UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

OPERATIVNO TVEGANJE V BANKAH

Ljubljana, junij 2005 TINA DREMELJ

IZJAVA

Študent/ka _____*Tina Dremelj*_____ izjavljam, da sem avtor/ica tega diplomskega dela, ki sem ga napisala pod mentorstvom__*mag. Saše Jazbec* ___ in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 13.6.2005 Podpis:

KAZALO

UVOD

V poslovnem svetu obstaja veliko vrst tveganj; v zadnjem času se največ govori o operativnem tveganju. Pojavlja se v vseh sferah poslovanja, tako v podjetjih kot v bankah. Njegova težava je v tem, da se ga težko izmeri in okvantificira.

Šolski primer takega tveganja je propad banke Barings (opisan v prvem poglavju). Zaradi tega propada in še nekaterih drugih škandalov (glej Tabelo 1 na strani 3) je nastal Baselski sporazum, na podlagi katerega so poskušali operativno tveganje definirati, ga izmeriti in ga na sploh umestiti v samo poslovanje banke, zato sem v diplomski nalogi poskušala predstaviti operativno tveganje z vidika bančnega poslovanja.

Prvo poglavje govori predvsem o tem, kako je operativno tveganje definirano, kaj nanj vpliva, kdaj se lahko pojavi. To poglavje govori tudi o dveh dejavnikih, ki močno vplivata na samo operativno tveganje in reševanje le-tega. To sta organizacijska struktura in terminologija.

Drugo poglavje je namenjeno podatkovnemu modelu. Podatkovni model predstavlja bazo podatkov, ki jo mora posamezna banka vzpostaviti, če želi pridobiti kvalitetne informacije o prisotnosti tveganja v določeni poslovni enoti.

Tretje poglavje opisuje upravljanje z operativnim tveganjem; predvsem o tem, kakšen je cilj upravljanja z njim ter o korakih pri upravljanju.

Bančni strokovnjaki so razvili različne metode merjenja operativnega tveganja. Z njimi lahko ugotavljamo višino operativnega tveganja in kje se v posamezni poslovni enoti nahaja. Poslovodstvo banke se lahko odloča, na katerem nivoju bo zbiralo podatke; na nivoju poslovne enote ali celotne banke. Te metode so predstavljene v četrtem poglavju.

Bančni regulatorji so za zaščito pred škodnimi dogodki iz naslova operativnega tveganja določili minimalne kapitalske zahteve za banke. Zahteve prav tako lahko računamo na podlagi več metod, ki so opisane v petem poglavju.

Šesto poglavje govori o zavarovalnih policah in možnostih zaščite pred škodnimi dogodki z njim. Poglavje je predstavljeno z vidika regulatorja.

Sedmo poglavje opisuje trenutno situacijo v Sloveniji. Ker so ti podatki zaupni in zato za javnost nedostopni, žal ne morem natančneje pisati o tveganju v slovenskih bankah. Bo pa v tem poglavju predstavljena študija, ki jo je izvedla Banka Slovenije na temo operativnega tveganja v slovenskih bankah in njihovo pripravljenost na uvedbo minimalne kapitalske zahteve.

1. OPERATIVNO TVEGANJE

»Tečaj je zdrsnil za desetino centa. Izpuhtelo je deset tisoč dolarjev…Še za desetino. Izgubljenih je dodatnih deset tisoč dolarjev…In nova desetina centa in novih deset tisoč dolarjev izgube…Potem pride prvih sto tisoč dolarjev minusa in pozneje prvi izgubljeni milijon….

Finančni trgovec je v takšnih trenutkih povsem sam. Krči v želodcu postanejo redni spremljevalci. Pojavi se želja, da bi prikril izgubo pred nadrejenimi v banki, borzni hiši ali podjetju. Večini to ne uspe. Zlasti takšnim, ki znajo posle tudi knjižiti. Po prvem uspešno prikritem poslu se začne resnična katastrofa. Izgube se nabirajo: milijon, dva, tri, deset, dvajset milijonov dolarjev minusa. Špekulant izgubi sposobnost trezne presoje razmer. Kazalce, ki vplivajo na tečaje, ocenjujejo površno, na hitro in narobe. Razlog: tako obupno si želi, da bi se razmere na trgu obrnile njemu v prid. Kupuje ali prodaja nove in nove tisoče delnic, terminskih pogodb ali nove milijone dolarjev. Tveganja in izgube so vse večje; moči,da bi – kot pravijo na finančnih trgih – zaprl pozicijo, pa je vse manj« (Hočevar, 2002).

S tem uvodom je začel novinar Financ Borut Hočevar članek o milijonski izgubi Riječke banke zaradi bančnega delavca Eda Nodile, ki je izgube prikrival že od leta 1998. Ta primer povezujejo s primerom Nicka Leesona, ki je izgubil dobro milijardo dolarjev in zato je banka Baring's[1] leta 1995 propadla. Med njima je veliko podobnosti:

1) Na začetku sta oba bila navadna delavca; Edo je trgoval z devizami, Nick pa je bil borzni posrednik s terminskimi pogodbami za delniški indeks Nikkei 225.
2) Ker so se hrvaške banke centralizirale, je Edo napredoval; postal je glavni trgovalec z devizami (»chief dealer«). Uspešno izvedena špekulacija z indeksom Nikkei je povzročila, da so Nicka poslali v Singapur, kjer je bil vodja tako zaledne pisarne (»back office) kot tudi trgovanja (»front office«). Nihče ju ni kontroliral. Priborila sta si sloves zanesljivih in poštenih ljudi.
3) Zaradi knjigovodskih nepravilnosti in netočnostih v bilanci je Edo Nodilo povzročil izgubo v višini 60 milijonov evrov, kar je usodno vplivalo na poslovanje. Svoje izgube je skrival na posebnem kontu. Ker je bilo vodstvo površno, izgub ni odkrilo in ni moglo preprečiti propada banke. Oba sta uspela svoje izgube precej dolgo skrivati. Nick Leeson

[1] BARINGS PLC – Banka je februarja leta 1995 izgubila 1,3 milijarde $. Izguba je postala sinonim za operativno tveganje v bankah in takrat se je začelo govoriti o tveganju in odpravljanju le-tega. Izguba je bila večja od celotnega kapitala in rezerv, ki jih je imela banka, prav tako je povzročila velikanske likvidnostne težave. Banka je morala razglasiti stečaj Takrat jo je kupila nizozemska banka ING. Dogodek je šokiral vso bančno javnost (Mishkin, 2001, str. 238).
Vso izgubo je povzročil Nick Leeson, 28-letni borzni posrednik pri Baringsovi poslovalnici v Singapurju. Julija 1992 je Leeson začel špekulirati z delniškim indeksom NIKKEI 225. Do konca leta 1992 je že izgubil 3 miljone dolarjev, ki jih je skril na posebnem kontu. Zaradi slabih internih kontrol mu je uspelo prepričati celotno vodstvo podjetja, da ustvarja ogromne profite. Banka mu je namreč dopuščala, da je sam trgoval z indeksom ter tudi sam nadziral knjige. Tako ni imel nikakršne kontrole nad svojim početjem. Do leta 1994 je ustvaril 250 milijonov dolarjev izgube. Vrhunec njegovih izgub je bil potres v mestu Kobe, takrat je v enem dnevu izgubil 75 milijonov dolarjev.

je povzročil izgubo v višini 1,3 milijarde dolarjev, kar je povzročilo propad banke Barings.

4) Nihče od njiju se z goljufijo ni okoristil osebno.

Podoben primer se je zgodil ameriški poslovalnici banke Daiwa. Bančni delavec Toshihide Iguchi je 11 let skrival izgube, ki so nastale na podlagi poslovanja z obveznicami. Iguchi je imel vpogled v zaledno pisarno in v trgovalni del. Izguba je dosegla višino 1,1 milijarde dolarjev. Leta 1995 je svojo izgubo razkril svojim nadrejenim, ki pa so jo prikrili ameriškim regulatorjem. Ko so ameriški regulatorji ugotovili, da jim je Daiwa Bank prikrila izgubo v višini 1,1 milijarde dolarjev, ji je prisodila 340 milijonov dolarjev kazni ter prepovedala nadaljnje poslovanje te banke na ozemlju Združenih držav Amerike (Mishkin, 2001, str. 238).

Takih primerov je še veliko; za nekatere vemo za druge ne. O njih se govori šele zadnja leta, ko je Baselski komite podpisal nov Baselski sporazum, v katerem je opredeljeno operativno tveganje, kaj ga sestavlja ter kako ga merimo.

V spodnji tabeli je navedenih še nekaj podobnih primerov, kjer so banke/podjetja izgubljala milijone dolarjev, ker so preveč zaupala svojim zaposlencem in niso dovolj kontrolirala njihovega poslovanja.

TABELA 1: Največje trgovalne izgube kot posledica (ne)obvladovanja operativnega tveganja

PODJETJE	IZGUBA (v USD)	LETO	ZAKAJ
Našteto finančnih institucij ter ostala podjetja	20.000.000*	2001	Teroristični napad na World Trade Center-ZDA. Veliko število civilnih žrtev ter propad številnih podjetij in ne samo bank.
Tokio Shinkin Bank	2.300.000.000	1990-1991	Od julija 1990 do avgusta 1991 je manager podružnice te banke pozabil 19 certifikatov v vrednosti 416 bilijonov jenov. Ti certifikati so bili namenjeni borznim operacijam v skupni vrednosti 172,5 bilijonov. Vrednost pozabljenih certifikatov je tako dosegla celotno vrednost depozitov te banke. Banka je v letu 1992 propadla.
Banca Nazionale del Lavoro	1.800.000.000	1992	Bivši zaposlenci so bili obtoženi posojanja nedovoljenih posojil v Irak.
Daiwa bank	1.100.000.000	1983-1995	Izguba zaradi nepooblaščenih in nekontroliranih prenosov denarja v korist zaposlenca.
Barings	1.300.000.000	1995	Dogodek, ki je banke naučil osnove operativnega tveganja. Izguba zaradi nezadostne notranje kontrole in notranje revizije, ki je povzročila propad Barings banke. Nick Leeson je bil v poziciji, kjer je lahko skrival milijonske izgube na posebnem kontu, ki ga nikoli nihče ni odkril (vse do propada).

* Začetna ocena

Vir: Hoffman, 2002, str.27.

Zaradi deregulacije in globalizacije finančnih storitev ter vedno večje sofisticiranosti finančnih tehnologij postaja poslovanje bank bolj kompleksno. Z razvijanjem bančne prakse

in različnih postopkov se v bankah, ki so mednarodno dejavne, poleg kreditnega in tržnega tveganja pojavljajo tudi druga tveganja; obrestna in valutna tveganja ter tudi operativno tveganje. Vedeti moramo, da se banke čedalje bolj zavedajo nestabilnosti poslovnega sveta, saj je s tem ogrožena stabilnost njihovega poslovanja. Vprašljiva je tudi zvestoba zaposlencev in pravilnost delovanja naprednih sistemov, ki jih poznamo danes.

Zaradi uporabe bolj avtomatiziranih postopkov bančnega poslovanja se lahko tveganja napak pri ročni obdelavi pretvorijo v tveganja sistemskih napak, ker se bolj naslanjamo na celovito povezane sisteme. Tudi povečan obseg elektronskega poslovanja prinaša s seboj morebitna tveganja (prevare od zunaj in vprašanja varnosti sistema), ki jih v celoti še ne poznamo. S pojavom bank, ki delujejo kot ponudniki in izvajalci zelo obsežnih storitev, se ustvarja potreba po nenehnem vzdrževanju visoke stopnje notranjih kontrol in dodatnih varnostnih sistemov.[2]

Operativno tveganje se po vsebini zelo razlikuje od drugih vrst tveganj (valutno, kreditno), saj se pojavlja pri običajnem poteku poslovnih aktivnosti banke, kar močno vpliva na značaj procesa upravljanja z njim.

Termin operativno tveganje ima lahko v bančni industriji različne pomene: za interne potrebe lahko banka celo prevzame lastno definicijo operativnega tveganja. Kakršnakoli že je uradna definicija operativnega tveganja, je za učinkovito upravljanje in nadzor nad njim bistveno, da banke razumejo, kaj le-ta sploh je. Pomembno je, da banke upoštevajo vse vrste operativnega tveganja, s katerimi se srečujejo, in glede na to locirajo vse najpomembnejše razloge za nastanek velikih izgub zaradi operativnega tveganja.

1.1. DEFINICJA OPERATIVNEGA TVEGANJA

Operativno tveganje je definirano kot »tveganje izgube kot posledica neprimernega ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi ali delovanja sistemov oziroma zaradi zunanjih dejavnikov« (Baselski komite za bančni nadzor, 2001). Definicija vključuje pravno tveganje in izključuje strateško tveganje ter tveganje izgube ugleda. [3]

[2] Nova Ljubljanska banka ima veliko ponudb, kako plačevati, spremljati stanje na bančnem računu. Govorimo o Teledomu, Kliku, Mobi,… Da zagotovi popolno varnost mora veliko časa in denarja nameniti varnosti ter notranjim kontrolam. Banki se lahko kadarkoli poruši sistem oziroma varnost. Že v začetni fazi uvajanja transakcijskega računa so se ji dogajale neprijetnosti z zagotavljanjem varnosti.

[3] Postavlja se vprašanje, zakaj tveganje ugleda ni vključeno v samo definicijo operativnega tveganja. Če pogledamo primer treh večjih japonskih bank, ki so se združile, bi lahko šteli izgubo ugleda v eno izmed kategorij operativnega tveganja. Zaradi nekompatibilnosti njihovih informacijskih sistemov so imeli pred implementacijo skupnega inforamcijskega sistema nemalo težav pri povezovanju in postavljanju skupne baze podatkov. Ko so nov sistem uvedli v produkcijo, so zaradi premajhne testiranosti programov nastale težave pri bankomatih, komitenti so s težavo dvigovali svoj denar,.. ugled banke je bil močno načet in tako se postavlja vprašanje, zakaj tveganje izgube ugleda ni eno izmed dejavnikov operativnega tveganja. Tveganje izgube ugleda vsebuje vse dejavnike operativnega tveganja: združitev bank, napake v informacijski tehnologiji, napake pri vodenju notranjih procesov (The new Basel Capital Accord, 2001, str.120).

