Upravljanje pogreškama u uslužnom sustavu na primjeru banke

Udovičić, Anita

Sveučilište u Zagrebu

Ekonomski fakultet

Diplomski sveučilišni studij Poslovna ekonomija – Menadžment

UPRAVLJANJE POGREŠKAMA U USLUŽNOM SUSTAVU NA PRIMJERU BANKE

Diplomski rad

Anita Udovičić

Zagreb, rujan, 2019.

Sveučilište u Zagrebu

Ekonomski fakultet

Diplomski sveučilišni studij Poslovna ekonomija – Menadžment

UPRAVLJANJE POGREŠKAMA U USLUŽNOM SUSTAVU NA PRIMJERU BANKE

ERROR MANAGEMENT IN THE SERVICE SECTOR ON THE BANK EXAMPLE

Diplomski rad

Anita Udovičić, 0067497947

Mentor: Izv. prof. dr. sc. Jasna Prester

Zagreb, rujan, 2019.

Anita Udovičić

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu, 02.09.2019. _____

(potpis)

SAŽETAK

Razvoj financijskih usluga s rastućom razinom informacijske tehnologije, čine aktivnosti banaka, a time i njihove profile rizika sve složenijima pri čemu se ističe značajan utjecaj operativnih rizika na konačne rezultate poslovanja. Sve češće zabilježeni slučajevi velikih operativnih gubitaka, jačaju svijest organizacija o važnosti uspostavljanja djelotvornog sustava za upravljanje operativnim rizicima te identificiranje ključnih mjera za sprječavanje i ublažavanje istih. U postizanju navedenog, vidljiva je važna uloga adekvatnog menadžmenta koji obuhvaća skup vrijednosti zaposlenika i organizacije, stavova, sposobnosti i ponašanja koji određuju stil i metode uspješnog upravljanja. Teorijski dio rada, zajedno s empirijskim, ukazuje na ključne aspekte operativnih rizika te izdvaja relevantne elemente učinkovitog okvira upravljanja.

Ključne riječi: operativni rizik, bankovni sektor, menadžment, usluge

SUMMARY

The development of financial services with the increasing level of information technology makes banks' activities, their time and their risk profiles increasingly complex. This makes a significant impact of operational risks to final business results. Increasingly reported cases of major operational losses are raising the organization's awareness of the importance of having an effective operational risk management system and identifying key measures for preventing and mitigating them. In achieving this, the important role of adequate management is evident, which is encompassing a set of employee and organization values, attitudes, abilities and behaviors that determine the style and methods of successful management. The theoretical part of the paper, together with the empirical one, points to various aspects of operational risks and highlights the relevant elementary management frameworks.

Key words: operational risk, bank sector, management, services

SADRŽAJ

1. Uvod

1.1. Područje i cilj rada

Stalni rast i razvoj financijskih usluga podržan odgovarajućim tehnološkim razvojem čini aktivnosti bankama sve složenijima što povećava mogućnost nastanka grešaka, a time i potencijalnih gubitaka, bilo zbog propusta djelatnika ili neadekvatnih informacijskih sustava. Takvi operativni rizici mogu imati značajan utjecaj na svakodnevno poslovanje banaka i njihov konačni financijski rezultat.

Stoga predmet ovog rada jesu ključni aspekti upravljanja pogreškama u bankarskom sektoru koji operativne rizike svode na minimum. Cilj rada je ukazati na važnost menadžmenta pri kreiranju jasne i uspješne strategije upravljanja pogreškama u poslovanju banaka. Svrha rada jest izdvojiti relevantne elemente učinkovitog okvira za upravljanje operativnim rizikom koji mogu biti univerzalno primjenjivi u svim bankama neovisno o različitostima u njihovoj veličini i opsegu rada.

1.2. Izvori i metode prikupljanja podataka

Teorijski dio rada temelji se na sekundarnim izvorima podataka kao što su knjige, znanstveni članci, doktorske disertacije te internetski izvori relevantne literature koja se bavi problematikom operativnih rizika i upravljanja pogreškama u bankarskom sektoru.

Empirijski dio rada obuhvaća studiju slučaja, u sklopu koje će se razmotriti primjer poslovne banke s fokusom na operativne rizike koji se javljaju u poslovanju. Ključni operativni rizici sagledat će se s aspekta grešaka vezanih uz sustav te grešaka vezanih uz osoblje.

Studija slučaja provedena je metodom intervjua. Intervju je proveden sa tri predstavnika banke, na tri razine menadžmenta: top menadžment, srednji menadžment te operativni menadžment.

1.3. Sadržaj i struktura rada

Rad se sastoji od 5 poglavlja. U prvom uvodnom poglavlju istaknuto je područje te cilj rada, navedeni su izvori te metode prikupljanja podataka u teorijskom i empirijskom dijelu te je naposljetku iznesen sadržaj rada.

U drugom poglavlju definira se pojam operativnog rizika u bankarstvu te njegove glavne vrste u poslovanju banaka. Nadalje, u drugom poglavlju su izneseni ključni aspekti i specifičnosti operativnih rizika u banci.

Treće poglavlje naglašava utjecaj grešaka na poslovanje i financijski rezultat banaka te je većim dijelom fokusirano na menadžerske aktivnosti pri upravljanju pogreškama u bankarskom poslovanju putem različitih mjera za sprječavanje, ublažavanje i uklanjanje grešaka.

Četvrto poglavlje obuhvaća studiju slučaja pogrešaka u uslužnom sektoru na primjeru banke podijeljenu na analizu grešaka sustava te analizu grešaka osoblja s konačnim utjecajem na operativno poslovanje banke.

Završni dio rada odnosi se na pregled ključnih točaka iznesenih u radu te iznošenje konačnog zaključka.

Na samom kraju nalazi se popis literature, slika, tablica te ostalih priloga prikazanih u diplomskom radu.

2. Operativni rizici u poslovanju banaka

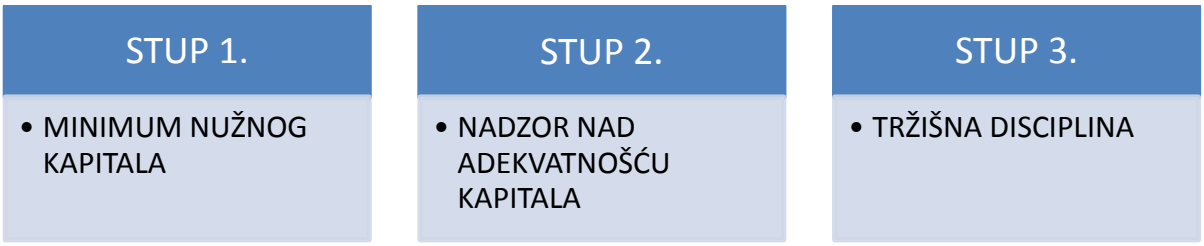
2.1. Pojam operativnih rizika u bankarstvu

Operativni rizici predstavljaju stalnu prijetnju s kojom se financijska industrija neprekidno susreće. Banke su oduvijek provodile organizirane mjere i aktivnosti s ciljem sprečavanja i zaštite od ključnih prijetnji za svoje poslovanje. Strategije upravljanja takvim prijetnjama uglavnom su u prošlosti bile fokusirane na praktične tehnike za smanjivanje potencijalnih gubitaka poput uspostavljanja funkcionalnog zaštitarskog sustava, dok je s druge strane, tek nekolicina bila usmjerenja kreiranju efikasnog cjelovitog sustava za upravljanje operativnim rizikom.

S kontinuiranim razvojem financijskih usluga, a time i popratne informacijske podrške, banke s vremenom sve više mijenjaju smjer svog djelovanja u načinu zaštite i suočavanja sa prijetnjama njihovom poslovanju, te se danas ulaže značajna energija upravo u široke okvire upravljanja operativnim rizikom na razini cijele organizacije. Na promjenu takvih stavova, velikim dijelom je utjecala i potražnja dioničara za transparentnošću i dostupnošću ove vrste informacija. Najvažniji poticaj u mijenjaju stavova prema operativnom riziku, svakako je regulacija propisana od strane Bazelskog odbora za nadzor banaka koja obvezuje banke na primjenu propisane skupine načela koja čini okvir za djelotvorno upravljanje i nadzor nad operativnim rizikom (Crouhy, Galai, Mark, 2006).

Ključna karakteristika Bazelskog sporazuma je njegova struktura koja se temelji na tri osnovna stupa prikazana slikom 1.

Slika 1. Struktura Bazelskog sporazuma



Izvor: Basel (2003)

Stupovi su međusobno komplementarni i doprinose ostvarivanju ukupnog cilja Bazelskog sporazuma, a to je poboljšanje kvalitete upravljanja rizicima te osiguravanje financijske stabilnosti. Stup 1 definira pravila za izračunavanje kreditnog i operativnog rizika, pri čemu za operativni rizik nudi tri metode izračuna kapitalnih zahtjeva:

1) pristup osnovnog pokazatelja
2) standardizirani pristup
3) pristup naprednog mjerenja

Obzirom da su banke izložene i nizu drugih rizika, kapitalni zahtjevi koji proizlaze iz stupa 1 nisu dovoljni za pokriće ostalih rizika. Upravo zbog toga, stupom 2 definiran je sustav nadzora nad ostalim rizicima pri čemu je posebno naglašena uloga revizije. Stup 3 također služi kao podrška stupu 1. Naime, primjena propisanih standarda mjerenja kreditnog i operativnog rizika, nosi sa sobom obvezu objavljivanja dodatnih informacija što utječe na veću transparentnost poslovanja i otpornost financijskog sustava na rizike.

Nadalje, prema Bazelskom odboru za nadzor banka (2003) operativni rizik predstavlja rizik od gubitka koji proizlazi iz neodgovarajućih ili neuspješnih unutarnjih procesa koji mogu biti rezultat ljudskih pogrešaka ili pogrešaka sustava te nepredvidljivih vanjskih utjecaja i neusklađenosti sa zakonskim regulativama, isključujući strateški i reputacijski rizik.

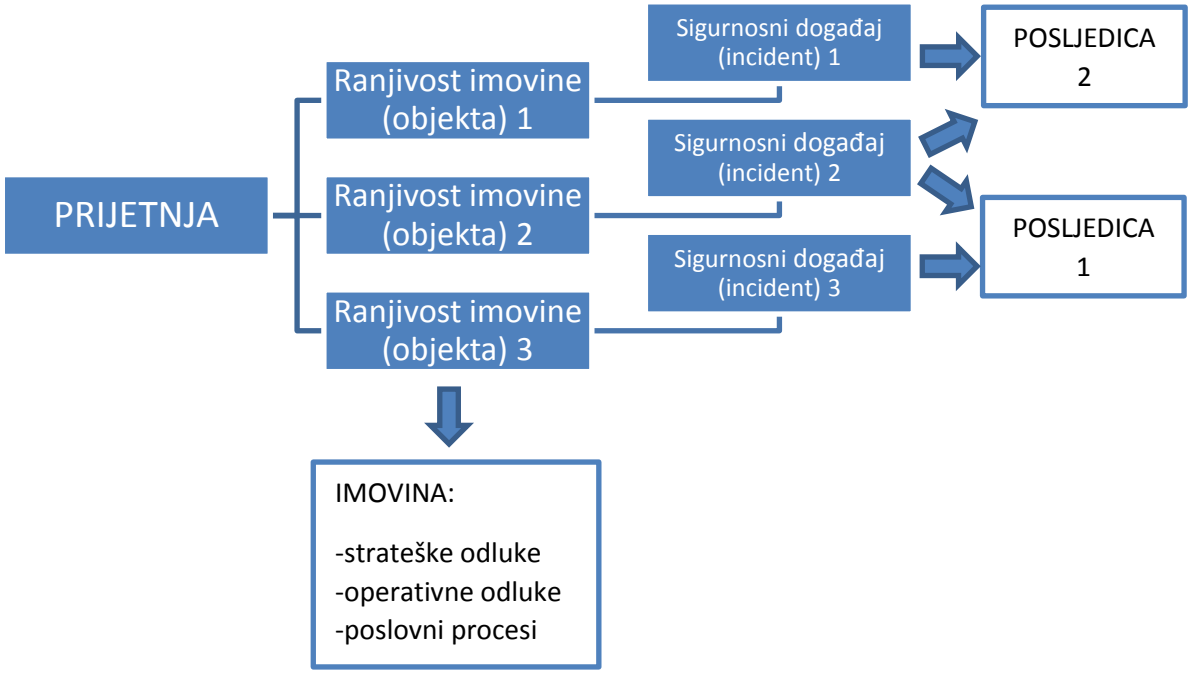
Međutim, operativni rizik može imati mnoštvo različitih definicija i značenja unutar bankarske industrije te stoga pojedine banke mogu odabrati i usvojiti različite definicije operativnog rizika sukladno njihovom internom poslovanju. Prilikom kreiranja vlastite definicije važno je da banke imaju jasnu sliku o tome što se podrazumijeva pod operativni rizik budući da je to ključno za učinkovito upravljanje i kontrolu rizika te ostvarivanje konkurentske prednosti.

Također je važno da interna definicija razmatra cijeli spektar različitih vrsta operativnih rizika s kojima se banka suočava te da ujedno obuhvaća najznačajnije uzroke ozbiljnih operativnih gubitaka. Za kreiranje adekvatne definicije nužno je pravilno razumijevanje ključnih pojmova u okviru operativnih rizika informacijskih subjekata. Stoga, informacijski sustav subjekata prema HANFA (2014), predstavlja sustav međusobno povezanih organizacijskih, tehnoloških

i ljudskih elemenata subjekata uključenih u procese obrade podataka, u cilju raspolaganja informacijama potrebnima za ostvarivanje poslovnih ciljeva.

Nadalje, informacijska tehnologija je element informacijskog sustava, čija je svrha automatizacija obrade podataka te obuhvaća različite hardverske i softverske komponente. Korisnici informacijskog sustava su sve pravne i fizičke osobe koje, kao zaposlenici subjekta, vanjski suradnici, klijenti, regulatorne institucije ili u bilo kojoj drugoj ulozi, sudjeluju u procesima obrade podataka, a ona obuhvaća sve ručne ili automatizirane aktivnosti vezane uz podatke tijekom njihovog cjelokupnog životnog ciklusa poput prikupljanja, unosa i pohrane. Provedbu takvih aktivnosti omogućuju razni resursi kao što su zaposlenici, vanjski suradnici, tehnologija, licence, stručna znanja i ostalo. Prema tome, rizik informacijskog sustava podrazumijeva vjerojatnost da određena prijetnja iskorištavanjem ranjivosti resursa ostvari negativan učinak na poslovanje subjekta. Ukoliko se to dogodi, dolazi do pojave sigurnosnog događaja, odnosno incidenta. Grafički prikaz procesa operativnog rizika prikazan je slikom 2. gdje se može vidjeti da je problem pojave rizika vrlo složen i višedimenzionalni problem, odnosno vidljiva je ovisnost o nizu faktora koji se djelomično mogu kontrolirati, ali ujedno i ovisnost o nizu faktora koji su van dometa i utjecaja poslovnog sistema, odnosno organizacije.

Slika 2. Grafički prikaz procesa nastanka operativnog rizika



Izvor: Adelsberger, Buntak (2011)

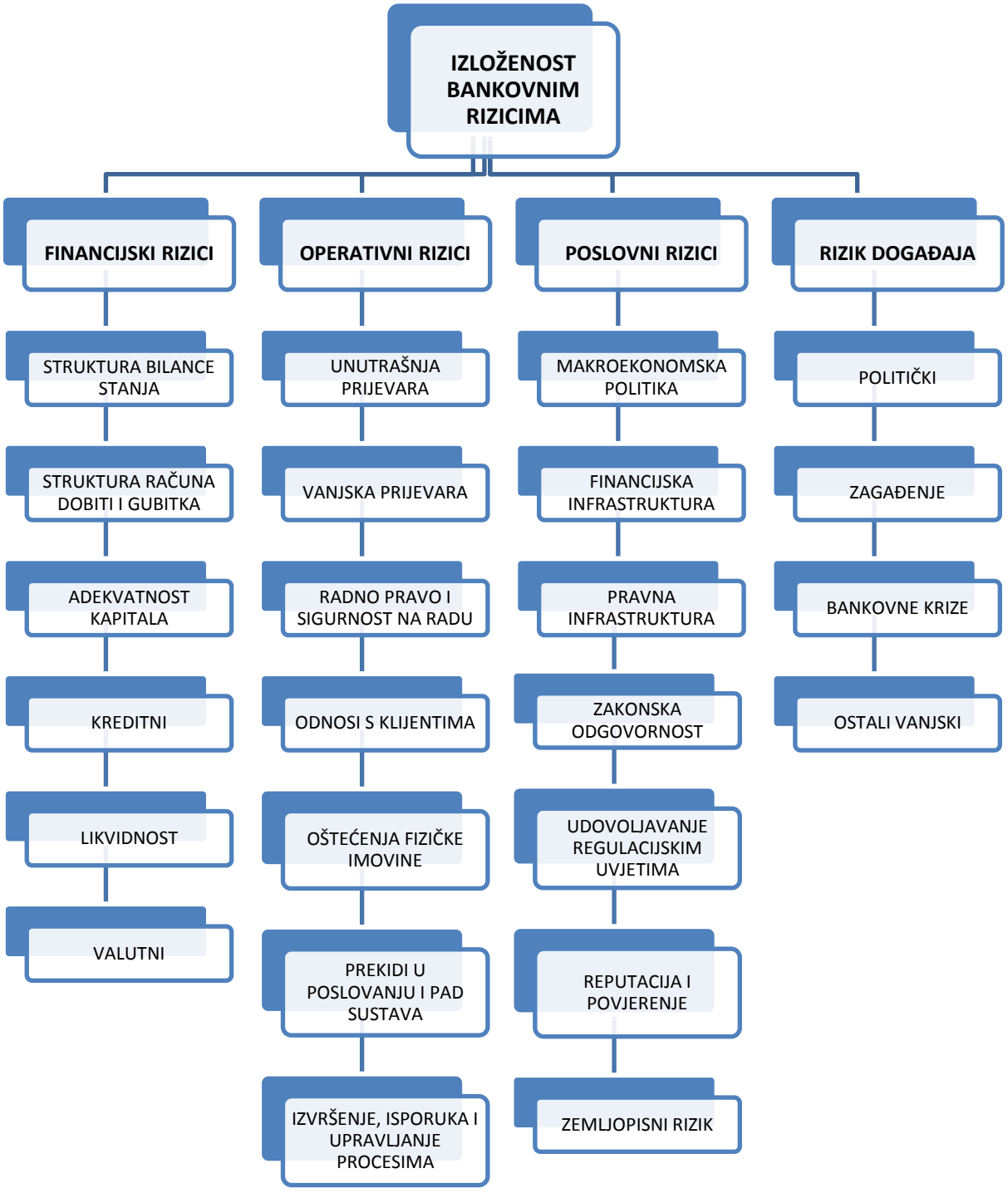
Preduvjet i rješenje uspješnog praćenja operativnih rizika je jasna identifikacija događaja operativnog rizika (Brzović, 2016). Ključan događaj operativnog rizika nije uvijek lako uočiti budući da su djelatnici često zaokupljeni rješavanjem svakodnevnih operativnih poslovnih problema i obavljanjem vlastitih dužnosti. Također, djelatnici mogu izbjegavati prijavu ključne greške zbog straha od mogućih sankcija. Ukoliko se problem redovito ponavlja, često se može percipirati kao normalna vrijednost te se stoga neće prepoznati kao operativni rizik. Ponekad se prijava takvih grešaka namjerno neće prijaviti iz razloga što njome nisu prouzročeni konkretni gubici. U određenim slučajevima problemi se mogu riješiti, a da pritom ne dovedu do konkretnih gubitaka za tvrtku, stoga operativni rizici ne moraju nužno prelaziti u operativne gubitke.

