjer je dogodek nastal, ter vse ostale informacije, ki bi lahko bile v pomoč pri ocenjevanju relevantnosti škodnega dogodka za ostale banke.
- Pogosto se velikost izgub poveže z velikostjo institucije in tako prilagaja izgubo ene institucije nivoju možnih izgub druge institucije (Beck, 2005, str. 8). Kot prvo se tu postavlja vprašanje, s čim sploh opredeliti velikost institucije. Ali je to velikost aktive, obseg transakcij (število oz. znesek), število zaposlenih ipd.? Kot drugo, ta povezava vedno ne vzdrži in niti ni vedno linearna. Na primer, ali je notranja goljufija odvisna od velikosti? Banka je lahko bolj ranljiva na dogodke manjših organizacijskih enot, ki niso jedro poslovanja in njihovo področje ni dovolj poznano. Zato se lahko izvede regresijska analiza za določanje odnosa med velikostjo banke in frekvenco škodnih dogodkov in odnosa med resnostjo izgub in velikostjo banke.
- Pri uporabi zunanjih podatkov je težko delati prilagoditve razlikam v notranjih kontrolah. Morda se to lažje izvaja za večje izgube, čeprav to prilagajanje lahko postane podobno analizi scenarijev. Eden izmed načinov je, da se premakne pričakovana izguba na podlagi zunanjih podatkov izgubam na podlagi notranjih

podatkov in se nato prilagodi na enak način tudi nepričakovana izguba. Ta postopek sicer nosi predpostavko, da je kontrola pri pričakovanih in nepričakovanih izgubah enaka, kar pa ni vedno res (Beck, 2005, str. 8).

Za ponazoritev težavnosti naloge omenjenega prilagajanja naj navedem ugotovitev pregleda svetovne bančne prakse na temu področju: čeprav večina bank priznava pomembnost prilagajanja zunanjih podatkov glede na velikost podjetja in ostalih ključnih faktorjev, doslej nobena ni razvila delujoče metodologije za tovrstno prilagajanje (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 28).

6.4 Podatki na osnovi scenarijev

Analiza scenarijev je pomemben element v ugotavljanju bančne izpostavljenosti OT. Uporaben je pri modeliranju dogodkov tipa »nizka frekvenca/velik vpliv«, predvsem v primerih, ko so notranji podatki omejeni. Prav tako omogoča prilagoditi velike škodne dogodke okoliščinam, ki so za banko specifične. Ponuja usmerjenost v prihodnost, kar se pogreša ob samostojni uporabi notranjih podatkov.

Analizo scenarijev lahko opredelimo kot napovedovanje izgub iz OT in škodnih dogodkov, ki te izgube povzročijo, s pomočjo strokovnega mnenja (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk, 2003, str. 16). Podobno kot samoocenjevanje in točkovanje tudi scenariji izkoriščajo znanje zaposlenih. Vendar se prvi dve orodji uporabljata predvsem za upravljanje z OT, scenariji pa ustvarjajo podatke, ki so uporabni neposredno v modelih za izračun zahtevanega kapitala (Beck, 2005, str. 6).

Proces analize scenarijev vključuje tri ključne faze (Anders, 2004, str. 347-353 in Beck, 2005, str. 6-7):

1. Tvorba scenarijev

Cilj te faze je določitev scenarijev, ki pokrivajo vsa poglobljena tveganja, ali pa scenarijev za primere, ko banka oceni, da so ostali viri podatkov pomanjkljivi oziroma ne odražajo zadovoljivo sprememb v notranjem in zunanjem okolju.

Za tvorbo scenarijev je potrebno najprej identificirati ključne potencialne škodne dogodke, ki vplivajo na profil OT. V ta namen se lahko uporabi standardna Baslova kategorizacija. Seznam služi kot osnova vsem organizacijskim enotam, da izberejo dogodke, ki so za njih relevantni (npr. če enota ni izpostavljena izpadom informacijskega sistema, ne bo ocenjevala tega tveganja). Izvajanje temelji na znanju, izkušnjah in pričakovanih sodelujočih. Za usmerjanje te faze v pravo smer se uporabljajo tehnike delavnic in vodenih diskusij.

2. Ocenjevanje scenarijev

Organizacijske enote v naslednji fazi ocenijo tako frekvenco škodnih dogodkov kot resnost potencialnih izgub. Ocene temeljijo na skupku informacij, kot so, na primer, pretekle izgube, ključni indikatorji tveganj, pokritje z zavarovanjem, prisotnost plana neprekinjenega poslovanja, kvaliteta relevantnih dejavnikov tveganj in kontrolnega okolja kot tudi izkušnje ostalih finančnih institucij v panogi.

Podobno kot pri tvorbi scenarijev se ocenjevanje izvaja s pomočjo vodenih diskusij ali formaliziranih vprašalnikov.

Primer: izpad informacijskega sistema

Potencialni škodni dogodek se lahko zgodi v okviru treh tipov scenarijev - za vsakega je potrebno oceniti frekvenco in velikost izgube.

	Optimističen	Pesimističen	Poguben scenarij
	pričakovana izguba	nepričakovana resna izguba	nepričakovana katastrofalna izguba
frekvenca	1-krat letno	2-3 leta	več kot 10 let
znesek izgube	10.000 EUR	100.000 EUR	1.000.000 EUR

Iz navedenih ocen je potrebno pridobiti tehtano povprečno pričakovano vrednost izgube potencialnega škodnega dogodka (v nasprotnem primeru bi imeli ocenjene vrednosti za tri škodne dogodke). V ta namen je potrebno vsakemu tipu scenarija pripisati verjetnost njegovega nastanka, ki ustreza oceni frekvence dogodka. V našem primeru bi bile te verjetnosti: za optimističen scenarij 60% verjetnost, za pesimističen 30% in za poguben 10%.

Pričakovana izguba za potencialen izpad informacijskega sistema:

$$(10.000 \text{ EUR} * 0,6) + (100.000 \text{ EUR} * 0,3) + (1.000.000 \text{ EUR} * 0,1) = \mathbf{136.000 \text{ EUR}}$$

3. Pregled kvalitete podatkov (validacija)

Ta faza je ključna za uporabo scenarijev pri ustvarjanju sintetičnih podatkov. Rezultate scenarijev kreirajo vodje organizacijskih enot, ki lahko nimajo zadosti izkušenj za ustrezno oceno redkih škodnih dogodkov, po drugi strani pa imajo interes, da znižujejo nivo tveganja, saj bo od tega odvisna alokacija kapitala njihovi enoti.

Validacijo rezultatov analize scenarijev se lahko opravlja s kombinacijo različnih možnosti (An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk, 2003, str. 24-25):

- *validacija z notranjimi podatki*: S časom lahko postane to najboljša metoda za validacijo rezultatov, vsaj za pričakovano izgubo in za srednji del distribucijske

porazdelitve. Nivo validacije se s časom izboljšuje, saj je na razpolago daljša serija podatkov.

- *preverjanje sprejemljivosti*: Sprejemljivost rezultatov scenarijev se lahko pregleduje po organizacijskih enotah na podlagi opredeljenih frekvenc škodnih dogodkov in resnosti izgub.
- *različnost vnosov (inputov)*: Če se zbirajo podatki s pomočjo različnih tehnik, na primer delavnic in vprašalnikov, se rezultati le-teh lahko primerjajo.
- *validacija z zunanjimi podatki*: Rezultati se lahko primerjajo s primerljivimi panožnimi podatki. Če institucija meni, da ima upravičeno različen profil OT, kot to kažejo zunanji podatki, mora biti sposobna to utemeljiti.
- Ustreznost rezultatov lahko skozi revizijske postopke zagotavlja *notranja ali zunanja revizija*.

Ob preudarni uporabi validacijskih tehnik bodo rezultati procesa analize scenarijev dovolj kvalitetni, da bodo ti podatki služili kot dobra osnova za nadaljnje kalkulacije kapitala oziroma kot ključen doprinos za napredne modele.

Scenarije je potrebno relativno redno ažurirati, čeprav sta čas in stroški ključni oviri. Vsekakor je to potrebno izvesti ob vsaki bistveni spremembi notranjih ali zunanjih dejavnikov poslovnega in kontrolnega okolja (Beck, 2005, str. 7).

7 ANALIZA PODATKOV IN POROČANJE

Analiziranje podatkov o izgubah iz OT je eden ključnih elementov za razumevanje tega tveganja. Temelji na vzpostavljenem dokumentiranem okviru oziroma standardih analize podatkov in na vzpostavljenem procesu analiziranja podatkov in njihovega vključevanja v poročila. Potrebno je opredeliti vrste podatkov, ki bodo predmet analize, pri čemer morajo podatki omogočati izdelavo ustreznih kvalitativnih³² in kvantitativnih informacij oziroma statistik, ki so potrebne za učinkovito seznanjanje posameznih vodstvenih ravni o profilih OT (Kralj, 2005, str. 20).

³² Primeri pomembnejših kvalitativnih informacij, ki naj bi jih vsebovala poročila (Operational Risk Regulatory Approach, 2001, str. 25):

- kritična OT, s katerimi se je institucija srečala oz. potencialna OT, s katerimi bi se lahko srečala;
- škodni dogodki in planirani korektivni ukrepi;
- učinkovitost dosedanjih akcij;
- podroben plan za obvladovanje izpostavljenosti OT;
- kakšen status imajo posamezni koraki ukrepov za obvladovanje OT.

Analizi sledi poročanje o rezultatih. To je pomemben korak in v večini primerov je to trenutek, ko uprava in ostale vodstvene ravni dobijo prvo realno predstavo o velikosti potencialne in dejanske izpostavljenosti banke in/ali posameznih organizacijskih enot OT.

Bistvo poročil je, da v celoti osvetlijo problemska področja ter hkrati motivirajo zaposlene za pravočasne korektivne akcije na perečih področjih (Sound Practices for the Management and Supervision of Operational Risk, 2003, str. 9). Sistem poročanja mora biti neodvisen, kar pomeni, da ne sme dopuščati negativnih pritiskov na poročevalce s strani neposrednih vodstvenih struktur, kar bi se odrazilo v opuščanju nekaterih poročil (Kavšek, 2005, str.72).

Tudi poročanje mora temeljiti na vzpostavljenem dokumentiranem okviru oziroma standardih poročanja in procesu poročanja. Potrebno je opredeliti ciljne prejemnike poročil (praviloma so to vse vodstvene ravni banke, mednje lahko uvrščamo tudi funkcije upravljanja s tveganji (oddelek, skupina, odbor ...) in kontrolne funkcije (npr. revizija), namen, vsebino, obliko in minimalen nabor informacij za posamezne vrste standardiziranih poročil.

Poročila za nižje vodstvene ravni vsebujejo informacije o dogodkih iz OT, ki se nanašajo na področje poslovanja, za katerega je odgovorno to vodstvo, višje vodstvo pa prejema poročila s pretežno zbirnimi informacijami o dogodkih iz OT na nivoju banke.

Primer predloga okvirne razmejitve vsebine poročanja za različne ciljne prejemnike je naveden v prilogi 7, kjer so ciljni prejemniki opredeljeni v skladu s klasično organizacijsko strukturo na sliki 9.

Proces poročanja določa infrastrukturo za sporočanje podatkov³³, odgovornost za izdelavo in distribucijo poročil, frekvenco poročanja³⁴, in postopek za poročanje o izjemnih situacijah iz IT (nestandardizirana poročila) (Kralj, 2005, str. 20).

Poročila morajo biti (Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, 2007):

- transparentna: poročila so transparentna, če vsebujejo jasne, razumljive in natančne informacije o tveganjih;
- popolna: poročila so popolna, če obravnavajo vsa pomembna tveganja ter skupaj omogočajo celovit pregled nad trenutno izpostavljenostjo tveganjem;
- koristna: poročila so koristna, če vsebujejo pomembne informacije o tveganjih;

³³ Orodje, ki omogoča distribucijo standardiziranih in nestandardiziranih poročil posameznim vodstvenim ravnam in ostalim prejemnikom poročil.

³⁴ Frekvenca je odvisna tudi od nivoja informacijske podprtosti tega področja. V najbolj informacijsko razvitih bankah bo takšno poročanje lahko bolj pogosto (po potrebi dnevno, tedensko, mesečno) kot v manj razvitih. Vendar pa le ažurni podatki omogočajo banki, da sprejema prave odločitve, zato morajo vse banke stremeti k rednemu in ažurnemu poročanju (Kavšek, 2005, str. 72).

- primerljiva in združljiva: poročila so primerljiva in združljiva, če je njihova oblika čim bolj poenotena glede na informacije, ki jih vsebujejo;
- pravočasna: poročila so pravočasna, če omogočajo sprejemanje potrebnih ukrepov v realnem času.

Skladno s to zahtevo, kot jo eksplicitno navaja tudi naša zakonodaja, dobra praksa narekuje (Sabatini, 2002):

- Poročilo naj bo grafično naravnano in z jasno vsebino. Grafike so namreč dobrodošle za usmerjanje pozornosti, z vsebinskega vidika so pomembne dodatne analize in priporočila.
- Poročila naj vključujejo analize rezultatov, objektivna dejstva, ki spremljajo primere, trende in primerjave, kjer je to možno. Primerjava je lahko tako glede na zunanje institucije kot tudi med notranjimi poslovnimi funkcijami.
- Posredovane informacije morajo izpostaviti ključne zadeve.
- Nivo podrobnosti mora biti prirejen glede na prejemnike.

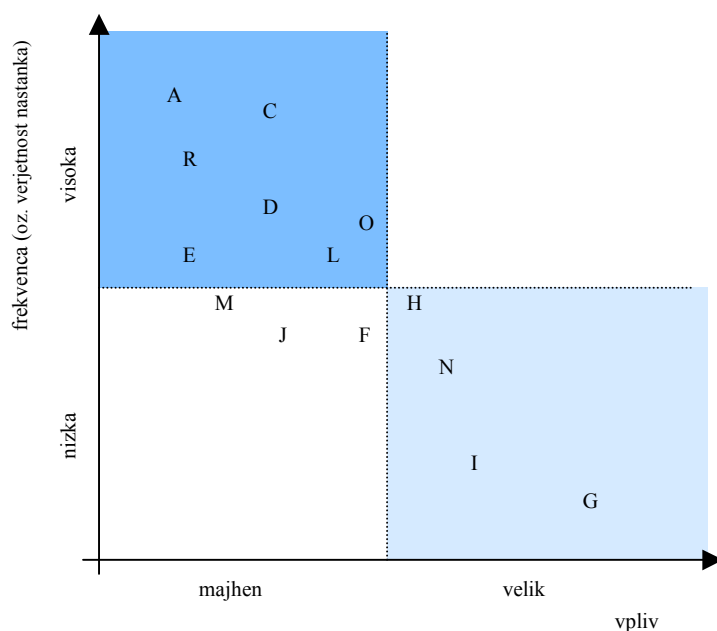
Poročila lahko segajo od najbolj enostavnih pregledov, kjer gre za enostaven zbir podatkov iz različnih virov, agregacijo in/ali prilagoditev na ustrezen način do bolj kompleksnih, ki vključujejo izračun splošnega profila OT in ustreznosti kapitala.

Primer: razsevni grafikon za prikaz profila OT

Zaradi svoje jasnosti in enostavnosti je ena najstarejših oblik analiziranja in predstavitve grafično uvrščanje škodnih dogodkov glede na velikost vpliva oz. izgube (abcisa) in frekvenco škodnega dogodka oziroma verjetnost nastanka dogodka (ordinata), s čemer dobimo poenostavljen prikaz profila operativne tveganosti, kar je kot primer prikazano na sliki 7. Viri podatkov za ustrezen postopek tovrstnega analiziranja so lahko tako notranji podatki o škodnih dogodkih kot tudi rezultati analize scenarijev in samoocenjevanja.

Če graf razdelimo v štiri kvadrante, dobimo klasično sliko s področja upravljanja z OT.

SLIKA 8: Prikaz profila operativne tveganosti³⁵



VIR: Prilagojeno po Hoffmanu, 2002, str. 276.

Primarni izziv predstavljajo škodni dogodki vrste »nizka frekvenca/velik vpliv«, saj lahko močno vplivajo na kapital finančne institucije, predstavljajo grožnjo njenemu ugledu ter v najslabšem primeru povzročijo celo njen propad. Te dogodke je težko razumeti, saj se ponavadi realizirajo kot rezultat številnih dejavnikov ter med seboj povezanih dogodkov. So predmet podrobnih analiz, planov neprekinjenega poslovanja in politike zavarovanja (Holmes, 2003, str. 24).

V naši zakonodaji so tovrstni dogodki poimenovani kot pomembni dogodki ter izpostavljenosti iz OT. Zanje se v okviru splošnih standardov upravljanja z OT zahteva poročanje organom vodenja ali nadzora ter višjemu vodstvu banke. Poročilo mora vključevati vsaj opis vrste izgube iz OT, najpomembnejše vzroke za realizacijo škodnega dogodka, obseg izgube ter seznam izvedenih ukrepov. Za slednje mora biti zagotovljeno spremljanje njihovega uresničevanja (Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, 2007).

Škodni dogodki vrste »visoka frekvenca/majhen vpliv« predstavljajo na področju upravljanja z OT sekundarni izziv za finančno institucijo. Ker takšni dogodki ne predstavljajo tipične grožnje organizaciji, se v praksi finančne institucije raje kot na samo zmanjševanje materialnih tveganj osredotočijo na zmanjševanje frekvence teh škodnih dogodkov z različnimi programi zmanjševanja stroškov. Ker so ti dogodki pogostejši, je

³⁵ Črke predstavljajo različne škodne dogodke.

zaradi pridobljenih izkušenj laže razumeti vzroke njihovega nastanka ter sprejeti ustrezne ukrepe oziroma jih predvideti že pri oblikovanju cene produkta (Holmes, 2003, str. 24).