Če želimo definicijo operativnega tveganja razumeti, jo moramo razdeliti na več delov in jo na podlagi te delitve tudi razlagati. Vsi »glavni akterji« definicije (procesi, ljudje, sistemi ter zunanji dejavniki) pomembno vplivajo na operativno tveganje in jih moramo razumeti, če ga želimo analizirati (Hoffman, 2002, str. 41-47). V Tabeli 2 so zbrani dejavniki, ki vplivajo na operativno tveganje

TABELA 2: Kategorije tveganj, primeri ter odgovornosti

KATEGORIJE TVEGANJA	PRIMERI	ODGOVORNOSTI
LJUDJE	Človeške napake, notranja nepoštenost.	Kadrovska služba, varnostna služba.
ODNOSI	Pravna in pogodbena nesoglasja.	Prodajna in nabavna služba, management, pravna služba.
TEHNOLOGIJA IN PROCESI	Sesutje programa zaradi virusov, povečanje stroškov zaradi neprimernega programa.	Tehnološki oddelek v podjetju, infrastruktura podjetja, podatkovni center.
OSNOVNA SREDSTVA	Izguba sredstev zaradi naravnih katastrof ali neprimernega ravnanja z njimi.	Operativni management.
OSTALI ZUNANJI DEJAVNIKI	Spremembe zakonodaje ali zunanje kraje.	Varnostna služba, pravni oddelek.

Vir: Hoffman, 2002, str. 39.

1.1.1. RAVNANJA LJUDI

Ta del definicije je povezan z zaposlovanjem ljudi. Zaposlenci hote ali nehote povzročajo izgube v bankah[4].

a. Zaposlenčeve napake:
   - dokumentacijske napake,
   - programske napake,
   - cenovne napake.

Zaposlenčeve napake povzročijo motnje v poslovnem procesu podjetja; lahko so nehotene ali hotene. Vodstvo z dobrimi notranjimi kontrolami in križnimi sistemi preverjanja lahko dokaj hitro odkrije nehoteno zaposlenčevo napako. Težje je pri napakah, ki so storjene namerno in jih lahko že štejemo med naslednjo skupino možnih akterjev za pojavo operativnega tveganja v banki.

b. Zaposlenčeva hudodelstva:
   - notranja goljufija (vključuje na primer namerno napačno poročanje pozicij, krajo s strani zaposlenih, notranje trgovanje na račun zaposlenca),
   - kraja iz strankinega transakcijskega računa na zaposlenčev transkacijski račun.

[4] Primer: Decembra 1994 je okraj Orange County v ameriški zvezni državi Kaliforniji objavil izgubo v višini 1,6 milijarde dolarjev, ki je bila posledica premajhnega nadzora nad investiranjem zaposlenca Roberta Citrona, področnega blagajnika. (Hoffman, 2002, str. 42).

Zaposlenčeva hudodelstva povzročijo motnje v poslovnem procesu, ki se odražajo kot zaposlenčeva nepoštenost, nagnjenost k goljufiji ali zlobne aktivnosti proti banki.

c. Zaposlenčeva dostopnost:
   - izguba intelektualnega kapitala, ko ključni zaposlenec odide iz banke,
   - izguba intelektualnega kapitala zaradi smrti, poškodbe ključnega zaposlenca,
   - stavka zaposlencev.

Zaposlenčeva dostopnost se odraža predvsem kot nedosegljivost zaposlenca v ključnih trenutkih banke, ali pa na odhodu zaposlenca z delovnega mesta takrat, ko ga banka najbolj potrebuje.

d. Kadrovska politika podjetja:
   - neprimerna terminologija,
   - spolna, rasna diskriminacija,
   - zaposlovalna diskriminacija.

Kadrovska politika podjetja lahko banki povzroči ogromne izgube; predvsem zaradi diskriminacije, raznega nadlegovanja zaposlencev ali kakšnih drugih kršitev človekovih pravic (zavarovanja, ugodnosti zaposlencev).

Zgoraj naštete točke so samo nekaj primerov najpogostejših napak, ki nastanejo zaradi človeškega faktorja.

1.1.2. DELOVANJE SISTEMOV, TEHNOLOGIJE

V drugo kategorijo tveganja uvrščamo tehnologijo, ki povzroča, da je poslovanje banke prekinjeno zaradi napake v sistemu. Lahko gre za zunanje motnje ali motnje znotraj samega sistema. Za operativno tveganje je bolj pomembno, kako motnje znotraj samega sistema vplivajo na tveganje banke.

a. Zunanje motnje

Zunanje motnje vsebujejo tveganje zaradi sistemske napake, ki se nahaja zunaj banke (izpad električnega toka). Na to tveganje banke skoraj nimajo vpliva in morajo nanj računati, saj se lahko pojavi nenadoma, zato je dobro, da si banka zagotovi varnostne mehanizme, npr. če pride do izpada električne energije, lahko zagon računalnikov preklopijo na dodatni generator.

b. Motnje znotraj samega sistema

Tukaj gre predvsem za napake na programski opremi, nezmožnost programa, da osveži podatke, računalniške viruse, neuspešno nadgradnjo programske opreme. [5]

[5] 26.novembra 1999 je motnja znotraj samega sistema povzorčila izgubo ugleda in denarno izgubo Banke Halifax. Njihov internetni menjalni sistem, Sharexpress, je doživel varnostno verzel. Varnostna verzel je dovolila uporabniku programa Sharexpress, da je videl podatke o vseh uporabnikih tega programa. Vsak uporabnik progama je lahko trgoval preko drugih računov. Napaka je nastala zaradi kombinacije faktorjev nadgradnje sistema, ki pa jih le-ta ni razumel. Napaki bi se lahko izognili, če bi takrat bolj poznali e-bančništvo. Iz banke so takoj po ugotovitvi napake pozvale svoje komitente, da preverijo

1.1.3. OSNOVNA SREDSTVA

V to kategorijo uvrščamo računalniško in pisarniško opremo, ki jo imajo posamezne banke, in oprema ima za banko kar precejšno vrednost.

Osnovna sredstva so izpostavljena poškodbam ali celo uničenju, ki ga lahko povzročijo naravne nesreče (požari, poplave, potresi), lahko pa je rezultat nemarnega ravnanja zaposlencev; npr. neredno ali slabo vzdrževanje. Pred poškodbami pri naravnih nesrečah se lahko zaščitimo, tako da sredstva zavarujemo pri zavarovalnici (glej šesto poglavje). Pred uničenjem opreme zaradi neprimernega ravnanja zaposlenca pa se ne moremo zaščititi.

1.1.4. ZUNANJI DEJAVNIKI (zunanje goljufije, zakonske spremembe)

V zadnjo kategorijo sodijo predvsem dejavnikih, ki niso odvisni od obnašanja zaposlencev. Tukaj gre za goljufije tretjih oseb (kraja, špekulacija) ter učinke sprememb zakonodaje. Ti dejavniki za samo operativno tveganje niso tako zelo pomembni.

Na splošno lahko rečemo, da »operativno tveganje« obsega pretežno splošna in poslovna tveganja, ki lahko izvirajo iz napak ali pomanjkanja ustreznega nadzora nad dokumentacijo, postopki, izvedbo in knjiženjem poslovnih dogodkov ter splošno iz vseh drugih tveganj, ki jim je banka izpostavljena pri opravljanju svoje dejavnosti.

Podrobna klasifikacija škodnih dogodkov iz naslova operativnega tveganja se nahaja v Prilogi 1. V tej klasifikaciji najdemo opis dogodkov na dveh nivojih. Prvi nivo je široko zastavljena kategorija (notranja in zunanja goljufija,varstvo pri delu). Drugi nivo razdeli prvega na več delov ter pri vsaki podkategoriji opredeli, katere vrste škodni dogodki spadajo v določeno kategorijo.

Zaradi boljše preglednosti ter pomena operativnega tveganja je ta klasifikacija vsaki banki lahko v veliko pomoč.

1.2. UMESTITEV OPERATIVNEGA TVEGANJA V ORGANIZACIJSKO STRUKTURO PODJETJA

Preden banka začne izvajati ukrepe uravnavanja operativnega tveganja, se mora soočiti s problemi, ki jo čakajo. Le-ti so povezani z merjenjem tveganja, z orodji, ki so namenjena

---

na svojih računih, če je vse v najlepšem redu. Napaka je povzročila škodo pri desetih komitentih banke, vendar škoda ni bila prevelika. Ta problem je zelo vplival na sam ugled Halifax banke, ker se je oglaševala kot vodilna e-banka in si take napake v sistemu ne bi smela privoščiti. Rezultat te napake je bil, da so nekateri komitenti zapustili banko in s tem naredili negativno reklamo za samo banko (Hoffman, 2002, str. 45).

merjenju operativnega tveganja, raznimi kalkulacijami. Ker vsaka banka zahteva drugačen pristop do uveljavljanja operativnega tveganja, mora razmisliti o organizacijski kulturi in klimi zaposlencev.

Operativno tveganje prinaša banki veliko izgub, zato mora biti cilj vsake banke zmanjšanje le-teh. Kot smo že na začetku omenili, se v zadnjem času dogaja, da banke naredijo veliko izgub zaradi operativnega tveganja, vendar če banka želi nanj vplivati, mora razumeti, kaj vpliva na pojav tveganja, kakšne izgube ima zaradi njega, kako ga lahko meri (izsledi), kako se lahko pred njim zavaruje.

Uspešnost banke se kaže tudi v tem, kako uspešno je umestila kategorijo operativnega tveganja med svoje zaposlence in kako ji ga je uspelo zmanjšati. Novi Baselski sporazum zahteva, da vsaka banka poveča svojo kapitalsko ustreznost za nivo operativnega tveganja, ki ga izmeri.

Najtežje pri uravnavanju operativnega tveganja je samo merjenje ter ugotavljanje le-tega. Nekatere kategorije tveganja so na žalost opisne narave in so težko izmerljive.[6]

Na začetku mora banka rešiti dva osnovna problema, s katerima se sreča pri umeščanju operativnega tveganja v proces poslovanja in odločanja (Advances in operational risk, 2003, str. 78-81):

a) razdrobljenost,
b) terminologija.

1.2.1. RAZDROBLJENOST (Granularity)

Prvi problem je razdrobljenost (Granularity). Operativno tveganje se pojavlja na vseh nivojih banke, zato se mora odločiti, kako »globoko« bo šla v pridobivanju informacij v samo organizacijsko strukturo banke. Ali bo to na nivoju celotne banke (najvišjem nivoju) ali na nivoju posameznih sektorjev ali znotraj posameznega sektorja (najnižjem nivoju).

Logično je, da globlje, ko gremo v samo organizacijo, višje stroške imamo in več časa nam vzameta zbiranje informacij in analiza zbranih podatkov.

Tako na primer zbiranje informacij na najvišjem nivoju zahteva veliko »ročnega« dela, kot so intervjuji, vprašalniki, ankete in druga orodja za pridobivanje informacij. Pri tem lahko pride do napak in površnosti. To pomeni, da je potrebno pri najvišjem nivoju zbiranja informacij biti zelo natančen, da ne pride do nepotrebnih napak in s tem do ponavljanja izvedbe analize.

[6] Primer težko izmerljivega tveganja so predvsem tveganja, ki so povezana s samimi zaposlenci. Kako izmeriti operativno tveganje, če nam zaposlenec goljufa s čeki in to ustrezno zakrije? Banka na žalost tega ne more odkriti, če ima slabo notranjo kontrolo. Kako se banka zaščiti? Baselski odgovor na to vprašanje bi verjetno bil z višjo kapitalsko ustreznostjo banke. Kako naj banka izmeri takšno tveganje; goljufija s čeki? Odgovor je v nadaljevanju.

Zbiranje informacij na najnižjem nivoju pa pomeni veliko kompleksnejše delo in tudi dražje. Tu morajo tisti, ki zbirajo informacije, zelo dobro poznati organizacijsko strukturo banke in njihove značilnosti. Imeti morajo popolno podporo vodstva in zaposlencev. Na razpolago morajo imeti ustrezni podatkovni model, na podlagi katerega zbirajo potrebne informacije.

Banka se mora tu zavedati pomena stroškov in rezultatov pridobljenih s pomočjo analize na različnih nivojih. Ni rečeno, da globlje ko bo šla v organizacijo, da bo dobila boljše rezultate. Torej banka mora vedeti, kakšne rezultate bo dobila z ustrezno raziskavo operativnega tveganja na različnih nivojih bančne organizacijske strukture (Advances in operational risk, 2003, str. 78-81).

Tu se Basel zavzema za čim bolj podrobno analizo tveganja v bankah (zbiranje informacij znotraj posameznega sektorja), saj drugače banka ne bo mogla zadovoljiti ustreznim kapitalskim zahtevam (več o tem v petem poglavju). Videli smo, da se operativno tveganje nahaja v vsaki stopnji poslovanja, zato mora banka zelo dobro poznati organizacijsko strukturo, da lahko ugotavlja tveganje.

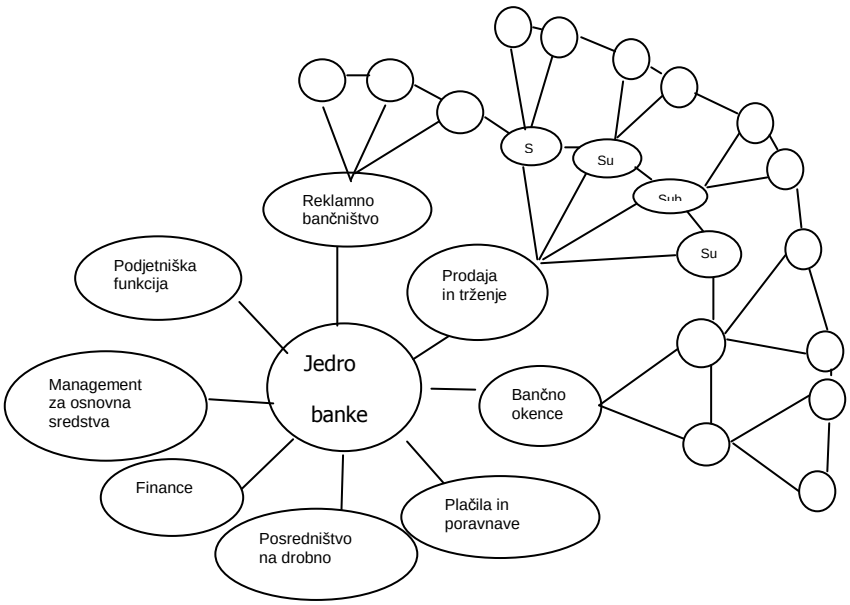
Da banka pridobi določeno kontrolo nad posameznim delovnim mestom, mora uvesti sistematizacijo delovnih mest, kajti samo tako lahko ugotavlja, kje in v kakšnem obsegu se lahko v organizacijski strukturi pojavi operativno tveganje.