Nerazumijevanje operativnog rizika uvelike otežava identifikaciju i klasifikaciju operativnih rizičnih događaja, što negativno utječe i na druge faze u procesu upravljanja operativnim rizicima. Stoga je kreiranje efikasnog okvira za upravljanje operativnim rizicima, koji su svugdje prisutni, svakako jedan od najvećih izazova za svaku odgovornu osobu i za tvrtku u cjelini. Svjesnost prisutnosti operativnih rizika preduvjet je uspješnog poslovanja i težnja kvalitetnijem i efikasnijem poslovanju te ostvarivanju boljih poslovnih rezultata (Brzović, 2016).

2.2. Vrste operativnih rizika u poslovanju banaka

Razvoj bankovnih praksa koji se najviše očituje u povećanom korištenju složene tehnologije sukladno zahtjevima povećanog opsega poslovanja sa stanovništvom i korištenja elektronskog bankarstava, upućuje na to da, osim kreditnoga, kamatnoga i tržišnog rizika i ostali rizici mogu biti veoma značajni. Prepoznavanje ovih promjena i njihovih utjecaja na povećani stupanj izloženosti operativnom riziku, uvjetovalo je ulaganje sve većih napora i resursa za pravilno razumijevanje i identifikaciju, a zatim i adekvatno upravljanje različitim vrstama operativnog rizika. Slika 3. prema Greuning, Bratanović (2012), pokazuje da su banke izložene čitavom spektru rizika u svojem poslovanju te da upravo operativni rizik pripada jednoj od 4 osnovne skupine.

Slika 3. Spektar bankovnih rizika



Izvor: Greuning, Bratanović (2012)

Iz slike 3. vidimo da su operativni rizici vezani uz ukupnu bankovnu organizaciju i funkcioniranje unutrašnjeg sustava uključujući informatičku tehnologiju i ostale tehnologije, usklađenost bankovnih politika i procedura te mjere zaštite prijevara od pogrešaka u poslovanju (Greuning, Bratanović, 2012). Odnosno, navedene vrste događaja zbog kojih nastaje operativni rizik mogu dovesti do značajnih gubitaka.

Unutarnja prijevara se tako može očitovati kroz namjerno pogrešno izvješćivanje o pozicijama ili različite oblike krađe zaposlenika. Prema Baselu (2003), vanjska prijevara se najčešće očituje kroz pljačke, krivotvorenja, izdavanje čekova bez pokrića te neovlaštene uporabe tuđeg računala. S druge strane, u okviru praksi koje su vezane za zapošljavanje i zaštitu na radnom mjestu, može doći do kršenja pravila o zdravlju i zaštiti zaposlenika, diskriminacije, što dovodi do potraživanja radnika vezana uz različite naknade. Najčešći uzročnici operativnih rizika u okviru kategorije odnosa s klijentima, proizvoda i poslovne prakse jesu kršenje povjereničkog odnosa, zloupotreba povjerljivih informacija o klijentima, neprimjerene aktivnosti trgovanja na računu banke, pranje novca te prodaja neovlaštenih proizvoda (Foot, 2002). Značajne gubitke također uzrokuju i prekidi u poslovanju koju nastaju uslijed zastoja tehničke i informatičke podrške kao što su kvar hardvera i softvera te razni telekomunikacijski problemi. Oštećenja materijalne imovine uzročnicima poput terorizma, vandalizma, potresa, poplava i ostalih vremenskih neprilika, imaju manji stupanj učestalosti ponavljanja pa samim time i rjeđe uzrokuju gubitke. Nadalje, greške zaposlenika u unosu podataka klijenata i ostalih relevantnih informacija također mogu uzrokovati operativni rizik koji obuhvaća rizične događaje vezane za izvršavanje, isporuku i upravljanje procesima gdje se kao česti primjeri javljaju greške poput izrade nepotpune pravne dokumentacije te loša komunikacija sa vanjskim izvršiteljima usluge. Obzirom na vidljivi raznoliki spektar uzročnika operativnih rizika, svaka organizacija dužna je identificirati postojeće izvore operativnog rizika kao i potencijalne izvore tog rizika koji mogu nastati uvođenjem novih poslovnih proizvoda, sistema ili aktivnosti.

Prema definiciji operativnog rizika prema Baselu (2003) pojašnjenoj u prvom poglavlju radu, primjećujemo da je Bazelski odbor ostavio mogućnost da svaka banka promijeni osnovnu definiciju, a time i identificira vlastite ključne vrste operativnog rizika. Prema tome, pojedine vrste operativnih rizika možemo promatrati upravo u okviru gore navedenih događaja i primjera koji uzrokuju operativni rizik te su isti detaljno prikazani u tablici 1.

Tablica 1. Vrste operativnih rizika u okviru uzrokovanih događaja

1. INTERNE PRIJEVARE	**1.1 Neovlaštene aktivnosti** Gubici zbog kršenja zakona, ugovora, internih pravila i procedura	Neprijavljene ili neovlaštene transakcije
		Pogrešno obavljene operativne aktivnosti
		Namjerno manipuliranje dokumentacijom
	1.2 Krađe i prijevare Gubici zbog aktivnosti čiji je cilj stjecanje vlastite (ekonomske) koristi	Kreditna prijevara, podmićivanje i/ili pranje novca
		Iznuđivanje, pronevjera i/ili pljačka
		Zloupotreba imovine banke
	1.3 Unutrašnji sistem	Zloupotreba IT sistema
2. EKSTERNE PRIJEVARE	**2.1 Krađe i prevare** Gubici zbog aktivnosti čiji je cilj stjecanje vlastite (ekonomske) koristi	Krivotvorenje
		Provala / krađa - neovlašteno korištenje bankomata
		Zloupotreba čeka (izdavanje čeka bez pokrića)
	2.2 Vanjski sistem Gubici zbog nedozvoljenog pristupa ili pokušaja pristupa IT sistemu banke s ciljem manipuliranja podacima banke	Nedozvoljen pristup i oštećenje aplikacija
		Oštećenje mrežnog servera
		Upad kompjuterskih virusa
	2.3 Druge namjerne aktivnosti Gubici zbog namjerno prouzrokovane štete banci, ali bez osobne koristi za počinioca štete	Vandalizam
		Oštećenje imovine banke
3. ODNOS PREMA ZAPOSLENIMA I SIGURNOST RADNOG OKRUŽENJA	**3.1 Odnos prema zaposlenima** Gubici zbog neprimjenjivanja zakona o radu	Potraživanja zaposlenih vezana za naknade i beneficije ili nelegalan prestanak radnog odnosa
		Organizirane sindikalne ili radničke aktivnosti
	3.2 Sigurnost radnog okruženja Gubici zbog neprimjenjivanja zakona i regulativa vezanih za zdravstvenu i socijalnu zaštitu zaposlenih	Fizičke povrede zaposlenih
		Kršenje pravila o zdravlju i sigurnosti zaposlenih
	3.3 Različitost i diskriminacija	Potraživanja vezana za sve oblike diskriminacije zaposlenih/kandidata za posao
4. KLIJENTI, PROIZVODI I POSLOVNA PRAKSA	**4.1 Prikladnost, transparentnost i povjerljivost** Gubici zbog neprofesionalnog ponašanja prema klijentima	Kršenje tajnosti podataka
		Netransparentnost prema klijentima
		Nedozvoljena trgovinska praksa
	4.2 Neadekvatna poslovna praksa Gubici zbog neodgovarajuće tržišne prakse	Kršenje antimonopolske regulative
		Tržišna manipulacija i/ili nedozvoljena trgovina
		Obavljanje nelicencirane aktivnosti
	4.3 Greške u proizvodima/uslugama Gubici zbog grešaka u proizvodima/uslugama ili modelima i/ili greške u ugovorima	Greške u modelima
		Nejasne ili kažnjive klauzule ugovora
	4.4 Selekcija, sponzorstvo i izloženost prema klijentima	Greške u selekciji i ispitivanju klijenata
	4.5 Savjetodavne aktivnosti	Sporovi u vezi sa obavljanjem savjetodavnih aktivnosti i/ili žalbe na informacije
	4.6 Nezgode i opća sigurnost	Fizičke povrede klijenata unutar prostora banke
		Štete ili povrede trećih lica učinjene resursima
5. ŠTETE NA FIKSNOJ IMOVINI	**5.1 Prirodne katastrofe**	Oštećenja imovine i ljudski gubici
	5.2. Katastrofe uzrokovane ljudskim faktorom	Svi troškovi i dugovi zbog prekida i obnove uslijed katastrofa prouzrokovanih ljudskim faktorom
	5.3 Zakonski i politički rizik	Zakonske promjene
		Političke promjene
6. PREKIDI POSLOVANJU	**6.1 Neadekvatnost, neefikasnost, loše funkcioniranje ili pad IT sistema**	Nedostupnost aplikacija/primanja i slanja podataka
	6.2 Neraspoloživost vanjskih usluga	Pad sistema javnih usluga
7. IZVRŠENJE, ISPORUKA I UPRAVLJANJE PROCESIMA	**7.1 Upravljanje procesima, obuhvaćanje i izvršavanje transakcija**	Greške pri unosu podataka/održavanju
		Propuštanje rokova i drugih preuzetih obaveza
		Računovodstvene greške
		Propusti u isporuci
	7.2 Nadzor i izvještavanje Gubici zbog neažurnog/netočnog izvještavanja	Propusti u obaveznom izvještavanju
		Netočni eksterni izvještaji
	7.3 Prijem klijenta	Nepotpuna dokumentacija klijenta
	7.4 Vođenje računa klijenta	Neovlašten pristup računu klijenta
	7.5 Poslovni partneri	Loš rad poslovnih partnera / sporovi

Izvor: Kozarević (2006.)

Iz tablice 1. vidimo široki spektar različitih događaja koji uzrokuju brojne vrste i podvrste operativnih rizika čija učestalost varira u pojedinim bankama. Osim prikazanog načina identifikacije operativnih rizika u okviru uzrokovanih događaja, banke također mogu vršiti identifikaciju prema linijama svog poslovanja kao što su poslovanje sa privredom, trgovina i prodaja, poslovanje sa stanovništvom, komercijalno bankarstvo, plaćanja i obračuni, agentski poslovi, poslovi upravljanja imovinom te brokerski poslovi sa stanovništvom.

Prema odboru za nadzor banaka (Basel, 2003) moguća su 4 sljedeća pristupa identifikaciji operativnih rizika: razvrstavanje rizika, indikatori rizika, mjerenje te samoprocjenjivanje. Proces razvrstavanja rizika provodi se kroz sve organizacijske jedinice kako bi se dobile informacije o njihovim izloženostima različitim tipovima rizika. Indikatori rizika su statistički podaci koji upućuju na rizične aktivnosti svake jedinice poput primjerice broja žalbi korisnika ili broja propalih trgovinskih transakcija. Pojedine banke, u svrhu identifikacije, koriste i prošle podatke iz svojih sustava o ostvarenim gubicima te ih kombiniraju sa eksternim podacima ili analizama mogućih modela i scenarija. U tu svrhu se može primijeniti predložak evidencije incidenata prikazan u tablici 2. Svaka organizacija razvija svoj način evidencije, ali prikazani primjer dobro ilustrira što se obično registrira za svaki incident.

Tablica 2. Primjer evidencije incidenata operativnih rizika

RD. BR.	**DATUM POČETKA DOGAĐAJA**	**ORG. JEDINICE**	**VRSTA DOGAĐAJA ID**	**STATUS ID**	**UZROK ID**	**TIP ID**	**OPIS DOGAĐAJA**	**PRIJEDLOG MJERE**
				OTVOREN	LJUDSKI FAKTOR	GUBITAK		
				ISTRAŽUJE SE	PROCESI	OPERATIVNA DOBIT		
				KOMPLETIRAN	SISTEMI	IZBJEGNUTI GUBITAK		
				ODOBREN	VANJSKI FAKTOR	PROPUŠTENA DOBIT		
				ZATVOREN				

Izvor: Adelsberger, Buntak (2011)

Jedan od čestih formalnih oblika samoprocjenjivanja jest upotreba listi za provjeru. Tablica 3. prikazuje jedan od primjera liste za provjeru interne prijevare putem kojih odgovorno osoblje svake organizacijske jedinice odgovara na listu pitanja.

Tablica 3. Lista za provjeru interne prijevare

Pitanje	Primjeri	LISTA ZA PROVJERU – interne prijevare								
		Status		Priroda rizika		Nivo rizika				Komentar
		Da	Ne	Poten. (P)	Real. (R)	Frek.	Utjecaj			
							LMH	MPL	PML	
1	2	3	4	5	6	7	8	9	10	11
1) Postoje li rizici kršenja zakona, ugovora, internih pravila i procedura od strane zaposlenika u cilju stjecanja vlastite koristi?	Neprijavljene transakcije									
	Neovlaštene transakcije									
	Pogrešno obavljene operativne aktivnosti									
	Pogrešno utvrđivanje i izvještavanje o pozicijama									
	Namjerno manipuliranje dokumentacijom									
	Zloupotreba povjerene odgovornosti									
	Ostalo									
2) Postoje li rizici krađa i prevara od strane zaposlenika?	Kreditna prijevara									
	Iznuđivanje, pronevjera i/ili pljačka									
	Zloupotreba imovine banke									
	Zlonamjerno uništavanje imovine banke									
	Ostale zlonamjerne i nelegalne aktivnosti									
	Ostalo									
3) Postoje li rizici nedozvoljenog pristupa i korištenja informacija iz IT sistema banke, zlonamjerne manipulacije, oštećenja i/ili brisanja podataka od strane zaposlenika?	Zloupotreba IT sistema									
	Manipuliranje programima									
	Loša upotreba povjerljivih podataka									
	Ostale vrste kompjuterskog kriminala									
	Ostalo									

Izvor: Kozarević (2006.)

Kategorija ostalo u tablici podrazumijeva rizike koji nisu obuhvaćeni prethodno navedenim primjerima, a koji se mogu svrstati u pripadajuću potkategoriju operativnog rizika, u skladu sa postavljenim pitanjem. Oznake LMH, MPL i PML označavaju mali, srednji, veliki utjecaj te maksimalni mogući gubitak i maksimalni vjerojatni gubitak.

Osnovne liste za provjeru sastoje se od niza pitanja sa ponuđenim odgovorima na koje odgovorene osobe daju pozitivan ili negativan odgovor. U kompleksnijim organizacijama, takav tip identifikacije u pravilu provode specijalizirane organizacije za upravljanje rizicima sa unaprijed prilagođenim listama za pojedine djelatnosti. Složenije liste obuhvaćaju proširene upitnike koji pored osnovnih definiranih pitanja sadrže i dodatna koja nisu unaprijed pripremljena. Izrada odgovarajuće učinkovite liste izrazito je zahtjevna aktivnost koja najviše ovisi o vještinama ovlaštenog kadra odgovornog za izradu i provedbu. Stoga se subjektivni rezultat javlja kao najveći nedostatak samoprocjenjivanja putem lista za provjeru te s ciljem izbjegavanja istog, nužno je da više osoba sastavlja liste te kasnije procjenjuje rezultate.

Također, još jedan od mogućih načina samoprocjenjivanja može biti i provedba radionica koje u pravilu vode eksperti, odnosno nezavisno osoblje. Radionice podrazumijevaju rasprave odgovornog osoblja o temama izloženosti riziku, njegovoj kontroli te mogućim aktivnostima koje bi trebalo poduzeti u svrhu zaštite od rizika.