Ostala dva kvadranta praviloma nista predmet posebne pozornosti³⁶.

Da bi zagotovili uporabnost in zanesljivost poročil, mora vodstvo redno preverjati pravočasnost, natančnost in ustreznost sistemov poročanja. Pri tem pa vodstvo lahko uporabi poročila iz zunanjih virov, kot so poročila revizorjev in nadzornikov (Sound Practices for the Management and Supervision of Operational Risk, 2003, str. 9).

Nekaj ostalih predlogov poročil je predstavljenih v Prilogi 8.

Posebna poročila od bank seveda zahteva tudi slovenski regulator s Sklepom o poročanju o kapitalu in kapitalskih zahtevah bank in hranilnic (2007), in sicer v obliki:

- **obrazca OPR** (Izračun kapitalske zahteve za operativno tveganje) in
- **obrazca OPR Bruto izgube** (Bruto izgube po poslovnih področjih in vrstah dogodkov), ki od bank neposredno zahteva ustrezno podatkovno bazo realiziranih škodnih dogodkov (priloga 9).

Podrobnejši opis in namen obrazcev presega namen te naloge.

Nenazadnje želim opozorim še na dejstvo, da se širjenje informacij o OT ne sme končati s poročanjem vodstvenim strukturam. Banka lahko z različnimi okrožnicami seznanja praktično vse zaposlene o ključnih operativnih tveganjih in morda tudi tako vpliva na njihovo zavedanje in zavzetost za to področje, kar je lahko uvod v naslednje poglavje.

8 KULTURA IN OSTALI KLJUČNI POGOJI UČINKOVITEGA OBVLADOVANJA OPERATIVNEGA TVEGANJA

Eden ključnih izzivov za vodstvo podjetja ob uveljavljanju programa za upravljanje z OT je zagotovo vgraditev ustrezne kulture, kar je tudi eden pglavitnih pogojev učinkovitega procesa zbiranja podatkov, o čemer sem že pisala v tem delu. Določa odnos zaposlenih in vodstva do OT. V kulturi, kjer je agresivno sprejemanje tveganja nagrajeno in vodstvo zaradi usmerjenosti v kratkoročne dobičke ignorira ali celo kaznuje slabe informacije (med drugim tudi o škodnih dogodkih), bo zbiranje podatkov o OT neučinkovito.

Oglejmo si praktičen primer. Referent v bančni enoti lahko z nekim nepravilnim dejanjem ali neustreznim odnosom povzroči, da komitent zapre račun pri banki. Banka je s tem utrpela določeno finančno škodo iz naslova izgube prihodkov, ki bi jih imela od tega komitenta, dogodek pa je neprijeten tudi z vidika dobrega imena banke. Čeprav gre za

tipičen škodni dogodek iz OT, ni nujno, da bo kot tak sploh zapisan v bazi podatkov. Vodja enote se lahko namreč samovoljno odloči, da o dogodku ne bo poročal v centralo zaradi bojazni pred ukrepi nadrejenih.

Doslednost in popolnost informacij pri zbiranju je pomembna v okviru vseh doslej opisanih skupin podatkov. Če strnem značilnosti posameznih:

- **Podatki o realiziranih škodnih dogodkih** odražajo preteklo dogajanje OT v banki. Praviloma jih zaposleni, ki so lahko vpleteni v sam dogodek, zbirajo ročno. Večina podatkov je o napakah zaposlenih: ali kot vzrok (npr. napačen vnos podatkov) ali kot dejavnik, ki je vplival na dogodek (npr. neustrezna kontrola), kar povzroča strah pred morebitnim kaznovanjem. To vodi v pomanjkljivo poročanje. Poleg tega je zbiranje podatkov že samo po sebi nadležna naloga, zato zaposleni o manjših izgubah niti ne poročajo, ker se jim zdijo druge zadolžitve bolj pomembne. Čeprav je razmerje med številom in velikostjo izgub in iz tega izračunana zahtevana stopnja kapitala s pomočjo npr. verjetnostne porazdelitve izgub precej kompleksno področje, je v osnovi princip enostaven: več oziroma večje izgube vodijo v višji zahtevani kapital, kar je za vodstvo neugodno. Vse to se kaže v tem, da obstajajo številne vzpodbude za prikrivanje izgub.
- **Samoocenjevanje** pomaga pri zbiranju pogleda zaposlenih na specifična tveganja. Številni strokovnjaki se strinjajo, da se rezultati tega postopka lahko s pridom uporabijo za izboljšanje kvalitete različnih modelov (Haas, 2005). Boljša je ocena na podlagi samoocenjevanja³⁷, nižji kapital je alociran tej enoti, kar zmanjšuje objektivnost pri ocenjevanju OT. Ocene so lahko osnova za opuščanje določenih produktov in storitev. Prav tako so pokazatelj kvalitete upravljanja v organizacijski enoti. Vse to lahko vodi v zavestno prikrivanje tveganj.
- **Ključni indikatorji tveganja** so nekakšen zgodnji opozorilni sistem, ki preprečuje izgube s pravočasnimi ukrepi. Ustrezni indikatorji lahko pokažejo, da določena tveganja niso bila ustrezno upravljana. Zato se lahko takšen indikator namerno izpušča iz preučevanja.
- **Analize scenarijev** izpostavljajo potencialno tvegane situacije, ki se še niso dogodile. Definiranje in ovrednotenje ustreznega scenarija lahko prikaže posamezne strateške odločitve kot neugodne, zato se lahko scenariji z neželenim izplenom izpustijo. Pripis nizke verjetnosti in majhne izgube določenim scenarijem znižuje zahtevo kapitala.

³⁶ Dogodki tipa »nizka frekvenca/majhen vpliv« za obravnavo niso pomembni, dogodki »visoka frekvenca/velik vpliv« pa nerelevantni, saj bi njihov obstoj praktično ogrozil banko v tolikšni meri, da ne bi mogla več poslovati.

³⁷ Kar pomeni nižji nivo izpostavljenosti OT.

Obstaja torej neka splošna tendenca k prikrivanju podatkov o OT. Zato je pomembno, da ko zahtevamo od zaposlenih, naj delijo svoje napake, ob temu ustvarimo pozitivno okolje, ki jih bo vzpodbujalo, da govorijo odkrito o zaskrbljujočih tveganjih in odkrivajo izgube in operativne napake za dobrobit banke.

Pozitivno okolje lahko opredelimo kot kulturo upravljanja z OT.

Kljub temu da se bo morda poglavje o kulturi komu zdelo samo naštevanje nečesa, kar je vsem že znano in očitno, pa izvajanje tega ni ravno lahka naloga. V eni od raziskav so kot največjo oviro pri upravljanju z OT, poleg težav z zbiranjem podatkov, vprašani navedli prav težave, povezane s kulturo, med drugim tudi slabo zavedanje med zaposlenimi (Operational Risk Management in the Financial Service Industry, 2004).

8.1 Značilnosti kulture

Basel II je sicer osnoval splošno definicijo te kulture, in sicer »kot kombinacijo vrednot zaposlenih in vrednot banke, odnosov, pristojnosti in vedenja, in ki določa obvezo banke do upravljanja in načina upravljanja z operativnim tveganjem« (Sound Practices for the Management and Supervision of Operational Risk, 2003, str. 1). Sama pa sem želela poiskati odgovor na vprašanje, kakšne so konkretne značilnosti ustrezne kulture upravljanja s tveganji, ki so lahko osnova za določanje priporočil in ukrepov pri doseganju prej omenjenega pozitivnega okolja.

Literatura za to področje je skopa, verjetno tudi zato, ker je kultura širok pojem in različnim ljudem lahko predstavlja različne reči. In povsem očitne. Eden redkih avtorjev je poskušal opredeliti značilnosti zdrave kulture upravljanja z OT z vidika njenih dejavnikov (Holmquist, 2007). Seznam še zdaleč ni popoln in se lahko sčasoma spreminja:

- **Zavedanje:** zaposleni se morajo zavedati dejanskih groženj, tveganj, kontrol in razlogov zanje ter najti način, kako se vključiti v to celoto.
- **Komunikacija:** močna kultura upravljanja s tveganji deli informacije, začnši z vizijo in strategijo pa vse do konkretnih težav.
- **Odzivnost:** sposobnost odgovoriti hitro in učinkovito na spremembe, nepričakovane dogodke, neuspehe in celo negotovosti.
- **Stalno izpopolnjevanje:** močna kultura upravljanja s tveganji stalno išče načine za izboljšave in ne čaka na škodne dogodke za spodbujanje k spremembam.
- **Lastništvo:** pomembna je pripravljenost, da zaposleni prevzamejo lastništvo nad procesi, tveganji in škodnimi dogodki.
- **Preglednost:** močna kultura upravljanja s tveganji vidi operativne izzive, nepričakovane dogodke in celo škodne dogodke kot možnosti za izboljšave, ne kot neprijetnosti in motnje poslovanja.

- **Odgovornost:** zaposleni prevzemajo odgovornost za procese in so odgovorni ne samo za škodne dogodke, ampak tudi proaktivno iščejo načine za izboljšanje procesov.
- **Samostojnost:** ustvarja okolje, kjer zaposleni ne čakajo na aktivnosti drugega. V takšnem okolju nikakršna goljufija ni sprejemljiva in njihovo odkrivanje ni odvisno zgolj od kontrol.
- **Integritetnost:** upravljanje z OT ni samo alineja na seznamu oziroma ni samo korak v procesu. Je del sistema, v katerem zaposleni razumejo njegovo vrednost in ga vidijo kot boljši način izvajanja nalog.

8.2 Izzivi pri vzpostavitvi kulture v praksi

Vsak zaposleni je motiviran različno, je v različnem življenjskem obdobju, je različno pripaden podjetju in mu prinaša edinstven sklop vrednot. Določen odstotek zaposlenih si išče drugo službo. Nekateri sovražijo svoje delo ali vodje ali sodelavce in nimajo interesa za pospeševanje boljšega poslovanja. Druga skupina si neizmerno prizadeva, da ne bi bila odpuščena kljub svojemu slabemu izvajanju nalog, drugi usmerjajo vso energijo v napredovanje za vsako ceno. Obstajajo seveda tudi takšni, ki so zaskrbljeni glede OT in aktivno sodelujejo pri izvajanju strategij za njihovo zmanjševanje.

Ta različnost ustvarja določene okoliščine pri kreiranju zdrave kulture tveganj (Holmquist, 2007):

- Dejstvo je, da veliko ljudi opravlja naloge na svoj način. Ponavadi nobeni standardi, procedure in protokoli tega ne spremenijo.
- Za veliko ljudi je tveganje, da bodo videti slabi delavci ali bodo prišli v težave, veliko bolj pomembno kot dejstvo, da bo podjetje izgubilo denar, ali da obstaja priložnost za izboljšave.
- Usmeritev izključno na dobiček ne dopušča zdrave kulture tveganj.
- Graja ogroža sodelovanje.
- Dejstvo je, da je za večino ljudi bolj udobno odzivati se na dogodke kot planirati njihovo naključje. Kakorkoli, učinkovito upravljanje z OT ne more biti samo reaktivno.
- Preveč ljudi meni, da je upravljanje OT intuitivno, in bolj kot je izkušen vodja, bolj je to mnenje prevladujoče.
- Napačen smisel za brezskrbnost glede OT je posledica dejstva, da stvari ne gredo narobe prav pogosto. »Deluje danes in bo delovalo tudi v prihodnje.«
- Lahko obstaja mnenje, da gre pri upravljanju z OT zgolj za ustreznost in učinkovitost kontrol³⁸.

³⁸ Čeprav velja poudariti, da je učinkovita notranja kontrola nedvomno del trdne kulture upravljanja z OT (Gup, 2005, str. 14).

- Dejstvo je, da si ne glede na postavljeno raven sprejemljivosti OT v okviru institucije vsak posameznik ustvari svoje meje.
- Vsak človek je edinstven, kar po eni strani predstavlja največji izziv, po drugi pa največje premoženje.

Ob človeškem faktorju so še druge karakteristike, ki jih je vredno izkoristiti kot priložnosti pri oblikovanju strategije za obvladovanje OT (Holmquist, 2007a):

- Kulturne spremembe se lahko zgodijo le na dolgi rok. Za temeljito spremembo je potreben čas, postati mora del norm, kar pomeni, da jo sprejme kritično število zaposlenih.
- Kulturo ne moremo opredeliti z besedami kot npr. dobra, slaba, prava, napačna. Osredotočiti se moramo na relativno trdnost kulture, kar omogoča več vidikov in nivojev njene učinkovitosti.
- Negotovost, ki izhaja iz pomanjkanja informacij, uničuje kulturo.
- Ustrezna kultura je lahko zgrajena le na zaupanju in medsebojnem spoštovanju. Okolje s strahom in zastraševanjem, zmerjanjem in zasmehovanjem ter nepoštenostjo ne more biti temelj za graditev trdne kulture.

8.3 Ukrepi za vzpostavitev ustrezne kulture

Ugotavljamo lahko, da kulture ne bo možno vzpostaviti zgolj s pravili, standardi ali regulatornimi zahtevami. Spremeni ali okrepi se lahko postopoma, kot posledica sklopov odločitev.

Poleg aktivnosti, ki izhajajo iz uveljavljanja ustreznega okvira upravljanja OT in že same po sebi povečujejo oz. krepijo kulturo (npr. v tej nalogi navedeni postopek zbiranja podatkov in samoocenjevalni postopek krepite zavedanje o OT, ustrezno poročanje omogoča učenje na podlagi napak drugih), izkušnje kažejo na sklop konkretnih ukrepov, ki pripomorejo pri prizadevanju za doseganje ustrezne kulture.

Kot prvo naj izpostavim ukrepe v povezavi s **komunikacijo**.

Na kulturo (v negativnem smislu) vplivajo v večji meri neizrečene reči kot izrečene. To še posebej drži, ko so poslovni cilji nejasni, etične kršitve in kršitve politike niso ustrezno obravnavane ali zaposlenim ni potrebno odgovarjati za njihove akcije. Komunikacija in kultura sta močno povezani. Aktivna komunikacija je kritična za ustvarjanje močne kulture (Holmquist, 2007).

Glede na to lahko pomaga (Haubenstock, 2004, str. 457):

- zagotavljanje rednega izobraževalnega programa: organizacija tovrstnih internih predstavitev in seminarjev ter podpiranje udeleževanja zaposlenih na (domaćih in mednarodnih³⁹) seminarjih in delavnicah o OT;
- posredovanje informacij zaposlenim prek sistemov internega komuniciranja (interna glasila, okrožnice ipd.) in dostopnost vsega relevantnega gradiva na medmrežju (poleg vseh strategij, politik, navodil in pravilnikov tudi informacije o večjih projektih, napakah in škodnih dogodkih z namenom učenja na izkušnjah);
- organiziranje rednih konferenc za vse udeležence, vključene v posamezne procese upravljanja OT, npr. zbiranje podatkov, o katerih je možno izmenjati mnenja, zastaviti vprašanja, pridobiti informacije o novih procesih in tehnologijah, pridobiti izkušnje.

Za uspešnost komunikacije je pomembno zagotoviti **skupen oziroma enoten jezik za področje OT**, ki zagotavlja, da zaposleni na enak način govorijo o OT. Sicer se lahko zgodi, da se na škodo izvajanja osnovnih odgovornosti porabi preveč časa za reševanje tovrstnih nesporazumov.

Konkretni predlog formiranja takšnega jezika vključuje (Espersen, 2007):

- razvoj jezika, ki je razumljiv za vse,
- jasna in enostavna predstavitev ključnih pojmov,
- uporaba primerov iz resničnega sveta,
- oblikovanje besednjaka, prilagojenega področju OT.

Poleg komunikacije in skupnega jezika obstajajo še drugi dejavniki za ustvarjanje pozitivnega okolja (Holmquist, 2007b in Haubenstock, 2004, str. 461):

- Spodbujanje ustvarjalnosti in inovacij: potrebno je prisluhniti idejam za izboljšave in najboljše tudi ustrezno nagraditi.
- Spoznavanje zaposlenih: naj ne bo priložnost za spoznavanje zaposlenih samo v primeru neuspešnih dejanj in dogodkov. Potrebno je najti način za spoznavanje predvsem v primerih, ko se naloge izpeljejo dobro.
- Izogibanje iskanju krivca: v primeru škodnih dogodkov je bistveno vprašanje »Kaj bomo storili?« in ne »Kdo je kriv?«.
- Nenamerni škodni dogodki in napake naj ne bodo povod za disciplinske ukrepe, temveč sredstvo za nadaljnje akcije, ki bodo preprečile tovrstne dogodke v bodoče.
- Anonimnost poročanja: naj se pri poročanju o škodnih dogodkih izloči vsa imena iz opisa dogodkov, poročil in diskusij.
- Naj ne bo upravljanje z OT namenjeno samo izvršilnemu vodstvu in izračunavanju zahtevanega kapitala, temveč naj zagotavlja vrednost tudi poslovnim področjem pri izboljšavah obvladovanja tveganja.

³⁹ Npr. za Slovenijo so mednarodni seminarji in delavnice zanimivi glede na to, da se lahko trenutno učimo prav na podlagi tujih praktičnih izkušenj.