Če ima banka dobro razdelano organizacijsko strukturo in sistematizirana delovna mesta, bo lažje odkrivala ter definirala kategorije operativnega tveganja (glej Prilogo 1).

Delovno mesto, ki je zadolženo za operativno tveganje, mora razviti metodo, kako ostati v stiku z zaposlenci in tako izvedeti kar največ o dogajanju v sami banki. Da je ta stik mogoče obdržati, je teorija razvila t.i. »operational risk membrane« (glej Sliko 1, na str. 10). Membrano sestavljajo ljudje, ki so zaposleni v posameznem sektorju banke, specializirani so za določena področja; npr. pravo, IT, prodajo, nabavo, računovodstvo, revizijo. Skupaj z vodstvom operativnega tveganja se dobivajo na kolegijih, kjer razpravljajo o napakah, poročajo o rezultatih merjenj.

Membrana operativnega tveganja zelo lepo prikazuje, kako mora biti banka organizirana, da zadosti kriterijem operativnega tveganja. Vsaka bančna enota o dogajanju poroča vodji in vodja to poroča naprej vodstvu. Seveda mora imeti vsaka banka notranje kontrole, ki se vzpostavijo takrat, ko se dela samo sistematizacijo delovnih nalog. Notranje kontrole so pomembne, ker pomagajo pri odpravljanju napak s strani programov ter s strani zaposlencev. Pri sami vzpostavitvi notranjih kontrol banki pomaga notranja revizija, ki ima podoben pomen kot samo delovno mesto, ki je zadolženo za operativno tveganje.

SLIKA 1: Membrana operativnega tveganja (Operational risk membrane).



Vir: Advances in operational risk, 2003, str. 77.

Notranja kontrola je stalen proces, ki ga oblikujejo tako uprava, poslovodstvo kot tudi drugi zaposlenci. Njen namen je zagotavljati izpolnitev ciljev glede uspešnosti in učinkovitosti poslovanja banke, zanesljivosti finančnih poročil in izpolnjevanja veljavnih predpisov (Priporočila za vzpostavljanje in izvajanje sistema notranjega nadziranja v bankah).

Med notranjo kontrolo spada tudi notranja revizija, katere namen je zagotavljanje ustreznosti in učinkovitosti organizacijskih in postopkovnih kontrol ter njihovo izvajanje. Notranja revizija mora spremljati dogajanje znotraj same banke, poznati mora informacijski sistem ter vse povezave med zaposlenci, če želi uspešno izvajati svoje naloge. Glavna naloga notranje revizije je ocenjevanje notranjih kontrol in s tem prispevanje k povečevanju učinkovitosti le-teh. Napačno je misliti, da je notranja revizija lahko nadomestilo za delovno mesto, ki je zadolženo za operativno tveganje.

Delovno mesto, ki je zadolženo za operativno tveganje, mora samo vzpostaviti notranje kontrole in preko le-teh merjenje operativnega tveganja. Notranja revizija opravlja sam nadzor in povezave med njimi, zato morata ti dve delovni mesti tesno sodelovati drugo z drugim, kajti brez tega sodelovanja se banka ne more zavarovati pred tveganjem.

Težave, na katere naletimo pri notranji kontroli in reviziji, so zelo pogoste predvsem s strani zaposlencev, ki se zaradi tega počutijo zapostavljene, zato mora vodstvo banke pri vzpostavljanju le-teh upoštevati tudi njih ter njihove želje.

1.2.2. TERMINOLOGIJA (Terminology)

Problem pri upravljanju z operativnim tveganjem je v pridobivanju informacij in v organiziranju banke, da bi delovala v okviru odpravljanja operativnega tveganja. Banke bi morale identificirati vse vrste operativnega tveganja, s katerimi se soočajo, pri tem morajo upoštevati tako interne kot zunanje faktorje. Na začetku morajo definirati navodila, po katerih se bo vzpostavljalo upravljanje s tveganjem. Navodila morajo definirati točke, različne elemente okvirnega plana operativnega tveganja ter povezave med njimi, vsebovati morajo primere, definicije, razlage terminologije, komunikacijske kanale, kategorije operativnega tveganja, odgovornosti ter potrebe poročanja. Njihov najpomembnejši element mora biti poročanje, predvsem je potrebno definirati kaj, kdo, komu ter kako poroča (Advances in operational risk; 2003, str. 78-81).

Banka ne sme nikoli pozabiti, da je lahko vsak njen zaposlenec vir operativnega tveganja, poleg njega pa tudi sami poslovni procesi in zunanji dejavniki. Zato mora določiti interna pravila, ki morajo biti zelo podrobna in jih morajo upoštevati vsi zaposlenci.

Na začetku mora banka sestaviti ekipo ljudi, ki bo zadolžena za odkrivanje operativnega tveganja. Ta ekipa mora biti neodvisna in samostojna enota v banki. Imeti mora podporo vodstva banke; natančno morajo določiti okvire, v katerih bodo delovali. Predvsem morajo določiti metode merjenja in odpravljanja operativnega tveganja.

Ekipa mora imeti tako finančno kot vidno podporo vodstva. S finančno podporo mislim predvsem na denarno pomoč pri razvoju orodij za odkrivanje operativnega tveganja. Z vidno podporo pa na to, da mora vodstvo banke narediti vse, da merjenje in odkrivanje operativnega tveganje postane sestavni del banke oziroma del njene kulture.

Ekipa mora vedno skrbeti za to, da vodstvo podjetja vsak trenutek ve, kaj in na kakšen način se dela ter je seznanjeno z rezultati dela.

Ko so odnosi med ekipo operativnega tveganja in vodstvom banke urejeni, se je potrebno odločiti, kako jo umestiti v organizacijsko strukturo banke, da bo kar se da učinkovita in bo lahko pridobila kar največ informacij.

Zavedati se mora, da podpora vodstva ni dovolj za uspešno in učinkovito izvajanje merjenja ter analiz. Delovati mora med zaposlenci, jih podpirati, zato da od njih dobi dobre in učinkovite informacije. Sodelovanje z zaposlenci je pomemben del predvsem zato, ker so izvajalci sprememb, ki nastanejo zaradi operativnega tveganja.

2. VZPOSTAVITEV PODATKOVNEGA MODELA

2.1. BAZA PODATKOV ZA OPERATIVNO TVEGANJE

Ustrezne baze podatkov o izgubah iz naslova operativnega tveganja so ključnega pomena pri razvijanju učinkovitega upravljanja z operativnim tveganjem. V svetu so banke večinoma šele na začetku sistematičnega zbiranja relevantnih podatkov o operativnem tveganju.

Opredelitev, primerjava in tolmačenje relevantnih podatkov iz operativnega tveganja na nivoju banke ali bančne skupine predstavljajo znaten izziv vsakemu bančnemu analitiku, ki se ukvarja s tovrstno problematiko. Uspešen razvoj okvira operativnega tveganja zahteva tri korake (Cruz, 2002, str. 10):

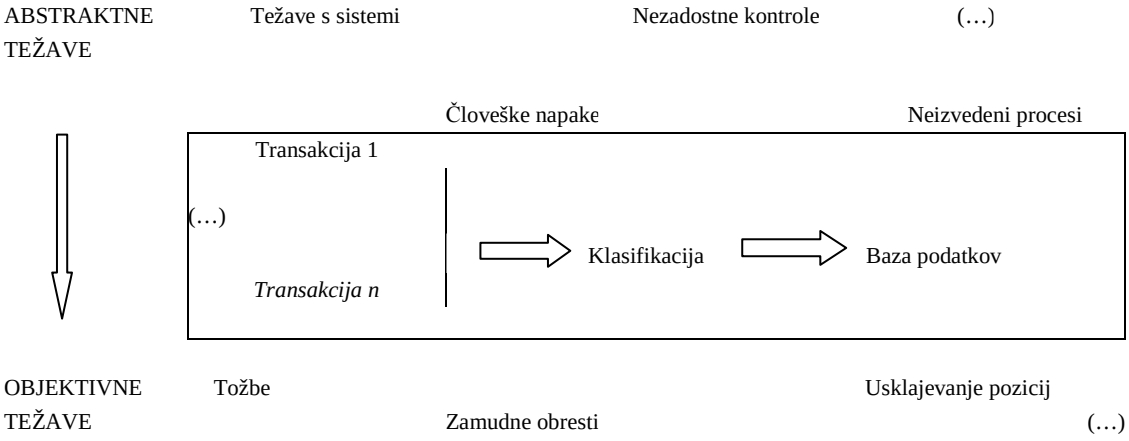
- vzpostavitev dosledne definicije vsake vrste operativnega tveganja (o tem smo govorili v prvem poglavju - terminologija), ki mu je banka izpostavljena, ter identifikacija podatkov, ki so v zvezi s posamezno vrsto tveganja pomembni za banko, je prav gotovo temeljni korak;
- šele na tej podlagi lahko banka v drugem koraku razvije in implementira ustrezen mehanizem za zbiranje definiranih podatkov. Gre za zelo zahteven proces, ki zahteva popolno podporo uprave banke ter višjega managementa;
- ko je ta proces zaključen, mehanizem pa vzpostavljen, čaka različne ravni vodstva še ena pomembna naloga, ki pogojuje učinkovito upravljanje z operativnim tveganjem - naučiti se tolmačiti izhodno informacijo ter jo hkrati prevesti v oceno stopnje posamezne vrste operativnega tveganja, ki mu je banka izpostavljena.

2.1.1. KLASIFIKACIJA ŠKODNIH DOGODKOV IN NJIHOVIH VZROKOV

Vsak analitik bo pri načrtovanju postopkov merjenja operativnega tveganja na začetku posvetil največ časa problemu transformacije podatkov iz operativnega tveganja v obliko, ki bo primerna za analizo. Na tej stopnji je potrebno opredeliti, katere informacije so potrebne in pomembne za učinkovito upravljanje z operativnim tveganjem.

Običajna klasifikacija vzrokov iz operativnega tveganja zajema zgolj kategorije, kot so »težave v zvezi s sistemi« ter »nezadostne kontrole«, kar lahko v praksi vodi do napačnega in dvojnega zajemanja podatkov. Ustreznejša klasifikacija opredelitve škodnih dogodkov bo na primer upoštevala, da vse »težave s sistemi« nimajo vpliva na izgubo oziroma dobiček. Prav zaradi tega je treba klasificirati škodne dogodke na podlagi njihovih posledic, kar pa je v praksi bolj težko izvedljivo. To pomeni, da bo banka potrebovala razvrstitev izgub na elemente, ki neposredno vplivajo na finančni rezultat (pravne zadeve, zamudne obresti).

SLIKA 2: Oblikovanje baze podatkov za operativno tveganje



Vir: Cruz, 2002, str. 10.

Naslednja odločitev, ki jo mora analitik sprejeti pri modeliranju vsebine baze podatkov, je povezana s pristopom pri klasifikaciji škodnih dogodkov. Slednja je lahko namreč izvedena z vidika posameznega procesa ali pa z vidika sistema kot celote. Modeliranje vsebine z vidika posameznega procesa je lahko dokaj neučinkovito, saj imajo večje banke ponavadi tudi po več tisoč procesov, ki jih je treba preučiti in obdelati, to pa je dokaj nerealen cilj. Morda je lažji obraten pristop – to je izbira določenega števila tipičnih operativnih napak, ki se v banki dogajajo, in preučitev, kako se odrazijo v procesih banke. Če se v določenem procesu pogostokrat dogajajo škodni dogodki iz operativnega tveganja, ki pa za banko nimajo resnejših finančnih posledic, se lahko klasifikacija teh škodnih dogodkov pusti za drugo ali kasnejšo fazo modeliranja vsebine baze podatkov.

Povedano bolj velja za manj kompleksne pristope (enostavni ter standardizirani), kjer se bo podatke o operativnem tveganju zbiralo zgolj zaradi managerskih potreb po vzdrževanju ustreznega pregleda nad operativnim tveganjem v banki. Pri uporabi kompleksnejših pristopov (napredni pristopi), kjer bodo podatki o izgubah in škodnih dogodkih služili tudi kot vhodni podatki v statistično-matematične modele izračunavanja in distribucije ekonomskega kapitala po poslovnih področjih, pa mora analitik sprejeti tudi odločitve glede stopnje kompleksnosti podatkovnega modela.

2.1.2. OBLIKOVANJE PODATKOVNEGA MODELA

Vzpostavitev trdnega in ustreznega podatkovnega modela je temelj učinkovitega sistema merjenja in upravljanja z operativnim tveganjem v banki. Zato je na tej stopnji definiranja vrst izgub, ki bodo predmet aplikativne obravnave in posledično podatkov o realiziranih in potencialnih škodnih dogodkov, ki se bodo zbirali znotraj organizacije, bistvenega pomena – natančnost. Natančnost je pomembna zaradi neločljive povezanosti operativnega tveganja s posameznimi delovnimi področji v banki, ki so z vidika merjenja in kontroliranja tveganja

zelo različna. Pri razvoju podatkovnega modela za operativno tveganje se bo moral analitik lotiti nekaterih temeljnih vprašanj, ki jih opisujem v nadaljevanju (Cruz, 2002, str. 11-12).

