

**UNIVERZITET SINGIDUNUM
DEPARTMAN POSLEDIPLOMSKIH STUDIJA**

MAGISTARSKI RAD

**RIZICI U BANKARSTVU SA POSEBNIM
OSVRTOM NA OPERATIVNI RIZIK**

Mentor:
Prof.dr Budimir Stakić

Student:
Vesna Vuković 11/2004

Beograd, 2009.

S A D R Ź A J

UVOD	5
------------	---

PRVI DEO BANKARSKI RIZICI PREMA BAZELSKIM SPORAZUMIMA

1.BAZELSKI SPORAZUMI	9
1.1. BAZELSKI SPORAZUM I	9
1.1.1. Definicija kapitala po Bazelskom sporazumu I	10
1.1.2. Standardi za bankarski kapital i tržišni rizik	11
1.1.3. Razlozi za uvođenje Bazelskog sporazuma II.....	13
1.2. BAZELSKI SPORAZUM II.....	15
1.2.1. Ciljevi Novog Sporazuma o kapitalu.....	16
1.2.2. Struktura Bazelskog sporazuma II.....	17
1.2.2.1. Stub I – minimum nužnog kapitala.....	19
1.2.2.2. Stub II – Nadzor nad adekvatnošću kapitala.....	23
1.2.2.3. Stub III – Tržišna disciplina.....	25

DRUGI DEO VRSTE RIZIKA U BANKARSTVU

2.VRSTE RIZIKA U BANKARSTVU.....	27
2.1. Rizik likvidnosti.....	28
2.2. Kamatni rizik.....	31
2.3. Rizici izloženosti banke prema jednom licu ili grupi povezanih lica.....	35
2.4. Rizici ulaganja banke u druga pravna lica i u osnovna sredstva.....	36
2.5. Rizik zemlje.....	36
2.6. Devizni rizik.....	38
2.7. Operativni rizik.....	40

TREĆI DEO OPERATIVNI RIZIK

3. OPERATIVNI RIZIK	42
3.1. Definisanje operativnog rizika.....	42
3.2. Izvori operativnog rizika.....	45
3.3. Upravljanje operativnim rizikom.....	47
3.3.1. Identifikacija.....	54
3.3.2. Ocena.....	56
3.3.3. Kontrola.....	58
3.3.4. Praćenje.....	61
3.4. Oblasti upravljanja operativnim rizikom.....	62
3.4.1. Upravljanje informacionim sistemom.....	68
3.4.1.1. Sigurnost informacionog sistema.....	74
3.4.1.2. Održavanje informacionog sistema i planiranje kontinuiteta poslovanja	78
3.4.1.3. Razvoj informacionog sistema	88
3.4.2. Upravljanje rizikom informacionog sistema.....	93
3.5. Uloge i odgovornosti pri upravljanju operativnim rizicima.....	101
3.6. E-banking.....	105

ČETVRTI DEO REGULATORNI OKVIRI

4. REGULATORNI OKVIRI.....	115
4.1. Propisi EU.....	115
4.2. Regulatorni okviri Republike Srbije.....	119
4.2.1. Bankarski sektor u Srbiji – razvoj i aktuelno stanje.....	120
4.2.2. Svrha i ciljevi uvođenja standarda Bazelskog komiteta za bankarsku superviziju.....	120
4.3. ISO standardi	122

ZAKLJUČNA RAZMATRANJA.....	128
----------------------------	-----

LITERATURA.....	132
Neautorizovani izvori.....	135
Elektronski izvori.....	135

U V O D

U V O D

Razvojem savremenog bankarstva i privrede, izloženost različitim vrstama rizika u poslovanju postaje sve veća. Blagovremeno identifikovanje svih vrsta rizika i adekvatne mere zaštite, postaju izuzetno važan faktor uspešnosti poslovanja, u sve složenijim uslovima privređivanja.

Rizici u poslovanju, kao merljiva verovatnoća događaja, poslednjih deset godina su najaktuelnija tema u debatama naučne i stručne javnosti. Velika izloženost banaka različitim rizicima, ali i složenost postupka njihove identifikacije i merenja, proces upravljanja, podigla je na nivo filozofsko-stručnog razmišljanja, što predstavlja stručno znanje i obrazovanje menadžera rizika, ali i visok stepen kreativnosti i inovativnosti u donošenju konačnih odluka.

U cilju stabilnosti u razvoju svog poslovanja i ravnopravnog učešća u velikoj tržišnoj konkurenciji, a pre svega radi zaštite svojih deponenata i očuvanja systemske stabilnosti i likvidnosti, banke moraju da u svoje strateške ciljeve ugrade strategije upravljanja bankarskim rizicima. Primena upravljanja i analiza rizika u bankarstvu, promovira se u neophodan proces ekspanzije zdravog i stabilnog bankarskog sistema.

U okviru ukupnih rizika koji prate poslovne aktivnosti banaka, privrede i drugih oblika organizovanja biznisa poseban značaj ima operativni rizik. Njegova priroda, ispoljavanje u fluidnoj formi i prisutnost u svim segmentima poslovnih aktivnosti, dovoljno govore o značaju koji ima i potrebi za njihovim upravljanjem. Permanentan rastući trend operativnih rizika je realnost sa kojom se suočavaju, ne samo bankarske institucije, već i subjekti u privrednom i vanprivrednom sektoru, što problematiku operativnog rizika čini izuzetno važnom i aktuelnom.

Upravljanje operativnim rizicima, kao posebnom i veoma kompleksnom kategorijom, veliki je izazov i za razvijene bankarske industrije, kao i privredne sisteme. Discipline upravljanja ovim rizikom relativno su mlade, pa su iskustva i znanja iz ove oblasti od izuzetnog značaja za reformisanu bankarsku industriju Srbije, koja se ubrzano približava evropskim standardima i pristupa definisanju strategija upravljanja najvažnijim vrstama rizika.

Predmet ovog magistarskog rada je da istraži savremena teorijska dostignuća upravljanja i analiziranja rizika u bankarstvu, sa posebnim osvrtom na operativni rizik, koja će pomoći smanjenju rizika, a time ojačati pozicije banaka, koje stvaraju zdrav bankarski sistem Republike Srbije, koji direktno utiče na stabilnosti nacionalnog finansijskog sistema, a sa težnjom :

- da se unapredi način na koji upravljački i operativni sistemi u bankama i privrednim sistemima, razumeju i osećaju proces upravljanja operativnim rizikom,
- da bording direktora i menadžerima rizika u bankama, omogućiti lakša prepoznavanja optimalnog puta za definisanje ukupnog okvira za upravljanje operativnim rizikom i njegovu implementaciju, primereno datom trenutku i stepenu razvijenosti bankarske industrije,

- da pomogne menadžerima u privrednim sistemima u kreiranju okvira za upravljanje operativnim rizikom, na osnovu iskustava i znanja iz bankarske prakse, s obzirom na to da su ona u najvećoj meri primenljiva i u drugim sistemima.

NAUČNI CILJ ovog istraživanja jeste naučna deskripcija savremenih procesa upravljanja operativnim rizikom u bankarstvu u Republici Srbiji; naučni opis činioca strukture procesa upravljanja rizicima u bankarstvu; naučni opis funkcija, odnosa i veza upravljanja operativnim rizikom i naučni opis svih kvantitativnih i kvalitativnih svojstava upravljanja operativnim rizikom u bankarstvu u Republici Srbiji.

DRUŠTVENI CILJ izrade ove magistarske teze jeste udovoljavanje praktičnim potrebama u toj oblasti. Rezultati istraživanja treba da ukažu na otvorena pitanja utvrđivanja potrebnog upravljanja operativnim rizikom u bankarstvu, kao i da usmere pažnju svih subjekata političkih i ekonomskih procesa u Srbiji na ta pitanja i da utiču na njihove stavove i ponašanje u procesu donošenja konkretnih odluka. Ovo zbog toga što je neosporno da svako istraživanje, a naročito ono koje se namerava da realizuje, podrazumeva određeni društveni odnos.

METODOLOŠKI PRISTUP u izradi ovoga rada postavljen je veoma kompleksno putem kombinacije osnovnih (analitičkih i sintetičkih), opštenaučnih (induktivnih i deduktivnih, hipotetičkih i empirijskih) i posebnih metoda (ekonomske analize), na način da budu primereni naslovu teze i izloženoj strukturi rada. Njegova adekvatna primena omogućiće da se steknu pouzdana saznanja o predmetu istraživanja, o činjenicama, pojavama, procesima i odnosima na kojima počiva i odvija se transformacija bankarskog sektora u Srbiji, ali i o pojmovima, stavovima, sudovima i zaključcima koji su relevantni za ispunjavanje svrhe ovoga rada.

Hipotetički okvir istraživanja sastoji se od sledećih stavki:

GENARALNA HIPOTEZA:

Oblik i suština pravnog, ekonomskog i političkog sistema i ekonomskih uslova privređivanja determinišu proces upravljanja rizicima u bankarstvu, i to za onoliko za koliko je ostvarena pravna sigurnost, pravda i pravičnost, slobodni uslovi tržišnog privređivanja i demokratičnost političkog sistema, najmanje za toliko su smanjeni rizici u bankarstvu, a time i nivo potrebnog kapitala banaka za zaštitu od rizika.

POSEBNA HIPOTEZA:

- Proces upravljanja operativnim rizikom u bankarstvu Republike Srbije determinisan je širokim krugom pravnih odredbi koje se javljaju u dvojnoj ulozi: u ulozi okolnosti (ambijenta) i u ulozi predmeta odlučivanja;
- Za onoliko za koliko banke u Republici Srbiji primenjuju Bazelski sporazum II najmanje za toliko su smanjeni rizici i olakšan proces upravljanja istim;
- Ekonomski procesi u Srbiji determinišu proces upravljanja rizicima u bankarstvu, tj. zahtevaju pravilniju procenu potencijalnih gubitaka i na toj osnovi potreban minimalni iznos kapitala kao branu sigurnosti.

POJEDINAČNA HIPOTEZA:

- Primena novih bankarskih pravila poslovanja u Republici Srbiji determinisana je međunarodnim regulatornim okvirima i pravnim propisima Republike Srbije;
- Upravljanje rizicima neposredno je determinisano visinom kapitala banke;
- Supervizija kontrolne funkcije omogućava primereno upravljanje rizicima - smanjenje istog;
- Za onoliko za koliko je prisutna transparentnost u radu banke i ukupna finansijska disciplina, najmanje za toliko je omogućen proces upravljanja operativnim rizikom;
- Za onoliko za koliko se obavezno ocenjuje kreditni rejting svakog korisnika kredita, za toliko su smanjeni rizici;
- Ekonomski i politički procesi u Srbiji zahtevaju od banaka da procenjuju rizike svake poslovne transakcije koja bi trebalo da bude predmet kreditiranja;
- Od ekonomske snage banke direktno zavisi upravljanje operativnim rizikom, tj. što je kapital banke veći, za toliko je veće pokrivanje rizika.

U prvom delu magistarske teze, koji nosi naziv „Bankarski rizici prema Bazelskim sporazumima“ biće razmotrena regulativa, prvenstveno pravila Bazelskog sporazuma I, a potom i Bazelskog sporazuma II, sa posebnim osvrtom na rizike u bankarstvu, kao i kvalitativni i kvantitativni kvalifikacioni kriterijumi za predložene pristupe kalkulaciji ekonomskog kapitala po osnovu izloženosti operativnom riziku i predloženih pristupa za kalkulaciju ekonomskog kapitala (Pristup osnovnog indikatora, Standardizovani i Viši pristup).

U drugom delu ove teze, koji nosi naziv „Rizici u bankarstvu“ biće razmotrene najrasprostranjenije vrste rizika u bankarstvu, a tu su: rizik likvidnosti, kamatni rizik, rizici izloženosti banke prema jednom licu ili grupi povezanih lica, rizici ulaganja banke u druga pravna lica i u osnovna sredstva, rizici koji se odnose na zemlju porekla lica kome je banka izložena, devizni i naravno operativni rizik.

U trećem delu je detaljno objašnjen operativni rizik, izvori operativnog rizika, kao i proces upravljanja, koji ukazuje na važnost obuhvatnog i preciznog definisanja pojma operativnog rizika i dinamiku procesa, koja se odvija na nekoliko nivoa : identifikacija, ocena, kontrola i praćenje. Ukazano je na značaj upravljanja operativnim rizikom , kao i nezaobilazni e-banking i svakako značaj kulture profesionalnog ponašanja u odnosu na moguće izloženosti operativnom riziku, na neophodnu komunikaciju na svim nivoima unutar banke.

Četvrti deo ovog rada koji nosi naziv „Regulatorni okviri“ posvećen je propisima Evropske unije, ISO standarim i naravno propisima Republike Srbije.

Na kraju rada data su „Zaključna razmatranja“, kao i spisak korišćene literature i drugih izvora pri izradi ove magistarske teze.

PRVI DEO

BANKARSKI RIZICI PREMA BAZELSKIM SPORAZUMIMA

1. BAZELSKI SPORAZUMI

1.1. BAZELSKI SPORAZUM I

Bankama pripada značajno mesto u finansijskom mehanizmu svake privrede. Od banaka mnogo zavisi finansijska snaga privrede, a sa svoje strane, snaga banaka opredeljena je snagom nacionalne privrede u svakoj zemlji¹. Stoga, međunarodno bankarstvo posvećuje izuzetnu pažnju minimalnim supervizorskim standardima, koje banka mora da ispuni da bi dobila, a samim tim i zadržala licencu za poslovanje. Osnovi razlog za to je da se celokupan finansijski sistem, deponenti i investitori obezbede od rizika koji sa sobom nosi bankarsko poslovanje. Tokom sedamdesetih godina razvoj bankarstva je doživeo tako veliku ekspanziju, da regulatorni organi pojedinih zemalja nisu imali snage i moći da se nose sa kontrolom poslovanja sve većeg broja finansijskih institucija, od kojih su mnoge, zbog sve veće globalizacije finansijskih tržišta, dolazile iz različitih zemalja i poslovale po različitim kapitalnim i supervizorskim standardima. Takva distorzija stvarala je nepovoljno okruženje za liberalizaciju i konkurentnost međunarodnog finansijskog tržišta. Da bi centralne banke svih zemalja mogle da vrše kontolu i da posluju po zajedničkim supervizorskim standardima, bilo je potrebno konstituisati telo koje će izvršiti potrebnu koordinaciju u ovoj oblasti i postići dogovor o minimumu zajedničkih standarda koji će se primenjivati.

Taj zadatak dobila su dva takozvana supranacionalna tela: Komisija Evropske zajednice i Bazelski komitet. Prvo telo imalo je zadatak da oblikuje zajedničke standarde supervizije koji će se primenjivati u zemljama EZ, odnosno EU². Drugo telo – Bazelski komitet, tretira samo banke koje posluju i van svojih matičnih zemalja, obavezujući ih da ispunjavaju propisane standarde. Koreni ovog tela datiraju od 1974. godine.

Pun naziv Komiteta je "*Committee on Banking Regulations and Supervisory Practices*", ali se upotrebljava skraćeni naziv - Bazelski komitet³. Sačinjen je od predstavnika centralnih banaka i regulatornih tela zemalja osnivača. Svrha komiteta je tokom vremena evoluirala i obuhvata:

- definisanje uloga regulatora u situacijama sa nejasnim jurisdikcijama;
- kontrolu da međunarodne banke i bankarske holding kompanije ne izbegnu detaljnu superviziju od strane »domaćih« regulatornih tela;
- promociju uniformnih koeficijenata solventnosti, kako bi banke iz različitih zemalja mogle da učestvuju na tržištu pod ravnopravnim uslovima⁴.

Bazelski komitet je 1988. godine izdao set standarda o minimumu nužnog kapitala za međunarodno aktivne banke. Ovi standardi su ušli u pravo zemalja G10 (Belgija,

¹ Dr Slobodan Barać, Dr Budimir Stakić : Međunarodne finansije, Fakultet za finansijski menadžment i osiguranje, Beograd 2003., str. 34

² Ugovor o EU potpisan je u Matrihtu 07.02.1992. - «Evropa od A do Š » , naslov originala »Werner Weidenfeld, Wolfgang Wessels (Hrsg.) Europa von A bis Z » , izdavač BPB Savezna centrala za političko obrazovanje Fondacija Konrad Adenauer, Beograd 2003. pp 112.

³ Bank of England (1995) Report of the Board of Banking Supervision. Inquiry into the Circumstances of the Collapse of Barings, London.

⁴ Koeficijent solventnosti predstavlja odnos između sopstvenih sredstava i rizične aktive i vanbilansnih stavki – Jeremić, Finansijska tržišta, FFMO, Beograd 2003. str. 246.

Kanada, Francuska, Nemačka, Italija, Japan, Holandija, Švedska, Švajcarska, Engleska i SAD) u 1992. godini, samo je japanskim bankama odobren dodatni tranzicioni period. Ovi standardi su kasnije postali poznati pod nazivom »1988 Basle Accord« (u daljem tekstu Bazel I). Zabrinutost guvernera centralnih banaka G10 zbog erozije kapitala krupnih banaka usled trajne međusobne konkurencije, bio je glavni razlog za uvođenje standarda, jer je to pretilo neredom na svetskom finansijskom tržištu.

Bazel I je prevashodno bio usmeren na kreditni rizik. Aktiva banaka je podeljena u nekoliko grupa, zasnovanih na nivou rizika, kojoj je odgovarao jedan ponder rizika - risk weight (u daljem tekstu ponder). Obično su potraživanja od državnih institucija zemalja G10 imala ponder 0%; ponder za potraživanja od banaka G10 je bio 20%; a ostala potraživanja 100%. Banke su imale obavezu da u rezervi drže kapital u iznosu ne manjem od 8% od rizične aktive, tj. 8% od iznosa ponderisane aktive.

Glavni ciljevi Bazelskog sporazuma I bili su obezbeđivanje:

1. adekvatnog nivoa kapitala u međunarodnom bankarskom sistemu i
2. lojalne konkurencije na tržištu bankarskih usluga, tako da nijedna banka više ne može da posluje ako nema adekvatni obim kapitala.

Ovi ciljevi su ostvareni. Stoga je u toku 1990 - tih godina bazelski Sporazum o kapitalu prihvaćen kao svetski standard. Više od sto zemalja primenilo je bazelski okvir na svoj bankarski sistem. U osnovi ga je prihvatila i naša zemlja.

1.1.1. Definicija kapitala po Bazelskom sporazumu I

Glavna forma kapitala podobnog da pokrije tržišne rizike sastoji se od akcionarskog kapitala i zadržanih prihoda (*tier 1 capital*) i dodatnog kapitala (*tier 2 capitala*) kako su definisani u Sporazumu iz 1988. godine⁵. Ali banke prema diskrecionom pravu njihovih nacionalnih organa kontrole, mogu da primene kapital trećeg tiera (*tier 3*) sačinjen od kratkoročnog subordiniranog duga i to jedino da bi ispunile proporciju zahteva u pogledu kapitala za tržišne rizike, pod sledećim uslovima:

- banke imaju pravo da koriste tier 3 kapital samo da bi podržale tržišne rizike,
- tier 3 kapital se ograničava na najviše 25% od bančinog tier 1 kapitala, koji je potreban da podržava tržišne rizike,
- tier 2 elementi mogu zameniti tier 3 do istog limita od 25% tako da ukupni limiti iz Sporazuma iz 1988. godine ne budu prekoračeni, tj. podoban tier 2 kapital ne sme da nadmaši ukupan tier 1 kapital, a dugoročni subordinirani dug ne sme da nadmaši 50% tier 1 kapitala.

Komitet veruje da je tier 3 kapital jedino pogodan da pokriva tržišni rizik. Međutim, veliki broj zemalja članica su opredeljene da se zadrži princip iz Sporazuma da tier 1 kapitala predstavlja najmanje polovinu od ukupnog kvalifikovanog kapitala, tj. da zbir ukupnog tier 2 i tier 3 kapitala ne sme da bude veći od ukupnog tier 1.

Komitet je zaključio da odluku o tome prepusti diskrecionom pravu nacionalnih organa.

⁵ www.bis.org

Da bi se kratkoročni subordinirani dug kvalifikovao kao tier 3 kapital, potrebno je da ispuni uslov da postane deo trajnog kapitala banke i da na taj način bude u mogućnosti da apsorbuje gubitke u slučaju insolventnosti.

Zato mora najmanje:

- da bude neosiguran, subordiniran i u potpunosti uplaćen,
- da ima prvobitnu ročnost od najmanje dve godine,
- da ne dospeva pre ugovorenog datuma otplate, osim ako organi kontrole to prihvate,
- da ima klauzulu o fiksiranju (lock-in clause) koja predviđa da ni kamata ni glavnica ne mogu biti otplaćeni (čak i kod dospeća) ako ta otplata znači da će banka da padne ispod ili da ostane ispod zahteva za minimumom kapitala.

1.1.2. Standardi za bankarski kapital i tržišni rizik

Zahtevi za kapitalom kod opšteg tržišnog rizika imaju za cilj da pokriju rizik od gubitka koji nastaje iz promena kamatnih stopa na tržištu⁶. Dozvoljen je izbor između dva glavna metoda za merenje rizika: metod dospeća (maturity) i metod ročnosti (duration). Kod oba metoda, terećenje kapitala je zbir četiri komponente:

- neto kratka ili duga pozicija u celokupnoj trgovinskoj knjizi,
- mala proporcija uparenih pozicija u svakom vremenskom rasponu (vertikalno ograničenje),
- veća proporcija uparenih pozicija kroz različite vremenske raspone (horizontalno ograničenje),
- neto terećenje za pozicije u opcijama, gde je to primereno.

U međuvremenu došlo je do značajnih promena u bankarskom poslovanju, tj. u praksi upravljanja rizikom, pristupu nadzora nad delatnošću banaka i na finansijskim tržištima. Uočene su i izvesne teškoće. Od početka 1998. godine, banke su bile u obavezi da i pored merenja i terećenja kapitala u pogledu kreditnih rizika, rade to i za tržišne rizike.

Sporazum o kapitalu iz 1988. godine nije tretirao tržišni rizik koji je bivao sve prisutniji u bankarskom poslovanju⁷. Stoga je Bazelski komitet 1996. godine doneo amandman, kojim se uvodi obaveza merenja i terećenja kapitala u odnosu na izloženost tržišnom riziku. Tržišni rizik se definiše kao rizik od gubitaka u bilansnim i vanbilansnim pozicijama, koji mogu da nastanu kao posledica kretanja cena na tržištu.

Značajan deo bančinog internog sistema merenja tržišnog rizika predstavlja skup faktora tržišnog rizika, tj. tržišnih stopa i cena koje utiču na bančine trgovinske pozicije. Faktori rizika sadržani u sistemu za merenje tržišnih rizika moraju da budu dovoljni da obuhvate rizike koji se nalaze u bančinom portfoliju i vanbilansnim trgovinskim pozicijama. Banke imaju diskreciono pravo da specificiraju faktore rizika u svojim internim modelima, ali se moraju pridržavati sledećih smernica:

- a) Kod kamatnih stopa, mora da postoji skup faktora rizika koji odgovaraju kamatnim stopama za svaku valutu u kojoj banka ima bilansne ili vanbilansne pozicije osetljive na kamatnu stopu.

⁶ Basel Committee on Banking Supervision Risk Management Group (2000) *Other Risks Preliminary Survey*, Basel.

⁷ www.nbs.rs

b) Kod deviznih kurseva sistem merenja rizika mora da obuhvati faktore rizika, koji odgovaraju pojedinim stranim valutama u kojima su denominirane bančine pozicije. S obzirom na to da će broj za *value – at – risk* izračunat sistemom za merenje rizika biti izražen u bančnoj domaćoj valuti, svaka neto pozicija denominirana u stranoj valuti uvodi kursni rizik. Otuda moraju da postoje faktori rizika koji odgovaraju kursu po kome se domaća valuta razmenjuje za svaku stranu valutu u kojoj banka ima znatniju izloženost.

c) Za cenu akcija, mora da postoje faktori rizika koji odgovaraju svakom tržištu akcija na kome banka drži značajne pozicije.

d) Kod cene robe mora da postoje faktori rizika koji odgovaraju tržištu svake robe u kojoj banka drži značajne pozicije.

Veoma je važno da organi kontrole mogu da se uvere da banke koje koriste modele imaju sisteme za upravljanje tržišnim rizicima koji su konceptualno zdravi i da se primenjuju dosledno. U skladu sa tim, organ kontrole će dati specifikaciju određenog broja kvalitativnih kriterijuma koje banke moraju da ispune pre nego što dobiju dozvolu da koriste pristup zasnovan na modelima. Stepenu u kome banke ispunjavaju kvalitativne kriterijume može da utiče na nivo koji će organi kontrole ustanoviti za multiplikacioni faktor. Samo one banke čiji su modeli u strogoj saglasnosti sa kvalitativnim kriterijumima mogu biti podobne za primenu minimalnog multiplikacionog faktora. Kvalitativni kriterijumi obuhvataju sledeće:

a) Banka mora da ima nezavisnu jedinicu za kontrolu rizika koja je odgovorna za koncipiranje i primenu bančinog sistema za upravljanje rizikom. Ova jedinica treba da sačinjava i analizira dnevne izveštaje o autputu bančinog modela za merenje rizika, uključujući procenu odnosa između mera izloženosti riziku i trgovinskih limita. Ova jedinica mora da bude nezavisna od poslovnih trgovinskih jedinica i mora da podnosi izveštaje neposredno visokom menadžmentu banke.

b) Ova jedinica mora da sprovodi redovne programe testiranja unazad (*back – testing*), tj. *eks-post* poređenja mera rizika, koje je model generisao sa stvarnim dnevnim promenama vrednosti portfolija tokom dužih vremenskih perioda, kao i sa hipotetičkim promenama zasnovanim na statičkim pozicijama.

c) Bord direktora i viši menadžment moraju da budu aktivno uključeni u proces kontrole rizika i moraju da se odnose prema kontroli rizika kao prema suštinskom aspektu poslovanja kome moraju da se posvete značajni resursi⁸. U ovom pogledu, dnevni izveštaji koje priprema nezavisna jedinica za kontrolu rizika moraju da budu revidirani na nivou menadženta, koji je dovoljno visok i sa dovoljno ovlašćenja, da obezbedi smanjenje pozicija koje su uzeli pojedinačni trgovci i da se smanji opšta bančina izloženost riziku.

d) Bančin interni model za merenje rizika mora da bude blisko integrisan u dnevni proces upravljanja rizikom banke. Njegov autput mora u skladu sa tim da bude integralni deo procesa planiranja, praćenja i kontrole bančinog profita tržišnog rizika.

e) Sistem merenja rizika mora da se koristi u vezi sa internim limitima za trgovinu i izloženost. U tom pogledu, trgovinski limiti moraju da budu povezani sa bančnim modelom merenja rizika na način koji je konzistentan kroz vreme i koga su vrlo dobro shvatili i trgovci i viši menadžment.

⁸ Izveštaj, *Risk management guidelines*, koji je izdao Bazelski komitet jula 1994 godine dalje razrađuje odgovornosti borda direktora i višeg menadžmenta.

f) Rutinski i rigorozni program stresnog testiranja treba da je operativan kao dodatak analizi rizika zasnovanoj na svakodnevnom autputu bančinog modela za merenje rizika⁹. Menadžment mora periodično da revidira rezultate stresnog testiranja i oni moraju da imaju svoj odraz u politici i limitima koje postavljaju menadžment i bord direktora. Kada testovi pokažu naročitu ranjivost na dati skup okolnosti, moraju da se preduzmu brzi koraci da bi se takvim rizicima moglo da upravlja na odgovarajući način.

g) Banke moraju da primenjuju operativnu rutinu koja obezbeđuje pridržavanje dokumentovanog skupa internih politika, kontrola i procedura koje se odnose na funkcionisanje sistema za merenje rizika. Bančin sistem za merenje rizika mora da bude dobro dokumentovan.

h) Obavezno je da se sprovodi redovno nezavisna revizija sistema merenja rizika u sklopu bančinog internog procesa revizije. Ova revizija mora da obuhvati aktivnosti poslovnih trgovinskih jedinica i nezavisnu jedinicu za kontrolu rizika, koja treba da se naročito odnosi na minimum, koji obuhvata:

- adekvatnost dokumentacije sistema upravljanja rizikom i procesa;
- organizaciju jedinice za kontrolu rizika;
- integraciju merenja tržišnog rizika u dnevno upravljanje rizikom;
- proces prihvatanja modela za utvrđivanje cene rizika i sistema valorizovanja koje koristi personal u prednjoj i pozadinskoj službi;
- ozvaničenje značajnih promena u procesu merenja rizika;
- skalu tržišnih rizika uključenih u model merenja rizika;
- integritet menadžerskog informacionog sistema;
- preciznost i potpunost podataka o poziciji;
- verifikovanje konzistentnosti, blagovremenosti i pouzdanosti izvora podataka koji se koriste za vođenje internih modela, uključujući nezavisnost takvih izvora podataka;
- preciznost i adekvatnost pretpostavki volatilnosti i korelacije;
- preciznost izračunavanja valorizacije i transformacija rizika;
- verifikaciju preciznosti modela kroz često povratno testiranje.

Revizija celokupnog procesa upravljanja rizikom mora da se odvija u redovnim intervalima (najmanje jednom godišnje)

1.1.3. Razlozi za donošenje Bazelskog sporazuma II

Karakteristike pravila Bazela I:

- Identifikovane su glavne vrste kapitala koje su prihvatljive nadzornim agencijama (uključujući primarni ili osnovni kapital i sekundarni ili dodatni kapital) i uveden je prvi formalni standard za kapital, koji je uzimao u obzir izloženost riziku od transakcija sa vanbilansnim stavkama.

- Bazel I primarno je bio usmeren na kreditni rizik ili rizik neuspeha koji je nasleđen u aktivni u knjigovodstvenom bilansu banke i među vanbilansnim stavkama (kao što su ugovori o derivatima i kreditne obaveze), sa uključenom izloženosti tržišnom riziku od promene kamatne stope, strane valute i robnih cena koje su kasnije dodate.

⁹ Mada će banke imati izvesno diskreciono pravo kako da sprovedu stresne testove, njihov organ kontrole će tražiti da se pridržavaju generalnih linija.

- Ovaj ugovor postavio je uslove za određivanje potrebnog nivoa kapitala svake banke pojedinačno koristeći istu formulu i isti set stopa rizika.

- Primenjivani su isti minimalni nivoi potrebnog kapitala za sve banke zemalja članica (uključujući minimalni koeficijent od 4% primarnog kapitala prema ukupno ponderisanoj rizičnoj aktivni i minimalni koeficijent od 8% primarnog plus sekundarnog kapitala prema ukupno ponderisanoj rizičnoj aktivni).

Karakteristike pravila Bazela II:

- Bazel II obezbeđuje veću osetljivost na arbitražne poslove i inovacije na finansijskom tržištu, što zahteva fleksibilnije propise za banke nego što je dozvoljavao Bazel I.

- Prepoznaje različitu izloženost riziku kod različitih banaka, eventualnu primenu drugačijih metoda da bi se izvršila procena njihove jedinstvene izloženosti riziku i moguće podvrgavanje zahtevima za određivanje različitog nivoa potrebnog kapitala (uključujući različite propise za velike bankarske kompanije u odnosu na male).

- Proširuje vrste rizika koje se uzimaju u obzir prilikom utvrđivanja potrebnog nivoa kapitala i uspostavlja minimalni nivo potrebnog kapitala za pokrivanje kreditnog, tržišnog i poslovnog rizika. Rezultati ovih i drugih promena, takvi su da je Bazel II u suštini mnogo osetljiviji na rizike od Bazela I.

- Zahteva od svake banke da razvija sopstvene interne modele rizika upravljanja i testove na stres u procenjivanju sopstvenog stepena izlaganja riziku/VAR ili rizik vrednosti, u različitim tržišnim uslovima.

- Zahteva da svaka banka utvrdi sopstvene potrebe za kapitalom, bazirane na proračunu izloženosti riziku, koji može da bude podvrgnut reviziji od strane nadzornih organa vlasti imajući u vidu pojam »razumnosti«.

- Promoviše veće učešće javnosti u uvid stvarnog finansijskog stanja svake banke što stvara mogućnost veće primene tržišne discipline prema onim bankama za koje se procenjuje da preuzimaju preveliki rizik.

Bazel II - Sporazum o bankarskom kapitalu (obavezan od 2007. godine) je prevazišao nedostatke Bazela I, obuhvatajući inovacije i uvodeći procenu unutrašnjeg rizika (da ga same utvrde, uz nadzor), a u isto vreme i napredak u modelima kreditnog rizika. Tri metodologije: simulacija zasnovana na istorijskim kretanjima, "delata-norma" i Monte Carlo simulacija.

Slabosti VaR:

- 1) kretanja na tržištu nisu po "normalnoj distri",
- 2) kretanja iz prošlosti nisu uvek dobra aproksimacija kretanja u budućnosti,
- 3) ocene VaR bazirane na stanju na kraju dana (ne uzimaju u obzir trgovanje u toku dana),
- 4) model ne dozvoljava rizik koji je rezultat izuzetno ekstremnih okolnosti na tržištu,
- 5) mnogo pojednostavljenja (naročito kod opcija).

1.2. BAZELSKI SPORAZUM II

Sporazum o kapitalu iz 1988. godine je stavljao naglasak na adekvatnost kapitala banke, koji jeste životno važan za snižavanje rizika od insolventnosti banke i rizika od bankrota banke za njene deponente¹⁰. Iako se fokusira uglavnom na kreditni rizik, implicitno su, ali u nedovoljnoj meri pokriveni i neki drugi rizici. Bazel I je u velikoj meri izmenjen 1996. godine, kada su u njega uključeni standardi o minimumu nužnog kapitala za tržišne rizike u knjizi trgovanja.

Taj standard je prihvaćen i primenjuje se u više od stotinu zemalja. Međutim, bez obzira na pozitivne učinke, koje je imao na sigurnost poslovanja banaka, poslednjih nekoliko godina je postalo jasno da su potrebne radikalne promene, ako želi da se postigne da bonitetna regulativa zadrži svoj dosadašnji značaj za održavanje sigurnosti i stabilnosti bankarskog sistema u uslovima velikog broja inovacija i razvoja novih tehnika upravljanja rizicima.

Slabosti postojećeg standarda ogledaju se u sledećim:

- Adekvatnost kapitala se ne procenjuje u odnosu na stvarni rizični profil banke (ograničena diferencijacija kreditnog rizika, operativni rizik nije obuhvaćen);

- Procena rizika zemlje nije primerena;

- Ne pruža dovoljno motiva za primenu tehnika za smanjivanje rizika. Naime, ako je za banku cena odobrenog kredita jednaka za visoko i nisko rizične klijente, a banka naplaćuje višu kamatu od visoko rizičnih klijenata, onda menadžeri banke koji ciljaju na maksimizaciju profita imaju jak motiv da klijentima visokog rizika zamene svoje niskorizične klijente;

- Omogućuje regulatornu arbitražu putem sekjuritizacije.

U junu 1999. godine Bazelski odbor je objavio prvi predlog novog standarda koji će zameniti Bazel I¹¹. Mnogo detaljniji skup konsultativnih dokumenata izdat je u januaru 2001. godine (CP2 – *Consultative paper 2*). Nakon intenzivne interakcije sa predstavnicima banaka u aprilu 2003. godine nastao je treći konsultativni papir (CP3). U procesu usvajanja konačne verzije Bazela II, Bazelski odbor je objavio i niz saopštenja za javnost i drugih dokumenata, a u junu iste godine Odbor je objavio i konačni tekst. Time je bio unet jedan sasvim novi pristup u načinu regulisanja poslovanja banaka, što će sigurno obeležiti ovu deceniju u bankarstvu i bankarskoj superviziji.

Sporazum o kapitalu iz 1988. godine je stavljao naglasak na adekvatnost kapitala banke, koji jeste životno važan za snižavanje rizika od insolventnosti banke i rizika od bankrota banke za njene deponente. Novi Sporazum, uvažavajući značaj adekvatnosti kapitala, ide korak dalje, da ojača sigurnost i zdravo poslovanje finansijskog sistema, naglašavajući značaj kvalitativnog aspekta: unutrašnji bankarski nadzor, odgovornost posloводства banke, novi postupak nadzora nad bankom i tržišna disciplina.

Samim tim novi Sporazum je kompleksniji od sporazuma iz 1988. godine. Ključna novina je u većoj osetljivosti na rizik. On sadrži niz opcija za merenje kreditnog rizika (*credit risk*) i rizika poslovanja (*operational risk*). Sem toga, Novi Sporazum podvlači značaj i ulogu procesa nadzora nad bankama i tržišne discipline kao bitnih dopuna minimumu nužnog kapitala.

¹⁰ Dr Slobodan Barać, Dr Budimir Stakić, Dr Marko Ivaniš: Praktikum za bankarstvo i finansije, Fakultet za finansijski menadžment i osiguranje, Beograd, 2003. str.53

¹¹ www.24x7.rs

U predloženoj reviziji Sporazuma iz 1988. godine je posebno važno mesto dobilo oslanjanje banaka na sopstvene procene rizika kome su izložene u proračunavanju minimuma nužnog iznosa kapitala.

U čemu je novi Sporazum drugačiji od starog? U stvari, glavna novina je u tome što novi Sporazum napušta uniformnu meru adekvatnosti kapitala i obezbeđuje mogućnost bankama da biraju najprimereniji način procene obima nužnog kapitala. To znači, novi Sporazum je osetljiviji na merenje različitih vrsta rizika i zato predlaže složenije tehnike za merenje rizika i za izračunavanje adekvatnosti kapitala. Ali, banke neće morati da se povinuju novom sporazumu u ovom pogledu. One će moći da zadrže način izračunavanja adekvatnosti kapitala kakav je danas na snazi.

Bazel II se zasniva na fleksibilnosti i sofisticiranim pristupima merenju kreditnog i operativnog rizika, što je nov način i pristup obavljanju supervizije. Bez obzira na složenost standarda, njihova primena bi trebalo da doprinese stabilnosti finansijskog sektora, jer će minimum nužnog kapitala, utvrđen novim metodama, realnije odražavati visinu rizika kojima je izložena svaka pojedinačna banka.

1.2.1. Ciljevi Novog Sporazuma o kapitalu

Novi Bazelski sporazum je namenjen organima koji vrše nadzor nad poslovanjem banaka¹². Polazna svrha je pomoć u izgradnji politike nadzora nad bankama. Pravno, on definiše okvir za utvrđivanje adekvatnosti kapitala banaka samo u zemljama članicama Bazelskog komiteta. Ali, očekuje se da će ga, kao i prethodni Sporazum, prihvatiti nadzorni organi u celom svetu. Opštoj primeni Sporazuma doprinose i Međunarodni monetarni fond i Svetska banka tako što koriste standarde Bazelskog komiteta u svojim misijama.

Bazelski komitet je u novom Sporazumu o kapitalu na nov način definisao njegove ciljeve. Krajnji cilj je jačanje finansijskog sistema kombinovanjem kvantitativnih i kvalitativnih standarda. Adekvatnost kapitala sada se povezuje sa mogućim rizikom u bankarskom poslovanju.

To treba da se postigne ostvarivanjem sledećih neposrednih ciljeva:

- a) povećavanje sigurnosti i poslovnosti finansijskog sistema zbog čega se i u novom okviru zadržava najmanje sadašnji opšti nivo kapitala;
- b) učvršćivanje načela jednakosti uslova konkurencije;
- c) izgradnja celovitijeg pristupa upravljanju rizikom;
- d) adekvatnost kapitala treba da bude na odgovarajući način osetljiva na stepen rizika u bankarskom poslovanju;
- e) Sporazum stavlja težište na banke sa međunarodnim poslovanjem, mada je poželjno da njegova načela budu primenljiva i na druge banke.

Drugim rečima, na osnovu dosadašnjeg iskustva Bazelski komitet je došao do zaključka da njegovi ciljevi ne mogu biti ostvarivani oslanjanjem samo na kvantitativni standard – minimum nužnog kapitala. Stoga su ovom kvantitativnom standardu u Novom Sporazumu dodata dva nova – kvalitativne prirode: nadzor nad bankama i tržišna disciplina.

¹² Dr Slobodan Barać, Dr Budimir Stakić, Dr Marko Ivaniš, op.cit. str.52

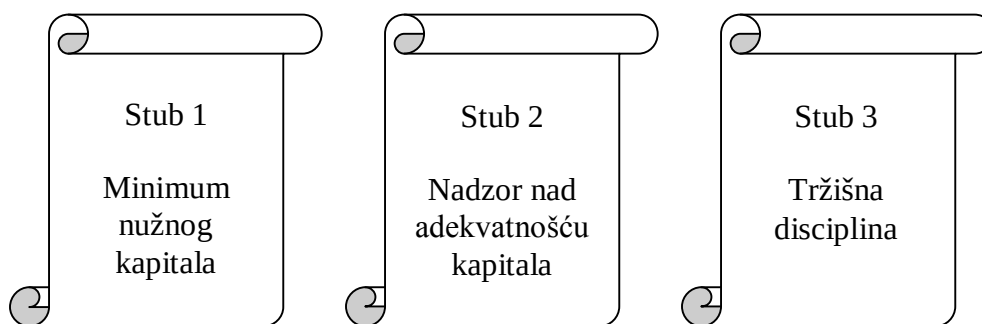
Komiteta podvlači da je na poslovođstvu banaka krajnja odgovornost za upravljanje rizikom i obezbeđivanje iznosa kapitala primenjenog stepenu sposobnosti banke da upravlja rizikom.

Konačni tekst Bazela II objavljen je krajem juna 2004. godine. Primena standardizovanog pristupa i osnovnog pristupa internog raspoređivanja počela je od kraja 2006. godine. Primena naprednih pristupa se odgađa do kraja 2009. godine, jer Bazelski odbor je smatrao da je bilo potrebno još neko vreme za analizu učinaka i paralelni obračun minimuma nužnog kapitala.

1.2.2. Struktura Bazelskog sporazuma II

Ključna karakteristika Bazela II je njegova struktura koja se temelji na tri osnovna stuba:

Slika 1. Struktura Bazela II



Stubovi su međusobno kompetentarni i svaki od njih omogućuje nešto što druga dva nisu u mogućnosti da pruže i svaki je bitan za ostvarenje ukupnog cilja Bazela II – na mikro-nivou, to je poboljšanje kvaliteta sistema upravljanja rizicima, a na makro-nivou, doprinos finansijskoj stabilnosti.