- Naj bodo posamezni postopki upravljanja z OT enostavni, naj bodo zahteve pri zbiranju podatkov takšne, da bo poročanje o dogodkih hitro in enostavno, za kar naj se poskrbi z ustrezno tehnološko podporo.

8.4 Vodstvo in organizacijska struktura

Bistven pogoj za uspeh vsega napisanega je zavzemanje najvišjega vodstva za to področje. Vodstvo mora vzpodbuditi kulturno spremembo znotraj banke, kjer bo upravljanje z OT doseglo najvišjo prepoznavnost in podporo.

Zavedanje vodstva o OT je tudi temeljna zahteva baselskih dokumentov, ki je sistemsko vgrajena v razvoj in okvir upravljanja z njim. Zelo težko bi v svetu našli banko, ki bi brez izrazite podpore svoje uprave in njenega višjega managementa uspešno implementirala tako radikalne spremembe v pristopu z upravljanjem banke. Predvsem uprava banke in višji management sta torej tista, ki ju je treba prepričati, da bo ustrezen okvir upravljanja z OT prinesel dodano vrednost, zmanjšal izgube, učinkovito nadzoroval OT pri njegovih izvorih ter hkrati izpolnil zahteve regulatorjev. Če bodo nižji nivoji banke spoznali, da vodstvo banke z vseh vidikov podpira razvoj, bo njihov odziv v smeri učinkovitega vključevanja pozitiven.

Podpora vodstva mora biti tako finančna kot tudi aktivna. Finančna v smislu odobravanja zadostnih sredstev za razvoj ustreznih orodij in začetka zbiranja osnovnih podatkov o OT, aktivna pa v smislu vključevanja upravljanja z OT v vodstveno kulturo banke na vseh nivojih. Slednje se lahko doseže z izpostavitvijo obravnavane problematike v letnih načrtih kot enem ključnih področij, na katero se mora banka usmeriti v prihodnjih letih (Kennett, 2001, str. 68).

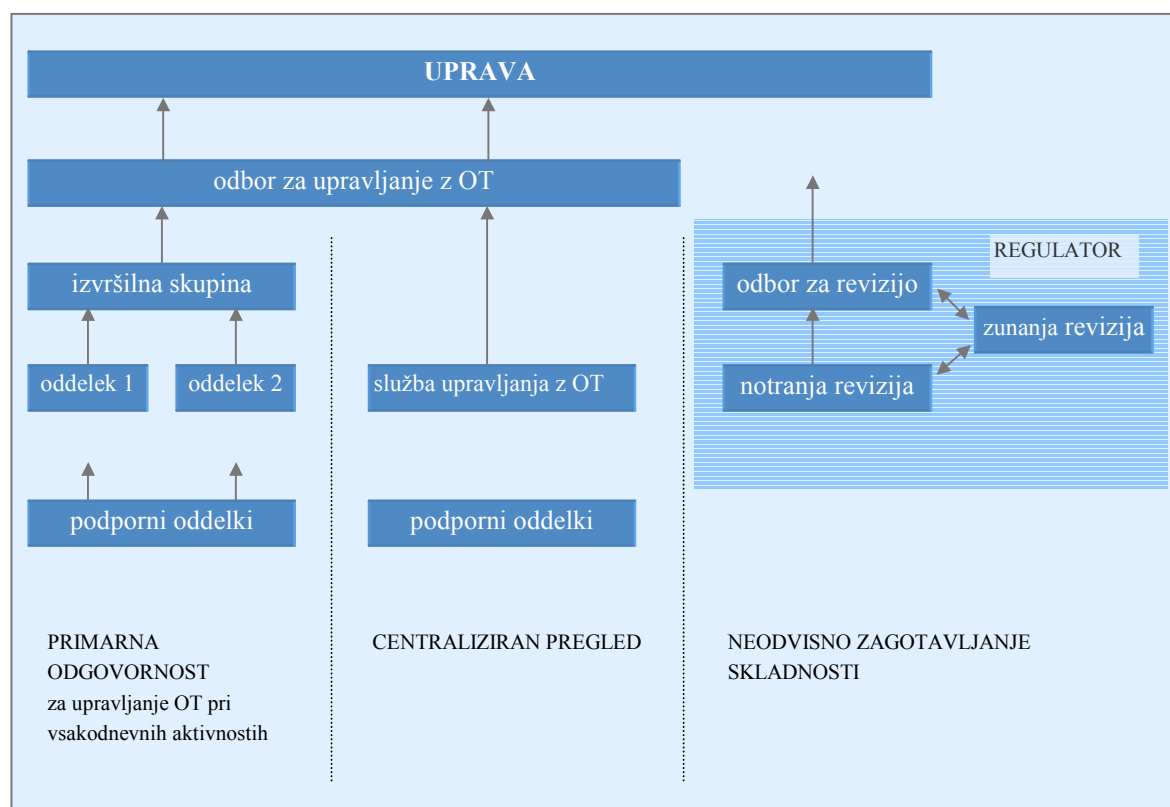
8.4.1 Organizacijska struktura

Naslednji pogoj za ustvarjanje pravega okolja za obvladovanje OT so tudi jasno opredeljene odgovornosti in pristojnosti za izvajanje nalog s področja OT. V ta namen je potrebno oblikovati ustrezno organizacijsko strukturo, kar je naloga vodstva, vključno z njeno neomejeno podporo takšni strukturi.

Ob tem je pomembno zagotoviti, da se oblikuje profesionalna in neodvisna funkcija za upravljanje z OT, ki bo odgovorna za zagotavljanje in nadzor nad izvajanjem nalog upravljanja z OT. Pomanjkanje neodvisnosti bi pomenilo, da funkcija upravljanja z OT postane neposredno povezana z lastništvom določenega OT, kar bi zmanjšalo sposobnost strokovne neodvisne presoje, nepristranskost priporočil in učinkovito implementacijo okvira upravljanja z OT (Observed range of practice in key elements of Advanced Measurement Approaches (AMA), 2006, str. 6).

Slika 9 predstavlja primer klasične organizacijske ureditve, ki izhaja iz treh različnih vlog pri upravljanju z OT: neposredne odgovornosti pri vsakodnevnom poslovanju, centraliziranega pregleda in neodvisnega zagotavljanja skladnosti. Puščice označujejo smeri poročanja.

SLIKA 9: Vgraditev področja upravljanja z OT v organizacijsko strukturo banke



VIR: Basel II: A Closer Look, 2005, str. 23.

Vloga funkcije oziroma službe upravljanja z OT je v vzpostavitvi specifičnih standardov in politik, v sodelovanju in koordinaciji, v integraciji in agregaciji profila OT. Bolj konkretno med drugim to zahteva pripravo enotne definicije OT, razvoj in pospeševanje implementacije orodij za upravljanje z OT, kot na primer bazo podatkov o škodnih dogodkih in postopkov samoocenjevanj OT, poročanje izvršilnemu vodstvu in upravi, razvoj modelov, na primer za izračun kapitalske zahteve (Haubenstock, 2001, str. 26).

Kot dopolnilo službi upravljanja z OT se pogosto v bankah oblikuje odbor za OT, sestavljen iz članov najvišjega vodstva, čigar naloga je razumevanje profila OT, zagotavljanje resursov in ustrezna alokacija, potrjevanje politike, vključno z alokacijo kapitala (Haubenstock, 2001, str. 26).

Nižje ravni vodstva so odgovorne za upravljanje OT pri vsakodnevnih aktivnostih, saj so prav oni v okviru poslovnih področij tisti, ki so neposredno v stiku s strankami, ponujajo produkte, vodijo večino zaposlenih, upravljajo procese in tehnologijo in se ukvarjajo z ostalimi zunanjimi dejavniki. Zaposleni v oddelkih, kot so upravljanje s človeškimi viri, informacijska tehnologija, finance in računovodstvo, pravne zadeve, razvijajo specifično politiko in procedure, nadzorujejo nastajanje OT in svetujejo organizaciji s svojimi specifičnimi znanji glede teh tveganj (Haubenstock, 2001, str. 26).

9 SLOVENSKA BANČNA PRAKSA

Doslej sem se v magistrskem delu bolj ali manj opirala na izkušnje tuje bančne prakse. To pa ne pomeni, da slovenske banke na temu področju doslej niso storile ničesar; če ne drugega, jih k temu sili Zakon o bančništvu, ki je stopil v veljavo 1. januarja 2007. V kakšni fazi realizacije zahtev zakona so, bom predstavila v nadaljevanju, kot prvo pa na kratko izpostavljam bolj ali manj »domače« odmevnejše škodne primere iz naslova OT v zadnjem obdobju.

9.1 Primeri škodnih dogodkov

- Leta 2003 je **Nova ljubljanska banka** zaradi slabega vodenja projekta »SIGMA« ob migraciji starih prilivno/odlivnih računov v nove transakcijske račune in ob hkratnem uvajanju novega informacijskega sistema padla v hudi krizo, ki se je pri komitentih odražala v nepravilnih stanjih na transakcijskih računih, napačnih izpiskih, onemogočenem kartično-bankomatskem poslovanju, omejenem poslovanju preko interneta in še bi lahko naštevali. Banka je krizo občutila s 400.000 EUR nerazporejenih sredstev zaradi neustreznega avtomatskega razporejanja sredstev, kot izjemno povečanje nedovoljenih negativnih stanj na transakcijskih računih zaradi neustreznih notranjih kontrol in nedelovanja opominjevalnih postopkov ter tudi kot izjemno povečanje reklamacij in pritožb bančnih komitentov (Tomsits, 2005, str. 1).

Poleg tega naj bi po nekaterih ocenah 3% komitentov pri banki zaprlo račun, dodatnih 4% pa pričelo uporabljati račune še pri drugih bankah. Zaradi zmanjšanja ugleda banke so bili manjši prihodki od planiranih, obenem so se povečali stroški zaradi stabilizacije razmer na področju informacijskih sistemov banke in marketinških akcij za ohranjanje ugleda. Na podlagi prejetih poročil o odškodninskih zahtevkih občanov zaradi domnevnih nepravilnosti pri poslovanju z osebnimi računi naj bi bila banka po njenih ocenah izpostavljena OT v višini 80.000 EUR. Zaradi nastalih negativnih stanj na osebnih računih in stanja izvršb je morala banka oblikovati dodatne rezervacije v višini 650.000 EUR, še dodatnih 2,7 mio EUR pa zaradi napačnega obračunavanja negativnih obresti (Tomsits, 2005, str. 50-70).

- V **Banki Celje** so poleti 2006 ob spremembi sistema kontrol po naključju odkrili notranjo goljufijo ene izmed svojih uslužbenk, ki si je s pomočjo prekoračitve pooblastil in ponarejanja podpisov na račun svojega podjetja nakazala vrsto manjših vsot v skupni vrednosti 474.000 EUR (Kos, 2006, str 2).
- Vzorčen primer škodnega dogodka je tudi odmevni rop sefov **SKB banke** v Ljubljani, kjer so v noči na 1. november 2005 neznani storilci ukradli vsebino 420 sefov (Tomažič, 2006). Ne glede na to, da banka po lastnih zagotovilih razen nekaj

odstotnega povečanja operativnih stroškov zaradi odprave posledic rop ni utrpela pomembnejših neposrednih posledic (vso škodo oškodovancem naj bi pokrile zavarovalnice), ki bi vplivale na finančni izkaz (Poslovno leto 2006 - zaključeno z dobičkom, 2007), so zagotovo nastali določeni oportunitetni stroški kot posledica omajanega ugleda banke in zmanjšanega zaupanja v varnost poslovanja banke.

- V naši neposredni bližini je tretjo največjo banko na Hrvaškem **Riječko banko** leta 2002 doletela finančna goljufija, s katero je vodja deviznega trgovanja Edo Nodilo banki z zgrešenimi špekulacijami v obdobju od 1998 do 2002 povzročil izgubo v višini okoli 90 milijonov dolarjev. Špekulant je redno prekoračeval dnevne limite, posle pa je sklepal kljub neugodnim tečajnim razlikam. Izgube je prikrival z uničevanjem dokumentov in s knjiženjem navideznih poslov (Hočevar, 2002, str. 54). Avstrijska **Hypo Alpe-Adria Bank** je zaradi špekulativnih poslov v trgovanju z valutami po nekaterih ocenah leta 2004 izgubila 328 milijonov evrov (Kos, 2006, str 3).

Navedene primere navajam kot opozorilo, da tudi naše banke niso imune na tovrstna tveganja, tudi z vidika pomembnejših škodnih dogodkov, ki lahko bistveno ogrozijo posamezne dele, če ne celotno poslovanje banke, in kot odgovor tistim, ki se morda sprašujejo o smiselnosti regulatornih zahtev na temu področju.

9.2 Upravljanje z operativnim tveganjem

Banke so po stanju 30.6.2007 pripravile simulacijo ocen izračuna kapitalskih zahtev v skladu z novo kapitalsko ureditvijo. Na podlagi simulacije bi se kapitalske zahteve pri večini bank povečale, povprečno za 6,5%. Povečanje izhaja predvsem iz uvedbe kapitalskih zahtev za OT, ki bodo na podlagi simulacij predstavljale 7% vseh kapitalskih zahtev. Najbolj naj bi se povečale pri majhnih bankah, za 9,3%, najmanj pri bankah v večinski tuji lasti, za 3% (Poročilo o finančni stabilnosti, 2008, str. 120). Ugoden rezultat bank v večinski tuji lasti morda govori tudi v prid uporabi naprednih pristopov, saj je edina banka, ki ji je nadzornik Banka Slovenije (v nadaljevanju: BS) odobrila uporabo naprednega pristopa za izračun kapitalske zahteve za OT in ga že uporablja z letom 2008, prav banka v večinski tuji lasti – SKB d.d. (Letno poročilo SKB za leto 2007, str. 35). Vprašanje je, v kakšni meri bodo takšni podatki vzpodbuda domačim bankam, da čim prej pristopijo k naprednejšim sistemom. BS je namreč v svojem poročilu povzela, da bo večina bank pri izračunu kapitalske zahteve za OT na začetku uporabila enostaven pristop, vendar da nameravajo v letih 2010–2012 večinoma preiti na standardiziran pristop. Konkretno z letom 2008 naj bi standardiziran pristop uporabljalo pet bank, napredni pristop (AMA) pa ena banka (Poročilo o finančni stabilnosti, 2008, str. 120).

Ključno vlogo pri temu, kako hitro bodo banke napredovale v svojih prizadevanjih za izpolnjevanje kriterijev naprednejših pristopov, imajo predvsem uprave banke. Že leta

2003 je bilo na podlagi ankete, ki jo je izvedla BS v sodelovanju z Združenjem bank Slovenije razvidno, da so uprave naših bank sicer dobro seznanjene z novimi kapitalnimi standardi in se zavedajo pomena upravljanja s tveganji, vendar se vse ustavi, ko je potrebno v ta namen zagotoviti sredstva in zaposliti ustrezno usposobljen kader. Banke se zavedajo, da bodo v to morale vložiti veliko časa in denarja, ob tem pa niso prepričane, da bodo koristi vzpostavljenega sistema večje od stroškov, ki bodo pri tem nastali (Slak, 2005, 125). Bolj očitno je, da se izplača usmeriti v izpolnjevanje naprednejših kriterijev pri kreditnem tveganju, kar izkazujejo tudi rezultati t. i. študije QIS5⁴⁰, kjer uporaba naprednih pristopov predstavlja pomembnejše prihranke v smislu manjših kapitalnih zahtev, medtem ko v primeru kapitalnih zahtev za OT rezultati v ta namen niso ravno prepričujoči (Results of the fifth quantitative impact study (QIS5), 2006).

V okviru upravljanja z OT so se doslej banke zanašale predvsem na mehanizme internih kontrol po posameznih poslovnih področjih in na funkcijo notranje revizije, kar vnaprej sicer ne ostaja nepomembno, a je potrebno to nadgraditi s specifičnimi strukturami in procesi, ki bodo namenjeni celovitemu upravljanju OT. Kako so posamezne banke pristopile k temu s podatkovnega vidika, je na podlagi njihovih letnih poročil za leto 2007 zbrano in podrobno predstavljeno v prilogi 10⁴¹. Povzetku namenjam naslednje poglavje.

9.3 Upravljanje s podatki o operativnem tveganju

Na podlagi omenjenega pregleda letnih poročil v nadaljevanju izpostavljam nekaj bistvenih ugotovitev o upravljanju s podatki o OT.

Praviloma so vse slovenske banke k procesu celovitega upravljanja z OT poleg načrtov neprekinjenega poslovanja in okrevanja po katastrofi pristopile prav z zbiranjem podatkov o škodnih dogodkih. Vse banke že kar nekaj časa uporabljajo aplikacije za vnos škodnih dogodkov. V podatkovno bazo praviloma vključujejo zgolj škodne dogodke, ki vplivajo na poslovni izid, kar po mojem mnenju predstavlja pomembno pomanjkljivost zbiranja podatkov. Tako iz nabora izpadejo številni škodni dogodki, ki na poslovni izid nimajo neposrednega vpliva in s tem zmanjšujejo vrednost pridobljenih informacij o dejanski in celoviti izpostavljenosti OT (npr. izpadi informacijskega sistema, ki nimajo neposrednega vpliva na poslovni izid, kraja informacij, odhodi komitentov zaradi slabega odnosa bančnih delavcev ipd.).

⁴⁰ Baselski komite je s t. i. kvantitativnimi študijami učinkov (angl. *Quantitative Impact Study - QIS*) poskušal raziskati vpliv različnih metodoloških rešitev za izračun kapitalnih zahtev za kreditno in operativno tveganje na kapitalno ustreznost bank. Od prvega posvetovalnega dokumenta za Basel II, ki ga je izdal junija 1999, pa do danes je izvedel že pet študij, zadnja, torej peta je bila zaključena leta 2006.