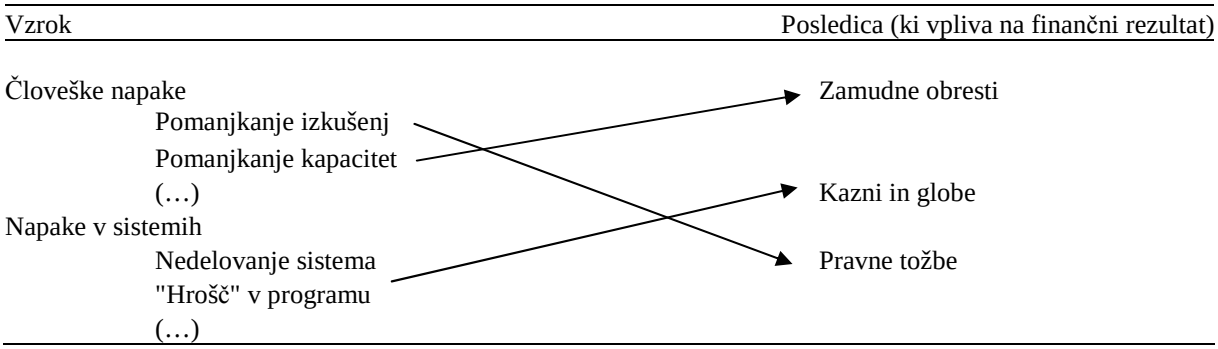
1. Klasifikacija glede na neposredne in posredne izgube

Neposredne izgube so tiste, ki imajo neposreden vpliv na finančni rezultat; to je npr. plačilo globe nadzorniku zaradi določenih nepravilnosti pri poslovanju. Posredne izgube pa so tiste, ki nastanejo zaradi nekega drugega, posrednega vzroka. Zaradi okvare sistema v popoldanskih urah se na primer vrsta transakcij ne(pravilno) poravna. To ima lahko za posledico nastanek tveganja izgube dobrega imena banke, odškodninske zahtevke po zamudnih obresti ipd., kar ima posreden učinek na finančni rezultat banke. V prid ustreznega pregleda nad operativnim tveganjem mora analitik izdelati sistem učinkovite obravnave obeh vrst izgub.

2. Klasifikacija glede na vzroke in posledice škodnih dogodkov

V praksi se pogosto zamenjuje vzroke in posledice škodnih dogodkov iz naslova operativnega tveganja. Klasifikacija, ki temelji samo na vzrokih, je nagnjena k napakam in nesporazumom, zlasti pri obravnavi velikega števila škodnih dogodkov. V slednjem primeru je namreč zelo težko razlikovati med napakami, ki jih je povzročil sistem, in napakami, ki jih je povzročil »človek«, še zlasti, če se človeško napako pri vzroku klasificira kot »neizkušenost« ali »pomanjkljivo kontrolo«. Pri tej stopnji se je treba izogniti subjektivni oceni škodnih dogodkov, kar se najlažje doseže s hkratno obravnavo vzrokov in posledic.

SLIKA 3: Razmerje med vzroki in posledicami istovrstnih škodnih dogodkov



Vir: Cruz, 2002, str. 12.

Pri tem je treba upoštevati, da ima lahko vsak iz podatkov o izgubi različne lastnosti, ki izhajajo iz različnih dejavnikov. Posamezen niz podatkov se lahko nanaša na posamezno vrsto tveganja, na različna poslovna področja in lahko izvira iz različnih sistemov ali procesov. Tveganje lahko lažje merimo, če so ti dejavniki merljivi, oziroma če jih lahko kako ovrednotimo. Ker jih ne moremo, jih lahko opisno merimo z različnimi metodami. To so v glavnem ocenjevalne lestvice, na podlagi katerih določimo, ali je posamezna aktivnost bolj ali manj tvegana.

2.1.3. PODATKI O ŠKODI IN POMEMBNOSTI ZAJEMANJA PODATKOV NA NIVOJU ŠKODNEGA DOGODKA

Priporočljivo je, da je baza podatkov za operativno tveganje modelirana na nivoju posameznih transakcij, kar v osnovi pomeni na nivoju posameznih škodnih dogodkov. Banka torej ne bo zbirala teh podatkov na nivoju tedenskega ali celo mesečnega agregatnega zbira transakcij. Modeliranje operativnega tveganja sicer temelji na dveh procesih – frekvenci in resnosti škodnih dogodkov kot dvema ključnima elementoma potrebovanih nizov podatkov o škodi. Frekvenca kaže, kako pogosto se realizira posamezen dogodek, resnost pa se odraža pri vplivu na finančni rezultat banke. Kljub temu pa je za managerja bistvena informacija, kdaj in zakaj se je zgodil posamezen škodni dogodek. Zaradi izračuna deleža izgube, ki ga nosi posamezen škodni dogodek, je potrebno identificirati glavni vzrok izgube iz operativnega tveganja.

PRIMER
Borzni posrednik je zaprl določen posel ob naslednji poziciji:

Nakup	100.000.000 USD po 0,9 EUR	= 90.000.000 EUR,
Prodaja	100.000.000 USD po 0,9005 EUR	= 90.050.000 EUR,
Dobiček		= 50.000 EUR.

Obe transakciji sta bili izvedeni istočasno, tako da je bil posrednik zadovoljen z realiziranim dobičkom. Zatem pa se zgodita dve napaki:
1. napačno poročanje o zneskih transakcij,
2. napaka pri poravnavanju transakcij v zaledni službi.

Ti dve napaki povzročita, da se transakcija izvede šele tri dni kasneje, kot bi se morala. Nasprotne stranke v poslu so zaradi tridnevne zamude zaračunale 55.000 EUR kazni, kar pomeni, da je banka v bistvu realizirala skupno izgubo v višini 5.000 EUR. Zaradi neučinkovitega merjenja operativnega tveganja te napake niso bile sistemsko povezane z vzroki njihovega nastanka, saj so se zgodile šele določen čas po zaključku posrednikovega posla. To pomeni, da se je izguba sicer zavedla na določenih kontih izrednih odhodkov, vendar podatek o dejanskih povzročiteljih izgub ni bil zaveden nikjer (Cruz, 2002, str. 12).

Zajemanje podatkov na nivoju posameznih škodnih dogodkov je priporočljivo tudi zaradi učinkovitejšega pregleda nad pričakovanimi in nepričakovanimi izgubami in s tem boljšim upravljanjem s tveganjem na posameznih poslovnih področjih. Operativne izgube so namreč neločljivo povezane tako s poslovnim procesom kot tudi s stabilnostjo okolja, v katerem banka posluje.

3. UPRAVLJANJE OPERATIVNEGA TVEGANJA

Sedaj, ko smo se seznanili s tem, kar vpliva na operativno tveganje, si lahko postavimo vprašanje, zakaj bi se banke sploh ukvarjale z operativnim tveganjem. Odgovor na to vprašanje ni enostaven. Za upravljanje različnih vidikov operativnega tveganja banke potrebujejo dostop do vrhunskih znanj s področja IT tehnologije oz. IT varnosti, kadrovskega managementa in pravnih vprašanj. Za banko je zelo dobro, če zna vsa ta znanja povezati v okvir operativnega tveganja.

Cilj upravljanja z operativnim tveganjem je zmanjševanje frekvence in resnosti škodnih dogodkov iz operativnega tveganja. Za finančno institucijo predstavlja ta cilj dva vodstvena izziva – osredotočenje na škodne dogodke vrste »nizka frekvenca/visoka izguba« ter na škodne dogodke vrste »visoka frekvenca/nizka izguba« (Rotovnik, 2004, str. 1).

TABELA 3: Izzivi na področju upravljanja z operativnim tveganjem

	MAJHNE IZGUBE	**VELIKE IZGUBE**
MAJHNA FREKVENCA	Ni pomembno …	PRVI IZZIV: ° propad banke ali izguba ugleda; ° težko razumeti in postaviti prioritete; ° podobnosti s problematiko iz operativnega tveganja v drugih industrijah (letalstvo, farmacija,…).
VISOKA FREKVENCA	DRUGI IZZIV: ° na splošno ne predstavlja grožnje banki; ° z izkušnjami je lažje razumeti težave, meriti tveganje ter ustrezno ukrepati; ° lahko se vključi v oblikovanje cene produkta (npr. kartične prevare).	Ni relevantno … (če bi bilo, bi že prenehali s poslovanjem).

Vir: Rotovnik, 2004, str. 1.

Primarni izzivi so škodni dogodki vrste »nizka frekvenca/visoka izguba«, saj lahko močno vplivajo na kapital finančne institucije, predstavljajo grožnjo njenemu ugledu ter v najslabšem primeru povzročijo njen propad. Te dogodke je težko razumeti, saj se ponavadi realizirajo kot skupek različnih, medsebojno povezanih škodnih dogodkov, ki jih lahko povzroči skupina ljudi ali posameznik (Nick Leeson je kot posameznik s kopico škodnih dogodkov uspel povzročiti propad Barings banke).

Škodni dogodki vrste »visoka frekvenca/nizka izguba« predstavljajo za finančno institucijo na področju upravljanja z operativnim tveganjem sekundarni izziv. Ker taki 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 raznimi programi za zmanjševanje stroškov. Ti dogodki so ponavadi manjši in jih

lahko s podrobnim preučevanjem tudi preprečimo oziroma te izgube vgradimo v samo poslovanje banke.

Da banka lahko pride do ugotovitve, kateri škodni dogodek spada v katero skupino, mora opraviti proces, ki ga imenujemo upravljanje z operativnim tveganjem. Proces ima štiri stopnje (Advances in operational risk, 2003, str. 26):

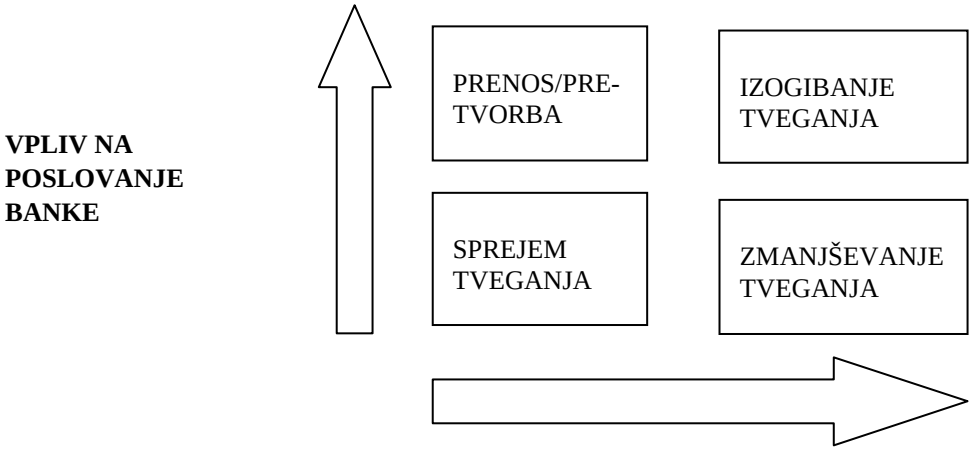
1. Ocenitev tveganja
Na začetku banke definirajo tveganje opisno; tako lažje ocenijo resnost tveganja, ki je lahko visoko, srednje in nizko. Kasneje bomo opisali, kako lahko merimo tveganje in na kakšen način ugotovimo, ali gre za visoko, srednje ali majhno. Ko ugotovijo, za kakšno od omenjenih vrst tveganja gre, se odločijo, ali bodo naredile tudi kvantitativne študije. Večje mednarodne banke se lotijo kvantitativnih študij v vsakem primeru, ne glede na višino tveganja.

2. Kontrola tveganja oziroma ublažitev le-tega
Ko je tveganje ocenjeno, imamo štiri možnosti za reševanje problema:

a) Izognitev tveganju
   Izogibanje reševanju problema, ko se tveganje pojavi ni najboljša rešitev, saj lahko pripelje še do slabšega položaja. Tako lahko zaradi izogibanja tveganju banka doživi propad ali velike izgube. Banke lahko izgubijo tudi licenco za opravljanje svoje dejavnosti, če nimajo primerne kapitalske ustreznosti. Do kapitalske neustreznosti lahko pripelje prav izogibanje reševanju zmanjševanja tveganja. Banke se izogibajo tveganju takrat, ko to bistveno ne vpliva na samo poslovanje banke, vendar morajo to tveganje vseskozi spremljati, da tveganje ne dobi razsežnosti visokega tveganja.
b) Zmanjševanje tveganja
   Zmanjševanje tveganja vodi v določene stroške; predvsem v tiste, ki so povezani z odkrivanjem tveganja, iskanjem rešitve ter končno s samo izvedbo reševanja. Banka si mora zastaviti vprašanje, ali se ji splača iskati rešitev, saj se na koncu lahko izkaže, da je bilo iskanje rešitve dražje od zmanjšanih stroškov iz naslova rešenega tveganja. Zato se mora banka, na podlagi odkritega tveganja odločiti, ali se ji splača zmanjševati tveganje in zapravljati sredstva za neko rešitev, ki ne bo obrodila sadov.
c) Prenos tveganja
   Tretja možnost, ki jo ima banka na voljo, ko odkrije tveganje, je prenos aktivnosti, ki povzroča tveganje.
d) Prevzemanje tveganja
   Zadnji korak, ki ga lahko banka naredi, ko odkrije tveganje je, da ga prevzame. To naredi tako, da preuči tveganje in temu prilagodi svoje poslovanje in kapitalsko ustreznost. Pri tem mora paziti, da ji tveganje ne uide iz nadzora. V vsakem trenutku mora vedeti, kako veliko je tveganje.

V praksi banke naredijo kombinacijo zmanjševanja, prevzema in transformacije tveganja. To je tudi najboljša rešitev. Banka prevzame tveganje tako, da prilagodi kapital, seveda poskuša z raznimi sredstvi zmanjšati tveganje, ali pa ga celo transformirati v drugo obliko.

SLIKA 4: Izbire pri koraku kontrole tveganja



Vir: Advances in Operational Risk; 2003, stran 29.

3. Ocenitev in analiza odstopanj/razhajanj

Tretji korak je raziskava ter ocenitev tveganja po izvedenem drugem koraku; torej gre za meritev tveganja, ki še ostane kljub kontroli tveganja (zmanjševanje, izogibanje, neukrepanje). Na tej stopnji želimo ugotoviti, ali je bilo tveganje, ki je ostalo, v višini pričakovanega.

4. Ponavljanje kroga »Upravljanje z operativnim tveganjem«

Prvi trije koraki upravljanja z operativnim tveganjem predstavljajo krog, ki ga mora banka, če želi priti do želenih rezultatov, večkrat ponoviti. Ker se kar naprej pojavljajo nova tveganja, mora banka imeti vzpostavljen standardizirani proces odkrivanja in reševanja problema operativnega tveganja.