Stub 1, pre svega, definiše pravila za izračunavanje kreditnog i operativnog rizika. Suština je u tome što se pokazalo da se poslovanje i rizici kojima su banke izložene među bankama dosta razlikuju, pa zbog toga jednak način merenja rizika ne daje odgovarajuće rezultate kod svih banaka. Zbog toga Bazelski odbor u ovom standardu nudi nekoliko opcija za izračunavanje kreditnog i operativnog rizika, tako da svaka banka odabere onaj način koji je najprimereniji njenim specifičnostima.

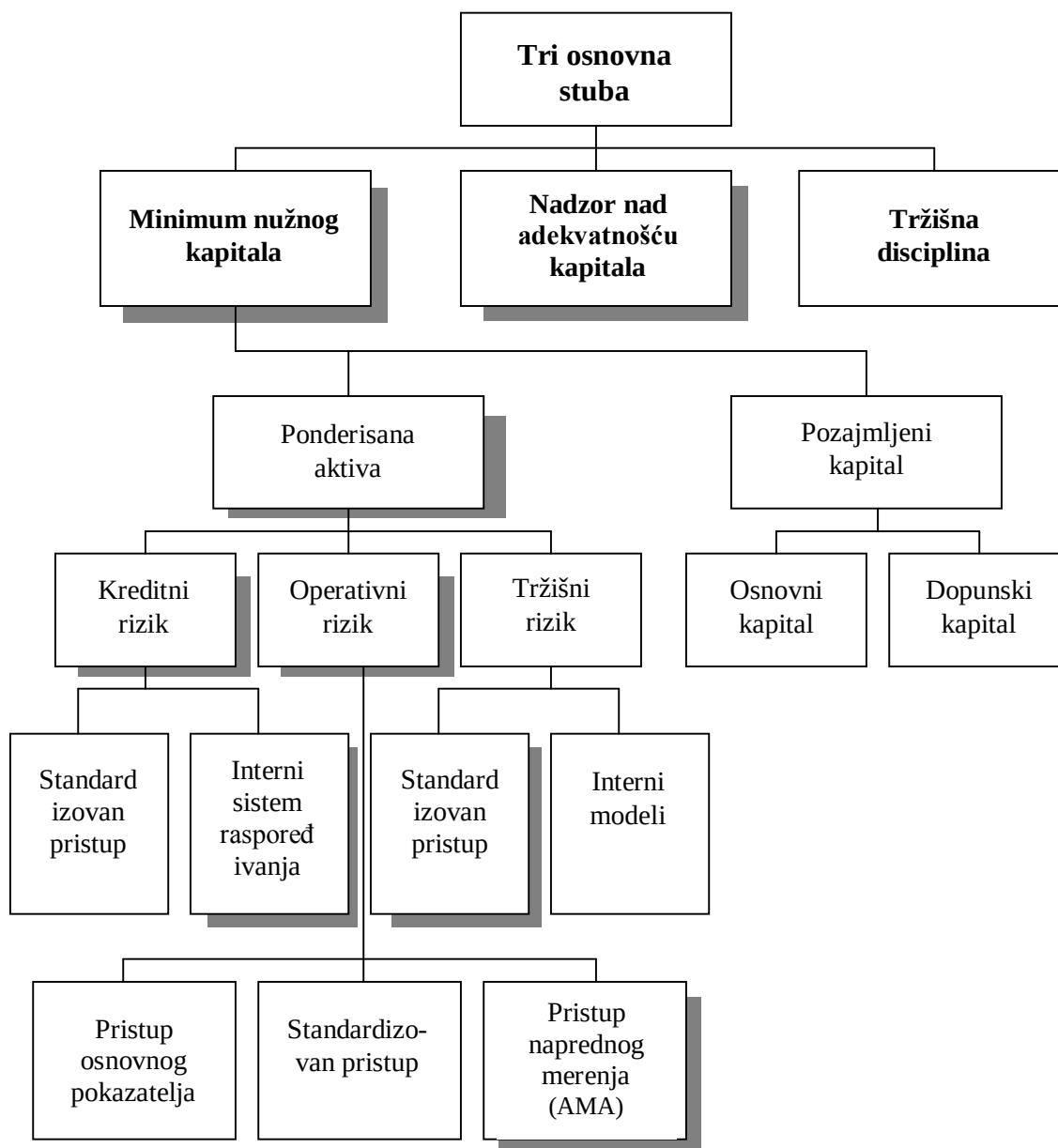
Kako su banke izložene i nizu drugih rizika, kapitalni zahtevi koji proizilaze iz Stuba 1 nisu dovoljni za pokriće ostalih rizika. Upravo zbog toga je Stubom 2 definisano da banka treba da vodi računa o izloženosti ostalim rizicima i u skladu s tim da osigura adekvatne minimume nužnog kapitala. Uloga super-vizora je ovde posebno naglašena, pa im zakonodavnim okvirom treba odobriti diskreciona prava pri odlučivanju o pojedinim bankama. Prema tome, Stubovi 1 i 2 su komplementarni i samo zajedno dovode do nivoa kapitala koji je optimalan za pokriće svih rizika neke banke.

Stub 3 takođe služi kao podrška Stubu 1. Naime, primena najnaprednijih pristupa merenju kreditnog i operativnog rizika nosi obavezu objavljivanja dodatnih informacija.

Veća transparentnost poslovanja banaka trebala bi da doprinese većoj otpornosti finansijskog sistema na šokove, pa time i pozitivno utiče na njegovu stabilnost, što je

svakako i jedan od ciljeva Bazela II. Bazelski odbor smatra da tržište može biti snažan saveznik formalnoj superviziji i regulatoru. U nekim slučajevima tržišna disciplina može bankama postaviti veća ograničenja od samih regulatora. Ona treba da deluje kao korektivni činilac i da daje dodatni motiv bankama za zdrav način poslovanja i kvalitetno upravljanje rizicima, što je suština Stuba 2. Ipak, transparentnost čini samo deo posla i za potpuni učinak mora se kombinovati sa drugim delovima regulatorne politike (sa ostalim stubovima).

Slika 2. Struktura Bazela II



1.2.2.1. Stub I – minimum nužnog kapitala

Iako su mnogi elementi Bazela I izmenjeni, treba napomenuti da je kategorija pozajmljenog kapitala ostala ista u odnosu na postojeći standard. Podsećamo da se stopa adekvatnosti kapitala izračunava kao odnos pozajmljenog kapitala banke i visine rizika kojima je banka izložena, odnosno ponderisane aktive. Stopa izračunata na taj način ne sme biti manja od 8% prema Bazelu I. U okviru Stuba 1 predložene su dve važne novine vezane za ponderisanu aktivu. Prva se odnosi na suštinske izmene proračuna kreditnog rizika, a druga na uvođenje eksplicitnih pravila za merenje operativnog rizika koji će biti uključen u ponderisanu aktivu. Kao što se iz prikaza strukture Bazela II vidi, u oba slučaja se uvode različite opcije za izračunavanje tih rizika. Razlog tome leži u nastojanjima Bazelskog odbora da standard učini što fleksibilnijim, čime bi trebala da se osigura i veća efikasnost jer svaka banka bira sebi najprimereniji pristup.

Kreditni rizik

Metode merenja kreditnog rizika, predviđene Bazelom II su sledeće:

1. Standardizovani pristup;
2. Interni sistem raspoređivanja – osnovni pristup (FIRB);
3. Interni sistem raspoređivanja – napredni pristup (AIRB).

Standardizovani pristup merenju kreditnog rizika. Veoma je sličan postojećem standardu po tome što banke svojim potraživanjima dodeljuju propisane pondere rizika zavisno od karakteristika potraživanja. Kategorije potraživanja definisane u standardizovanom pristupu obuhvataju potraživanja od državnih institucija, banaka, trgovačkih društava, stanovništva, te potraživanja osigurana zalogom nad nekretninama. Svako od ovih kategorija dodeljuje se propisani ponder rizika zavisno od spoljašnjeg kreditnog rejtinga, te se na taj način postiže veća osetljivost na rizike. Sledeća važna novina se odnosi na prošireno obuhvatanje kolaterala, garancija i kreditnih derivata kojima se banke mogu koristiti u okviru standardizovanog pristupa, te na taj način mogu da smanje minimum nužnog kapitala.

Interni sistem raspoređivanja – osnovni pristup i napredni pristup. Interni sistem raspoređivanja (*internal ratings – based approach*, IRB) jedna je od najinovativnijih karakteristika Bazela II. Takav pristup merenju kreditnog rizika uveden je sa namerom da podstakne banke na dalja ulaganja u interne sisteme upravljanja rizicima, a ujedno je i sam preuzet iz dosadašnje prakse velikih internacionalnih banaka. Takve sisteme banke razvijaju kako bi poboljšale svoje konkurentske pozicije i kao zaštitu od gubitaka. Banke, koje će primenjivati IRB pristup moći će da kvantifikuju ključne karakteristike dužnikove kreditne sposobnosti pri određivanju potrebne visine kapitalnog zahteva. Tu leži bitna razlika u odnosu na standardizovani pristup u kojem sve parametre različitosti za utvrđivanje minimuma nužnog kapitala zadaje regulator.

Prema pristupu internog sistema raspoređivanja banka razvrstava svoja potraživanja u sledeće grupe prema zajedničkim karakteristikama rizičnosti:

- trgovačka društva,
- državne institucije,
- banke,
- stanovništvo,
- vlasnički vrednosni papiri.

Unutar grupa trgovačkih društava i stanovnika potraživanja se dalje raspoređuju u nekoliko podgrupa.

Za svaku grupu potraživanja bitno je odrediti sledeća tri ključna elementa:

1. Komponente rizika,
2. Funkcije pondera rizika,
3. Minimalni zahtevi.

Za većinu grupa potraživanja, Bazelski odbor¹³ je omogućio primenu *osnovne* (FIRB) i *napredne* (AIRB) verzije internog sistema raspoređivanja. Te verzije se primarno razlikuju jedna od druge po tome određuje li komponente rizika banka vlastitim procenama ili ih određuje supervizor.

Ako uporedimo pondere rejting organizacija koje će banke morati da koriste u standardnom pristupu (nema mnogo promena u odnosu na Bazel I), sa sopstvenim ponderima koje će banke koristiti u internom sistemu raspoređivanja, jasno je zbog čega banke insistiraju na što složenijim pristupima. Naime, takvi pristupi, iako složeni i skupi za uvođenje, u velikoj meri smanjuju cenu investicija sa malim rizikom, dok investicije sa visokim rizikom neuporedivo poskupljuju. Ovo i jeste logično i ispravlja veliki nedostatak Bazela I, a to je jak podsticaj investiranju sa visokim rizikom, jer je za banku cena i visoko i niskorizičnih investicija bila ista.

Bazel II dopušta da se IRB banke pouzdaju u sopstvene procene ključnih parametara rizika samo ako su zadovoljeni strogi kvalitativni i kvantitativni zahtevi postavljeni u standardu. Naglasak se stavlja na sposobnost banke da rangira i kvantifikuje rizik na konzistentan i pouzdan način. Želi se osigurati da sistem procene rizika omogući primerenu procenu karakteristika dužnika i transakcije, primerenu diferencijaciju rizika, tačnu i konzistentnu kvalitativnu procenu rizika. Dalje, treba osigurati integritet kritičnih ulaznih podataka i uveriti se da su ti inputi proizašli iz sistema koji banka koristi u svakodnevnim poslovima, a ne da oni služe samo za procenu regulatornog kapitala, dok banka svoje poslovne odluke zasniva na nekim drugim podacima i pokazateljima. Banka mora imati jedinstven sistem i koristiti njegove rezultate i za potrebe regulatora i u procesu donošenja poslovnih odluka.

¹³ Basel Committee on Banking Supervision (1999b) *Update on Work on a New Capital Adequacy Framework*, Basel.

S obzirom na to da postoje razlike u tržištima, metodologija raspoređivanja, bankarskim proizvodima i praksama, banke i supervizori moraju operativne procedure prilagoditi svojim specifičnostima. Bazelski odbor nema nameru da diktira oblik ili tehničke detalje politike i prakse upravljanja rizicima neke banke. No, supervizor će biti u obavezi da razvije detaljne procedure kojima će osigurati adekvatnost sistema i kontrole tako da mogu da posluže kao dobra osnova za primenu IRB pristupa. Prema tome, primena IRB pristupa nije moguća bez prethodne saglasnosti supervizora.

Neki od najvažnijih zahteva odnose se na dizajn i strukturu sistema raspoređivanja, njegovo operativno funkcionisanje, raspoloživost i kvalitet podataka, nadzor nad sistemom i korporativno upravljanje.

Dizajn internog sistema raspoređivanja ključan je element njegove efikasnosti. On mora osigurati kvalitetnu distribuciju izloženosti banke po različitim stepenima rizika bez prevelikih koncentracija. Da bi ostvarila taj cilj, banka mora imati najmanje osam rizičnih grupa za raspoređivanje svojih dužnika. Minimalni standardi za ovo područje propisani u Bazelu II nadograđuju se na vodeću praksu upravljanja rizicima razvijenu u bankarstvu. Pri uspostavljanju sistema raspoređivanja bankama je izazov jasno i objektivno utvrđivanje kriterijuma za raspoređivanje dužnika u pojedinu rizičnu grupu i osiguravanje kvalitetne procene kreditnog rizika.

Važno je napomenuti da dobro dizajniran interni sistem raspoređivanja sam po sebi nije dovoljan – on mora biti integralni deo procesa upravljanja kreditnim rizikom. Od banaka se očekuje da IRB koriste ne samo pri donošenju odluke o odobravanju kredita već i pri određivanju cene proizvoda, rezervacija i pri internoj alokaciji ekonomskog kapitala. Što banka više koristi IRB, supervizor ima više poverenja u njegove rezultate za procenu potrebnih kapitalnih zahteva.

Nezaobilazno je pitanje kvaliteta i raspoloživosti podataka potrebnih za procene različitih komponenti rizika. Poznato je da je svaki sistem dobar onoliko koliko su dobri i kvalitetni njegovi ulazni podaci. Bankama je dopušteno da koriste podatke iz internih ili eksternih izvora pod uslovom da dokažu da su ti podaci relevantni za njihova potraživanja. Za određivanje parametara rizika potrebne su višegodišnje vremenske serije podataka i to je bankama zapravo jedna od najvećih prepreka za primenu IRB pristupa.

Uloga menadžmenta banke je od presudne važnosti i sve materijalno značajne aspekte procesa procene rizika i određivanja rejtinga moraju odobriti uprava i nadzorni odbor. Upravljačke strukture banke moraju biti vrlo dobro upoznate s celim procesom dodeljivanja rejtinga i pripadajućim sistemom izveštavanja. U tom smislu se pretpostavlja da će banke ulagati u izgradnju odgovarajućeg IT sistema koji će podržati celi proces procene rizika i generisati odgovarajuće izveštaje za potrebe menadžmenta i nadzornog odbora.

Operativni rizik

Operativni rizik je rizik od gubitka koji nastaje zbog neadekvatnosti, odnosno manjkavosti internih procesa, ljudskih resursa, sistema za podršku ili zbog spoljnih uticaja (Basel Committee 2004) ¹⁴. Komitet takođe ukazuje da ova definicija isključuje sistemski rizik, pravni rizik i rizik reputacije (negativnog publiciteta). U tekstu standarda ponuđene su tri metode za izračunavanje kapitalnih zahteva za operativni rizik, od vrlo jednostavnih do složenih internih modela:

1. Pristup osnovnog pokazatelja (*The Basic Indicator Approach*);
2. Standardizovani pristup (*The Standardised Approach*);
3. Pristup naprednog merenja (*Advanced Measurement Approach, AMA*).

Eksplicitno uvođenje minimuma nužnog kapitala za operativni rizik prvi put se pojavljuje s Bazelom II. Kako je poznavanje ovog rizika na dosta niskom nivou, još nije razvijena ni regulativa iz tog područja. Naime, značaj rizika nije bio dovoljno priznat sve dok se nisu pojavili slučajevi gde je upravo, neprepoznavanje i neadekvatno upravljanje operativnim rizikom banke, dovelo do velikih gubitaka. U poslednje vreme sve više preovladava mišljenje da je operativni rizik drugi po značaju u bankarskom poslovanju.

Ovaj deo standarda bilo je najteže definisati s obzirom na to da ne postoji dugogodišnja praksa banaka u upravljanju tim rizikom. Zbog toga je to područje regulisano vrlo fluidno, posebno pristup naprednog merenja. U tekstu standarda je navedeno da će Bazelski odbor pratiti razvoj novih pristupa merenju operativnog rizika u bankarstvu i nadalje kako bi se pronašli pristup i način merenja tog rizika koji bi proizveo verodostojne i konzistentne procene potencijalnih gubitaka. Nakon toga, postoji mogućnost da se revidira, bude li potrebno, taj deo standarda.

Zbog heterogene prirode operativnog rizika, neadekvatnih baza podataka i neodgovarajuće IT podrške teško je upravljati operativnim rizikom na jednoznačan način u svim poslovnim područjima banke, posebno ako se ne primenjuje AMA pristup ¹⁵. S obzirom na to da bi primena AMA pristupa trebalo da rezultuje adekvatnim kapitalnim zahtevima, banke bi trebalo stimulisati da unapređuju svoje sisteme upravljanja rizicima i što više primenjuju AMA pristup za one delove poslovanja koje model pokriva. Iz tog razloga proizilazi mogućnost da se dopusti delimična primena AMA pristupa za određeni segment poslovanja, dok se za ostale delove mogu primenjivati preostala dva modela navedena u standardu.

Pristup osnovnog pokazatelja. Ovo je najjednostavniji metod izračunavanja minimuma nužnog kapitala. Trogodišnji prosek neto operativnog prihoda banke množi se sa fiksnim alfa postotkom (15%). Kako je najjednostavnija metoda najčešće ujedno najmanje precizna, pristup osnovnog pokazatelja se ne preporučuje za velike internacionalne banke.

Standardizovani pristup. Minimumi nužnog kapitala se prema standardizovanom pristupu izračunavaju tako da se ukupne aktivnosti banke podele na osam poslovnih linija (korporativne finansije, trgovanje i prodaja, poslovanje sa stanovništvom,

¹⁴ Milivoje Cvetinović, "Upravljanje rizicima u finansijskom poslovanju", Univerzitet Singidunum, Beograd 2008, str.16

¹⁵ www.hnb.hr

komercijalno bankarstvo, plaćanje i naplata, agencijske usluge, upravljanje imovinom, maloprodajna brokerska delatnost), potom se neto operativni prihod svake poslovne linije množi sa beta faktorom propisanim za svaku poslovnu liniju. Ukupni minimum nužnog kapitala za banku izračunava se kao zbir pojedinačnih minimuma za osam poslovnih linija.

Banke moraju zadovoljiti minimalne kvalitativne zahteve koje je propisao Bazelski odbor, da bi mogle primenjivati standardizovani pristup za proračun minimuma nužnog kapitala:

1. Banka mora da formira organizacionu jedinicu koja će imati jasnu odgovornost za upravljanje operativnim rizikom;
2. Banka mora da osigura redovno praćenje podataka o operativnom riziku, uključujući značajne gubitke po pojedinoj poslovnoj liniji;
3. Viši izvršni menadžent banke, uprava i nadzorni odbor trebalo bi da dobijaju redovne izveštaje o izloženosti operativnom riziku;
4. Sistem upravljanja operativnim rizikom treba da bude dobro dokumentovan (interne politike, kontrole i procedure vezane uz sistem upravljanja operativnim rizikom);
5. Sistem upravljanja treba redovno podvrgavati nezavisnim proverama.

Pristup naprednog merenja – AMA. Pristupom naprednog merenja definiše se tako da se za proračun minimuma nužnog kapitala koriste bankarski interni sistemi za upravljanje operativnim rizikom pod uslovom da su zadovoljeni kvantitativni i kvalitativni zahtevi navedeni u standardu. Za korišćenje AMA pristupa banka mora da zatraži i dobije prethodnu saglasnost supervizora.

Kvalitativni zahtevi su gotovo identični onima koje banka mora zadovoljiti da bi primenjivala standardizovani pristup.

Kod kvantitativnih zahteva se ne navode specifični parametri modela niti se specificira neki određeni pristup za proračun minimalnih zahteva jer upravljanje tim rizikom kontinuirano evoluiralo, što se na ovaj način dodatno podstiče. Ipak, banka mora da dokaže da je svojim modelom obuhvatila potencijalno ozbiljne „debele“ krajeve distribucije koji obuhvataju mali broj gubitaka s katastrofalnim posledicama.

Kvantitativni zahtevi, dalje, regulišu obavezu redovnog prikupljanja internih podataka o gubicima i korišćenje eksternih podataka u određenim slučajevima; angažovanje stručnjaka koji će sprovoditi analizu. U obzir treba uzeti i ključne karakteristike okruženja i činilaca interne kontrole koji mogu izmeniti svoj profil operativnog rizika, te korišćenje tehnika za smanjivanje izloženosti operativnom riziku.

1.2.2.2. Stub II – Nadzor nad adekvatnošću kapitala

Stub 1 definiše minimum nužnog kapitala i predstavlja poseban pristup obavljanju supervizije. Primena uniformnih pravila koje on donosi i kojih se banke moraju pridržavati poboljšava transparentnost regulatornog procesa i bankama olakšava međusobno poređenje i stvaranje osećaja o relativnoj visini solventnosti. S druge strane, jednaka pravila nose sa sobom dosta nedostataka. Obično su vrlo kruta i stoga

onemogućavaju ili ignorišu inovativnost. Primena takvih pravila je, takođe, potpuno nedelotvorna za banke netipičnog rizičnog profila.

Stub 2 nudi rešenja za neke od tih problema. On uvodi supervizorsku procenu kao jedan od elemenata regulatorne politike. Supervizorima se dodeljuju diskreciona prava pri određivanju kapitalnih potreba banaka relevantnih za njihov poslovni i rizični profil. Upravo element diskrecije čini regulativni okvir fleksibilnim i otvorenim za različite promene i inovacije. Ipak, preveliko oslanjanje na sistem koji dopušta bezgraničnu diskreciju nije poželjan ni u kojem slučaju. Korišćenje diskrecionih prava u odsustvu ostala dva stuba dovodi do negativnih posledica na ujednačenost uslova poslovanja, jer bi banke poslovale prema različitim kriterijumima. Stoga bi ugrozile zdravu konkurenciju i tržišnu utakmicu.

Bazelski odbor je identifikovao četiri ključna načela na kojima se zasniva *Stub 2*, i to:

1. Banke bi trebalo da imaju uspostavljene procedure merenja adekvatnosti kapitala u odnosu na rizike kojima su izložene kao i strategiju održavanja potrebnog nivoa kapitala;

2. Supervizori treba da ocene interne sisteme i strategije banaka u upravljanju kapitalom, kao i njihovu sposobnost da prate i osiguravaju poštovanje regulatornih kapitalnih pokazatelja. Supervizori bi trebalo da preduzmu korektivne mere ako nisu zadovoljni rezultatima takvih kontrola;

3. Supervizori očekuju od banaka da posluju iznad minimalnih propisanih kapitalnih pokazatelja, a trebalo bi da imaju i mogućnost davanja naloga bankama da održe nivo kapitala iznad propisanih minimalnih vrednosti;

4. Supervizori bi trebalo da deluju preventivno, da spreče negativne trendove u adekvatnosti kapitala pojedinih banaka, te da deluju brzo i efikasno na restrukturiranje banaka s poteškoćama u poslovanju.

Suština *Stuba 2* je dakle, da se osigura optimalna visina kapitala u skladu s različitim profilom svake pojedinačne banke. Supervizor očekuje od banke da prema svojoj metodologiji utvrdi minimum nužnog kapitala za sve rizike koji nisu obuhvaćeni pravilima iz *Stuba 1* (kreditni, operativni i tržišni rizici). Poznato je da je banka izložena i brojnim drugim rizicima osim onima striktno navedenim u *Stubu 1*. Možemo navesti neke od njih: kamatni rizik u bankarskom delu poslovanja, rizik likvidnosti, rizik koncentracije itd. Kako uprava banke vodi poslove banke, odgovorna je za njeno poslovanje i adekvatnost kapitala koja će obuhvatiti sve njene rizike.

Primena *Stuba 2* nosi ozbiljne implikacije i za banke i za supervizore. Banka mora da ima procedure za procenu adekvatnosti kapitala za sve svoje rizike i strategiju za održavanje potrebne visine kapitala. Supervizor, ipak, ima pravo i obavezu da preispita bankarsku procenu minimuma nužnog kapitala i po potrebi zahteva povećanje kapitala. Supervizor se ovde nalazi u zahtevnoj i izazovnoj situaciji jer mora raspolagati odgovarajućim brojem stručnjaka koji će obavljati nadzor. Naime, pravo banke na sopstvenu metodologiju otežava rad supervizora jer mu se povećava posao s obzirom na to da sam mora prethodno dobro da se upozna s određenim metodologijama da bi mogao da proceni njenu ispravnost.

1.2.2.3. Stub III – Tržišna disciplina

Svrha odredbi *Stuba 3* je pružanje potpore minimalnim kapitalnim zahtevima (*Stub 1*) i nadzoru nad adekvatnošću kapitala (*Stub 2*). Kada banke objave dovoljno informacija o svojim adekvatnostima, učesnicima na tržištu mogu da stvore snažne podsticaje za zdrav način poslovanja. Tržište može nagraditi banke koje upravljaju rizicima na odgovarajući način i kazniti one koje održavaju kapital na preniskom nivou u odnosu na rizični profil. Treba napomenuti da tržište može da bude vrlo neefikasno pa će preterano reagovati na neki mali događaj, dok, s druge strane, može potpuno ignorisati pojavu značajnih indikatora rizika. Uvažavajući ove činjenice, *Stub 3* je samo jedan od tri stuba celokupnog standarda, čiji je cilj međusobno dopunjavanje.

Bazelski odbor¹⁶ podupire tržišnu disciplinu tako što je razvio skup zahteva za objavljivanje podataka koji će učesnicima na tržištu omogućiti pristup ključnim delovima informacija o obuhvatu primene Bazela II, visini i strukturi kapitala, izloženosti riziku, procesu procene rizika i adekvatnosti kapitala institucije.

Kako banke već imaju određenih obaveza objavljivanja Međunarodnim računovodstvenim standardima koje su šire u obuhvatu od zahteva koji proizilaze iz *Stuba 3*, Bazelski odbor je uložio velike napore da ta dva zahteva uskladi. Podaci koji prelaze okvir računovodstvenih objavljivanja moraju se javnosti prikazati na neki drugi način, o čemu odlučuju same banke. Pritom one mogu koristiti internet i druge medije. Takođe, nema obaveze revizije podataka koji nisu obuhvaćeni računovodstvenim zahtevima za objavljivanje.

Iz *Stuba 3* za banke proizilazi jasna i nedvosmislena obaveza donošenja formalne politike objavljivanja koju mora odobriti nadzorni odbor banke. Politikom treba odrediti pristup banke pri odlučivanju o tome koji će se podaci i informacije objaviti.

Načelo materijalnosti¹⁷ primenjuje se pri odlučivanju o tome koji su podaci relevantni za objavljivanje. Informacija se smatra materijalnom ako njeno izostavljanje ili pogrešno iskazivanje može promeniti ili uticati na već donetu procenu ili odluku korisnika te informacije.

Informacije se, po pravilu, trebaju objavljivati u polugodišnjim intervalima, ali ima i određenih izuzetaka od tog pravila. U skladu sa tim, podaci koji se odnose na bančine ciljeve i politike upravljanja rizicima, izveštajni sistem i definicije mogu se objavljivati jednom godišnje. Sa druge strane, podaci koji se odnose na kapital banke i njegovu strukturu, te na stopu adekvatnosti kapitala, moraju se objavljivati tromesečno. Isto se odnosi i na podatke koji su podložni brzim promenama.

¹⁶ Basel Committee on Banking Supervision (1999b) *Update on Work on a New Capital Adequacy Framework*, Basel.

¹⁷ Geiger, H. and Piaz, J.-M. (2000) Identifikation und Bewertung operationeller Risiken, In *Handbuch Bank-Controlling* (ed., Schierenbeck, H.) Wiesbaden. (forthcoming) Greenbaum, S. I. and Thakor, A. V. (1995) *Contemporary Financial Intermediation*, Fort Worth.

DRUGI DEO

VRSTE RIZIKA U BANKARSTVU

2. VRSTE RIZIKA U BANKARSTVU

Rizik predstavlja svaku neizvesnu situaciju u poslovanju banaka, odnosno verovatnoću gubitka (smanjenja dobitka) nastalu kao rezultat dejstva neizvesnih događaja u poslovanju banaka¹⁸. U zavisnosti od sklonosti bankarskih menadžera prema riziku, svaka banka može prihvatiti više ili manje rizika, pozicionirajući se između dva ekstrema: apsolutne averzije prema riziku i apsolutnog prihvatanja rizika. Nivo prihvaćenog rizika mora biti srazmeran sposobnosti banke da apsorbuje eventualne gubitke i ostvari prihvatljivu stopu prinosa.

Rizici u poslovanju banaka su karakteristika svakog bankarskog posla, tako da ni neutralni bankarski poslovi nisu bez rizika, a osvajanjem novih instrumenata, novih tehnika i strategija, finansijskog inženjeringa, novih bankarskih proizvoda, a naročito finansijskih derivata, lista rizika se neprestano širi.

Kao disciplina, upravljanje rizikom (*risk management*) je novijeg datuma i razvilo se iz delatnosti osiguranja, jer se tradicionalnim procesima osiguranja nisu mogli efektivno i ekonomično rešavati problemi rizika u svim situacijama. Upravljanje rizikom se može definisati kao bančina funkcija osiguranja od rizika, odnosno pod upravljanjem rizikom se podrazumeva skup aktivnosti:

- 1) identifikaciju izloženosti riziku za sve kategorije sredstava uz procenu potencijalnih gubitaka;
- 2) procenu rizika koja obuhvata merenje i analizu gubitaka u prošlosti, kako bi se procenile varijable koje će uticati na budućnost;
- 3) kontrolu rizika, u smislu smanjenja ili eliminisanja rizika gubitka;
- 4) finansiranje rizika obezbeđenjem rezervi, uključujući i osiguranje;
- 5) razvoj administrativnih tehnika i korišćenje stručnih znanja.

Upravljanje rizikom u bankarstvu ima dva osnovna cilja. Prvi cilj je da se izbegne nesolventnost banke, a drugi cilj je da se maksimizira stopa prinosa na kapital uz korekciju za rizik.

Banka je dužna da identifikuje, meri i procenjuje rizike kojima je izložena u svom poslovanju i da upravlja tim rizicima u skladu sa Zakonom o bankama, drugim propisima i svojim aktima.

Rizici kojima je banka naročito izložena u svom poslovanju su:

- 1) Rizik likvidnosti,
- 2) Kamatni rizik,
- 3) Rizici izloženosti banke prema jednom licu ili grupi povezanih lica,
- 4) Rizici ulaganja banke u druga pravna lica i u osnovna sredstva,
- 5) Rizici koji se odnose na zemlju porekla lica prema kome je banka izložena (rizik zemlje),
- 6) Devizni rizik, i
- 7) Operativni rizik.

¹⁸Bruhn, M. (1996) Qualitätsmanagement für Dienstleistungen. Grundlagen, Konzepte, Methoden, Berlin, Heidelberg, New York. p.p. 121

2.1. RIZIK LIKVIDNOSTI

Likvidnost banke je njena sposobnost da izmiri sve tekuće obaveze u rokovima dospeća. Trajnija nelikvidnost vodi u nesolventnost i pokazatelj je nestabilnosti poslovanja banke. Likvidnost može da se posmatra kao stok ili tok. Ako se likvidnost posmatra kao stok, onda se za ocenu likvidnosti koriste bilansni podaci. Posmatra se obim aktive u bilansu koja lako može da se pretvori u gotovinu. Poredi se obim raspoloživih likvidnih sredstava sa potrebama za likvidnim sredstvima. Aktiva se klasifikuje prema stepenu likvidnosti i u slučaju nelikvidnosti, banka može da proda deo svoje aktive i povuče likvidna sredstva sa finansijskog tržišta ili od CB. Pretpostavka da banka ne dođe u nelikvidnost je kvalitet bankarske aktive. Ako se likvidnost banke posmatra kao tok, onda se posmatra ne samo aktiva i pretvaranje njenih delova u gotovinu, nego i sposobnost banke da, putem odgovarajućih finansijskih operacija, ostvari i priliv potrebnih likvidnih sredstava. Pozicija likvidnosti posmatra se dnevno, nedeljno, mesečno ili tromesečno i sagledava potreba obezbeđenja sredstava za slučaj nelikvidnosti, iz sredstava rezervi ili na finansijskom tržištu. Posmatranje likvidnosti kao toka proističe iz bankarske sposobnosti ročne transformacije kratkoročnih sredstava u dugoročne plasmane. Za procenu likvidnosti optimalna je komplementarna primena i jednog i drugog pristupa.

Procena likvidnosti zasniva se na prognoziranju rasta depozita i potrebi angažovanja dodatnih izvora likvidnosti. Potreba za dodatnim likvidnim sredstvima može da se javi ako banka odobri veći obim kredita od rasta depozita, ili ako odobri kredit saglasno rastu depozita, ali u međuvremenu CB poveća stopu obavezne rezerve. Dodatne izvore likvidnosti banka može da koristi ili zaduženjem kod CB ili kod drugih banaka. U zemljama razvijene tržišne privrede prevladavanje nelikvidnosti može da se premosti repo aranžmanima i emitovanjem vrednosnih papira, najčešće depozitnih sertifikata. Repo aranžmani su prodaja finansijske aktive sa obaveznom reotkupom u dogovorenom roku i po dogovorenoj ceni. Repo aranžmani su specijalni aranžmani za likvidnost koji se vrše tako što banka prodaje vrednosne papire sa aranžmanom reotkupa sa dnevnim dospećem. Plaćanja se mogu vršiti na dva načina:

1) zaduživanjem kupca koji ima račun kod banke, čime se smanjuje obim depozita banke ali uz oslobađanje dela obavezne rezerve u korist likvidnih resursa;

2) banka, koja je prodala HoV, dobije ček od kupca koji se uplaćuje od druge banke, gde se vode sredstva kupca, čime se prelivaju likvidni potencijali između banaka.

Rizik likvidnosti je rizik mogućnosti nastanka negativnih efekata na finansijski rezultat i kapital banke usled nesposobnosti banke da ispunjava svoje dospele obaveze.

Rizik likvidnosti je u grupi vodećih finansijskih rizika u bankarstvu. Javlja se sa promenom likvidne pozicije banke, u kojoj njena likvidna aktiva nije dovoljna za izmirenje njenih obaveza. Izvori rizika likvidnosti u bankarstvu najčešće su drugi finansijski rizici, čija realizacija uzrokuje poremećaje u novčanom toku:

- kreditni rizik, u smislu visoke koncentracije rizične aktive u kreditnom portfoliju banke, visokog iznosa dospelih neizmirenih potraživanja banke po kreditnim poslovima, ili

- tržišni rizici, u smislu pozicija za trgovanje koje su u nelikvidnoj aktivu, što umanjuje mogućnost njene likvidacije.

Poremećaje u novčanim tokovima banke mogu uzrokovati i drugi razlozi, kao što su:

- ročna i valutna neusaglašenost pozicija aktive i pasive u bilansu stanja banke,
- uvođenje novih usluga sa neadekvatnom procenom uticaja na likvidnost,
- nagli rast izloženosti banke rizicima po osnovu vanbilansnih pozicija,
- nagli rast aktive koji se oslanja na promenljivu depozitnu strukturu,
- trend pada poslovne dobiti u vremenskoj seriji.

Strategija upravljanja rizikom likvidnosti sastavni je deo strategije upravljanja drugim rizicima, ili ukupnom izloženošću rizicima banke, s obzirom na uzročno – posledičnu povezanost i sinhronizovano delovanje različitih rizika.

Kao i u slučaju drugih rizika, uspešno upravljanje rizikom likvidnosti pretpostavlja da u banci postoji:

- jasno definisan proces upravljanja rizikom likvidnosti (identifikacija, procena, merenje, monitoring izloženosti i kontrola celog procesa) kao i procedure,
- razvijen informacioni sistem koji predstavlja osnovu uspešnog upravljanja rizikom likvidnosti na dnevnoj osnovi i njegove kontrole,
- plan obezbeđenja sredstava za teško predvidive i vanredne situacije, na kratak i dugi rok, koji bi trebalo da uveri da banka može preventivno i efikasno da upravlja kako rutinskim, tako i neočekivanim promenama svoje likvidne pozicije.

Objektivno, obuhvatna mera rizika likvidnosti ne postoji, kao i mera standardizacije u pristupu. Razlozi su velika raznolikost banaka i specifičnosti njihovih bilansnih struktura. U tom smislu, banke obično koriste:

1. određene tehnike upravljanja aktivom i pasivom, u funkciji održavanja potrebnog, ili željenog nivoa likvidnosti,
2. modeliranje pristupa politici depozitnog potencijala u smislu izbegavanja prevelike koncentracije sredstava i obezbeđenja stabilne dinamike dospeća obaveza, kao preventivu velikim i iznenadnim odlivima sredstava,
3. projekciju *cash flow*-a ili novčanog toka na dnevnoj/mesečnoj osnovi u funkciji procene izloženosti riziku likvidnosti i operativnom upravljanju ovim rizikom,
4. scenario analizu, u slučajevima kada su oscilacije u likvidnoj poziciji teško predvidive. Osnovu modela čine brojna konstruisana scenarija kojima su obuhvaćena tržišna kretanja, moguća neizmirenja obaveza u određenom vremenskom periodu i projekcija *cash flow*-a na dnevnoj osnovi za svaki scenario.

Upravljanje rizikom likvidnosti, osim analize bančinih bilansnih i vanbilansnih pozicija u odnosu na buduće gotovinske tokove, pretpostavlja i obezbeđenje izvora sredstava za održavanje optimalnog nivoa likvidnosti. To znači da je neophodno da banka blagovremeno identifikuje tržišta sredstava, ispita njihovu prirodu i sigurnost. Obično je reč o međubankarskim tržištima, kao značajnom izvoru likvidnosti. Zbog toga je bitno, da se strategijom upravljanja rizikom likvidnosti predvide moguće teškoće i troškovi pozajmljivanja sredstava na ovim tržištima, za potrebe očuvanja likvidne pozicije banke.

U proceni likvidne pozicije banke, menadžment banke može da se opredeli da koristeći statičku stopu likvidnost utvrdi zonu likvidnosti na način da uključi efekat obavezne rezerve kao faktor imobilizacije sredstava, salda priliva i odliva kao faktora oslobođenja ili blokiranja novčanih sredstava. Mogućnost korišćenja kredita za likvidnost kod CB značajan je faktor za ocenu likvidne pozicije.

Svoju likvidnost banka treba da obezbedi, pre svega, putem formiranja odgovarajuće primarne i sekundarne likvidnosti i mora biti oprezna kod korišćenja kredita na tržištu kako bi se izbegli neželjeni rizici. Nelikvidnost banke može da se spreči ako se upravlja aktivom na način da se rizici poslovanja smanje na najmanju meru, odnosno njima pravilno upravlja.

Za upravljanje finansijskim rizicima potrebno je, pre svega, da se prepozna koja je vrsta finansijskih rizika u pitanju i koji je stepen izloženosti riziku, da se utvrde instrumenti i odredi taktika upravljanja rizicima da bi se oni izbegli i da bi se banka zaštitila od mogućnosti rizika. Ključni element za upravljanje rizicima je prepoznavanje rizika. S tim ciljem rukovodstvo banke utvrđuje koji su to događaji koji mogu da imaju negativan efekat na banku. Banka po pravilu treba da utvrdi postupke za praćenje rizika, koji obezbeđuju sistemsku analizu i ključne pokazatelje rizika, dokumentovanje rizika i sistem kontrole nad njima. Pored toga rukovodstvo banke treba da vrši stalnu analizu odgovarajućih informacija da bi procenilo mogućnost nastanka određenog nepovoljnog događaja, njegove posledice i mogućnost gubitka, odnosno način izbegavanja i zaštite od rizika. Da bi se rizik ograničio rukovodstvo banke treba da utvrdi nivo rizika koji je prihvatljiv, a zatim da minimizira mogućnost nastanka događaja koji bi mogao da izazove gubitak ili da minimizira iznos gubitka koji bi nastao ako se rizik ostvari ili pak da rizik prenese na treće lice.

Najvažniji rizici u poslovanju banke koji mogu da ugroze njenu likvidnost i solventnost su:

1. kreditni rizik,
2. kamatni rizik,
3. valutni rizik,
4. rizik portfolia.

Kreditni i kamatni rizici javljaju se kada dužnik nije u mogućnosti da o roku vrati glavnicu i pripadajuću kamatu. Valutni rizik nastaje sa promenom valutnih kurseva što utiče na dinarsku protivvrednost aktive i pasive. Rizik portfolia se javlja sa promenom ročne transformacije sredstava u banci što menja i odnose već odobrenih sredstava i ročne strukture pasive.

2.2. KAMATNI RIZIK

Kamatni rizik – predstavlja rizik od pada tržišne vrednosti portfelja usled neizvesnosti promena kamatnih stopa¹⁹. Kamatni rizik se sastoji u promeni kamatnih stopa na plasmane i obaveze, ukoliko su promene kamatnih stopa nepovoljne za banku. Drugim rečima, to je rizik od gubitka ili se manifestuje kao smanjenje profita usled promena kamatnih stopa. Važan je za banke jer menja visinu kamatne marže na više ili suprotno. Kamatni rizik delom proističe iz nepotpune sinhronizacije promena kamatnih stopa na aktivu i pasivu, a pošto banke vrše ročnu transformaciju sredstava, to pri fiksnim kamatnim stopama banke postaju osetljive na porast tržišnih kamatnih stopa. Kada se osamdesetih godina XX veka povećala kolebljivost kamatnih stopa, banke su počele da posvećuju više pažnje kamatnom riziku. Bazičnu meru kamatnog rizika predstavlja koeficijent između stavki aktive i pasive koje su osetljive na promenu kamatne stope.