Uzimajući u obzir sve navedene moguće načine prepoznavanja i identificiranja operativnih rizika, vidljiv je široki spektar njihovih potencijalnih vrsta i podvrsta te je nemoguće odrediti njihov točan broj i univerzalnu klasifikaciju. Nužno je stoga da svaka banka formira vlastitu klasifikaciju ključnih vrsta u skladu sa vlastitim postavljenim poslovnim ciljevima, strategijama i poslovnom procesima (HANFA, 2014). Odnosno, potrebno je odrediti sve resurse koji imaju ulogu u ostvarivanju poslovnih ciljeva te podrške poslovnim procesima, a zatim procijeniti i njihovu važnost u tim ulogama kako bi se mogao odrediti realan utjecaj rizika na cjelokupno poslovanje. Takva pravilna procjena i identifikacija ključnih operativnih rizika predstavlja preduvjet uspješnog upravljanja istima s ciljem ostvarivanja konačnog uspješnog poslovnog rezultata.

2.3. Ključni aspekti operativnih rizika u banci

Bankarsko poslovanje puno je rizika, velikih i malih. Najveći rizici tako zahtijevaju i najveću pozornost, a njihovo kategoriziranje razlikovat će se po pojedinoj organizaciji.

Prema nizu intervjua provedenih kroz protekle 3 godine od strane Risk.net (2018) s vodećim svjetskim stručnjacima iz područja upravljanja rizikom u različitim organizacijama za financijske usluge, uzimajući u obzir ponajviše banke, može se izdvojiti 10 najčešćih vrsta operativnih rizika. Tako u 2017. godini prema Risk.net (2017) top 10 operativnih rizika redom od najviše učestalog prema najmanje učestalom čine:

1) Kiber napadi sigurnost podataka
2) Regulacija propisa
3) Vanjsko suradništvo
4) Geopolitički rizik
5) Rizik ponašanja
6) Organizacijske promjene
7) Neuspjeh informatičke tehnologije
8) Aktivnosti pranja novca
9) Unutarnje i vanjske prevare
10) Fizički napadi

Prijetnja od kiber napada u konstantnom je porastu te se isti pojavljuju u sve više različitih oblika te samim time dodatno otežavaju pravovremeno uočavanje i sprečavanje (BCG, 2018). Kako bi se povećala sigurnost osobnih podataka, Europska unija 2018. godine propisuje Opću uredbu o zaštiti podataka, GDPR, prema kojoj u slučaju povrede privatnosti, organizacije mogu imati trošak kazni u iznosu i do 4% od ukupnog globalnog godišnjeg prometa.

Regulatorne promjene na tržištu su stalne te s njima dolazi i do povećanog operativnog rizika kojim se mora na odgovarajući način upravljati. Rizici povezani s regulacijom propisa najviše se očituju u okvirima rasprostranjenosti reformi tržišne strukture te dalekosežnih računovodstvenih praksi. Novčane kazne za nepoštivanje propisa predstavljaju sve složenije prijetnje za financijske organizacije.

Treće mjesto najučestalijih rizika zauzimaju aktivnosti poslovanja sa vanjskim suradnicima. Dodatno, uvođenjem obvezne uredbe GDPR, banke moraju uložiti veće napore u praćenje vanjskih suradnika i njihovo pravilno upravljanje korisničkim podacima. Također, tu se ističe i rizik reputacije koja može biti ozbiljno narušena u slučaju neadekvatnih kontroli i usklađenosti poslovanja vanjskih suradnika s matičnom organizacijom.

Promjenjivo vanjsko okruženje financijske industrije predstavlja uzrok velike nesigurnosti za uspješno poslovanje i opstanak financijskog sektora stoga je nužno pravovremeno razmišljati o mogućim scenarijima, rizicima trećih strana, rizicima preseljenja te upravljanja novim procesima što ujedno uključuje i rizik ponašanja odgovornih osoba pri donošenju ključnih odluka. Kako bi očuvali konkurentsku prednost, vodeće osobe organizacije dužne su prepoznati prijetnje i prilike učestalih tehnoloških promjena i inovacija te na iste odgovoriti adekvatnim organizacijskim promjenama i restrukturiranjem resursa kojima raspolažu.

U top 10 operativnih rizika 2017. godine prema Risk.net (2017) klasifikaciji nalazi se također i rizik gubitaka uzrokovan neuspjehom informatičke tehnologije koji za razliku od kiber kriminala sadrži manje nepoznatih varijabli, ali također može biti jednako štetan. Pored izravnih financijskih gubitaka, uzrokuje istovremeno i indirektne gubitke poput velikog broja postojećih i potencijalnih kupaca.

Nadalje, povećanje količine i brzine globalnih prekograničnih bankarskih transakcija te sofisticiranosti tehnologije pružaju mnoge prilike za različite kažnjive aktivnosti pronevjere novca. Zadnjih godina, takve aktivnosti najviše su zabilježene na području Sjedinjenih Američkih Država te stoga ne čudi kako se upravo na tom području provode i najsnažnije mjere za sprječavanje transakcija sa rizičnim subjektima. Eksterne i interne prijevare, kritični su rizici za svaku organizaciju te zahtijevaju snažne sustave unutarnje kontrole i revizije za izbjegavanje namjernih pogrešaka.

Posljednje mjesto na top ljestvici zauzima rizik fizičkih napada, od kojih je najučestaliji primjer terorizma sa naglaskom na zaštitu zaposlenika, klijenata te financijskih objekata. Poredak navedenih najučestalijih rizika mijenja se svake godine, od kojih se pojedini redovito pojavljuju.

Iz tablice 4. prema Risk. net (2018), vidimo da je u 2018. godini u odnosu na 2017. godinu došlo do pojave novih oblika operativnih rizika s kojima se financijske institucije svakodnevno suočavaju.

Tablica 4. Poredak najučestalijih operativnih rizika u 2017. i 2018. godini

	2018.	2017.	PROMJENA
INFORMACIJSKO TEHNOLOŠKI PREKIDI	1.	1	⇒
SIGURNOST PODATAKA	2.	1	⇒
REGULACIJSKI RIZIK	3.	2	⇓
PRIJEVARE	4.	9	⇑
VANJSKA SURADNJA	5.	3	⇓
POGREŠNA PRODAJA	6.	5	⇓
RIZIK TALENATA	7.	-	-
ORGANIZACIJSKE PROMJENE	8.	6	⇓
NEAUTORIZIRANA TRGOVINA	9.	5	⇓
RIZIK MODELA	10.	-	-

Izvor: Risk.net (2018)

Jedan od novih učestalih oblika jest rizik talenata koji se očituje u stalnoj borbi financijskih industrija da privuku, obučavaju i zadržavaju najkvalitetnije ljudske potencijale na cjelokupnoj organizacijskoj razini, a ponajviše upravo na području menadžerskih pozicija upravljanja (Härle, 2015). Tablica također pokazuje da je u odnosu na prethodnu godinu povećan rizik od unutarnjih i vanjskih prijevara, a s druge strane je smanjen rizik od neovlaštenog trgovanja budući da je značajnije reguliran propisanim zakonskim regulativama i normama dok se na unutarnje i vanjske prijevare i dalje može utjecati u velikoj mjeri sukladno sve većem tehnološkom razvoju koji omogućava rizične napade. Prvo mjesto u obje godine čvrsto zadržava rizik od gubitaka povezan sa tehničkim i informatičkim prijetnjama.

U 2019. godini najavljuje se široki raspon potencijalno rizičnih događaja na koje bi mogao utjecati aktualni Brexit u okviru rizika trećih strana od novih odnosa s dobavljačima, pravnih

rizika od prepravljanja brojnih financijskih ugovora te regulacija zapošljavanja i obuke novog osoblja.

Nadalje, prema Crouhy, Galai, Mark (2006), identifikacija ključnih operativnih rizika može se također vršiti po linijama poslovanja te događajima u kojima postoji značajna izloženost operativnom riziku. Identifikaciju operativnih rizika po linijama poslovanja možemo iščitati iz tablice 5.

Tablica 5. Poslovne linije i vrste događaja koji uzrokuju operativne gubitke

POSLOVNE LINIJE	**VRSTE DOGAĐAJA KOJI UZROKUJU OPERATIVNE GUBITKE**							
	INTERNA PRIJEVARA	EKSTERNA PRIJEVARA	RADNI SPOROVI I SIGURNOST NA RADU	KLIJENTI, PROIZVODI I POSLOVNE USLUGE	OŠTEĆENJA FIZIČKE IMOVINE	PREKIDI POSOVNIH PROCESA I PAD SUSTAVA	IZVRŠENJE, ISPORUKA I UPRAVLJANJE PROCESIMA	**NAJVEĆA UČESTALOST NOVČANIH GUBITAKA**
KORPORATIVNO FINANCIRANJE								
TRGOVINA I PRODAJA								
POSLOVI SA STANOVNIŠTVOM								
KOMERCIJALNO BANKARSTVO								
PLAĆANJE I NAPLATA								
POSREDNIČKE I SKRBNIČKE USLUGE								
UPRAVLJANJE IMOVINOM								
PRODAJA USLUGA INVESTICIJSKOG BANKARSTVA SEKTORU STANOVNIŠTVA								
NAJVEĆA UČESTALOST NOVČANIH GUBITAKA								

Izvor: Greuning, Bratanović (2012)

Iz tablice 5. prema Greuning, Bratanović (2012), najveća učestalost novčanih gubitaka na svjetskoj razini prouzročena je upravo događajima eksterne prijevare, aktivnostima vezanim

za izvršavanje i upravljanje procesima te poslovnu praksu s klijentima i proizvodima. Najznačajniji poslovi koji uzrokuju gubitke vezani su za trgovanje i prodaju, transakcije sa stanovništvom i poduzećima.

Tablica 6. Udjeli operativnih gubitaka po poslovnim linijama za područje Sjedinjenih Američkih Država

POSLOVNA LINIJA	POSTOTAK SVIH GUBITAKA
Poslovanje s privredom	4%
Trgovina i prodaja	9%
Poslovanje sa stanovništvom	39%
Komercijalno bankarstvo	16%
Obračuni i plaćanja	1%
Agentski poslovi	3%
Poslovi upravljanja imovinom	6%
Brokerski poslovi sa stanovništvom	22%

Izvor: Kozarević (2009.)

Tablica 7. Udjeli operativnih gubitaka po tipu događaja za područje Sjedinjenih Američkih Država

TIP DOGAĐAJA	POSTOTAK SVIH GUBITAKA
Interne prijevare	27%
Eksterne prijevare	16,6%
Odnos prema zaposlenima i sigurnost na radu	3,3%
Klijenti, proizvodi i poslovna praksa	48,1%
Štete na fiksnoj imovini	0,3%
Prekidi u poslovanju i pad sustava	0,4%
Izvršenje, isporuka i upravljanje procesima	4,2%

Izvor: Kozarević (2009)

Iz tablica 6. i 7. vidimo da je poslovna linija sa najviše zapažanja poslovanje sa stanovništvom što zauzima 39% svih gubitaka, dok se najučestaliji tip događaja odnosi na klijente, proizvode i poslovnu praksu sa 48,1% svih događaja. Međutim, nije pravilo da najučestalija poslovna linija ili najučestaliji tip događaja ima u isto vrijeme gubitke s najvećim iznosom. Štoviše, češći slučajevi su da događaji koji rjeđe uzrokuju operativne gubitke upravo donose i veće novčane posljedice, dok s druge strane oni najučestaliji tipovi operativnih gubitaka imaju i manje ili srednje značajne novčane gubitke (Kozarević, 2009).

Prema podacima iz 2006. godine, većina banaka u Hrvatskoj nije provodila procjenjivanje, a od 11 banaka koje su prikupljale podatke pokazalo se da je većina gubitaka bila uzrokovana eksternim prijevarama te izvršavanjem i upravljanjem poslovnim procesima što pokazuje da nema značajnih odstupanja u odnosu na procjenjivanja na svjetskoj razini te na procjenjivanja na području Sjedinjenih Američkih Država u istom razdoblju.

Osim propisanih obveznih normi iz Bazelskog sporazuma, financijskim institucijama su na raspolaganju i ostale brojne smjernice za procjenjivanje i ocjenjivanje operativnih rizika. U Hrvatskoj su tako najznačajnije izdane od strane Hrvatske narodne banke te Hrvatske agencije za nadzor financijskih usluga s ciljem razvijanja svijesti o potencijalnim rizicima i upoznavanja s dobrim praksama ublažavanja istih. Hrvatska narodna banka (2016.) stoga kao ključne aspekte ističe da su financijske institucije dužne donijeti i provoditi primjerene politike upravljanja operativnim rizikom, a za tu potrebu dužne su prvenstveno definirati internu definiciju operativnog rizika te odgovarajuće planove postupanja u kriznim situacijama i planove poslovanja kojima se osigurava kontinuitet poslovanja i ograničavaju gubici u slučajevima znatnijeg narušavanja ili prekida poslovanja.

3. Upravljanje grešakama u bankarskom sektoru

3.1. Utjecaj grešaka na poslovanje banaka

Pojava novih prijetnji i grešaka poslovanja, osim direktnih posljedica, može također dovesti i do niza indirektnih posljedica koje uzrokuju još veće dodatne gubitke. Takve indirektne posljedice često nastaju uslijed angažmana i zadržavanja zaposlenika isključivo na rješavanju pojedinog problema, a da se pritom zanemaruju ostale potencijalne prijetnje što u konačnici čini uzročno posljedični krug grešaka (Bickford, 2016). Na prvi pogled lako su uočljive kratkoročne posljedice kao što su financijski gubitak, pravni troškovi i regulatorne kazne, a s druge strane tu su i neizravni učinci poput većih kreditnih troškova te dugotrajnih šteta od reputacije koja može neizbrisivo utjecati na način na koji klijenti, dioničari, regulatori i druge ugovorne stranke gledaju na banku.

U praksi upravljanja operativnim rizicima, banke najčešće veću pozornost pridaju aktivnostima koje mogu prouzročiti veće značajne gubitke, međutim rutinske administrativne pogreške isto tako ne treba zanemarivati. Svakodnevni mogući propusti osoblja poput pogrešnog ili nepravovremenog unosa podataka mogu rezultirati kašnjenjem isporuke usluge što u velikoj mjeri utječe na nezadovoljstvo klijenta i potencijalno stvaranje loše reputacije (Severović, Žajdala, Cvetković, Šoštarić, 2009). Male tehničke pogreške poput unosa tek nekoliko neispravnih znamenki mogu izazvati krucijalne gubitke, bilo na računu banke ili na računu klijenta (Domingo, 2003).

Utjecaj grešaka na poslovanje banaka možemo promatrati kroz međusobne povezane odnose organizacije, zaposlenika i klijenata. Česta praksa za sprječavanje nastanka budućih grešaka osoblja jest upotreba sankcija i kazni za zaposlenike sa nezadovoljavajućom efikasnošću. U okviru takvih sankcija mogući su odbici od plaća, degradiranje na nižu radnu poziciju ili otkaz te ukidanje određenih povlastica. Greške tako direktno utječu na status zaposlenika, budući da od nadređenih dobiva negativne ocjene i novčane kazne što može utjecati na zaposlenikovu motiviranost ili demotiviranost. S jedne strane, takve mjere mogu zaposlenike potaknuti da budu bolji i da se trude izbjegavati ponavljanje učinjenih grešaka, dok s druge strane, kontinuiramo opterećenje i strah od moguće pogreške može upravo izazvati da se greške učestalo ponavljaju.

Kako bi izbjegli sankcije, zaposlenici moraju konstantno voditi brigu o pravovremenom prepoznavanju, rješavanju i sprječavanju problema, što može izazivati veliki pritisak u njihovom svakodnevnom obavljanju radnih aktivnosti i izvršavanju radnih zadataka. Zbog stresnog okruženja i velikog pritiska da se zadaci obave efikasno, može doći do potrebe za prekovremenim radom kojeg mogu zahtijevati nadređeni ili sam zaposlenik kako bi ostvario zadovoljavajuće ciljeve. Međutim, prekovremeni rad i umor može čak i besprijekornim zaposlenicima narušiti koncentraciju i dovesti do nehotičnih pogrešaka.

Takvo radno okruženje s visokom razinom stresa utjecat će na nezadovoljstvo zaposlenika, a u konačnici i potencijalnim promjenama radnog mjesta. Greške stoga indirektno utječu i na velike fluktuacije ljudskih resursa u organizaciji (Bilby, 2015). Gubitak zaposlenika organizaciji donosi nove troškove adekvatnog pronalaska, zapošljavanja i obučavanja novih zaposlenika. Za organizaciju to predstavlja cjelokupan proces i angažman odjela za ljudske resurse što iziskuje dodatno vrijeme i novac. Ukoliko poduzeće pravovremeno ne nađe odgovarajuću zamjenu za zaposlenika koji je napustio radno mjesto, također se mogu pojaviti i sporedni troškovi zbog kašnjenja u obavljanju poslovnih zadataka i pružanju adekvatne usluge.

U konačnici imamo klijente koji čekaju na potrebnu uslugu što uzrokuje njihovo nezadovoljstvo i protest. Pojava grešaka na direktnu štetu klijenata zahtjeva njihovo ulaganje vremena i truda da bi zajedno sa zaposlenicima došli do rješenja problema. Greške tako utječu i na stres klijenata zbog potencijalnih novčanih gubitaka i gubitka njihovog vremena. Njihovo nezadovoljstvo time raste što može rezultirati širenjem negativnih recenzija i loše reputacije. Također, ovisno o razini tolerancije klijenata na pojavu pogrešaka, organizacija može trajno izgubiti jedan dio svojih potrošača. Klijenti koji odlaze nezadovoljni, utjecat će loše stečenim dojmom i iskustvom na druge potencijalne klijente što dovodi organizaciju do višestrukog gubitka postojećih i potencijalnih potrošača. Kako bi se smanjio negativan utjecaj loše reputacije, poduzeće može popraviti dojam kod klijenata kojima je učinjena pogreška raznim oblicima naknada i kompenzacija što također predstavlja određeni dodatni trošak za organizaciju.