4. METODE MERJENJA OPERATIVNEGA TVEGANJA

Banka mora identificirati in oceniti operativno tveganje pri vseh glavnih proizvodih, aktivnostih, procesih in sistemih; še posebej mora biti pozorna, ko uvaja nove proizvode, aktivnosti, procese in sisteme.

Za učinkovito spremljanje in nadzor operativnega tveganja je najpomembnejša identifikacija tveganja. Da je identifikacija tveganja učinkovita, mora vključevati tako interne faktorje (npr.: strukturo banke, naravo bančnih aktivnosti, kvaliteto človeških resursov, organizacijske

spremembe, fluktuacijo delovne sile) kot tudi zunanje faktorje (npr.: spremembe v industriji, tehnološki napredek), ki lahko neugodno vplivajo na doseganje bančnih ciljev.

Poleg identifikacije potencialno najbolj neugodnih tveganj mora banka oceniti tudi svojo občutljivost na ta tveganja. Učinkovito ocenjevanje tveganj omogoča banki boljše razumevanje svojega profila tveganosti in s tem učinkovitejše razporejanje resursov, ki so zadolženi za upravljanje s tveganji.

Orodja za identifikacijo operativnih tveganj lahko razdelimo na dve osnovni dimenziji in potem še znotraj vsake dimenzije. Prva dimenzija je primerjava metod merjenja od zgoraj navzdol in od spodaj navzgor (»top down versus bottom up« - high level portfolio-based views to specific bottom up processes), druga dimenzija je primerjava kvalitativnih metod proti kvantitativnim (»qualitative versus quantitative assessment«).

4.1. PRVA DIMENZIJA: STRATEGIJE OD ZGORAJ NAVZDOL PROTI STRATEGIJAM OD SPODAJ NAVZGOR

V procesu ocenjevanja operativnega tveganja se mora banka osredotočiti na svoje pomembnejše dele; to so tisti deli, ki bistveno vplivajo na poslovanje banke. Pri tej dimenziji ocenjevanja govorimo predvsem o obsegu. Različni ljudje v banki potrebujejo različne informacije o tveganju; tako bo na primer vodja poslovne enote potreboval specifične podatke o izpostavljenosti tveganju, vodja enote za tveganja na področju zavarovanja pa samo podatke glede na vrsto tveganja, ki se pojavlja v banki, da lahko naredi program zavarovanja pred njimi.

Ti dve strategiji predstavljata metode merjenja operativnega tveganja na dveh ravneh. Strategije od spodaj navzgor so metode, ki pomagajo meriti tveganje na osnovi posameznih poslovnih enot. Strategije od zgoraj navzdol pa so tiste, ki merijo tveganje na osnovi celotne banke; zato lahko govorimo o razdrobljenosti. Banka se sama odloči, katero metodo bo izbrala; izbira je odvisna od velikosti banke (koliko poslovalnic ima, kje so locirane) ter od tega, kje se tveganje največ pojavlja. Če se tveganje največkrat pojavi na ravni poslovnih enot, potem se banki splača meriti tveganje na posamezni poslovni enoti (glej Tabela 3, na strani 24).

Če želimo tveganje zelo dobro oceniti, je najbolje, da uporabimo kombinacijo obeh strategij, saj nam ena sama ne da zadovoljivih informacij. Strategije od zgoraj navzdol pogosto uporablja višje vodstvo (ocenitev tveganja na podlagi celotne banke-across business lines) za ocenitev širokega spektra tveganja ter za ocenitev tveganja celotne banke. Poleg njih jih uporabljajo tudi vodje posameznih poslovnih enot v banki, ki bi radi ocenili tveganje v svoji enoti. Ti se ukvarjajo predvsem z ugotavljanjem tveganja na podlagi vsakodnevnih aktivnosti v banki.

4.1.1. STRATEGIJE OD SPODAJ NAVZGOR

Strategije od spodaj navzgor so treh vrst. Vse tri se izvajajo na ravni poslovnih enot (business level scenarios analysis), uporabljajo jih za samoocenjevanje, neodvisno revizijo ter ocenjevanje tveganja s sodelovanjem. Z njihovo pomočjo vsaka poslovna enota lahko v vsakem času ve, kakšnemu obsegu tveganja je izpostavljena.

Problem, ki se pojavi pri teh strategijah, je, da so lahko zelo podrobne, zato vzamejo veliko časa za pripravo in analizo podatkov, na koncu pa se lahko zgodi, da izgubimo občutek velikosti tveganja ter občutek za stanje tveganja. Drugi problem, ki se pojavi pri teh strategijah, je, da so zaradi svoje podrobnosti ponavadi izpeljane oziroma analizirane preko svetovalcev in zunanjih sodelavcev namesto vodij poslovnih enot (business managerjev). To pa zato, ker se vodje poslovnih enot (business managerji) nimajo časa spuščati v take detajle, ki jih zahtevajo te vrste strategij.

Njihova prednost je prav v njihovih podrobnostih, ko lahko vsak vodja najde pravo oceno tveganja, na podlagi katere sprejme ukrepe za zmanjševanje tveganja.

4.1.2. STRATEGIJE OD ZGORAJ NAVZDOL

Zgoraj navzdol strategije so opisane kot strategije, ki definirajo potencialno tveganje za celotno banko (poslovanje, organizacija). Ne proučujejo dnevnih transakcij kot spodaj navzgor strategije.

Med te strategije štejemo uvrščanje tveganja na podlagi določenih scenarijev (risk mapping) in aktuarska strategija.

Uvrščanje tveganja na podlagi določenih scenarijev je ena izmed najstarejših metod, ki se uporablja za ocenjevanje tveganj. Je preprosta in da zelo jasne rezultate.

TABELA 4: Primerjava med strategijami od spodaj navzgor in od zgoraj navzdol

	Od spodaj navzgor	**Od zgoraj navzdol**
Opis strategije	Identifikacija, ocenitev in kvantificiranje potencialnega tveganja pri vsakodnevnih aktivnostih v posamezni poslovni enoti.	Identifikacija, ocenitev in kvantificiranje potencialnega tveganja v banki.
Uporaba	* pomoč pri aktivnostih, ki so potencialni povzročitelji tveganja, * za postavitev kontrole tveganja (kontrola tveganja pri tehnologiji).	* podpora pri izračunu kapitalske ustreznosti bank, * pomoč pri načrtovanju zavarovanja pred tveganjem * podpora pri zunanji reviziji,.
Taktika in tehnika	* kontrola samoocenjevanja, * analiza scenarijev na nivoju poslovnih enot (scenario analysis na nivoju business unit), * pregled novih storitev, * VAR kalkulacije * anketa na nivoju poslovnih enot.,	* inventura tveganja, * uvrščanje tveganja na podlagi izbranih scenarijev, * analize scenarijev na podlagi celotne banke, * VAR kalkulacije na podlagi celotne banke, * ankete na višjih vodstvenih nivojih banke.

Vir: Hoffman, 2002, str. 185.

4.2. DRUGA DIMENZIJA: KVALITATIVNE NASPROTI KVANTITATIVNIM

Druga dimenzija sooča obe vrsti metod ocenjevanja operativnega tveganja; tako imamo kvantitativne od zgoraj navzdol in kvantitativne od spodaj navzgor strategije ter kvalitativne od spodaj navzgor in kvalitativne od zgoraj navzdol strategije. Na eni strani je torej kvalitativna oziroma subjektivna metoda, na drugi strani pa kvantitativna oziroma numerična metoda. Povezave med obema dimenzijama lahko pokažemo s spodnjo tabelo. Najboljšo metodo si mora banka izbrati sama.

TABELA 5: Kvalitativne ter kvanitativne od zgoraj navzdol ter od spodaj navzgor metode

	Od spodaj navzgor strategije	**Od zgoraj navzdol strategije**
Kvalitativne	Poslovna enota-nivo * Kontrola samoocenitve (CSA) * Ocenjevalni intervjuji	Banka (najvišji nivo) * Intervjuji * Delfi metoda
Kvantitativne	Poslovna enota-nivo * Regresija * Loss distributions Analysis * Baysean Belief Network Analysis * System Dynamics Approach	Banka (najvišji nivo) * Trendi/ Regresija * Loss distribution/ Actuarial Analysis * Score cards

Vir: Hoffman, 2002, stran 186.

5. MINIMALNA ZAHTEVANA KAPITALSKA USTREZNOST BANK

Merjenje in ugotavljanje operativnega tveganja ima cilj, ki je jasno napisan v novem Baselskem sporazumu, kjer se zahteva, da se po novem v minimalni kapitalski ustreznosti bank upošteva še operativno tveganje. Če banke ne poznajo operativnega tveganja in če niti ne vedo, »kje naj ga iščejo«, potem naletijo na velik problem, zato se o tem tveganju čedalje več govori. Banke, bodo morale, zaradi uvedbe baselskega sporazuma uvesti nove metode ugotavljanja minimalnih kapitalskih zahtev.

Definicija operativnega tveganja bazira na osnovi dogodkov, ki so težko merljivi. Rezultati merjenja operativnega tveganja so zahtevana stopnja osnovnega kapitala bank, zato bodo morale banke v prihodnje v višino osnovnega kapitala vračunavati tudi operativno tveganje; tu govorimo o zavarovanju pred njim. Ker imajo banke zaradi operativnega tveganja prevelike izgube, so predlagatelji Baselskega sporazuma odločili, da je treba povišati kapitalsko ustreznost bank. Tako naj bi banke odkrivale operativno tveganje in ga poskušale zmanjševati, hkrati pa naj bi bile pred njim zaščitene s kapitalsko ustreznostjo. Zato je pomembno, da banke poznajo obseg operativnega tveganja, ki ga imajo v vsaki svoji poslovalnici.

Največji izziv je kvantificiranje operativnega tveganja s statističnimi metodami; npr., kako kvantificirati okvaro računalniškega sistema. Operativno tveganje je ocenjevanje verjetnosti, da se zgodi okvara računalniškega sistema ter kakšne stroške ta okvara povzroči posamezni banki. Banka se lahko z merjenjem operativnega tveganja zavaruje pred raznimi neopaznimi napakami, ki povzročijo izgube.

Celotni kapital mora biti seštevek 8% kreditnega tveganja, celotnega operativnega in tržnega tveganja:

celotni kapital = 0,08 * (kreditno tveganje + tržno tveganje + operativno tveganje).

Dane so bile 3 možnosti za izračun operativnega tveganja. Vse tri temeljijo na EI[7] indikatorju, ki je računovodska mera za bančno aktivnost.

5.1. ENOSTAVNI PRISTOP

Banka, ki uporablja za izračun kapitalske zahteve operativnega tveganja enostavni pristop, mora oblikovati kapital za operativno tveganje v višini fiksnega odstotka (alfa) povprečnega letnega bruto prihodka zadnjih treh let. Kapitalska zahteva je izražena na naslednji način (Advances in operational risk, 2003, str. 151):

[7] EI indikator (exposure indicator) je bruto prihodek, ki služi kot ocena izpostavljenosti operativnemu tveganju (Advances in operational risk, 2003).

$K_{ep} = BP \times \alpha$,

kjer je:
K_{ep} = kapitalska zahteva pri enostavnem pristopu,
BP = povprečni letni bruto prihodek v zadnjih treh letih[8],
α = 15%; vrednost je predpisana s strani Komiteja in se nanaša na višino zahtevanega kapitala na nivoju industrije.

Bruto prihodek je definiran kot vsota neto obrestnega prihodka in neto neobrestnega prihodka. Ta mera ne sme prikazovati rezervacij (npr. neplačanih obresti), ne sme upoštevati realiziranega dobička/izgube iz naslova prodaje vrednostnih papirjev, ki se vodijo kot bančne postavke in ne sme upoštevati izredne ali neredne postavke, kot tudi prihodka iz naslova zavarovanja.

5.2. STANDARDIZIRANI PRISTOP

Pri standardiziranem pristopu so aktivnosti banke razdeljene v osem poslovnih področij.

TABELA 6: Razdelitev aktivnosti bank

POSLOVNA PODROČJA	INDIKATOR	BETA FAKTOR V %
Podjetniško financiranje	Bruto dohodek	18%
Posli trgovanja	Bruto dohodek	18%
Poslovanje s prebivalstvom	Bruto dohodek	12%
Komercialno bančništvo	Bruto dohodek	15%
Plačilni instrumenti	Bruto dohodek	18%
Agentske storitve	Bruto dohodek	15%
Upravljanje s sredstvi	Bruto dohodek	12%
Posredovanje pri kupoprodaji vrednostnih papirjev prebivalstva	Bruto dohodek	12%

Vir: Advances in operational risk, 2003, str. 152.

Bruto dohodek je osnovni indikator za vsako poslovno področje. Služi kot približek obsega operacij oziroma obsega izpostavljenosti operativnemu tveganju vsakega poslovnega področja. Kapitalska zahteva za posamezno poslovno področje se izračuna kot produkt bruto prihodka in faktorja Beta, ki pripada temu poslovnemu področju. Beta predstavlja približek razmerja med izgubo iz operativnega tveganja za posamezno poslovno področje in agregatno višino bruto prihodka tega poslovnega področja na nivoju industrije. Pri tem pristopu je bruto prihodek vezan na posamezno poslovno področje in ne na celotno institucijo.

[8] Bruto prihodek je definiran kot vsota neto obrestnega prihodka in neto neobrestnega prihodka. Ta mera ne sme vsebovati rezervacij (neplačane obresti), realiziranega dobička/izgube iz naslova prodaje vrednsotnih papirjev, ki se vodijo kot bančne postavke in ne sme upoštevati izredne ali neredne postavke, kot tudi prihodke iz naslova zavarovanja (The New Basel Capital Accord, April 2003, str.121).

Celotna kapitalska zahteva je izračunana kot vsota delnih kapitalskih zahtev po posameznih poslovnih področjih. Izražena je z naslednjo formulo:

$KZ_{ksp} = \sum (BP_{1-8} * \beta_{1-8})$,

kjer je:

KZ_{ksp} = celotna kapitalska zahteva za standardizirani pristop,
BP_{1-8} = bruto prihodek za vsakega izmed osmih poslovnih področij (Exposure indicator); upošteva se letno povprečje treh let,
β_{1-8} = fiksen odstotek, predpisan s strani Komiteja, ki se nanaša na višino zahtevanega kapitala glede na bruto prihodek za vsako posamezno poslovno področje.