Primer: Ako banka ima aktivu od 40 mil. evra i obaveze 50 mil. evra, onda porast kamatne stope od 1% dovodi do negativnih posledica jer se kamatni prihodi povećavaju za 400, a rashodi – za 500 hiljada evra. Ako kamatna stopa aktive poraste 1,2%, a na pasivu 1%, onda je efekat promene kamatne stope na neto kamatnu maržu – 20 hiljada evra.

Marža neto kamate banke ili druge finansijske institucije je pod uticajem nekoliko faktora²⁰ :

1. Promena u nivou kamatnih stopa, naviše ili naniže;
2. Promena u odnosu između prihoda od aktive i troškova od pasive (što se često vidi na promenljivom obliku *krive prinosa* između dugoročnih i kratkoročnih stopa zato što je veliki deo aktive kratkoročan, dok je znatan deo aktive finansijske kompanije dugoročan);
3. Promena u obimu aktive koja vuče kamatu (prihodi) usled povećanja ili smanjenja ukupnog obima poslovanja finansijske institucije;
4. Promena u obimu pasive koja vuče kamatu a koja se koristi za finansiranje prihovne aktive usled povećanja ili smanjenja obima poslovanja finansijske institucije;
5. Promena u sastavu aktive i pasive koju rukovodstvo koristi kada dolazi do nesklada između aktive i pasive sa fluktuirajućom kamatnom stopom, aktive i pasive sa fiksnom kamatnom stopom, aktive i pasive sa kraćim i dužim dospećem, i kod aktive koja ostvaruje veće prihode i aktive koja ostvaruje manje prihode (npr. pomeranje sa manje količine gotovine ka većim količinama zajmova, ili sa potrošačkih zajmova i zajmova za nekretnine koji ostvaruju veće prihode ka komercijalnim zajmovima koji ostavruju manje prihode).

U neku ruku, kroz premije za rizike preko bazne referentne interesne stope, kamatni rizik reflektuje integralni koncept upravljanja rizikom. Napori u upravljanju rizikom kamatne stope primoravaju banke da:

- uspostave jasan finansijski cilj za neto kamatni prihod,
- mere svoju izloženost kamatnom riziku,
- formulišu strategije da dodju do željenog cilja.

¹⁹ Milivoje Cvetinović, op.cit.str. 11

²⁰ Saunders, A. (1999) Financial Institutions Management. A Modern Perspective, Boston et al. Shadow Financial Regulatory Committees of Europe Japan and the U.S. (1999) Improving the Basle Committee's New Capital Adequacy Framework, New York.

Većina banaka koristi:

- Funding Gap modele,
- Duration modele,
- Simulacione modele,
- VaR.

Ove modele banke koriste u kombinacijama a oni se razlikuju u:

- Cilju,
- Oceni rizika, i
- Strateškim preporukama.

Na kamate utiču:

- I. Platni bilans i cifre unutar njega,
- II.Devizni kurs,
- III.Kamatne stope u drugim zemljama,
- IV.Nivo trošenja vlade,
- V.Stopa inflacije,
- VI. Ponuda i cena novca od strane centralne banke,
- VII. Ekonomska politika vlade,
- VIII. Ekonomski ciklusi.

Zavisno od *cash flow* karakteristika bančinih pozicija u aktivni i pasivi promene kamatne stope, mogu povećati ili sniziti neto kamatni prihod i tržišnu vrednost potraživanja i obaveza (tržišnu vrednost kapitala tj. akcija).

1. RIZIK REINVESTIRANJA

Pod ovom vrstom rizika podrazumevaju se:

- Rizik da banka neće moći reinvestirati gotovinske tokove koje proizvodi njena aktiva odnosno refinansirati preuzete obaveze ili preuzeti nove obaveze po izvesnoj kamatnoj stopi u budućnosti,
- troškovi uzajmljenih sredstava se stavljaju u odnos prema prihodu na plasiranim sredstvima.

2. RIZIK CENE

Pod ovom vrstom rizika podrazumevaju se:

- Promene u kamatnim stopama prouzrokuju i promene u vrednosti potraživanja i obaveza (pozicija aktive i pasive),
- Duže dospeće (duracija) FA znači veću promenu u vrednosti za datu promenu kamatne stope,
- Pozitivan duracioni gep (znači udar na tržišnu vrednost kapitala):
 - Ako se očekuje porast kamatnih stopa na tržištu: produžiti ročnost izvora i maksimalno skratiti ročnost plasmana;
 - Takođe u slučaju skoka krive prinosa, nasuprot interesima klijenata, banke se trude da smanje kamatno osetljivu pasivu, uvećaju kamatno osetljivu aktivu i maksimalno skrate rokove otplate/povraćaja svojih plasmana.

Analiza jaza :

Minimiziranje kamatnog rizika (usled teškoća u predviđanju budućeg kretanja kamatne stope najlakše se postiže bilansnim prestrukturiranjem stavki aktive i pasive osetljivim na kamatnu stopu, tako da koeficijent osetljivosti na kamatnu stopu teži ka 1. To često nije moguće, pa se pribegava analizi jaza (*gap analysis*). Jaz (*gap*) – razlika između aktive i pasive osetljivih na kamatnu stopu pri unapred definisanom intervalu ročnosti. Prvi korak u analizi jaza: podela bankarskih bilansa u više “repricing” intervala (npr. do 1 mesec, 1-3, 3-6, 6-12 meseci, 1-2 godine itd.). Banka sa više kamatno osetljive aktive od pasive ima +jaz.

- $Gap\ ratio = \frac{\text{Kamatno osetljiva aktiva}}{\text{Kamatno osetljiva pasiva}}$
- Ukoliko je $Gap\ ratio > 1$, prvi izvod kamatne marže po vremenu će biti pozitivan i vice versa,
- $Gap = ISA - ISL$
- $Income\ effect = Gap \times di$

Kada je u pitanju rizik kamatnih stopa, jedan od važnih ciljeva je zaštita *profita* – neto prihod posle oporezivanja svih ostalih troškova – od uticaja fluktuirajućih kamatnih stopa. Bez obzira na pravac kretanja kamatnih stopa, menadžeri finansijskih institucija uvek teže ka tome da profit bude ostvaren na očekivanom i stabilnom nivou.

Da bi se postigao taj cilj, rukovodstvo mora da ima u vidu one elemente portfelja aktive i pasive institucije, koji su najosetljiviji na kretanja kamatnih stopa. Obično se pod ovim podrazumevaju zajmovi i investicije na strani aktive bilansa stanja – prihodovna sredstva – i depoziti koji vuku kamatu kao i zaduživanja na tržištu novca, na strani pasive. Da bi se zaštitio profit od negativnog promena u kamatnim stopama, rukovodstvo zahteva da pokriće neto kamate (*net interest margin* NIM) finansijske institucije ostane fiksno, što se izražava na sledeći način:

$$NIM = \frac{\text{Neto prihod od kamate posle troškova}}{\text{Ukupna prihodovna aktiva}}$$

Prednosti i nedostaci analize jaza:

- Jednostavna za primenu,
- Ne zahteva poznavanje matematike,
- Uklapa se u zahteve regulatornih tela,
- Vezana za računovodstvene sisteme,
- Prihvatljiv je indikator, naročito kod banaka sa jednostavnim bilansom stanja,
- Statistička mera koja ignoriše vremensku neusklađenost unutar svake grupe ročnosti,
- Ne uzima u obzir očekivane promene u strukturi bil.stanja i ignoriše se rizik da će se cena terminskog ugovora promeniti u odnosu na fin.ins
- Statičan,
- Da bi se koristile prednosti analize jaza, najbolje je kombinovati je sa analizom trajanja i simulacionom anal.

Analiza trajanja (duration analysis):

Potencira **tržišnu vrednost** (za razliku od analize jaza, koja potencira knjigovodstvenu vrednost) stavki aktive i pasive iz bilansa banke. Dozvoljava razlike između prosečnog veka (duration) stavki aktive i pasive i njihovog dospeća. Trajanje kredita (mesečna otplata) je različito od roka dospeća, pa se tako stvara vremenski jaz i izloženost kamatnom riziku. Prvi put primenjena je kod obveznica.

Prednosti i nedostaci analize trajanja:

- Kvantifikuje uticaj promena kamatne stope na kamatni prihod banke,
- Uzima u obzir **sve** tokove gotovine,
- Vreme trajanja je jedinstvena mera,
- Dugoročna perspektiva u fokusu,
- Kompleksnost koncepta i teškoće da ga analitičari shvate, a zahteva i veliki utrošak vremena,
- Prilikom interpretacije dobijenih rezultata treba biti oprezan zbog manjkavosti koje počivaju na linearnoj vezi između kamat. stopa i vrednosti aktive (koja je konvek-sna), tako da je dobra za male promene kamatne stope,
- Polazi od pretpostavke da se kriva prinosa paralelno pomera kada nastane promena kamatnih stopa,
- Potrebna moćna baza podataka koja uključuje: tokove gotovine, prinos za svaku stavku i bilo koji odabrani rok itd.

Simulaciona analiza :

Ispituju se različiti scenariji (sa različitom promenom kamatne stope). Obavezno se uključuje i najgori scenario po banku, a očekivani prinos je **verovatnoća** ponderisanog proseka za različite scenarije, za razlike od ALM modela gde se ne pokrivaju svi mogući scenariji. Na osnovu ALM modela se definiše (samo po likvidaciji i kamatnom riziku) najgori scenario za postojeći portfelj po kamatnoj stopi, a onda se modeliraju čitava lepeza kreditnih i tržišnih rizika. Drugi razlog zašto se ALM modeliranje ne oslanja isključivo na postojeći portfolio, već koristi i projektovani je vremenska dimenzija (srednji i dugi rok), pa se simulacije proširuju na projekcije tako što se dodaju nove stavke aktive i pasive kao rezultat različitih scenarija poslovne aktivnosti banke, čime se uključuje i operativni rizik.

Prednosti i nedostaci simulacione metode:

- Dinamički koncept čije rezultate analize je lakše interpretirati,
- Preciznije je obuhvaćena vremenska dinamika tokova gotovine pošto se svaka stavka tretira zasebno,
- Njenom primenom se smanjuje uloga upravljanja u slučaju krize.

2.3. RIZICI IZLOŽENOSTI BANKE PREMA JEDNOM LICU ILI GRUPI POVEZANIH LICA

Rizici izloženosti banke obuhvataju rizike izloženosti banke prema jednom licu ili prema grupi povezanih lica, kao i rizike izloženosti banke prema licu povezanom s bankom²¹.

Ukupna izloženost banke prema jednom licu ili prema grupi povezanih lica predstavlja zbir svih bilansnih potraživanja i vanbilansnih stavki koji se odnose na to lice ili grupu povezanih lica, osim:

- sredstava po viđenju i sredstava oročenih do sedam dana na računima kod banaka;
- potraživanja od Narodne Banke Srbije ili Republike Srbije i potraživanja obezbeđenih njihovim безусловnim garancijama plativim na prvi poziv;
- potraživanja od vlada i centralnih banaka zemalja članica Organizacije za ekonomsku saradnju i razvoj i potraživanja obezbeđenih njihovim безусловnim garancijama plativim na prvi poziv;
- potraživanja obezbeđenih hartijama od vrednosti Narodne Banke Srbije ili Republike Srbije;
- pokrivenih akreditiva za koje je pokriće obezbeđeno na posebnom računu kratkoročnih depozita na ime pokrića po akreditivima – do visine pokrivenosti;
- potraživanja obezbeđenih gotovinskih gotovinskim depozitom kod banke, u visini depozita, pod uslovom da je ugovoreno da depozit služi kao obezbeđenje za ta potraživanja, da rok dospeća depozita odgovara roku dospeća potraživanja i da jedino banka može raspolagati tim depozitom – u visini dospelog nenaplaćenog potraživanja;
- potraživanja obezbeđenih безусловnim garancijama plativim na prvi poziv banaka

Velika izloženost banaka prema jednom licu ili prema grupi povezanih lica je izloženost koja iznosi najmanje 10% kapitala banke. Zbir svih velikih izloženosti banke uključuje i izloženost banke prema licima povezanim sa bankom. Izloženost banke prema jednom licu ili prema grupi povezanih lica ne sme preći 25% kapitala banke. Izloženost banke prema jednom licu povezanom s bankom ne sme preći 5% kapitala banke.

²¹ www.nbs.rs

2.4. RIZICI ULAGANJA BANKE U DRUGA PRAVNA LICA I U OSNOVNA SREDSTVA

Rizici ulaganja banke obuhvataju rizike njenih ulaganja u lica koja nisu lica u finansijskom sektoru i u osnovna sredstva²².

Ulaganje banke u jedno lice, koje nije lice u finansijskom sektoru ne sme preći 10% kapitala banke.

Pod ulaganjem banke podrazumeva se ulaganje kojim banka stiče udeo ili akcije lica, koje nije lice u finansijskom sektoru.

Ukupna ulaganja banke u lica koja nisu lica u finansijskom sektoru i u osnovna sredstva banke ne smeju preći 60% kapitala banke.

Ulaganjima nije obuhvaćeno sticanje akcija radi njihove dalje prodaje u roku od šest meseci od dana sticanja tih akcija.

2.5. RIZIK ZEMLJE

Rizik zemlje predstavlja mogućnost da dužnik ne može izmiriti svoju obavezu prema inostranom kreditoru zbog političkih, socijalnih, pravnih i ekonomskih poremećaja koji se dešavaju u njegovoj zemlji²³.

Izražava se verovatnoćom da zemlja dužnik ili dužnik iz neke zemlje ne može ili nije voljan da izmiri svoje obaveze zbog postojanja razloga koji nisu uključeni u okviru uobičajenog kreditnog rizika.

Osnovni oblici ispoljavanja rizika zemlje su:

- rizik neplaćanja - obuhvata slučajeve u kojima zbog političkih i ekonomskih razloga dužnik nije u mogućnosti da uredno izvršava svoje obaveze (domaća finansijska organizacija nije u mogućnosti da naplati svoja potraživanja od dužnika iz neke zemlje), što znači da dužnik nije solventan;

- rizik transfera - predstavlja verovatnoću da solventan dužnik iz neke zemlje nije u mogućnosti da dug otplati u ugovorenoj valuti usled određenih poremećaja u njegovoj zemlji;

- rizik garancija - rizik koji je karakterističan za finansijske organizacije koje izdaju garancije dužnicima iz inostranstva za plaćanje u trećoj zemlji. Gubitak nastao usled aktiviranja garancije za dužnika iz zemlje iz koje dugovi ne mogu biti normalno servisirani za finansijsku organizaciju isti je kao nenaplativo potraživanje.

Pod rizicima koji se odnose na zemlju porekla lica prema kome je banka izložena (rizik zemlje) podrazumevaju se mogući negativni efekti na finansijski rezultat i kapital banke zbog nemogućnosti banke da naplati potraživanja od ovog lica iz razloga koji su posledica političkih, ekonomskih ili socijalnih prilika u zemlji porekla tog lica²⁴. Ova vrsta rizika obuhvata političko-ekonomski rizik i rizik transfera.

²² www.nbs.rs

²³ Parsley, M. (1996), Risk Management's Final Frontier, Euromoney, September, 74 - 79.

²⁴ www.nbs.rs

Rizik da zemlja neće otplatiti kredit banci koja joj je dala ili za koji ona garantuje, za banke je to poseban rizik jer ne može da koristi metode naplate duga kao kod pravnih i fizičkih lica, jer nema uobičajenih instrumenata obezbeđenja poput zaloge. Koristi se izraz “politički rizik”, o obuhvata deviznu kontrolu, regulisanje kamatnih stopa, nacionalizaciju. Postoji i ratni rizik, koji se ređe događa, ali može biti fatalan po banku. Zato se ovi rizici (uz transportni) osiguravaju.

Pod rizicima koji se odnose na zemlju porekla lica prema kome je banka izložena (rizik zemlje) podrazumevaju se negativni efekti koji bi mogli nastati na finansijski rezultat i kapital banke zbog nemogućnosti da naplati potraživanja od ovog lica iz razloga koji su posledica političkih, ekonomskih ili socijalnih prilika u zemlji porekla tog lica.

Rizik zemlje obuhvata²⁵:

- političko – ekonomski rizik, pod kojim se podrazumeva verovatnoća ostvarivanja gubitka zbog nemogućnosti naplate potraživanja banke zbog ograničenja utvrđenih aktima državnih i drugih organa zemlje porekla dužnika, kao i opštih i sistemskih prilika u toj zemlji,

- rizik transfera, pod kojim se podrazumeva verovatnoća ostvarivanja gubitka zbog nemogućnosti naplate potraživanja iskazanih u valuti koja nije zvanična valuta zemlje porekla dužnika, i to zbog ograničenja plaćanja obaveza prema poveriocima iz drugih zemalja u određenoj valuti, utvrđenih aktima državnih i drugih organa zemlje dužnika.

Banka mora uspostaviti adekvatan sistem za upravljanje rizikom zemlje, koji obuhvata politike i procedure kojima se uređuje:

- identifikacija postojećeg rizika zemlje;
- merenje rizika zemlje utvrđivanjem procedura i metoda za tačnu i blagovremenu procenu tof rizika;
- praćenje rizika zemlje analiziranjem stanja u toj zemlji;
- kontrolisanje rizika zemlje njegovim održavanjem na nivou prihvatljivom za rizični profil banke;
- utvrđivanje ovlašćenja i odgovornosti u procesu preuzimanja i upravljanja rizikom zemlje;
- sistem za redovno informisanje nadležnih organa banke o upravljanju rizikom zemlje.

Banka limite izloženosti riziku zemlje utvrđuje pojedinačno po zemljama porekla dužnika, po koncentraciji izloženosti ovom riziku na regionalnoj osnovi, a po potrebi, utvrđuje ih i prema pojedinim geografskim regionima.

²⁵ Luhmann, N. (1991) *Soziologie des Risikos*, Berlin, New York, pp. 323

2.6. DEVIZNI RIZIK

Devizni rizik (engl. foreign exchange risk, nem. Devisenrisiko) postoji uvek kada preduzeće/banka obavlja poslovne transakcije u valuti različitoj od vlastite²⁶. Uzrok postojanja deviznog rizika jesu fluktuirajući devizni kursevi glavnih svetskih valuta. Od 1973. godine kada je prestao važiti Sporazum iz Bretton Woods-a, tj. kada su ukinuti fiksni devizni kursevi vezani uz zlatni standard (za vreme važenja Sporazuma iz Bretton Woods-a devizni kursevi za većinu valuta industrijaliziranih zemalja bili su relativno stabilni, a fluktuacije su bile povremene i slabog intenziteta, pa su poslovne transakcije u stranim valutama bile prilično sigurne u pogledu deviznog rizika), uvedeni sistem fluktuirajućih deviznih kurseva proizvodi pojačanu nepostojanost u cenama valuta. Ovisno o određenom razdoblju, preduzeće može biti u opasnosti od gubitka znatnih svota novca zbog izloženosti fluktuaciji valuta. Naročito u slučaju dugoročnih transakcija (dve-tri godine) fluktuacije deviznih kurseva mogu imati ekstremne efekte i hitno izmeniti očekivanu profitabilnost poslovne transakcije. Preduzeće je izloženo deviznom riziku: a) kada poseduje novčana sredstva u jednoj valuti i očekuje da izvrši konverziju u drugu valutu kako bi realizirao profit; b) kada su mu potraživanja denominirana u jednoj valuti koja mora biti konkretizirana u drugu po nekoj očekivanoj vrednosti; c) kada poseduje novčana sredstva u nekoj valuti, te u trenutku vraćanja mora vršiti konverziju vlastite u stranu valutu kako bi se vratilo dug (devizni rizik to je prisutniji što je vreme kreditiranja duže; d) kada kupuje robu u jednoj valuti, prodaje u drugoj, a ostvareni prihod treba konvertirati u treću kako bi ostvarilo planirani profit.

Rizik deviznih kurseva predstavlja potencijalne promene u prihodima, imovini i konkurentskoj poziciji finansijske organizacije koje su izazvane promenama deviznih kurseva. Promene deviznih kurseva izazivaju promene u prihodu finansijske organizacije kod koje postoji neadekvatna usklađenost potraživanja i obaveza izraženih u nekoj stranoj valuti.

Gubitak za finansijsku organizaciju, odnosno tzv. negativne kursne razlike, biće ostvaren kada je otvorena pozicija pozitivna, a dođe do pada vrednosti strane valute u odnosu na domaću, kao i ukoliko u situaciji negativne otvorene valutne pozicije vrednost strane valute izražene u domaćoj poraste.

Osnovne determinante koje utiču na nivo rizika deviznih kurseva možemo podeliti na tri osnovne grupe:

- ekonomska,
- transakciona i
- bilansna (konverzionna).

Ekonomska izloženost riziku deviznih kurseva obuhvata efekte promene deviznih kurseva na spoljnotrgovinsko poslovanje (izvozne i uvozne cene). Ekonomski uzroci rizika deviznih kurseva, vezani za realne a ne za nominalne promene deviznih kurseva, nastaju pre ekonomske transakcije.

Transakciona izloženost riziku deviznih kurseva javlja se u situaciji kada ne postoji vremenska podudarnost između ostvarivanja potraživanja u određenoj valuti i njegove naplate, kao i između preuzimanja obaveze i njenog plaćanja.

²⁶ Parsley, M. (1996), Risk Management's Final Frontier, Euromoney, September, pp. 74 - 79.

Bilansna izloženost riziku deviznih kurseva obuhvata uticaj promene kurseva na aktivu i pasivu bilansa stanja i prihode i rashode bilansa uspeha finansijske organizacije.

Upravljanje (defanzivno) se svodi na:

1. Ograničavanje devizne izloženosti (za međunarodno aktivnu banku praktično neizvodljivo),
2. Limitiranje neto otvorenih pozicija,
3. Indeksacija ili stipuliranje devizne klauzule na strani plasmana,
4. Hedging valutnim derivatima.

Aktivističko upravljanje deviznim rizikom podrazumeva:

1. Korigovanje neto otvorenih pozicija u svakom segmentu deviznog podbilansa u dosluhu sa anticipiranim promenama kursa,
2. Špekulacija na deviznim tržištima u skladu sa jednačinom (ne)pokrivene kamatne arbitraže,
3. Eksploatacija trenutne precenjenosti/podcenjenosti pojedinih valuta na različitim segmentima svetskog deviznog tržišta.

Rizik da će banka da zabeleži gubitak usled promene deviznog kursa, kada postoji “otvorena devizna pozicija”²⁷. Naročito značajan za banke koje posluju internacionalno. Posebna vrsta tržišnog rizika usled fluktuacije cena valuta. Znatno je porastao usled globalizacije, kada transakcije rastu ne samo po robnoj, već i po finansijskoj osnovi (najveći deo deviznih transakcija ostvaruje se po međunarodnim tokovima kapitala). Osim za banke, značajan je i za bančine klijente. Hedžing (tehnike zaštite) i spekulacije (namerno ulaženje u otvorene pozicije sa ciljem zarade).

Operativno upravljanje deviznim rizikom na nivou banke može da se sprovedi na nekoliko načina:

- Da se odredi visina valutnog rizika koji banka prihvata. Razlikuju se diling (dealing) pozicija (nastala na osnovu tekućeg deviznog priliva/odliva) i “strukturalna” pozicija (dugoročnijeg karaktera i rezultat menadžmenta banke),

- Terminske transakcije kao oblik hedžinga.

Razlike između spot i terminskog kursa uglavnom oslikava procene tržišta u razlici buduće stope inflacije u 2 zemlje:

- Zaštita od deviznog rizika putem derivata (fjučersi i opcije)
- Banka namerno može ići u rizik (špekulacija), gde mogu ostvariti velike prihode, ali i pretrpeti gubitke.

²⁷ Saunders, A. (1999) Financial Institutions Management. A Modern Perspective, Boston et al. Shadow Financial Regulatory Committees of Europe Japan and the U.S. (1999) Improving the Basle Committee's New Capital Adequacy Framework, New York.

Shimpi, P. A. (ed.) (1999) Integrating Corporate Risk Management, Zurich.

2.7. OPERATIVNI RIZIK

Operativni rizik odnosi se na mogućnost nastanka negativnih efekata na finansijski rezultat i kapital banke koji su posledica propusta u radu zaposlenih, neodgovarajućih internih procedura i procesa, neadekvatnog upravljanja informacionim i drugim sistemima, kao i usled nepredvidivih eksternih događaja²⁸.

- Rizik od gubitka (direktnog ili indirektnog) nastalog usled neadekvatnih internih bankarskih procesa/ljudi/sistema ili usled eksternih događaja.
- Cilj nije eliminisanje Operativnog rizika, već zadržavanje na "prihvatljivom" nivou.
- Rizik da će nastati slučaj koji izaziva gubitak kod banaka je: Ljudski faktor, tehnički faktor procesne radnje, informacione tehnologije, nedovoljno iskustvo, nedisciplinisanost kod poštovanja ustanovljenih procedura i politika (i etika).

Operativni rizici su u grupi nefinansijskih rizika, koji nastaju iz poslovnog procesa, zbog grešaka koje čini čovek u tom procesu, sistemskih propusta, neadekvatnih procedura, nedovoljno obuhvatne i konzistentne kontrolne funkcije ali i eksternih faktora. Ovako širok spektar ovih rizika, čini mogućom i različite kvalifikacije.

Opšta klasifikacija, široko prihvaćena, poznaje sledeće kategorije operativnih rizika:

- rizike neadekvatne ili nedovoljne infrastrukture (zastarele mere i kapaciteti, nejasno definisan sistem odgovornosti, nedostatak praktičnog iskustva zaposlenih i ostalo),
- tehnološke rizike (u savremenom bankarstvu, to su pre svih rizici informacione podrške),
- rizike operacija ili poslovnog procesa (neadekvatne ili zastarele procedure, kritični delovi procesa zbog tehničko – tehnoloških problema i drugo),
- rizike ljudskog faktora (nedovoljna kultura ponašanja u odnosu na izloženost operativnim rizicima, nedovoljan broj zaposlenih, rizik upravljanja, interne kriminalne aktivnosti i drugo) i
- rizike eksternih događaja (eksterne kriminalne radnje, prirodne katastrofe i drugo).

²⁸ Levine, M. and Hoffmann, D. G. (2000) Enriching the Universe of Operational Risk Data: Getting Started on Risk Profiling, Operational Risk, pp. 25 - 39.

TREĆI DEO

OPERATIVNI RIZIK

3. OPERATIVNI RIZIK

Operativni rizik je rizik gubitaka koji nastaju zbog neadekvatnih procedura i neuspelih internih procesa, ljudskog faktora, sistemskih ili eksternih događaja. Ova definicija operativnih rizika ugrađena je u Novi okvir kapitalne adekvatnosti – Bazel II i rezultat je duže debate vođene između regulatora i industrije iz više različitih jurisdikcija na temu obuhvatnosti pojma operativnih rizika²⁹. Osim toga, Bazelski komitet eksplicitno naglašava da definicija operativnih rizika data u ovom dokumentu obuhvata zakonski rizik, ali isključuje strateški i reputacijski rizik.

Iako je bila predmet kritičnih osvrta u kojima je sugerisano da se ne bazira na generalno prihvaćenom razumevanju operativnih rizika, da je propustila da specificira neke bitne elemente operativnih rizika i njihovu vezu sa ostalim rizicima, ova definicija je ipak prihvaćena od strane šire stručne i naučne javnosti, uz uvažavanje činjenice da omogućuje realizaciju dva važna cilja:

1. Kreiranje zajedničkog okvira iz koga će se moći kalkulisati obim troškova kapitala po osnovu operativnih rizika ali i
2. Definirati okvir za istraživanje i prikupljanje podataka (formiranje baze podataka) i postavljanje temelja za upravljanje ovim rizicima u bilo kojoj kulturi ili sistemu.

U tom smislu, za potrebe kalkulacije kapitalne adekvatnosti, definicija operativnih rizika iz Bazelskog Sporazuma II³⁰ će verovatno biti svetski prihvaćeni standard, ako se ima u vidu broj zemalja koje nameravaju da primene ovaj dokument.

3.1. DEFINISANJE OPERATIVNOG RIZIKA

Termin operativni rizik je definisan u poslednjih nekoliko godina³¹. Rizik se definiše kao opasnosti ili negativni efekti kojima potencijalne buduće aktivnosti mogu rezultirati. Ova definicija ukazuje na to da banka ne prihvata rizik samo kao sudbinu, već se suočava sa njim aktivno. Rizik se meri kao verovatnoća i uticaj negativnih devijacija. To proizilazi iz definicije da je rizik mogućnost. Drugi autori definišu rizik neutralno, da uključuje i negativne i pozitivne devijacije. To nije relevantno za operativni rizik. Za razliku od kreditnog ili tržišnog rizika, operativni rizik ne generiše veći prihod. Ova definicija, što je jako važno istaći, ne klasifikuje svaki gubitak kao rizik, samo neočekivani gubitak. Uzmimo primer pozajmica: samo oni zajmovi za koje se očekuje da će biti sa gubitkom, se smatraju rizičnim. Ove ideje su bazirane na manje ili više

²⁹ Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards, A revised Framework, Comprehensive Version*, Bank for International Settlements, June 2006, www.bis.org

³⁰ 95 zemalja prema istraživanju koje je sproveo Financial Stability Institute i objavio pod nazivom *Implementation of the new capital adequacy framework in non – Basel Committee member countries*, Summary of responses to the 2006, follow-up Questionnaire on Basel II implementation, Occasional paper No.6. , Bank for International Settlements, September, 2006.

³¹ British Bankers' Association, International Swaps and Derivatives Association and Robert Morris Associates (2000), *Operational Risk Management - The Next Frontier*, The Journal of Lending & Risk Management, March, pp. 38 - 44.

validnim informacijama o budućnosti eksternog okruženja sa jedne strane i budućnosti internog okruženja banke sa druge strane. Ranija iskustva uglavnom igraju glavnu ulogu. Druga definicija je takođe značajna za razumevanje rizika: on nije samo razlika između „očekivanih“ i „neočekivanih“ gubitaka koji su značajni, već je i razlika između „prihvatljivih“ i „neprihvatljivih“. Ova dva termina ukazuju na bankinu sposobnost da upravlja rizikom i njenom stavu prema riziku. Prihvatanje neočekivanih gubitaka se određuje ne samo kao ekonomski već i u velikoj meri kao i sociološki i psihološki elementi.

Nastojanja za, u osnovi, validnom definicijom operativnog rizika u bankarstvu je pojačana u poslednjih nekoliko godina. Ova definicija treba da se uklopi u okvir opšte definicije rizika. Za razliku od industrije, upravljanje bankarskim rizicima se u prošlosti uglavnom odnosilo na kreditni i tržišni rizik, gde su matematičko modeliranje i merenje igrali veliku ulogu.

Poslednjih nekoliko godina traži se osnovni koncept operativnog rizika. Definicija se može podeliti u dve kategorije: indirektnu i direktnu definiciju. Indirektna definicija podrazumeva da se pod operativnim rizikom podrazumevaju svi oni oblici rizika koji se ne mogu podvesti pod kreditne ili tržišne rizike. Pošto je ovo prilično jednostavna definicija, ova formulacija je bila dobrodošla od strane nadzornih organa do pre nekoliko godina. Ali bliža ispitivanja pokazuju da je indirektna definicija nezadovoljavajuća u praktičnom i teoretskom okruženju. Izveštaj definicija objavljen u poslednjih nekoliko godina od strane 16 banaka, konsultantskih i nadležnih organa, ukazuju na to da se sledeće reči najčešće pojavljuju: procesi i procedure, kadrovi i faktori ljudskih grešaka, interna kontrola, unutrašnji i spoljašnji događaji, direktni i indirektni gubici, tehnologija i sistemi. Skoro sve definicije naglašavaju unutrašnju stranu operacija, ali su i često neočekivani spoljašnji događaji takođe klasifikovani kao operativni rizik. Mnogi pristupi govore o gubicima, i o direktnim finansijskim gubicima, a i o indirektnim, onim koji se pojavljuju zbog gubitka reputacije banke i gubitkom njene pozicije na tržištu. Jedna od najboljih definicija operativnog rizika je ona koju je dala Britanska Bankarska Asocijacija (BBA): Operativni rizik je rizik direktnog ili indirektnog gubitka koji nastaje zbog neadekvatnih ili neuspešnih internih procesa, kadrova ili sistema ili zbog spoljašnjih događaja. Kada se ova definicija adaptira opštoj definiciji rizika dobija se sledeća definicija: Operativni rizik je izraz opasnosti od direktnih ili indirektnih gubitaka koji su rezultat neadekvatnih internih procesa, ljudi i sistema ili zbog spoljašnjih događaja. Najznačajnij karakteristike ove definicije su:

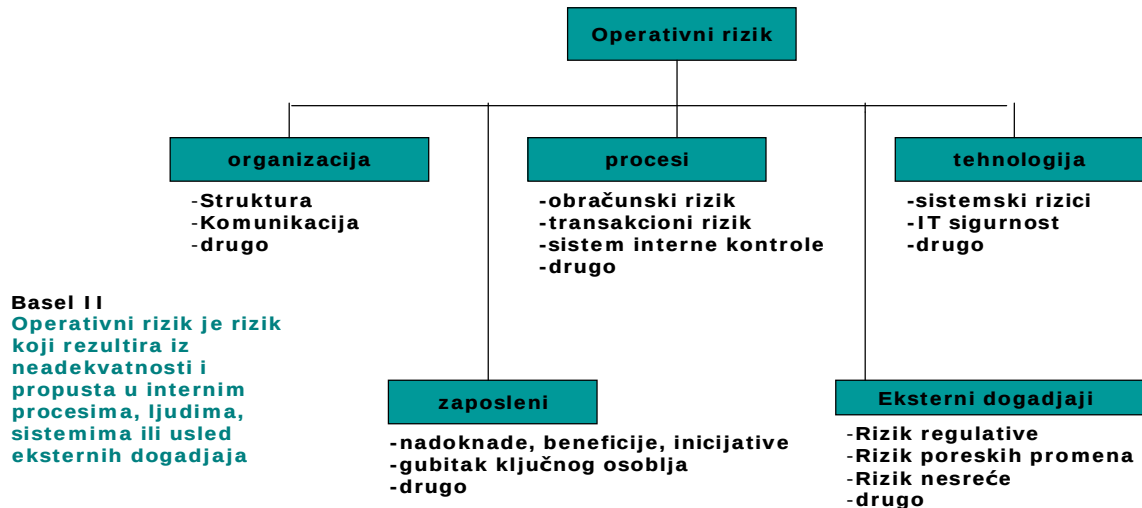
- Fokusirana je na interne aspekte koje banka može i treba da stvori i na njih utiče. To su uglavnom neuspešne aktivnosti banke i njenog osoblja. Ovi rizici su jasno odvojeni od tržišnih i kreditnih rizika;
- Značaj orijentacije ka procesima u konceptu operativnog rizika. Operativni rizici u bankarskom sektoru su sličniji rizicima u industriji, nego tržišnim i kreditnim rizicima;
- Presudnu ulogu igra ljudski faktor i greške koje pri tome nastaju. Postoje tri tipa operativnog rizika u ovom kontekstu: rizici, greške, konflikti;
- Spoljašnji incidenti su prirodni, politički ili vojni događaji, gubici ili deficiti tehničke infrastrukture, kao i promene i problemi sa zakonskim, poreskim i drugim sistemima, svi oni koji se događaju van oblasti kreditnog i tržišnog rizika.;

- Značajnu ulogu igra sistem unutrašnje kontrole, elementi i pravila koja su poznata i prihvaćena tokom proteklih godina ali se često zaboravljaju ili negiraju tokom perioda restrukturiranja proizvoda i inovacije procesa. Mnogi od opšte poznatih gubitaka u nedavnoj istoriji bankarstva su mogli biti izbegnuti ili ograničeni da su se pratila pravila.

Izazovi za operativni rizik:

- Nema najbolje prakse (prvi pokušaj je u BIS-ovoj Sound Practices...);
- Veliko pitanje: Kvalitet i kvantitet potrebnih podataka?
- Izvesne operativne rizike je teško, čak i nemoguće kvantifikovati;
- Trošak kapitala za operativne rizike: može proizvesti paradoksalne pobude;
- Upravljanje operativnim rizicima je na početnom stadijumu, i veliki je izazov stavljen pred risk management;
- Za sada postoje tri velike prepreke koje treba prevazići: podaci, procena i uključenost višeg menadžmenta.

ŠTA JE OPERATIVNI RIZIK?



3.2. IZVORI OPERATIVNOG RIZIKA

Bazelski odbor za nadzor banaka uviđa da će konkretan pristup upravljanju operativnim rizikom koji izabere pojedina banka zavisiti od niza činilaca, uključujući njenu veličinu i nivo tehničke opremljenosti, kao i prirodu i složenost njenih aktivnosti. Međutim, uprkos tim razlikama, jasne strategije i nadzor odbora direktora i više uprave, snažna kultura operativnog rizika³², kao i kultura unutrašnje kontrole (koja, između ostalog, podrazumeva jasnu hijerarhiju nadležnosti i podelu dužnosti), delotvorno unutrašnje izveštavanje kao i planiranje za slučaj nepredviđenih okolnosti, ključni su elementi okvira za delotvorno upravljanje operativnim rizikom banaka svih vrsta i veličina.

Deregulacija i globalizacija finansijskih usluga, zajedno sa rastućim nivoom finansijskih tehnologija, čine aktivnosti banke, a time i njihove profile rizika (tj. nivo rizika u aktivnostima banke i/ili kategorije rizika) sve složenijim. Razvoj bankarskih praksi upućuje na to da, osim kreditnog, kamatnog i tržišnog rizika, i ostali rizici mogu biti značajni. Neki primeri tih novih i rastućih rizika su:

- ako se pravilno ne kontroliše, veća upotreba visoko automatizovane tehnologije može rizike koji nastaju iz grešaka u ručnoj obradi podataka pretvoriti u rizike sistema, s obzirom na to da je sve prisutnije oslanjanje na globalno integrisane sisteme;
- rast elektronskog poslovanja nosi sa sobom potencijalne rizike (npr. unutrašnja i spoljašnja prevara i pitanja sigurnosti sistema), koji još nisu potpuno shvaćeni;
- sticanja, spajanja, razdvajanja i kosolidacije velikih razmera testiraju odvažnost novih ili nedavno integrisanih sistema;
- nastanak banaka koje posluju kao pružaoci usluga velikih razmera stvaraju potrebu za kontinuiranim održavanjem unutrašnjih kontrola i sigurnosnih sistema visokih nivoa;
- banke mogu primenjivati tehnike za smanjenje rizika (npr. kolateral, kreditni izvedeni instrumenti, sporazumi o saldiranju i sekjuritizaciji imovine) kako bi optimizirale svoju izloženost tržišnom i kreditnom riziku, ali te tehnike mogu dovesti do pojave ostalih oblika rizika;
- sve češće poveravanje određenih poslova spoljašnjim izvršiteljima na osnovu sporazuma o eksternizaciji i učešću u sistemima kliringa i namere mogu smanjiti neke rizike, ali ujedno nose druge značajne rizike za banku.

Prethodno naveden skup različitih rizika može se nazvati operativni rizik. To je rizik od gubitka koji nastaje zbog neprimerenih ili neuspešnih unutrašnjih procesa, ljudi ili sistema ili zbog spoljašnjih uticaja³³. Definicija obuhvata pravni rizik, ali uključuje i strateški i reputacioni rizik.

Operativni rizik ima različita značenja unutar bankarskog sektora, te banke zbog toga za unutrašnje potrebe mogu odlučiti da usvoje svoje vlastite definicije operativnog rizika. Bez obzira na tačnu definiciju, za delotvorno upravljanje tim rizikom i kontrolu

³² Unutrašnja kultura operativnog rizika označava kombinovani skup vrednosti pojedinca i trgovačkog društva, stavova, sposobnosti i ponašanja koji određuju odlučnost banke u upravljanju operativnim rizikom i stil upravljanja operativnim rizikom.

³³ Definicija je preuzeta od bankarskog sektora do koje je Bazelski odbor došao utvrđujući minimalni iznos zagarantovanog kapitala koji je potreban za pokriće operativnog rizika.

nad tom kategorijom rizika ključno je da banke jasno razumeju šta se podrazumeva pod operativnom rizikom. Takođe je važno da definicija uzme u obzir celokupan skup značajnih operativnih rizika s kojima se suočava banka, a time da obuhvata najznačajnije uzroke velikih poslovnih gubitaka. Sledeće vrste događaja mogu dovesti do velikih gubitaka, i zbog njih nastaje operativni rizik:

- Unutrašnja provera. Na primer, namerno pogrešno izveštavanje o pozicijama, krađa od strane zaposlenih i trgovanje upućene osobe iz banke na vlastitom računu.
- Spoljašnja provera. Na primer, pljačka, krivotvorenje, izdavanje čekova bez pokrića kao i šteta nastala zbog neovlašćene upotrebe tuđeg kompjutera;
- Prakse vezane za zapošljavanje i zaštitu na radnom mestu. Na primer, potraživanja radnika vezana uz naknade, kršenje pravila o zdravlju i zaštiti zaposlenih, organizovane radničke aktivnosti, potraživanja vezana uz diskriminaciju i opštu odgovornost;
- Klijenti, proizvodi i poslovne prakse. Na primer, kršenje povereničkog odnosa, zloupotreba poverljivih informacija o klijentima, neprimerene aktivnosti trgovanja na računu banke, pranje novca i prodaja neovlašćenih proizvoda;
- Oštećenje materijalne imovine. Na primer, terorizam, vandalizam, potresi, požari i poplave;
- Poremećaji u poslovanju i kvar informacionog sistema. Na primer, kvar hardvera ili softvera, telekomunikacijski problemi i prekid rada postrojenja;
- Izvršavanje, isporuka i upravljanje procesima. Na primer, greške u unosu podataka, propusti u upravljanju kolateralom, nepotpuna pravna dokumentacija, neovlašćeni pristup računima klijenta, loše postupanje druge ugovorne strane koja nije klijent i sporovi sa spoljašnjim izvršiteljima usluga.