Prilikom pojave određene greške, nužna je raspodjela radne snage, budući da se dio zaposlenika fokusira na rješavanje izvanrednog problema, a drugi dio na obavljanje redovnih aktivnosti. Stoga je važno da poduzeće raspolaže obučenim zaposlenicima postavljenim na

odgovarajuće radne pozicije što se postiže ulaganjem u kontinuirane treninge i osposobljavanja. Pored troškova edukacija, pojavljuju se i troškovi nagrada koji povećavaju motiviranost zaposlenika kako bi što bolje obavljali svoje dužnosti i postizali željene rezultate uz najnižu razinu pojavljivanja pogrešaka.

Svi navedeni utjecaji grešaka, međusobno se nadopunjuju i nadovezuju jedni na druge, što naposljetku dovodi do direktnih novčanih gubitaka uzrokovanih greškama osoblja i sustava te ukupno smanjenog obujma poslovanja te lošeg konačnog rezultata (Direct Kaspereit, 2017).

Nadalje, HANFA (2014), utjecaj grešaka promatra u odnosu na informacije kao najvažnije resurse informacijskog sustava. Primjeri informacija s kojima mogu raspolagati subjekti u poslovanju su: informacije o ponuđenim proizvodima i uslugama, informacije o klijentima te informacije o novčanim transakcijama i slično. Raspoloživost točne i pravodobne informacije može utjecati na donošenje ispravnih poslovnih odluka, dok s druge strane, dostupnost osjetljive informacije neovlaštenim osobama može dovesti do gubitka prednosti nad konkurencijom, gubitka povjerenja klijenata, a također i do nepoštivanja mjerodavnih propisa.

U okviru upravljanja greškama u bankarskom sektoru, izuzetno je važno upravljati i sigurnošću informacija i podataka s kojim poduzeće raspolaže. Informacijska sigurnost može se definirati kao zaštićenost informacija i podržavajuće infrastrukture od neautoriziranog pristupa ili modifikacija, slučajnog ili namjernog karaktera, koji mogu nanijeti neprihvatljive gubitke subjektima informacijskih odnosa, pa u tom smislu i vlasniku i korisniku informacija kao i podržavajućoj infrastrukturi. Analizom informacijskih rizika, određuju se mogući poslovni gubici, procjenom prijetnji i ranjivosti i izbora odgovarajućih kontrola, da bi se postigli poslovni zahtjevi za osiguravanjem informacijske sigurnosti na troškovno efikasan način.

Promatrano sa stajališta informacijske sigurnosti, informacije imaju tri ključna svojstva čije narušavanje predstavlja rizik za poslovanje subjekata. Navedena svojstva informacija u okviru odabranih primjera utjecaja grešaka na poslovanje banaka, prikazana su u tablici 8.

Tablica 8. Ključna svojstva informacija s posljedicama narušavanja

KLJUČNA SVOJSTVA INFORMACIJA:	POSLJEDICE NARUŠAVANJA:
POVJERLJIVOST **Svojstvo informacije da je raspoloživa isključivo osobama i sustavima koje za to imaju valjano ovlaštenje**	-gubitak konkurentske prednosti -gubitak povjerenja klijenata -nepoštivanje mjerodavnih propisa -financijski gubici
CJELOVITOST **Svojstvo informacije da postoji razumno uvjerenje u njezinu točnost odnosno da nije neovlašteno ili nepredviđeno izmijenjena, slučajnim ili namjernim djelovanjem, što podrazumijeva i naknadno dodavanje, izmjenu ili brisanje informacija bez traga o provedenim aktivnostima koji se može slijediti**	-donošenje pogrešnih poslovnih odluka -gubitak povjerenja klijenata -nepoštivanje mjerodavnih propisa
DOSTUPNOST **Svojstvo informacije da po potrebi i u prihvatljivom roku bude dostupna ovlaštenim osobama i sustavima**	-nemogućnost isporuke proizvoda i usluga -nepoštivanje mjerodavnih propisa -nemogućnost ispunjavanja ugovornih obveza

Izvor: HANFA (2014)

Narušavanjem svojstava informacija navedenih u tablici 8., nastaju štetni učinci operativnih rizika koji proizlaze iz djelovanja različitih prijetnji. Upravo zbog toga je izrazito bitno identificirati prijetnje i ranjivosti resursa informacijskih sustava te procijeniti rizike i njihove štetne učinke, prema kojima bi se postupalo primjenom odgovarajućih mjera.

3.2. Važnost menadžmenta pri upravljanju greškama u poslovanju banaka

Sastavni dio svakodnevnog poslovanja subjekata čine različiti procesi upravljanja rizicima. Organizacije pritom nastoje prepoznati sve potencijalne aktivnosti i prijetnje koje bi mogle imati negativan utjecaj na ostvarivanje njihovih konačnih ciljeva. Stoga učinkovito upravljanje ovim najrašireniji rizicima predstavlja izvor komparativne prednosti za svako poduzeće u čemu se upravo ogleda važnost uspješnog menadžmenta.

Prema Baselu (2003), upravljanje operativnim rizikom sastoji se od utvrđivanja, procjenjivanja te nadziranja i kontrole rizika. Sustavni pristup menadžmenta takvoj identifikaciji te primjeni mjera i postupaka, kroz proces upravljanja rizicima, može donijeti brojne prednosti za poduzeće, poput primjerice: kvalitetnije zaštite važnih poslovnih procesa i resursa, manje vjerojatnosti nepoštivanja mjerodavnih propisa, kvalitetnije podrške pri donošenju poslovnih odluka, manjem neučinkovitom trošenju sredstava na zaštitne mjere kao i manji utrošak vremena na upravljanje zaštitnim mjerama te još mnoge druge.

Osnovni preduvjet za identifikaciju i procjenu operativnih rizika je ponajprije pravilno poznavanje poslovnih ciljeva, poslovne strategije i poslovnih procesa subjekta, kako bi se mogao procijeniti realni utjecaj rizika na cjelokupno poslovanje (HANFA, 2014). U okviru svakog značajnog operativnog rizika kojeg je banka identificirala, potrebno je također donijeti odluku o upotrebi odgovarajućih postupaka za sprječavanje, smanjenje rizika ili prihvaćanje rizika uz primjenu aktivnosti daljnjeg praćenja. Redovno praćenje može rezultirati brzim otkrivanjem i ispravljanjem nedostataka u politikama, procesima i postupcima upravljanja operativnim rizikom što može značajno umanjiti pojave i ozbiljnost gubitaka. Rezultati praćenja aktivnosti banke trebaju biti sadržani u redovnim izvještajima koja analiziraju članovi odgovornog menadžmenta na različitim razinama te na temelju podataka donose odluke koje mogu biti od krucijalne važnosti za poslovanje banke.

Uzimajući u obzir brojne negativne posljedice koje mogu prouzročiti različiti oblici rizika, vidljivo je da za svako poduzeće, ključno je imati adekvatan organiziran sustav upravljanja koji počiva na pripadajućim adekvatnim menadžerskim vještinama, kako u konačnici poduzeće ne bi bilo izloženo značajnim gubicima. Bit efikasnog upravljanja operativnim rizicima je usvajanje i razvijanje kulture rizika u tvrtki, kako se isti tip rizika ne bi ponavljao u

budućnosti, a svemu prethodi jasno razumijevanje osnove prirode operativnih rizika (Birndelli, Ferretti, 2017).

Problem nerazumijevanja operativnog rizika vrlo je prisutan u praksi i uvelike otežava identifikaciju i klasifikaciju operativnih rizičnih događaja, što se dalje negativno odražava i na ostale faze u procesu upravljanja operativnim rizicima (Brzović, 2016). Shodno tome, kreiranje djelotvornog okvira za upravljanje operativnim rizicima predstavlja jedan od najvećih izazova za svaku odgovornu osobu i cjelokupnu organizaciju budući da svaka uspješna tvrtka ima cilj staviti pod nadzor operativne rizike, te s njima postupati u skladu sa propisima i sa specifičnostima svog poslovanja.

Odgovorni menadžment kao bitna funkcija u organizaciji za koordiniranje ljudskih resursa prema ostvarivanju željenih rezultata, ima ključan zadatak u prepoznavanju vlastitih rizika, određivanju metoda upravljanja i mjerenja te procjene utjecaja na poslovanje. Neuspješno upravljanje operativnim rizikom, koji je prisutan u gotovo svim transakcijama i aktivnostima banke, može uvelike povećati vjerojatnost da neki rizici ostanu neprepoznati i nekontrolirani, (Basel, 2003). Stoga su sve razine menadžmenta odgovorne za stvaranje organizacijske kulture koja daje prioritet djelotvornom upravljanju operativnim rizikom te ustrajanju u provođenju dobrih operativnih kontrola. Upravljanje operativnim rizikom najdjelotvornije je kad organizacijska kultura banke ističe visoke standarde etičnog ponašanja na svim razinama. Odbor i viša uprava trebaju promicati organizacijsku kulturu kojom se djelom i riječima uspostavlja očekivani integritet svih zaposlenika prilikom obavljanja svakodnevnih aktivnosti.

Također, povećana tržišna orijentacija banaka izlaže ih novim rizicima i izazovima zahtijevajući kontinuirane inovacije u načinu upravljanja poslovanjem kako bi se održala njihova konkurentnost. Odgovornost za održivost bankovnih sustava i tržišta redefinirana je u velikom broju država tako da je postala partnerstvom između ključnih sudionika koji upravljaju različitim dimenzijama financijskih i operativnih rizika. Takav pristup potvrđuje da je kvaliteta upravljanja bankom, s naglaskom na proces upravljanja rizicima, ključna za održavanje sigurnosti i stabilnosti kako na razini pojedinačne banke, tako i na razini bankovnog sustava u cijelosti (Greuning, Bratanović, 2006). Tablica 9. pokazuje partnerstvo u upravljanju rizicima u kojoj svaki od ključnih sudionika ima jasno određenu odgovornost za specifičnu dimenziju pojedinog područja upravljanja rizicima.

Tablica 9. Partnerstvo u korporativnom upravljanju bankom

KLJUČNI SUDIONICI I ODGOVORNOSTI	STRUKTURA BILANCE STANJA / STRUKTURA RDG / RIZIK SOLVENTNOST / KREDITNI RIZIK / RIZIK LIKVIDNOSTI / TRŽIŠNI RIZIK / KAMATNI RIZIK / VALUTNI RIZIK / OPERATIVNI RIZIK
SUSTAVNI SUDIONICI:	
Zakonodavna i regulacijska tijela	Uspostava regulacijskog okvira, uključujući ograničenja izloženosti riziku i ostale parametre upravljanja rizicima koji će optimizirati upravljanje u bankovnom sektoru
Tijela za uređivanje i nadzor	Nadzor financijske održivosti i učinkovitosti upravljanja rizicima te provjere udovoljavanju zakonskim propisima
INSTITUCIONALI SUDIONICI:	
Dioničari	Odabir primjerenih nadzornih i izvršnih odbora te revizora
Nadzorni odbori	Osmišljavanje politika za upravljanje rizicima
Izvršni odbori	Stvaranje sustava za primjenu politike nadzornog odbora
Unutrašnja revizija	Provjera usklađenosti politika upravljanja
Vanjska revizija	Pružanje mišljenja o financijskim izvješćima
JAVNOST I KLIJENTI:	
Ulagači	Razumijevanje odgovornosti i ustrajnost na odgovarajućoj objavi podataka
Ocjenjivačke agencije	Informiranje javnosti
Analitičari	Analiziranje informacija o rizičnoj izloženosti i savjetovanje klijenata

Izvor: Greuning, Bratanović (2006)

Nadalje, prema Baselskom odboru (2003), važnost menadžmenta pri upravljanju greškama u poslovanju banaka očituje se kroz 10 načela u okviru sljedećih aktivnosti:

- razvijanje primjerene okoline za upravljanje rizikom
- upravljanje rizikom
- uloga supervizora
- uloga objavljivanja

Načela prema Baselu (2003) su sljedeća:

1) Odbor direktora treba biti svjestan glavnih aspekata operativnog rizika banke kao specifične kategorije rizika kojim treba upravljati, te usvojiti i periodično pregledavati bankovni sustav upravljanja operativnim rizikom. Sustav treba sadržavati odgovarajuću definiciju operativnog rizika na razini banke te postaviti načela prema kojima će se operativni rizik utvrđivati, procjenjivati, nadzirati i kontrolirati odnosno smanjivati.

   Odbor je nadležan za uspostavljanje upravljačke strukture sposobne za primjenu učinkovitog sustava upravljanja operativnim rizikom. Budući da se značajan dio sustava upravljanja operativnim rizikom odnosi na uspostavljanje snažnih unutarnjih kontrola, izuzetno je važno da odbor uspostavi jasnu hijerarhiju upravljačkih nadležnosti, odgovornosti i izvješćivanja. Također, potrebno je razdvojiti nadležnosti i hijerarhiju izvješćivanja funkcija kontrole operativnog rizika, poslovnih aktivnosti i popratnih funkcija kako bi se izbjegli potencijalni sukobi interesa. Sustav također treba jasno odrediti koje procese upravljana operativnim rizikom banka treba imati.

2) U nadležnosti odbora direktora, također je i odgovornost da bankovni sustav upravljanja operativnim rizikom podliježe djelotvornoj i sveobuhvatnoj unutarnjoj reviziji koju obavlja operativno neovisno, primjereno obrazovano i sposobno osoblje. Potrebno je osigurati da su opseg programa revizije i učestalost provođenja primjereni izloženostima riziku. Revizija je odgovorna za periodičnost provjere djelotvorne provedbe sustava upravljanja operativnim rizikom u svim dijelovima banke.

3) Viša uprava odgovorna je za provedbu sustava upravljanja operativnim rizikom koji odobrava odbor direktora. Sustav treba biti dosljedno proveden unutar cijele bankovne organizacije, a zaposlenici na svim razinama dužni su razumjeti svoje odgovornosti koje se odnose na upravljanje operativnim rizikom. Viša uprava također treba biti odgovorna za razvijanje politika, procesa i postupaka upravljanja operativnim rizikom povezanim sa svim značajnim proizvodima, procesima i sustavima banke.

   Okvir za upravljanje operativnim rizikom, uspostavljeno od strane odbora direktora, uprava treba prevesti u konkretne politike, procese i postupke koji se mogu provesti i

provjeriti unutar različitih poslovnih organizacijskih jedinica. Iako je svaka razina uprave nadležna za primjerenost i djelotvornost politika, procesa, postupaka i kontrola koje ulaze u njezin djelokrug, viša uprava odgovara za jasnu raspodjelu ovlasti, nadležnosti i odnose izvješćivanja kako bi potaknula i sačuvala tu odgovornost te osigurala dostupnost resursa potrebnih za djelotvorno upravljanje operativnim rizikom.

Viša uprava osigurava da aktivnosti banke obavlja isključivo kvalificirano osoblje koje posjeduje potrebno iskustvo, tehnički je osposobljeno i koje ima pristup potrebnim resursima. Također, viša uprava treba osigurati da je bankovna politika nagrađivanja u skladu s njezinom sklonosti riziku. Politike nagrađivanja koje nagrađuju osoblje koje odstupa od politike negativno utječu na bankovne postupke upravljanja rizikom.

4) Banke trebaju utvrditi i procijeniti operativni rizik povezan sa svim značajnim proizvodima, aktivnostima, procesima i sustavima. Nadalje, trebaju osigurati da prije uvođenja novih proizvoda, procesa i sustava ili prije poduzimanja novih aktivnosti operativni rizik koji je s njima povezan bude podvrgnut pravilnim postupcima procjenjivanja.

5) Banke su odgovorne za redovno nadziranje profila operativnog rizika i značajnih izloženosti gubicima. Djelotvoran proces nadziranja ključan je za adekvatno upravljanje operativnim rizikom. Aktivnosti redovnog nadziranja mogu rezultirati brzim otkrivanjem i ispravljanjem nedostataka u politikama, procesima i postupcima upravljanja operativnim rizikom. Pravovremeno otkrivanje tih nedostataka i bavljenje s njima može značajno smanjiti potencijalnu učestalost kao i ozbiljnost pojave gubitaka.

6) Banke trebaju imati politike, procese i postupke za kontroliranje odnosno smanjenje operativnih rizika. Važno je periodično preispitivati svoje strategije za ograničavanje i kontroliranje rizika te, s obzirom na svoju sveukupnu sklonost riziku i profil, prilagoditi svoj profil rizika uporabom primjerenih strategija. Odbor direktora, kao i viša uprava nadležni su za uspostavljanje snažne kulture unutarnje kontrole, u kojoj su kontrolne aktivnosti sastavni dio redovnih aktivnosti banke. Kontrolama koje su

sastavni dio redovnih aktivnosti omogućuje se brzo reagiranje na promjenljive uvjete i izbjegavaju nepotrebni troškovi.

7) Banke trebaju izraditi planove za nepredviđene okolnosti i planove za očuvanje kontinuiteta poslovanja kako bi osigurale svoje trajno poslovanje i ograničile gubitke ukoliko dođe do značajnog poremećaja u poslovanju.

8) Bankovni supervizori trebaju zahtijevati da sve banke, bez obzira na veličinu, imaju djelotvoran sustav utvrđivanja, procjenjivanja, nadziranja i kontroliranja značajnih operativnih rizika u sklopu svojega sveukupnog pristupa upravljanju rizikom.