5.3. ALTERNATIVNI STANDARDIZIRANI PRISTOP

Standardizirani pristop so kritizirali zaradi dvojnega obravnavanja tveganja pri nekaterih poslih banke. Najprej na strani kreditnega tveganja z visokim obveznim kapitalom zaradi tveganja ne vrnitve posojila, potem pa še na strani operativnega tveganja zaradi visokih kapitalskih zahtev.

Metodologija določanja kapitalske zahteve je enaka kot pri standardiziranem pristopu; razen za dve poslovni področji; poslovanje s prebivalstvom in komercialno bančništvo. Pri teh poslovnih področjih se bruto dohodek nadomesti z drugim indikatorjem izpostavljenosti, ki se imenuje »krediti in zunaj bilančne kreditne obveznosti«[9], pomnoženimi s fiksnim faktorjem »m«.

Višina faktorja β je za obe poslovni področji enaka kot pri standardiziranemu pristopu. Formula za izračun kapitalske zahteve pri poslovnem področju »poslovanje s prebivalstvom« je izražena na naslednji način (za poslovno področje »komercialno bančništvo« je formula ustrezno enaka):

$K_{RB} = \beta_{RB} \text{ x } m \text{ x } LA_{RB,}$

kjer je :

K_{RB} = kapitalska zahteva za poslovno področje »poslovanje s prebivalstvom«,
β_{RB} = faktor Beta za poslovno področje »poslovanje s prebivalstvom«,

[9] Zunanje bilančne kreditne obveznosti pomenijo odobrene in nečrpane kredite, ki se vodijo v zunaj bilančnih postavkah do prvega črpanja oziroma do prenosa na bilančno pozicijo.

LA_{RB} = celoten znesek kreditov in zunanje bilančnih kreditnih obveznosti na področju prebivalstva (netehtanih in brez upoštevanja rezervacij); upošteva se povprečje zadnjih treh let,
m = 0,035.

Da se banka lažje odloči, kateri pristop bo uporabila, obstajajo določeni kriteriji, ki jih določi komite.

5.4. NAPREDNI PRISTOPI

Banke lahko uporabljajo svoje interne sisteme za merjenje operativnega tveganja za izračun kapitalske zahteve, če jim nacionalni nadzornik to odobri. Odobritev uporabe naprednih pristopov je odvisna od ustrezanja kvalitativnim in kvantitativnim kriterijem s strani Baselskega komiteja ter kriterijev s strani nacionalnih nadzornikov.

Preden se napredni pristopi lahko uporabijo v regularne namene, so podvrženi začetnemu opazovalnemu obdobju. Z začetnim opazovalnim obdobjem banka pridobi potrebne informacije, na podlagi katerih lahko uporabi napredne pristope pri računanju svoje kapitalske ustreznosti.

5.5. KVALIFIKACIJSKI KRITERIJI

Da se banka kvalificira za uporabo standardiziranega ali naprednega pristopa, mora izpolnjevati naslednje minimalne kriterije (The New Basel Capital Accord, 2003, str. 125):

a) uprava in višji management banke morata biti aktivno udeležena pri nadziranju upravljanja okvira operativnega tveganja v banki;
b) ima implementiran sistem upravljanja s tveganji, ki je konceptualno transparenten in celovit in
c) ima dovolj resursov za delo na pristopu po posameznih poslovnih področjih, kot tudi na področju kontrole in revizije.

Nadzorniki imajo pravico zahtevati določeno opazovalno obdobje uporabe standardiziranega pristopa, preden ga bo banka lahko uporabila v regulatorne namene.

Tudi napredni pristopi bodo podvrženi začetnemu opazovalnemu obdobju s strani nadzornikov, preden jih bo banka lahko uporabila v regulatorne namene. To obdobje bo omogočilo nadzornikom presojo, ali je konkreten pristop banke verodostojen in ustrezen.

5.5.1. KRITERIJI ZA STANDARDIZIRANI PRISTOP

Mednarodno aktivne banke bodo morale za uporabo standardiziranega pristopa imeti implementiran ustrezen sistem upravljanja z operativnim tveganjem. Za njih bodo veljali naslednji kriteriji uporabe standardiziranega pristopa (The New Basel Capital Accord, 2001, str. 96):

a) Banka mora imeti sistem upravljanja z operativnim tveganjem z jasnimi odgovornostmi funkcije za upravljanje z operativnim tveganjem. Omenjena funkcija je odgovorna za: razvijanje strategij pri identificiranju, ocenjevanju, spremljanju in kontroli/zmanjševanju operativnega tveganja; za izdelavo tovrstne politike banke ter postopkov, ki se nanašajo na upravljanje in kontrolo upravljanja z operativnim tveganjem; za oblikovanje in implementacijo metodologije banke za ocenjevanje tveganja; za oblikovanje in implementacijo sistema poročanja.
b) Kot del internega sistema banke za ocenjevanje operativnega tveganja mora banka sistematično zbirati relevantne podatke o tveganju hkrati z izgubami iz le-tega po posameznih poslovnih področjih. Sistem banke za ocenjevanje operativnih tveganj mora biti tesno integriran v celoten proces upravljanja s tveganji v banki.
c) Vzpostavljeno mora biti redno poročanje o izpostavljenosti morebitnim izgubam iz naslova operativnega tveganja ter o konkretnih izgubah iz tega naslova vodstvu poslovnih enot, višjemu managementu in upravi banke.
d) Sistem upravljanja s tveganjem mora biti v banki dobro dokumentiran. Banka mora rutinsko zagotavljati skladnost z dokumentirano zbirko internih poslovnih politik, kontrol in postopkov, ki se nanašajo na sistem upravljanja z operativnim tveganjem.
e) Procesi upravljanja z operativnim tveganjem ter sistemom ocenjevanja teh tveganj morajo biti odobreni in podvrženi rednim in neodvisnim pregledom. Ti pregledi morajo zajemati tako aktivnosti v poslovnih enotah kot tudi funkcijo upravljanja z operativnim tveganjem. Sistem banke za ocenjevanje operativnega tveganja mora biti podvržen rednim pregledom zunanjih revizorjev.

5.5.2. KRITERIJI ZA NAPREDNI PRISTOP

Banka mora za uporabo naprednih pristopov za izračun kapitala za operativna tveganja izpolnjevati naslednje kriterije (The New Basel Capital Accord, 2001, str. 97):

a) Banka mora imeti neodvisno funkcijo upravljanja z operativnim tveganjem, ki je odgovorna za oblikovanje in implementacijo okvira za upravljanja z operativnim tveganjem v banki. Funkcija je odgovorna: za izdelavo poslovnih politik banke ter postopkov, ki se nanašajo na upravljanje in kontrolo upravljanja z operativnim tveganjem; za oblikovanje in implementacijo metodologije merjenja operativnega tveganja; za oblikovanje in implementacijo sistema poročanja o operativnem tveganju; za razvijanje

strategij za identificiranje, merjenje, spremljanje in kontroliranje/zmanjševanje operativnega tveganja.

b) Interni sistem merjenja operativnega tveganja v banki mora biti tesno integriran v dnevni proces upravljanja s tveganji. Njegov rezultat mora biti hkrati sestavni del procesa spremljanja in kontroliranja profila operativne tveganosti banke. To na primer pomeni, da mora tovrstna informacija igrati pomembno vlogo v poročilih o tveganjih, poročilih managementu in raznih analizah tveganja. Banka mora imeti izdelane tehnike za alokacijo kapitala za pokrivanje operativnega tveganja po glavnih poslovnih področjih ter za kreiranje vzpodbud, ki bi izboljšale upravljanje z operativnim tveganjem v banki.
c) Vzpostavljeno mora biti redno poročanje o izpostavljenosti operativnemu tveganju ter o izgubah iz operativnega tveganja vodstvu poslovnih enot, višjemu managementu in upravi banke. Banka mora imeti implementirane procedure za izvedbo ustrezne akcije glede na informacijo v poročilih vodstvu.
d) Sistem upravljanja s tveganjem mora biti v banki dobro dokumentiran. Banka mora rutinsko zagotavljati skladnost procesa upravljanja z dokumentirano zbirko internih poslovnih politik, kontrol in postopkov, ki se nanašajo na sistem upravaljanja s tveganjem. Slednji mora hkrati zajemati tudi politiko obravnavanja zadev, ki niso zajeta v predpisih.
e) Interni ali zunanji revizorji morajo izvajati redne preglede procesa upravljanja z operativnim tveganjem ter sistemov merjenja tveganja banke. Ti pregledi se morajo nanašati tako na aktivnosti v poslovnih enotah kot tudi na neodvisno službo upravljanja z operativnim tveganjem.
f) Odobritev sistema merjenja operativnega tveganja s strani zunanjih revizorjev ali nadzorniških institucij mora vsebovati naslednje:
   - Potrditev, da interni procesi odobritve potekajo na zadovoljiv način.
   - Zagotovitev, da je pretok podatkov in procesov, ki so povezani s sistemom merjenja tveganja, transparenten in dostopen. Še zlasti je pomembno, da imajo revizorji in nadzorniki pri izvajanju pregleda, v okviru ustreznih procedur, omogočen enostaven dostop do specifikacij in parametrov sistema.

Banka lahko z razvojem svojih bančnih storitev in z večanjem svojih poslovnih zmožnosti napreduje iz merjenja minimalnih kapitalskih zahtev na podlagi enostavnega pristopa na nivo merjenja na podlagi standardiziranega ali naprednega pristopa. Seveda lahko napreduje samo, če ima izpolnjene kriterije, ki so predstavljeni zgoraj.

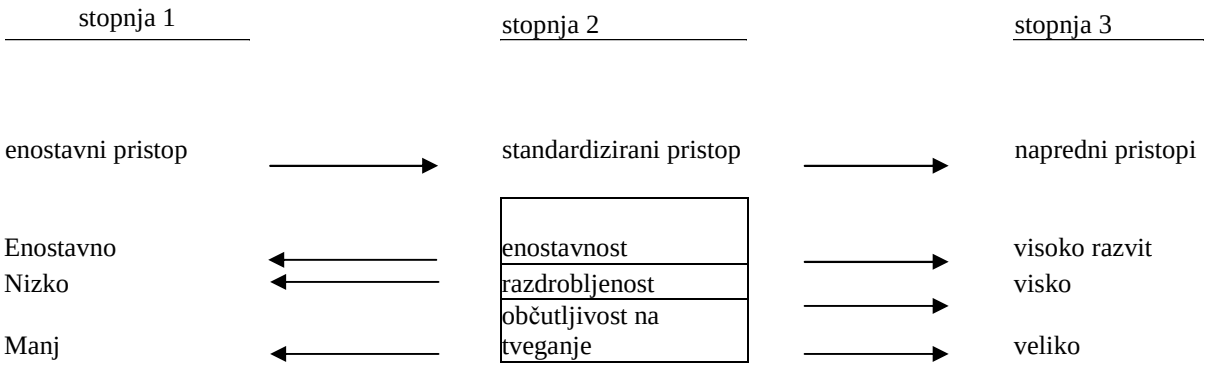
Enostavni pristop omogoča enostavno merjenje in ugotavljanje minimalne kapitalske zahteve, prisotna je nizka razdrobljenost[10] in manjša občutljivost na tveganje (ne pričakujemo velike izgube na podlagi operativnega tveganja). Enostavni pristop uporabljajo manjše banke, ki nimajo veliko komitentov in je tudi sam nadzor nad upravljanjem lažji in enostavnejši. Ko se banka poveča in postane njeno poslovanje kompleksnejše, lahko - če izpolni kriterije (glej peto poglavje), ki jih zahtevajo regulatorji - ugotavlja minimalno kapitalsko zahtevo na

[10] Nizka razdrobljenost pomeni, da nam ni treba iti globoko v samo organzacijo banke, da bi lahko ugotovili, kakšnemu tveganju je izpostavljena. Tu govorimo predvsem o ugotavljanju tveganja na nivoju celotne banke (glej prvo poglavje).

podlagi standardiziranega pristopa. Tu govorimo že o višji stopnji razdrobljenosti, prav tako moramo iti globlje v samo bančno strukturo, da lahko ugotovi, kje se nahaja operativno tveganje. Informacije pridobivamo na nivoju posameznih sektorjev.

Tretja stopnja je namenjena velikim bankam, ki imajo poslovalnice tudi v tujini in izpolnjujejo kriterije za merjenje minimalne kapitalske zahteve na podlagi naprednih pristopov. Tu govorimo o visoko razvitem sistemu merjenja operativnega tveganja. Razdrobljenost je tu najvišja – pridobivanje informacij je znotraj posameznega sektorja. Banka mora imeti dobro razdelano organizacijsko strukturo ter notranje kontrole. Prav tako je na tej stopnji banka veliko bolj občutljiva na tveganje,saj se ga bolj zaveda ter je zaradi svoje velikosti in kompleksnosti toliko bolj »na udaru« glede operativnega tveganja. Stopnje napredovanja od enostavnega do naprednega pristopa merjenja minimalne kapitalske zahteve so prikazane na Sliki 5.

SLIKA 5: Stopnje napredovanja od enostavnega do naprednega pristopa merjenja minimalne kapitalske zahteve



Vir: Advances in operational risk, 2003, str. 153.

Banka mora zelo dobro razmisliti v katero razvojno stopnjo spada. Pri tem »razmišljanju« ji mora pomagati regulator, katerega naloga je spremljanje in svetovanje bankam, ki uvajajo minimalne kapitalske zahteve na podlagi kateregakoli pristopa. Banka mora zelo pazljivo iti čez vse stopnje ugotavljanja in merjenja operativnega tveganja, da lahko vzpostavi pravi sistem ter ekipo, ki se bo ukvarjala s tem.