Banka je dužna da identifikuje postojeće izvore operativnog rizika, kao i potencijalne izvore tog rizika koji mogu nastati uvođenjem novih poslovnih proizvoda, sistema ili aktivnosti³⁴.

Pod identifikacijom izvora rizika³⁵ podrazumevaju se:

- 1) interne greške i zloupotrebe, i to:
 - neovlašćeno postupanje zaposlenih,
 - zloupotreba službenog položaja;
- 2) eksterno kršenje propisa, i to:
 - nezakonito postupanje lica koja nisu zaposlena u banci;
 - propusti u sistemu obezbeđenja;
- 3) propusti u sistemu zapošljavanja i zaštite na radu, i to:
 - odnosi između zaposlenih u banci,
 - sigurnost na radu,
 - diskriminacija na radnom mestu;
- 4) problemi u funkcionisanju sistema odnosa s klijentima, u plasmanu proizvoda i u poslovnim procedurama – ako su neadekvatni, i to:
 - standardizacija proizvoda, zaštita podataka i poslovne tajne,
 - poslovne procedure,
 - poslovni tokovi (tokovi odlučivanja i tokovi informacija),

³⁴ Jameson, R. (1998), *Playing the Name Game, Risk*, October, pp. 38 - 42.

³⁵ www.nbs.rs

- izbor klijenata i izloženost prema njima,
- savetodavna funkcija;
- 5) štete na imovini banke usled prirodnih katastrofa i drugih događaja;
- 6) poremećaji u organizaciji banke i greške u funkcionisanju uspostavljenih sistema;
- 7) sprovođenje poslovnih procedura i odluka, i to:
 - obnavljanje i provera finansijskih transakcija,
 - nadzor i izveštavanje,
 - prijem klijenata i dokumentacije,
 - upravljanje potraživanjima i obavezama prema klijentima,
 - odnos s drugim poslovnim partnerima,
 - odnos s dobavljačima.

Izvore operativnih rizika banka je dužna da prati po poslovima utvrđenim u skladu sa organizacijom i delatnošću banke, a pre svega po sledećim poslovima:

- poslovi s privredom,
- poslovi s licima u finansijskom sektoru u smislu Zakona o bankama,
- poslovi sa stanovništvom,
- komercijalni poslovi,
- poslovi platnog prometa,
- agencijski poslovi,
- poslovi upravljanja imovinom,
- brokersko-dilerski poslovi.

Aktivna razmena ideja između supervizora i bankarskog sektora ključna je za kontinuirani razvoj odgovarajućih smernica za upravljanje izloženostima koje su povezane sa operativnim rizikom.

3.3. UPRAVLJANJE OPERATIVNIM RIZIKOM

Upravljanje operativnim rizikom nije nova praksa³⁶. Bankama je uvek bilo važno da pokušaju da spreče prevare, održe integritet unutrašnjih kontrola, smanje greške u obavljanju transakcija itd. Međutim, relativno je nov pogled na upravljanje operativnim rizikom kao na sveobuhvatnu praksu. U prošlosti su se banke u upravljanju operativnim rizikom gotovo u potpunosti oslanjale na mehanizme unutrašnjih kontrola svojih poslovnih aktivnosti, koje su bile dostupne funkcijom revizije. Iako su ti mehanizmi i dalje važni, u poslednje su se vreme pojavile specifične strukture i procesi kojima je cilj upravljanje operativnim rizikom. U tom smislu sve više organizacija dolazi do zaključka da programom upravljanja operativnim rizikom osigurava sigurnost i zdravlje banke, te stoga napreduju u bavljenju operativnim rizikom kao posebnom klasom rizika na sličan način na koji tretiraju ostale rizike.

³⁶ Saunders, A. (1999) *Financial Institutions Management. A Modern Perspective*, Boston et al. Shadow Financial Regulatory Committees of Europe Japan and the U.S. (1999) *Improving the Basle Committee's New Capital Adequacy Framework*, New York.

Osnovna načela za upravljanje operativnim rizikom:

1. Načelo: Odbor direktora³⁷ treba da bude svestan glavnih aspekata operativnog rizika banke kao specifične kategorije rizika kojim treba upravljati, usvojiti i periodično preispitivati bankarski sistem upravljanja operativnim rizikom. Sistem treba da sadrži definiciju operativnog rizika na nivou banke, zatim postaviti načela prema kojima će se operativni rizik identifikovati, ocenjivati, pratiti i kontrolisati.

2. Načelo: Odbor direktora treba da se pobrine da bankarski sistem upravljanja operativnim rizikom podleže delotvornoj i sveobuhvatnoj unutrašnjoj reviziji koju obavlja operativno nezavisno, primereno obrazovano i sposobno osoblje. Funkcija unutrašnje revizije ne bi smela biti direktno nadležna za upravljanje operativnim rizikom.

3. Načelo: Viša uprava treba biti nadležna za sprovođenje sistema upravljanja operativnim rizikom koji odobrava odbor direktora. Sistem treba biti dosledno sproveden unutar cele bankarske organizacije, a zaposleni na svim nivoima treba da razumeju svoje nadležnosti koje se odnose na upravljanje operativnim rizikom. Viša uprava takođe treba da bude nadležna za razvijanje politika, procesa i postupaka upravljanja operativnim rizikom povezanim sa svim značajnim proizvodima, procesima i sistemima banke.

4. Načelo: Banke treba da utvrde i procene inherentni operativni rizik povezan sa svim značajnim proizvodima, aktivnostima, procesima i sistemima. Banke takođe trebaju osigurati da pre uvođenja novih proizvoda, procesa i sistema ili pre preduzimanja novih aktivnosti inherentni operativni rizik koji je sa njima povezan bude podvrgnut adekvatnim procesima ocenjivanja.

5. Načelo: Banke treba da uvedu postupak redovnog nadziranja profila operativnog rizika i značajnih izloženosti gubicima. Viša uprava i odbor direktora treba da budu redovno izveštavani o informacijama koje mogu pomoći u aktivnom upravljanju operativnim rizikom.

6. Načelo: Banke treba da imaju politike, procese i postupke za kontrolisanje/smanjenje operativnih rizika. Banke treba da periodično preispituju svoje strategije za ograničavanje i kontrolisanje rizika te, s obzirom na svoju celokupnu sklonost riziku i profil, prilagode svoj profil rizika upotrebom primerenih strategija.

7. Načelo: Banke treba da izgrade planove za nepredviđene okolnosti i planove za očuvanje kontinuiteta poslovanja kako bi osigurale svoje trajno poslovanje i ograničiti gubitke ako dođe do ozbiljnog poremećaja u poslovanju.

8. Načelo: Bankarski supervizori treba da zahtevaju da sve banke, bez obzira na veličinu treba da imaju delotvoran sistem identifikovanja, ocenjivanja, praćenja i kontrolisanja značajnih operativnih rizika u sklopu svoga sveukupnog pristupa upravljanju rizikom.

9. Načelo: Supervizori treba da obavljaju, direktno ili indirektno, redovno vrednovanje politika, postupaka i praksi banke povezanih sa operativnim

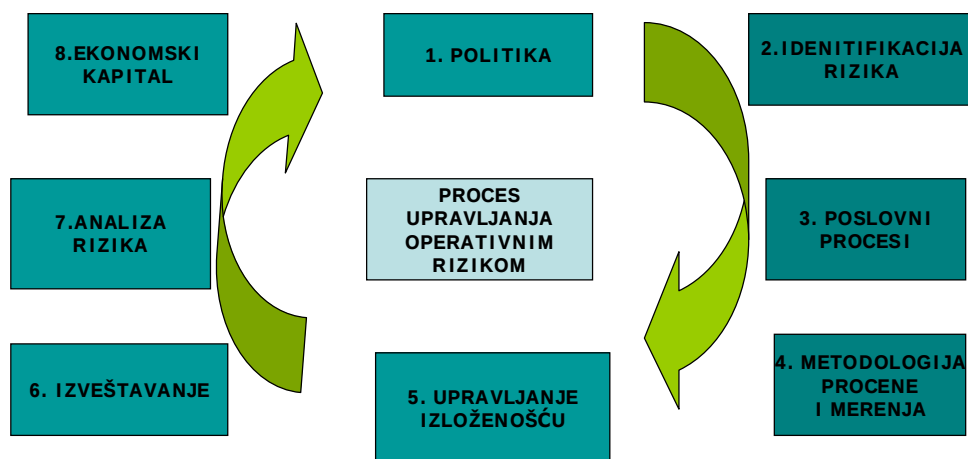
³⁷ Upravljačka struktura treba da se sastoji od odbora direktora i više uprave. Među zemljama postoje značajne razlike u zakonskim i pravnim sistemima s obzirom na funkcije odbora direktora i više uprave. U nekim zemljama glavna, ako ne i isključiva funkcija odbora je nadziranje izvršnog tela kako bi osigurao da izvršno telo ispunjava svoje zadatke. Zbog toga se odbor direktora u nekim slučajevima naziva nadzorni odbor. To znači da taj odbor nema izvršne funkcije. Nasuprot tome, u nekim zemljama taj odbor ima šira ovlašćenja, u smislu da određuje opšti okvir za upravljanje bankom. Zbog tih se razlika pojmovi *odbor direktora* i *viša uprava* ne koriste kao pravna određenja, već da bi se označile dve funkcije unutar banke koje su zadužene za donošenje odluka.

rizicima. Supervizori treba da osiguraju da postoje primereni mehanizmi koji im omogućuju da budu obavešteni o kretanjima u bankama.

10. Načelo: Banke treba da objavljuju dovoljno informacija kako bi učesnicima na tržištu omogućile da procene njihov pristup upravljanju operativnim rizikom.

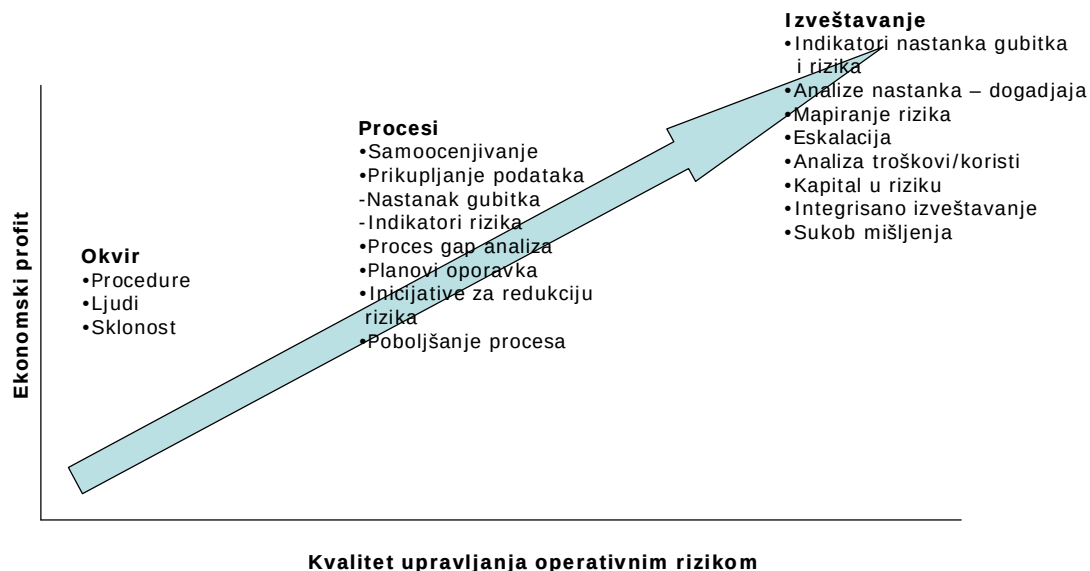
Slika 3. Upravljanje operativnim rizikom

UPRAVLJANJE OPERATIVNIM RIZIKOM



Slika 4. Kvalitet upravljanja operativnim rizikom

KVALITETE UPRAVLJANJA OPERATIVNIM RIZIKOM



Vrednost iz investiranja u rešenja koja su vezana za upravljanje operativnim rizikom

Upravljanje operativnim rizikom iz ugla praktičnih perspektiva:

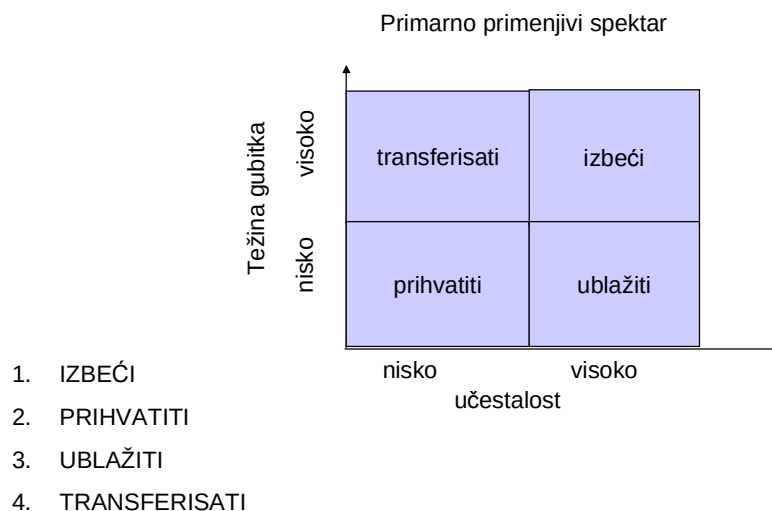
1. Politika operativnog rizika / identifikacije rizika / analize rizika,
2. ORM organizacija (dodeljeni resursi: operativni risk menadžer),
3. Kontinuirano planiranje poslovanja,
4. Implementacija Basel II i njegovih čvrstih zahteva za praksom,
5. Analize poslovnih procesa (reinženjering poslovnih procesa),
6. Ključni indikatori rizika / koncept za izveštavanje o operativnom riziku,
7. Interna baza podataka o gubicima / eksterna baza,
8. Implementacija Baselovog AMA – advanced measurement approach.

Ciljevi upravljanja operativnim rizikom:

1. Prevencija od potencijalnog događaja kojim se manifestuje operativni rizik,
2. Ublažavanje efekata koji su nastali u okviru operativnog rizika i smanjenje njihovog udara,
3. Adekvatna kontrola nastale štete u slučaju manifestacije operativnog događaja.

Slika 5. Alternative pri upravljanju operativnim rizikom

ALTERNATIVE PRI UPRAVLJANJU OPERATIVNIM RIZIKOM



Slika 6. Alokacija kapitala potrebnog da se pokriju operativni rizici

ALOKACIJA KAPITALA POTREBNOG DA SE POKRIJU OPERATIVNI RIZICI



Ključne funkcionalnosti upravljanja operativnim rizikom:

SAMOOOCENJIVANJE: dobro struktuiran način da se identifikuju rizici i oceni (barem grubo) izloženost riziku;

RIZIK I SISTEM INTERNE KONTROLE: rizici bivaju ocenjeni zajedno sa respektivnim sistemom interne kontrole, slabosti preko sistema interne kontrole bivaju registrovane, upravljane i izveštavane;

KLJUČNI INDIKATORI RIZIKA: definicija i registrovanje internih indikatora za određeni operativni rizik, cilj: uspostavljanje sistema ranog upozorenja, izveštaja o ključnim indikatorima rizika;

INTERNA BAZA PODATAKA O GUBICIMA: sakupljanje i pravljenje interne baze podataka o gubicima (greškama) pomaže banci da poboljša svoje procese i TQL, izbegne mnoge gubitke, obuhvati sve relevantne informacije za upravljanje operativnim rizikom, kao preduslov za mnogo kompleksnije pristupe tima AMA/Basel II.

IZVEŠTAVANJE O OPERATIVNIM RIZICIMA

Razlozi da banke prihvate aktivan ORM pristup u budućnosti:

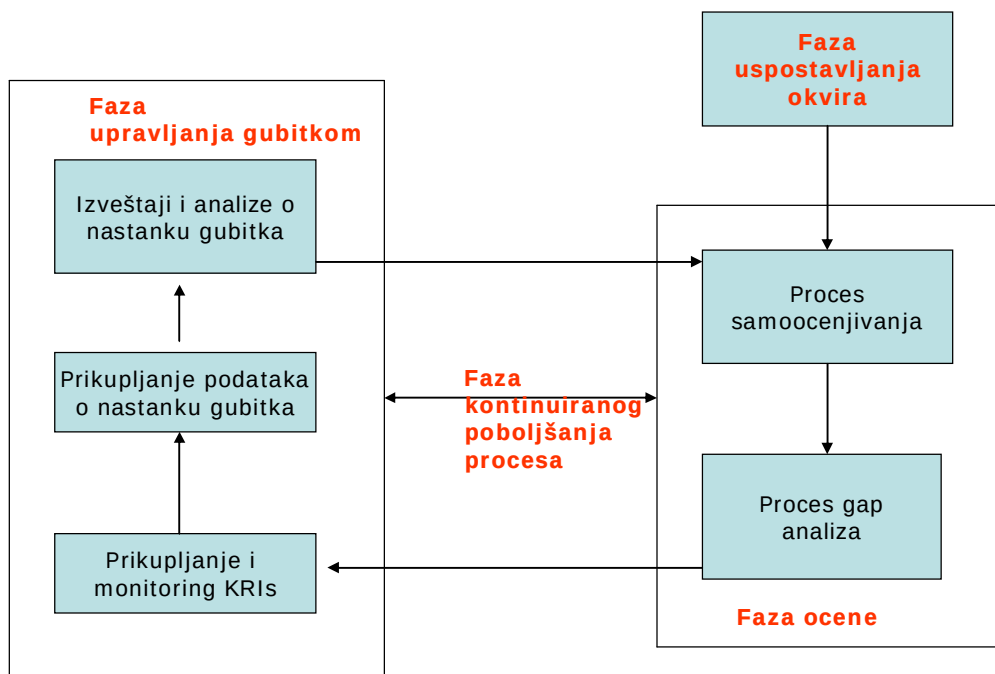
1. Finansijske institucije treba da prepoznaju vrednost pristupa aktivnog upravljanja rizicima:
 - izbegavajući gubitke koji proizilaze iz operativnih rizika (uzroka),
 - smanjujući reputacioni rizik,
 - smanjivanje troškova / poboljšanje kvaliteta (optimizirajući procese),
2. BIS-ova "Sound Practices" biće budući standard za sve banke;
3. Basel II će i dalje isticati operativni rizik uvodeći nove zahteve za kapitalom.

Slika 7. Upravljanje operativnim rizicima prema Bazelu II



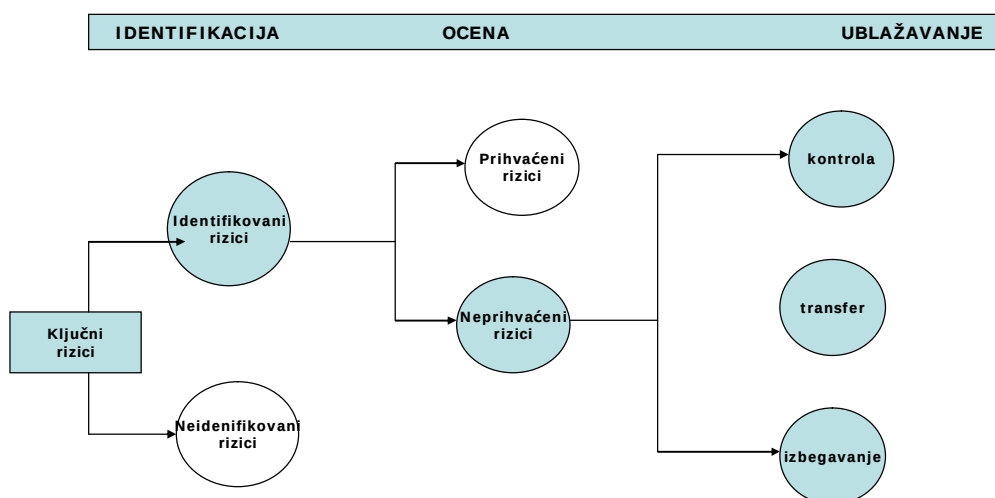
Slika 8. Okvir upravljanja operativnim rizikom

OKVIR UPRAVLJANJA OPERATIVNIM RIZIKOM



Slika 9. Segregacija rizika

SEGREGACIJA RIZIKA



Da bi banka uspostavila upravljanje operativnim rizicima potrebno je da razvije četiri faze okvira³⁸ upravljanja operativnim rizicima:

1. Identifikacija
 - Definisanje
 - Utvrđivanje obuhvata rizika
 - Klasifikacija
 - Kategorija (Nivo 1)
 - Pod – kategorija (Nivo 2)
 - Aktivnost (Nivo 3)
2. Ocena
 - Samoocenjivanje
 - Bodovanje rizika
 - Mapiranje rizika
 - Merenje rizika
3. Kontrola
 - Politika
 - Programi upravljanja
 - Smernice kontrole
 - Upravljačka struktura
 - Struktura izveštavanja
4. Praćenje
 - Aktivno osoblje
 - Integrisana interna i eksterna kontrola
 - Periodično ocenjivanje
 - Redovno izveštavanje

3.3.1. Identifikacija

Prvi korak u usvajanju programa upravljanja operativnim rizikom, jeste da zaposleni usvoje definiciju operativnog rizika kao:

“Rizik gubitka³⁹ koji rezultira iz neadekvatnih ili loše vođenih internih procesa, ljudi i sistema ili prouzrokovan spoljnim uticajem”⁴⁰

Operativni rizik uključuje pravni rizik ali isključuje strateški, reputacioni, sistemski rizik.

³⁸ Okvir je razvijen na osnovu studije „Uspešne prakse za upravljanje i praćenje operativnog rizika“ (Sound Practices for the Management and Supervision of Operational Risk) koju je pripremila Risk Menadžment grupa Bazelskog komiteta supervizije banaka u julu 2002. godine

³⁹ NetRisk (2000) Methodology for the Classification of Operational Losses.

⁴⁰ Definiciju je usvojila bankarska industrija kao deo Bazelskog komiteta o superviziji rada banaka u oblasti definisanja minimalnog kapitala za operativne rizike.

Slika 10. Identifikacija

Pregled okvira- Identifikacija

Identifikacija omogućava razvijanje strukture merenja i razumevanje profila rizika :

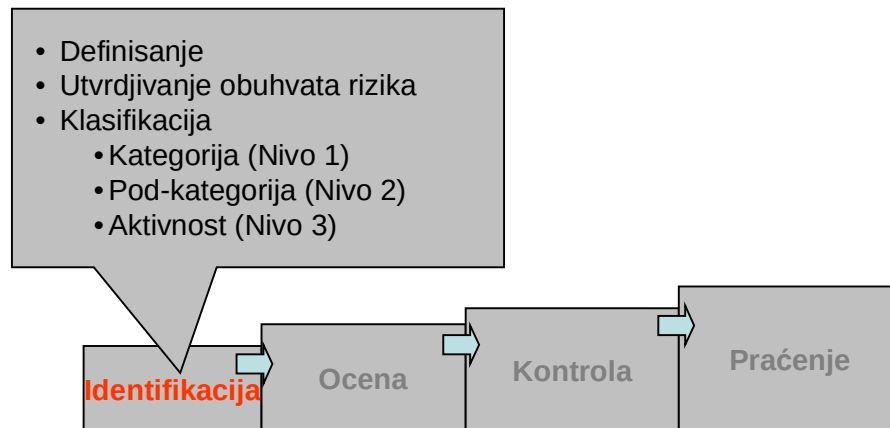


Tabela 4. Identifikacija – Utvrđivanje obuhvata rizika

Tipovi operativnog rizika	
Kategorija (Nivo 1)	Opis
1. Interna obmana	Radnje koje uključuju prevaru, nelegalno prisvajanje imovine, nepoštovanje zakona koje je banka usvojila, a uključuje bar jedno interno lice
2. Eksterna pronevera	Radnje koje preduzima eksterno lice koje uključuju pronevere, nelegalno prisvajanje imovine ili remećenje zakona
3. Praksa vezana za zaposlene i bezbednost na radnom mestu	Radnje koje ugrožavaju zdravlje i bezbednost zaposlenih i koje rezultiraju utuženjem
4. Klijenti, proizvodi i poslovna politika	Nenamerno ili nemarno neispunjavanje profesionalnih obaveza prema klijentima ili kao rezultat prirode ili dizajna proizvoda
5. Fizička oštećenja imovine	Gubitak ili oštećenje fizičke imovine koje rezultira iz prirodnih nepogoda ili drugih događaja
6. Remećenje poslovnih operacija i padovi sistema	Remećenje poslovnih procedura ili padovi sistema
7. Izvršavanje, isporuka i process upravljanja	Neizvršenja obrade transakcija, neadekvatno upravljanje procesima i odnosima sa trećim licima i dobavljačima

Identifikovanje rizika najvažnije je za kasniji razvoj održivog sistema praćenja i kontrolisanja operativnog rizika⁴¹. Delotvorno identifikovanje operativnog rizika uzima u obir i unutrašnje činioce (kao što su struktura banke, priroda aktivnosti banke, kvalitet ljudskih potencijala banke, organizacione promene i promet po zaposlenom) i spoljašnje činioce (kao što su promene u bankarskom sektoru i tehnološki napredak) koji mogu negativno uticati na ostvarenje ciljeva banke.

3.3.2. Ocena

Okvir upravljanja operativnim rizicima⁴² – SAMOOCENJIVANJE

Samooocenjivanje je proces gde poslovne jedinice:

- Identifikuju i ocenjuju rizike,
- Identifikuju i ocenjuju nivoa kontrole koje su uspostavljene radi upravljanja rizicima,
- Pripremaju planove akcije za poboljšanje (program upravljanja operativnim rizicima.).

Samooocenjivanje⁴³ je neophodno jer:

- Određuje odgovornost za operativni rizik u okviru poslovne jedinice –poslovne jedinice snose odgovornost za operativne rizike kao i za gubitke koji proizilaze iz operativnih rizika. Direktori poslovnih jedinica su odgovorni za potpune rezultate samooocenjivanja.

- Pojačava kulturu otvorenosti i transparentnosti – o operativnim rizicima je potrebno otvoreno razgovarati kako bi se povećala svest i odredili odgovarajući resursi. Procesom samooocenjivanja se stvara forum za otvorenu raspravu o tim pitanjima.

- Implementirati proaktivni a ne reaktivni proces–poslovanje će biti daleko uspešnije kada se anticipiraju i ispravljaju problemi pre nego što nastanu. Samooocenjivanjem se idetifikuju slabosti u kontrolama u okviru postojećeg procesa i pripremaju novi planovi akcija za ispravljanje nedostataka.

- Identifikacija nedostataka – rezultat samooocenjivanja je identifikacija nedostataka u kontrolama i priprema zadataka za ispravljanje uočenih nedostataka. Podaci se prikupljaju iz različitih izvora i služe za pripremu planova za poboljšanje, određivanje odgovornosti i vremenskih prioriteta (program upravljanja).

- Poboljšava uvid i odlučivanje – rezultate samooocenjivanja pregleda Generalni direktor kako bi se razumela izloženost banke rizicima i planove za upravljanje.

- Poboljšavanja produktivnost revizije – kako se poboljšava pouzdanost samooocenjivanja, to omogućava revizorima da se posvete bitnijim pitanjima sa kojima je banka suočena a ne toliko kontrolisanjem transakcija detalja sa stanovišta grešaka.

⁴¹ NetRisk (2000) Methodology for the Classification of Operational Losses.

⁴² Young, B. (1999), Raising the Standard, Risk Magazine, Special Report on Operational Risk, November.

⁴³ Levine, M. and Hoffmann, D. G. (2000) Enriching the Universe of Operational Risk Data: Getting Started on Risk Profiling, Operational Risk, pp. 25 - 39.

Slika 11. Ocena

Pregled okvira - Ocena

Ocena određuje visinu rizika unutar poslovnih jedinica:

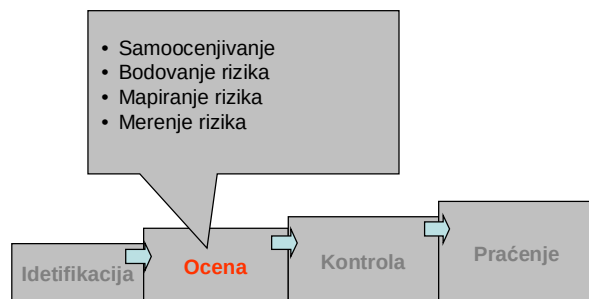


Tabela 5. Samoocenjivanje operativnih rizika

Jedinica 1	Sektor ABC	Direktor sektora	
Kategorija rizika		Frekvencija rizika	Mera rizika
Kategorija (Nivo 1)	Pod-kategorija (Nivo 2)		
1. Interna pronevera	Neovlašćene aktivnosti (1UA)		
	Pronevera (1TF)		
2. Eksterna pronevera	Pronevera (2 TF)		
	Bezbednosni sistemi (2 SS)		
3. Praksa vezana za zaposlene i bezbednost na random mestu	Odnosi prema zaposlenim (3 ER)		
	Bezbednost na radu (3 SE)		
	Diskriminacija (3 DD)		
4. Klijenti, proizvodi i poslovna praksa	Pogodnosti, razotkrivanje i zaštita interesa klijenata (4 SDF)		
	Neprikladni poslovi (4 IB)		
	Proizvodi sa greškom (4 PF)		
	Selekcija i izloženost (4 SSE)		
	Aktivnosti savetovanja (4 AA)		
5. Fizička oštećenja imovine	Nepogode (5 DOE)		
6. Remećenje poslovnih operacija i padovi sistema	Padovi sistema (6 SF)		
	Ključni pojedinci (6 KI)		
7. Izvršavanje, isporuka i upravljanje procesom	Identifikovanje transakcija, izvršavanje i održavanje (7 TCEM)		
	Nadgledanje i izvršavanje (7 MR)		
	Prijem klijenata i dokumentacije (7 CID)		
	Upravljanje računima klijenata (7 CAM)		
	Klijenti (7 TC)		
	Prodavci i dobavljači (7 VS)		

- Samooocenjivanje ili procenjivanje rizika⁴⁴: banka procenjuje svoje operacije i aktivnosti s obzirom na katalog potencijalnih osetljivosti na operativni rizik. Ovaj se proces sprovodi iznutra i često uključuje kontrolne popise i/ili radionice za utvrđivanje jakih i slabih strana okruženja u vezi sa operativnim rizikom. Na primer, bodovne liste (*scorecards*) način su da se kvalitativne procene prevedu u kvantitativnu metriku koja daje relativan rejting različitih vrsta izloženosti operativnom riziku. Neki se bodovi mogu odnositi na rizike, koji su svojstveni određenoj poslovnoj aktivnosti, dok se drugima mogu rangirati rizici koji se pojavljuju u različitim poslovnim aktivnostima. Bodovi se odnose na inherentne rizike, kao i na kontrole za njihovo smanjivanje. Osim toga, banke se mogu koristiti bodovnim listama u raspodeli ekonomskog kapitala različitim poslovnim aktivnostima u zavisnosti od njihove uspešnosti u upravljanju i kontrolisanju različitih aspekata operativnog rizika.

- Razvrstavanje rizika (*mapping*): u ovom se procesu ovom se procesu različite poslovne jedinice, organizacijske funkcije ili poslovni tokovi razvrstavaju pema vrsti rizika. Ovaj zadatak može otkriti područja slabosti i pomoći upravi u određivanju prioriteta daljih aktivnosti.

- Pokazatelji rizika: pokazatelji rizika su statistički i/ili metrički podaci, često finansijski, koji mogu dati uvid u različitu poziciju banke. Ovi se pokazatelji obično redovno preispituju kako bi se banke upozorile na promene koje mogu biti indikativne za problem povezan sa rizikom. Takvi su pokazatelji, na primer, broj propalih transakcija, stopa prometa po zaposlenom i učestalost i/ili ozbiljnost grešaka i propusta.

- Merenje: neke su banke počele kvantificirati svoju izloženost operativnom riziku koristeći se različitim pristupima. Na primer, podaci o iskustvu banke koje se odnosi na istorijski gubitak mogu dati značajne informacije za procenu izloženosti banke operativnom riziku i razvijanju politike za smanjenje tog rizika. Delotvoran način da se te informacije dobro upotrebe jeste uspostavljanje sistema za sistematično nadgledanje i evidentiranje učestalosti i ozbiljnosti pojedinih slučajeva gubitaka i ostalih relevantnih informacija o njima. Neke banke takođe kombinuju unutrašnje podatke o gubicima sa spoljašnjim podacima o gubicima, analizama scenarija i činionicima za procenu rizika.

3.3.3. Kontrola

Kontrolne aktivnosti osmišljene su za postupanje sa operativnim rizicima koje je banka identifikovala⁴⁵. U pogledu svakog značajnog operativnog rizika koji je identifikovala banka treba odlučiti hoće li upotrebiti odgovarajuće postupke za kontrolisanje i/ili smanjenje rizika ili će snositi rizik. Što se tiče onih rizika koji se ne mogu kontrolisati, banka treba da odluči da li će ih prihvatiti, smanjiti nivo povezane poslovne aktivnosti ili se u potpunosti povući iz te aktivnosti. Banke treba da autvrde kontrole procese i postupke i da imaju svoj sistem koji će osigurati poštovanje

⁴⁴ Saunders, A. (1999) *Financial Institutions Management. A Modern Perspective*, Boston et al. Shadow Financial Regulatory Committees of Europe Japan and the U.S. (1999) *Improving the Basle Committee's New Capital Adequacy Framework*, New York.

⁴⁵ Saunders, A. (1999) *Financial Institutions Management. A Modern Perspective*, Boston et al. Shadow Financial Regulatory Committees of Europe Japan and the U.S. (1999) *Improving the Basle Committee's New Capital Adequacy Framework*, New York.

dokumentovanog skupa unutrašnjih politika koji se odnose na sistem upravljanja rizikom.

Među glavnim elementima tog skupa politika mogu se svrstati:

1. preipitivanja, na najvišem nivou, postignutog napretka prema navedenim ciljevima;
2. provera poštovanja politika sa kontrolama uprave;
3. politike, procesi i postupci koji se odnose na preipitivanje, tretman i rešavanje pitanja nepoštovanja politika i
4. sistem dokumentovanih odobrenja i ovlašćenja kako bi se osigurala odgovornost odgovarajućeg nivoa uprave.

Iako je sistem formalnih pisanih politika i postupaka ključan, on se mora pojačati snažnom kulturom kulture koja pomiče dobre prakse upravljanja rizikom. I odbor direktora i viša uprava nadležni su za uspostavljanje snažne kulture unutrašnje kontrole, u kojoj su kontrolne aktivnosti sastavni deo redovnih aktivnosti banke. Kontrolama koje su sastavni deo redovnih aktivnosti omogućuje se brzo reagovanje na promenljive uslove i izbegavaju nepotrebni troškovi.

Delotvoran sistem unutrašnjih kontrola takođe zahteva odgovarajuću podelu dužnosti, tako da nadležnosti osoblja nisu raspodeljene na način na način koji bi mogao dovesti do sukoba interesa. Ako se pojednicima ili grupi dodele dužnosti koje bi mogle kod njih prouzrokovati sukob interesa, one bi im mogle omogućiti prikrivanje gubitaka, grešaka ili neprimerenih aktivnosti. Zbog toga se područja sukoba interesa trebaju utvrditi, minimizirati i podvrgnuti pažljivom nezavisnom nadziranju i preispitivanju.

Osim podele dužnosti, banke treba da osiguraju da postoje ostale unutrašnje prakse koje su prikladne za kontrolisanje operativnog rizika. To mogu, na primer, biti:

1. pažljivo nadziranje poštovanja dodeljenih limita ili pragova rizika,
2. zaštita pristupa sredstvima i evidenciji banke kao i njihovoj upotrebi,
3. osiguranje odgovarajuće stručnosti i obrazovanja osoblja,
4. utvrđivanje poslovnih delatnosti ili proizvoda kod kojih se čini da dobit nije u skladu sa realnim očekivanjima, i
5. redovna provera i usklađivanje transakcija i računa.

Nepostojanje ovakve prakse dovelo je do značajnih operativnih gubitaka nekih banaka tokom poslednjih godina.

Operativni rizik može biti izraženiji kad se banke počnu baviti novim aktivnostima ili kad razvijaju nove proizvode (posebno ako te aktivnosti ili proizvodi nisu u skladu sa osnovnim strategijama poslovanja banke), kad uđu na nepoznata tržišta i/ili započnu poslovati na mestima koja su geografski udaljena od sedišta banke⁴⁶. Uz to, u mnogim takvim slučajevima banke ne osiguravaju da kontrolna infrastruktura upravljanja rizikom održava korak sa rastom poslovne aktivnosti. Nekoliko najvećih gubitaka i gubitaka najvišeg profita, do kojih je došlo poslednjih godina, dogodio se kad je postojao jedan ili više prethodno navedenih okolnosti. Zbog toga je važno da banke osiguraju da se posebna pažnja posvećuje aktivnostima unutrašnje kontrole kad se jave takve okolnosti.

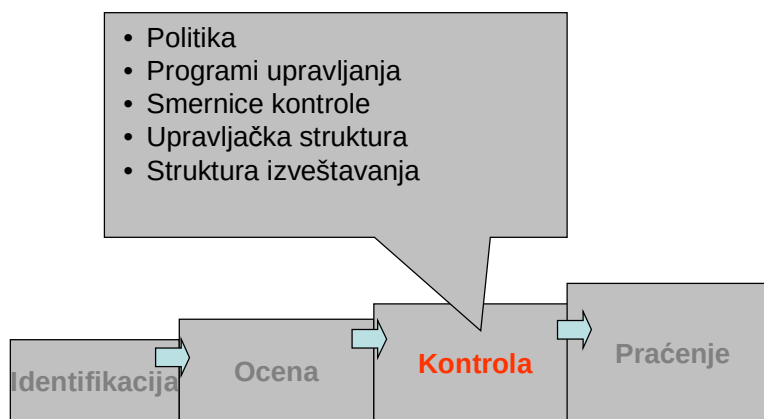
Neki značajni operativni rizici malo su verovatni, ali bi mogli dovesti do ozbiljnih finansijskih posledica. Dalje, ne mogu se kontrolisati svi rizični događaji (npr. prirodne katastrofe). Alati ili programi za smanjivanje rizika mogu se upotrebiti za smanjenje izloženosti tim događajima ili učestalosti i/ili ozbiljnosti tih događaja.

⁴⁶ Levine, M. and Hoffmann, D. G. (2000) Enriching the Universe of Operational Risk Data: Getting Started on Risk Profiling, Operational Risk, pp. 25 - 39.

Banke treba da gledaju na alate za smanjenje rizika kao na dopunu temeljnoj unutrašnjoj kontroli operativnog rizika, a ne kao njenu zamenu⁴⁷. Izloženosti se mogu značajno smanjiti ako postoje mehanizmi za brzo prepoznavanje i ispravljanje opravdane greške u vezi sa operativnim rizikom. Takođe, potrebno je pažljivo razmotriti u kojoj meri alati za smanjenje rizika zaista smanjuju rizik, a koliko rizik prenose na drugi sektor ili područje poslovanja ili čak stvaraju novi rizik (npr. pravni rizik ili rizik druge strane).

Pregled okvira - Kontrola

Kontrola pomaže u razvijanju upravljanja rizikom i izveštavanju:



Slika 12. Kontrola

Politika upravljanja operativnim rizicima treba da uključuje sledeće principe:

1. Okvir,
2. Organizaciona odgovornost,
3. Interna revizija,
4. Ocena,
5. Kontrola,
6. Nadgledanje,
7. Kontinuirano planiranje.

⁴⁷ Geiger, H. and Piaz, J.-M. (2000) Identifikation und Bewertung operationeller Risiken, In Handbuch Bank-Controlling (ed., Schierenbeck, H.) Wiesbaden. (forthcoming) Greenbaum, S. I. and Thakor, A. V. (1995) Contemporary Financial Intermediation, Fort Worth.

Okvir upravljanja operativnim rizicima – Program upravljanja.

Program upravljanja rizicima se sastoji od:

1. samoocenjivanje kontrola za smanjivanje kategorija rizika,
2. identifikacija kontrolnih gepova,
3. pripremanje planova unapređivanja, određivanjem odgovornosti i vremenskih prioriteta.

3.3.4. Praćenje

Delotvoran proces praćenja ključan je za adekvatno upravljanje operativnim rizikom. Aktivnosti redovnog praćenja mogu rezultirati brzim otkrivanjem i ispravljanjem nedostataka u politikama, procesima i postupcima upravljanja operativnim rizikom. Brzo otkrivanje tih nedostataka i bavljenje sa njima može značajno smanjiti potencijalnu učestalost i/ili ozbiljnost pojave gubitaka.

Pregled okvira - Praćenje

Praćenje je periodican i integrisan proces:



Slika 13. Praćenje

Osim praćenja slučajeva operativnog gubitka, banke treba da utvrde koji će pokazatelji dovoljno rano upozoriti na uvećani rizik od nastanka budućih gubitaka. Ti pokazatelji (često se nazivaju i ključni pokazatelji rizika ili pokazatelji ranog upozorenja) treba da budu usmereni ka napred, a mogu odražavati potencijalne izvore operativnog rizika, kao što su na primer, brz rast, uvođenje novih proizvoda, promet po zaposlenom, prekidi transakcija, razdoblje u kome je sistem van upotrebe itd. Kada su pragovi direktno povezani sa ovim pokazateljima, delotvoran proces praćenja može na nedvosmislen način pomoći u utvrđivanju ključnih značajnih rizika i time omogućiti banci da primereno postupi prema tim rizicima.

Učestalost praćenja treba da odražava prisutne rizike, kao i učestalost i prirodu promena u poslovnom okruženju⁴⁸. Praćenje treba da bude sastavni deo aktivnosti banke. Rezultati tih pratećih aktivnosti banke treba da budu sadržani u redovnim izveštajima upravi i odboru, kao i rezultati preispitivanja poštovanja pravila koje je sprovedla funkcija nadležna za nadzor mogu takođe sadržati informacije o tom praćenju, a o njemu trebaju biti obavešteni i viša uprava i odbor, prema potrebi.