9) Izravno ili neizravno, supervizori obavljaju redovno vrednovanje politika, postupaka i praksa banke povezanih s operativnim rizicima. Također trebaju osigurati da postoje i primjereni mehanizmi koji im omogućuju da budu obaviješteni o kretanjima u bankama.

10) Banke trebaju objavljivati dovoljno informacija kako bi sudionicima na tržištu omogućile da procijene njihov pristup upravljanju operativnim rizikom., budući da pravodobno i učestalo objavljivanje relevantnih informacija banaka može dovesti do poboljšane tržišne discipline, te stoga i do djelotvornijeg upravljanja rizikom. Količina objavljenih podataka treba biti razmjerna veličini, profilu rizika i složenosti aktivnostima banke.

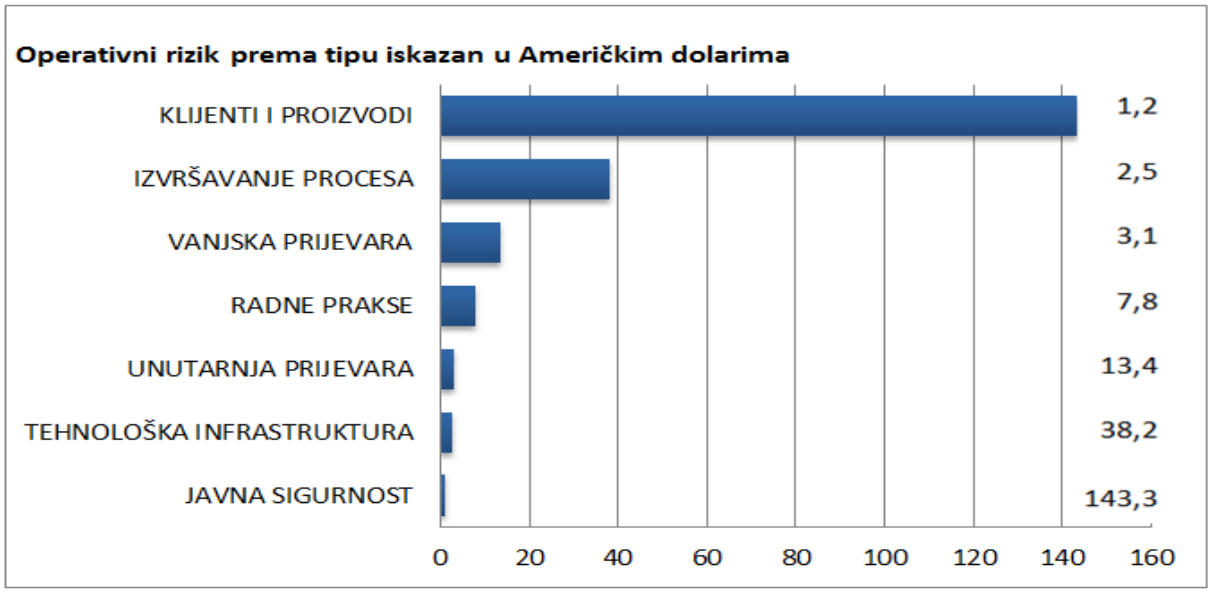
Operativni rizik jedan je od glavnih uzroka najvećih pojedinačnih padova cijena dionica vodećih tvrtki diljem svijeta, što pokazuje da organizacije današnjice još uvijek nedovoljno pažnje pridaju formiranju funkcionalnog sustava za upravljanje rizicima ili ne raspolažu efikasnim resursima koju su odgovorni za kreiranje istog. Stoga je za poduzeća od izuzetne važnosti kvalitetno organiziran menadžment na svim razinama, kao proces uspješne koordinacije ljudskih, materijalnih, financijskih te informacijskih resursa kako bi se postigli zadani organizacijski ciljevi, a prije svega profit i stabilnost. Uspješan menadžment ogleda se tako u posjedovanju temeljnih konceptualnih, socijalnih te tehničkih znanja i vještina koje doprinose kreiranju i ostvarivanju programa za uspješno upravljanje greškama u poslovanju banaka i ostalih financijskih institucija.

3.3. Mjere za sprječavanje, ublažavanje i uklanjanje grešaka u poslovanju banaka

U vremenu nakon završetka globalne financijske krize koja je ostavila značajne posljedice na cjelokupno gospodarstvo, financijske organizacije postale su svjesne značajnosti uspostavljanja regulatornog sustava za upravljanje rizicima te potrebe za ulaganjem dodatnih napora u kreiranje funkcionalnih mjera za upravljanje operativnim rizikom. Prema već spomenutim brojnim negativnim utjecajima operativnih pogrešaka, vidljivo je da takvi gubici mogu biti katastrofalni za poslovanje banaka, kako u novčanom smislu, tako i u pogledu utjecaja na ukupno poslovanje i reputaciju banke, a ponekad i s prijetnjom na opći opstanak organizacije.

Prema Bain & company (2018) u razdoblju od 2011. do 2016. zapaženi su značajni gubici u bankama širom svijeta, uzrokovani upravo operativnim rizikom te je zabilježen ukupan gubitak od približno 210 milijardi američkih dolara. Većina tih gubitaka proizašla je iz grešaka nastalih u interakciji zaposlenika i sustava s klijentima te nedostacima u načinu na koji su se transakcije obrađivale, ili izravnom prijevarom što je vidljivo iz grafa 1.

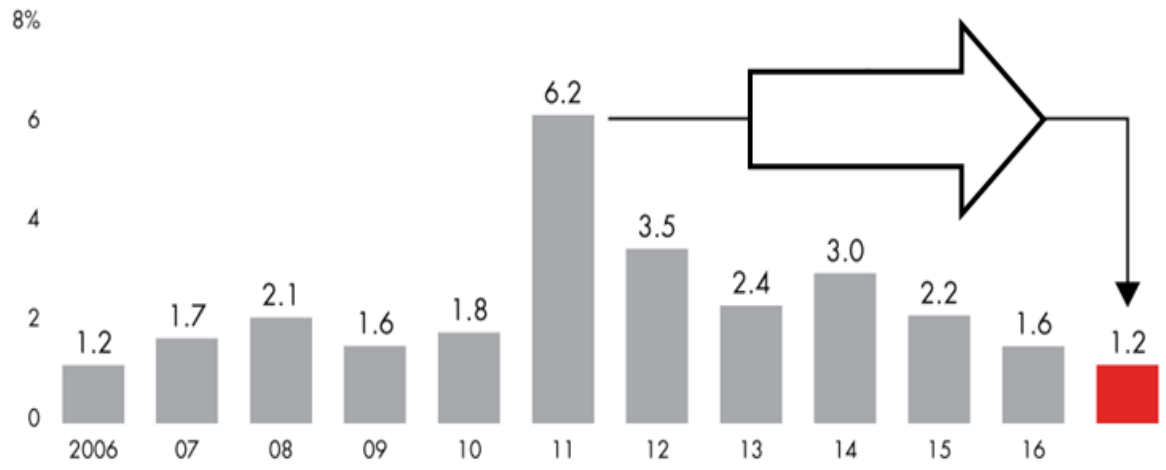
Grafikon 1. Gubici prema tipu operativnog rizika u razdoblju od 2011. do 2016. iskazani u milijardama Američkih dolara



Izvor: ORX, Bain & Company (2018)

Međutim, unatoč velikom ukupnom gubitku u navedenom razdoblju, podaci kroz godišnja razdoblja pokazuju opći pad gubitaka od operativnih rizika što je vidljivo iz grafa 2. U 2011. godini gubici od operativnog rizika zauzimali su 6.2 % ukupnog prihoda te su u 2016. godini pali na najnižu razinu od 1.2 %.

Grafikon 2. Operativni rizik prikazan u postocima ukupnog prihoda



Godišnja razdoblja 2006. – 2016.

Izvor: ORX, Bain & Company (2018)

Takav trend pokazuje da su financijske organizacije sve više usredotočene ka kreiranju djelotvornog sustava upravljanja operativnim rizikom i mjerama za sprječavanje istog.

Banke koje imaju sveobuhvatan pristup upravljanju operativnim rizicima, prilikom kreiranja odgovarajućih mjera uzimaju u obzir 4 ključna ranjiva područja u organizaciji:

- Organizacijska struktura
- Ljudski resursi
- Informacijski sustav
- Regulacijska pravila i procedure

U cilju sprječavanja grešaka, sustav upravljanja operativnim rizikom polazi od 4 načela:

1. U svim poslovnim područjima mora biti primjena aktivnosti menadžmenta upravljanja operativnim rizikom koji se integrira u ukupnu strukturu upravljanja rizicima unutar banke
2. Sve uloge menadžmenta upravljanja rizicima moraju biti jasno definirane i dodijeljene zaposlenicima sa odgovarajućim znanjima i vještinama
3. Sve povratne informacije moraju biti zaprimljene i adekvatno obrađene kako bi se osiguralo kontinuirano učenje, kako od grešaka tako i od uspjeha
4. Zadana načela i mjere moraju se redovito preispitivati i prilagođavati sukladno promjenama

Prvi korak u izgradnji djelotvornog sustava jest potpuna procjena i identifikacija postojećeg profila rizika, a zatim izgradnja baze podataka i mape svih unutarnjih i vanjskih rizičnih događaja. Tada banka razvija ključne pokazatelje rizika koji služe kao rani znak upozorenja o potencijalnim problemima. Jednom kada banka prepozna i kategorizira svaki rizik, može odlučiti o mogućnostima i mjerama ublažavanja. Ključ učinkovitosti polazi od osposobljavanja ljudskih potencijala da predvide koje greške bi se mogle pojaviti, posebno kada se uvode inovacije u poslovanje, poput novog proizvoda ili usluge. U cilju predviđanja i sprječavanja grešaka, mogu se koristiti različite metode izrade mogućih scenarija s podrškom tehnologije za naprednu analitiku pomoću koje se spremaju i obrađuju velike količine podatka za kontinuirano praćenje operacija banke.

Prema Adelsberger (2015), moguće opcije tretiranja rizika jesu sprječavanje, ublažavanje, prijenos te prihvaćanje. Sprječavanje podrazumijeva eliminaciju rizičnog procesa, odnosno resursa ukoliko je subjekt zaključio da je taj rizik neprihvatljiv. U pravilu se mjere sprječavanja obvezno primjenjuju u slučaju rizika koji se učestalo pojavljuju, a mogu uzrokovati velike gubitke. Mjere ublažavanja koriste se za rizike s visokom učestalošću pojavljivanja, ali manjom težinom gubitka za organizaciju. Prijenos podrazumijeva transfer posljedica štetnog učinka rizika na druge fizičke ili pravne osobe ukoliko su mogući potencijalno visoki gubici, dok će s druge strane, poduzeće prihvatiti sve rizike za koje smatra da bi troškovi provođenja određenih mjera bili veći od potencijalnih izgubljenih prihoda i gubitaka.

Nadalje, HANFA (2016) propisuje detaljnije smjernice za kreiranje adekvatnih mjera za upravljanje rizicima te ističe kako sprječavanje grešaka polazi od podrške uprave subjekta.

Uprava je odgovorna za organizaciju, strateško odlučivanje, dodjelu resursa i donošenje pravila i procedura u kontekstu upravljanja, što obuhvaća i procese izdvojene vanjskim pružateljima usluga. Ukoliko uprava subjekta nije na primjeren način uključena u upravljanje, subjekt se može izložiti rizicima kao što su neusklađenost strategije poslovnog razvoja i razvoja sustava upravljanja rizicima te neučinkovito trošenje sredstava za razvoj i održavanje istog.

U svrhu sprječavanja rizika, preporučljivo je da uprava subjekta primijeni minimalno sljedeće mjere i postupke:

- Uspostava primjerene organizacijske strukture potrebne za funkcionalnost i sigurnost sustava sukladno poslovnim ciljevima subjekta (Gosh, 2012)
- Osiguravanje resursa potrebnih za primjerenu funkcionalnost i sigurnost sustava, poglavito u kontekstu stručnih kadrova, hardvera, softvera i podržavajuće infrastrukture
- Imenovanje osobe odgovorne za upravljanje informacijskim procesima i operacijama
- Osiguravanje kontinuirane upoznatosti uprave s relevantnim činjenicama vezanima uz funkcioniranje i sigurnost, bilo kroz neformalnu komunikaciju s osobama odgovornima za funkcioniranje i sigurnost ili kroz formalni sustav izvješćivanja
- Usklađivanje strategije razvoja sustava i razvoja poslovne strategije subjekta (Šverko, 2007)
- Formiranje odbora za upravljanje
- Razdvajanje funkcije upravljanja sigurnošću sustava od drugih zaduženja vezanih uz sustav
- Razdvajanje međusobno nesukladnih dužnosti u procesu upravljanja informacijskom tehnologijom
- Formiranje sustava unutarnjih kontrola (Tarantino, 2008)
- Dokumentiranje i usvajanje politika, pravila, standarda, smjernica, uputa i radnih procedura

Kako bi se umanjili štetni učinci prijetnji nastalih ljudskim djelovanjem, preporučljivo je osigurati sljedeće:

- Djelatnici imaju primjerena znanja i vještine za dužnosti koje obavljaju u skladu s pozicijama na kojima se nalaze

- Djelatnici imaju primjerena znanja i vještine u vezi uporabe tehnoloških resursa koje koriste pri izvršavanju radnih zadataka
- Djelatnici imaju primjerenu razinu svijesti o sigurnosti sustava
- Uspostava procesa provjere kandidata za zapošljavanje, a taj proces može uključivati provjeru istinitosti navoda o radnom iskustvu i obrazovanju, provjeru o počinjenim kaznenim djelima čime se smanjuje mogućnost zapošljavanja osoba koje bi mogle predstavljati sigurnosni rizik
- Uspostava procesa kontinuirane edukacije djelatnika u cilju podizanja svijesti o sigurnosti, što može uključivati planiranje i provedbu edukacije te prikupljanje povratnih informacija od sudionika
- Preusmjeravanje radne snage tako da zaposlenici nisu opterećeni radnim preopterećenjem (Domingo, 2003)
- Redizajn i pojednostavljenje zadatka uklanjanjem nepotrebnih koraka u izvršavanju aktivnosti (UBM Tech, 2013)
- Redovito ažuriranje uputa za rad, definiranih na razumljivom rječniku za zaposlenike
- Kontinuirano održavanje treninga i edukacija zaposlenika sukladno promjenama u poslovanju
- Stvaranje ugodne organizacijske klime i radnog okruženja koje doprinosi povećanju učinkovitosti
- Osiguravanje pouzdano i pravilno održavanih resursa i opreme potrebnih zaposlenicima za rad
- Osiguravanje primjerenog sustava nagrađivanja zaposlenika

S ciljem ublažavanja štetnih učinaka prijetnji nastalih zbog neprimjerenog održavanja informacijskog sustava, potrebno je:

- Osigurati primjereno održavanje hardvera, softvera i potporne infrastrukture, u vidu nadogradnji i ispravljanja pogrešaka u softveru, redovnog servisiranja hardvera i povezane infrastrukture, zamjene zastarjelih i dotrajalih komponenti
- Ograničiti ovlaštenja za izmjene na hardveru, softveru i potpornoj infrastrukturi isključivo na osobe koje imaju odgovarajuća stručna znanja i vještine
- Primjereno nadzirati ključne pokazatelje funkcionalnosti, kao što su primjerice slobodni kapaciteti medija za pohranu podataka i raspoloživost sistemskih resursa poslužiteljskih računala

Kako bi se umanjili rizici nemogućnosti nastavka poslovanja uslijed djelovanja štetnih događaja te omogućilo uklanjanje grašaka, organizacije trebaju provoditi sljedeće aktivnosti:

- Identificirati ključne poslovne procese i resurse potrebne za njihovo izvršavanje, što uključuje informacijsku tehnologiju, kadrove, uredsku opremu, ugovore i licence
- Analizirati kako prekid poslovnih procesa utječe na poslovanje u cjelini s obzirom na različite dužine vremena u kojima su procesi u prekidu te na taj način odrediti najveće prihvatljive dužine vremena prekinutosti procesa
- Usvojiti i dokumentirati planove nastavka poslovanja u slučaju prekida poslovnih procesa
- Uspostava pričuvnog računalnog centra na udaljenoj lokaciji koji svojim kapacitetima može osigurati nastavak poslovanja u slučaju nedostupnosti primarnog
- Uspostava alternativne lokacije za oporavak poslovnih procesa u slučaju neupotrebljivosti primarne poslovne lokacije
- Osigurati pričuvne baze podataka i informacija za raspolaganje u slučaju nedostupnosti primarnih baza
- Definirati sustav i procese upravljanja odnosima s potrošačima s ciljem ispravljanja i uklanjanja negativnih posljedica i reputacija
- Organizirati adekvatno osoblje za upravljanje odnosima s potrošačima i javnosti koje će pravovremeno pružiti sve potrebne informacije
- Osigurati prijenos rizika na druge osobe

Odluka o načinu postupanja s rizicima u pravilu ovisi o samim rizicima te vrijednostima izloženih procesa i resursa. Mnogim financijskim institucijama, jedan od najvećih izazova postaje upravo stvaranje organizacijske i upravljačke strukture koja može uspješno kontrolirati operativne rizike te međusobno povezane čimbenike koji doprinose operativnom riziku, uključujući ljudsko ponašanje, organizacijske procese i informacijske sustave. Banke koje formuliraju pobjednički pristup stvaraju kulturu rizika utemeljenu na formalnim pravilima o upravljanju i kapitalnim zahtjevima, kao i nematerijalnim elementima kao što su obuka i vođenje primjerom. Banke koje su integrirane i pro aktivne u načinu upravljanja organizacijskim rizikom mogu ostvariti stvarne financijske koristi i što je još važnije, spriječiti gubitke koji mogu imati višegodišnje posljedice na poslovanje.