⁴¹ Med pregledanimi so letna poročila naslednji bank: Abanka Vipava, Banka Celje, Banka Koper, Gorenjska Banka, NLB, Nova KBM, SKB in UniCredit Banka Slovenije.

Zanimivo je, da v nasprotju s predlagano tujo prakso, ki omenja vrednosti 10.000 evrov, naše banke zajemajo podatke o škodnih dogodkih z izrazito nizkim pragom zbiranja podatkov, tudi manj kot 100 evrov, kar kaže na problem premajhnega vzorca škodnih dogodkov, če bi se omenjeni prag zviševal s predlaganim zneskom tuje prakse. Odgovorni za OT v bankah se morajo ob temu zavedati, da zanašanje na rezultate analiz in modeliranje na osnovi tovrstnih dogodkov majhnih vrednosti lahko vodi v preusmerjanje pozornosti z resnih in velikih potencialnih nevarnosti in napačnih zaključkov glede vzrokov škodnih dogodkov, ki so pri velikih praviloma bolj kompleksni.

V nalogi je bila omenjena težava relevantnosti zbranih podatkov, saj so pri zaposlenih številni motivi za prikrivanje izgub. Zato za izvirno smatram rešitev, ki jo je uvedla Abanka Vipa in sicer, da loči pri zbiranju dve aplikaciji: intranetno aplikacijo za prijavo škodnih dogodkov in aplikacijo za popis le-teh. Prva je namenjena vsem zaposlenim v banki in omogoča anonimno prijavo škodnih dogodkov, v drugi pa poročevalci popisujejo škodne dogodke. Ena je torej namenjena anonimnemu zbiranju škodnih dogodkov, druga pa spremljanju škodnih dogodkov.

Zbrani podatki o škodnih dogodkih največje slovenske banke NLB kažejo, da največ škodnih dogodkov (47%) spada v kategorijo strank, produktov in poslovne prakse. Sledijo škodni dogodki (36%), ki so nastali zaradi izvedbe, prenosa in upravljanja procesov. Manjšina je škodnih dogodkov, ki so nastali kot posledica zunanega kriminala, in sicer zaradi skimminga oz. zlorab bančnih kartic, postopkov zaposlenih in varstva pri delu ter napak pri sistemih. Na podlagi teh podatkov bi tveganja posameznih kategorij OT rangirali povsem v nasprotju s svetovno bančno prakso in raziskavami (glej opombo 27), kjer je izpad informacijskih sistemov ocenjen kot najbolj tvegana kategorija OT. Seveda je možno, da v izbranem obdobju banka ni utrpela bistvenih izgub iz tega naslova, obstaja pa tudi možnost neustreznega zajemanja škodnih dogodkov (zajemanje zgolj tistih škodnih dogodkov, ki vplivajo na poslovni izid).

Zaradi pomanjkanja notranjih podatkov predvsem o škodnih dogodkih tipa »nizka frekvenca/velika izguba« bodo ob uveljavljanju naprednejših pristopov pomembne tudi ostale vrste podatkov o OT. Zaenkrat je zbiranje le-teh precej omejeno, kar je po eni strani razumljivo zaradi uporabe enostavnejših pristopov. Tako nekatere banke poleg notranjih podatkov o realiziranih škodnih dogodkih uporabljajo ocene na podlagi postopkov samoocenjevanj. Ključne indikatorje tveganj poleg SKB, ki uporablja napredni pristop, omenja še Banka Celje, in sicer hitro rast, gibanje delovne sile in frekvenco zaustavitvev sistemov. UniCredit Banka Slovenije, kot edina uporablja prednosti analiz scenarijev. Zunanji podatki so očitno zaenkrat pri vseh bankah neizkoriščen vir informacij, saj nobena (niti v tuji lasti) ne omenja katero od v tej nalogi omenjenih oblik zunanjih podatkov.

Ob teh ugotovitvah je morda zanimivo vprašanje, kakšne so možnosti osnovanja slovenskega konzorcija bank, ki bi za potrebe naprednih pristopov za OT začele zbirati podatke o lastnih škodnih dogodkih iz OT v skupni bazi podatkov. Da bi do tega prišlo

kmalu, je verjetno nerealno pričakovati, saj kot prvo trenutno za to niti ni ustreznih pogojev. Za začetek tovrstnega razmišljanja je namreč potrebna namera določenega števila bank, da v okviru implementacije Basla II razvijejo napredni pristop za izračun kapitalske zahteve za OT. Kot drugo pa izkušnje kažejo, da so začetki takšnih skupnih projektov ponavadi dokaj težavni, poleg tega je treba vedno počakati najšibkejši člen. Večja je možnost, da se bo posamezna banka raje odločala za vstop v kakšnega izmed že delujočih tujih konzorcijev bank. Vendar tudi če se na prvi pogled zdi, da je lažje izvesti vstop v skupno bazo podatkov tujega konzorcija bank kot na novo osnovati domači konzorcij bank, po izkušnjah nekaterih tujih bank to ni čisto tako. Vstop v tuj konzorcij bank je dokaj težak, saj se mora banka najprej prilagoditi zahtevam skupne baze podatkov, poleg tega pa segajo interesi ostalih članic večinoma do okvira njim primerljivih bank (Rotovnik, 2004b, str. 63). Zato tudi na tem področju ponovno vidim prednosti za banke s tujimi lastniki.

9.4 Praktični primer aplikacije za zbiranje podatkov o škodnih dogodkih

V nadaljevanju predstavljam praktičen primer zbiranja podatkov v eni izmed slovenskih bank⁴², poimenujmo jo kar Banka X.

9.4.1 Zajem škodnih dogodkov

Kot večina slovenskih bank je tudi Banka X škodni dogodek opredelila kot dogodek, ki ima za posledico finančno izgubo. Ugotavljanje in kontrola se opravlja s pomočjo ločenih kontov odhodkov, kamor se izguba beleži. Zbiranje podatkov o škodnih dogodkih oziroma bruto izgubi poteka s pomočjo intranetne povezave v okolju Lotus Notes v aplikaciji »Operativna tveganja«. Podatki se v aplikacijo zajemajo iz dveh osnovnih virov:

- škodni dogodki, ki so posledica knjižb organizacijske enote banke na izbrane konte drugih odhodkov in organizacijske enote, zavezujejo k poročanju;
- škodni dogodki, ki predstavljajo odškodninski zahtevek banke do zavarovalnice.

Oseba, ki vnaša podatke o škodnem dogodku na dan knjiženja oz. najkasneje do konca meseca, v katerem je škodni dogodek nastal, vnese v aplikacijo naslednje podatke:

- organizacijsko enoto lastnika škodnega dogodka,
- datum nastanka škodnega dogodka,
- vrsto dogodka (iz šifranta »Seznam vseh možnih škodnih dogodkov po Baslu II« izbere ustrezno vrsto),
- znesek bruto izgube v EUR (znesek knjižbe na konte izrednih odhodkov),

- opis dogodka (podatek, ki mora vsebovati čim podrobnejši opis dogodka, saj se na podlagi tega preverja pravilnost izbrane vrste dogodka),
- konto in datum knjiženja.

Osnovni ekranski sliki aplikacije sta prikazani v prilogi 11.

9.4.2 Izdelava poročil

Aplikacija 5. delovni dan v mesecu samodejno kreira poročila in jih razpošlje direktorjem posameznih organizacijskih enot. Poročilo zajema škodne dogodke, kjer je bilo kot lastnik dogodka navedeno stroškovno mesto v njegovi pristojnosti. Banka želi s tovrstnimi poročili poleg informiranja uvajati med svoje zaposlene tudi kulturo upravljanja z OT.

Obenem je dolžnost poročevalcev škodnih dogodkov, da do 5. v mesecu iz aplikacije izpišejo poročilo o prometu na kontih za svoje vnose in ga podpisanega pošljejo v sektor računovodstva. Tu se opravi ustrezna kontrola podatkov. Če so pravilni, vnos potrdijo, v nasprotnem primeru mora poročevalec podatke popraviti.

Na osnovi podatkov iz aplikacije se v okviru centralne funkcije upravnika aplikacije in vseh podatkov lahko pripravi poročilo za BS (obrazec OPR Bruto izgube, glej prilogo 9). Ta je namenjen posredovanju notranjih podatkov o izgubah preteklega leta. Banke so ga dolžne posredovati BS na njeno zahtevo v okviru uporabe naprednih pristopov za izračun kapitalne zahteve za OT.

Aplikacija v ta namen omogoča ažurni, tudi dnevni vpogled po poslovnih področjih in vrstah škodnih dogodkov.

9.4.3 Prednosti in slabosti rešitve

Programska rešitev ima določene prednosti, saj je zasnovana na način, da podpira širjenje kulture upravljanja z OT, ima vzpostavljene linije poročanja in zagotavlja ustreznost podatkov s pomočjo računovodske kontrole.

Slabost rešitve je, da je zajem škodnih dogodkov omejen na dogodke z neposredno finančno posledico, ki se jo ugotavlja preko ustreznih kontov. Zato je smiselno, da ta nabor s pridobljenimi izkušnjami in spoznanji sčasoma postaja vse širši in vključuje tudi dogodke, katerih izguba se ne izkazuje neposredno v poslovnih izkazih temveč ima posredne a kljub temu pomembne posledice za bančno poslovanje.

⁴² Povzeto po Slaku (2007, str. 15-24).

10 SKLEP

Napredek v tehnologiji, infrastrukturi in komunikacijah, številne inovacije in razvoj kompleksnih produktov ter nenazadnje veliki finančni škandali so sprožili potrebo po novem kapitalskem sporazumu, ki banke na področju obvladovanja OT postavlja pred pomembne izzive. Do nedavnega je bilo to tveganje obravnavano zgolj kot vsako drugo tveganje, ki ni kreditno ali tržno tveganje. Po vseh omenjenih spremembah in dogodkih pa je postalo preveč očitno in predstavlja preveliko grožnjo, ki lahko omaja finančno stabilnost ne zgolj posamezne institucije, temveč širšega bančnega sistema, da bi lahko še vnaprej ostalo brez ustrezne regulatorne obravnave.

Leta usklajevanj in prizadevanj Baselskega komiteja so na področju OT prinesla povsem nove in mestoma zapletene zahteve, katerim morajo banke prilagoditi svoje poslovanje. Basel II sicer dopušča bankam, da se glede na svoje značilnosti same odločijo za nivo kriterijev, ki ga želijo sprejeti v svoje poslovanje, vendar bodo verjetno nacionalni regulatorji zaradi vloge in pomena bančnega sektorja zainteresirani, da vzpodbujajo uporabo naprednejših pristopov in s tem upoštevajo bolj stroge kriterije. Ti od bank zahtevajo proces zbiranja, vrednotenja, nadzora in poročanja o dogodkih in izgubah iz OT, in sicer že danes, če želijo prvič začeti uporabljati napredne pristope čez tri leta.

Že dosedanja praksa je pokazala pot do učinkovitega obvladovanja OT, ki se prične prav z zbiranjem podatkov o OT. S strani regulatorja je predpisana široka usmeritev, vsaka banka pa mora zase določiti podrobnosti in ustrezne postopke. Nekatere bodo morda želele vzpostaviti širšo prakso, kot so zahteve Basla II. Tudi če je zbiranje omejeno zgolj na predpisane zahteve, je najpomembnejše, da se pravila postavijo jasno in da se jih dokumentira in integrira v vse pore poslovanja, ne glede na poslovno področje, storitev ali geografsko lokacijo.

Prvi problem, s katerim se srečujejo snovalci sistema upravljanja z OT in zbiranja podatkov, je raznolikost narave OT. S pomočjo smernic, ki jih ponuja Basel II, izkušenj dobre poslovne prakse ter z izkoriščanjem največjega vira znanja in izkušenj, se pravi zaposlenih, si lahko banka zagotovi dobre pogoje, da bodo vloženi naporji dosegli zelene rezultate: zagotavljanje takšnih informacij, ki bodo osnova za pravilne poslovne odločitve managementa. S tem ciljem v mislih in s sistematičnim pristopom sem želela v pričujočem delu tudi sama predstaviti koncept oblikovanja ustrezne baze podatkov.

Vprašanj je bilo nedvomno veliko, podobna se bodo pojavljala tudi ob zbiranju podatkov v praksi, kot na primer: Kako zagotoviti, da bo baza podatkov odraz dejanskega stanja in dejanske izpostavljenosti OT, kar pomeni točnost, doslednost in ustreznost zbranih podatkov? Ali so včerajšnji podatki danes še relevantni, glede na številne spremembe, ki smo jim priča? Ali lahko podatke in rezultate med enotami primerjamo?

Izhodišče oz. vodilo za aktivnosti pri vzpostavitvi mehanizma za zbiranje podatkov so naslednje ključne točke: enotno in jasno definirani ključni pojmi, standardizacija za banko relevantnih kategorij v največji možni meri, čim boljša dokumentiranost postavljenih pravil in politike ter ustrezno vgrajeni nadzorni in kontrolni mehanizmi. S tem lahko namreč bistveno pripomoremo k boljši kvaliteti podatkov.

Ena izmed glavnih kritik zbiranja notranjih podatkov je pomanjkanje podatkov o večjih škodnih dogodkih, kar lahko privede do izkrivljene slike o dejanski izpostavljenosti banke OT. Odgovor najdemo v zagotavljanju celovitega podatkovnega modela, s čimer se pomanjkljivosti notranjih podatkov kompenzirajo z uporabno vrednostjo ostalih virov podatkov: ključnih indikatorjev tveganja, samoocenjevanja tveganj, analize scenarijev in zunanjih podatkov. S takšno celovitostjo dosežemo obenem tudi ustrezno ravnotežje med preteklimi izkušnjami notranjih in zunanjih podatkov in ustreznimi predvidevanji in napovedmi za prihodnost ostalih vrst podatkov, ki odražajo hitro spreminjajoče se okolje.

Ponujena rešitev v tej smeri je žal zaenkrat zasnovana predvsem na teoretičnih osnovah. Trenutna praksa se namreč ob uporabi navedenih orodij srečuje z dodatnimi težavami: ključni indikatorji tveganja ne predstavljajo bistvenih koristi pri upravljanju z OT, samoocenjevanja so močno podvržena subjektivni presoji in so ti podatki zato lahko dvomljive kvalitete, pri zunanjih podatkih se srečujemo s težavami pri njihovem prilaganju specifičnim razmeram. Morda še največ koristi lahko pričakujemo od analize scenarijev ob predpostavki, da so zagotovljeni ustrezni validacijski postopki rezultatov. Ker praksa na temu področju hitro napreduje, verjamem, da bo čas prinesel marsikatero dodatno izkušnjo, ki bo zagotovila več koristi posameznemu ali celotnemu sklopu ponujenih podatkovnih možnosti.

Eden izmed pogojev in hkrati ključnih izzivov, od katerega sta odvisni tako kvaliteta kot razpoložljivost podatkov za učinkovito **obvladovanje** OT, je podpora vodstva. Kot vsako upravljanje s tveganjem morda upravljanje z OT celo bolj zahteva multidisciplinarno timsko sodelovanje, željo po kljubovanju uveljavljenim navadam in okolje, v katerem lahko zaposleni prosto govorijo o tveganjih, napakah in grožnjah. Nič od tega ni samoumevno samo po sebi, razen če se za to zavzame najvišje vodstvo. Na njih je odgovornost za vzpodbujanje spremembe kulture znotraj banke, kjer bo upravljanje z OT doseglo najvišjo prepoznavnost in podporo. V ta namen se zahteva kreiranje ustreznih delovnih mest, vključno z delegiranjem odgovornosti in pristojnosti za izvajanje ustrezne politike. Nekatera izhodišča za izvajanje dodatnih konkretnih ukrepov, ki naj bi vzpodbudili ustrezno kulturo, so bila podana v tem delu. Ta izhodišča naj bodo vodilo tudi snovalcem postopka zbiranja podatkov in zagotavljanja celovitosti podatkovnega modela, da na odločitve o izbiri med različnimi možnostmi posameznih rešitev vpliva tudi dejstvo, v kolikšni meri posamezna rešitev širi zavedanje o pomenu OT v banki.

In kakšna je zgodba slovenskega bančnega prostora, ko proučujemo predstavljeno tematiko? Skladno z rezultati anket se vodstva slovenskih bank zavedajo pomena, ki ga

ima OT na njihovo poslovanje. Drugo je, ko je projektu potrebno nameniti dejansko moralno in finančno podporo.

Oseбно menim, da v Sloveniji zaenkrat, kljub pozitivnim zagotovilom, ozračje ni dovolj naklonjeno učinkovitim naprednejšim pristopom za upravljanje OT. Problematika v nasprotju s tujo bančno prakso še ni dovolj dozorela, da bi se zavedali njenega pomena. Menim, da so trenutni napor in dinamika razvoja na temu področju usmerjeni pretežno v zagotavljanje skladnosti z zakonodajo, predvsem z vidika njenih osnovnih zahtev. Kar je tudi nekako razumljivo in s kratkoročnega vidika morda smiselno. Resursi so omejeni (tako kadrovske kot finančne), zahteve regulatorja kompleksne, ob primerjavi koristi in stroškov uvajanja naprednejših pristopov pri upravljanju z OT verjetno slednji prevzemajo prevladujočo vlogo. Večje neposredne koristi lahko banke skladno z ugotovitvami različnih študij pričakujejo od učinkovitega obvladovanja kreditnega tveganja, kar podpira odločitve o usmeritvi omejenih resursov v napredne pristope za izračun kreditnega tveganja.