Viša uprava treba da prima redovne izveštaje od odgovarajućih delova banke, npr. od poslovnih jedinica, funkcija grupe, odeljenja za upravljanje operativnim rizikom i unutrašnje revizije. Izveštaji o operativnom riziku treba da sadrže unutrašnje finansijske i operativne podatke, kao i podatke o poštovanju pravila, informacije o spoljašnjem tržištu koje se odnose na događaje i uslove koji su relevantni za donošenje odluka. Izveštaji trebaju biti dostavljeni odgovarajućim nivoima uprave i delovima banke na koja problematična područja mogu uticati. Izveštaji treba da nedvosmisleno upozoravaju na područja u kojima su utvrđeni problemi. Kako bi se osigurala pouzdanost i korisnost tih izveštaja o reviziji i riziku, uprava treba da redovno proverava pravovremenost, tačnost i relevantnost sistema izveštavanja i unutrašnjih kontrola uopšte. Uprava se takođe može poslužiti izveštajima koja su pripremili spoljašnji izvori (revizori, supervizori) kako bi procenila korisnost i pouzdanost unutrašnjih izveštaja. Izveštaje treba analizirati u cilju poboljšanja postojeće uspešnosti upravljanja rizikom, kao i radi razvoja novih politika, postupaka i praksi upravljanja rizikom.

3.4. OBLASTI UPRAVLJANJA OPERATIVNIM RIZIKOM

U poslednjih nekoliko decada mogućnosti informacione tehnologije da olakša poslovne procese organizacionih entiteta dramatično su se uvećale, zbog čega je širenje njihove primene dostiglo neočekivane razmere. Upravo iz tih razloga biznis postaje sve zavisniji od ove tehnologije, pa je posledično nastala i rapidno se širila i potreba zaštite informacionih dobara. Ta potreba se vremenom transformisala u zahtev koji je postao imperativan u sadašnjem, ali za verovati je da će takav ostati i u budućem korišćenju ove tehnologije.

U ranijim vremenima, dok su sistem i računarska mreža bili izolovani od spoljnih uticaja, zaštitom su se bavila tehnička lica, takoreći van vidnog polja ostalih zaposlenih. Za njih se znalo samo ako dođe do ispada sistema i prekida u radu. Međutim, kada su organizacioni entiteti izašli iz svog lokalnog okruženja i počeli da se povezuju sa drugim mrežama i sistemima – problem zaštite je dobio sasvim nove dimenzije. Broj mogućnosti i broj pretnji se dramatično uvećao i pitanje zaštite je moralo da izađe iz informatičkog sektora i da se proširi na ceo organizacioni entitet.

Za top-menadžment informaciona bezbednost postaje jedno od strateških pitanja čije uspešno razrešavanje obezbeđuje stabilno i perspektivno funkcionisanje kompanije. Imajući tu činjenicu u vidu jasna je potreba da se ovo pitanje razrešava osmišljeno, kvalitetno i celovito. Navedene konstatacije su i jasne i obavezujuće, ali kada je reč o

⁴⁸ British Bankers' Association, International Swaps and Derivatives Association and Robert Morris Associates (2000), Operational Risk Management - The Next Frontier, The Journal of Lending & Risk Management, March, pp.38-44.

konkretizaciji ostaje i dalje otvoreno pitanje KAKO? Odgovori na ovo pitanje, posebno kada je reč o praksi, veoma su raznoliki, često nelogični, nerazumljivi, kontradiktorni, nerealni, neprimenjivi, ...

Pojam informacione bezbednosti (IB) je nastao u SAD na osnovama teorije informacionog ratovanja (IW - *information warfare*).

Modeli informacione bezbednosti su aproksimativni okviri koji, na očigledan način, kvalitativno i kvantitativno predstavljaju problematiku informacione bezbednosti.

1. Kvalitativni modeli informacione bezbednosti

Integralni model informacione bezbednosti

Integralni model informacione bezbednosti (McCumber INFOSEC model) je prvi put publikovan 1991. godine. Reč je o modelu zasnovanom na integralnom prilazu svim aspektima informacione bezbednosti⁴⁹. U skladu, sa tada važećom definicijom informacione bezbednosti, definisane kao: «**zaštita** informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija bilo u skladištenju, obradi ili prenosu i protiv **lišavanja** usluga autorizovanih korisnika, uključujući neophodne mere detekcije, dokumentovanja i otklanjanja takvih pretnji, model informacione bezbednosti tretira tri aspekta:

1. **stanje** u kojima se nalaze informacije (prenos, čuvanje i obrada),
2. **bezbednosne usluge** (raspoloživost, integritet i poverljivost) i
3. **bezbednosne protivmere** (u oblasti tehnologija, politika i procedura kao i obuke)

Ovako definisan model je trodimenzionalan.

Model informacione garancije

Model informacione garancije (IA) predstavlja novi, multidisciplinarni i multidimenzionalni pogled na važne elemente McCumber-ov modela.

Informaciona garancija je definisana kao: «**Informacione operacije zaštite i odbrane** informacija i informacionih sistema obezbeđujući njihovu raspoloživost, integritet, autentičnost, poverljivost i neporicijivost. Ovo podrazumeva **restauraciju** informacionih sistema inkorporiranim mogućnostima zaštite, detekcije i reakcije».

Za razliku od informacione bezbednosti, informaciona garancija je definisana kao **informacione operacije** sa skupom svih odbrambenih i proaktivnih komponenti što njihovu razliku čini suštinskom, a ne samo semantičkom. Informaciona garancija obuhvata ulogu informacione bezbednosti.

Informaciona garancija je proširila listu bezbednosnih zahteva (poverljivost, raspoloživost i integritet) i na svojstva informacija kao što su autentičnost (*authentication*) i neporicijivost (*non-repudiation*). Pored navedenih bezbednosnih servisa, informacionu garanciju (IA) karakterišu operativnost (*operational in nature*) i osetljivost na vreme (*time-sensitive*).

Ešelonirani model informacione bezbednosti

⁴⁹ Maconachy V., Schou C., Ragsdale D., Welch D., A model for Information assurance: an integrated approach, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, 2001

Sa svakim novim dostignućem u oblasti informacionih tehnologija (npr. «virtuelna organizacija» x) javljaju se novi aspekti informacione bezbednosti. Jedan od primera «virtuelnih organizacija» je **Globalna informaciona mreža** (GIG – *global information grid*) nastala za potrebe Pentagona koja treba da omogući upravljanje mobilnim i kompaktnim borbenim sastavima.

Klasični modeli IB zasnovani na autonomnosti i lokalnosti resursa IS, ne zadovoljavaju savremene network-centric zahteve. Rešenje je ešelonirani, višeslojni model IBxi. Koncept ešeloniranog modela obuhvata skup komponenata koje realizuju funkcije monitoringa, zaštite i adaptacije informacionih resursa.

Kako savremena teorija i praksa informacione bezbednosti zahteva racionalan pristup, koji omogućava efikasno korišćenje svih raspoloživih resursa (ljudski, finansijski i materijalni), to ečelonirani model mora zadovoljiti i uslove **adaptivnog upravljanja bezbednošću** (*adaptive network security*)xii zasnovanog na **koncepta upravljanja rizikom**.

Model zaštitnih prstenova

Model ešelonirane višeslojne informacione bezbednosti svoju detaljnu, preglednu i lako shvatljivu razradu, na nivou pojedinačnog informacionog sistema, dobio je u **modelu zaštitnih prstenova**⁵⁰ koji, IB IS, razmatra sa više aspekata: pravne norme, organizacione mere, mere neposredne zaštite, zaštita opreme, zaštita programske podrške i zaštita baza podataka.

Zaštitni prstenovi su: **humani prsten** (personal koji radi sa svojim motivima, spremnošću i mogućnošću delovanja), **normativni prsten** (obavezuje i propisuje izvršenje i način izvršenja neke radnje, definisan matricom ovlašćenja), **organizacioni prsten** (mere i aktivnosti, nadležnosti i obaveze korisnika i izvršilaca), **prsten fizičke zaštite** (onemogućava fizički pristup napadača), **zaštita softvera** (kontrolisano čuvanje i kopiranje operativnog sistema i aplikativnih programa), **zaštita (rezidentnih) podataka** (obuhvata ograničenje pristupa podacima, evidentiranje pristupa podacima i sprečava neovlašćeni pristup podacima), **zaštita infrastrukture** (obezbeđuje optimalne uslove za funkcionisanje svih komponenti IS), **protivpožarna zaštita** (građevinske mere, primena odgovarajućih sredstava za gašenje i obuku osoblja), **zaštita IS u radu u mrežnom okruženju** (kontrola pristupa mreži i kriptozastita poruka koje se prenose u difuznoj računarskoj mreži) i **kriptozastitni bezbednosni prsten** (kriptozastita podataka tranzicijom ili supstitucijom).

U modelu zaštitnih prstenova uočavamo, na nivou pojedinačnog informacionog sistema, ešeloniranu po dubini zaštitu informacija. Model pokriva široku lepezu mogućih napada što je karakteristično za uslove savremenog življenja. U njemu se vide i elementi integrisanih sistema.

Na višem nivou uopštavanja zaštitne prstenove možemo definisati kao: legalnu i društvenu kontrolu (pravni okvir), administrativnu kontrolu (organizacione mere), fizičku zaštitu i kontrolne procedure u sistemu.

Model sa objektno-orijentisanim prilazom informacionoj bezbednosti

⁵⁰ D. K. Hsiao, D.S. Kerr, S.E. Madnik, Computer security, Academic Press, New York, san Francisko, 1979

Rodić B., Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija (*doktorska disertacija*), Vojnotehnička akademija, Beograd, 2001

Prema shvatanju V. Galatenka informaciona bezbednost je **zaštićenost** informacija i podržavajuće infrastrukture od slučajnih ili namernih dejstava prirodnog ili veštačkog karaktera koja mogu naneti **neprihvatljive gubitke subjektima informacionih odnosa** pa, u tom smislu, i vlasniku i korisniku informacija kao i podržavajućoj infrastrukturi.

Definicija uvodi kategorije *informacionih odnosa* (između različitih subjekata sa različitim interesima) i *neprihvatljivih gubitaka* (apsolutna zaštita ne postoji zbog čega se uvodi upravljanje rizicima koje podrazumeva uvođenje praga prihvatljivosti gubitaka – obično materijalno izraženi).

Polazeći od činjenice da su informacioni sistemi uglavnom bazirani na kompjuterima i tehnikama programiranja, V. Galatenko smatra da je u tretiranju IB, umesto strukturnog prilaza, potrebno koristiti najsavremenije tehnologije programiranja – objektno- orijentisano (OO) programiranje.

Savremeni informacioni sistemi predstavljaju distribuirani skup uzajamno delujućih objekata. Svaki objekat pruža drugom objektu neke usluge (servise). U ovako tretiranom pojmu IS, informaciona bezbednost je obezbeđena sledećim servisima: identifikacija/autentifikacija, razgraničenje pristupa, protokoliranje/audit, ekraniranje, tuneliranje, enkripcija, kontrola integriteta, kontrola zaštićenosti, detekcija i neutralizacija otkaza, operativna restauracija i upravljanje.

Objektna dekompozicija (ponašanje sistema se opisuje u terminima uzajamnog delovanja objekata) i principi OO programiranja (detaljizacija, nasleđivanje, polimorfizam i inkapsulacija) omogućavaju da se cilj IB (svojstva informacija: raspoloživost, integritet i poverljivost) i sredstva za njegovo postizanje (zakonodavne mere, administrativne mere, proceduralne mere i programsko-tehničke mere) predstave tzv. granama (nitima) OO programiranja (relativno nezavisne karakteristike objekata).

Servise bezbednosti se objedinjavaju, u cilju dizajniranja **ešelonirane odbrane**, metodama OO programiranja – pomoću aktivnih agenata. Na svojstvima objekata, kontejnera i unikalnih identifikatora, formiraju se funkcionalni paketi, bazni i izvedeni profili zaštite u skladu sa standardima u oblasti informacione bezbednosti.

Konceptualni model informacione bezbednosti

Shvatanje pojma informacione bezbednosti u širem smislu prisutno je u konceptualnom modelu istraživača iz domena društvenih nauka (A.D.Ursul i T.N. Cirdja).

Konceptualni model informacione bezbednost je zasnovan na sledećim postavkama. Informaciona bezbednost je bezbednost u informacionoj sferi - **infosferi**. Fizički infosfera se sastoji od tri elementa: informacione infrastrukture (uređaji za prenos i obradu informacija), informacija i njihovih tokova i personala koji obavlja različite delatnosti.

Informaciona sfera je nastala kao posledica nastanka nove društvenoekonomske formacije društva – informacionog društva. Nova društveno-ekonomska formacija društva povlači za sobom i nove suprotnosti i nove pretnje (opasnosti). Nove pretnje iziskuju nove pristupe. U domenu informacione sfere, s jedne strane, potrebno je obezbediti društvo informacionim resursima a, sa druge strane, formirati sistem zaštite informacionih potencijala. Imperativ informacionog društva je informaciona dominacija

u životno važnim oblastima. **Osnovni sukob informacionog društva je je sukob u mogućnosti pristupa informacijama**⁵¹.

Ako je bezbednost odsustvo pretnji ili mogućnost pouzdane zaštite od njih⁵², onda je «informaciona bezbednost odsustvo informacionih pretnji, ili stanje zaštićenosti, i stabilnost osnovnih sfera ljudskih delatnosti u odnosu na moguća informaciona dejstva». U tom kontekstu informaciona bezbednost je svojstvo socijalnog sistema pozvana da garantuje takvo stanje informacionih pojava koje obezbeđuju čoveku i društvu u celini informacione uslove preživljavanja i daljeg stabilnog razvoja. Informaciona bezbednost se rasprostire na sve pojave infosociosfere čiji elementi, direktno ili indirektno, «rade» na optimalnoj evoluciji društvenog sistema obezbeđujući uslove za bezbedan razvoj a samim tim i progres.

Na taj način «informaciona bezbednost je **spособnost** države, društva, socijalnih grupa i ličnosti:

1. *da obezbede sa određenom verovatnoćom dovoljne i zaštićene informacione resurse i socijalni intelekt, optimalnu socijalnu entropiju i infosferu za podršku životnih delatnosti i životnih sposobnosti, stabilnog funkcionisanja i razvoja sociuma,*

2. *da se suprotstave informacionim pretnjama i napadima, negativnim informacionim delovanjima na individualno i društveno znanje i psihi ljudi kao i na računarske mreže i druge tehničke izvore informacija,*

3. *da formiraju lične i grupne navike umeća bezbednog ponašanja,*

4. *da podrže konstantnu raspoloživost u odnosu na adekvatne mere informacione protivodbrane,*

5. *da konstantno i, po određenom programu bezbednosti, iterativno inkorporiranje veštačku inteligenciju u socisredinu.*

U takvoj interpretaciji, **informaciona bezbednost se javlja ne samo kao jedan od oblika bezbednosti, već i kao presek svih tih oblika u sferi delovanja u kojima informacione tehnologije zauzimaju važno mesto**».

Sistemske prilaze obezbeđenja informacione bezbednosti u infosferi obuhvata tri eline:

1. *humanitarnu* povezanu sa razvojem duhovne sfere društva i pravima građana u oblasti informacionih delatnosti (formiranje i korišćenje informacionih resursa),

2. oblast *informatizacije* (formiranje i razvoj jedinstvenog informacionog prostora regiona, zemlje i svetskog informacionog polja) i

3. oblast obezbeđenja bezbednosti funkcionisanja *informacione infrastrukture*.

Sistemske prilaze u objašnjenju suštine i sadržaja pojma informacione bezbednosti predstavljen je u **konceptualnom modelu**.

⁵¹ А.Д.Урсул, Т.Н. Цырдя, Информационная безопасность, сущность, содержание и принципы ее обеспечения, журнал Факт № 2, 2000

⁵² П.В. Константинович, От информационных войн к управляемой конфронтации и сотрудничеству, журнал Факт № 9, 2001

Informacija	
Izvori informacija	ljudi, dokumenta, publikacije, sredstva masovnih informacija, tehnički nosioci (medijumi), tehnička sredstva, proizvodnja, proizvodni otpadci
Pretnje (opasnosti)	integritetu, poverljivosti, potpunosti, pouzdanosti pristupa
Izvori napada	protivnici, konkurenti, prestupnici, korupcioneri, strukture vlasti
Ciljevi	upoznavanje, modifikacija, uništavanje
Objekti napada	podaci o sastavu, stanju i delatnostima
Načini pristupa	na račun razglašavanja, na račun oticanja, na račun neovlašćenog pristupa
Pravci zaštite	pravni, organizacioni, tehnički
Sredstva zaštite	fizička, hardverska, softverska, kriptografska
Metode zaštite	predupređenje, odvrćanje, presecanje, protivdejstva

Model integralne zaštite informacija

Model integralne zaštite informacija je zasnovan na konceptu **integralne bezbednosti** (D.V.Barsukov).

Osnovni smisao pojma integralne bezbednosti se sastoji u *neobhodnosti obezbeđenja takvog stanja uslova funkcionisanja čoveka, objekata i informacija* u kom su oni pouzadno zaštićeni od svih realnih vidova pretnji u toku neprekidnog proizvodnog procesa i svih životnih delatnosti. Naime, u svakodnevnom životu ljudi se susreću sa različitim vrstama bezbednosti: od požara, ličnoj, finansijskoj, ekološkoj itd. Naravno, ovakva podela je uslovna. *Ako posmatramo informacije, jasno je da je njihova efikasna zaštita moguća samo u tom slučaju ako je bezbednost, od svih vrsti pretnji, garantovana ne samo podacima, već i uređajima u kojima se oni obrađuju i čuvaju, kao i licima koji rade sa tim podacima*⁵³.

2. Kvantitativni modeli informacione bezbednosti

Kvantitativni model Džozefa Bogarda

Kvantitativni model Džozefa Bogarda (Josef Beauregard) je zasnovan na metodologiji fokusiranog vredonosnog mišljenja (VFT – *value focused thinking*) i modelu IAAM (*information assurance analysis model*).

Model IAAM omogućava trodimenzionalno razmatranje problema informacione garancije.

⁵³ Барсуков Д., Интегральная защита информации, "Электроника. Наука, технология, бизнес" № 3-4, 1998г.

Informaciona garancija je proces koji uključuje sposobnost zaštite informacija i informacionih sistema, detekciju događaja koji mogu interferirati sa informacijama i IS i osobinu reakcije u nastaloj neželjenoj situaciji podrazumevajući i sposobnost restauracije osnovnih funkcija sistema. Ovako definisana IA nije sinonim za kompjutersku bezbednost. Reč je o mnogo širem, robusnom konceptu koji obuhvata celokupan proces zaštite informacija, informacionog sistema i informacionog procesa.

3.4.1. Upravljanje informacionim sistemom

Informaciona bezbednost (IB) je, kao jedan od novijih pravaca istraživanja u sferi bezbednosti, posledica tehnološkog razvoja i odraz novog pogleda na svet. Ona se javlja ne samo kao jedan od vidova (oblika) bezbednosti, već i kao presek svih drugih vidova bezbednosti u kojima informacione tehnologije zauzimaju važno mesto. O značaju informacione bezbednosti govori i činjenica da je ona postala jedna od osnovnih komponenta nacionalne bezbednosti.

Informaciona bezbednost je definisana kao: ***zaštita** informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija bilo u čuvanju, obradi ili prenosu i protiv **lišavanja** usluga autorizovanih korisnika, uključujući neophodne mere detekcije, dokumentovanja i otklanjanja takvih pretnji*⁵⁴.

Informacionu bezbednost je moguće definisati i na drugačiji način, kao npr. *informaciona bezbednost je **zaštićenost** informacija i podržavajuće infrastrukture od slučajnih ili namernih dejstava prirodnog ili veštačkog karaktera koja mogu naneti **neprihvatljive gubitke subjektima informacionih odnosa** pa, u tom smislu, i vlasniku i korisniku informacija kao i podržavajućoj infrastrukturi*⁵⁵.

Postoji dosta termina koji se koriste da definišu pojam rizika vezanog za informatiku, odnosno informatičkog rizika. ISF (Information Security Forum) definiše informatički rizik kao mogućnost ili verovatnoću poslovne štete kao rezultat gubitka poverljivosti, integriteta ili dostupnosti informacija⁵⁶.

Analiza informatičkih rizika je proces određivanja mogućeg poslovnog gubitka, procenom pretnji i ranjivosti i izbora odgovarajućih kontrola (mera zaštite) da bi se postigli poslovni zahtevi za informatičkom bezbednošću na troškovno efikasan način. Analiza rizika je proces i sprovodi se kroz niz određenih koraka. Poslovni gubitak (business impact) je priroda i nivo gubitka koji organizacija može iskusiti kroz gubitak poverljivosti, integriteta ili dostupnosti informacija. Pretnje su mogućnosti da poverljivost, integritet i dostupnost informacija budu ugroženi.

Ranjivosti su slabosti i okolnosti koje se mogu kontrolisati, a koje povećavaju mogućnost događanja bezbednosnog incidenta. Mere IT bezbednosti i zaštite (ili

⁵⁴ Podržavajuća infrastruktura podrazumeva sisteme elektro-, vodo- i toplotnog snabdevanja, kondicionere, sredstva komunikacija i, konačno, osoblje.

⁵⁵ Definicija uvodi kategorije informacionih odnosa između različitih subjekata sa različitim interesima i neprihvatljivih gubitaka. Apsolutna zaštita ne postoji i zbog toga se uvodi upravljanje rizicima koje podrazumeva uvođenje praga prihvatljivosti gubitaka – obično materijalno izraženih. В.Галатенко, Основы информационной безопасности, Институт ИТ, Москва

⁵⁶ Information Risk Management in Corporate Governance, ISF Workshop, 2003.

kontrole) su politike, pravila, metode, procedure, uređaji, softver ili programski mehanizmi koji se koriste radi saniranja ranjivosti⁵⁷.

Potreba da se sprovede analiza informatičkih rizika mogu se sagledati prema poslovnom uticaju, pretnjama i ranjivostima ili merama zaštite:

U odnosu na poslovni uticaj analiza rizika može održati svest u organizaciji o kritičnim sistemima, sačiniti prioritete, definisati poslovne potrebe za informatičkom bezbednošću i doprineti razumevanju mogućih gubitaka.

Analiza rizika identifikuje slabosti (weakness) u oblasti IT bezbednosti i zaštite i tipove pretnji, doprinosi razumevanju pretnji informacionom sistemu i proceni verovatnoće događanja incidenta.

Analiza rizika određuje najefektivnije mere IT bezbednosti i zaštite, pomaže u identifikovanju potreba za sprovođenje mera, proceni uspešnosti investicija (ROI) i opravdavanju uvođenja novih mera.

Analiza informatičkih rizika je deo šire analize poslovnih rizika u organizaciji, mada u velikoj meri može biti sprovedena samostalno.

ANALIZA POSLOVNIH RIZIKA

Rizici informatičke bezbednosti se mogu posmatrati kao operativni rizici poslovanja. U ovakve rizike spadaju prekidi poslovnih procesa, nedostaci u kontroli, greške, omaške i spoljni događaji. Osnovne klase operativnih rizika su:

- Ljudski rizici (npr. greške, omaške, nesporazumi)
- Povezani rizici (npr. naplaćene kazne)
- Tehnološki rizici (npr. kvarovi informacionih tehnologija, rizici informatičke bezbednosti)
- Fizički rizici (npr. oštećenje imovine)
- Ostali eksterni rizici (npr. prevara, promena zakona).

Prema drugoj podeli, rizici kojima treba u organizaciji upravljati mogu biti:

- strateški
- informatički
- vezani za reputaciju i ugled
- tehnološki
- tržišni
- operativni
- kreditno/finansijski
- kadrovski
- legalni.

Prema definiciji ICGN (International Corporate Governance Network), organizacije pod pokroviteljstvom OEBS-a: Upravni odbor (the board) treba da zna gde postoji rizik i šta sve rukovodstvo čini da ga smanji. Upravni odbor preduzeća treba da osigura da je odgovornost pravilno raspodeljena. Upravljanje rizikom je ključna komponenta unutrašnje kontrole.

Mnoge organizacije se već godinama suočavaju sa upravljanjem rizikom. Tradicionalna struktura upravljanja rizikom kod ovakvih organizacija zavisi od jake

⁵⁷ IRAM Training Presentation Pack, ISF, 2007.

interne revizije, izveštavanja rukovodstva o organizacionim rizicima i izveštavanja izuzetaka upravnom odboru, obično kroz audit komitet. Ono što je nedostatak ovakve strukture je mogući zaostatak u rešavanju problema (post-festum izveštavanje i korektivne akcije). Interna revizija, osim toga, teži da se fokusira na izuzetke u rešavanju problema pre nego na pojedinačne rizike.

Postoji veliki broj organizacija koje se opredeljuju za drugačiju strukturu koja omogućava sakupljanje informacija o riziku kako one nastaju i njihovu asimilaciju na jednom mestu. Takva alternativna struktura ustanovljava funkciju koordiniranja rizika i slanja informacija upravnom odboru preko komiteta za rizik i upravljača rizikom (risk committee and risk officer). Funkcija koordinacije rizikom nije odgovorna za upravljanje rizikom – ta odgovornost se prepušta pojedinačnim izvršnim funkcijama. Uloga funkcije koordinacije je da postavi standarde za upravljanje rizikom, izveštavanje o riziku i integritet celog procesa.

ANALIZA RIZIKA U OKVIRU USPOSTAVLJANJA ISMS

Koncept uspostavljanja sistema za upravljanje informatičkom bezbednošću ISMS (Information Security Management System) se bazira na standardu ISO 27001 iz 2005. godine i obuhvata definisanje odgovarajuće politike prilagođene konkretnoj organizaciji. ISMS se uspostavlja na osnovu usklađenosti sa kontekstom strateškog upravljanja rizikom i specifikacije kriterijuma u odnosu na koje se procenjuje rizik⁵⁸.

Analiza rizika se sprovodi u okviru prve i najznačajnije faze planiranja ISMS-a i njeno sprovođenje je obavezno. Međutim, ne postoji obavezujuća metodologija kojom bi se analizirao rizik u okviru uspostavljanja ISMS⁵⁹. Analiza rizika se sprovodi posle definisanja granica sistema u kome se upravlja informatičkom bezbednošću i kreiranja politike informatičke bezbednosti najvišeg nivoa. Pristup proceni informatičkih rizika u organizaciji mora da obuhvata:

- Identifikovanje odgovarajuće metodologije analize rizika
- Razvijene kriterijume po kojima se rizik prihvata
- Identifikovanje prihvatljivog nivoa rizika
- Sigurnost da procene rizika daju rezultate koji se mogu međusobno porediti i koristiti za druge analize.

Identifikovanje informatičkih rizika uključuje identifikovanje:

- Sredstava (assets) i „vlasnika“ sredstava u okviru ISMS
- Pretnji navedenim sredstvima
- Ranjivosti koje te pretnje mogu iskoristiti
- Posledica (impacts) koje se mogu osetiti u gubitku poverljivosti, integriteta i dostupnosti navedenih sredstava.

Pod „vlasnikom“ sredstava podrazumeva se lice koje je odgovorno za sprovođenje poslovnih funkcija povezanih sa odgovarajućim sredstvima.

Pretnje su definisane kao potencijalni uzroci neželjenih incidenata koji mogu imati za posledicu oštećenje sistema ili organizacije. Ranjivosti su slabosti na sredstvu ili grupi sredstava, koje bi pretnje mogle iskoristiti. Ranjivost sama po sebi ne prouzrokuje

⁵⁸ Ivan Vukadinović: Uspostavljanje sistema za upravljanje informatičkom bezbednošću, Infotech 2006.

⁵⁹ ISO 27001:2005 ISMS Implementation, BSI Management Systems, 2007.

oštećenje, to je uslov ili skup uslova koji mogu imati za posledicu ostvarenje neke pretnje.

Rezultati analize rizika su:

- Identifikovanje bilo kakvog značajnog rizika prema svim navedenim sredstvima u kontekstu njihove upotrebe.

- Razumljiv i iscrpan izveštaj rukovodstvu

- Izveštaj bi trebalo da rangira rizike prema mogućnosti poslovnog gubitka

- Trebalo bi da identifikuje brza rešenja, gde god je moguće smanjiti rizike brzo i uz mala ulaganja

- Gde je moguće, trebalo bi da identifikuje alternativna rešenja.

Dalji korak je identifikovanje i procena opcija tretiranja rizika u kontekstu poslovnog okruženja:

- Primena odgovarajućih kontrola (mera zaštite)

- Prihvatanje rizika

- Izbegavanje rizika

- Transfer rizika

Mere zaštite se implementiraju na osnovu ISO 27001. Izbor mera zaštite uključuje i one koje se već koriste, odnosno njihovo uklanjanje ili unapređenje. Izbor mera zaštite može da da predlog dodatnih mera. Konačni rezultat ovog procesa je Izjava o primenljivosti (Statement of Applicability) –dokument koji opisuje ciljeve i mere zaštite koje su relevantne i sprovodljive za konkretan ISMS.

INFORMATION SECURITY FORUM (ISF)

ISF je renomirana međunarodna organizacija koja se bavi poboljšanjem IT bezbednost i zaštite. Članovi ISF-a su preko 250 organizacija, uključujući banke, vladine institucije, informatička preduzeća i telekomunikacione provajdere. Telekom Srbija je jedini član ISF-a u našoj zemlji i okruženju. ISF sprovodi razne aktivnosti, kao što je anketiranje (Survey) svojih članica o stanju IT bezbednosti i zaštite, radionice, godišnji kongresi i bavljenje specifičnim pitanjima, gde spada i analiza informatičkog rizika. Na osnovu svojih aktivnosti ISF kreira Standard dobre prakse koji uključuje relevantne oblasti IT bezbednosti i zaštite.

U okviru svog standarda ISF veliku pažnju posvećuje upravljanju informatičkim rizikom sa sledećim zahtevima da:

- Struktura upravljanja informatičkim rizicima pokriva celu organizaciju.

- Proces dodeljivanja informatičkih rizika je konzistentan i obuhvata prirodu rizika, verovatnoću ostvarenja i cost-benefit analizu.

- Ustanovljavanje nivoa prihvatljivog rizika, adekvatno obaveštavanje i sprovođenje kontrolnih mera.

- Proces regularnog izveštavanja sa mogućnošću povratne informacije.

- Proces interne i eksterne komunikacije⁶⁰.

Na osnovu dugogodišnjeg bavljenja analizom informatičkih rizika, i ranijih alata SPRINT i SARA, ISF je razvio IRAM pristup. S obzirom da obuhvata anketiranje o pojavi bezbednosnih incidenata i stanja IT bezbednosti i zaštite, i upoređivanje sa

⁶⁰ Ivan Vukadinović: Telekom član Information Security Foruma, JISA 2004.

podacima dobijenim od drugih organizacija članica, Survey se može koristiti kao značajna podrška u procesu upravljanja informatičkim rizicima.

IRAM

IRAM (Information Risk Analysis Methodology) je pristup analizi informatičkog rizika koji je razvio ISF (Information Security Forum). Ovaj pristup uključuje odgovarajuću metodologiju, podršku i alate. Alati su bazirani na Excel tabelama koje obuhvataju analizu poslovnih gubitaka, pretnji, ranjivosti i izbor mera za smanjenje informatičkih rizika.

Karakteristike IRAM pristupa su:

- Jasnost i jednostavnost metode.
- Dokumentovanost svake faze primene metodologije.
- Nepostojanje skrivenih algoritama ili „magičnih formula“
- Baziranost na više izvora informacija – zasnovan je na znanju
- Potpuno beleženje odluka i pretpostavki za dalje analize
- Primarna orijentacija na sisteme (aplikacije, sistemski softver, podatke, baze podataka, hardver, računarsku mrežu).

Ovako definisan pristup analizi informatičkog rizika zahteva visok nivo znanja o sistemu i spoljnim okolnostima ljudi koji procenjuju rizike u organizaciji. Analitičar rizika sam procenjuje značaj unetih podataka i procena, uz minimalnu asistenciju softvera. Odgovarajuće predefinisane matrice omogućavaju procenu ukupnog nivoa rizika na osnovu pretnji, ranjivosti i poslovnog uticaja. Tako se dobija lista najvećih informatičkih rizika koji prete organizaciji.

IRAM se sastoji iz tri faze:

- BIA (Business Impact Analysis) – procena mogućeg poslovnog gubitka u slučaju ugrožavanja poverljivosti, integriteta i dostupnosti podataka.
- T&VA (Threat and Vulnerabilities Analysis) –procena nivoa pretnji, ranjivosti i ukupnog rizika.
- CS (Control Selection) – analitička pomoć u izboru mera IT bezbednosti i zaštite koje treba sprovesti.

ANALIZA MOGUĆEG POSLOVNOG GUBITKA (BIA)

BIA (Business Impact Analysis) je jednostavan, poslovno orijentisan alat za definisanje koliko su u odgovarajućim granicama sistema (informacionog sistema koji se analizira, odnosno ISMS-a) bitni poverljivost, integritet i dostupnost podataka. Značaj ovih elemenata IT bezbednosti i zaštite se dobija na osnovu procene poslovnih gubitaka koji mogu nastati ako svaki od njih pojedinačno bude ugrožen.

Mogući poslovni gubitak se ocenjuje na skali od A do E (very high – very low). Poslovni gubitak ocenjuje se za vremenski period u kome podaci nisu dostupni. Izraženi su gubici finansijski, operativni, povezani sa korisnicima i ljudskim resursima. Rezultat ocenjivanja je značaj svakog od navedenih faktora i period u kome je dostupnost okruženja kritična. Značaj faktora analitičar određuje prema najvećem pojedinačnomgubitku. Alat to ne određuje automatski, pa je analitičar slobodan da donese svoju odluku.

Rezultat analize je konačna procena ugroženosti sistema u odnosu na gubitak poverljivosti, integriteta i dostupnosti podataka. Dobija se i kritični raspon vremena koji nam govori posle kog vremena gubitak dostupnosti podataka postaje kritičan. Predlog sledećih akcija, na osnovu ove faze analize, je:

-U slučaju niskog poslovnog gubitka (D, E) okončava se proces analize rizika i sprovode se osnovne mere IT zaštite.

-U slučaju srednjeg poslovnog gubitka (B, C) sprovodi se standardna analiza pretnji i ranjivosti.

-U slučaju visokog poslovnog gubitka (A) sprovodi se detaljna analiza pretnji i ranjivosti.

Podaci dobijeni sprovođenjem BIA su ulazni parametri za sledeći korak u analizi rizika, a to je procena nivoa pretnji, ranjivosti i ukupnog rizika

PROCENA NIVOA PRETNJI, RANJIVOSTI I UKUPNOG RIZIKA (T&VA)

T&VA (Threat and Vulnerabilities Analysis) je alat za određivanje verovatnoće incidenata, baziran na proceni pretnji i ranjivosti. Koristi se niz upita, interni podaci, podaci ISF-a i eksterni podaci kroz relevantne Internet adrese. T&VA je tehnički orijentisana aktivnost procene rizika. Procene rizika su u velikoj meri zavisne od ekspertize analitičara. Nedostatak ovog alata je mala asistencija od strane softvera, jer i listu od 10 najvećih rizika analitičar unosi sam. T&VA se sprovodi kroz niz koraka, što praktično znači popunjavanje odgovarajućih Excel tabela. Ti koraci su:

- Procena pretnji
- Procena ranjivosti
- Provera verovatnoće rizika
- Određivanje nivoa rizika
- Utvrđivanje ukupnih rezultata i sledećih koraka[2].

Procena pretnji se sprovodi tako što se prvo odrede pretnje koje su relevantne za granice sistema. Ulazni podaci za procenu su podaci dostavljeni od strane ISFa (anketiranje organizacija članica), interni podaci same organizacije i eksterni podaci (Internet), od kojih su za neke pretnje već obezbeđene korisne Internet adrese. Analitičar rizika sam procenjuje ukupan nivo pretnji.

Za svaku relevantnu pretnju, procenjuje se ranjivost sistema koja bi joj omogućila da se ispolji. Ranjivosti se procenjuju na osnovu analize postojećih mera zaštite (control analysis) i analize okruženja, sistema i tehnologije. Ulazni podaci za procenu ranjivosti dobijaju se korišćenjem alata Security Healthcheck koji služi za procenu sprovedenih mera IT zaštite i njihovo poređenje sa relevantnim standardima (COBIT, ISO 17799). Analitičar rizika sam procenjuje ukupan nivo ranjivosti.

Ukupna verovatnoća rizika se izračunava automatski na osnovu matrice verovatnoće rizika (Likelihood Reference Table) koja uparuje odgovarajuće vrednosti nivoa pretnji i ranjivosti. Ukupna verovatnoća rizika se može promeniti promenom u matrici verovatnoće rizika.

Ukupan nivo rizika se automatski izračunava na osnovu verovatnoće rizika i procene poslovnog gubitka, dobijene na osnovu BIA, po odgovarajućoj matrici

(Information Risk Reference Table), koju je moguće prilagođavati sopstvenim potrebama.

Izračunati ukupni nivo rizika analitičar može prihvatiti ili ga eventualno sam promeniti. Konačni rezultat ove faze je profil informatičkog rizika koji se dobija za sledeće grupe rizika:

- Eksterni napadi
- Interne zloupotrebe i greške
- Krađe
- Sistemske otkazi
- Prekidi servisa
- Ljudske greške
- Nepredviđeni rezultati promena

Na osnovu ukupnog nivoa rizika donosi se odluka o tome da li će se sprovesti samo osnovne ili neke specijalizovane mere IT zaštite. Rezultati T&VA su ulaz u narednu fazu primene IRAM metode – izbor mera IT zaštite koje treba sprovesti.

3.4.1.1. Sigurnost informacionog sistema

Mnoge zemlje u svetu su definisale politiku upravljanja rizicima vezano za svoje informacione sisteme. Australija je jedna od njih. Samo priključenje na Internet može da predstavlja novi i nešto različitiji skup rizika u odnosu na dosadašnje situacije. U svetu, kompanije, Vladina odeljenja i agencije imaju tradicionalne zahteve za upravljanjem bezbednošću sredstvima informacionog sistema, bilo da su memorisana elektronski ili na neki drugi način. Proces i postupci upravljanje savremenim rizicima može da bude preduzet kroz različite načine. Neke od elementa dosledne i kvalitetne primene upravljanja rizicima se najbolje uočavaju na praktičnim modelima. To uključuje:

- analizu mogućih pretnji, rizika i procena za agencijske Internet prezentacije,
- razvoj i planiranje Internet “gateway-a”⁶¹ politike bezbednosti,
- detaljan odgovor na incidente i kontinuirano planiranje poslovanja, – uključivanje izveštajnih mehanizama u upravljački sistem,
- povećanje svesnosti osoblja i obavljanje pogodnih i detaljnih treninga,
- utvrđivanje odgovornosti osoblja za upravljanje i implementaciju bezbedonosnih mera.

Takvi upravljački “alati” mogu biti zastupljeni i primenjeni unutar različitih organizacionih struktura i situacija da bi se efikasno upravljalo pripadajućim rizicima unutar Interneta. ANAO prepoznaje da značajan broj Vladinih departmenta i agencija u Australiji već sada imaju mere koje su poverene specijalizovanim kompanijama na izvršavanje, takozvani outsourcing⁶² rad, vezano za svoje IT infrastruktura. Priručnik Vlade Australije za zaštitu bezbednosti⁶³ podržava stav da jedna agencija ili odeljenje

⁶¹Gateway –proritetan termin za ovaj pojam je "eng. protokol converter", pretvarač protokola odnosno priključenje mreža koje koriste različite protokole. Izvor rečnik foldoc.

⁶² **Outsourcing;** plaćanje nekoj drugoj kompaniji da obezbedi servis ili uslugu koju kompanija može inače da obavi sama, zapošljavajući svoje sopstveno osoblje, na primer, razvoj softverskih rešenja. Izvor rečnik foldoc.

⁶³ Commonwealth Protective Security Manual – Priručnik komonvelta, veza za zaštitu i bezbednost.

mora zastupati stav za primenu čvrstih upravljačkih odluka za ultimativnu odgovornost za bezbednost vladinih informacija. Pri tom odgovornost ostaje na odgovarajućim relevantnim sekretarima ili šefovima i izvršnim rukovodiocima zaposlenih u gencijama. Sama funkcija bezbednosti može biti delegirana na "outsorce" rad **ali odgovornost ne može**. Važno je napomenuti da agencije ili odeljenja koja imaju primenjena "outsorsing" rešenja na deo ili ukupnu Internet prezentaciju su sposobna da koriste iste menadžment alate i da ostvare iste efekte zaštite kao da funkcionišu u kući (eng. in house). U "outsorsing" situacijama, menadžment pripadajućeg rizika u jednoj Internet prezentaciji postaje sastavni deo u ugovornom menadžmentu. Sama politika bezbednosti mora biti kreirana od strane ugovarača ili Vladine agencije, međutim, ultimativna odgovornost za zaštitu informacija leži na agencijskom vrhu. Agencije bi trebalo da efikasno upravljaju posredstvom ugovarača zaduženim za "outsorsing" rad koji je dužan da isporuči izlaze i rezultat koji će predočiti kroz definisanu politiku i projektovane procedure. Određena iskustva, mada nedovoljna, postoje na planu zaštite i kod nas i obavljaju se kroz rad sa VPN⁶⁴-om, odnosno tehnološkim rešenjima u kojim se stvara poseban "kriptografski tunel" kod razmene podataka između dve mreže putem Interneta. Taj metod, je moguće primeniti u kompanijama u kojim postoji više dislociranih mreža. Međutim, dosadašnji transfer podataka između mreža unutar jedne kompanije se najčešće vrši klasičnim komutacionim linijama, odnosno fajl transferom, bez ikakve zaštite. Procenjujemo da će na našim prostorima vrednost poslovnih podataka sve više da dobija na značaju sa povećanom konkurencijom i da će poslovni podaci dobijati određenu tržišnu vrednost. Samim tim će učestati napadi na postojeće informacione sisteme kompanija. U praksi se već sada prodaju "ilegalno" prikupljene liste poslovnih e-mail adresa. Posebnu cenu u kriminalnim radnjama imaju brojevi elektronskih kartica za plaćanje. Sve ovo upućuje da se određene baze podataka u poslovnim sistemima moraju posebno zaštititi. Bez malo u svim definisanim poslovnim linijama, posebno u poslovnim linijama koje su namenjene ASP⁶⁵ poslovanju, moraju se sprovesti rigorozne mere zaštite. Procenjujemo da će samo softverska rešenja koja korisnicima garantuju apsolutnu zaštitu poslovnog integriteta i sigurnost u radu, dugoročno imati prođu na našem tržištu. Smatramo da se ovom problemu mora prići krajnje ozbiljno i profesionalno i da kompanije moraju detaljno razraditi sopstvene modele kriptografske zaštite kao svoj standard, kako u zaštiti sopstvenih baza podataka tako i u zaštiti pojedinih softverskih rešenja koja imaju plasman kroz ponuđene informatičke usluge na tržištu. Bezbednost podataka predstavlja jednu od investicija koja je u ovom trenutku nužna i koja u prvom trenutku ne može doneti direktni finansijski efekat. Međutim, može se očekivati da će stečeno znanje iz ove oblasti naći svoje potencijalne kupce pre svega u velikim poslovnim sistemima koji ovom poslu nisu blagovremeno prišli, a imaju potrebu da se u relativno kratkom vremenu adekvatno zaštite. U tom trenutku može doći do pune komercijalizacije tako formiranog znanja, ali, nažalost, to ne treba očekivati u skorom vremenskom periodu.