4. Studija slučaja pogrešaka u uslužnom sektoru na primjeru banke

U sklopu empirijskog istraživanja pogrešaka u operativnom poslovanju, razmotriti će se primjer poslovne banke s fokusom na operativne rizike koji se javljaju u poslovanju. Ključni operativni rizici sagledat će se s aspekta grešaka vezanih uz sustav, te grešaka vezanih uz osoblje.

Empirijsko istraživanje provedeno je metodom intervjua. Intervju je proveden sa tri predstavnika banke, na tri razine menadžmenta: top menadžment, srednji menadžment te operativni menadžment. Intervju se sastoji od 10 pitanja, koja su postavljena svim ispitanicima. Prvih pet pitanja su usmjerena na razumijevanje sustavnih grešaka, dok je preostalih pet pitanja usmjereno na razumijevanje grešaka osoblja. Odgovori ispitanika izdvojeno su prezentirani, te je na svaki odgovor pružen kratki osvrt autora.

Svrha provedbe empirijskog istraživanja je stjecanje uvida u ključne aspekte operativnih rizika, najznačajnije greške te razumijevanje mjera za uklanjanje grešaka u svakodnevnom poslovanja banaka.

4.1. Analiza grešaka sustava na primjeru banke

Greške vezane uz sustav predstavljaju jednu od osnovnih kategorija operativnih rizika u bankarskom poslovanju. S obzirom da se suvremene banke u značajnoj mjeri oslanjaju na potporu informacijskih sustava koji obrađuju veliki broj podataka i informacija, svaka pogreška, propust i nedostatak sustava može rezultirati velikim financijskim štetama za banku. U nastavku se nalaze rezultati intervjua, u sklopu kojeg je postavljeno pet pitanja vezanih uz greške poslovnog sustava u banci.

1. Možete li identificirati najznačajnije kategorije operativnih rizika s aspekta grešaka vezanih uz poslovni sustav banke?

"Operativni rizik je u principu svaki rizik koji se javlja zbog potencijalne pogreške u poslovanju. Veoma je teško definirati specifične kategorije rizika vezanih za poslovni, lakše bi bilo identificirati odjele u kojima se greške češće javljaju. To su odjeli koji se u velikoj

mjeri oslanjaju na sistemsku podršku, te čije je poslovanje u velikoj mjeri automatizirano. Na primjer odjel kreditnih analiza te odjel ocjene kreditnog rizika."

"Poslovni sustavi su sve kompleksniji u bankama. Upravo zato banke kontinuirano ulažu u razvoj informacijskih sustava te u trening eksperata za razvoj i održavanje sistema. Ključno područje koje se izdvaja s aspekta rizika vezanih uz poslovni sustav banke je zasigurno aplikativna podrška. Većina poslovnih banaka nema unificirani razvoj aplikacija (dio se razvija interno, dio razvijaju specijalizirana informacijsko tehnološka poduzeća), pa je teško uskladiti inicijalno nepovezane aplikacije. To zahtjeva veliki angažman informacijskih resursa, te se čak i mala neslaganja između aplikacija koje bi trebale biti povezane mogu očitovati kroz značajne probleme, primarno s aspekta nezadovoljstva korisnika."

"Ovisno o tome kako definirate operativni rizik. Postoje greške koje se događaju često, no nemaju veliki rizik u smislu utjecaja na financijski rezultat banke. S druge strane, dovoljno je da se dogodi samo jedna greška kod odobravanja velikog kredita, zbog koje banka može snositi veliku financijsku štetu. Kada bi sistemske rizike razmotrili sa stajališta štete koja može nastati, rekao bih da je neznačajniji rizik loša informacijsko tehnološka infrastruktura, ne nužno u našoj banci, već generalno gledajući. Banke barataju velikim količinama podataka, ujedno na sintetičkoj i analitičkoj bazi, te drže i pohranjuju podatke u velika virtualna skladišta podataka. Ukoliko se informacijsko tehnološka infrastruktura ne održava redovito i kvalitetno, javlja se rizik da nastanu greške pri obradi tih podataka. Ukoliko pritom uzmete u obzir da je skladište podataka povezano s brojnim aplikacijama, možete razumjeti koliki problem nastaje ako sustav nije kvalitetno postavljen.

Razmatranjem dobivenih odgovora na postavljeno pitanje, moguće je zaključiti kako su stajališta o ključnim kategorijama sistemskih rizika u bankama različita. Također, definiranje sistemskih rizika ovisi o razumijevanju i tumačenju ovog pojma od strane ispitanika. No vidljivo je kako zajednički nazivnik sistemskih rizika predstavlja povezanost, odnosno nepovezanost komponenata poslovnog sustava, poput povezanosti korisničkih i poslovnih aplikacija koje nisu razvijene na istoj podlozi, te povezanosti skladišta podataka s poslovnim aplikacijama. Ispitanici smatraju kako se sistemski rizici povećavaju ako informacijski sustav nije adekvatno postavljen i ažuriran, te se slažu kako banke moraju ulagati značajne resurse kako bi sistemska podrška u poslovanju skladno funkcionirala.

2. Kako sistemski rizici mogu naštetiti poslovanju banke?

„Sistemski rizici mogu veoma značajno utjecati na poslovanje banke, s aspekata financijskog rezultata i zadovoljstva korisnika. Svaki problem vezan uz poslovni informacijski sustav može uzrokovati velike gubitke za banku.“

„Poslovanje banaka zasniva se na povjerenju korisnika, koje je uvelike vezano za pouzdanost našeg poslovnog sustava. Kada bi se dogodio značajniji sigurnosni propust, riskirali bismo gubitak značajnog broja klijenata. Propusti se događaju u svakoj organizaciji i to na dnevnoj bazi, no važno je da se ti propusti ne manifestiraju kao ugrožavanje sigurnosti ili financijske imovine klijenata.“

„Sigurnosni propusti sa sistemskog aspekta manifestiraju se kao gubitak i krađa informacija, što u krajnjoj mjeri može rezultirati napuštanjem od strane klijenata. Pritom morate uzeti u obzir činjenicu da je klijentima relativno lako promijeniti banku, te je zato potrebno imati stabilan poslovni sustav i redovito ga ažurirati i održavati. Naposljetku je moguće zaključiti kako sistemski rizici mogu imati veoma značajan negativni utjecaj na poslovanje banke.“

Razmatranjem prikupljenih odgovora vidljivo je kako rizici vezani uz poslovne sustave mogu u značajnoj mjeri utjecati na poslovni rezultat banaka. Sistemski rizici očituju se kroz sigurnosne propuste, koji mogu uzrokovati financijske i podatkovne probleme za klijente, što u konačnici rezultira smanjenjem prihoda ili povećanjem troškova, odnosno lošijim sveobuhvatnim poslovni rezultatom. Prema tome, može se zaključiti kako banke u svakom slučaju moraju poduzimati mjere za identifikaciju, sprječavanje i ublažavanje sistemskih rizika.

3. Koje su mjere za sprječavanje i ublažavanje sistemskih rizika u bankama?

„Uvijek je bolje spriječiti štetu prije nego što nastane, nego minimizirati štetu koja je već nastala. Zato se menadžment banke primarno usmjerava na poduzimanje mjera za sprječavanje rizika. Najčešće metode za sprječavanje rizika podrazumijevaju temeljito planiranje sustavne podrške u poslovanju. To konkretno znači da je potrebno planirati razvoj i održavanje sistemskih i korisničkih aplikacija, te kako te aplikacije povezati da međusobno rade bez zastoja i pogrešaka. Uz to, sprječavanje sistemskih rizika provodi se kroz redovite

kontrole sustava i „stres testove“, kojima je cilj simulirati rizično okruženje te vidjeti kako će se poslovni sustav ponašati. Implementacijom planiranja i kontrole poslovnog sustava menadžment u većini slučajeva može detektirati rizična područja i spriječiti štetu prije nego što nastane.“

„Problem sa sistemskim rizicima je što ih je mnogo teže identificirati nego ljudske pogreške, te ih se često uopće ne primjećuje, sve dok ne nastane značajni problem. Zato se kao primarna mjera prevencije takvih rizika mora oformiti i osposobiti tehnički tim inženjera i analitičara, koji na redovnoj bazi kontroliraju funkcionalnost sustava i nalaze potencijalne probleme. Banke su ovdje posebice osjetljive jer upravljaju velikim novčanim iznosima, kao i osjetljivim korisničkim podacima i zato je veoma važno spriječiti probleme sa sustavom. Ovdje je važno istaknuti i sigurnost od proboja sustava, što se također može prevenirati adekvatnim održavanjem i ažuriranjem sigurnosnih aplikacija.“

„Prevencija i ublažavanje rizika je uvijek izazov za menadžment, jer su rizici brojni i često ih nije moguće uočiti sve do trenutka kad situacija eskalira. Ublažavanje sistemskih rizika je praktički nemoguće, pa su stoga svi napori usmjereni na potpunu prevenciju tih rizika, što se uz implementaciju kvalitetnog sustava planiranja i nadzora svakako može postići. Važno je da se pri prevenciji rizika svo osoblje banke aktivno uključi, s obzirom da odgovornim ponašanjem značajno smanjujemo propuste sustava.“

Razmatranjem prikupljenih odgovora vidljivo je kako su svi ispitanici primarno usmjereni na prevenciju, a ne ublažavanje sistemskih rizika. Menadžment banke smatra kako su sistemski rizici veoma značajni za poslovanje banaka te kako je potrebno postaviti odgovarajuće sigurnosne mjere, kako bi se rizici predvidjeli i na vrijeme spriječili. Kao temeljne mjere za sprječavanje rizika navode se uspostava ažurnost sustava planiranja i kontrole, formiranje ekspertnih timova za nadzor poslovnih sustava i identifikaciju rizika te ažuriranje sigurnosnih aplikacija. Također, ističe se kako su sistemski rizici često nezamijećeni sve do trenutka kada se dogodi šteta, te je stoga važno redovito provoditi kontrole sustava i ukloniti potencijalne greške i propuste u što je moguće kraćem vremenskom roku.

4. Koja je uloga menadžmenta banke u upravljanju sistemskim rizicima?

„Menadžment ima veoma značajnu ulogu u upravljaju svim rizicima, pa tako i sistemskim rizicima. Jedna od naših zadaća je postaviti sustav u kojem se kontrole i održavanja odvijaju na redovnoj bazi te da u organizaciji postoje educirani stručnjaci za nadzor takvih rizika, kao i za njihovo otklanjanje.“

„Iako u bankama postoji izdvojeni odjel čija je zadaća upravljanje rizicima, cjelokupni menadžment banke mora biti usmjeren na prevenciju rizika. Ne smije se zaboraviti da su menadžeri promicatelji korporativne kulture, što podrazumijeva uključivanje svih zaposlenika u prevenciju rizika. To je možda malo manje izraženo kod sistemskih rizika jer ne ovise toliko o ljudskoj pogreški kao što ovise o greškama u sustavu, no ovdje je važno naglasiti kako bi svi zaposlenici pravovremeno morali prijaviti rizik ili problem s kojim su se suočili u svakodnevnom poslovanju. To omogućava stručnom osoblju da otkloni sistemski rizik prije nego što uzrokuje financijsku štetu za banku.“

„Menadžeri moraju biti aktivno angažirani u praćenje svih poslovnih procesa u banci, kako bi na vrijeme uočili sve rizike. To je osobito važno jer sistemski rizici mogu uzrokovati velike probleme, kako za korisnike, tako i za osoblje banke. Menadžeri moraju poticati komunikaciju u banci, kako bi osoblje koje radi u segmentima koji su u većoj mjeri izloženi sistemskim rizicima na vrijeme upozorilo o potencijalnim rizicima.“

Razmatranjem prikupljenih odgovora vidljivo je kako menadžment banke aktivnosti upravljanja sistemskim rizicima smatra veoma važnim dijelom menadžerskog posla, primarno zbog potencijalnog negativnog učinka na poslovanje banke. Prema tome, menadžment mora imati veoma značajnu ulogu pri upravljanju sistemskim rizicima, te poticati zaposlenike koji su uključeni u procese izloženije sistemskim rizicima da samostalno identificiraju te prijavljuju rizike, kako bi se provelo uspješno uklanjane nastanka štete. Nadalje, menadžment banke mora aktivno biti uključen u aktivnosti planiranja poslovnih sustava i uzeti u obzir da se sustav mora redovno održavati, što je veoma važna komponenta pri upravljanju sistemskim rizicima.

5. Možete li navesti primjer greške koja je nastala zbog propusta informacijskog sustava te mjere za sprečavanje, ublažavanje ili otklanjanje štete nastale tom greškom?

„Obzirom na veliki broj podataka, te isto tako veliki broj korisnika tih podataka, značajne greške koje nam se javljaju u okviru informacijskog sustava vezane su uz dopremanje tih podataka na zajedničko virtualno mjesto koje se naziva skladište podatka. Skladište podataka koristimo kako bi sintetizirali podatke iz različitih izvora te kako bi svi podaci bili dostupni zaposlenicima s jednog centralnog mjesta. No povremeno se događa da zbog pada informacijskog sustava dostava podataka u skladište ne bude pravovremena, odnosno da podaci kasne. Iako se ovdje ne radi o značajnom kašnjenju (u pravilu 1-2 radna dana), takva kašnjenja nam uzrokuju poteškoće za uspješno obavljanje zadanih aktivnosti, osobito ako se radi o podacima koji su zaposlenicima potrebni na dnevnoj bazi (npr. podaci za regulatorno izvještavanje ili podaci o sumnjivim transakcijama). Takva greška dogodila nam se kao posljedica vanjskih faktora. Došlo je do prekida napajanja našeg sustava od strane vanjskog poslužitelja koji nas opskrbljava elektronskom telekomunikacijskom i internetskom mrežom što je uzrokovalo zaposlenicima nemogućnost pristupa informacijama potrebnim za obavljanje njihovih zadataka. Odmah nakon uočavanja nastale greške, osoblje je obaviješteno i upućeno u nastalu poteškoću. U otklanjanje nastale greške bio je uključen odgovorni tehnički tim u koordinaciji s vanjskim poslužiteljem. U periodu nastanka greške, tehničari su u kratkom roku omogućili da se informacije zaposlenicima osiguraju iz pomoćnih skladišta podataka, kojima se serveri nalaze na dislociranim mjestima. Osoblje je zatim također informirano o poduzetim mjerama i postupcima kojih su se pridržavali pri preuzimanju podataka iz pomoćnih baza. Na taj način privremeno smo otklonili pogrešku pomoćnim bazama, dok vanjski poslužitelj nije u potpunosti uklonio svoju poteškoću nakon čega je uspostavljeno ponovno redovno poslovanje. “

„Najznačajnije greške koje su nam se javljale u informacijskim sustavima su dvostruke provedbe transakcija, što znači da se uplatitelju dva puta skida novac s računa pri obavljenoj transakciji. Takve greške nam predstavljaju veliki problem, s obzirom da uzrokuju vrlo visoku razinu nezadovoljstva korisnika, pa čak i potencijalni gubitak klijenata. Greške u obradi platnih transakcija događaju se zbog prekida u platnoj mreži (SWIFT). Ukoliko se transakcija dogodi u trenutku prekida u mreži koja omogućava platni promet, mreža će klasificirati transakciju kao nastalu neposredno prije prekida, te je istovremeno provesti neposredno nakon prekida. Ovakva se odstupanja ne javljaju često zbog stabilnosti mreže platnog prometa te činjenice da prekid traje maksimalno nekoliko sekundi, ali i činjenice da se prekid mreže mora dogoditi u sekundi prije izvršenja transakcije. Unatoč rijetkom pojavljivanju, ipak imamo zabilježene takve slučajeve i značajne prigovore naših korisnika, budući da su svi

klijenti najviše osjetljivi na povredu vlastitih sredstava. Slučaj ovakve greške otklanjamo uspostavom kvalitetne korisničke podrške, kojoj se klijenti mogu obratiti čim primijete da su im sredstva dva puta skinuta s računa, te će im se novac vrati u roku od 24 sata od prijave greške. S obzirom da je banci vidljivo u kojem se trenutku dogodio prekid mreže, eliminira se mogućnost za pokušajem prevare (namjerno provođenje dvije iste transakcije, te traženje povrata novca za jednu). Odjel zadužen za rješavanje prigovora korisnika, otklanja posljedice negativne reputacije kod klijenta radi nastale greške na način da se korisnik pravovremeno obavijesti o rješavanju problema, primjerice, odmah nakon primitka prigovora klijentu se šalje odgovor da je prigovor zaprimljen zajedno s odgovarajućim objašnjenjem da će biti riješen u najkraćem roku, a odgovor će klijent zaprimiti najkasnije unutar 3 radna dana. Takav pristup ulijeva povjerenje klijentu da je njegov slučaj preuzet te da će biti pravovremeno i riješen što umanjuje klijentov negativan dojam zbog nastale greške. U konačnici je pogreška otklonjena tako da su sredstva vraćena na klijentov račun o čemu je korisnik bio informiran s odgovarajućim objašnjenjem i isprikom radi nastalih poteškoća .“

„Greške vezane uz informacijske sustave često su vezane uz probleme s radom aplikacija za pozadinsku obradu podataka. Dok zaposlenici u redovnom poslovanju rade s korisničkim aplikacijama, aplikacije za pozadinsku obradu podataka rade kalkulacije i strukturiraju podatke koji se zaposlenicima prikazuju putem korisničkih aplikacija. Kao primjer može se navesti aplikacija za izračun kreditnih rejtinga. Dok se zaposlenici u odjelu rizika bave unosom parametara za definiranje rizika, u pozadini postoji druga aplikacija koja koristi unesene podatke za automatski izračun ukupnog rizika, te po završetku kalkulacije vraća korisnicima rezultate kroz korisničku aplikaciju. Primjer takve greške očitovao nam se u usporenom radu korisničke aplikacije te kratkom periodu nemogućnosti korištenja iste. Uzrok je bio preveliki trenutni broj korisnika koji je unosio veliki broj podataka u aplikaciju te je došlo do greške preopterećenosti sustava. Tehnička podrška otklonila je problem oporavkom aplikacije te su poduzete mjere sprječavanja da se ista greška ponovi u budućnosti, i to na način da se sada za svakog novog zaposlenika mora raspisati i odobriti zahtjev od tehničke podrške. Razlog tome je mogućnost preinaka na aplikaciji od strane informatičkog odjela, ukoliko se procjeni da je broj korisnika prevelik za normalno funkcioniranje postojeće pozadinske aplikacije. U tom slučaju vrši se nadogradnja ili razvoj nove i brže aplikacije. Iako se ovakve greške ne događaju osobito često, predstavljaju veliku prijetnju poslovanju banke, s obzirom da su u slučaju pada aplikacije sve aktivnosti zaposlenika koji rade u toj aplikaciji onemogućene, čime se gubi značajna količina vremena i novca.“

Primjeri sistemskih grešaka koje su naveli ispitanici zajedno s mjerama uklanjanja koje su koristili, prikazani su u tablici 10.