6. ZAVAROVANJE OPERATIVNEGA TVEGANJA

Kot smo videli v prvem poglavju, so v baselsko definicijo operativnega tveganja všteta različna tveganja, ki so bolj ali manj primerna za zavarovanje. Glede na to, da se razvija tudi svet zavarovalništva, bi bilo dobro, da bi regulatorji pomislili tudi na to možnost zavarovanja pred tveganjem. Vprašanje, ki se tu pojavi, je, ali so banke same sposobne obvladovati svoja

operativna tveganja preko specializiranih zavarovalniških produktov ali naj se v proces obvladovanja tveganja vmeša regulator s svojimi zahtevami.

Kaj vse spada pod operativno tveganje, je našteto v Prilogi 1. Prva stvar, ki jo opazimo, je, da govorimo o zelo širokem spektru tveganj, ki niso niti natančno opredeljena in se jih težko kvantitativno izmeri. Najprej morajo banke ugotoviti, kje se pri njih operativno tveganje pojavlja in v kakšnem obsegu. Šele potem lahko ugotavljajo, kako se bodo pred njim zavarovale.

6.1. ZAVAROVALNE POLICE ZA OPERATIVNO TVEGANJE

Zavarovalni produkti, ki pokrivajo operativno tveganje, so v zadnjih letih doživeli velik razvoj. Trenutno so v bančnem svetu najpopularnejša sledeča zavarovanja (Rotovnik, 2003, str. 2):

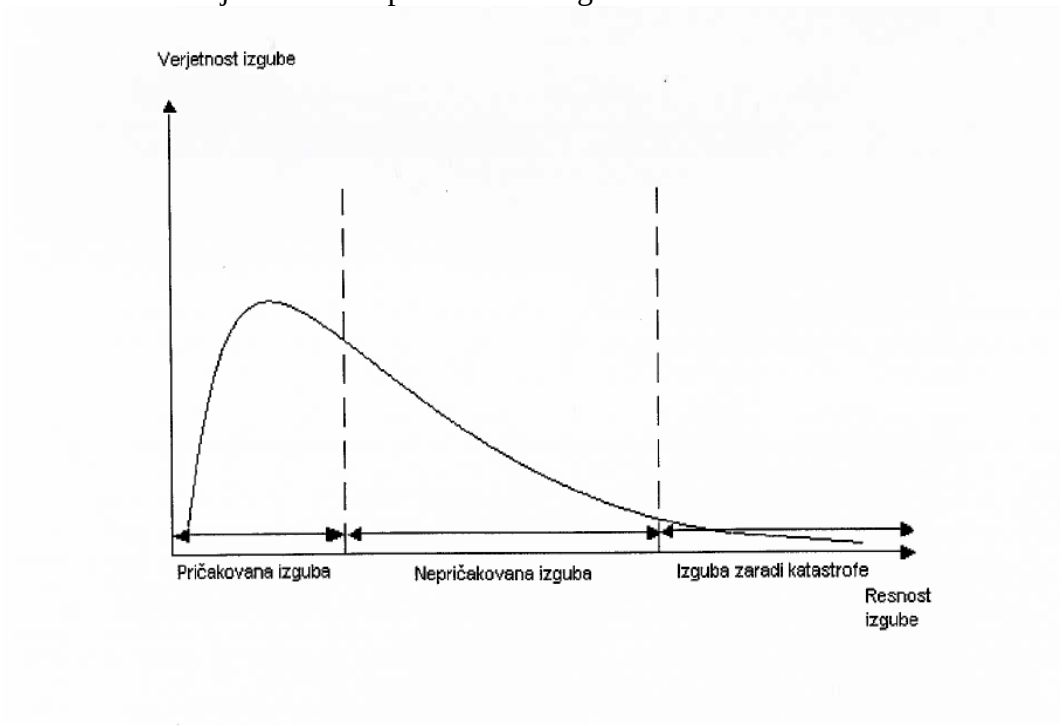
a) zavarovanje proti goljufiji zagotavlja pokritje izgub iz naslova nepoštenih dejanj zaposlenih, kot so prevare in poneverbe;
b) zavarovanje proti računalniški zlorabi zagotavlja pokritje izgub iz naslova računalniških virusov, težav pri prenosu podatkov ipd;
c) poslovno odškodninsko zavarovanje je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

Zavarovalnice ponavadi tovrstna zavarovanja ponujajo samo največjim finančnim institucijam, zaradi cene njihovih produktov ter manjše verjetnosti za nastanek škodnega dogodka. Za banke tovrstno zavarovanje pomeni velik strošek. Poleg tega bi morale banke v primeru sklenitve zavarovanja prav tako ugotavljati in meriti, kje se operativno tveganje pojavlja ter v kakšnem obsegu. Skratka na koncu mora banka ugotoviti, kaj je zanjo večji strošek, ali zavarovalna polica ali kapitalska ustreznost izračunana po eni izmed metod, ki so predstavljene v šestem poglavju. Ostane še tretja možnost, in to je - kombiniranje zavarovalnih polic in kapitalske ustreznosti.

6.2. KATEGORIZACIJA OPERATIVNEGA TVEGANJA GLEDE NA VERJETNOST NASTOPA ŠKODNEGA DOGODKA

Opredelitve operativnih tveganj pri baselski definiciji in tudi pri razvoju zavarovalnih polic temeljijo na vzroku in posledici posamezne vrste tveganja. Banke bi morale, že zaradi stroškov povezanih s tveganjem, posamezna operativna tveganja razdeliti statistično glede na pričakovanje posameznega dogodka in velikost izgube. S tem bi se lažje odločili, katera tveganja bi krili z zavarovalno polico in katera s pomočjo kapitala.
Recimo majhne, a zelo pogoste izgube, ki se zaradi napak zaposlencev ali še nestabilnih aplikacij dogajajo vsak dan, se običajno krijejo iz operativnih stroškov. Te izgube so predvidljive in se jim banke zaradi narave svojega dela težko izognejo. Drugače je z izgubami, ki sicer nastajajo manj pogosto, a spadajo v kategorijo srednjih in visokih izgub. Ker niso popolnoma predvidljive in so za banko veliko bolj resnega značaja, je nujno, da se pred njimi zavarujejo s pomočjo kapitala ali primernih zavarovalnih polic. Končno so tu redke, a izjemno visoke izgube iz naslova operativnega tveganja, ki nastanejo kot posledica naravnih katastrof ali podobnih dogodkov. Le-ti predstavljajo spodnji del porazdelitvene krivulje (Rotovnik, 2003, str. 3) (glej Slika 6).

SLIKA 6: Krivulja statistične porazdelitve izgube



Vir: Rotovnik, 2003, str. 3.

Kar se tiče zavarovalnih polic, niso v dvomih samo banke, ampak tudi regulatorji. Dejstvo je, da se vsega ne da zavarovati, poleg tega so zavarovalnice zelo skeptične, ko gre za zavarovanje škodnih dogodkov, ki jih ne morejo predvideti.

6.3. POMISLEKI REGULATIVE V ZVEZI Z ZAVAROVANJEM OPERATIVNIH TVEGANJ

Če so zaradi regulatorja zavarovalne police enakovredne kapitalski ustreznost za zaščito pred operativnim tveganjem, potem se lahko zgodi, da se bo banka odločila za nakup zavarovalne police samo zato, da bi se izognila izpolnjevanju kapitalskih zahtev. Kot smo ugotovili, bi imele banke v primeru, da bi bile zavarovalne police dovoljene, na voljo tri možnosti za zaščito pred pojavom propada iz naslova operativnega tveganja. Ena je izračun kapitalske ustreznosti po eni izmed metod opisanih v prejšnjem poglavju. Druga je, da kupi zavarovalno polico in se zavaruje. Tretja možnost pa je, uporaba kombinacije obeh (zavarovalna polica in kapitalska ustreznost).

Če se odloči za drugo možnost, potem se regulatorju lahko pojavijo nekatera vprašanja oziroma pomisleki (Rotovnik, 2003, str. 4):

a) Tveganje neizpolnitve nasprotne strani
   S podpisom zavarovalne police je banka v milosti/nemilosti zavarovalnice. Zavarovalnica gre lahko v stečaj in tako ob nastopu škodnega dogodka ni sposobna izplačati pogodbene vsote; torej bi tu »prenesli« operativno tveganje na zavarovalnico. Poleg tega ni nujno, da zavarovalnica podaljša police za naslednje obdobje, banka pa zelo težko na hitro prilagodi svojo kapitalsko ustreznost, zato bi nekaj časa ostala brez kritja za nastanek škodnega dogodka iz naslova operativnega tveganja.

b) Hitrost plačila s strani zavarovalnice
   Ko nastopi škodni dogodek, mora zavarovalnica najprej ugotoviti, če ima banka ta dogodek zavarovan na zavarovalni polici, potem pa še preučiti, ali je šlo res za škodo iz naslova operativnega tveganja. Tako pri zavarovalnicah vedno nastane zamuda pri plačilu zavarovalnine. Banka pa ima kapital za pokrivanje tveganja vedno na razpolago.

c) Omejitve pri ponudbi zavarovalnih produktov
   Zavarovalni produkti so zelo specifični glede na vrsto tveganj, ki jih pokrivajo. Za regulatorje je to pomemben poudarek, ko gre za odločanje, katera zavarovalna polica lahko šteje kot nadomestek za regulatorni kapital. Ne bi bilo dopustno, da bi se banka izognila izpolnjevanju kapitalskih zahtev z nakupom desetih milijard dolarjev vredne police za zavarovanje proti računalniškim zlorabam, če predstavlja njeno glavno operativno tveganje sedež na zelo potresnem območju. Težavo bi se dalo odpraviti s t.i. paketom, ki bi vseboval za vsako posamezno banko ustrezne police. Paketno zavarovanje je šele v povojih in bi bilo potrebno učinkovitost zavarovanja še ovrednotiti.

6.4. KORISTI ZAVAROVANJA ZA REGULATORJE

Določeni tipi zavarovanj so za vse banke obvezni že sedaj, to so predvsem požarna zavarovanja in zavarovanja proti goljufijam zaposlencev (Rotovnik, 2003, str. 6).

a) Razpršitev tveganja
   Zavarovanje nedvomno vodi k razpršitvi tveganja na več institucij in s tem k zmanjševanju finančne izgube. Če mora banka sama kriti izgube vseh operativnih tveganj, lahko določenih škodnih dogodkov ne bo mogla več pokrivati le s svojim kapitalom. Banka lahko kljub upoštevanju kapitalske ustreznosti zelo težko zbere dovolj kapitala za pokritje izgub zlasti iz spodnjega dela krivulje statistične porazdelitve izgube (glej Sliko 6, str.30).

b) Zbiranje podatkov in strokovno znanje
   Razumevanje upravljanja z operativnim tveganjem ter zavarovanje operativnega tveganja je marsikje šele na začetni stopnji razvoja, kar velja tudi za regulatorje, zato je pomembno, da pri nadaljnjem razvoju tako regulatorji kot tudi banke izkoristijo že pridobljeno strokovno znanje zavarovalnic. Na drugi strani bodo morale tudi zavarovalnice pri oblikovanju zavarovalnih produktov zbrati čim več relevantnih podatkov o dejanskem bančnem upravljanju z operativnim tveganjem.

Zaključujemo z ugotovitvijo, da bi banke morale imeti kapitalsko ustreznost na eni strani in zavarovalne police na drugi strani. Zavarovalne police bi po mojem mnenju morale imeti predvsem za pokritje izgub, ki nastanejo zaradi katastrofe. Tako bi banka imela dva vira za pokritje izgub.

Ne glede na to, kako bodo banke odločale, bodo morale v vsakem primeru zaradi operativnega tveganja vedeti, v kakšnem obsegu ter kje se pojavljajo škodni dogodki. Odločiti se bodo morale tudi, kako se bodo izgube zaradi operativnega tveganja pokrivale; ali z zavarovalnimi policami ali kapitalsko ustreznostjo. Kapitalsko ustreznost bi morale imeti vsaj zaradi ohranjanja zaupanja ljudi v bančni sistem.

7. OPERATIVNO TVEGANJE V SLOVENIJI

V Sloveniji se na operativno tveganje pripravljamo predvsem zaradi zahteve, ki je je postavil Baselski sporazum. Ta zahteva je, da bodo morale banke do leta 2007 imeti izračunan minimalni zahtevani kapital po eni izmed metod, opisanih v petem poglavju. Glede na to, da so slovenske banke po obsegu manjše od tujih bank, bodo lahko merile minimalno zahtevano kapitalsko ustreznost po dveh metodah:

a) enostavni pristop,
b) standardizirani pristop.

Za ostala dva pristopa se slovenske banke verjetno ne bodo odločale, saj pomenita dodatni napor pri pridobivanju informacij.

Banka Slovenije je v analizi, ki je bila končana avgusta leta 2004, izvedla prve kvantitativne ocene vpliva spremenjenih kapitalskih pravil na kapitalsko ustreznost slovenskega bančnega sistema, saj slovenske banke niso bile vključene v nobeno izmed treh baselskih kvantitativnih študij učinkov novega kapitalskega sporazuma.

Namen te študije je raziskati vpliv različnih metodoloških rešitev za izračun kapitalskih zahtev za kreditno in operativno tveganje na kapitalsko ustreznost bank. Rezultati te študije so po individualnih bankah za javnost nedostopni, so pa vsi rezultati objavljeni v zbirni obliki. Banka Slovenije je analizo vpliva novih kapitalskih pravil izvedla po 128 scenarijih. Ugotovila je, da devet slovenskih bank ni še sprejelo formalne odločitve o izbiri scenarija za izračun minimalne kapitalske zahteve ter da so v štirih bankah nejasne priprave na učinkovito upravljanje operativnega tveganja.

Iz tega lahko razberemo, da nekatere banke niso vzele resno vpliva operativnega tveganja na samo poslovanje, kar se mi zdi čista neresnost, saj ima večina prebivalstva svoje prihranke še vedno shranjene na banki. Banka tako tvega, da izgubi denar svojih komitentov in s tem tudi, da se zmanjša kupna moč prebivalstva zaradi morebitnega škodnega dogodka.

Edini primer v Sloveniji, ki ga lahko štejemo za operativno tveganje, je primer Nove ljubljanske banke iz obdobja uvedbe transakcijskih računov. Tu gre predvsem za tveganje iz naslova programskega tveganja, saj je progam Sigma zatajil in povzročil za banko veliko izgubo. Kakšna je ta izguba, ne vemo, saj je škandal še dokaj »svež« in verjetno številk še ni zbranih. Lahko pa v tem primeru ugotovimo, da je banka izgubila veliko ugleda in s tem tudi strank/komitentov.