Obezbeđena celovita zaštita u elektronskom poslovanju je zapravo preduslov rada elektronskog poslovanja. Bezbedan rad može da bude ugrožen sa više strana, a

⁶⁴ VPN – Virtual Private Network – Privatna virtuelna mreža – formirana posebno, pod Linux operativnim sistemom uslovno rečeno "privatni tunel" kroz Internet mrežu koji obezbeđuje sigurnu jeftinu razmenu podataka koja je kriptografski zaštićena od napada spolja (prema elektronskom rečniku foldoc).

⁶⁵ ASP - Application Service Provider – servis, odnosno usluga koja se obezbeđuje pristupom sa udaljene lokacije u jedan aplikacioni program kroz mrežni protokol. Izvor rečnik foldoc.

menadžment kompanija mora da bude upoznat sa mogućim problemima na koje može delovati određenim organizacionim merama.

– **Zlonamerni udari unutar korporacije:** Svetska praksa pokazuje da menadžment mora da preduzme mere da se zaštiti od nesavesnih radnji svojih službenika. Na to ukazuju i revizorski standardi koji predviđaju i zahtevaju čitav niz mera koje su potrebne da se sprovedu kako bi obrada u okviru informacionog sistema korporacije, pa i u okviru elektronskog poslovanja bila maksimalno zaštićena. Bilo bi idealno, da se naročito u velikim korporacijama uspostavi **posebno koordinaciono telo** na vrlo visokom hijerarhijskom nivou, koje bi povremeno (najmanje jednom mesečno) analiziralo ugroženost informacionog sistema i elektronskog poslovanja i preduzimao potrebne preventivne mere zaštite u skladu sa svetskim trendovima.

– **Kompjuterski »virus« koji napada PC:** Sadašnji informacioni sistemi su sada najčešće postavljeni na personalnim računarima. Ovakva tehnološka postavka ih izlaže napadima od strane "hackera" koji fabrikuju kompjuterske "viruse", koji uništavaju programe i podatke na kompanijskim diskovima. Savetuje se menadžmentu kompanija da preduzmu mere korišćenja antivirus programa poznatih svetskih kompanija i da ih ažuriraju na dnevnoj osnovi.

– **Zlonamerni udari spolja u IS:** Informacije koje su memorisane u računarima kompanije postaju meta napada konkurencije u cilju dolaženja do podataka o kretanju poslovanja i dugoročnim strateškim planovima. Popularan savremeni naziv za takav vid napada konkurencija je najčešće "industrijska špijunaža". Menadžment određenim merama preventivne zaštite, pre svega lozinkama, kriptografijom, kao i fizičkim obezbeđenjem, uz analizu pristupa pojedinim strateškim podacima (ko je pristupio, sa kog telefona, sa kog računara, u koje vreme) može da obezbedi potrebnu zaštitu.

Kao rekapitulativni pregled osnovnih bitnih elementa koji moraju biti ugrađeni u bezbedonosnu politiku kompanije, sa ciljem da se maksimalno obezbede poslovne transakcije spada rešavanje pitanja:

1. Poverenja,
2. Privatnosti,
3. Autentičnosti,
4. Neporicanja.
5. Integriteta,
6. Enkripcije.

Da bi ubrzala svoje elektronsko poslovanje i obezbedila bezbednost u radu kroz razvoj opšte identifikacije i poverenja, plaćanje i trgovačke standarde koji su interoperabilni, Australija je pristupila korišćenju Identrusa⁶⁶ i u sklopu toga je primenila sve potrebne propozicije kod primene "Business to Business – B2B13" tehnologije. Samim tim ona omogućava svojim članovima da isporuče totalno integrisano neposredno rešenje za oba aktera i za kupca i za prodavca. Pri tom su definisani osnovni kriterijumi koji moraju da se ispune i to:

⁶⁶ **Identrus** - konzorcijum opštih finansijskih institucija formiran da olakša povećanje bezbednosti B2B i B2C elektronskog poslovanja. "Identrus" rešenja počinju sa prihvatanjem standarda PKI tehnologije za proveru autentičnosti i bezbednosti transakcija. Međutim to je mnogo više nego kolekcija tehničkih rešenja. Identrus je kompletna infrastruktura za pomoć kompanijama da efikasno i bezbedno funkcionišu na Internetu, kroz međunarodne ekonomske i političke granice, sa prisnim poslovnim partnerima i novim individualcima. Tehnologija koju uključuje Identrus rešenja obuhvata: PKI zasnovanu krypto-bezbednost digitalne identifikacije i u realnom vremenu proveru potrebnih identiteta.

- Autentičnost,
- Neopozivo plaćanje,
- Uslovno plaćanje (po izvršenoj isporuci),
- Garancija plaćanja,
- Neposredno neopozivo trenutno plaćanje,
- Datum budućeg plaćanja (pri čemu se podrazumevaju normalni trgovački termini),
- Usaglašenje.

Sistemi informacionih tehnologija su u praksi najčešće vrlo pouzdani, ali slično svemu drugom i oni mogu biti subjekt nepredviđenih događaja. Kada se dogodi nepredviđeni događaj, korisnik se nalazi pred situacijom da ono, u šta su svi verovali da je dostojno poverenja, odnosno Informacioni sistem kompanije, postane neupotrebljiv. U takvim situacijama korisnici moraju da budu sposobni da nastave redovno poslovanje za vreme perioda neupotrebljivosti računara, odnosno informacionog sistema, što može biti od nekoliko sati, dana, a prema primerima iz prakse i do nekoliko meseci. Treba imati u vidu da uzrok duže neupotrebljivosti sistema informacionih tehnologija može biti vrlo redak, ali kada se to desi, on može biti katastrofalan po organizaciju, ako nisu načinjene planske, unapred potrebne mere predostrožnosti. Potreba za pouzdanošću informacionih tehnologija se svakim danom povećava. U modernom poslovanju postoji malo oblasti koje su bez uslovljenosti od strane informacionih tehnologija i koje neće trpeti posledice ako su njegove performanse pogoršaju. U kompanijama se potencijalni rizik primene Informacionih tehnologija stalno povećava i postaje sve više raznolik po svom uzroku, na primer; korisnici informacionih tehnologija sada imaju situaciju da se suočavaju sa rizikom od dejstva hakera, infekcije “kompjuterskih virusa”, destruktivnim industrijskim akcijama uperenim neposredno od strane sopstvenog nezadovoljnog kompjuterskog osoblja ili drugih insajdera. Kako se važnost kompjuterske obrade unutar poslovne organizacije kontinuirano povećava, tada su efekti mogućeg prekida kompjuterskog sistema, potencijalno višestruko štetni. Pored toga, korišćenjem globalne svetske mreže, kompjuterski sistemi se povećano izlažu potencijalnim pretnjama od napada hakera i ulaska kompjuterskih “virusa”. Za vreme trajanja smanjenja vremena rada Informacionog sistema u Kompaniji, može se očekivati da eskalira gubitak u Kompaniji.

Zato je neophodno da se vreme kada je kompjuter, odnosno Informacioni sistem neupotrebljiv, svede na minimum. Planiranje nepredviđenih situacija je proces u okviru kojeg menadžment kompanije priprema da radi sa jednim neplaniranim događajem koji je izazvao katastrofu i prekid u radu. U terminu informacionih tehnologija to najčešće znači gubitak ili trajnu dužu neupotrebljivost kompjuterskog sistema. Kako se stepen kompjuterizacije unutar jedne organizacije stalno nastavlja i povećava, tako su efekti mogućeg “ispadanja” (eng. breakdown) kompjuterskog sistema potencijalno mnogo opasniji događaji. Pored toga, izlaskom Kompanija na Internet, povećana je izloženost kompjuterskog sistema od drugih potencijalnih pretnji.

3.4.1.2. Održavanje informacionog sistema i planiranje kontinuiteta poslovanja

Primenom računara u biznisu zavisnost od informacionih sistema raste, čime raste i njihova važnost i vrednost za biznis pa svako ugrožavanje ove vrednosti predstavlja rizik po kontinualnost poslovanja. Informaciona dobra predstavljaju imovinu preduzeća pa ju je kao i svaku drugu imovinu potrebno štititi, odakle proističe suštinsko pitanje da organizacija identifikuje svoje zahteve za sigurnošću informacija. Rizik po neki biznis je različit zavisno od veličine i prirode poslovanja tako da će se odluka o uspostavljanju ovakvog sistema sigurnosti informacija doneti na osnovu procene mogućeg uticaja povreda **poverljivosti, raspoloživosti i integriteta** informacija na dobit, gubitak ili čak na zatvaranje binisa ukoliko je šteta tako velika da nastavak rada više nije moguć.

Poverljivost - informacija je dostupna samo onima sa ovlašćenim pristupom.

Integritet - informacija je tačna i potpuna a metode obrade informacija su zaštićene.

Dostupnost – ovlašćeni korisnici mogu pristupiti informacijama kada su im potrebne.

Proces – svim aktivnostima zaštite informacija moraju se identifikovati njihovi ulazi i izlazi.

Osnovni cilj zaštite informacija jeste smanjenje rizika a vrši se sistematskim uvođenjem i primenom dokumentovanih kontrola i pisanih procedura, a sve ovo iz razloga što se u praksi ispostavilo da je primena samo tehničkih sredstava jako ograničena i nedovoljna.

Međunarodnim iskustvom, u mnogim radnim organizacijama u svetu došlo se do saznanja da SIGURNOST INFORMACIJA zahteva **UPRAVLJANJE**, što neminovno povlači za sobom i učešće svih zaposlenih u ovom procesu. Ovo naročito dolazi do izražaja ako se podsetimo da su informacione strukture u današnjim uslovima sve povezanije i isprepletanije, da se integrišu i postaju više međuzavisne. Međunarodni standardi su zapravo esencija dobre prakse u svetu i ideje da je samo tehnička zaštita informacionih sistema POTREBNA ali i NEDOVOLJNA i da je neophodno **upravljanje** da bi se informaciona dobra efektivno i efikasno zaštitila.

Najčešći problem uspostavljanja i funkcionisanja sistema sigurnosti jeste njegova efikasnost, odnosno postizanje ciljeva sistema bez ometanja ostalih procesa u radnoj organizaciji. Takođe, vrlo čest problem je što se sigurnost informacija od strane rukovodstva tretira kao sekundarna u odnosu na funkcionalnost ostalih procesa biznisa. Ipak se svest o potrebi sigurnosti informacija u radnoj organizaciji pojavljuje, učvršćuje i najčešće dolazi iz sledećih izvora:

-Pojava **sigurnosnih rizika**, koji ako se ostvare donose veliki gubitak radnoj organizaciji.

-**Pravne, zakonske i ugovorne obaveze** koje se moraju ispuniti.

-**Politike** koje se sprovode u radnoj organizaciji, sa svojim ciljevima i zahtevima.

Značaj i nivo dokumentovanja svakog koraka procesa upravljanja rizikom informacija je imperativ iz sledećih razloga:

-Pokazuje da je proces ispravno izveden do kraja.

-Obezbeđuju se dokazi o donetim odlukama i uspostavljenim procesima.

-Obezbeđuje se mehanizam nadležnosti.

-Omogućava se nastavak nadgledanja i revizije.

- Obezbeđuje se ažuriranje i arhiviranje podataka.
- Omogućava se istovremeno korišćenje i prenos informacija.

Da bi se obezbedio princip efikasnosti dokumentovanja sistema sigurnosti, potrebno je takođe uspostaviti i **procedure kontrole celokupne dokumentacije** koje će biti ugrađene i biti sastavni deo ovog intranet sajta i koje će omogućavati i obezbeđivati:

- Blagovremenu dostupnost dokumentacije.
- Periodično revidiranje i ažuriranje dokumentacije.
- Primena kontrole verzija na dokumentacije.
- Povlačenje dokumentacije koja više nije u upotrebi.
- Prosleđivanje dokumentacije po osnovu principa “need-to-know”.

PLAN SIGURNOSTI INFORMACIJA koji zapravo postavlja aktivnosti koje treba preduzeti radi implementacije potrebnih kontrola. Plan treba da sadrži rezultate analize rizika, akcije koje prvo treba preduzeti, srednje i dugoročne vremenske okvire u kojima ih treba postići i održavati adekvatan nivo sigurnosti, troškove i plan aktivnosti implementacije. On u principu treba da uključi:

- Sigurnosne ciljeve kada su u pitanju *poverljivost, integritet i dostupnost*.
- Pristup analizi rizika.
- Procenu prihvaćenih preostalih rizika nakon implementiranja identifikovanih kontrola.
- Listu odabranih kontrola koje treba implementirati.
- Ocenu instalacije i troškova sprovođenja ovih kontrola.
- Ocenu ljudskih resursa potrebnih za implementaciju ovih kontrola.
- Detaljno opisano radno mesto za implementaciju plana sigurnosti.
- Razvoj svesti o sigurnosti i procedure obuke za zaposlene i krajnje korisnike.
- Redosled aktivnosti odobravanja procesa koje treba uspostaviti tamo gde je to potrebno.
- Redosled aktivnosti za prateće procedure.

Međunarodni standardi za sigurnost informacija

-ISO/IEC 27001 : 2005⁶⁷ **Informacione tehnologije, Tehnike sigurnosti – Sistem za upravljanje sigurnošću – Zahtevi**, predstavlja zahteve koji se obavezno moraju ispuniti

-ISO/IEC 17799 : 2005⁶⁸, **Informacione tehnologije, Tehnike sigurnosti – Pravila prakse za upravljanje sigurnošću informacija** rezultat je rada **Združenog tehničkog komiteta za informacione tehnologije (IT) ISO-IEC JTC 1, Potkomiteta SC 27, Radne grupe 1: Zahtevi, servisi sigurnosti, zaštite i smernice**, svi njegovi zahtevi ne predstavljaju obaveznu primenu već predstavlja smernice i opšte principe (best practice) koji su u praksi provereni i koji su pokazali svoju vrednost u mnogim radnim organizacijama i korporacijama širom sveta i služi za ugled, kako jedan dobro postavljen sistem sigurnosti informacija treba da izgleda i kakvi zaista danas postoje u firmama u

⁶⁷ ISO/IEC 27001 : 2005 Information technology — Security techniques — Information security management systems — Requirements

⁶⁸ ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice or information security management

svetu koje su ga uspešno primenile ili sertifikovale. Ciljevi kontrolisanja i same kontrole iz ovog standarda su namenjene za implementaciju kako bi se ispunili zahtevi koji su identifikovani postupkom ocenjivanjem rizika.

Pretnje po sigurnost informacija i **ranjivosti** informacionog sistema dve su osnovne karakteristike koje treba imati u vidu kod ocena i analiza **poverljivosti, raspoloživosti i integriteta** informacija i donošenja odluka o potrebnom nivou zaštite svakog pojedinog informacionog dobra biznisa. Da bi se ovo ostvarilo, putem **politike sigurnosti informacija**, do koje se dolazi preko identifikacije zahteva za sigurnošću čiju osnovu čini ocenjivanje **verovatnoće** pojavljivanja rizika i stvarne ugroženosti, rukovodstvo objavljuje svoje namere i ciljeve sigurnosti informacija čime se zapravo definišu zahtevi biznisa za sigurnošću informacija. Troškovi ovako postavljenih budućih kontrola ne bi smeli biti u neravnoteži sa troškovima koji mogu nastati kao rezultat otkaza sistema sigurnosti, dakle ne bi se smelo uvoditi premalo ili previše kontrola. Naravno da se politika sigurnosti periodično preispituje pa se ovakve neusaglašenosti vremenom eliminišu i dovode u zadovoljavajuće okvire. Takođe se i ocenjivanje rizika ponavlja periodično kako bi se obuhvatile izmene koje bi mogle uticati na rezultate prethodnih ocenjivanja rizika, što je takođe sasvim razumljivo imajući u vidu neverovatnu dinamičnost ovakvih pojava u današnjem vremenu koje ugrožavaju sigurnost informacija na sve novije i inovativnije načine.

Preostali rizik dobijamo kada na **procenjeni rizik** primenimo odgovarajuće **kontrole**, odnosno odgovarajućeg tretmana. Procenjeni rizik izračunali smo tako što smo pomnožili verovatnoću pojavljivanja neke pretnje sa uticajem ostvarenja te pretnje na poslovanje radne organizacije izraženo u novčanim jedinicama. **Prihvatljiv rizik** je preostali rizik za koji rukovodstvo smatra da ga ne treba obuhvatiti kontrolama sistema sigurnosti.

Kontrole se mogu odabrati iz samih standarda a mogu se uvoditi i nove kontrole koje bi zadovoljavale neke specifične potrebe unutar biznisa. Takođe izabrane kontrole treba da podležu i svim odgovarajućim nacionalnim i međunarodnim zakonima ili uredbama.

Kontrole koje se najčešće biraju u praksi:

- Zaštita podataka i tajnost informacija o ličnosti.
- Zaštita zapisa biznisa.
- Zaštita prava na intelektualnu svojinu.
- Politika sigurnosti informacija.
- Odgovornosti za sigurnost informacija.
- Obuka o sigurnosti informacija.
- Korektnost procesiranja u aplikacijama.
- Upravljanje tehničkom ranjivošću.
- Upravljanje kontinuitetom poslovanja.
- Upravljanje pri incidentima narušavanja sigurnosti.

Međunarodni standard **ISO/IEC 17799 : 2005, Informacione tehnologije, Tehnike sigurnosti – Pravila prakse za upravljanje sigurnošću informacija** prikazuje sistem sigurnosti informacionih sistema preko sledećih elemenata (prikazani redni brojevi su preuzeti iz standarda):

- 5) Politike sigurnosti i zaštite;
- 6) Organizovanja sigurnosti informacija;
- 7) Upravljanja imovinom;
- 8) Sigurnosti ljudskih resursa;
- 9) Fizičke sigurnosti i sigurnosti okruženja;
- 10) Upravljanja komunikacijama i operativnim radom;
- 11) Kontrola pristupa;
- 12) Nabavke, razvoja i održavanja informacionih sistema;
- 13) Upravljanja incidentima narušavanja sigurnosti;
- 14) Upravljanja kontinuitetom poslovanja;
- 15) Usklađenosti sa propisima.

Radi efikasne primene standarda i održavanja sigurnosti informacija na željenom nivou kao i zbog potrebe obezbeđivanja adekvatnog upravljanja i određivanja potrebnog nivoa odgovornosti, potrebno je svu imovinu popisati i dodeliti joj imenovanog vlasnika. Vlasnik će u procesu implementacije a i kasnije kada sistem sigurnosti informacija zaživi u organizaciji, biti sve vreme odgovoran kako za održavanje odgovarajućih kontrola tako i za njihovu redovnu, svakodnevnu primenu.

Vlasnik informacionog dobra ne može svoju odgovornost za to dobro preneti ni na koga drugoga u organizaciji, ali može poslove održavanja kontrola i njihovo redovno sprovođenje u praksi da delegira, pri čemu odgovornost i dalje ostaje na njemu. Naročito je to izvodljivo ako su u pitanju rutinski poslovi koji ne zadiru recimo u kontrolu proizvodnje, razvoja, održavanja, korišćenja ili sigurnosti informacionog dobra.

Kod popisa imovine, nije potrebno praviti nekakve posebne paralelne spiskove za informacionu imovinu ako takvi spiskovi već ionako postoje u organizaciji i za svu ostalu postojeću imovinu, već će biti dovoljno da se samo naznači referenca gde se podaci o dotičnoj stavci mogu pronaći u organizaciji za potrebe kontrola i održavanja sigurnosti informacija. Krajnji cilj ovakvog inventara je jasna identifikacija kao i dodela važnosti svakog objekta budućeg sistema sigurnosti.

Druga specifičnost ovoga inventara je i u tome što bi on trebalo da sadrži i informacije koje su neophodne za obnavljanje posle neke havarije ili nepogode. U podatke treba uključiti tip imovine, formu u kojoj je reprezentovana, lokaciju gde se trenutno nalazi i gde se može naći, informaciju o rezervnim kopijama, informacije o licencama i poslovnoj vrednosti i informacije o vlasniku. Inventar informacionih dobara predstavlja i važan preduslov za kasnije sprovođenje postupka procene i upravljanja rizicima.

Da bi smo bili sigurni da će informaciona dobra koja budu popisana imati odgovarajući i zadovoljavajući nivo sigurnosti potrebno je izvršiti njihovu klasifikaciju. Time zapravo definišemo potrebu, prioritete i stepen sigurnosti koje dodeljujemo informacijama imajući stalno u vidu kako će se sa tako definisanim statusom u pogledu sigurnosti dalje u praksi sa njima postupati. Pošto nemaju sve informacije istu važnost, stepen kritičnosti i osetljivosti za rad i rezultate biznisa, potrebno je u tu svrhu izraditi, usvojiti, primeniti i kontrolisati određenu šemu ili standard koga će se svako pridržavati i koristiti ga kada bude radio na problemu klasifikacije informacionih dobara. Tako bi smo dobili nekakvu šemu za klasifikaciju informacija kojom bi smo unapred definisali pravila

prema kojima bi se ova aktivnost sprovela i obuhvatila sva informaciona dobra koja su kritična za budućnost i postojanje biznisa.

Kod razvrstavanja informacija u kategorije treba voditi računa o potrebi da te kategorije ne budu brojnije nego što bi trebalo, niti da ih ima premalo, jer kod odlučivanja po tom pitanju potrebno je uzeti u obzir i činjenicu da bez obzira što ova šema jeste putokaz svim budućim klasifikacijama i ona sama se u toku vremena menja, pa ako imamo glomaznu i nepreglednu šumu kategorija i podkategorija biće zamašan posao ažurirati i izmeniti postojeću šemu, a onda i svu klasifikaciju preraditi prema njenim poslednjim izmenama. Najčešće potrebe za izmenama klasifikacione šeme dolaze od izmena politike sigurnosti informacija, a koja se sa svoje strane menja kao odgovor na nove pretnje, slabosti i zahteve koji se kumuliraju u toku rada biznisa i promenama kako u okruženju tako i u sopstvenim unutrašnjim promenama uslova poslovanja. Pa i same informacije tokom nekog vremenskog perioda gube na svom značaju, recimo ako bude objavljena neka poverljiva informacija, nikakve više potrebe nema da je tretiramo na istom sigurnosnom nivou, jer njihova važnost i kritičnost prestaju da postoje.

Kada biramo određeni nivo sigurnosti informacija imamo u vidu njihovu vrednost po biznis, potrebe da se zadovolje najnovije izmene u zakonskoj regulativi, kao i koliko je koja grupa informacija kritična i osetljiva po svom mogućem uticaju na poslovanje. Takođe je potrebno odrediti period i vršiti redovno i sistematsko preispitivanje (audit) klasifikacionih šema kao i samu klasifikaciju da bi se obezbedila njena ažurnost a kao povoljna posledica održavanje sigurnosti na zadovoljavajućem nivou, niti preterana sigurnost niti premala i jedno i drugo sa negativnim konotacijama na rad biznisa. Ovaj posao kontrole i primene ažurnih klasifikacionih šema i klasifikacije informacionih dobara treba da se pridruži redovnim dužnostima koje ima vlasnik informacionog dobra, a koji je i po definiciji odgovoran za njihovu sigurnost.

Tri su najčešća kriterijuma po kojima ćemo razvrstavati informaciona dobra putem šeme za klasifikaciju:

POVERLJIVOST INTEGRITET RASPOLOŽIVOST

Kod označavanja (postavljanja labela) stepena sigurnosti, trebalo bi se na neki način upoznati na koji način su neke druge radne organizacije rešile isti ovaj problem, tako da bi smo u nekoj našoj budućoj saradnji sa njima ovu činjenicu imali u vidu i izbegli nesporazume ili obostrano kršenje i povrede politike sigurnosti informacija. Označavanje i postupanje sa informacijama podležu strogim postupcima ili procedurama koje treba razviti u organizaciji a odnosi se na:

-INFORMACIJE: baze podataka i datoteke sa podacima, ugovore i sporazume, sistemsku dokumentaciju, informacije o istraživanjima, uputstva za korisnika, materijal za obuku, procedure za rad ili podršku, planove za kontinuitet poslovanja, planove za povratak u prethodno stanje, tragove za proveru i arhivske informacije;

- SOFTVERSKA** dobra: aplikativni softver, sistemski softver, razvojne alate i pomoćne programe;
- FIZIČKA** dobra: računarsku opremu, komunikacionu opremu, prenosive medijume i ostalu opremu;
- USLUGE**: računarske i komunikacione usluge, opšte usluge, npr. grejanje, osvetljenje, električno napajanje, klimatizaciju;
- OSOBLJE** i njegove kvalifikacije, znanja i iskustva;
- NEMATERIJALNE**, kao što su ugled i imidž organizacije.

Bez obzira da li je informacija u elektronskoj ili fizičkoj formi svaka od njih mora se obuhvatiti nekom od procedura koja će se oslanjati na postojeću šemu klasifikacije informacionih dobara koja je usvojena u organizaciji. Procedure po ovom pitanju potrebno je razvrstati prema stepenu klasifikovanosti informacija. Što se tiče njihovog sadržaja, one treba da obuhvate postupanje sa informacijama koje su u raznim fazama i pojavnim oblicima kao recimo: da li se informacije nalaze u procesu obrade, da li se nalaze negde uskladištene i čuvaju ili se radi o informacijama koje više ne treba klasifikovati ili koje treba uništiti.

Takođe kao i svaka procedura po samoj svojoj definiciji i svrsi, mora da bude praćena adekvatnim uputstvima za primenu i naročito svaka procedura mora da propisuje obaveznu formu i način beleženja i čuvanja svih podataka o događanjima koja su posledica primene procedure u praksi. Ovi **zapis**i služe kasnije za kontrolisanje sistema sigurnosti i ujedno kao dokaz o njegovom adekvatnom funkcionisanju ili kao dokaz da se sistem uopšte primenjuje u biznisu.

Problem može postojati, ali se svakako mora primereno rešiti, kako vidljivo označiti i prikazati informacije koje su klasifikovane kao izuzetno osetljive, ali se nalaze u elektronskom obliku, kao na primer na ekranu terminala, na disku kompjutera ili na CD, disketi ili bilo kom drugom magnetnom medijumu koji nije tako jednostavno označiti kao ostala dobra koja su u fizičkom obliku recimo kada označavamo kompjutere, servere, printere i slično, ili se možda informacija jednostavno nalazi na papiru posle izlaska sa štampača.

Fizičko označavanje može biti mnogo jednostavnije, recimo preko običnih nalepnica koje će nedvosmisleno ukazivati na stepen zaštite i specijalnog tretmana i kontrole informacionog dobra u organizaciji. Sasvim je poseban problem ako se informacija prenosi elektronskim putem, recimo kada je informacija u elektronskoj pošti ili se prenosi bežičnim putem ili recimo telefaksom.

U slučaju da se informacijski sistem ili njegovi delovi zajednički koriste sa drugim organizacijama, procedure treba i ovo da obuhvate, naročito ako se radi o tome da se zajedničko korišćenje informacija ugovara u pismenoj formi, kada procedura treba da obuhvati i slučajeve korišćenja i potrebne kontrole i evidencije koje će biti dokaz da se

ugovor o zajedničkom korišćenju informacija između ugovornih strana poštuje ili ne poštuje. Takve informacije potrebno je posebno označavati i kontrolisati.

Tamo gde je zaista teško staviti bilo kakvu oznaku o stepenu sigurnosti može se pribеći označavanju preko metapodataka u programima ili na samom dokumentu ili oznake sigurnosti unositi u same procedure.

Preko politike sigurnosti informacija, rukovodstvo biznisa je dužno da obezbedi specifična pravila ili smernice po pitanju, šta je to što bi se u radnoj organizaciji moglo podvesti pod prihvatljivo korišćenje informacionih dobara. Ova pravila biće kasnije ugrađena u same procedure i kontrolisana u praksi. Sa ovim pravilima korišćenja informacionih dobara potrebno je upoznati sve zaposlene, korisnike informacija sa kojima se ugovara korišćenje informacija kao i svakoga ko se može podvesti pod treću stranu. Naročito se insistira na pravilima koja će se odnositi na prihvatljivo korišćenje informacionih dobara elektronske pošte i Interneta. Takođe posebna pažnja u ovim pravilima posvećuje se i korišćenju prenosivih uređaja koji se mogu izneti iz radne organizacije i kako će se na bezbedan način koristiti u takvim situacijama.

Dokumentacija za standarde sigurnosti informacija

Postoji veliki broj dokumenata sistema sigurnosti informacija koji su obavezni i oni koji se međunarodnim standardima preporučuju kao dobra praksa u svetu. Glavna svrha dokumentacije i dokumentovanja je postojanje zapisa pojedinačnih odluka menadžmenta koji će kasnije služiti kao trag koji će voditi od preduzetih akcija po pitanju sigurnosti informacija ka politici sigurnosti informacija i usvojenim i primenjenim kontrolama, dakle, biće dokaz da se politika sigurnosti informacija u radnoj organizaciji sprovodi. Ovi zapisi treba da budu veza između izabranih kontrola koje se primenjuju za umanjenje procenjenog rizika i preko postojeće procene rizika i postupaka u vezi sa tim rizicima da ukažu da se ciljevi iskazani u politici sigurnosti informacija ostvaruju na zadovoljavajući način.

Dokumenti koji su obavezni prema **ISO/IEC 27001 : 2005 Information technology – Security technoloques - Information security management systems – Requirements:**

Glavna svrha dokumentacije sistema sigurnosti je uspostavljanje veze između odluka rukovodstva, politike sigurnosti, ciljeva sistema, procene rizika, postavljenih kontrola i procedura sa rezultatima preduzetih praktičnih akcija, čime se zapravo dokumentovano može dokazivati funkcionisanje sistema sigurnosti informacija u radnoj organizaciji.

- Dokument politike sigurnosti informacija.

- o Okvir za postavljanje ciljeva i jedne opšte smernice za pravce i principe akcije.
- o Uzima u obzir zakonsku regulativu i ugovorne obaveze u vezi sigurnosti.
- o Postavlja kontekst strategijskog upravljanja rizikom u čijim okvirima će se kretati održavanje sistem sigurnosti informacija.
- o Postavlja kriterijume na osnovu kojih će se vršiti procena rizika.
- o Obavezno se odobrava od strane rukovodstva.

- Dokument domena i opisa sistema sigurnosti informacija.

- o Definiše granice i domen sistema sigurnosti u skladu sa karakteristikama biznisa, organizacije, lokacije, sredstava i tehnologije.
- o Svako odstupanje od standarda treba da je definisano i odobreno od strane rukovodstva

- Dokumentovane procedure koje podržavaju sistem sigurnosti informacija sadrže:

- o Domen ili područje primene procedure
- o Opis drugih dokumenata koja su u vezi sa procedurom
- o Opšta pravila i definicija korišćenih termina za sprovođenje procedure
- o Dijagram toka koji opisuje aktivnosti koje se sprovode procedurom
- o Opis aktivnosti, ŠTA se radi, ko radi, gde radi
- o Dodeljene odgovornosti za primenu procedure
- o U prilogima se obavezno navode sva UPUTSTVA kao i ZAPISI koji objašnjavaju kako se aktivnosti iz procedura sprovode.

- Dokumentovane kontrole koje podržavaju u ostvarenju ciljeva sistema sigurnosti informacija mogu biti:

- o Organizacione i upravljačke
- o Fizičke i kontrole okruženja
- o Operativne
- o Tehničke
- o Kontinualnosti poslovanja
- o Usklađenosti i revizije

<> Funkcije kontrola:

- o Sprečavanje, izbegavanje, prevencija
- o Zaštita
- o Identifikovanje, detektovanje
- o Odgovor, reagovanje, suprotstavljanje
- o Rekonstruisanje i povratak integriteta, dostupnosti i poverljivosti

<> Ciljevi kontrola:

Politika sigurnosti informacija: Da menadžment obezbedi usmerenje i podršku sigurnosti informacija, u skladu sa poslovnim zahtevima i odgovarajućim zakonima i regulativom.

Interno organizovanje: Upravljanje sigurnošću informacija unutar organizacije.

Odgovornost za imovinu: Da se ostvari i održava odgovarajuća zaštita imovine organizacije.

Sigurnost ljudskih resursa: Osiguranje da zaposleni, izvođači radova i korisnici sa treće strane razumeju svoje odgovornosti, kao i da su pogodni za svoje uloge, kao i da se smanji rizik od krađe, prevare ili zloupotrebe.

Fizička sigurnost i sigurnost u okruženju: Da se spreči neovlašćen fizički pristup, oštećenje i ometanje u prostorijama i na informacionim dobrima organizacije.

Upravljanje komunikacijama i operativnim radom: Da se osigura ispravan i siguran operativni rad sredstava za procesiranje informacija.

Kontrola pristupa: Kontrola pristupa informacijama.
Nabavka, razvoj i održavanje informacionih sistema: Da se obezbedi da sigurnost bude sastavni deo informacionih sistema.

Upravljanje incidentima narušavanja sigurnosti informacija: Da se osigura da se o događajima u vezi sigurnosti informacija i slabostima vezanim za informacione sisteme obaveštava na način koji omogućuje blagovremeno preduzimanje korektivnih mera.

Upravljanje kontinuitetom poslovanja: Da se uspostave protivmere za prekide u poslovnim aktivnostima, kako bi se kritični poslovni procesi zaštitili od uticaja većih otkaza ili katastrofa i da bi se osiguralo blagovremeno nastavljjanje sa radom.

Usklađenost sa zakonskim odredbama: Da se izbegnu kršenja bilo kojeg zakona, statutarnih, regulativnih ili ugovornih obaveza, kao i bilo kojeg zahteva za sigurnost.

- Dokumentovana i usvojena metodologija procene rizika.

- o Metodologija procene rizika treba da je usklađena sa sistemom sigurnosti i zakonskim i regulatornim zahtevima.
- o Potrebno je razviti kriterijume za prihvatanje vrste rizika i nivoa prihvatljivog rizika za radnu organizaciju.
- o Ova metodologija ima za cilj da obezbedi da će sve vrste procene rizika koje će se u budućnosti sprovoditi biti uporedive i davati iste rezultate u istim uslovima ispitivanja.

- Dokumentovan procenjen rizik.

-

Procena rizika vrši se na osnovu izabranih kontrola i ciljeva izabranih kontrola.

- Plan postupanja sa preostalim rizikom. Preostali rizik se deli na dva dela, rizik na koji će se primeniti **kontrole** sa ciljem da se svedu i smanje i drugi deo koji se označava kao **prihvatljiv rizik**.

- Dokumentovane procedure koje će osigurati **efektivno planiranje, sprovođenje i kontrolu** procesa sistema sigurnosti sa opisom kako će se u organizacija meriti efektivnost postavljenih kontrola.

ZAHTJEVI ZA KONTROLISANJEM I ZAŠTITOM DOKUMENTACIJE

Za kontrolu i zaštitu dokumentacije sistema sigurnosti informacija potrebno je napisati procedure koje će omogućiti:

- Da dokumenta pre primene budu odobrena od strane rukovodstva čime se potvrđuje njihova adekvatnost.
- Preispitivanje i ažuriranje dokumenata i po potrebi da budu ponovo odobrena.
- Osigurati da tekuća verzija sadrži poslednje važeće izmene.
- Osigurati da su relevantna dokumenta dostupna svim vlasnicima informacionih dobara.
- Osigurati da su dokumenta lako pristupačna i da se lako identifikuju.
- Osigurati da se lako može utvrditi njihov izvor.
- Osigurati da se distribucija dokumenata vrši kontrolisano, planski i organizovano.
- Osigurati da ne dođe do upotrebe zastarelih dokumenata.

U radnoj oraganizaciji potrebno je da postoje i da se ažurno održavanju zapisi sistema čime se obazbeđuju dokazi ispunjavanja zahteva standarda kao i efektivnost sistema sigurnosti. Zapisi treba da su zaštićeni i kontrolisani i treba takođe voditi računa o svim zakonskim i ugovornim obavezama.

Najopštija struktura dokumentacije zahtevana međunarodnim standardima može se HIJERARHIJSKI prikazati kao na slici:



Hijerarhijski dijagram dokumentacije sistema sigurnosti

Iz ovog hijerarhijskog dijagrama **dokumentacije sistema sigurnosti informacija** može se steći utisak i predstava o obimu i strukturi dokumentacije koja mora postojati u radnoj organizaciji i to na način kako je to opisano u dokumentu "ISO/IEC 27001 : 2005 Information technology – Security technouques - Information security management systems – Requirements".

3.4.1.3. Razvoj informacionog sistema

Danas je nezamisliv razvoj distribuiranih informacionih sistema bez računarskih mreža i koncepta objektnoorijentisanog razvoja aplikacija. Time se uvode konkretniji standardi u računarskoj tehnologiji, koji omogućavaju povezivanje udaljenih komponenti distribuiranog hardvera ili softvera. Prelazak sa strukturnog i modularnog programiranja u objektnoorijentisano programiranje redukuje cenu softvera. Takve *softverske komponente* integrišu se sa aplikacijama, a aplikacije u celoviti sistem.

Zbog toga je razvoj *komponentnih modela* postao popularan poslednjih godina. Brz tehnološki razvoj, posebno pojava internet tehnologije, uzrokuje promene u navedenim metodološkim pristupima. Problem kod većine postojećih informacionih sistema jeste heterogenost i veliki broj neintegrisanih podsistema. Zbog toga se teži definisanju određenih standarda koji umanjuju ove probleme. Oni omogućavaju da se komponente softvera mogu koristiti ako su već jednom napisane ili da se mogu nabaviti od drugih proizvođača. Standard se odnosi na interfejs koji bi trebalo da omogući da distribuirane komponente, pisane u različitim jezicima, međusobno sarađuju. To je od velikog značaja za definisanje metodoloških pristupa u razvoju informacionih sistema kod velikih organizacionih sistema.

Posebno su značajna iskustva u primeni metoda i standarda u razvoju informacionih sistema sa primenom internet tehnologije. Pojava različitih proizvođača stvara dileme u opredeljenju za pristup u razvoju kompleksnijih informacionih sistema.

Pristup u razvoju informacionih sistema

Cilj procesa razvoja sistema je izrada kvalitetnog softvera koji će zadovoljiti potrebe korisnika. Pored toga, razvoj softvera treba da predstavlja proces s predvidivim vremenskim trajanjem i budžetom. Postoji više različitih procesa razvoja sistema, a primena određenog procesa zavisi od domena problema, tehnologije koja se može koristiti u implementaciji i sposobnosti i veštini projektnog tima. metoda i alata⁶⁹. Za velike sisteme, preporučuju se standardizovani postupci i metodologije za razvoj informacionih sistema. Postoje različiti metodološki pristupi u razvoju informacionih sistema: **sistemski integralni pristup razvoju** (od projektovanja, implementacije do uvođenja i održavanja) i **razvoj informacionih sistema kao tehničko-tehnološke strukture** (standardna mreža računara i servisa). **Kombinacija** ova dva pristupa vodi efikasnom rešenju u razvoju informacionih sistema, pri čemu treba imati u vidu **koncept „otvorenih sistema“** koji omogućavaju da različiti informatički standardi i servisi mogu da funkcionišu na tim sistemima (uključujući operativne sisteme, baze podataka, računarske komunikacije i korisničke interfejse).

Osnovni problem u razvoju složenijih informacionih sistema jeste savladavanje njihove složenosti. Pri tome, analiziraju se dva aspekta: **podela celokupnog razvoja na faze** i **dekompozicija sistema**. Podela razvoja na faze može se posmatrati kroz poznati konvencionalni životni ciklus informacionih sistema: **1. planiranje razvoja, 2. analiza i specifikacija zahteva, 3. projektovanje, 4. implementacija (kodiranje i testiranje), 5. uvođenje, 6. održavanje.**

⁶⁹ **Metode** predstavljaju skup postupaka, dok su **alati** sredstva u procesu razvoja informacionih sistema (na primer: dijagrami toka podataka, dijagrami objekti – veze, objektni dijagrami – dijagrami klasa, dijagrami promene stanja, Petrijeve mreže, itd.).

Pojedinačne metode koriste skup alata, tehnika i aktivnosti za rešavanje problema u razvoju informacionih sistema. U pojedinim fazama životnog ciklusa informacionih sistema mogu se koristiti različiti alati i metode.

Aplikativno najpogodniji je **objektni pristup**. Kod različitih pristupa postoji problem izbora metoda projektovanja, odnosno stvaranja optimalnog metodološkog pristupa razvoja informacionih sistema. Takođe, postoji problem razvoja zbog parcijalne automatizacije u uslovima masovnog uvođenja personalnih računara. U takvim uslovima često se pristupa razvoju informacionih sistema kao infrastrukture i definisanju standarda, ne čekajući globalni projekat. Nakon izvesnog vremena postoji mogućnost da dođe do redundancija i haosa, zbog čega je potrebno ostvariti kontrolu i upravljati razvojem. Koordinacija nad lokalnim podsistemima, pored standarda, podrazumeva **rečnik podataka**, što znači postojanje „informacionog sistema o informacionim sistemima“. Ovakav pristup u razvoju informacionih sistema zahteva dosta znanja.