Tablica 10. Primjeri sistemskih grešaka s mjerama uklanjanja

SISTEMSKI RIZIK:	MJERE UKLANJANJA:
Neraspoloživost usluge vanjskog poslužitelja	• komunikacija s vanjskim poslužiteljem • interna komunikacija sa zaposlenicima • podrška tehničkog tima • omogućavanje pristupa pomoćnim bazama
Prekid internog informatičkog sustava platne mreže	• tehnička podrška sustavu • ispravak pogrešnih transakcija • obrada korisničkih prigovora • ispravljanje negativnog dojma kod korisnika
Nedostupnost korisničke aplikacije	• tehnička podrška • interna komunikacija sa zaposlenicima • prilagođavanje procedura i procesa • nadogradnja i razvoj brže aplikacije

Izvor: Izrada prema odgovorima iz intervjua provedenog s predstavnicima menadžmenta jedne banke

4.2. Analiza grešaka osoblja na primjeru banke

6. Možete li identificirati najznačajnije kategorije operativnih rizika za banku s aspekta grešaka osoblja?

„S obzirom da se dobar dio posla u bankama još uvijek obavlja manualno, operativni rizik u smislu grešaka osoblja može se javiti u bilo kojem odjelu, ili bilo kojem procesu, gdje je potreban intenzivniji ljudski angažman. Takvi se slučajevi najčešće javljaju u odjelima procjene kreditnog rizika ili verifikacije kolaterala. U spomenutim se odjelima osoblje često susreće sa specifičnim kreditnim zahtjevima, što povećava mogućnost pogreške. Nepostojanje standardnih procedura i adekvatnih treninga i edukacija također je izvor operativnih rizika. Ukoliko osoblje nije adekvatno osposobljeno za provedbu određenog procesa, naravno da je veća vjerojatnost da će se dogoditi greška.“

„Smatram da su najveće kategorije operativnih rizika poslovanje s klijentima i procjena kreditne sposobnosti klijenta. Kod poslovanja s klijetima, konzultanti u našim poslovnicama

svaki dan obrađuju mnogo korisničkih zahtjeva, te je za realizaciju svake usluge potrebno ručno upisati podatke klijenata. Svako ručno upisivanje podataka smatra se operativnim rizikom, no takvi rizici u pravilu nisu veoma opasni za banku. Druga značajna kategorija rizika je svakako procjena kreditne sposobnosti klijenta. Iako postoji jasan set kriterija za utvrđivanje kreditne sposobnosti, djelatnici u specifičnim slučajevima moraju temeljem vlastite procjene finalizirati ocjenu kreditne sposobnosti. Ukoliko se ocjena pokaže pogrešnom, plasman se može odobriti potencijalno nelikvidnim ili insolventnim klijentima. Ovaj je rizik veoma opasan za poslovanje banke, jer se izloženosti prema problematičnim klijentima moraju rezervirati, što predstavlja financijski gubitak za poslovanje banke. Važno je naglasiti i da se greške osoblja često pogrešno identificiraju kao sistemski rizici. Ukoliko djelatnik pogrešno upiše podatke ili provede pogrešnu operaciju, iako će se greška vidjeti u sustavu, to neće biti sistemska greška jer sustav samo zaprima inpute od strane djelatnika."

„Greške osoblja u banci se događaju mnogo češće nego sistemske greške, s obzirom da su programi standardizirani i namijenjeni izvršavanju identičnih operacija. Upravo je i varijabilnost procesa glavni izvor grešaka osoblja. Ukoliko svaki zaposlenik koji radi na određenom procesu napravi neki od koraka na svoj način, povećava se vjerojatnost da će se negdje u procesu javiti problem. No važno je napomenuti kako se greške vezane uz osoblje u pravilu lakše identificiraju te nisu toliko opasne kao problemi sa sustavom, gdje je mnogo teže identificirati problem, te je u pravilu potrebno mnogo više vremena da se problem otkloni, što može rezultirati značajnim financijskim gubicima ili ugrožavanjem osobnih podataka naših klijenata."

Rizici vezani uz greške osoblja također se smatraju značajnom kategorijom rizika u poslovanju banaka, no menadžment ističe kako su u takvi rizici obično manje opasni s aspekta financijskih gubitaka u odnosu na sistemske rizike, s obzirom na činjenicu da je sistemske rizike teže identificirati i otkloniti štetu ukoliko se rizik realizira. Kao najznačajnija područja nastanka grešaka osoblja navode se odjeli i procesi s visokim volumenom aktivnosti, poput poslovne mreže gdje se na dnevnoj bazi obavlja veliki broj usluga i transakcija, te odjeli u kojima se provode složenije analize, poput ocjene kreditne sposobnosti klijenta. Nadalje, menadžment banke smatra kako su greške osoblja češće od sistemskih grešaka, no s obzirom da u pravilu nisu kritične za poslovanje banke, ne promatra ih se kao kritični rizik za cjelokupno poslovanje.

7. Kako rizici vezani uz greške osoblja mogu naštetiti poslovanju banke?

„Šteta koja se događa realizacijom operativnih rizika očituje se na isti način, bilo da se radi o sistemskim rizicima ili greškama osoblja. Realizacija rizika u svakom slučaju ugrožava poslovanje banke s aspekta smanjenja prihoda ili povećanja troškova. Ukoliko se radi o rizicima u poslovanju s klijetima, šteta se očituje kroz potencijalni gubitak klijenata, što znači manje prihode. Ukoliko se radi o rizicima u odjelima ili procesima podrške, uklanjanje štete uzrokuje povećanje troškova za banku. Potrebno je napomenuti kako menadžment mora planirati nastanak određenog broja rizika te u budžet uključiti dodatne troškove za uklanjanje štete.“

„Ukoliko se više puta dogodi greška u smislu odobravanja prevelikog iznosa kredita, banka se izlaže narušavanju rezervi likvidnosti, što može rezultirati neusklađenosti sa regulatornim standardima, a time i plaćanjem kazne. No takvi su slučajevi veoma rijetki: da bi se dogodila takva situacija, potrebno je više puta za redom napraviti istu grešku. Naravno, trening i edukacija osoblja važan su faktor izbjegavanja ovog rizika, što je puno transparentnije nego kod sistemskih rizika, koji su uglavnom skriveni sve dok se ne dogodi problem i nastane šteta.“

„Greške osoblja izravno utječu na zadovoljstvo, odnosno na nezadovoljstvo klijenta. Kao primjer može se navesti krivo upisivanje podataka, zbog čega je potrebno naknadno kontaktirati klijenta. To se može percipirati kao nekompetentnost osoblja, te se zbog toga može izgubiti dio klijenata, što nam nikako nije u interesu.“

Razmatranjem prikupljenih odgovora moguće je zaključiti kako greške osoblja mogu naštetiti poslovanju banke s aspekata gubitaka korisnika i problema s regulatornim tijelima. Gubici korisnika, koji mogu biti potaknuti greškama osoblja izravno utječu na smanjenje prihoda banke, dok problemi s regulatornim tijelima mogu značajno povećati rashode banke, bilo da se radi o zahtjevima za usklađivanjem ili o kaznama. Nadalje, rizici u izravnom poslovanju s klijentima mogu naštetiti poslovanju s aspekta smanjenja poslovnih prihoda, dok rizici u poslovnima podrške mogu povećati poslovne rashode banke.

8. Koje su mjere za sprječavanje i ublažavanje rizika vezanih uz greške osoblja u bankama?

„Prva ključna mjera koju bih istaknuo je svakako adekvatna edukacija osoblja o najčešćim greškama i propustima koji se javljanju pri svakodnevnim aktivnostima. Osoblje banke, pogotovo djelatnici u poslovnicama imaju veliki obujam posla na dnevnoj bazi, te ukoliko nisu dobro upućeni u potencijalne propuste, povećava se mogućnost za javljanjem pogrešaka. Uz to, edukacija mora biti kontinuirana i pravovremena: nužno je upoznati djelatnike čim nove aktivnosti i procedure stupe na snagu. Kao drugu ključnu mjeru istaknuo bih standardizaciju poslovnih procesa. Ukoliko postoji velika varijabilnost, te svaki zaposlenik provodi proces na svoj način, može se očekivati znatno veći broj propusta i pogrešaka. Standardizacija poslovnih procesa podrazumijeva postojanje jasnog hodograma aktivnosti koji svaki zaposlenik koji radi na određenom procesu mora provesti. To ne znači da zaposlenici moraju biti roboti, već da se određena pravila i procedure moraju poštivati. U standardizaciju poslovnih procesa moraju biti uključeni i zaposlenici i menadžeri, kako bi se našlo optimalno rješenje, koje rezultira učinkovitim i lako razumljivim i izvodljivim poslovnim procesom.“

„S obzirom da se greške često ne prijavljuju zbog straha od penalizacije, jedna od najvažnijih mjera sprječavanja i ublažavanja operativnih rizika je zasigurno uspostava jasnog lanca odgovornosti i komunikacije prema nadređenima. Nadalje, zaposlenicima je potrebno jasno komunicirati da se povremene greške neće penalizirati, jer nitko ne može očekivati savršene performanse od svojih zaposlenika. Također je potrebno komunicirati da je glavni benefit komunikacije pravovremeno reagiranje i otklanjanje problema. Kao primjer mogu se navesti pritužbe klijenata na pogrešno ili presporo odrađene zahtjeve. Ukoliko zaposlenik ne komunicira ovakvu situaciju svojim nadređenima, javlja se rizik od gubitka klijenta. Ukoliko pak se greška komunicira na vrijeme, voditelj poslovnice može kontaktirati nezadovoljnog klijenta te ponuditi ispriku uz određenu beneficiju, što uz zadržavanje klijenta može rezultirati i povećanjem povjerenja. Kao komplementarna mjera sprječavanje grešaka osoblja može se implementirati adekvatni sustav nagrađivanja zaposlenika koji na mjesečnoj ili godišnjoj razini počine najmanje operativnih grešaka. Smatram kako je nagrađivanje uvijek bolje od kažnjavanja, stoga nastojimo poticati izvrsnost osoblja kroz razne financijske i nefinancijske kompenzacije.“

„Istraživanja pokazuju kako su greške osoblja mnogo češće kod manje iskusnih zaposlenika, s obzirom na činjenicu da nisu adekvatno upoznati s poslovnim procedurama, te im je potrebno više vremena da bi izvršili korisnički zahtjev. Mentorstvo se pokazalo jednom od najboljih

metoda za prevenciju grešaka. Iskusno osoblje koje dobro razumije poslovne procese i aktivnosti koje su u najvećoj mjeri izložene operativnim greškama kroz program mentorstva može novim zaposlenicima kroz praksu ukazati na greške, te kako iz izbjeći. Program edukacije zaposlenika kroz mentorstvo mnogo je bolje rješenje od teoretskih edukacija, jer se kroz praksu najbolje uči, te se ne iziskuje dodatno vrijeme za provedbu edukacije, s obzirom da se nove zaposlenike mentorira kroz rješavanje stvarnih korisničkih zahtjeva na dnevnoj bazi.“

Razmatranjem prikupljenih odgovora moguće je zaključiti kako postoje brojne mjere za sprječavanje i ublažavanje rizika vezanih uz greške osoblja u bankama. Kao temeljna mjera prevencija navodi se adekvatna edukacija osoblja te implementacija programa mentorstva, čime se manje iskusnim zaposlenicima ukazuje na najčešće propuste, te im iskusniji zaposlenici kroz praksu pokazuju kako izbjeći pogreške. Nadalje, standardizacija poslovnih procesa navedena je kao važna mjera prevencije i ublažavanja operativnih rizika. Cilj standardizacije je smanjenje varijabilnosti, odnosno osiguranje da svaki zaposlenik koji provodi proces ponovi unaprijed definirani set koraka. Time se smanjuje mogućnost da će se zbog odstupanja od standardiziranih aktivnosti pri provedbi procesa dogoditi greška. Naposljetku, uspostava jasnog lanca odgovornosti i komunikacije navedena je kao jedna od ključnih mjera sprječavanja i ublažavanja operativnih rizika. Zaposlenike se mora poticati da pravovremeno komuniciraju potencijalne probleme i propuste, kako bi nadređeni mogli reagirati te ih spriječiti ili otkloniti prije nego što se dogodi veća šteta za poslovanje banke.

9. Koja je uloga menadžmenta banke u upravljanju rizicima vezanim uz greške osoblja?

„Temeljna uloga menadžmenta banke je osiguranje edukacija i treninga za osoblje koje sudjeluje u potencijalno rizičnim procesima. Menadžment se mora brinuti o tome da su zaposlenici osposobljeni za provedbu svih aktivnosti u procesu te da se pri svakoj većoj promjeni procesa ili procedura zaposlenicima razloži kako moraju postupati. Kao primjer se može navesti uvođenje nove aplikacije za obradu korisničkih podataka. Nova aplikacija zahtjeva i novi set koraka koje zaposlenici moraju napraviti. Ukoliko menadžment ne osigura edukaciju o novoj aplikaciji i trening zaposlenika usmjeren na korištenje nove aplikacija, može se očekivati da će greške biti češće. Uz to, menadžment mora identificirati poslovne proces i organizacijske jedinice koje su u najvećoj mjeri izložene operativnim rizicima. Tu se najčešće radi o procesnim jedinicama s velikim opsegom posla. Uloga menadžmenta u ovom

aspektu je da se zaposlenicima u segmentima banke koji su izloženiji riziku osiguraju češće edukacije i treninzi.“

„Prva zadaća menadžmenta pri upravljanju operativnim rizicima je razumjeti prirodu grešaka. Dobar dio propusta događa se zbog kompleksnih i neučinkovitih poslovnih procedura, no dio grešaka događa se i zbog nepažnje i brzopletosti zaposlenika. Uloga menadžmenta je prepoznati uzrok nastanka pojedine greške. Potom, ukoliko se radi o propustu zaposlenika, ukazati na rizik i potaknuti zaposlenike na dogovorniji i temeljitiji pristup. Ukoliko se radi o problematičnim poslovnim procesima, potrebno je provesti mjere za optimizaciju procesa, kako bi zaposlenici lakše mogli razumjeti i provoditi korake. Također, moramo pratiti zadovoljstvo klijenata, jer pad zadovoljstva i pritužbe često su izravno povezani s operativnim greškama. To je zahtjevna aktivnost i iziskuje mnogo napora, ali klijenti su uvijek na prvom mjestu, i potrebno se pobrinuti da ih ne gubimo zbog operativnih propusta. Zato moramo pravovremeno reagirati ako se uoči da se zadovoljstvo smanjuje, te da klijenti imaju tendenciju napuštanja banke.“

„Smatram da je edukacija osoblja o poslovnim procesima temelj prevencije operativnih rizika, i menadžment banke mora kontinuirano raditi na tome. Osobito za nove zaposlenike i za zaposlenike koji rade na kompleksnim procesima, te su automatski izloženiji operativnim rizicima. Uz to, mislim da je jedna od uloga menadžmenta osigurati da se u budžetu nađe prostora za dodatne troškove pokrivanja šteta od operativnih rizika. Nemoguće je očekivati da će se rizici potpuno otkloniti, u ljudskoj je prirodi da se greške povremeno događaju, no zato menadžment mora biti spreman.“

10. Možete li navesti primjer greške koja je nastala zbog propusta zaposlenika te mjere za sprečavanje, ublažavanje ili otklanjanje štete nastale tom greškom?