Dolgoročno verjetno lahko pričakujemo, da bodo tudi naše banke sledile tuji praksi in pričele z bolj aktivnim angažiranjem na temu področju, ne samo v pogledu zbiranja podatkov o lastnih realiziranih škodnih dogodkih z neposrednimi finančnimi izgubami. Morda bo s časom tudi BS kot nadzorna institucija našla nove učinkovite načine, ki bodo banke k temu še dodatno motivirali. Upajmo, da ne bodo za to potrebni novi škodni primeri.

LITERATURA

1. Algo OpRisk Case Study. Algorithmics Incorporated. 3 str. [URL: <http://www.algorithmics.com/EN/media/pdfs/HBOS.pdf>], 29.1.2008.
2. Andersen Arthur: Operational risk and financial institutions. London: Risk Books, 1998. 187 str.
3. Anders Ulrich, Gerrit Jan van den Brink: Implementing a Basel II Scenario-Based AMA for Operational Risk. The Basel Handbook. A Guide for Financial Practitioners. London: Incisive RWG, Ltd., 2004, str. 343-368.
4. Anders Ulrich, Platz Jürgen: Creating an op risk loss-collection framework. Incisive Media Plc. [URL: <http://www.baselalert.com/public/showPage.html?page=18417>], september 2003.
5. An LDA-Based Advanced Measurement Approach for the Measurement of Operational Risk. Industry Technical Working Group on Operational Risk. 25 str. [URL: http://www.gloriamundi.org/picsresources/con0529p_1.pdf], maj 2003.
6. Barriga Linda, Rosengren Eric: Innovations in Risk Management – Lessons from the Banking Industry. 24 str. [URL: <http://www.bos.frb.org/bankinfo/oprisk/innrisk.pdf>], 2004.
7. Basel II: A Closer Look. KPMG, junij 2005. 42 str.
8. Beck Tim et al.: Bank Operational Risk Assessment Methodology. Criteria Report. New York: Fitch Ratings, 2005. 13 str.
9. Capital Requirements Directive Implementation. Industry Feedback: Advanced Measurement Approaches. London: The Financial Stability Authority (FSA), marec 2006, 9 str.
10. Cagan Penny: Seizing the tail of the dragon. FOW Magazine/Operational Risk, julij 2001, str. 18-23.
11. Cruz Marcelo G.: Modeling, Measuring and Hedging Operational Risk. West Sussex: John Wiley & Sons, Ltd., 2002. 330 str.
12. Data Integrity and Validation Issues. London: The Financial Stability Authority (FSA), AMA Quantitative Working Group, december 2005, 4 str.
13. Davidson Clive: Bracing for Basel. [URL: <http://db.riskwaters.com/public/showPage.html?page=129170>], februar 2004.
14. Dev Ashish, Sahay Anupam: Measuring and Calculating Capital for Operational Risk: Achieving AMA compliance. RMA Journal, Philadelphia, marec 2004.,
15. Doering Hans-Ulrich: Operational Risks in Financial Services - An Old Challenge in a New Environment. Credit Suisse Group. 135 str. [URL: http://www.credit-suisse.com/governance/doc/operational_risk.pdf], januar 2001.
16. Emerging Trends in Operational Risk within the financial services industry. Raft International, junij 2002, 20 str.

17. Espersen Donald: The language of risk: organizations can improve risk management and audit processes by communicating risks in terms that everyone understands. Internal Auditor, junij 2007.
18. Geiger Hans: Regulating and Supervising Operational Risk for Banks. Working paper. Zurich: University of Zurich - Swiss Banking Institute, 2000. 19 str.
19. Gup Benton E.: Basel II: Operational Risk, Moral Hazard, and Corporate Culture. Eastern Finance Association Annual Meeting. Norfolk (VA). [URL: <http://www.fma.org/Siena/Papers/530061.pdf>], april 2005, 21 str.
20. Haas Marcus, Kaiser Thomas: Prerequisites for op risk decisions and management. OpRisk&Compliance. [URL: http://db.riskwaters.com/public/showPage.html?validate=0&page=oprisk_login2&url=%2Fpublic%2FshowPage.html%3Fpage%3D215926], april 2005.
21. Haubenstock Michael: The Evolving Operational Risk Management Framework. RMA Journal, Suite, Philadelphia, december 2001, str. 26-29.
22. Haubenstock Michael: Constructing an Operational Event Database. The Basel Handbook. A Guide for Financial Practioners. London: Incisive RWG Ltd., 2004, str. 429-466.
23. Hiwatashi Junji: Solutions on Measuring Operational Risk. Capital Market News. Chicago: Federal Reserve Bank of Chicago, 2002, 4.str.
24. Hočevar Borut: Edo Nodilo: Hrvaški Nick Leeson. Finance, Ljubljana, 2002, 19.3.2002, str. 54.
25. Hoffman Douglas G.: 20 Firmwide Best Practice Strategies. New York: John Wiley & Sons, Inc., 2002, 534 str.
26. Holmes Mark: Operational risk: looking at the bigger picture. Risk Magazine, London, 2003, 8, str. 24-27.
27. Holmes Mark: Measuring operational risk: a reality check. Risk Magazine, London, 2003a, 9, str. 84-87.
28. Holmquist Eric: Harnessing our differences. [URL: <http://db.riskwaters.com/public/showPage.html?page=436446>], marec 2007.
29. Holmquist Eric: Changing culture. [URL: <http://db.riskwaters.com/public/showPage.html?page=440700>], april 2007a.
30. Holmquist Eric: From small acorns.... [URL: <http://db.riskwaters.com/public/showPage.html?page=444543>], maj 2007b.
31. Hübner Robert, Laycock Mark, Peemöller Fred: Managing Operational Risk. Advances in Operational Risk: Firm-wide Issues for Financial Institutions. London: Risk Waters Group, Ltd., 2001, str. 3-28.
32. Implementation of the Capital Accord for Operational Risk. ORIAG. 54 str. [URL: <http://www.globalriskregulator.com/resources/oriagpaper.pdf>], december 2002.

33. Implementation of Basel II: Practical Considerations. Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2004. 36 str.
34. Internal Loss Data Issues. London: The Financial Stability Authority (FSA), AMA Quantitative Working Group, december 2005, 7 str.
35. Jameson Rob: How to Hit a Moving Target? The Week in Risk. [URL: http://www.bankingrisk.com/analysis/archives/2004/07/09/how_to_hit_a_moving_target], julij 2004.
36. Kaishan Bidyut: Business Continuity Management as a Component of Operational Risk Management. I-flex Consulting. [URL: www.gtnews.com/article/6755.cfm], maj 2007.
37. Kavšek Polona: Uvajanje standardiziranega pristopa upravljanja z operativnim tveganjem v bankah. Magistrsko delo. Ljubljana: Ekonomska fakulteta, 2005. 96 str.
38. Kennett Roland: How to Introduce an Effective Operational Risk Management Framework. Advances in Operational Risk: Firm-wide Issues for Financial Institutions. London: Risk Waters Group, Ltd., 2001, str. 67-86.
39. Kin Ying Alvis Lo: A study of rogue trading and the implication of Basel II. Disertacija. Nottingham : Nottingham University Business School - MA Risk Management, 2004. 147 str.
40. Komljenovič Maja: Operativno tveganje na področju zakladniškega poslovanja v srednje veliki banki. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2007. 46 str.
41. Kos Suzana: Žensko sumijo goljufije vredne 113 milijonov tolarjev. Finance, Ljubljana, 2006, 137 (19.7.2006), str. 2-3.
42. Kralj Irena: Upravljanje z operativnimi tveganji v bankah. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2005. 43 str.
43. Kroszner Randall S.: Basel II Implementation in the United States. [URL: <http://www.federalreserve.gov/newsevents/speech/kroszner20070712a.htm>], julij 2007.
44. Kühnert Enno, Stubbs Lavinia: Building a Data Model for Operational Risk Management and Control. Advances in Operational Risk: Firm-wide Issues for Financial Institutions. London: Risk Waters Group, Ltd., 2001, str. 103-113.
45. McLenaghan: The data puddle challenge. OpRisk&Compliance. Str. 24-30. [URL: <http://www.riskbusiness.com/InterestingReading/TmL%20Puddles%20July%202024%202007.pdf>], avgust 2007.
46. Mishkin Frederic: The economics of money, banking and financial markets. Boston: Addison Wesley Longman, 2001. 737 str.
47. Muzzy Ladd: The pitfalls of gathering operational risk data: a tightrope without a net. RMA Journal, Suite, Philadelphia, februar 2003, str. 58-62.
48. Newberry Jay: Collecting operational risk event data: A series designed to introduce readers to the tools used in the management of operational risk today's financial service industry. RMA Journal, Suite, Philadelphia, april 2002, str. 40-42.

49. Observed range of practice in key elements of Advanced Measurement Approaches (AMA). Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2006. 32 str.
50. Operational Risk Management. Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 1998. 9 str.
51. Operational Risk Regulatory Approach. London: International Swaps and Derivatives Association, 2001, 27 str. [URL: <http://www.isda.org/press/pdf/orradp900.pdf>]
52. Peccia Anthony: An Operational Risk Ratings Model Approach to Better Measurement and Management of Operational Risk . The Basel Handbook: A Guide for Financial Practitioners (KPMG). London: Incisive RWG, Ltd., 2004, str. 397-429.
53. Poročilo o finančni stabilnosti. Ljubljana: Banka Slovenije. Maj 2008. 165 str.
54. Power Michael: The Invention of Operational Risk. Discussion Paper. London: The London School of Economics and political Science - ESRC Centre for Analysis of Risk and Regulation, 2003. 20. str.
55. Pregled tretjega posvetovalnega dokumenta »Novi kapitalski sporazum« v delu, ki govori o operativnem tveganju s poudarkom na spremembah – povzetki v slovenščini. 19. str. [URL:http://www.bsi.html/basel2/05_publicacije/dokumenti/C/povzetki/Operativno%tveganje_CP_3.pdf], april 2003.
56. Priporočila za vzpostavitev in izvajanje sistema upravljanja z operativnim tveganjem. Posvetovalni dokument v obdobju 25.7.–25.10.2005. Ljubljana: Banka Slovenije in Združenje bank Slovenije, 2005. 64 str.
57. Ramadurai Krishnan et al.: The Oldest Tale but the Newest Story: Operational Risk and the Evolution of its Measurement under Basel II. Special Report. New York: Fitch Ratings, 2004. 7 str.
58. Ramadurai Krishnan et al.: Operational Risk Management & Basel II Implementation: Survey results. Special Report. New York: Fitch Ratings, 2004a. 8 str.
59. Rotovnik Tomaž, Janevska Lidija: Poročilo z udeležbe na seminarju »New Basel Capital Accord and Problem Bank Resolution«. Vilnius, Litva, 2.-6. september 2002. 22 str.
60. Rotovnik Tomaž: Operativno tveganje in Basel II – Pripravljenost bank v Sloveniji na zahteve novega kapitalskega sporazuma. Zbornik 9. strokovno posvetovanje o bančništvu. Portorož: Zveza ekonomistov Slovenije, 2003, str. 47-61.
61. Rotovnik Tomaž: Operativna tveganja pri Baslu II – Vidik oblikovanja podatkovne baze. 11. konferenca o revidiranju in kontroli IS. 16 str. [URL: <http://www.bsi.si/library/includes/datoteka.asp?DatotekaId=536>], september 2003a.
62. Rotovnik Tomaž: Izzivi zunanjih baz podatkov za operativno tveganje. Bančni vestnik, Ljubljana, 2004, 1-2, str.57-63.

63. Rotovnik Tomaž: Proces nove evropske kapitalske ureditve in njene bistvene novosti. Bančni vestnik, Ljubljana, 2004a, 10, str. 43-47.
64. Rotovnik Tomaž: Problematika in kritika naprednih pristopov za merjenje operativnega tveganja. Bančni vestnik, Ljubljana, 2004b, 12, str. 38-42.
65. Rubin Saša: Basel II tretjič. Bančni vestnik, Ljubljana, 2003, 9, str. 35-40.
66. Sabatini Joseph, Michael Haubenstock: OR: management reporting of operational risk; a series designed to introduce readers to the tools used in the management of operational risk in today's financial services industry. RMA Journal, Suite, Philadelphia, julij-avgust 2002.
67. Samad-Khan Ali: How to Categorize Operational Losses? Applying Principles as Opposed to Rules. OpRisk Advisory LLC. 8 str. [URL: http://www.opriskadvisory.com/docs/ORA_on_Categorization_-_A_Solution.pdf], marec 2002.
68. Slak Leon: Obvladovanje tveganj v bančnem poslovanju po novem kapitalskem sporazumu Basel II. Magistrsko delo. Kranj: Fakulteta za podiplomske državne in evropske študije, 2005, 135 str.
69. Slak Leon: Informacijska podpora zbiranja škodnih dogodkov – operativna tveganja po kapitalski ureditvi Basel II. Zbornik 15. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov. Rogaška Slatina. Slovenski inštitut za revizijo, 2007, str. 9-33.
70. Smithson Charles: Measuring op risk. Risk Magazine, London, 2000, 3, str. 58-61.
71. Sound Practices for the Management and Supervision of Operational Risk. Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2001. 23 str.
72. Sound Practices for the Management and Supervision of Operational Risk. Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2003. 14 str.
73. Taylor Charles, Davies Jonathan: Getting traction with KRIs: laying the groundwork. RMA Journal, Suite, Philadelphia, november 2003, str. 58-63.
74. Theodore Samuel: Bank Operational Risk Management – More Than an Exercise in Capital Allocation and Loss Data Gathering. Special Report. London: Moody's Investors Service, 2002, 10.str.
75. Thirlwell John: Insurance and Operational Risk. The Basel Handbook: A Guide for Financial Practitioners (KPMG). London: Incisive RWG, Ltd., 2004, str. 467-489.
76. Tomažič Janez: Rop sefov SKB še zmeraj neraziskan. Finance.si. [URL: <http://www.finance.si/166940>], 31.10.2006.
77. Tomsits Zoran Jurij: Projekt prenove novega informacijskega sistema Nove ljubljanske banke – »Sigma« z vidika Nadzora bančnega poslovanja Banke Slovenije. Specialistično delo. Ljubljana: Ekonomska fakulteta, 2005. 77 str.
78. Zabavnik Helena: Zgodovina Mednarodne banke za poravnave in njena vloga danes. Diplomsko delo. Ljubljana: Ekonomska fakulteta, 2003. 46 str.

VIRI

1. Direktiva 2006/48/ES Evropskega parlamenta in sveta z dne 14. junija 2006 o začetku opravljanja in opravljanju dejavnosti kreditnih institucij (Uradni list EU, št. L 177/1).
2. Direktiva 2006/49/ES Evropskega parlamenta in sveta, z dne 14. junija 2006, o kapitalski ustreznosti investicijskih podjetij in kreditnih institucij (Uradni list EU, št. L 177/1).
3. International Convergence of Capital Measuremen and Capital Standards. Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2006. 347 str.
4. Operational Risk Management in the Financial Service Industry. International benchmark survey. Heidelberg: SAS, 2004. 12 str.
5. ORX Database and Report. [URL: www.orx.org], ORX, 25.11.2008.
6. Poslovno leto 2006 - zaključeno z dobičkom. Sporočila za javnost. [URL: <http://www.skb.si/info/press/info-press-2007-02rezultati2006.html>], SKB d.d., 7.3.2007.
7. Proces ocenjevanja tveganj. Javni del. Ljubljana: Banka Slovenije. Nadzor bančnega poslovanja, februar 2007, 51 str.
8. Raft International: Operational Risk Management – Today and the Future. [URL: <http://www.gloriamundi.org/picsresources/ri.pdf>], GloriaMundi, 21.12.2006.
9. Results of the fifth quantitative impact study (QIS5). Basel: Basel Committee on Banking Supervision, Bank for International Settlements, 2006. 31 str.
10. Sklep o izračunu kapitalske zahteve za operativno tveganje za banke in hranilnice (Uradni list RS, št. 135/2006).
11. Sklep o poročanju o kapitalu in kapitalskih zahtevah bank in hranilnic (Uradni list RS, št. 104/07).
12. Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice (Uradni list RS, št. 135/06) in dopolnitve (Uradni list RS, št. 28/07 in 104/07).
13. The broadening scope of op risk management. OR&C Inteligence. April 2006.
14. Zakaj nova evropska kapitalska ureditev. [URL: <http://www.bsi.si/poslovanje-bank-in-podjetij.asp?MapaId=160>], Banka Slovenije, 11.10.2007.
15. Zakon o bančništvu (Uradni list RS, št. 131/06) in dopolnitve (Uradni list RS, št. 1/08).