Postoje različite objektnoorijentisane metode koje predlažu različite pristupe objektnoorijentisanoj analizi i projektovanju informacionih sistema. Među njima su najpoznatije **OMT metod** (*Object Modeling Technique*), **Boochov metod** i **OOSE metod** (*Object – Oriented Software Engineering*)⁷⁰. U OMT metodu posmatraju se tri različita modela: objektni, dinamički i funkcionalni. Oni predstavljaju različite poglede na sistem i međusobno su komplementarni. Ovaj metod daje prednost pristupu u kojem analiza sistema započinje definisanjem entiteta i formiranjem objektnog modela. Ovaj pristup naziva se **pristup orijentisan podacima** (*data driven approach*). U Boochovom metodu definisani su različiti dijagrami: dijagram klasa, dijagram objekata, dijagram interakcije objekata i dijagram prelaza stanja. Njima su predstavljene statičke i dinamičke karakteristike sistema. U ovom metodu posebno je naglašen onaj deo procesa razvoja sistema koji se odnosi na projektovanje i implementaciju sistema⁷¹. U OOSE metodu definisane su tri vrste objekata. To su objekti entiteta (*entity objects*), interfejs objekti (*interface objects*) i upravljački objekti (*control objects*). Za opis dinamike sistema uvedeni su slučajevi korišćenja (*use cases*). Ovaj metod daje prednost pristupu u kojem definisanje zahteva i analiza sistema započinju definisanjem slučajeva korišćenja i formiranjem modela slučajeva korišćenja. Ovaj pristup naziva se **pristup orijentisan slučajevima korišćenja** (*use case approach*). Uvidom u navedene objektnoorijentisane metode dolazi se do zaključka da sve te metode imaju jedan zajednički skup elemenata koji se koristi u modeliranju sistema.

Razvoj informacionog sistema:

- Analiza sistema
- Oblikovanje (dizajn) sistema
- Implementacija sistema
- Funkcionisanje sistema (uz nadgledanje i povremenu reviziju).

Upravljanje informacionim sistemom podrazumeva zadovoljavanje određenih potreba za informacijama radi rešavanja poslovnih problema.

Od informacionog sistema se očekuje da informacije:

- isporuči na vreme

⁷⁰ Prva verzija UML data je 1995. godine pod nazivom Unified Method, autora G. Boocha i J. Rumbaugh. Novije verzije prihvatile su i vodeće svetske kompanije u proizvodnji softvera, kao što su ORACLE, IBM, Digital Equipment, Microsoft i drugi.

⁷¹ Metode razvoja softvera – Larmanova metoda, prof.dr Vidojko Ćirić, mr Siniša Vlajić, FON.

- u okviru budžeta
- sa očekivanim karakteristikama
- bez grešaka i
- u skladu sa potrebama korisnika.

Osim zahteva klijenata, današnja sistemska analiza se suočava sa stalnom promenom razvojne metodologije i tehnologije, i otporom prema promenama.

Razvoj informacionog sistema vezan je za novčana ulaganja u obliku dugoročnih investicija i u obliku neposrednih troškova. Iz tih razloga potrebno je da se dobro projektuje i pripremi uvođenje novog informacionog sistema.

Fazna podela razvoja informacionog sistema može se sagledati sa više aspekata uz uključivanje određenih kriterijuma.

Postoje, u osnovi, dva opšta pristupa:

1. Linearni i
2. Evolutivni.

Karakteristike linearnog ili klasičnog pristupa projektovanju informacionog sistema jeste da se na sledeću fazu projektovanja prelazi samo kada je prethodna faza u potpunosti realizovana. Kod linearnog projektovanja često mogu nastali problemi u jednoj fazi da dovedu do revizije prethodne faze pa tada dolazi do zaustavljanja celog razvoja.

Svaki poslovni sistem treba da ima dugoročni plan razvoja informacionog sistema koji predstavlja okvir unutar koga se može planirati, projektovati i realizovati svaki poseban projekat određenog podsistema.

Postojanje ovakvog plana razvoja omogućava da svaki novi projekat bude:

- ekonomski opravdan
- da zadovoljava potrebe poslovnog sistema
- da bude usaglašen sa funkcionisanjem poslovnog sistema.

Za izradu ovakvog plana nisu potrebna neka specijalna ulaganja u sredstva, kadrove i vreme, a ne preporučuje se da plan bude previše detaljan. Pre nego što se pristupi izradi idejnog projekta informacionog sistema neophodno je da se izvrše prethodna istraživanja. Cilj ovih istraživanja je da se utvrdi spremnost poslovnog sistema da prihvati novi informacioni sistem podržan savremenom tehnologijom. Kroz ove aktivnosti utvrđuju se i eventualne prepreke koje treba ukloniti pre nego što se pristupi bilo kakvoj aktivnosti na projektovanju informacionog sistema.

U okviru spremnosti poslovnog sistema da prihvati novi informacioni sistem posebno se ispituju sledeće sposobnosti:

- opšta
- organizaciona
- kadrovska
- finansijska.

Opšta sposobnost podrazumeva da u poslovnom sistemu ne postoje, u bliskoj budućnosti, neke integracione ili dezintegracione aktivnosti odnosno promene u organizacionoj strukturi, da se ne posluje sa gubitkom itd.

Organizacione sposobnosti predstavljaju mogućnosti postojeće organizacije da prihvati savremeni informacioni sistem. Integralnost informacionog sistema, kao njegova najvažnija osobina, pretpostavlja da je organizaciona struktura izgrađena po jedinstvenoj koncepciji, kriterijumima i metodologiji.

Kadrovska sposobnost podrazumeva postojanje kadrova potrebnih za izgradnju i funkcionisanje informacionog sistema, a u širem smislu to je i sposobnost korišćenja informacionog sistema.

Finansijska sposobnost podrazumeva postojanje finansijskih sredstava za investicione izdatke, kako za opremu tako i za druge troškove, vezane za realizaciju projekta informacionog sistema.

Izrada idejnog projekta ima dva cilja:

- donošenje odluke o izgradnji integralnog informacionog sistema,
- donošenje odluke o troškovima i organizaciji informacionog sistema.

Kroz idejni projekat preciziraju se sve informacije neophodne za donošenje ovih odluka. Idejni projekat je osnova za izradu glavnog odnosno izvršnog projekta.

Osnovni elementi idejnog projekta informacionog sistema:

- opšti pristup izgradnji integralnog informacionog sistema,
- opis organizacije poslovnog sistema,
- analiza postojećeg informacionog sistema,
- koncepcija novog informacionog sistema,
- definisanje podsistema novog informacionog sistema,
- određivanje nivoa informisanosti,
- upravljanje izgradnjom i funkcionisanjem informacionog sistema.

Osnovni elementi idejnog projekta informacionog sistema:

- * tehničke i organizacione pretpostavke za izgradnju informacionog sistema,
- * položaj IS u odnosu na informacione sisteme u okruženju,
- * materijalni uslovi za izgradnju IS,
- * kadrovska osnova,
- * ekonomska opravdanost izgradnje IS,
- * definisanje prioriteta u izgradnji pojedinih podsistema,
- * dinamika projektovanja i izgradnje IS.

Cilj izvršnog projekta je da ostvari realizaciju, odnosno uvođenje nove organizacije informacionog sistema kao sastavnog dela poslovnog sistema. Izvršni projekat omogućava da uvođenje nove organizacije informacionog sistema prođe sa što manje teškoća i improvizacija veze sa sistemima iz okruženja itd.

Aktivnosti koje sadrži izvršni projekat:

- detaljno i precizno definisanje informacionih podsistema i njihovih segmenata,
- detaljan uvid u postojeće stanje i njegova analiza,
- prikupljanje dodatnih podataka i informacija,
- izrada nove organizacije,
- kreiranje strukture datoteka,
- kreiranje ulazne i izlazne dokumentacije,
- izrada organizacionih uputstava,
- izrada programskih zadataka,
- pisanje i testiranje programa obrade.

Za razliku od idjenog projekta, gde su dati samo opisi informacionog podsistema, u izvršnom projektu se svi podsistemi precizno razgraničavaju i utvrđuju se veze između njih.

Veze mogu da budu:

- zajedničke datoteke
- zajedničke šifre
- veze ulaza i izlaza podataka
- zajednička dokumentacija.

Uvid u postojeće stanje vrši se detaljno da bi se ustanovilo:

- gde se pojavljuju izvorni podaci,
- ko popunjava i ispostavlja dokumente,
- kuda idu dokumenti,
- gde se dokumenta odlažu,
- koji je sadržaj pojedinih dokumenata,
- koliko se dokumenata javlja u nekom vremenskom periodu,
- kakva je distribucija dokumenata itd.

U toku projektovanja vrši se i izrada sistema šifara, a jedna od veoma bitnih aktivnosti je kreiranje skladišta podataka (datoteka, baza podataka...).

Neophodno je, takođe, kreirati ulazni i izlaznu dokumentaciju koja obuhvata:

- dokumentaciju za unos podataka,
- organizaciona i programska uputstva,
- strukturu slogova i šifara,
- dijagrame tokova obrade,
- programske liste,
- liste rezultata itd.

Na osnovu svega ovoga kreiraju se uputstva za programere koji treba da napišu i testiraju programe. Uvođenje novog informacionog sistema u poslovni sistem predstavlja veoma osetljivu aktivnost. Zbog toga se uvođenje mora veoma pažljivo planirati. Ovo je veoma bitno jer promašaji i greške na početku uvođenja novog informacionog sistema mogu veoma da kompromituju ulogu informacionog sistema i da stvore otpor prema njegovom uvođenju.

Zbog osetljivosti prelaza na novu organizaciju koju donose novi, informacioni sistemi, veoma je čest slučaj da se uz novu organizaciju još izvestan period, zbog sigurnosti obrade, zadrži funkcionisanje stare organizacije, odnosno starog načina obrade podataka. To je faza paralelnog rada u toku kojeg se proverava i kontroliše kvalitet i pripremljenost novog informacionog sistema.

Novi informacioni sistem i organizacija koju on nameće moraju da budu savršeni od stare jer se koristi savršenija tehnologija što treba da doprinese kvalitetnijoj obradi podataka i informacija. Kontrola rezultata funkcionisanja ne može se sprovoditi pomoću mera stare organizacije.

Ocena funkcionisanja novog informacionog sistema treba da sadrži kritičko praćenje i vrednovanje organizacije i informacionih podsistema i informacionog sistema

kao celine. Ovo je neophodno jer se u toku postavljanja nove organizacije mogu napraviti razne greške i propusti koje se tek prilikom funkcionisanja informacionog sistema mogu uočiti.

Od projektovanja do realizacije projekta i stvarnog funkcionisanja informacionog sistema često se mogu promeniti okolnosti pod kojima sistem funkcioniše a da te okolnosti nisu mogle ranije da se predvide.

3.4.2. Upravljanje rizikom informacionog sistema

Rizik informacionog sistema⁷² definiše verovatnoću da će se u toku operativnog rada ili tokom njegovog razvoja i unapređenja pojaviti neželjeni i neprihvatljivi događaji. Rizici u informacionom sistemu mogu se klasifikovati u mnoge kategorije mada je jasno definisanje kategorija rizika koji se mogu primeniti na široku oblast upravljanja informacionim sistemima je prilično težak zadatak. Suština klasifikacije rizika nije u precizno definisanim kategorijama rizika, već u njihovom identifikovanju, opisu i upravljanju.

Osnovni tipovi rizika:

- predodređeni rizici – rizici koji će postojati, bez obzira na sve preduzete akcije,
- rizici performansi – rizici koji su vezani za izabrani pristup projektovanja, implementacije, upravljanja i rada IS,
- programski rizici – rizici vezani za organizacionu strukturu, stručnost, iskustvo i veštine zaposlenih,
- rizici dinamičkih planova – rizik da se neće ispoštovati vremenski rokovi,
- troškovni rizici – loše planiranje troškova i njegove posledice,
- tehnički rizici – problemi sa prestankom rada sistema,
- rizici vezani za podršku – neodgovarajuće ili potpuno nepostojanje podrške nakon isporuke proizvoda klijentu,
- rizici razvoja, i
- rizici vezani za komunikaciju – problemi u komunikaciji i nedovoljna komunikacija, problem prilikom uključivanja i obuke novih ljudi.

Sigurnosni rizici IS zasnovani na kontrolnim ciljevima ISO 17799:2005 (Bezbedonosne tehnike u informacionoj tehnologiji) dati su u tabeli:

oznaka	oblast rizika	primeri rizika
3.1 Politika sigurnosti informacija		
3.1.1	Dokument politike sigurnosti informacija	- Narušavanje sigurnosti zbog nepoznavanja ili pogrešnog razumevanja politike od strane zaposlenih. - Zaposleni nemaju razvijeni nivo svesti o politikama i standardima.
3.1.2	Proces pregleda i ocena	- Narušavanje sigurnosti zbog neažurirane politike i procedura zaštite.

⁷² Cascarino Richard, Information Systems Auditing, John Wiley & Sons Inc., USA, 2007

		- Narušavanje sigurnosti zbog toga što rukovodstvo ne podržava politiku
4. Sigurnost organizacije		
4.1 Sigurnost organizacije		
4.1.1	Odlučivanje o potrebi zaštite informacija	Zaposleni izvan informacione tehnologije nisu uključeni u razmatranje sigurnosti.
4.1.2	Koordiniranje sigurnosti informacija	Zaposleni izvan informacione tehnologije nisu uključeni u razmatranje sigurnosti.
4.1.3	Dodela odgovornosti o zaštiti informacija	Narušavanje sigurnosti zbog nejasno i neadekvatno dodeljenih odgovornosti za sigurnost.
4.1.4	Proces davanja ovlašćenja za sredstva informatičke obrade	- Nabavljanje neodgovarajuće opreme. - IT budžeti nisu usklađeni sa strateškim planovima. - Neovlašćena instalacija novog softvera.
4.1.5	Saveti stručnjaka iz sigurnosti informacija	Narušavanje sigurnosti zbog nedostataka ili neodgovarajućih konsultacija.
4.1.6	Saradnja među organizacijama	- Otkrivanje poverljivih informacija prilikom razmene podataka sa drugim organizacijama. - Procedure nisu u skladu sa politikama zaštite.
4.1.7	Nezavistan proces ocene sigurnosti informacija	- Nedostatak usklađenosti sa Politikom sigurnosti informacija. - Narušavanje sigurnosti zbog nesprovođenja kontrole.
4.2 Sigurnost pristupa spoljnih saradnika		
4.2.1	Identifikacija rizika od pristupa spoljnih saradnika	- Spoljni saradnici koji rade za nas ne moraju pristupiti u skladu sa propisima. - Otkrivanje poverljivih informacija zbog nedostatka sporazuma o zabrani otkrivanja.
4.2.2	Sigurnosni zahtevi u ugovorima sa spoljnim saradnicima	Neovlašćeni, neadekvatni, nekontrolisani logički i fizički pristup spoljnih saradnika.
4.3 Outsourcing		
4.3.1	Sporazum o sigurnosti sa trećom stranom	Narušavanje sigurnosti zbog nepostojanja ili neadekvatnosti sklopljenih ugovora o sigurnosti.
5. Klasifikacija i kontrola imovine		
5.1 Odgovornost za imovinu		
5.1.1	Inventar imovine	- Narušavanje sigurnosti zbog neidentifikovane imovine. - Narušavanje sigurnosti zbog nejasnog vlasništva imovine.
5.2 Klasifikacija informacija		
5.2.1	Klasifikacija informacija	Narušavanje sigurnosti zbog neadekvatne ili neažurne klasifikacije informacija.
5.2.2	Obeležavanje stepena tajnosti i važnosti, kao i	Narušavanje sigurnosti zbog nekorektnog obeležavanja informacija.

	upravljanje informacijama	
6. Sigurnost zaposlenih		
6.1 Sigurnost u definisanju poslova i nalaženju resursa		
6.1.1	Obuhvatiti sigurnost poslovnih dužnosti	Zaposleni narušavaju politiku sigurnosti zbog nejasnih i nedefinisanih dužnosti.
6.1.2	Politika kontrole zaposlenih	Prevara, krađa, zloupotreba sredstava za obradu informacija od strane zaposlenog.
6.1.3	Sporazumi o poverljivosti	Otkrivanje poverljivih ili ličnih informacija od strane zaposlenog.
6.1.4	Uslovi zapošljavanja	Nedostatak usklađenosti sa politikom i standardima iz oblasti sigurnosti.
6.2 Obuka korisnika		
6.2.1	Edukacija i obuka iz oblasti zaštite informacija	Narušavanje sigurnosti zbog niskog nivoa svesti o politici sigurnosti informacija, kontrolama i pravnim odgovornostima.
6.3 Reagovanje na incidente i sigurnosne propuste		
6.3.1	Izveštavanje o sigurnosnim incidentima	Neuspešno izveštavanje o incidentima zbog nedostatka ili neadekvatnih kanala komunikacije
6.3.2	Izveštavanje o sigurnosnim slabostima	Neuspešno izveštavanje o incidentima zbog nedostatka ili neadekvatnih kanala komunikacije
6.3.3	Izveštavanje o grešakama u zaštiti softvera	Neuspešno izveštavanje o incidentima zbog nedostatka ili neadekvatnih kanala komunikacije
6.3.4	Učenje na osnovu prethodnih iskustava	Ponavljanje incidenata/neadekvatne ili nedovoljne procedure za rukovanje incidentima
6.3.5	Disciplinski postupak	Nepostojanje disciplinskog postupka
7. Fizička zaštita i sigurnost okruženja		
7.1 Bezbedne zone		
7.1.1	Parametar fizičke bezbednosti	Neovlašćeni fizički pristup zbog nedostatka kontrola ulaza.
7.1.2	Kontrole fizičkog ulaza	Neovlašćeni fizički pristup zbog nedostatka kontrola ulaza.
7.1.3	Kancelarije, sobe i bezbedonosna oprema	Neovlašćeni fizički pristup zbog nedostatka kontrola ulaza.
7.1.4	Rad u bezbednim zonama	Neovlašćeni pristup informacijama i sredstvima za obradu informacija.
7.1.5	Izolovane zone	Neovlašćeni pristup informacijama i sredstvima za obradu informacija preko nezaštićenih izolovanih zona.
7.2 Zaštita opreme		
7.2.1	Smeštaj i zaštita opreme	- Krađa. - Nedostupnost informacija i/ili sredstava za obradu informacija.
7.2.2	Napajanje električnom energijom	Prestanak ili neadekvatno napajanje električnom energijom.
7.2.3	Osiguranje kablova i	- Oštećenje kablova.

	izolacija	- Nedostupnost informacija i/ili sredstava za obradu informacija.
7.2.4	Održavanje opreme	- Hardverske greške. - Nedostatak sigurnosne opreme. - Neažurna dokumentacija.
7.2.5	Zaštita opreme koja se koristi izvan kancelarija	- Prenosni računari i mobilni telefoni mogu biti ukradeni. - Neodgovarajuće osiguranje. - Otkrivanje, menjanje i uništenje poverljivih informacija. - Neovlašćeni pristup.
7.3 Opšte kontrole		
7.3.1	Politika urednog stola i zaključavanja računara	Nedostupnost informacija i/ili sredstava za obradu informacija.
7.3.2	Uklanjanje imovine	Krađa.
8. Komunikacije i upravljanje operacijama		
8.1 Operativne procedure i odgovornosti		
8.1.1	Dokumentovane operativne procedure	Zloupotreba sredstava za obradu informacija.
8.1.2	Kontrola operativnih promena	Pad sistema zbog neovlašćenih promena.
8.1.3	Procedure upravljanja incidentima	- Nemogućnost podnošenja izveštaja o incidentima zbog nedostatka procedura. - Narušavanje sigurnosti ili kršenje zakona zbog neodgovarajućeg odgovora na incidente iz domena sigurnosti.
8.1.4	Razdvajanje dužnosti	Prevara/falsifikovanje/zloupotreba sistema.
8.1.5	Razdvajanje razvojnog i produkcionog okruženja	- Neovlašćena modifikacija fajlova ili sistemskog okruženja. - Unos neovlašćenog i netestiranog koda aplikacije ili malicioznog koda - Neovlašćena izmena operativnih podataka.
8.1.6	Upravljanje spoljnim kapacitetima	
8.2 Planiranje i prihvatanje novih sistema		
8.2.1	Planiranje kapaciteta	Ne postoji dovoljno sistemskih resursa.
8.2.2	Prihvatljivost sistema	Pad i nestabilan rad novog sistema.
8.3 Zaštita od malicioznog softvera		
8.3.1	Kontrole malicioznog softvera	Virusi.
8.4 Arhiviranje		
8.4.1	Backup informacija	Gubljenje ili oštećenje informacija.
8.4.2	Logovi operatera	Nedostatak monitoringa.
8.4.3	Logovi grešaka	Nedovoljane i neadekvatne korektivne akcije nakon pojave greške.
8.5 Upravljanje mrežom		

8.5.1	Kontrola mreže	Neovlašćeni pristup informacijama.
8.6 Upravljanje medijima i zaštitom		
8.6.1	Upravljanje prenosnim računarskim medijima	Neovlašćeno uklanjanje računarskih medija/otkrivanje, modifikacija i gubitak informacija.
8.6.2	Odlaganje medija	Otkrivanje poverljivih medija trećoj strani.
8.6.3	Procedure za upravljanje informacijama	Otkrivanje, modifikacija i gubitak informacija.
8.6.4	Bezbednost sistemske dokumentacije	Nedostupnost informacija i sredstava za obradu informacija.
8.7 Razmena informacija i softvera		
8.7.1	Sporazumi o razmeni informacija i softvera	Neovlašćeni pristup informacijama koje se razmenjuju među organizacija.
8.7.2	Sigurnost medija tokom transporta	Nepouzdanost offsite čuvanja podataka.
8.7.3	Sigurnost elektronske trgovine	Spori veb servisi.
8.7.4	Sigurnost elektronske pošte	- Maliciozni softveri koji su preuzeti ili se nalaze u porukama. - Kršenje zakona o privatnosti. - Pogrešno usmeravanje ili preusmeravanje pri slanju poruka. - Prekidi i prisluškivanje. - Kompromitovanje organizacije.
8.7.5	Sigurnost elektronskih sistema u kancelarijama	
8.7.6	Dostupni sistemi elektronskog publikovanja	Neovlašćeni pristup i neovlašćeno preuzimanje softvera od treće strane.
8.7.7	Druge vrste razmene informacija	Otkrivanje poverljivih informacija.
9. Kontrola pristupa		
9.1 Poslovni zahtev za kontrolom pristupa		
9.1.1	Politika kontrole pristupa	Neovlašćeni pristup sredstvima za obradu informacija.
9.2 Upravljanje korisničkim pristupom		
9.2.1	Registrovanje korisnika	- Neovlašćeni pristup informacijama. - Nepostojanje jedinstvene identifikacije i autentifikacije korisnika.
9.2.2	Upravljanje prilikom pristupa i pravima pristupa	- Neovlašćeni pristup zbog nepostojanja procesa upravljanja lozinkama. - Nezaštićeno rukovanje lozinkama. - Izostanak redovnog pregleda pristupa i dodeljenih privilegija.
9.2.3	Upravljanje korisničkim lozinkama	- Neovlašćeni pristup zbog nepostojanja procesa upravljanja lozinkama. - Nezaštićeno rukovanje lozinkama.

		- Izostanak revodnog pregleda pristupa i dodeljenih privilegija.
9.2.4	Proces pregleda korisničkih prava	- Neovlašćeni pristup zbog nepostojanja procesa upravljanja lozinkama. - Nezaštićeno rukovanje lozinkama. - Izostanak revodnog pregleda pristupa i dodeljenih privilegija.
9.3 Odgovornosti korisnika		
9.3.1	Korišćenje lozinke	Izbor loših lozinki.
9.3.2	Korisnička oprema bez nadzora	Neovlašćeni pristup opremi bez nadzora.
9.4 Kontrola pristupa mreži		
9.4.1	Politika upotrebe mrežnih servisa	
9.4.2	Putanja pristupa	
9.4.3	Autentifikacija korisnika spoljnih konekcija	Neovlašćeni pristup informacijama i mrežama.
9.4.4	Autentifikacija čvorova	
9.4.5	Zaštita udaljenog dijagnostičkog priključka	
9.4.6	Razvdajanje mreža	
9.4.7	Kontrola mrežne konekcije	
9.4.8	Kontrola usmerenja mreže	
9.4.9	Sigurnost mrežnih servisa	
9.5 Kontrola pristupa operativnom sistemu		
9.5.1	Automatska identifikacija terminala	Neovlašćeni pristup računarima.
9.5.2	Log on procedure terminala	Neovlašćeni pristup računarima, mrežama i servisima.
9.5.3	Identifikacija i autentifikacija korisnika	Nepostojanje jedinstvene identifikacije korisnika.
9.5.4	Alati za upravljanje lozinkama	
9.5.5	Korišćenje pomoćnih sistemskih programa	Zloupotreba pomoćnih sistemskih programa.
9.5.6	Upozorenje o potrebi za sprovođenjem mera zaštite korisnika	Neovlašćeni pristup računarima, mrežama i servisima.
9.5.7	Time out terminala	Neovlašćeni pristup/neadekvatno kašnjenje pre time out-a.
9.5.8	Ograničeno vreme konekcije	Neovlašćeni pristup računarima, mrežama i servisima.
9.6 Kontrola pristupa aplikacijama		
9.6.1	Kontrola pristupa aplikacijama, ograničeni	Neovlašćeni pristup informacijama i aplikacijama.

	pristup informacijama	
9.6.2	Izolacija osetljivih informacija	Neovlašćeni pristup informacijama i aplikacijama.
9.7 Nadgledanje pristupa i korišćenja sistema		
9.7.1	Evidencija događaja	Nepostojanje provere evidencije sistemskih događaja.
9.7.2	Nadgledanje korišćenja sistema	Nepostojanje provere evidencije sistemskih događaja.
9.7.3	Sinhronizacija vrmeena	Nedostatak dokaza.
9.8 Rad na prenosnom računaru i rad od kuće		
9.8.1	Rad ne prenosnom računaru	Neovlašćeni pristup informacijama i opremi.
9.8.2	Rad od kuće	Neovlašćeni pristup informacijama i opremi.
10. Razvoj i održavanje sistema		
10.1 Sigurnosni zahtevi sistema		
10.1.1	Analiza i specifikacija sigurnosnih zahteva	Nedovoljna sigurnost informacija ugrađena u sistem
10.2 Sigurnost u aplikacijama		
10.2.1	Obrada ulaza i verifikacija izlaza	Greška
10.2.2	Kontrola interne obrade podataka u aplikacijama	Greška
10.2.3	Autentifikacija poruka	Oštećenje poruka
10.2.4	Validacija izlaznih podataka	
10.3 Kontrole šifrovanja (kriptografije)		
10.3.1	Politika sprovođenja kontrole šifrovanja	
10.3.2	Proces šifrovanja	Prekidi i prisluškivanje.
10.3.3	Digitalni potpisi	
10.3.4	Servisi za neporecivost	
10.3.5	Upravljanje ključevima za šifrovanje	
10.4 Sigurnost sistemskih fajlova		
10.4.1	Kontrola operativnog softvera	– Oštećenje operativnih sistema – Ažuriranje i unošenje promena u operativni sistem bez ovlašćenja – Nepostojanje backup-a prethodnih verzija
10.4.2	Zaštita sistema podataka za testiranje	– Korišćenje produkcionih podataka za testiranje – Zajedničko razvojno, produkciono i testno okruženje – Nedostatak formalnog prihvatanja testiranja od strane korisnika – Razdvajanje dužnosti pri testiranju – Neovlašćeni pristup test podacima
10.4.3	Kontrola pristupa biblioteci	Oštećenje računarskih programa/ neovlašćeni

	izvornih programa	pristup bibliotekama izvornih programa
10.5 Sigurnost u procesima razvoja i pružanja podrške		
10.5.1	Promena u kontrolnim procedurama	Neovlašćene promene u softveru
10.5.2	Tehnički pregled promena u operativnom sistemu	Narušavanje sigurnosti zbog promena u funkcionisanju softvera
10.5.3	Ograničenja u promenama softverskih paketa	Neovlašćena modifikacija softverskih paketa
10.5.4	Tajni ulazi aplikacije	Maliciozni kod
10.5.5	Outsourcing softvera	Narušavanje sigurnosti od strane ugovarača
11. Upravljanje kontinuitetom poslovanja		
11.1 Aspekti upravljanja kontinuitetom poslovanja		
11.1.1	Proces upravljanja kontinuitetom poslovanja	Prekidi poslovnih funkcija
11.1.2	Upravljanje kontinuitetom poslovanja	– Nepostojanje planova/strategija – Pogrešna procena rizika i uticaja
11.1.3	Razvoj i implementacija planova za kontinuitet poslovanja	– Nepostojanje procedura za postupanje u hitnim slučajevima – Nepostojanje jasno definisanih odgovornosti – Nedostatak instrukcija za operativni rad – Potpuni oporavak sistema
11.1.4	Okvir za planiranje poslovnog kontinuiteta	– Nedoslednost planova za kontinuitet poslovanja – Nedovoljna informisanost kada treba aktivirati plan – Spoljni saradnici nemaju planove za vanredne slučajeve – Ne postoji jasno izvršena transformacija odgovornosti
11.1.5	Testiranje, održavanje i ponovna evaluacija planova za kontinuitet poslovanja	– Neefikasni planovi – Nepostojanje edukacije i testiranja – Nizak nivo svesti – Nepostojanje procesa pregleda i ažuriranja planova
12. Usklađenost		
12.1 Usklađenost sa šravnim zahtevima		
12.1.1	Identifikacija primenjivih zakonskih propisa	Neusklađenost sa primenjivim zakonskim propisima
12.1.2	Prava intelektualne svojine	– Kršenje prava intelektualne svojine – Kršenje softverskih autorskih prava
12.1.3	Mere zaštite evidencija u organizaciji	Uništavanje/falsifikacija/gubljenje značajnih evidencija u organizaciji
12.1.4	Zaštita podataka	Otkrivanje poverljivih podataka
12.1.5	Sprečavanje zloupotrebe sredstava za obradu podataka	Zloupotreba sredstava za obradu podataka

12.1.6	Propisi za kontrole šifrovanja	
12.1.7	Prikupljanje dokaza	Nemogućnost obezbeđivanja osnovnih dokaza
12.2 Procesi pregleda politike sigurnosti informacija i tehničke usklađenosti		
12.2.1	Usklađenost sa politikom sigurnosti informacija	Neusklađenost sa politikom sigurnosti informacija
12.2.2	Provera tehničke usklađenosti	Nedostatak testiranja mogućnosti upada u sistem
12.3 Razmatranje revizije čitavog sistema		
12.3.1	Kontrole sistemske revizije	
12.3.2	Dobijanje nezavisnih garancija	Nepostojanje nezavisne garancije kvaliteta internih kontrola

Data tabela obuhvata najčešće rizike informacionog sistema i može se koristiti kao dobra polazna osnova za identifikaciju rizika u svakoj konkretnoj organizaciji.

3.5. ULOGE I ODGOVORNOSTI PRI UPRAVLJANJU OPERATIVNIM RIZICIMA

Prikaz uloga i odgovornosti pojedinih organa pri upravljanju operativnim rizicima:

Nadzorni odbor:

Odgovornosti	➤ Obezbeđuje da okvir upravljanja operativnim rizicima bude izložen efektivnoj i sveobuhvatnoj internoj reviziji od strane nezavisnog i kompetentnog osoblja ➤ Obezbeđuje da upravljanje operativnim rizicima bude predmet eksterne revizije.
Odnosi sa drugim organizacionim delovima	Interna revizija

Predsednik izvršnog odbora:

Odgovornosti	➤ Usvaja periodično pregleda i odobrava okvir upravljanja operativnim rizicima ➤ Vršiti pregled mapiranja rizika i programa upravljanja rizicima ➤ Na osnovu preporuka donosi odluke o preduzimanju novih akcija kao što je definisano u programu upravljanja operativnim rizicima ➤ Vodi računa o izvršenju kontrola kao što je definisano u upravljačkom programu upravljanja rizicima
Odnosi sa drugim organizacionim delovima	Sektor upravljanja rizicima Odbor za informacionu tehnologiju

Interna revizija:

Odgovornosti	➤ Revizija delova oblasti operativnih rizika i interne kontrole upravljanje operativnim rizicima ➤ Preporuke za implementaciju internih kontrola u cilju minimiziranja identifikovanih rizika. ➤ Pregleda operativne rizike i kontroliše proces samoocenjivanja ➤ Ocenjuje efikasnost i efektivnost operativnog rizika i kontroliše proces samoocenjivanja
Odnosi sa drugim organizacionim delovima	Nadzorni odbor, Predsednik izvršnog odbora, Skupština Banke

IT Odbor:

Odgovornosti	Razmatra i daje preporuke strategije razvoja IS-a i funkcionisanja IS-a sa aspekta upravljanja operativnim rizicima (smernice procedura, obim razvoja, alati, razvoj informacionih tehnologija na globalnom nivou) Razmatra i daje preporuke politika i procedura za upravljanje operativnim rizicima sa aspekta funkcionisanja IS-a. Razmatra i daje preporuke za metodologiju razvoja IS-a sa aspekta upravljanja operativnim rizicima Odobrava implementaciju novih alata iz oblasti informacionih tehnologija, a u skladu sa strategijom razvoja IS-a i politikom i procedurom za upravljanje operativnim rizicima
Učesnici	Prema postojećoj strukturi

Funkcija upravljanja rizicima:

Odgovornosti	➤ Odgovornost za upravljanje operativnim rizicima ➤ Razvijanje i praćenje okvira upravljanja operativnim rizicima ➤ Praćenje izvršavanja politike operativnih rizika i procedura u banci ➤ Preporuke generalnom direktoru u vezi sa implementacijom internih kontrola koje su definisane u okviru upravljanja operativnim rizicima
Odnosi sa drugim organizacionim delovima	Predsednik izvršnog odbora Interna kontrola / Upravljanje operativnim rizicima Rukovodioci sektora Odbor za informacionu tehnologiju

Interna kontrola:

Odgovornosti	➤ Odgovornost za upravljanje operativnim rizicima ➤ Samoocenjivanje operativnih rizika u okviru poslovnih jedinica u bliskoj saradnji sa direktorima poslovnih sektora i zaposlenima ➤ Pripremanje programa upravljanja operativnim rizicima u okviru poslovnih sektora u saradnji sa direktorima tih poslovnih sektora i zaposlenima ➤ Odgovornost za razvijanje, implementaciju i funkcionisanje internih kontrola kao što je definisano u programu upravljanja operativnim rizicima ➤ Praćenje pridržavanja politike i procedura upravljanja operativnim rizicima ➤ Obezbeđenje da svi trenutno zaposleni kao i novo zaposleni razumeju i rade u skladu sa okvirom upravljanja operativnim rizicima ➤ Usklađivanje poslovanja banke sa zakonskim i pod zakonskim aktima u vezi sa upravljanjem operativnim rizicima ➤ Ocena planova poslovanja poslovnih jedinica u saradnji sa direktorima poslovnih sektora i zaposlenima, periodično ocenjivanje planova ➤ Ocena planova za obnovu informacionih sistema u slučaju pada zajedno sa direktorom sektora informacione tehnologije i periodično testiranje tih planova
Odnosi sa drugim organizacionim delovima	Odeljenje upravljanja rizicima Predsednik izvršnog odbora Rukovodioci sektora / Zaposleni zaduženi za operativne rizike Odbor za informacionu tehnologiju

Dijagnostički pregled – Upravljanje operativnim rizicima:

Oblast	Postojeća praksa (Korišćeni dokumenti)	Odgovornosti
1. Politika i procedure operativnih rizika koje obuhvataju: - Procese (Identifikaciju, Ocenu, Kontrolu i praćenje) - Pregled metodologija za identifikaciju i ocenu, - Struktura upravljanja, - Program upravljanja, - Struktura izveštavanja.	- Postoji politika i procedura Interne kontrole ali ne i sveobuhvatna politika i procedura za upravljanje operativnim rizicima u skladu sa Bazelom II. - Rad interne kontrole je utvrđen Odlukom o osnovnim principima organizacije i rada Interne kontrole banaka i drugih finansijskih organizacija ("Sl. list SRJ br. 39/02) i članovima Statuta banke Takođe postoji pravilnik o organizaciji i načinu rada Interne kontrole. Godišnji program kontrole koji donosi predsednik izvršnog odbora banke i operativni plan rada koji sadrži opis, obuhvat interne kontrole i definisane periode za kontrolu.	Sektor Interne kontrole

	- U okviru dobijenih materijala iz Sektora interne kontrole definisani su: - Spisak aktivnosti sektora interne kontrole u datoj godini, - Osnovi za pokretanje disciplinskog postupka, - Način rada interne kontrole, - Procedura izveštavanja.	
2. Procesi i Metodologije za identifikaciju rizika i ocenu koje obuhvataju: - Definisanje – Definisanje obuhvatnosti - Klasifikaciju, Samoocenjivanje - Bodovanje/Merenje - Mapiranje	- Operativni rizici su identifikovani kao: nedostaci organizacije banke, tehnologije, obrazovanje kadrova i nepažnja zaposlenih prilikom vršenja poslova. - Operativni rizici nisu identifikovani u skladu sa Bazelom II. - Procesi i metodologije za struktuiranu identifikaciju operativnih rizika nisu definisani. - Identifikacija rizika i metodologije za ocenu operativnih rizika (samoprocenjivanje i mapiranje) nisu u skladu sa Bazelom II.	Sektor Interne kontrole
3. Procesi za Kontrolu rizika i praćenje obuhvatajući: - Komunikaciju – tokove informacija, - Interne sisteme kontrole i kulturu kontrole, - Utvrđivanje ispravnosti, otklanjanje nedostataka i potvrdu– Interna revizija	- Ne postoje definisani procesi za kontrolu i praćenje rizika u skladu sa Bazelom II. - Interna revizija obavlja reviziju adekvatnosti procesa upravljanja operativnim rizicima. - Takođe, Interna revizija vrši pregled predloženih politika i procesa upravljanja operativnim rizicima pre njihovog usvajanja od strane upravnog odbora - Interna kontrola o svom radu izveštava upravni odbor.	Sektor Interne kontrole

3.6. E – BANKING

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja. Glavni cilj je postao da se bez obzira na geografske distance što brže i efikasnije povežu klijenti i tokovi informacija. U uslovima vrlo jake konkurencije gde postepeno nestaju razlike između banaka, investicionih banaka, brokerskih firmi i osiguravajućih kompanija, finansijske organizacije su pod stalnim pritiskom da zadrže korisnike svojih usluga, smanje troškove, upravljaju rizikom i koriste tehnologiju kao izvor konkurentne prednosti. Model globalne organizacije i jake konkurencije zahteva novu koncepciju pristupa banaka u njihovom poslovanju, o čemu svedoče sve veća ulaganja u specijalizovanu prema klijentu orijentisanu tehnologiju.

Banke su prvobitno imale odbojnost prema inovacijama koje donosi poslovanje na Internetu, ali su tokom vremena uvidele da to nije prolazni fenomen nego sve više deo poslovne stvarnosti sa još većom perspektivom u budućnosti.

Elektronsko bankarstvo, kao specifičan deo elektronskog poslovanja, ima mnoge prednosti u odnosu na klasično poslovanje. Tu spadaju smanjenje troškova transakcija,

brži obrt sredstava, siguran i bezbedan platni promet, ušteda u vremenu, mogućnost obavljanja transakcija sa radnog mesta kao i stalni uvid u stanje na računu i promet.

Do 60-tih godina prošlog veka osnovna funkcija banaka je bila kreditno-depozitna funkcija. Proces inovacija koji se odnosi na razvoj bankarskih proizvoda i usluga, razvoj žišta kapitala, kao i širenje konkurencije na međunarodnom finansijskom tržištu dovode o širenja palete bankarskih proizvoda i usluga. Tradicionalne bankarske poslove, sve više amenjuju savremeni bankarski poslovi kao što su: konsalting poslovi, emitovanje i trgovina hartijama od vrednosti, što sve dalje uslovljava i dovodi do organizovanja finansijskih konglomerata i stvaranja finansijskih supermarketa. Osnovni preduslov za stvaranje ovakvih integrisanih bankarskih sistema je razvoj i primena informacione tehnologije u bankarstvu. Početak uspostavljanja globalnog bankarstva i globalnog finansijskog tržišta vezuje se za pojavu bankarskog inženjeringa i reinženjeringa. Bankarski inženjering se odnosi na primenu bankomata, personalnih računara, i automatskih bankarskih šaltera, dok su za bankarski reinženjering karakteristične aktivnosti koje se odnose na daljinsko upravljanje bankom, odnosno kućno bankarstvo.

Informacione tehnologije su presudno doprinele razvoju usluga elektronskog bankarstva. Otvorene su nove mogućnosti za banke u delu depozitnih i kreditnih poslova, mogućnosti ponude novih proizvoda i usluga, poboljšanja konkurentne pozicije, smanjenja troškova, itd. Naravno, banke se prilikom pružanja usluga elektronskog bankarstva suočavaju s određenim specifičnim rizicima (koji su usmereni na *retail banking*), među kojima se izdvajaju operativni, reputacioni, pravni i rizik internacionalnog poslovanja. Savremeno bankarsko poslovanje je svakodnevno izloženo postojećim (evidentiranim) i novim rizicima.

Menadžment banke mora rizike identifikovati, proceniti, kontrolisati i finansirati. Upravljanje rizicima predstavlja proces projekt menadžmenta koji se obavlja u kontinuitetu, preko praćenja i procenjivanja.

Bez obzira što na razvoj elektronskog bankarstva utiče više faktora, najviše su prisutni sledeći faktori:

a) visok stepen informacione tehnologije i postojanje visoko stručnih kadrova, b) raznovrsna finansijska struktura, sa većim brojem finansijskih institucija i visoko frekventnim finansijskim tokovima,

c) deregulacija bankarskih i finansijskih tržišta, uz značajno prisustvo konkurencije i sl.