„Greška koja ima značajan utjecaj na poslovanje banke često se javlja pri procesu obrade kredita za stanovništvo. Prilikom izrade kreditnog zahtjeva zaposlenicima se događaju propusti u smislu krivog unosa rizičnih parametara poput klijentove platežne sposobnosti. Ukoliko se navede previsoka platežna sposobnost, klijentu se može odobriti značajno veći iznos kredita u odnosu na iznos koji bi klijent prema procjenama banke mogao adekvatno otplatiti. Kada se ovakva greška ne bi otklonila prije odobravanja kredita, banka bi mogla odobriti plasman koji predstavlja neprihvatljivo visok rizik za banku, jer ima neadekvatan

omjer iznosa kredita i platežne sposobnosti komitenta. Ovakve se greške češće događaju pri poslovanju sa stanovništvom, s obzirom da se u pravilu odobrava znatno veći broj kredita fizičkim nego pravnim osobama, te je sam proces odobravanja kredita stanovništvu manje kompliciran i restriktivan, slijedom čega zaposlenici u manjoj mjeri obraćaju pozornost na ispravnost unesenih podataka pri popunjavanju kreditnog zahtjeva. Kao mjera otklanjanja ove greške provodi se dvostruka verifikacija kreditnog zahtjeva, što znači da drugi zaposlenik i voditelj poslovnice u kojoj se kredit odobrava moraju pregledati kreditni zahtjev te provjeriti glavne rizične parametre. Upravo se pri drugoj razini pregleda kreditnog zahtjeva utvrđuju propusti te se tako banku štiti od potencijalnih gubitaka uzrokovanih odobravanjem kredita čiji je rizik previsok, odnosno za koje je platežna sposobnost klijenata preniska.“

„Značajne operativne greške u svakodnevnim bankovnim operacijama mogu se istaknuti u trgovanju devizama i vrijednosnim papirima. S obzirom da je trgovanje vrijednosnim papirima veoma intenzivna aktivnost te istovremeno veoma profitabilna djelatnost za banku, greške koje se javljaju pri provedbi svakodnevnih transakcija mogu rezultirati gubicima, bilo za klijenta (ako se trguje po nalogu klijenata) ili izravno za banku (ako se trguje za račun banke). Problematika grešaka pri trgovanju vrijednosnim papirima je da se ne može povratiti inicijalno stanje jednom kada se izvrši transakcija, kao što je to moguće s raznim internim sustavima banke. Također, velik broj naloga, osobito unutar dnevne transakcije potrebno je izvršavati velikom brzinom, što dovodi do nepažnje te kupnje prevelikog ili premalog iznosa novca ili vrijednosnih papira. Greške se stoga ne mogu otkloniti već samo ublažiti, što se provodi kroz dvije mitigacijske razine: prva razina podrazumijeva adekvatan trening brokera, prije čijeg završetka brokeri ne smiju obavljati transakcije sa stvarnim iznosima, već se na simulatoru treniraju da u uvjetima stresa obavljaju transakcije, kako bi se priviknuli na mentalni napor te u manjoj mjeri radili pogreške pri trgovanju sa realnim devizama ili vrijednosnim papirima. No s obzirom na faktor ljudske pogreške, ne može se očekivati kako se nikada neće provesti neispravna transakcija, stoga se kao druga razine ublažavanja ovakvih grešaka odvaja određeni iznos novca kao osiguranje za greške pri transakcijama. Izdvojeni iznos predstavlja svojevrsnu amortizaciju, odnosno zaštitni sloj, koji se unaprijed otpisuje iz imovine banke, te ako se greške dogode, ne utječu na ukupnu profitabilnost banke. Također, iznos za osiguranje transakcija koristi se ukoliko se pri pogrešnoj provedbi transakcije ošteti klijenta, te se slijedom toga klijentu vraća puni iznos provedene transakcije.”

„Po pitanju grešaka koje se događaju pri redovnom poslovanju može se istaknuti pogrešna procjena vrijednosti instrumenata osiguranja kojima se osiguravaju krediti. Instrumenti osiguranja (kolaterali) veoma su važni za banku, s obzirom da jamče sigurnost za povrat kredita ako klijent izgubi sposobnost vraćanja zajma. Zbog toga je pri uzimanju instrumenta osiguranja potrebno adekvatno procijeniti tržišnu vrijednost po kojoj banka može prodati taj instrument u svrhu namirenja neotplativog kredita. Procjene vrše ovlašteni procjenitelji, koji mogu biti zaposlenici banke ili vanjski suradnici koje banka angažira za jednokratnu procjenu prijesnosti nekretnine. No iako se radi o stručnjacima, greške nam se povremeno javljaju zbog velikog broja faktora koje je potrebno uzeti u obzir pri procjeni tržišne cijene nekretnine. Ako se nekretnina procijeni na premalu vrijednost, banka njezinom prodajom neće namiriti očekivani iznos za pokriće nenaplativog kredita. Istovremeno ako je vrijednost nekretnine procijenjena previsoko, banka će za takav kolateral odobriti veći kredit, te u slučaju nemogućnosti otplate vrijednost kolaterala neće biti dovoljna za namirenje cjelokupne vrijednosti kredita. Zbog toga smo kao zaštitnu mjeru postavili dvostruki sustav procjene vrijednosti nekretnina, u kojem zaposlenici banke vrše procjenu vrijednosti, dok se vanjskim suradnicima procjena šalje na verifikaciju, no važno je da se provede kontrola procjene vrijednosti prema istoj metodologiji po kojoj je provedena procjena, kako bi se na vrijeme utvrdila odstupanja i napravile korekcije vrijednosti kolaterala.“

U tablici 11. sažete su greške osoblja i mjere upravljanja na temelju navedenih primjera od strane ispitanika u provedenom intervju

Tablica 11. Primjeri grešaka osoblja i mjera upravljanja

GREŠKE OSOBLJA:	MJERE UPRAVLJANJA:
Pogrešan unos podataka *Nepotpuna dokumentacija* *Pogrešna procjena stupnja rizičnosti klijenta* *Nestručna upotreba aplikacija* *Pogrešna izrada financijskih izvještaja* *Nepravilno ugovaranje transakcija* *Neadekvatno upravljanje povjerljivim podacima* *Nepridržavanje internih pravila i procedura* *Zloupotreba mogućnosti pristupa informacijama*	• pravovremena i kontinuirana edukacija zaposlenika • standardizacija poslovnih procesa • uspostava jasnog lanca odgovornosti i komunikacije • uspostava adekvatnog sustava nagrađivanja zaposlenika • dvostruke kontrole provođenja rizičnih aktivnosti poput odobravanja značajnih kredita • osiguravanje od rizičnih transakcija • kontrole od strane unutarnje i vanjske revizije

Izvor: Izrada prema odgovorima iz intervjua provedenog s predstavnicima menadžmenta jedne banke

4.3. Zaključak studije slučaja

Razmatranjem prikupljenih odgovora moguće je zaključiti kako je uloga menadžmenta pri upravljanju rizicima vezanim uz greške osoblja veoma značajna. Menadžeri smatraju kako je nužno osigurati kontinuirane edukacije i treninge osoblja, osobito za nove zaposlenike te zaposlenike koji rade na procesima izloženim operativnim rizicima. Kao druga temeljna uloga menadžmenta naglašava se identifikacija poslovnih procesa koji su u velikoj mjeri izloženi rizicima, kako bi se zaposlenicima koji su uključeni u provedbu tih procesa osigurala temeljita edukacija i usavršavanje. Nadalje, razumijevanje prirode grešaka spomenuto je kao važna funkcija menadžmenta u upravljanju greškama osoblja. Naglasak je stavljen na greške koje se javljaju zbog nepažnje zaposlenika, te je zadatak menadžmenta da potiče zaposlenike na odgovornije i pažljivije obavljanje posla. Menadžment mora kontinuirano pratiti zadovoljstvo klijenata, jer je pad zadovoljstva često povezan s operativnim propustima i greškama osoblja. Ukoliko se zamijeti da klijenti nisu zadovoljni, menadžment mora istražiti uzrok problema te ga u najkraćem mogućem roku otkloniti. Menadžment ističe kako nije realno očekivati da će se greške osoblja potpuno otkloniti, te je zbog toga u budžetu potrebno osigurati sredstva za pokrivanje potencijalnih šteta koje nastaju zbog grešaka osoblja. No i dalje je potrebno aktivno educirati zaposlenike, kako bi se operativne greške svele na minimum. Naposljetu, važnost usmjeravanja značajnih napora i resursa u upravljanje operativnim rizicima uzrokovanim greškama osoblja, vidljiva je iz internih podataka banke prema kojima na poslovanje društva izrazito utječu rizici povezani s izvršavanjem i isporukom usluge klijentima što je prikazano u tablici 12.

Tablica 12. Stupanj utjecaja rizika na Društvo

VRSTA OPERATIVNOG RIZIKA:	UTJECAJ:
Interna prijevara	Vrlo nizak
Vanjska prijevara	Vrlo nizak
Kvarovi u tehnologiji i infrastrukturi	Vrlo nizak
Izvršenje, isporuka i upravljanje procesima	Umjeren
Klijenti, proizvodi i poslovni postupci	Umjeren
Katastrofe i javna sigurnost	Vrlo nizak

Izvor: Interni podaci banke u kojoj je provedena studija slučaja

4.4. Ograničenja istraživanja

Empirijsko istraživanje provedeno putem intervjua s tri predstavnika top, srednjeg i operativnog menadžmenta u jednoj poslovnici ne mora nužno biti dijeljeno stanje s drugim poslovnicama ili njihovim predstavnicima menadžmenta. Također prikupljeni i analizirani odgovori mogu biti pod utjecajem subjektivnog dojma ispitanika da prikaže svoj odjel ili poslovnicu u najboljem izdanju pa stoga isti ne moraju predstavljati i stvarno stanje u njihovoj organizaciji. Prema tome, istraživanje ne treba generalizirati na cjelokupno financijsko tržište koje je puno konkurenata koji nastoje postići svoju prednost različitostima i inovativnošću. Upravo radi očuvanja konkurentske prednosti, ali i politike povjerljivosti poslovanja, ispitanici su svoje odgovore prilagodili i ograničili sukladno obvezujućim ugovorima radnih pozicija i pripadajućih dopuštenja za dijeljenje djelomičnih podataka. Provedena analiza i doneseni zaključci mogu biti primjenjivi u svim financijskim institucijama, ali će se njihova primjena vjerojatno razlikovati ovisno o politikama i strategijama pojedinog poduzeća.

5. Zaključak

Razmatranjem iznesenih informacija u sklopu ovog diplomskog rada, može se zaključiti kako operativni rizici kao potencijalni rizici gubitaka, predstavljaju jedan od ključnih faktora u poslovanju financijskih institucija. Njihov značaj, odnosno utjecaj na poslovanje banaka može biti izrazito velik, a ogleda se u širokom spektru različitih događaja koji uzrokuju brojne vrste i podvrste operativnih rizika, a kao najznačajniji ističu se interna i eksterna prijevara te pogreške nastale u interakciji zaposlenika i sustava s klijentima. Shodno navedenom, potrebno je poduzeti odgovarajuće mjere kako bi se operativni rizici sveli na minimum, pri čemu se očituje važna uloga djelotvornog menadžmenta organizacije. Kao ključne elemente okvira za djelotvorno upravljanje operativnim rizikom banaka svih veličina i vrsta treba istaknuti jasnu strategiju i nadzor odbora direktora i više uprave, snažnu kulturu operativnog rizika, kulturu unutarnje kontrole koja, između ostaloga, podrazumijeva jasnu hijerarhiju nadležnosti i podjelu dužnosti, adekvatno unutarnje izvješćivanje te djelotvorno planiranje za slučaj nepredviđenih okolnosti.

Nadalje, provedenim empirijskim istraživanjem grešaka u svakodnevnom poslovanju banke, dolazi se do zaključka kako operativni rizici mogu uzrokovati smanjene prihoda ili povećanje troškova, što izravno negativno utječe na poslovni rezultat banke. Operativni rizici su razmotreni s aspekata sistemskih grešaka te grešaka vezanih uz osoblje, te je vidljivo kako realizacija rizika u obje dimenzije može nepovoljno utjecati na financijski rezultat banke, bilo da se radi o odlasku postojećih klijenata ili penala i kazni od strane regulatornih institucija.

Kao najznačajnije kategorije operativnih rizika identificirana su područja s visokim volumenom aktivnosti, poput poslovanja s klijentima u poslovnicama, gdje se na dnevnoj bazi odvija veliki broj transakcija, kao i područja s visokom razinom kompleksnosti, poput ocjene kreditnog rizika. Šteta koja nastaje realizacijom operativnih rizika u bankama promatra se kao smanjenje prihoda ili povećanje troškova. Rizici mogu utjecati na zadovoljstvo klijenata, što povećava vjerojatnost napuštanja banke i izravno smanjuje prihode. Također, operativni rizici mogu uzrokovati probleme u sustavu banke, te je potrebno povećati troškove kako bi se rizici otklonili te kako bi se poslovanje nesmetano nastavilo. U konačnici, može se zaključiti kako operativni rizici ugrožavaju poslovni rezultat banke.

Kao ključne mjere za sprječavanje i ublažavanje rizika u bankama, menadžment navodi kontinuirano nadgledanje poslovanja, razumijevanje poslovnih procesa te adekvatnu edukaciju i trening osoblja. Moguće je zaključiti kako se mjere moraju redovito provoditi, te svi zaposlenici moraju poštivati poslovna pravila i procedure, kako bi se operativni rizici sveli na minimum. Naposljetku, može se zaključiti kako je uloga menadžmenta pri upravljanju operativnim rizicima veoma značajna, te se očituje kroz planiranje edukacija zaposlenika i implementaciju programa mentorstva, kao i sustavno praćenje zadovoljstva klijenata, s ciljem pravovremene identifikacije potencijalnih problema i sprječavanja gubitka klijenata.

POPIS IZVORA

1. Banjo, S. (2015.), In a robot world, Goldman Sachs lists "human error" as new risk factor, https://qz.com/349900/in-a-robot-world-goldman-sachs-lists-human-error-as-new-risk-factor/, pristupljeno: 08.06.2018.
2. Basel Committee on Banking Supervision (2003), *Sound practices for the management and supervision of operational risk*, Bank for International Settlements, Basel
3. BCG (2018.), Risk management and compliance, https://www.bcg.com/industries/financial-institutions/risk-management.aspx, pristupljeno: 09.06.2018.
4. Bickford, J. (2016.), The five practices that set operational risk leaders apart, https://www.bcg.com/publications/2016/financial-institutions-operations-five-practices-operational-risk-leaders-apart.aspx, pristupljeno: 10.06.2018.
5. Bilby, K. (2015.), Reducing the risk of human error data loss, https://www.pandle.co.uk/reducing-the-risk-of-human-error-data-loss/, pristupljeno: 09.06.2018.
6. Birndelli, G., Ferretti, P. (2017.), *Operational Risk Management in Banks*, Palgrave Macmillan, London
7. Brzović, M. (2016.), Identifikacija i upravljanje operativnim rizicima, http://www.poslovnaucinkovitost.eu/kolumne/poslovanje/1372-identifikacija-i-upravljanje-operativnim-rizicima, pristupljeno: 05.06.2018.
8. Crouhy M., Galai D., Mark R. (2006.), *The essentials of risk management*, McGraw-Hill, New York
9. Adelsberger, Z., Buntak, K., Adelsberger, D. (2011.), Operativni rizici kao temelj sistema upravljanja, http://www.kresimir-buntak.com/Radovi/2012/48_Operativni_rizici.pdf, pristupljeno: 20.08.2019.
10. DirectKaspereit, T. (2017.), Systemic operational risk: Spillover effects of large operational losses in the European banking industry, *The Journal of Risk Finance*, 18(3): 252-267.
11. Domingo, R. (2003.), How to minimize clerical errors in banking, http://www.rtdonline.com/BMA/BSM/16.html, pristupljeno: 06.06.2018.
12. Foot, M. (2002.), Operational risk management for financial institutions, *Journal of Financial Regulation and Compliance*, 10(4): 313-316.

13. Gosh, A. (2012.), *Managing Risks in Commercial and Retail Banking*, Wiley Finance, London
14. Greuning, H., Bratanović, S. (2006.), *Analiza i upravljanje bankovnim rizicima*, Mate, Zagreb
15. HANFA (2014.), Smjernice za primjereno upravljanje rizicima informacijskih sustava subjekata nadzora, https://www.hanfa.hr/getfile/41744/7-Smjernice%20za%20primjereno%20upravljanje%20rizicima%20IS%20subjekata%20nadzora%20Agencije.pdf, pristupljeno: 14.06.2018.
16. Härle, P. (2015.), The future of bank risk management, https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.ashx, pristupljeno: 05.06.2018.
17. Kozarević, E. (2009.), Identifikacija operativnih rizika banke utemeljena na njihovoj taksonomiji, *Tranzicija*, 11(23-24): 58-70.
18. Risk.net (2017.), Top 10 operational risks for 2017, https://www.risk.net/risk-management/operational-risk/2480528/top-10-operational-risks-for-2017, pristupljeno: 10.06.2018.
19. Severović, K., Žajdala, N., Cvetković Šoštarić, B. C. (2009.), Konceptualni model kao alat za upravljanje kvalitetom bankarskih usluga, *Ekonomski vjesnik*, 1: 151-155.
20. Šverko, I. (2007.), *Upravljanje nekreditnim rizicima u hrvatskim financijskim institucijama*, H.I.B.O., Zagreb
21. Tarantino, A. (2008.), *Operational Risk Management in Financial Services*, Wiley, New York
22. UBM Tech (2013.), Innovative Workflows Reduce Errors in Banking Processes, http://media.lexmark.com/www/doc/en_GB/Innovative_Workflows_Reduce_Errors.pdf, pristupljeno: 07.06.2018.
23. Bain&Company (2018.), How Banks Can Manage Operational Risk, https://www.bain.com/insights/how-banks-can-manage-operational-risk/, pristupljeno: 20.08.2019.
24. HNB (2016.), Odluka o upravljanju rizicima, https://www.hnb.hr/documents/20182/525873/h-odluka-o-upravljanju-rizicima_npt.pdf/381be9bf-4fff-4eba-b1d3-157b776ca203, pristupljeno 14.08.2019.

POPIS TABLICA

POPIS ILUSTRACIJA