PRILOGE

KAZALO PRILOG

PRILOGA 1	Kategorizacija poslovnih področij	1
PRILOGA 2	Kategorizacija škodnih dogodkov iz OT	2
PRILOGA 3	Opredelitev ključnih kategorij definicije OT	5
PRILOGA 4	Kategorizacija učinkov OT	8
PRILOGA 5	Primer postopka kategorizacije škodnih dogodkov s pomočjo odločitvenega drevesa	10
PRILOGA 6	Praktični vidik problematike ločevanja operativnega od kreditnega in tržnega tveganja	12
PRILOGA 7	Razmejitev vsebine poročil glede na različne tipe prejemnikov	14
PRILOGA 8	Konkretni primeri uporabnih poročil	15
PRILOGA 9	Obrazec OPR Bruto izgube	16
PRILOGA 10	Povzetek letnih poročil posameznih bank za leto 2007 glede izvajanja aktivnosti na področju upravljanja z OT	17
PRILOGA 11	Aplikacija Operativna tveganja – ekranske slike	21

PRILOGA 1: Kategorizacija poslovnih področij

Poslovno področje	Seznam dejavnosti
Podjetniško financiranje in finančno svetovanje	<ul style="list-style-type: none">- Prva prodaja finančnih instrumentov in/ali ponudba finančnih instrumentov z obveznostjo odkupa- Storitve, povezane z izvedbo prvih prodaj vrednostnih papirjev- Investicijsko svetovanje- Svetovanje podjetjem na področju strukture kapitala, poslovne strategije in sorodnih zadev ter svetovanje in storitve, povezane z združitvami in nakupi podjetij- Raziskave na področju investicij in finančna analiza ter druge oblike splošnih priporočil v zvezi s posli s finančnimi instrumenti
Trgovanje in prodaja na veliko	<ul style="list-style-type: none">- Trgovanje za svoj račun- Posli posredovanja na denarnem trgu- Sprejemanje in prenos naročil v zvezi z enim ali več finančnimi instrumenti- Izvrševanje naročil za stranke- Ponudba finančnih instrumentov brez obveznosti odkupa- Upravljanje večstranskega sistema trgovanja
Posli z vrednostnimi papirji na drobno	<ul style="list-style-type: none">- Sprejemanje in prenos naročil v zvezi z enim ali več finančnimi instrumenti- Izvrševanje naročil za stranke- Ponudba finančnih instrumentov brez obveznosti odkupa
Komercialno bančništvo	<ul style="list-style-type: none">- Zbiranje depozitov in drugih vračljivih sredstev- Kreditiranje- Finančni zakup- Osebna kreditna jamstva in obveznosti
Bančništvo na drobno	<ul style="list-style-type: none">- Zbiranje depozitov in drugih vračljivih sredstev- Kreditiranje- Finančni zakup- Osebna kreditna jamstva in obveznosti
Plačila in poravnava	<ul style="list-style-type: none">- Storitve plačilnega prometa- Izdajanje in upravljanje plačilnih instrumentov
Agentske storitve	<ul style="list-style-type: none">- Hramba in administrativne storitve povezane s finančnimi instrumenti za račun strank, vključno s skrbništvom in sorodnimi storitvami, kot je upravljanje denarnih sredstev/zavarovanja
Upravljanje premoženja	<ul style="list-style-type: none">- Upravljanje portfeljev- Upravljanje KNPVP- Druge oblike upravljanja premoženja

VIR: Direktiva, 2006, str. 177-178.

PRILOGA 2: Kategorizacija škodnih dogodkov iz OT

1. raven (z definicijo)	2.raven	3.raven
Notranja goljufija Izgube zaradi dejanj vrste poneverba, odtujitev lastnine ali izogibanje predpisom, zakonu ali politiki podjetja, razen različnih dogodkov, ki izhajajo iz razlikovanja/diskriminacije, v katere je vpletena vsaj ena notranja oseba.	Neodobrene dejavnosti	<ul style="list-style-type: none"> - Namerno neprijavljene transakcije - Neodobrena izvedba določene vrste transakcije - Namerno napačno vrednotenje pozicije
	Tatvina in goljufija	<ul style="list-style-type: none"> - Goljufija, prevare v kreditnem postopku, lažni pologi - Tatvina, oderuštvo, pridobivanje denarja s prevaro (zaposleni uspešno krađe komitentom/strankam), kraja - Nezakonita prisvojitve sredstev - Namerno uničenje sredstev - Ponarejanje - Goljufija s čeki - Tihotapljenje, spretno skrivanje - Kraja računa/lažno predstavljane/itd. - Neusklajenost z davki/izogibanje (namerno) - Podkupovanje/prisvojitve dela delavčevega zaslužka - Insidersko trgovanje (ne za račun firme)
Zunanja goljufija Izgube zaradi dejanj vrste, katere cilj je poneverba, odtujitev lastnine ali izogibanje zakonu, s strani tretje osebe.	Tatvina in goljufija	<ul style="list-style-type: none"> - Kraja/rop - Poneverba - Goljufije s čeki
	Varnost sistemov	<ul style="list-style-type: none"> - Škoda zaradi hekerstva - Kraja informacij (ki se odrazi v denarni izgubi)
Ravnanja v zvezi z zaposlovanjem in varnostjo pri delu Izgube, ki izhajajo iz dejanj, neskladnih z zakoni ali pogodbami, ki urejajo zaposlovanje, zdravje ali varnost, iz plačila odškodninskih zahtevkov v zvezi z osebnimi poškodbami ali iz dogodkov, ki izhajajo iz razlikovanja/diskriminacije.	Odnosi z zaposlenimi	<ul style="list-style-type: none"> - Kompenzacije, podpore, vprašanja v zvezi s prenehanjem delovnega razmerja
	Varno okolje	<ul style="list-style-type: none"> - Splošna odgovornost (zdrs in padec zaposlenega ipd.) - Zdravje zaposlenih in dogodki v zvezi s pravili varnosti pri delu - Kompenzacije delavcem
	Razlikovanje in diskriminacija	<ul style="list-style-type: none"> - Vse vrste diskriminacij

<p>Stranke, produkti in poslovna praksa</p> <p>Izgube, ki izhajajo iz nenamerne neizpolnjevanja ali malomarnega izpolnjevanja strokovne obveznosti do določenih strank (vključno s zahtevami glede zaupnosti in ustreznosti poslovanja) ali iz narave ali sestave produkta.</p>	<p>Soglasje, razkritje in zaupnost</p>	<ul style="list-style-type: none"> - Kršitve zaupnosti/kršenje navodil - Soglasje/vprašanja razkritja podatkov - Kršitve iz naslova razkrivanja podatkov komitentov - fizičnih oseb - Kršitve zasebnosti - Agresivna prodaja (namerna prodaja neprimernega produkta ali deljenje napačnih nasvetov) - Umetno zviševanje vrednosti posla zaradi višje provizije - Zloraba zaupnih informacij - Obveznosti do upnikov
	<p>Neprimerne poslovne in tržne prakse</p>	<ul style="list-style-type: none"> - Monopolni dogovori (povezovanje in dogovori, ki zmanjšujejo konkurenčnost okolja) - Neprimerne trgovalne/tržne prakse - Tržne manipulacije - Insidersko trgovanje (na račun firme) - Dejavnosti brez ustrezne licence - Pranje denarja
	<p>Pomanjkljivosti v produktih</p>	<ul style="list-style-type: none"> - Napake v produktih (nedovoljene ipd.) - Napake v modelih (interne napake modela, ki nastanejo zaradi neprimernih parametrov, napačnega programiranja, napačnih predpostavk, matematičnih napak ipd.)
	<p>Izločanje, poroštvo in izpostavljenost</p>	<ul style="list-style-type: none"> - Neupoštevanje navodil pri poizvedovanju o komitentu - Prekoračenje dovoljenih izpostavljenosti pri komitentu
	<p>Svetovalne dejavnosti</p>	<ul style="list-style-type: none"> - Spor zaradi svetovalčeve dejavnosti
<p>Škoda na premičnem in nepremičnem premoženju</p> <p>Izgube, ki izhajajo iz izgube premičnega ali nepremičnega premoženja ali škode na tem premoženju zaradi naravnih nesreč in drugih dogodkov.</p>	<p>Katastrofe in drugi dogodki</p>	<ul style="list-style-type: none"> - Izguba zaradi naravnih katastrof - Izguba zaradi zunanjih človeških dejavnikov (terorizem, vandalizem)
<p>Poslovne motnje in izpadi sistemov</p> <p>Izgube, ki izhajajo iz poslovnih motenj ali izpadov sistemov.</p>	<p>Sistemi</p>	<ul style="list-style-type: none"> - Strojna in računalniška oprema - Programska oprema - Telekomunikacije - Primanjkljaj potrebnega materiala

Izvedba, dostava in upravljanje procesov Izgube, ki izhajajo iz neuspele obdelave poslov ali upravljanja postopkov, iz odnosov z nasprotnimi strankami in prodajalci.	Zajemanje transakcij, izvedba transakcij in vzdrževanje transakcij	<ul style="list-style-type: none"> - Napačna komunikacija - Vnos podatkov, vzdrževanje ali nalaganje podatkov - Prekoračen rok ali odgovornost - Napačno delovanje sistema/modela - Računovodska napaka/napačni pripisi - Napačno izvajanje drugih nalog - Napačen prenos - Nepravilno upravljanje z zavarovanji - Vzdrževanje referenčnih podatkov
	Spremljanje in poročanje	<ul style="list-style-type: none"> - Neizpolnitev obveznega poročanja - Nenatančno zunanje poročanje (izpostavljenost izgubi)
	Pridobivanje komitentov in dokumentacija	<ul style="list-style-type: none"> - Komitentom niso predstavljene njihove pravice/manjkajoče izjave - Pravni dokumenti manjkajo/nepopolni
	Upravljanje z računi strank/komitentov	<ul style="list-style-type: none"> - Neodobren dostop do računov komitentov - Napačni podatki o komitentu (izpostavljenost izgubi) - Izguba ali poškodba komitentove lastnine zaradi nemarnosti
	Nasprotne stranke v poslih trgovanja	<ul style="list-style-type: none"> - Neizvršitev storitve za nekomitenta - Različni spori z nekomitenti
	Prodajalci in dobavitelji	<ul style="list-style-type: none"> - Zunanji pogodbeni partnerji - Spori s prodajalci

VIR: Basel II, 2005, Aneks 9, str. 257

PRILOGA 3: Opredelitev ključnih kategorij definicije OT

a) Ljudje

Za uspešnostjo vsake organizacije stojijo njeni zaposleni. Zato kadrovska funkcija ali upravljanje človeških virov predstavlja v posamezni instituciji izredno pomemben člen pri obvladovanju tveganj (Proces ocenjevanja tveganj, 2007, str. 33). Kadrovska politika lahko preko upravljanja s človeškimi viri povzroči ogromne izgube, predvsem zaradi diskriminacije, nadlegovanja zaposlenih ali kršitev človekovih pravic (Komljenovič, 2007, str. 5).

Napake zaposlenih povzročajo motnje v poslovnem procesu, pri čemer so lahko namerne ali nenamerne in posledično povzročajo izgube. Dobre notranje kontrole in križni sistemi preverjanja vodstvu omogočajo odkrivanje nenamernih napak zaposlenih. Bolj zapleteno in težje je pri ugotavljanju napak, ki so storjene namerno. Le-te povzročajo motnje v poslovnem procesu, ki se odražajo kot nepoštenost zaposlenega, nagnjenost k goljufiji ali namerne aktivnosti proti banki, kjer je zaposlen (Komljenovič, 2007, str.5).

Vsaka banka naj bi svojo poslovno strategijo uresničevala s primerno strukturo zaposlenih na vseh ravneh. Pri tem naj bi upoštevala velikost, kompleksnost in transparentnost same organizacije, kompleksnost in raznovrstnost njene ponudbe ter kompleksnost sistemov, ki jih uporablja pri poslovanju (Proces ocenjevanja tveganj, 2007, str. 33).

b) Procesi

Dejavnosti se razlikujejo od banke do banke, kjer je število procesov določeno z velikostjo in organiziranostjo banke, številom ter kompleksnostjo produktov/storitev ter samo metodologijo upravljanja procesov. S procesnega vidika lahko dejavnosti razdelimo na (Proces ocenjevanja tveganj, 2007, str. 33):

- osnovne bančne procese (npr. stanovanjski krediti, zamenjava obrestnih mer, rentno varčevanje),
- procese upravljanja (nor. razvoj in spremembe poročil, obveščanje uprave, poročanje zunanjim institucijam),
- podporne procese (npr. izpeljava sprememb v informacijski opremi, dodeljevanje uporabniških dostopov),
- izboljševalne procese (obravnavanje pritožb, projektno vodenje).

Vsaka banka naj bi pri izoblikovanju svojih procesov upoštevala merila, kot so: celovitost poslovanja, standardizacija, urejenost, dokumentiranost, skladnost (z drugimi procesi, zakonodajo), obvladovanje, natančnost, pravočasnost, tehnična podprtost ter ustrezen nadzor. Posebej je potrebno izpostaviti mejnike v procesu⁴³, kjer je potencialno tveganje največje (Proces ocenjevanja tveganj, 2007, str. 33).

c) Sistemi

Pri tem elementu je največji poudarek na informacijskih sistemih in z njimi povezano infrastrukturo. Izpostavimo lahko naslednja področja upravljanja informacijskih sistemov (Proces ocenjevanja tveganj, 2007, str. 34):

- **Strategija:** povezanost oziroma usklajenost s poslovno strategijo banke z vidika podpore obstoječemu in prihodnjemu poslovanju. Pomemben je primeren odnos uprave do te tematike.
- **Obvladljivost:** v interesu banke je imeti čim bolj vzdrževane, prilagodljive, kompatibilne sisteme. Obvladljivost sistemov (strojna, programska, infrastrukturna informacijska oprema) je tem slabša, čim večja je njihova heterogenost.
- **Dostopnost:** na tem mestu poudarjamo kvaliteto obvladovanja in urejenost uporabniških dostopov, sistem avtorizacij (pravic) ter povezanost z zunanjimi subjekti (poskusi nasilnih vdorov v sistem, uporaba enkripcije, požarni zid ipd.).
- **Integralnost:** pomembnejši pokazatelji za ocenjevanje so stanje podatkovnega modela (konsistentnost, popolnost, ažurnost, dograjenost), usklajenost podatkov/informacij z zakonodajo in notranjimi določili, pravočasnost informacij.
- **Nadzor sistemov:** se obravnava z dveh plati – pred vpeljavo (sistemov ali njihovih sprememb), kjer govorimo o kvaliteti testiranja, organiziranosti notranjih razvojnih procesov in kontaktih z zunanjimi dobavitelji ter po vpeljavi, ko obravnavamo uvedbo kontrolnih točk, dokumentiranost, odzivnost notranjega in zunanjega osebja na napake.
- **Neprekinjenost delovanja:** pogostost prekinitev delovanja, potreben čas do vzpostavitve prejšnjega stanja, način varovanja podatkov, odnosi z zunanjimi izvajalci, organiziranost (dežurstva, krizni timi ipd.), primernost, kvaliteta in poznavanje načrta neprekinjenega delovanja, izvajanje stres testov.

⁴³ Mejniki so posebna skupina aktivnosti v poslovnem procesu, ki:

- zaznamujejo konec določene skupine aktivnosti,
- pomenijo preskok izvajanja aktivnosti ali prenos informacij iz ene organizacijske enote v drugo. Običajno služijo tudi za kontrolo kvalitete skupine aktivnosti in kontrolo doseganja zelenih nalog ali ciljev.

- **Uporabnost:** pomembna je primernost sistemov za poslovanje in nivo ter vrste produktov/storitev, ki jih ima banka, nadalje podprtost (nadomestitev ročnih postopkov z avtomatičnimi), poznavanje in stopnja uporabe s strani končnih uporabnikov ter uporabniška prijaznost z vidika kvalitete programske opreme in podpore strokovnjakov za informacijsko tehnologijo (notranji in/ali zunanji).

d) Okolje

Na spremembe in/ali dogodke v okolju banka praviloma nima vpliva. Pomembno je, da jih zna po eni strani v čim večjem obsegu predvideti, po drugi strani pa, da se z ustrezno organiziranostjo na njih pripravlja. Na nivo tveganja, ki izhaja iz okolja, vpliva veliko raznovrstnih faktorjev, na primer finančna, ekonomska in politična stabilnost trgov, na katerih je banka prisotna, pravna varnost v poslovnem okolju, verjetnost pojava naravnih katastrof, verjetnost pojava kriminala. Sem spadajo tudi goljufije tretjih oseb (kraja, špekulacije) ter učinki sprememb zakonodaje (Proces ocenjevanja tveganj, 2007, str. 35).