Kakšno je stanje v drugih naših bankah, ne vemo, saj je naša politika odkrivanja bančnega poslovanja dokaj konzervativna, tako da javnost lahko dobi samo splošne podatke in tiste, ki so po zakonu obvezni.

Problem, ki ga vidim pri slovenskemu uvajanju operativnega tveganja v bankah je tudi slovenski regulator, ki ima premalo nadzornikov, ki bi v bankah lahko nadzirali uvedbo minimalne kapitalske zahteve in na sicer izobraževali banke na tem področju. Sicer se aktivnosti Banke Slovenije na temo operativnega tveganja vežejo na samo izobraževanje zaposlencev v bankah, seminarji na to temo ter razne ankete. Na podlagi teh anket Banka Slovenije skuša nadzirati samo pripravljenost posameznih bank na uvedbo minimalne kapitalske zahteve. Samo jedro problema je tudi v matični banki, ki se sooča s problemom pomanjkanja kadra, ki bi se aktivneje osredotočil na uvajanje merjenja tveganja v posameznih lokalnih bankah.

Kar se tiče samega zavarovanja kot nadomestka za kapitalsko ustreznost, so tako naše banke kot zavarovalnice v razvoju precej zaostale. V Sloveniji je težava, ker so naše največje banke in zavarovalnice tako majhne v primerjavi s svetovnimi, da se jim mogoče res ne splača uvajati zavarovalnih polic za škodne dogodke iz naslova operativnega tveganja. Zavarovalnice bodo morale računati tudi na to, da lahko dobijo konkurenco iz tujine in bodo zato morale razširiti svojo ponudbo. Slovenske zavarovalnice ponujajo zavarovanje proti vlomu, požaru, odgovornosti, vendar so le-ta bolj namenjena podjetjem kot pa bankam.

SKLEP

Ugotovili smo, da je operativno tveganje zelo razširjen pojav v bankah in da so zadnje čase banke posvetile veliko časa in vložila veliko napora v to, da so naredile ustrezen sistem merjenja in ugotavljanja operativnega tveganja. V diplomski nalogi je predstavljen proces definiranja, ugotavljanja in merjenja operativnega tveganja ter zakonske zahteve obravnavanja operativnega tveganja.

Brez jasne definicije in dobro postavljenega operacijskega sistema, se je v »boj z operativnim tveganjem« nesmiselno spuščati, saj s tem banke izgubljajo denar in čas. Res je, da se v zadnjem času ne govori veliko o velikih izgubah, ki bi nastale zaradi operativnega tveganja s strani bank. To pomeni, da so se začele zavedati pomena tveganja in njegovih posledic. K temu je veliko pripomogel tudi Baselski sporazum, ki je operativno tveganje vpel med sam kapital banke in s tem dosegel, da so se banke zavarovale pred njim. S tem, ko je Basel definiral minimalno kapitalsko zahtevo, je prisil banke, da so začele razmišljati o vplivu operativnega tveganja na svoje poslovanje ter morebitne izgube.

Tako lahko rečemo, da se je v tujini stvar začela razvijati v pozitivno smer. V Sloveniji je situacija malo drugačna, saj so banke relativno majhne in zato niso bile aktivne pri pripravljanju nove minimalne kapitalske zahteve. Imajo pa možnost, da se kaj naučijo od bank, ki so se že začele pripravljati na minimalno kapitalsko zahtevo. Banka Slovenije je na temo operativnega tveganja pripravila zelo veliko gradiva, ki ga je posredovala slovenskim bankam. Prav tako je izvedla kvantitativno študijo pripravljenosti slovenskih bank na pojav operativnega tveganja ter na uvedbo minimalne kapitalske zahteve. Rezultati so pokazali, da vsaj devet slovenskih bank še ni sprejelo formalne odločitve o načrtovani vrsti pristopa za izračun kapitalskih zahtev za operativno tveganje. Upam, da bodo banke resno sprejele nalogo uvedbe minimalne kapitalske zahteve, saj je od tega odvisno, na kakšen način bo banka reagirala na škodni dogodek iz naslova tveganja.

Kot smo videli, se je na bančnem področju zelo veliko govorilo o tveganju samem in o reševanju le-tega ter o zaščiti pred njim, zato se je to tveganje v bankah zmanjšalo ali pa je vsaj pod nadzorom regulatorjev. Opazimo lahko, da se je operativno tveganje preselilo na poslovni svet in velika mednarodna podjetja, kot so Enron, WorldCom ter Parmalat. To so vsa

podjetja, ki so propadla zaradi škodnega dogodka iz naslova operativnega tveganja. Ker v Evropi še ni dodelane rešitve, ki bi preprečevala takšne izgube, se morajo podjetja sama zaščititi. V Združenih državah Amerike pa so sprejeli t.i. Sarbanes and Oxley – jev zakon, ki predvideva, da v podjetju ne sme priti do navzkrižja interesov, npr. ena oseba ne sme vnašati faktur, jih knjižiti, plačati in zapreti plačila.

V današnjih časih smo prišli do točke, kjer je vsaka še najmanjša napaka lahko pogubna za vsako banko/podjetje. Vse, kar jim ostane, je, da dobro poznajo svoje zaposlence, jih nadzirajo ter nagrajujejo za dobro opravljeno delo. Druga prav tako pomembna stvar je dober informacijski sistem, ki daje prave in koristne informacije. Kombinacija poštenih zaposlencev, dobrega informacijskega sistema in natančno postavljene notranje kontrole vodi v dober indikator operativnega tveganja in zaščite pred njim.

LITERATURA

1. Advances in operational risk: Firm-wide issues for financial institutions. London : Risk Books, 2003. 272 str.
2. Cruz Marcelo G.: Modeling, Measuring and Hedging Operational Risk. New York : John Wiley & Sons, 2002. 330 str.
3. Hoffman Douglas G.: Managing Operational Risk: 20 firmwide best practice strategies. New York : John Wiley & Sons, 2002. 543 str.
4. Dimitris Chorafas N.: Managing operational risk. London : Euromoney Books 2001. 237 str.
5. Mishkin Frederic: The economics of money, banking and financial markets. Boston : Addison Wesley Longman 2001. 737 str.
6. Mohorič Saša: Operativno tveganje v bankah. Bančni vestnik, Ljubljana, 51(2002), 5, str. 32-34.
7. Slak Leon: Obvladovanje tveganj v bančnem poslovanju po novem kapitalskem sporazumu Basel II. Magistrsko delo. Ljubljana : Fakulteta za podiplomske državne in evropske študije, 2005. 135 str.

VIRI

1. Operational risk (Consultative Document). Basel : Basel Committe on Banking Supervision. 2001. 26 str.
2. Hočevar Borut: Edo Nodila: Hrvaški Nick Leesoon. Časnik Finance, Ljubljana, 19.3.2002.
3. Sklep o kapitalski ustreznosti bank in hranilnic (Uradni List RS, št. 24/02, 85/02, 22/03, 36/04, 68/04).
4. Interna gradiva Banke Slovenija.
5. Internal audit and banking oragnizations and the relationship of the supervisory authorities with internal and external auditors. Consultative Paper issued by the Basel Committe on banking Supervision. Basel : Bank for international settlements, 2000. 23 str.
6. Ogrinc Petra, Rotovnik Tomaž: Ugotovitve slovenske kvantitativne študije učinkov. Banka Slovenije. 17 str. [URL:http://213.250.51.72/html/basel2/04_gradiva/dokumenti/OgrincRotovnik_končni.pdf], 2004.
7. Rotovnik Tomaž: Zavarovanje operativnega tveganja in Basel II. Banka Slovenije. Basel Committe on Banking Supervision: Operational Risk. 26 str. [URL:http://213.250.51.72/html/basel2/04_gradiva/dokumenti/Zavarovanje%20operativnega%20tveganja.pdf], 2001.
8. Rotovnik Tomaž: Operativno tveganje z regulatorne perspektive. Banka Slovenije. 17 str. [URL:http://213.250.51.72/html/basel2/04_gradiva/dokumenti/Portoroz_2_Operativno%20tveganje.pdf], 2004.

9. Rotovnik Tomaž: Izzivi zunanjih baz podatkov za operativno tveganje. Banka Slovenije. 11 str. [URL:http://213.250.51.72/html/basel2/04_gradiva/dokumenti/Zunanja_baza_podatkov1.pdf], 2004.
10. The New Basel Capital Accord. Bank for international settlements. 139 str. [http://www.bis.org/publ/bcbsca03.pdf], 2001.

PRILOGA 1

PODROBNA KLASIFIKACIJA ŠKODNIH DOGODKOV

KATEGORIJA ŠKODNIH DOGODKOV (1.NIVO)	DEFINICIJA	KATEGORIJE (2.NIVO)	PRIMERI AKTIVNOSTI
Notranja goljufija (Internal Fraud)	Izguba povzročena zaradi dejanj: °poneverbe, °nezakonite prisvojitve lastnine, °zavajajo čih predpisov, zakona ali poslovne politike institucije, pri čemer niso všteti diskriminatorni dogodki in v katero je vpleten vsaj en zaposleni.	Neodobrena aktivnost	°namerno n eprijavljene transakcije °neodobrena izvedba dolo čene vrste transka cije (ki se odrazi v izgubi) °neustrezno vodenje poz icije
		Tatvina in goljufija	°goljufija/poneverbe na ra čunih/ lažni pologi/tatvina/izsiljevanje/utaja/ kraja °nezakonita prisvojitev sredstev °ponarejanje, prevara °goljufije s čeki °prikrivanje °kraja ra čuna/lažno predstavljanje °dav čna utaja °notranje trgovanje (ne za ra čun banke)
Zunanja goljufija	Izguba povzročena zaradi dejanj: °poneverbe, °nezakonite prisvojitve lastnine °zavajajo čega zakona in v katero je vpletena zunanja stran	Tatvina in goljufija	°kraja/rop °ponevrba °goljufije s čeki
		Varnost sistemov	°škoda zaradi nepoobl aščenih vdorov v sistem °kraja informacij (ki se odrazi v denarni izgubi)
Postopki zaposlencev in varstvo pri delu	Izguba povzročena zaradi: °dejanj, ki niso v skladu s pravilniki oz. zakoni o zaposlovanju, zdravju in varstvom pri delu °pla čil zaposlenim iz naslova poškodb pri delu in diskriminacije	Odnosi z zaposlenci	°kompenzacije °podp ore °izgube iz n aslova prenehanja delovnega razmerja °organizirane delavske aktivnosti
		Varnost pri delu	°spl ošna odgovornost °zdravje zaposlencev in dogodki v zvezi s pravili varnosti pri delu °kompenzacije delavcem
		Različni dogodki in diskriminacija	°vse vrste diskriminacije
Klienti, produkti in poslovna praksa	Izguba povzročena zaradi: °nenamernega ali malomarnega dejanja zaradi katerega strokovna obveznost do določenih komitentov ni bila izpolnjena	Soglasja, razkritje in zaupnost	°kršitev zaupn osti °so glasje pri razkrivanju podtkov °kršitve za radi razkrivanja podatkov o pomembnih komitentih

KATEGORIJA ŠKODNIH DOGODKOV (1.NIVO)	DEFINICIJA	KATEGORIJE (2.NIVO)	PRIMERI AKTIVNOSTI
	(zahteve glede zaupnosti in soglasja so vključene) °narave ali sestave produkta/storitve banke		°kršitev zasebnosti °agresivna prodaja °zloraba zaupnih informacij °obveznost do upnikov
		Neprimerne poslovne in tržne prakse	°neprimerno trgovanje/tržne prakse °tržne manipulacije °interno trgovanje °nepooblaščene aktivnosti °pranje denarja
		Napake v produktih	°produktni defekti (nedovoljene sestavine) °napake v modelih
		Selekcija, jamstvo in izpostavljenost	°neupoštevanje navodil pri poizvedovanju o komitentu °prekoračenje dovoljenih izpostavljenosti pri komitentu
		Svetovalne storitve	°pritožbe zoper svetovalčeve aktivnosti
Poškodbe fizičnih (osnovnih) sredstev	Izguba povzročena zaradi: °škode ali °poškodbe fizičnih (osnovnih) sredstev kot posledice naravne katastrofe in ostalih dogodkov	Katastrofe in ostali dogodki	°naravne katastrofe °izgube zaradi zunanjih človeških dejavnikov (terorizem, vandalizem)
Prekinitev poslovanja in sistemske napake	Izguba povzročena zaradi prekinitve poslovanja ali sistemskih napak	Sistemi	°strojna in računalniška oprema - hardware °programska oprema °telekomunikacije °izpad zaloge potrebnih stvari
Izvedbe procesov in upravljanje postopkov	Izguba povzročena zaradi neuspelega procesiranja transkacij, napačnega vodenja postopkov iz naslova poslovanja z nasprotno stranjo ali komitenti	Zajemanje transakcij, izvedba transakcij in vzdrževanje transakacij	°napačna komunikacija °napačen vnos podatkov, vzdrževanje ali polnjenje podatkov v bazo °prekoračen končni rok ali odgovornost °napačno delovanje sistema/modela °računovodska napaka °napačno izvajanje ostalih nalog °napačna dostava °vzdrževanje referenčnih podatkov
		Spremljanje in poročanje	°neizpolnitev obveznega poročanja °neustrezno poročanje zunanjim institucijam
		Pridobivanje komitentov in dokumentacija	°pravni dokumenti manjkajo oz. so nepopolni
		Upravljanje s komitenti in produkti	°dodeljen neupravičen dostop do računov komitentov °napačni podatki o komitentu

KATEGORIJA ŠKODNIH DOGODKOV (1.NIVO)	DEFINICIJA	KATEGORIJE (2.NIVO)	PRIMERI AKTIVNOSTI
			° poškodba komitentove lastnine zaradi malomarnosti
		Poslovni partnerji	° neizvršitev obveznosti pogodbe ne stranke, ki ni komitent banke ° razli čni spori s pogodbenimi strankami
		Prodajalci in oskrbovalci	° zunanji dobavitelji ° spori s prodajalci

Vir: The New Basel Capital Accord, 2001 (Povzetki v slovenščini).