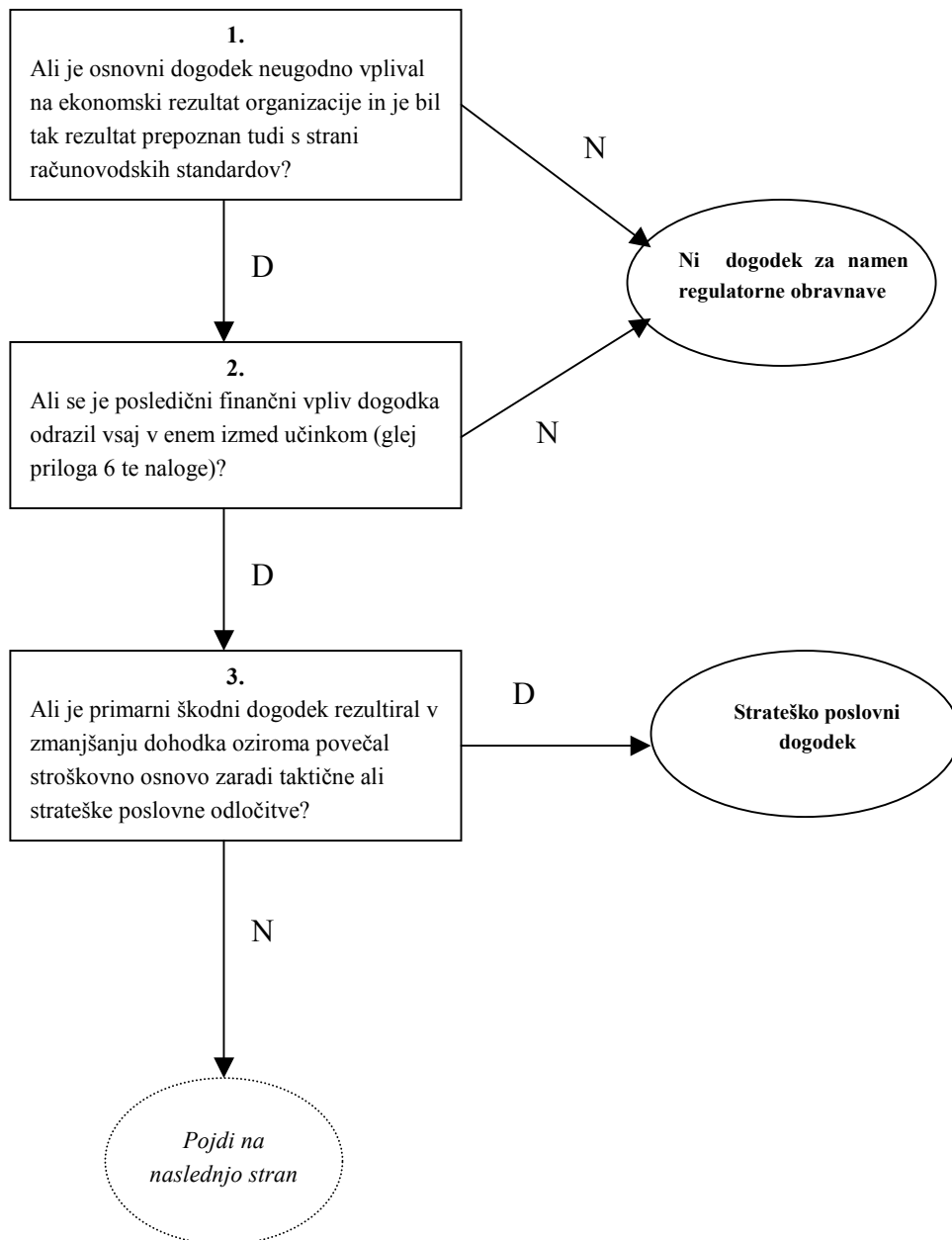
PRILOGA 4: Kategorizacija učinkov OT

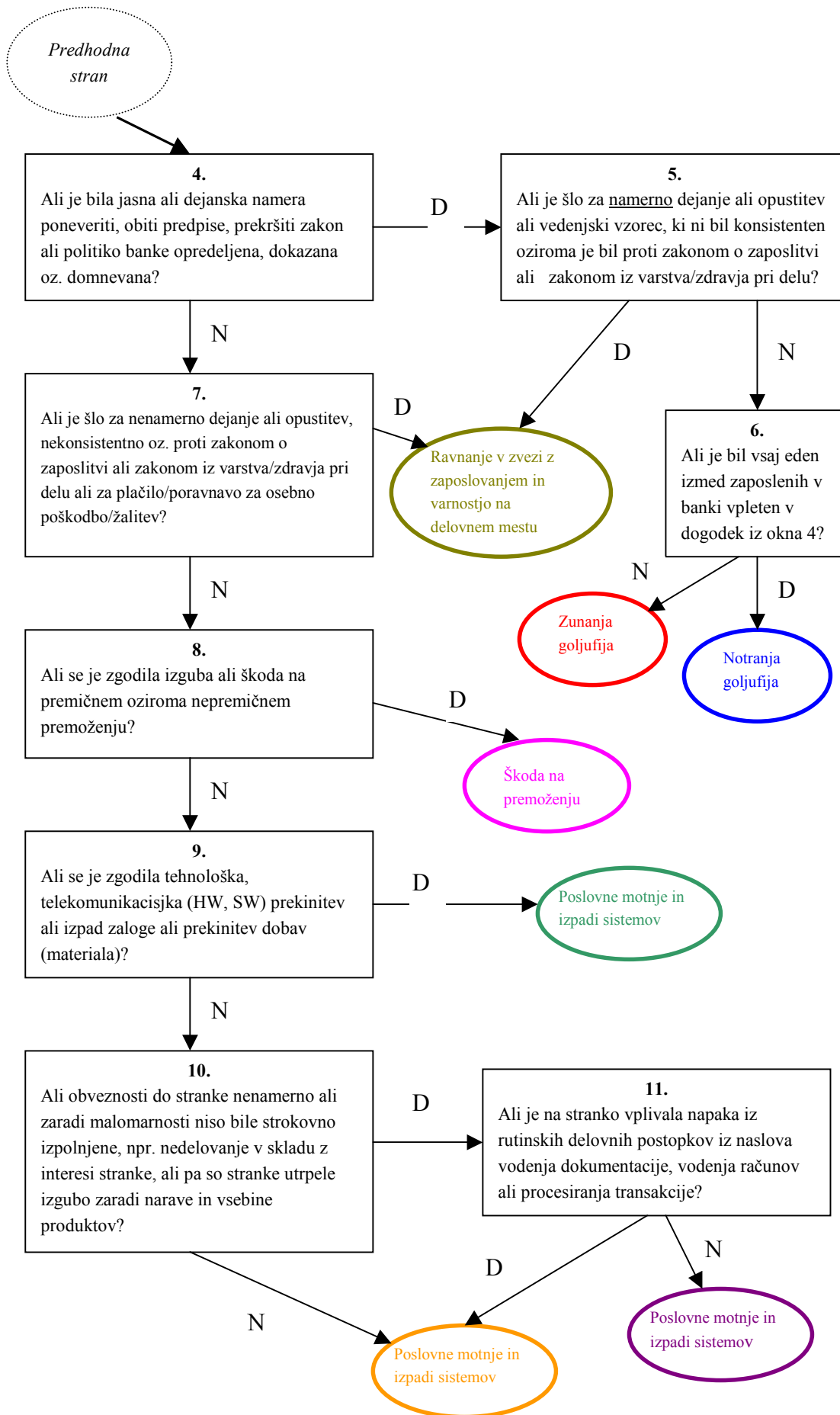
Vrsta učinka	Definicija	Vključuje (primeri)
Pravna odgovornost	Sodbe, poravnave in ostali pravni stroški iz naslova obrambe banke, povezanih oseb in premoženja; materialno in nematerialno.	<ul style="list-style-type: none"> - Plačila za poravnavo realiziranih ali potencialnih pravnih tožb - Plačila sodnih stroškov in podobnih stroškov povezanih s sodnim procesom - Plačila zunanjim pravnim svetovalcem in profesionalnim pričam
Regulatorna in davčna kazen	Globe ali neposredno plačilo za kazni, kot je npr. odvzem licence.	<ul style="list-style-type: none"> - Direktne kazni in globe nadzornim ali davčnim institucijam - Plačila zunanjim svetovalcem in profesionalnim pričam
Povračilo	Plačila drugi strani iz naslova izgub iz OT za katera je banka pravno odgovorna.	<ul style="list-style-type: none"> - Plačila strankam/komitentom ali vzpostavitev stanj na računih zaradi neposredne škode, ki jim jo je banka prizadejala
Izguba iz naslova neplačil	Izguba iz naslova neizpolnitve obveznosti s strani druge stranke, ki ima lastnosti napake ali dogodka iz OT.	<ul style="list-style-type: none"> - Terjatve za sredstva/naložbe in prihodke (provizije in obresti) zavedene v glavni knjigi, ki ne bodo ali ne morejo biti realizirane
Odpisi	Neposredno zmanjšanje vrednosti sredstev iz naslova kraje, prevare, neodobrene dejavnosti, operativnih napak.	<ul style="list-style-type: none"> - Napake v računovodskih praksah - Bistvene prekoračitve proračunov projektov ali neuspešnih projektov - Zmanjšanje vrednosti sistemom iz naslova zmanjšane funkcionalnosti ali učinkovitosti - Povečan prirast izgub iz naslova prevar - Neposredno zmanjšanje vrednosti neotipljivih sredstev - Neposredno zmanjšanje vrednosti sredstev ali povečanje stroškov iz naslova ponudbe neustreznih produktov
Izguba ali poškodba osnovnih sredstev	Neposredno zmanjšanje vrednosti fizičnega sredstva.	<ul style="list-style-type: none"> - Bruto izguba iz naslova fizičnih sredstev, nepremičnin, opreme, računalniške opreme, produkcijskih sistemov
Stroški popravila, povrnitve	Povečanje neposrednih stroškov iz naslova ponovne vzpostavitve operativnega delovanja poslovanja.	<ul style="list-style-type: none"> - Stroški popravila neustreznih produktov ali sistemov - Stroški pisne komunikacije za obveščanje komitentov o napakah - Stroški identifikacije in odprave neposrednih vzrokov dogodka - Plačane nadure za okrevanje daljšega nedelovanja procesnih sistemov

Izgubljen prihodek	Izgubljeni prihodek ali priložnost za prihodek, zmanjšana profitabilnost produkta.	- Izgubljena priložnost za provizijo ali obresti, ki niso zavedeni v glavni knjigi zaradi napak v določitvi cene, modeliranju, komunikaciji, izvedbi
Prekinitev poslovanja	Nezmožnost izvajanja dela v določenem obdobju.	- Neizrabljeni delovni čas zaposlenih

VIR: Priporočila za vzpostavitev in izvajanje sistema upravljanja z operativnim tveganjem, 2005, str. 58

PRILOGA 5: Primer postopka kategorizacije škodnih dogodkov s pomočjo odločitvenega drevesa





PRILOGA 6: Praktični vidik problematike ločevanja operativnega od kreditnega in tržnega tveganja

V nadaljevanju je opisanih nekaj praktičnih primerov, pri katerih se lahko pojavijo dileme uvrstitve dogodka v posamezno vrsto tveganja. Podano je razmišljanje, na kakšen način se lahko potegne ločnica.

1. OPERATIVNO IN KREDITNO TVEGANJE

Zloraba pooblastil pri odobravanju izrednega limita na računu

Primer: Vodja enote odobri stranki izredni limit v višini, ki presega znesek, do katerega je upravičen odobravati izredne limite. Stranka zaradi kakršnegakoli vzroka ne more pokriti limita ob njegovi zapadlosti.

Predlog: Kot znesek izgube iz OT se šteje znesek izgube nad zneskom, do katerega je vodja enote pooblaščen odobravati izredni limit.

Zunanja goljufija

Primer 1: Za pridobitev potrošniškega kredita je stranka posredovala napačne identifikacijske dokumente, ponaredila podpis na pogodbi ter zaradi goljufije postala neizsledljiva že od začetka vzpostavitve kreditnega razmerja, ne da bi povrnila kakršenkoli obrok.

Predlog: Takšna izguba se zaradi zunanje goljufije obravnava kot izguba iz OT, saj izhajamo iz strankine temeljne namere (goljufije), da si pridobi kredit in ga ne odplača.

Primer 2: Kreditojemalec je podal zavajajočo ali nepopolno informacijo o svojem prihodnjem finančnem stanju oz. o prihodnji finančni poziciji svojih produktov za pridobitev kredita. Nekaj obrokov je povrnil, ostalih ne more.

Predlog: V tem kontekstu situacije ne obravnavamo kot izgubo iz OT zaradi zunanje goljufije, temveč kot izgubo iz kreditnega tveganja, saj bo kreditojemalcu težko dokazati, da ni imel namere vrniti kredita (glavni vzrok je bila namera pridobiti kredit ali večji kredit in ne namera nevrnitve kredita).

Primer 3: Banka mora iz naslova zavarovanja kartic komitentu povrniti določen znesek v primeru zlorabe izgubljene ali ukradene kartic.

Predlog: Tovrstne izgube se obravnavajo kot izgube iz OT (glavni vzrok, kot je zlonamerna uporaba najdene, ukradene kartice spadajo na področje zunanje goljufije).

2. OPERATIVNO IN TRŽNO TVEGANJE

Vse izgube, ki izhajajo iz neugodnih gibanj vrednosti pozicij banke in ki imajo osnovni izvor v neizvedenih/neuspehlih procesih/procedurah oziroma v neuspelem izvajanju procesov in procedur, se obravnava kot izgube iz tržnega tveganja, ki jih je povzročilo OT.

Nekaj primerov, kjer je glavni vzrok izgube OT:

Primer 1: Banka izvrši naročilo stranke tik pred koncem trgovalnega dne, čeprav je stranka posel naročila tekom dneva. Zaradi velikosti in časa naročila ima posel znaten vpliv na zaključno ceno instrumenta (npr. delnice). Banka in nadzorniki raziščejo incident. Sodišče oz. nadzorna institucija odloči, da gre v tem primeru za manipulacijo trga s strani banke in banko denarno kaznuje ter zahteva ustrezne spremembe v njenih politikah in procesih.

Primer 2: Banka uporablja model za vrednotenje derivativov. Uporablja se za določanje dnevnih dobičkov in izgub in dnevne tvegane vrednosti. Izkaže se, da ima model napako. Napaka v modelu je odkrita ob primerjavi internega vrednotenja banke z ocenami tretje neodvisne stranke.

Primer 3: Banka prodaja neustrezen produkt strankam. Na primer, upokojujencem ponuja visoko tvegano rentno naložbo, ki bi bila bolj primerna za mlade ljudi. Pri tem strankam ni dovolj natančno razložena narava produkta, na primer, da se dobiček zaradi velikih gibanj na trgu oblikuje šele na daljši rok. Neka stranka ugotovi, da je produkt za obravnavano ciljno skupino neprimeren in se počuti izigrano. Na sodišču oz. pri nadzorni instituciji sproži ustrezen postopek. Sodišče oz. nadzorna institucija naloži banki, da povrne stranki(-am) sredstva v višini originalne cene produkta in obresti.

Ob ločevanju tržnega in operativnega tveganja je potrebno poudariti, da je treba izgube najprej odkriti, da se sploh lahko obravnavajo v okviru OT. V kolikor izguba ni odkrita, se samodejno obravnava v okviru tržnega tveganja.

Primer 1: Trgovalec po pomoti kupi napačne delnice. Ko to ugotovi, napačne delnice proda in kupi ustrezne. Pri tem ni nujno, da je napaka odkrita, saj lahko posel realizira majhne razlike v ceni.

PRILOGA 7: Razmejitev vsebine poročil glede na različne tipe prejemnikov

Prejemnik	Tip posredovanih informacij
Uprava	<ul style="list-style-type: none"> - Agregirani podatki o škodnih dogodkih na ravni banki - Rezultati samoocenjevanj in ključnih indikatorjev tveganj - Ekonomski in regulatorni kapital - Takojšnja poročila v primeru večjih škodnih dogodkov
Odbor za upravljanje z OT	<ul style="list-style-type: none"> - Agregirani podatki o škodnih dogodkih na ravni banki - Rezultati samoocenjevanj in ključnih indikatorjev tveganj - Ekonomski in regulatorni kapital - Takojšnja poročila v primeru večjih škodnih dogodkov
Vodje poslovnih enot	<ul style="list-style-type: none"> - Agregirani podatki o škodnih dogodkih na ravni poslovne enote - Rezultati samoocenjevanj in ključnih indikatorjev tveganj - Ekonomski in regulatorni kapital - Takojšnja poročila v primeru večjih škodnih dogodkov
Služba za upravljanje z OT	<ul style="list-style-type: none"> - Podrobni podatki o škodnih dogodkih, samoocenjevanjih, ključnih indikatorjih tveganj
Podporni oddelki	<ul style="list-style-type: none"> - Podrobnejši podatki glede na področje, ki ga oddelek pokriva (npr. kadrovski oddelek prejema podrobne informacije v zvezi z zaposlenimi)
Odbor za revizijo	<ul style="list-style-type: none"> - Odvisno od njihovih aktualnih zahtev
Notranja revizija	<ul style="list-style-type: none"> - Odvisno od njihovih aktualnih zahtev
Zunanja revizija	<ul style="list-style-type: none"> - Odvisno od njihovih aktualnih zahtev
Nadzornik – BS	<ul style="list-style-type: none"> - Regulatorni kapital - Izgube iz OT - Rezultati samoocenjevanj - Ključni indikatorji tveganj - Dodatne informacije glede na zahteve

VIR: Basel II: A Closer Look, 2005, str. 25

PRILOGA 8: Konkretni primeri uporabnih poročil

Poročilo	Opis
Poročilo o škodnih dogodkih in izgubah	Različne statistike in grafikoni na podlagi podatkov o škodnih dogodkih: absolutne, relativne in povprečne vrednosti, indeksi, trendi in napovedi, analizirano po poslovnih področjih in kategorijah tveganja. Vsaka bistvena sprememba in odstopanje je opisano.
Poročilo o večji škodnih dogodkih (npr. top 10)	Podrobni podatki o vsaki pomembnejši izgubi, škodnemu dogodku ali grožnji - kaj se je zgodilo, vzroki, možnost povezanih dogodkov, ukrepi za preprečitev teh v bodoče.
Poročilo o ključnih vzrokih in okoliščinah, v katerih prihaja do izgub	Ključno vprašanje za pripravo tovrstnega poročila: Ali lahko banka napove možen izid sprejema poslovnih odločitev (npr. zmanjšanje števila zaposlenih, povečanje števila transakcij ipd.)?
Poročilo o zunanjih dogodkih	Analize na podlagi relevantnih zunanjih dogodkov, trendov v panogi, najnovejše informacije o regulativi, konkurenci in ostalih zunanjih faktorjih OT, ki bi lahko bili zanimivi.
Poročilo o indikatorjih tveganja	Spremljanje enega ali manjšega števila ključnih indikatorjev tveganja; od specifičnih v okviru poslovne enote do splošnih na konsolidirani osnovi.
Poročilo o rezultatih samoocenjevanj	Podobno kot pri notranjih škodnih dogodkih se prikažejo glavne ugotovitve postopka samoocenjevanj: ključna tveganja in dejavniki tveganj, profil tveganja, trendi, ipd.
Poročilo o stroških OT	Analize zajemajo celotne izgube v računovodskem obdobju, izdatke iz naslova zavarovanj in ostalo načine financiranja tveganja ter morebitna povračila iz tega naslova ter investicije v obvladovanje tveganj.
Poročilo o učinkovitosti upravljanja z OT	Vključuje na primer informacije o izvajanju korektivnih ukrepov (opis ukrepov in njihov status, odgovornosti in ključni datumi), izvršena samoocenjevanja ipd.
Poročilo o zahtevanem kapitalu za pokrivanje izgub iz OT	Vključuje izračun kapitala in alokacijo po poslovnih področjih, trende, primerjave ipd.

VIR: Hoffman, 2002, str.161-166 in Sabatini, 2003.

PRILOGA 9: Obrazec OPR Bruto izgube

OPR Bruto izgube	BRUTO IZGUBE PO POSLOVNIH PODROČJIH IN VRSTAH DOGODKOV										v 150€ EUR	
	II. VRSTE ŠKODNIH DOGODKOV										IV. MEJE IZGUB ZA ZBIRANJE DOGODKOV	
	1	2	3	4	5	6	7	8	9	10	NAJVIŠJA MEJA IZGUB	NAJNIŽJA MEJA IZGUB
NOTRANJA GOLJUFIJA	ZUNANJA GOLJUFIJA	RAVNAVANJE V ZVEZI Z ZAPOSLJAVANEM/IN VARNOSTJO PRI DELU	ŠKODNA NA STRANKE, PRODUKTI IN POSLOVNA PRAKSA	ŠKODA NA PREMČIEM IN NEPREMČIEM PREMOŽENJU	POSLOVNE MOTNJE IN IZPADI SISTEMOV	IZVEDBA, DOSTAVA IN UPRAVLJANJE PROCESOV	III. SKUPAJ PO VRSTAH DOGODKOV					
1. RAZPOREDITEV IZGUB PO POSLOVNIH PODROČJIH												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
2. TRGOVANJE IN PRODAJA NA VELIKO												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
3. POSLI Z VREDNOSTNIMI PAPIRI NA DROBNO												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
4. KOMERCIALNO BANČNIŠTVO												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
5. BANČNIŠTVO NA DROBNO												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
6. PLAČILA IN PORAVNAVA												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
7. AGENTSKE STORITVE												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
8. UPRAVLJANJE PREMOŽENJA												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												
9. SKUPAJ PO POSLOVNIH PODROČJIH												
Število dogodkov												
Celoten znesek izgube												
Največja posamična izguba												

PRILOGA 10: Povzetek letnih poročil posameznih bank za leto 2007 glede izvajanja aktivnosti na področju upravljanja z OT

Abanka Vipava d.d. (Letno poročilo 2007, str. 115-116)

V letu 2007 je banka prešla na aplikacijsko podprto poročanje škodnih dogodkov. Interno sta bili razviti intranetna aplikacija za prijavo škodnih dogodkov in aplikacija za popis škodnih dogodkov. Prva je namenjena vsem zaposlenim v banki in omogoča anonimno prijavo škodnih dogodkov, v drugi poročevalci popisujejo škodne dogodke. Vse organizacijske enote banke imajo formalno določenega poročevalca, ki je odgovoren za popis škodnega dogodka od nastanka do ugotovitve končnih posledic za banko.

Na podlagi popisov škodnih dogodkov služba za upravljanje tveganj izdeluje trimesečna poročila za upravo in višje vodstvo banke.

Ažurno vzdržujejo načrt neprekinjenega poslovanja, imajo izdelan celovit načrt ukrepanja po katastrofi, in sicer zaenkrat za sektor plačilnega prometa in dve poslovalnici.

Enkrat letno izvajajo analizo tveganj informacijske tehnologije po 18-ih skupinah informacijskih virov. Podatke zbirajo z anketami in intervjuji. Kvalitativna analiza upošteva štiri stopnje groženj (glede na pogostost in vpliv) in štiri stopnje ranljivosti (glede na uvedenost posameznih kontrol in njihovo pomembnost) informacijskih virov.

Banka Celje d.d. (Letno poročilo 2007, str. 92-94)

Od leta 2004 ima banka vzpostavljeno evidenco škodnih dogodkov: po 7-ih vrstah, po organizacijskih enotah in 8-ih poslovnih področjih ter po njihovi bruto in neto vrednosti. V letu 2007 je bil izveden temeljit popis poslovnih procesov (37 procesov), ki bo omogočil izdelavo profila OT za posamezne procese ter dopolnitev kataloga vseh identificiranih OT. S tem naj bi zgradili celovito sliko izpostavljenosti OT, ki temelji na prikazu pogostosti in pomembnosti ocenjenih in spremljanih vrst OT. Glede na primerjavo kataloga tveganj z evidentiranimi škodnimi dogodki bodo določili limite prevzemanja OT po kategorijah škodnih dogodkov.

Identifikacija OT so izvedli v okviru popisa poslovnih procesov.

V merjenje so zajeti škodni dogodki, ki vplivajo na poslovni izid, njihova vrednost pa presega 40 evrov. Sistem evidentiranja je zasnovan tako, da se škodni dogodki evidentirajo na 90-ih mestih. Ugotavljajo indikatorje: hitra rast, gibanje delovne sile, frekvenco zaustavitev sistemov. Spremljajo potencialne škodne dogodke.

Sektor upravljanja z OT na osnovi trimesečnega poročanja vseh organizacijskih enot izdeluje različne analize in poročila ter seznanja upravo in višje vodstvo o realiziranih vseh večjih izgubah. Zagotovljeno je tekoče spremljanje uresničevanja sprejetih ukrepov upravljanja tega tveganja.

Za primer delovanja v pogojih hudih motenj poslovanja ima banka sprejete različne dokumente: načrt delovanja z nadomestno lokacijo, obnovitveni načrt dela po katastrofi, načrte neprekinjenega poslovanja.

V prvi fazi banka izračunava kapitalske zahteve za OT po enostavnem pristopu.

Banka Koper d.d. (Letno poročilo 2007, str. 108-109)

Sistem upravljanja z OT ureja Politika upravljanja z operativnim tveganjem. Sistem tvorijo: ustrezna organizacijska struktura, proces upravljanja z OT in sistem notranjih kontrol.

Proces upravljanja se izvaja s postopki ugotavljanja, merjenja oziroma ocenjevanja, obvladovanja in spremljanja OT.

Ugotavljanje se izvaja s procesom zbiranja škodnih dogodkov OT, ki je aplikativno podprt.

Služba upravljanja s tveganji pripravlja četrtletna poročila o OT za upravo.

Vzpostavljen je proces poročanja in ukrepanja v primeru nastanka škodnega dogodka s pomembno škodo.

Gorenjska banka d.d. (Letno poročilo 2007, str.61)

Banka ima vzpostavljen sistem za spremljanje OT oziroma škodnih dogodkov, ki so posledica OT.

Za izračun kapitalske zahteve uporabljajo enostaven pristop.

NLB d.d. (Letno poročilo 2007, str. 37-38)

Evidentiranje in spremljanje škodnih dogodkov iz naslova OT je omogočeno s programsko opremo za upravljanje z OT. Vnos in poročanje o škodnih dogodkih opravljajo za to zadolžene osebe (vnašalci oz. poročevalci). Poročevalec je odgovoren za poročanje škodnih dogodkov za enega ali več sektorjev oz. podružnic. Poročevalec je zadolžen za izdelavo ustreznih analiz iz naslova škodnih dogodkov za svoje nadrejene.

Kot škodni dogodek se poročajo vsi dogodki (tako pozitivni kot negativni), katerih vsota bruto izgube vpliva na poslovni izid in je enaka ali višja od 50 evrov.

Možni tipi škodnega dogodka so majhne škode (od 50 do 1000 evrov), velike škode (večje od 1000 evrov) ter blagajniški in bankomatski presežki oz. primanjkljaji.

V letu 2007 je bilo v banki zabeleženih 427 škodnih dogodkov, od tega 312 z negativno bruto škodo, 115 pa s pozitivno. Neto izguba v obravnavanem obdobju je znašala 74,5 tisoč evrov, kar predstavlja 0,54% vseh neto prihodkov, bruto izguba pa 164,3 tisoč evrov, kar predstavlja 1,18% vseh neto prihodkov.

Razdelitev škodnih dogodkov po vrstah škodnega dogodka kaže, da 47% (oziroma 202) vseh škodnih dogodkov spada v kategorijo strank, produktov in poslovne prakse. Sledijo škodni

dogodki, ki so nastali zaradi izvedbe, prenosa in upravljanja procesov, pri katerih so jih zabeležili 153. 43 škodnih dogodkov je nastalo kot posledica zunanjega kriminala, in sicer iz naslova »skimminga« oz. zlorab bančnih kartic. Ostalih 28 škodnih dogodkov je nastalo zaradi postopkov zaposlenih in varstva pri delu ter napak pri sistemih.

Nova KBM d.d. (Letno poročilo 2007, str. 175-176)

Banka je vzpostavila lastno aplikativno podporo za sistematično spremljanje škodnih dogodkov.

Načrtujejo standardizacijo internega poročanja.

Na podlagi samoocnitve so izdelali celovit profil tveganja, ki vključuje tudi OT. Samoocenjevanje se prek delavnic in anket stalno nadgrajuje, da bi ugotovili in odpravili morebitne vrzeli pri veljavnem sistemu notranjih kontrol.

Spodbujajo zavedanje zaposlenih o OT, cilj je vzpostavitev kulture upravljanja tveganj.

SKB d.d. (Letno poročilo 2007, str. 34-35)

Banka je vzpostavila postopek zbiranja podatkov o izgubah in s tem hkratno izvajanje korektivnih ukrepov s ciljem, da se zmanjšajo možnosti ponavljanja takih izgub.

Izguba se upošteva, če je bila dejansko vknjižena v stroške ali rezervacije. Vodje poslovnih področij so odgovorni za poročanje o svojih izgubah v predpisani bazi podatkov in so dolžni, da izgube posredujejo koordinatorju za OT, če te presežejo določen znesek. Banka Slovenije in Commission Bancaire Française sta skupini Société Générale in SKB odobrili uporabo naprednega pristopa za izračun kapitalske zahteve za OT (AMA). Banka ga uporablja z letom 2008.

V okviru naprednega pristopa je banka uvedla naslednje postopke za merjenje in obvladovanje OT:

- zbiranje podatkov o dogodkih, povezanih z operativnimi izgubami (baza preteklih podatkov);
- kontrolo izčrpnosti baze podatkov;
- samoocenjevanje tveganja in sistem kontrole in preprečevanja (RCSA);
- spremljanje ključnih kazalnikov tveganja (KRI);
- spremljanje korektivnih ukrepov za nadzor in zmanjševanje izpostavljenosti tveganju.

Probanka d.d. (Letno poročilo 2007, str. 39-40)

V letu 2006 je banka razvijala predvsem področje poročanja o škodnih dogodkih in snovanja temeljnih dokumentov za procese identifikacije in ocenitve tveganja.

Leta 2007 so nadgradili sistem poročanja o škodnih dogodkih, ki zagotavlja postopke neodvisnega vnosa vsakega škodnega dogodka iz kateregakoli področja poslovanja in kontrolo

odgovornih uslužbencev ter njihovo potrditev. Sistem se nadgrajuje s poročilnimi tokovi na vseh nivojih upravljanja s OT ter po predpisih in zahtevah v zunanje okolje.

Za identifikacijo OT uporabljajo informacijsko tehnologijo zunanjega dobavitelja, ki v ta namen ponuja poseben modul. Za operativno izvedbo postopkov identifikacije je banka sledila veljavnim Priporočilom za upravljanje z OT ZBS in BS ter razvila lastno metodologijo in pripravila ustrezne strokovne podlage v obliki navodil in sklepov lastnikom procesov in podatkov. Na podlagi tega bodo pripravili pričakovani profil tveganja banke.

Banka ima vzpostavljene načrte za okrevanje po katastrofi in načrte za neprekinjeno poslovanje.

Sistem poročanja je avtomatiziran, pri čemer so posamezni dogodki obravnavani na rednih sestankih varnostnega foruma. Vzpostavljen sistem neposrednega vnašanja škodnih dogodkov omogoča njihovo pregledovanje in potrjevanje ter izdelavo in pošiljanje poročil odgovornim osebam in organom.

UniCredit Banka Slovenija d.d. (Letno poročilo 2007, str. 94)

Banka zbira vse izgube in dobičke, ki so povezani z dogodki OT, z zneskom nad 100 EUR in vse potencialne izgube nad 10.000 EUR. Vsak dogodek OT se uvrsti v eno izmed sedmih kategorij tveganja po Baslu II.

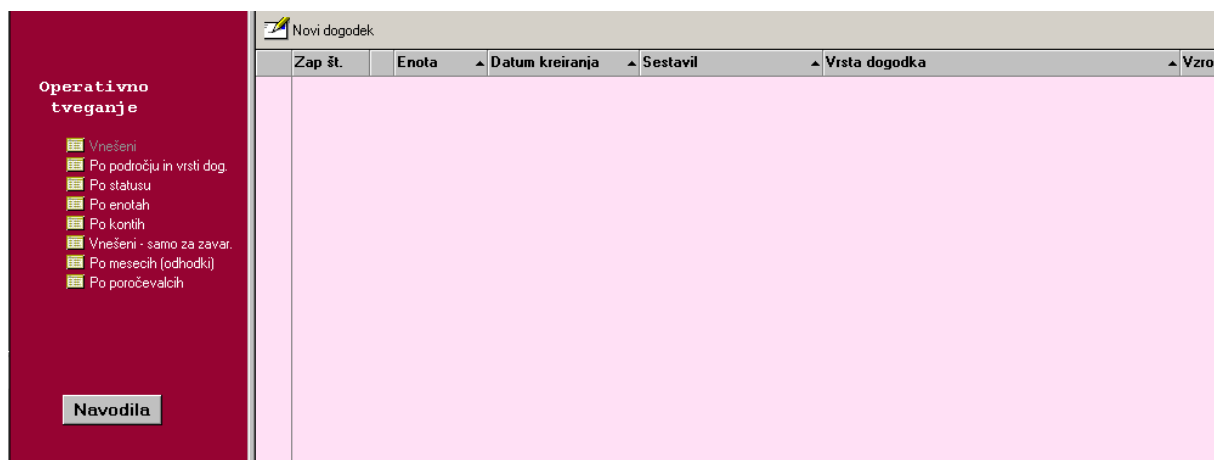
Izgube OT se redno usklajujejo z računovodskimi izkazi.

Izvajajo analize scenarijev, katerih namen je oceniti stopnjo izpostavljenosti banke OT. Scenarije se določi na podlagi analiz internih izgub, relevantnih zunanjih dogodkov, trenda ključnih indikatorjev OT, procesov, produktov in vrst dogodka. Upoštevajo se tudi izkušnje oseb v vlogi upravljalcev OT in predlogi notranje revizije ali ALCO.

Ko so scenariji identificirani, oddelek za upravljanje z OT opravi razgovor z vodji divizij in z osebami v vlogi OpRisk Manager. Rezultati v smislu najslabšega možnega scenarija, kritičnih procesov, predlogov ukrepov za zmanjšanje tveganja ali učinkov na tvegani kapital so opisani v poročilih scenarijev, ki jih izdelata oddelek za upravljanje z OT.

PRILOGA 11: Aplikacija Operativna tveganja – ekranske slike

SLIKA 1: Osnovna ekranska slika



VIR: Banka X

SLIKA 2: Vnosna ekranska slika za zajem škodnih dogodkov

✘ Prekliči ✔ Shrani in Izhod

Poročevalec:	
Organizacijska enota poročevalca:	
Organizacijska enota lastnika škodnega dogodka:	
Vodja enote:	
Prejemnik poročila:	
Datum nastanka dogodka	Vrsta dogodka
Bruto znesek v EUR	0,00
Opis dogodka	
Konto knjiženja	Datum knjiženja
Področje po Baslu:	Vzrok škodnega dogodka:
Upravljanje premoženja	

VIR: Banka X

SLOVARČEK SLOVENSКИH PREVODOV TUJIH IZRAZOV

Advanced Measurement Approach (AMA)	Napredni pristop
Bank for International Settlements (BIS)	Banka za mednarodne poravnave
Basic Indicator Approach	Enostavni pristop
Capital Accord	Kapitalski sporazum
Context Dependency	Odvisnost od danih razmer
Contributory Factors	Spremljajoči dejavniki
Decision trees	Odločitvena dreves
Event based approach	Pristop (kategorizacija) na osnovi dogodkov
Event Trigger	Povod za dogodek
Internal Measurement Approach	Pristop temelječ na internem merjenju
Key Risk Indicator (KRI)	Ključni indikator tveganja
Loss Distribution Approach	Pristop s statistično porazdelitvijo izgub
Near misses	Skoraj izgube
Risk and Control Self-assessment (RCSA)	Samocenjevanje tveganj in sistem kontrol
Scorecard Approach	Točkovni pristop
Scorecards	Točkovanje
Standardised Approach	Standardiziran pristop