Razvoj elektronskog bankarstva⁷³ podrazumeva da se sve više uvode savremene elektronske procedure plaćanja, isključivo zasnovane na elektronskom transferu sredstava. Elektronski transfer sredstava (Electronic Funds Transfer – EFT) eliminiše potrebu fizičkog prenosa kreditnih poruka na papirnim nosiocima podataka, odnosno primena EFT sistema omogućava da se za nekoliko sekundi izvrši plaćanje sa računa dužnika na račun poverioca. Treba praviti razliku između EFT i EPS sistema, jer je EFT sistem širi pojam od EPS sistema. EPS sistem (Electronic Payments System) se odnosi samo na elektronski sistem plaćanja, dok se EFT sistem odnosi na svaki oblik elektronskog prenosa sredstava.

⁷³ Rose S. Peter: Comercial Bank Management, Thind Edition, Irwin, 1995

RIZICI I UPRAVLJANJE RIZICIMA U ELEKTRONSKOM BANKARSTVU

Saglasno dokumentima Bazelskog komiteta za bankarsku superviziju, mogu se navesti sledeće vrste rizika u elektronskom bankarstvu⁷⁴:

- 1.) operativni rizik,
 - 2.) reputacioni rizik,
 - 3.) pravni rizik,
 - 4.) rizik internacionalnog poslovanja,
 - 5.) ostali rizici (kreditni, tržišni, kamatni, valutni, politički, zakonski, rizik likvidnosti, rizik solventnosti i rizik kapitala banke).
- trojaka: a) prihvatanje rizika, b) izbegavanje rizika, c) zaštita od potencijalnog rizika. Nakon izabrane taktike upravljački tim banke donosi odluku o izboru odgovarajućih instrumenata za upravljanje rizicima u banci. Proces kontrole rizika treba da uključi čitavu bankarsku hijerarhiju (od vrha do dna) radi minimiziranja rizika u elektronskom bankarstvu.

Operativni rizik nastaje iz potencijalnog gubitka usled nedostataka u sistemu pouzdanosti i integriteta. Razmatranje sigurnosti je od najveće važnosti, usled mogućnosti internih i eksternih napada na banku, odnosno njenih sistema i proizvoda. Operativni rizik može nastati i usled zloupotrebe od strane klijenata ili neadekvatnog dizajniranog ili implementiranog elektronskog bankarstva ili sistema elektronskog novca. Shodno iznetom, mogući su sledeći oblici operativnog rizika, i to:

- rizici sigurnosti (pouzdanosti i integriteta sistema),
- rizici dizajniranja, implementacije i održavanja sistema,
- rizici zloupotrebe proizvoda ili usluga od strane klijenata.

Rizici sigurnosti se pojavljuju u vezi sa kontrolom informacija pomoću kojih banka komunicira sa okruženjem, transfera elektronskog novca, kao i sprečavanja pronevere, odnosno falsifikata. Primer mogućeg rizika sigurnosti jeste neautorizovani pristup sistemu. To znači da poverljive informacije mogu biti presretane od strane neautorizovanih lica, na primer, od strane hakera koji ulaze u interne sisteme. Banke mogu da primene određene mere za upravljanje rizikom. Moguće je primeniti sigurnosne komunikativne mere, kao što su „fire wall“, lozinke, tehnologiju šifrovanja i autorizaciju korisnika. Potrebno je vršiti testiranje na „ranjivost“ sistema, kao i stalno proveravanje sistema na viruse.

Rizici dizajniranja, implementacije i održavanja sistema imaju bitan uticaj na azvoj sistema elektronskog bankarstva i elektronskog novca. Rizici koji se mogu manifestovati iz ovog delu su prekid ili usporavanje sistema, što može imati negativne konsekvence na klijente banke. Nije redak slučaj da se banke opredeljuju za spoljne provajdere i eksperte za implementaciju, funkcionisanje i podršku koja obezbeđuje nesmetano odvijanje elektronskog bankarstva i poslove sa elektronskim novcem. Jedan od mogućih rizika dizajniranja, implementacije i održavanja sistema, predstavljaju zaposleni i menadžment koji teže prihvataju inovacije. Izuzetno brze izmene tehnologije mogu da dovedu do toga da menadžment i zaposleni u banci nisu u potpunosti u mogućnosti da shvate prirodu nove tehnologije koja se primenjuje u bankama. Rezultat

⁷⁴ Horne C. Van James: Financial Management and Policy, Prentice-Hall Inc, New York, 1999

toga je slaba implementacija novih tehnologija i nemogućnost da se obezbedi kontinuirana podrška razvoju. Neophodno je sprovesti obuku, kao permanentni proces, i za menadžment i za zaposlene⁷⁵.

Zloupotreba proizvoda i usluga od strane klijenata, bilo namerna ili nenamerna, je još jedan izvor operativnog rizika. Rizik se povećava usled neadekvatne edukovanosti klijenata, od strane banke, o merama sigurnosti prilikom verifikacije transfera elektronskog novca. Personalne informacije klijenata banke koji učestvuju u elektronskom bankarstvu (broj kreditne kartice, broj računa u banci, i sl.) moraju biti posebno zaštićene prilikom transakcija elektronskog novca.

Reputacioni rizik je rizik negativnog javnog mnjenja, koji rezultira značajnom gubitku sredstava ili odlivu klijenata iz banke. Njegov negativan efekat na imidž banke, može da bude trajan. Može nastati i kao posledica preduzimanja akcija koje imaju za posledicu gubitak javnog poverenja u sposobnost banke da obavlja svoje poslovanje. Značajno narušavanje imidža banke može nastati i usled loših komunikacionih mreža, pri čemu klijenti nisu u stanju da saznaju informacije o stanju na svojim računima, i sl.

Da bi banka mogla da se zaštiti od reputacionog rizika, potrebno je da pruža usluge elektronskog bankarstva dosledno i konstantno, a sve u skladu sa visokim očekivanjima klijenata. Bitno je da se uspostave mehanizmi za vanredne situacije da bi se minimizirao reputacioni rizik koji može proizići iz neočekivanih događaja, uključujući interne i eksterne prodore u sistem koji mogu uticati na pružanje usluga elektronskog bankarstva.

Pravni rizik nastaje usled narušavanja ili neusaglašenosti sa zakonima, pravilima, regulativama ili propisane prakse ili u slučaju kada zakonska prava i obaveze učesnika u transakcijama nisu pravno regulisana. Posebno mora biti regulisano sprečavanje pranja novca, jer savremena mogućnost poslovanja u velikoj meri može biti veoma atraktivna za takav vid zloupotrebe. To dovodi do zaključka da banke koje primenjuju elektronsko bankarstvo i poslovanje sa elektronskim novcem, moraju posebnu pažnju posvetiti identifikaciji, odnosno autentifikaciji klijenta, kao i zaštiti privatnosti (kao metod autentifikacije banke mogu da koriste digitalne sertifikate).

Da bi banke minimizirale pravni rizik, povezanim sa poslovima elektronskog bankarstva koji se obavljaju u zemlji i inostranstvu, potrebno je da osiguraju pružanje adekvatnih informacija na svojim web stranicama. Na taj način bi se klijentima omogućilo da provere identitet i regulatorni status banke pre nego što se upuste u transakcije elektronskog bankarstva. Primera radi, informacije koje se mogu staviti na web sajt mogu biti ime banke i lokacija sedišta, kao i lokalne filijale, način na koji klijent može kontaktirati sa bankom po pitanju reklamacija, sumnje na zloupotrebu računa i sl., način na koji se klijenti mogu žaliti organu koje se bavi zaštitom potrošača, i dr.

Rizici internacionalnog poslovanja. Elektronsko bankarstvo i aktivnosti elektronskog novca su bazirani na tehnologiji koja ne poznaje geografske barijere. Banke koje se odluče da pružaju usluge klijentima na raznim nacionalnim tržištima trebalo bi da upoznaju razne nacionalne pravne zahteve, kao i da razumeju nacionalne razlike u očekivanju i poznavanju proizvoda i usluga od strane klijenata. Sa druge strane,

⁷⁵ www.eccf.su.ac.yu

neophodno je da banka proceni rizik zemlje i razvije planove nepredviđenih obaveza koji će predvideti aktivnosti u slučaju ekonomskih ili političkih problema na nacionalnom tržištu. Pod ekonomskim problemima se podrazumevaju promene privrednih kretanja, privrednog razvoja, uslova poslovanja u određenoj zemlji i njena spoljna likvidnost, dok se pod političkim problemima podrazumeva promena u sastavu vlade ili vladine politike, politički nemiri ili ratovi. Naravno da se navedene ekonomske i političke promene smatraju problemima ukoliko idu na štetu poslovanju banke.

Ostali rizici. Ostale bankarske rizike uključuje i kreditni rizik, rizik likvidnosti, kamatni rizik i tržišni rizik, koji mogu nastati iz elektronskog bankarstva i poslovanja sa elektronskim novcem.

Kreditni rizik je rizik koji se odnosi na korisnika kredita da neće ispuniti svoju obavezu u punoj vrednosti ili u predviđeno vreme. Banke imaju mogućnost da elektronskim putem prime zahteve za kredit i da ga odobre, što zahteva adekvatne procedure za utvrđivanje kreditne sposobnosti klijenata, jer se u protivnom povećava rizik za banku.

Rizik likvidnosti je rizik koji nastaje u slučaju da banka nije u mogućnosti da izvršava dospele obaveze koje nastaju tokom elektronskog bankarstva. Rizik likvidnosti je rizik mogućnosti nastanka negativnih efekata na finansijski rezultat i kapital banke usled nesposobnosti banke da ispunjava svoje dospele obaveze.

Banka svojom imovinom i obavezama upravlja na način koji joj omogućava da u svakom trenutku ispuni svoje dospele obaveze (likvidnost) i da trajno ispunjava sve svoje obaveze (solventnost). U cilju efikasnog upravljanja rizikom likvidnosti, banka usvaja i sprovodi politiku upravljanja likvidnošću, koja obuhvata planiranje priliva i odliva novčanih sredstava, praćenje likvidnosti i donošenje odgovarajućih mera za sprečavanje ili otklanjanje uzroka nelikvidnosti.

Kamatni rizik se odnosi na smanjenje kamatnih stopa do stepena kada negativna kretanja kamatnih stopa smanjuje vrednost imovine u zavisnosti od neispunjenih obaveza. Kamatni rizik se sastoji od rizika promene kamatnih stopa na plasmane i obaveze banke, naravno ukoliko su ove promene nepovoljne za banku. Rizik kamatne stope može da nastane u slučajevima kada banke odobre određene plasmane po fiksnim kamatnim stopama na duže vremenenske periode, koji nisu praćeni adekvatnom strukturom izvora sredstava banke. Ovo znači da je banka plasirala sredstva po određenoj kamatnoj stopi na duže rokove nego što ima obezbeđene depozite. U slučaju određenih poremećaja na tržištu, izvori sredstava mogu da poskupe, što bi dovelo do situacije da banke imaju određene gubitke na plasmanima – kreditima koji su odobravani na duže rokove i pod uslovima koji su trenutno neodrživi na tržištu.

Tržišni rizik koji može nastati usled promene u cenama na tržištu, uključivši i promene deviznog kursa, kojeg svakako karakterišu oscilacije, tako da su banke koje obavljaju plaćanja u formi elektronskog novca u stranoj valuti izložene riziku.

Elektronsko bankarstvo i poslovanje sa elektronskim novcem je postalo široko primenjivano od strane banaka, kao i od strane korisnika bankarskih usluga i trgovaca. To je doprinelo da ovaj savremeni vid poslovanja prate brojni rizici. Cilj banaka je da ostvare kontrolu i upravljanje rizikom. Proces upravljanja rizikom uključuje sledeće faze:

procenu rizika, upravljanje i kontrolu rizika i monitoring rizika. Ovi procesi moraju biti pod nadzorom top menadžmenta banke.

Procenu rizika potrebno je organizovati kao permanentan proces, koji se odvija u tri faze. U prvoj fazi potrebno je da banka identifikuje, a po mogućnosti i kvantifikuje rizike. Identifikacija rizika je ključna polazna pretpostavka u procenama rizika, s obzirom na to da su najopasniji rizici oni kojih banke nisu svesne, jer mogu da dovedu do velikih i neplaniranih troškova. Identifikacija rizika moguća je na nekoliko načina, a najčešći metodi odnose se na empirijska iskustva dosadašnjeg poslovanja banaka, kao i na razmenu iskustava između samih poslovnih banaka. Ukoliko nije moguće kvantifikovati rizik, potrebno je utvrditi kako potencijalni rizik nastaje i kakve su mogućnosti da se ovi rizici ograniče. Pored toga, bitno je i to da se utvrdi učestalost, odnosno frekvencija pojave rizika. U drugoj fazi određuje se mogućnost banke u pogledu nivoa tolerancije rizika, baziranoj na oceni gubitka koji će banka moći da podnese. Ključno za sve banke jeste da, kada postanu svesne rizika s kojim posluju, načina njegovog ispoljavanja i frekventnosti pojave, utvrde procenu ispoljavanja određenog rizika. Ova procena je izuzetno bitna s obzirom na to da na osnovu procenjene vrednosti - odnosno gubitka usled ispoljavanja određenog rizika, banka treba da definiše preventivne i korektivne mere. Prioritet svakako treba da bude definisanje preventivnih mera i eliminisanje svih preliminarnih faktora koji mogu da dovedu do nastajanja određenog rizika.

S tim u vezi banke bi trebalo da za svaki od utvrđenih rizika definišu koji su to indikatori, odnosno pokazatelji čije bi pojavljivanje moglo da ukaže na nastanak određene negativne pojave, tj. rizika i da na osnovu tih indikatora definišu listu akcija za otklanjanje istih. Korektivni faktori imaju samo dejstvo na ublažavanje posledica nastalih dejstvom određenog rizika odnosno negativnog slučaja u poslovanju banke. U trećoj fazi ocenjuje se da li se izloženost riziku kreće u okviru podnošljivih limita. Treća faza je faza u kojoj bi trebalo da se definiše nadgledanje rizika ukoliko se on i desi. Ovo se posebno odnosi na primenu korektivnih mera kojima bi rizik, odnosno njegov uticaj treba da se minimizira.

Upravljanje i kontrola rizika. Nakon što se procene rizici i odrede nivoi njihove tolerancije, na menadžmentu banke je da počne sa upravljanjem rizicima i njihovoj kontroli. Upravljanje rizikom uključuje aktivnosti: implementaciju sigurnosnih mehanizama i mera, koordinaciju interne komunikacije, vrednovanje i poboljšanje proizvoda i usluga, implementaciju mera za kontrolu rizika koji se odnose na spoljne davaoce usluga i planiranje nepredvidivih okolnosti.

Sigurnosni mehanizmi i mere koje se primenjuju pri upravljanju i kontroli rizika, podrazumevaju kombinaciju sistema zaštitnih mera, aplikacija i interne kontrole, koji se koristi da se osigura integritet, autentičnost i pouzdanost podataka, operativnih procesa (obrada) i izveštaja. Zaštita je bazirana na razvoju i implementaciji adekvatnih sigurnosnih mehanizama i mera za interne procese. Pored toga, razvijaju se i implementiraju mehanizmi i mere za komunikaciju između banke i eksternih sistema, sve u cilju smanjenja rizika od eksternih i internih napada na sistem elektronskog bankarstva i elektronskog novca. Sigurnosne mere su kombinacija hardverskih i softverskih alata. Kao sigurnosne mere koristi se: šifrovanje podataka, digitalni sertifikat, instalacija zaštitnih zidova, antivirusna kontrola, korišćenje PIN-a, i sl.

Za menadžment je od osnovnog značaja da uspostavi komunikaciju sa zaposlenima u banci koji su zaduženi za funkcionisanje elektronskog bankarstva (koordinaciju interne komunikacije). Takođe, neophodna je komunikacija menadžmenta sa IT sektorom u pogled funkcionisanja dizajniranog sistema i informisanja o eventulanim slabostima, sa predlogom mera za njihovo otklanjanje.

Za implementaciju i funkcionisanje elektronskog bankarstva potreban je visok nivo edukacije zaposlenih i korisnika usluga banke, što za rezultat ima direktno smanjenje operativnog i reputacionog rizika.

Monitoring rizika. Monitoring rizika je važan aspekt bilo kog procesa upravljanja rizikom. Banka može na nekoliko načina upravljati rizikom, a jedan od osnovnih „alata“ jeste ALM (engl. *Asset and Liability Management*) koncept ili upravljanje aktivom i pasivom poslovne banke. Proces ALM-a podrazumeva da se u okviru banke identifikuju i analiziraju svi rizici, definišu odgovarajući limiti rizika (koji su u saglasnosti sa strategijom alokacije kapitala), kao i da se kontrolisano prate limiti rizika preko savremenih informacionih sistema⁷⁶. [4] Primena ALM koncepta zahteva od „top“ menadžmenta da stalno modifikuje i popravlja sisteme upravljanja rizikom.

Primer monitoringa rizika u poslovanju banaka, s fokusom na elektronske kanale distribucije proizvoda, bila bi reakcija banke u slučaju „pada“ servera koji omogućuje nesmetanu realizaciju elektronskih naloga. Šta se dešava u ovom slučaju i na koji način banke reaguju, tema je koja treba da okupira ne samo internu reviziju nego i druge delove poslovne banke. Potrebno je da banka ima utvrđene mere koje je potrebno sprovesti u slučaju na primer „pada“ sistema. U tom slučaju, kada je izgrađen sistem preventivnih mera, dolazi do bržeg otklanjanja uzroka koji su doveli do grešaka. Ipak, ukoliko se ona desi, nastupa delovanje korektivnih faktora, na primer, postoji mogućnost uključivanja rezervnog servera što omogućuje nastavak nesmetane komunikacije sa klijentima.

PRINCIPI UPRAVLJANJA RIZIKOM ZA ELEKTRONSKO BANKARSTVO -BAZELSKI KOMITET

Bankarske institucije već godinama pružaju elektronske usluge na daljinu klijentima i privredi. Elektronski transfer sredstava, uključujući mala plaćanja i sisteme upravljanja novcem za privredu, kao i javno pristupačne automatske mašine za podizanje gotovine i upravljanje računima građana, predstavljaju globalni pribor. Međutim, povećano prihvatanje Interneta u svetu, kao kanala isporuke za bankarske proizvode i usluge, pruža nove poslovne mogućnosti za banke kao i uslužne pogodnosti za njihove klijente.

Nezavisno od značajnih koristi tehnoloških inovacija, brzi razvitak e-bankinga nosi rizike kao i koristi i važno je da bankarske organizacije identifikuju i upravljaju ovim rizicima na prudenčijalan način. Ovaj razlog naveo je Bazelski komitet za bankarsku kontrolu⁷⁷ sprovede sprovede preliminarno istaživanje implikacija upravljanja rizikom na e-banking i e-novac. Ova rana studija pokazala je jasno potrebu za još mnogo

⁷⁶ Vunjak N.: Finansijski menadžment, Proleter Bečej, Subotica, 2005, str. 340

⁷⁷ Risk Management for Eletronic Banking and Eletronic Money Activities, mart 1998. godine, dostupno na Bank for Intrenational Settlements, <http://www.bis.org>

rada u oblasti upravljanja rizikom e-bankinga i ta misija je poverena radnoj grupi sastavljenoj od kontrolora banaka i centralnih banaka, *Electronic Banking Group* (EBG).

Izazovi upravljanja rizikom. EBG je zabeležila da osnovne karakteristike e-bankinga (kao i e-trgovine uopšteno) nose jedan broj izazova za upravljanje rizikom:

- Brzina promena u vezi sa tehnološkim inovacijama u uslugama klijentima u e-bankingu je bez presedana. Istorijski, nove bankarske aplikacije bile su primenjivane u relativno dugim periodima i samo posle temeljnih provera. Danas, međutim, banke trpe konkurentske pritiske da spremne nove poslovne aplikacije u vrlo kratkim vremenskim okvirima – često samo nekoliko meseci od koncepta do produkcije. Ova konkurencija intenzivira izazove za menadžment da obezbedi da se adekvatne strateške procene, analize rizika i istraživanja sigurnosti sprovedu pre primena novih aplikacija e-bankinga.

- Transnacionalni e-banking veb-sajtovi i povezane aplikacije u poslovima sa građanima i sa privredom obično su integrisani što je moguće više u postojeće računarske sisteme da bi se postiglo neposredno procesuiranje elektronskih transakcija. Takvi neposredni automatizovani procesi smanjuju prostor za ljudske greške i prevare koje se javljaju kod manuelnih procesa, ali takođe povećavaju zavisnost od zdravog projektovanja i arhitekture sistema.

- E-banking povećava zavisnost banaka od informatičke tehnologije, povećavajući tehničku složenost mnogih operativnih i sigurnosnih pitanja i nastavljajući trend prema većem broju aranžmana partnerstva, alijansi i autorsinga sa trećim stranama, od koje mnoge nisu podvrgnute regulativi. Ovaj razvoj vodi stvaranju novih poslovnih modela koji uključuje banke i nebankarske subjekte, kao što su provajderi Internet usluga, telekomunikacione kompanije i druge tehnološke firme.

- Internet je svuda prisutan i globalan po prirodi. To je otvorena mreža kojoj mogu svuda u svetu pristupiti od nepoznate strane, rutiranjem poruka kroz nepoznate lokacije i putem bežičnih uređaja koji se brzo razvijaju. Otuda, Internet u velikoj meri povećava značaj kontrole sigurnosti, tehnika autentifikovanja klijenata, zaštite podataka, procedura vođenja dnevnika i standarda privatnosti klijenata.

Principi upravljanja rizikom. Bazelski komitet za bankarsku kontrolu naložio je *Electronic Banking Group* (EBG), da identifikuje ključne principe upravljanja rizicima koji bi pomogli bankarskim institucijama da prošire svoju postojeću politiku nadzora rizika i procese, tako da pokriju aktivnosti e-bankinga i takođe, da unapređuju sigurnu i zdravu elektronsku isporuku bankarskih proizvoda i usluga.

Identifikovano je četrnaest principa upravljanja rizikom za elektronsko bankarstvo, koji se dele u tri široke i često preklapajuće kategorije pitanja, koje su radi jasnoće grupisane na sledeći način⁷⁸:

1. Nadzor borda i menadžmenta;
2. Kontrola sigurnosti;
3. Upravljanje pravnim i reputacionim rizicima.

Principi upravljanja rizikom za elektronsko bankarstvo koji su identifikovani, nisu dati kao apsolutni zahtevi niti čak kao „najbolja praksa“, već kao smernice za unapređenje sigurnih i zdravih aktivnosti e-bankinga. Klijent veruje da postavljenje

⁷⁸ Vuković D.: Principi upravljanja rizikom za elektronsko bankarstvo, prevod, Jugoslovenski pregled, Beograd, 2007, str.101

detaljnih zahteva za upravljanjem rizicima u oblasti e-bankinga može da bude kontraproduktivno, makar i zbog toga što bi oni verovarno ubrzano postali zastareli zbog brzine promena u tehnološkim inovacijama i inovacijama proizvoda. Otuda ovi principi izražavaju očekivanja kontrolora u vezi sa opštim ciljem bankarske kontrole, da obezbedi sigurnost i zdravlje finansijskog sistema, a ne strožiju regulativu.

Klijent smatra da ta očekivanja kontrolora treba da budu krojena i adaptirana prema distribucionim kanalima ebankinga, ali tako da ne budu suštinski različita od očekivanja prema bankarskim aktivnostima koja idu drugim distribucionim kanalima. Otuda, principi koji se dalje izlažu uglavnom su izvedeni i adaptirani iz principa kontrole koje su već ranije izrazili klijent ili nacionalni kontrolori tokom proteklih godina. U nekim oblastima, kao što su upravljanje odnosima autsorsinga, kontrola sigurnosti i upravljanje pravnim i reputacionim rizicima, karakteristike i implikacije distribucionih kanala Interneta stvaraju potrebe za detaljnim principima od onih koji su do sada postojali. Klijent uvažava činjenicu da će banke morati da razvijaju procese upravljanja rizicima koji odgovaraju njihovom pojedinačnom profilu rizika, operativnoj strukturi i kulturi korporacionog upravljanja i koji su u skladu sa specifičnim zahtevima upravljanja rizicima i politici koju su postavili bankarski kontrolori u svojoj konkretnoj jurisdikciji.

Klijent ne pokušava da diktira konkretna tehnološka rešenja za tretman određenih rizika ili da postavlja tehničke standarde u vezi sa e-bankingom. Tehničkim pitanjima moraće neprestano da se bave bankarske institucije i različita tela za standarde onako kako se tehnologija razvija. Ova rešenja će se verovatno odnositi i na pitanja u vezi sa činjenicom da se banke razlikuju po veličini, složenosti i kulturi upravljanja rizicima i da se jurisdikcije razlikuju po svojim zakonskim i regulatornim okvirima. Iz ovih razloga, klijent ne veruje da pristup „jedna veličina pristaje svima“ odgovara upravljanju rizicima u e-bankingu i zato podržava razmenu dobre prakse i standarda radi bavljenja dodatnim dimenzijama rizika koje donose kanali isporuke e-bankinga. Očekuje se da principe upravljanja rizicima nacionalni kontrolori koriste kao alate i da ih primenjuju uz adaptacije koje će da odraze specifične nacionalne zahteve gde je to potrebno, da bi pomogli unapređenje sigurne i bezbedne aktivnosti i operacije e-bankinga.

Klijent uvažava da je profil rizika svake banke različit i da zahteva pristup ublažavanju rizika koji odgovara veličini operacija e-bankinga, stvarnim rizicima koji su prisutni i spremnosti i sposobnosti institucije da upravlja tim rizicima.

Ove razlike impliciraju da principi upravljanja rizicima, imaju za cilj da budu dovoljno fleksibilni da bi bili primenjeni kod svih relevantnih institucija u raznim jurisdikcijama. Nacionalni kontrolori će proceniti realnost rizika koji se odnose na aktivnosti e-bankinga prisutnih u datoj banci i da li u kom stepenu su principi upravljanja rizikom za e-banking adekvatno ispunjeni kroz bančin okvir za upravljanje rizicima.

ČETVRTI DEO

REGULATORNI OKVIRI

4. REGULATORNI OKVIRI

4.1. PROPISI EU

Implementacija Bazel standarda II u Evropskoj Uniji ostvarena je donošenjem i primenom Direktiva 2006/48/ES i 2006/49/ES, poznatiji kao CRD – Capital Requirement Directive koje su sve zemlje članice bile dužne da transponuju u nacionalne propise do kraja 2006. godine. Primena Bazel II standarda u EU počela je 1.1.2007. godine, ali je korišćenje naprednih pristupa za izračunavanje kapitalnih zahteva za kreditni i operativni rizik, uz prethodnu saglasnost supervizora, omogućeno od 1.1.2008. godine.

Direktive pružaju mogućnost nacionalnim supervizorima da, putem datih opcija i diskrecionih prava, prilagode primene Bazel II standarda specifičnostima konkretne zemlje i karakteristikama njenog finansijskog tržišta.

Iako je Komitet prevideo primenu Bazel II standarda barem za međunarodno aktivne banke, u Evropskoj uniji su oni, kroz Direktive, postali obavezujući za sve banke. Drugačiji pristup implementaciji Bazel II standarda postoji na primer u SAD, gde je primena ograničenja samo na manji broj velikih međunarodno aktivnih banaka.

CEBS (Committee of European Banking Supervisors) je telo koje ima savetodavnu ulogu u Evropskoj uniji, odnosno pruža savete Evropskoj komisiji u vezi sa pitanjima relevantnim za regulativnu banaka i podstiče saradnju i ujednačavanje prakse nacionalnih supervizora EU, kroz preporuke koje donosi. Prioritet i fokus svog delovanja, CEBS je trenutno usmerio na implementaciju CRD.

Aktuelna dešavanja na međunarodnom finansijskom tržišti i iskustva iz perioda inicijalne primene, uslovljavaju kontinuiran rad, kako BCBS, tako i relevantnih institucija u okviru EU, na unapređenju standarda odnosno propisa iz oblasti supervitije banaka. U skladu sa tim, u toku je razmatranje imena i dopuna CRD.

U prethodnoj deceniji došlo je do velikog zaostatka u pogledu načina funkcionisanja i kontrole rada bankarskog sistema kod nas u odnosu na EU, tako da je početkom 2001. godine domaća praksa bila daleko više zaostala u odnosu na stanje početkom devedesetih, a na žalost zaostala je i u odnosu na druge tranzitorne privrede. Mora se dodati da je od 2001. godine NBS naročito insistirala na zaoštavanju kontrole funkcionisanja bankarskog sistema i praveći rigoroznu kontrolu napravila je selekciju banaka, jer je veliki broj njih izgubio dozvolu po osnovu kontrole.

Donošenjem Zakona o banakama nastavljena je reforma bankarskog sistema, čime se stvaraju uslovi za dalji razvoj i modernizaciju domaćeg bankarstva. Prvenstveni razlozi za donošenje ovog zakona su: harmonizacija legalnog okvira poslovanja banaka sa direktivama Evropske unije, principima Bazelskog komiteta za nadzor nad poslovanjem banaka (tzv. Bazel II), uskladjivanje sa aktuelnim zakonodavnim tendencijama u uporednom pravu, kao i sa odredbama ranije donetih ključnih privrednih zakona – Zakonom o privrednim društvima, Zakonom o registraciji privrednih subjekata i Zakonom o stečajnom postupku.

U pogledu pravnog sistema, međutim, domaći bankarski sistem je uređen po ugledu na EU i naročito pravila Bazelskog sporazuma tj., međunarodno usvojene standarde bankarskog poslovanja. U postupku dobijanja dozvole za rad banke kod nas moraju ispuniti iste ili čak rigoroznije uslove nego u EU. Na primer, kapitalni cenzus u

EU je 5 mil evra, plus 5 mil evra za sopstveni fond, a kod nas je do kraja 2003. godine bio 5 mil evra, dok je od 2004. godine uveden cenzus od 10 mil evra.

Dakle, uslovi za dobijanje dozvole za rad banke (kreditne organizacije) u EU su:

1) početni kapital od 5 mil evra, sem izuzetaka kada je banka od ranije prisutna na tržištu,

2) iznos sopstvenog fonda kredita ne može biti manji od iznosa početnog kapitala tj. 5 mil evra, sem izuzetno za banke formirane pre 1993. godine,

3) lica koja počinju posao moraju biti iskusna i poznata,

4) svaka država članica može posebno zahtevati:

- centrala mora biti u državi koja je izdala dozvolu za rad,

- biznis mora biti razvijen prvenstveno u zemlji koja je izdala dozvolu za rad,

- identitet akcionara koji imaju preko 10% akcija ili preko 25% akcija mora biti poznat centralnoj banci,

- svaka dozvola se mora evidentirati,

- ne može se uslovljavati da filijale ili jedinice van zemlje matice obezbeđuju dozvolu,

- banka mora imati usvojene procedure i unutrašnju kontrolu.

Kada je banka registrovana može obavljati poslove nesmetano u svim zemljama članicama EU. Izuzetno država, odnosno centralna banka može povući dozvolu za rad: u slučaju izbegavanja striktnijih standarda zemlje u kojoj namerava da pretežno posluje, u slučaju postojanja bliskih veza banke sa vlastima zemlje od koje se dozvola traži, u slučaju procene da banka ne može valjano obavljati predviđene poslove.

Domaće zakonodavstvo takodje predviđa određenu proceduru i zadovoljavanje rigoroznih uslova za osnivanje banke. Pri tom upis u Registar privrednih subjekata pretpostavlja dobijanje dozvole za rad od strane NBS, za šta je neophodno ispuniti veći broj uslova od zadovoljavanja cenzusa novčanog dela kapitala do ispunjavanja kadrovskih i tehničkih uslova. Diskreciono pravo NBS da ne dovoli izdavanje dozvole ili dozvolu povuče, takodje je i kod nas prisutno.

Osim saglasnosti odnos harmonizacije zakonodavstva ona podrazumeva harmonizaciju nadzora nad poslovanjem banaka od strane monetarnog autoriteta. Nadzor nad bankama se obavlja:

a) upravnim nadzorom i

b) nadzorom nad savesnošću poslovanja, odnosno revizijom.

Upravni nadzor se vrši u smislu zakonitosti poslovanja banke od trenutka njenog osnivanja do trenutka gubitka dozvole za rad.

Nadzor nad savesnošću poslovanja je novijeg datuma i propisana je odlukama Bazelskog komiteta odakle je preuzet u pravo EU. Glavni instrumenti za nadzor nad savesnošću poslovanja su sopstveni fondovi, značajni udeli, koeficijent solventnosti i veliki krediti.

S tim u vezi prisutni su sledeći standardi međunarodno priznati kod bankarskog poslovanja:

- Banka je dužna da radi stabilnog i sigurnog poslovanja i ispunjenja obaveza prema poveriocima pokazatelj adekvatnosti kapitala, kojim se stavlja u odnos kapital banke prema rizičnoj aktivu, održava na nivou od najmanje 12%,

- mora se obezbediti saglasnost NBS u slučaju sticanja značajnog udela u ukupnom kapitalu banke i to od 5% do 20%, više od 20% do 33% i više od 50% ukupnog

kapitala od strane pojedinačnog akcionara,

- velika izloženost riziku ne sme preći 25%, što znači da se pojedinačni kredit odobren pojedinačnom klijentu ne sme preći 25% kapitala,
- izloženost prema povezanom licu ne sme preći 5% kapitala banke, odnosno ukupna izloženost banke prema povezanim licima ne sme preći 20% kapitala banke,
- zbir svih velikih izloženosti riziku ne sme biti manji od 400% niti veći od 800% kapitala banke,
- banka ne može imati preko 10% učešća u nekom drugom licu van finansijskog sektora,
- ukupna ulaganja u lica van finansijskog sektora i ulaganja u osnovna sredstva ne smeju preći 60% kapitala banke.

Obaveza revizije knjigovodstvenih izveštaja prisutna je i u pravu EU i to jednom godišnje.

Noviji propisi su imali presudan uticaj na razvoj organizacionog dela koji se bavi upravljanjem rizicima u bankama. Supervizorski okvir postavlja ograničenja i smernice koje inspirišu upravljanje rizicima i stimulišu razvoj internih modela upravljanja rizicima unutarbanaka. Međunarodna regulativa pod okriljem Bazelskog komiteta je doprinela promociji preciznije definicije rizika, adekvatnije metodologije za njihovo merenje, koncepta "rizičnog kapitala" ("risk-based capital") i stope adekvatnosti kapitala (kapital neophodan da se pokrijestvarni rizik banaka). U isto vreme, propisi koji postavljaju minimum zahtevanog kapitala su snažan podsticaj za poboljšanje mera rizika i kontrole. Za banke trošak dodatnog rizika postaje trošak dodatnog kapitala⁷⁹.

Problematika regulative leži u razlikama između ciljeva banaka i ciljeva organa koji propisuju regulative (propise). Da bi svet finansija bio što sigurniji i zdraviji na globalnomnivou je poslednjih dvadeset godina potrošeno mnogo vremena kako bi se postavili jedinstveni standardi poslovanja. U tom smislu, svet se okrenuo jačanju korporativnogupravljanja, uvođenju međunarodnih računovodstvenih standarda i standarda izveštavanja, kao i pripremi Novog Bazelskog okvira. U bankama postoje brojne inicijative za preuzimanje rizika. Međutim, preuzimanje rizika kreira »sistemski rizik« - rizik da će ceo bankarski sistem propasti. To je zato što su odnosi, veze i obligacije između banaka veoma tesno povezane. Zato, bankrot jedne institucije generiše rizik propasti svih drugih banaka koje imaju potraživanja prema banci koja je propala. Sistemski rizik je glavni izazov za supervizore. Pojedinačno gledano, banke se mnogo više bave svojim rizikom. Generalno gledano, supervizori se mnogo više brinu o riziku celokupnog sistema. Supervizori su obično suočeni sa nekoliko dilema kada pokušavaju da kontoliraju rizike. Regulativa i konkurencija su često u konfliktu, pošto prevelika regulativa deluje restriktivno na sveukupne operacije banke. Novi zakoni i podzakonska akta mogu generisati nepredvidivo ponašanje banaka sa ciljem da ih izbegnu. Zato regulatori moraju veoma oprezno da prilaze ovom poslu trudeći se da izgrade fer i otvoreno okruženje, bez naglih iotežavajućih promena, koje bi sa svoje strane mogle generisati još veću neizvesnost.

Zahtevi u pogledu visine kapitala su od 1996. godine prošireni i na tržišni rizik. Principi su:

- Tržišni rizik je rizik gubitka u toku minimalnog perioda koji je potreban da se likvidiraju transakcije na tržištu.

⁷⁹ Ivanović dr Perša, (2007.) Upravljanje bankarskim rizicima, skripta za studente BBA

- Minimalni period zavisi od tipa proizvoda.
- Potencijalni gubici zavise od kretanja tržišta u toku ovog perioda i osetljivostirazličitim aktivima.

Polazeći od generalnih principa, regulative procenjuju potencijalne gubitke od tržišnog rizika sa gubicima primenjivim na različite tipove aktiva i tržišnih indeksa. Takođe, moguće je osloniti se na interne modele potencijalnih gubitaka kao zamenu za ovu grupu gubitaka. Interni modeli su bazirani na VAR (vrednost u riziku - maksimalni mogući gubitak portfolija). Da bi banke mogle da koriste spomenutu metodologiju neophodno je da obezbede saglasnost supervizora.

Propisi koji se odnose na tržišni rizik su mnogo kompleksniji nego za kreditni rizik. Tržišni rizik je podložan diverzifikaciji, i ne bi trebalo da se dvaput izračunava kadgod ima kompenzacionih operacija.

Pored toga, osetljivosti i tržišne volatilnosti su primetne i variraju preko instrumenata i tržišta. Banke moraju da formiraju rezervacije za potencijalne gubitke kako bi obuhvatile sve ove efekte. Rizici su podeljeni na dve komponente. Opšti rizik (sistemski) je deo cenovnog rizika koji je generisan tržišnim kretanjima.

Poseban rizik (nesistemski) je drugi deo cenovnog rizika koji se vezuje za emitenta i nezavisan je od tržišnih kretanja. Opšti rizik se ne može diverzifikovati pošto je isti gledajući kroz instrumente. Za razliku od njega, poseban rizik može da bude diverzifikovan.

Kamatni rizik je proizveo mnogo debata i kontroverzi. Tekuća regulativa ne zahteva rezervisanje kapitala za eksplicitno pokrivanje rizika kamatne stope. Ali zahteva da interne mere budu na raspolaganju i uključene u eksterno izveštavanje prema regulatorima. Namera je da se takve informacije učine raspoloživim za nadležne institucije (pre svega centralnu banku), tako da one mogu da preduzmu korektivne aktivnosti ako primete da su one neophodne. Pravila u pogledu zahteva za minimalnim kapitalom su dizajnirana sa ciljem da se zaštite štedište i investitori od rizika bankrota banaka. Ova pravila su tu da obezbede da banke u svako doba poseduju određeni minimum kapitala.

Sa ciljem da se definišu i postavestandardi za odvijanje sigurnih i transparentnih finansijskih aktivnosti Evropska unija jedonela 14. juna 2006. godine dve direktive:

1. Direktiva koja se odnosi na otpočinjanje i bavljenje poslom kreditne institucije. Direktiva 2006/48/EC.

2. Direktiva koja se odnosi na adekvatnost kapitala kreditnih institucija i investicionih firmi. Direktiva 2006/49/EC.

Prva direktiva veoma precizno objašnjava ko sve može da se bavi tzv. bankarskim poslovima i na koji način. Drugim rečima, bankarstvo unutar Evropske unije se karakteriše kao univerzalno bankarstvo. Druga direktiva je naslonjena na prvu direktivu i zajedno sa njom (pored toga što „kapitalizuje finansijske institucije“) predstavlja opšti okvir za primenu Novog Bazelskog okvira u Evropskoj uniji. Stupanjem na snagu pomenutih direktiva Evropska unija je dobila nove standarde za upravljanje rizicima, kao i garanciju da će svi zaposleni u bankama (od upravnog odbora do prodavaca na šalteru i dilera na telefonu) bolje razumeti značaj rizika.

Bazelski komitet za bankarsku kontrolu naložio je *Electronic Banking Group* (EBG), da identifikuje ključne principe upravljanja rizicima koji bi pomogli bankarskim institucijama da prošire svoju postojeću politiku nadzora rizika.

4.2. REGULATORNI OKVIRI REPUBLIKE SRBIJE

Naša zemlja ima vrlo skromna iskustva u primeni Bazel standarda premda se njihovo prisustvo kod nas beleži još od kraja osamdesetih godina. Još tada ovi standardi su imali samo formalni karakter, odnosno nisu bili u aktivnoj upotrebi o čemu može da posvedoči i stanje našeg bankarstva u periodu 1991-1993. Čak ni nakon reforme zakonodavstva o bankama 1993. godine nije došlo do bitnijih promena. Iako su principi Bazela I bili znatno šire uključeni nego što je to bio slučaj na početku, formalna priroda ovih odluka nije se izmenila.

Novi talas usklađivanja našeg sistema kontrole i revizije banaka u skladu sa evropskim, pa i svetskim standardima počeo je 2006. godine, nakon što je u godini koja je prethodila donet novi Zakon o bankama. Od velikog značaja je bilo prepoznavanje operativnog i tržišnih rizika, kao i ustanovljena obaveza formiranja posebnih odeljenja za upravljanje rizikom.

Međutim, ni u ovoj fazi nije ostvaren suštinski pomak u odnosu na dotadašnju praksu, jer su uneti samo neki novi principi Bazel II standarda, ali je izveštavanje prema regulatoru tj. NBS i dalje bilo zasnovano na međunarodnim računovodstvenim standardima. U skladu sa tim banke su nastavile da izrađuju agregirane izveštaje, primera radi podnosi se izveštaj o sumi sredstava investiranih u akcije, pri čemu se ne pravi razlika između hartija sa različitim stepenom rizika.

Od 2008. godine Narodna banka Srbije je pristupila sprovođenju plana za uvođenje Bazel II standarda kod nas. U te svrhe formirana je Radna grupa u čijoj je nadležnosti izvršenje aktivnosti predviđenih donetom Strategijom i Operativnim planom. Planirano je da se do kraja 2009. godine donese sva neophodna regulativa, a da se od januara 2011. krene sa primenom izveštavanja u skladu sa Bazel II standardima.

Onog trenutka kada banke usvoje novi način izveštavanja biće ostvarena korist na dva polja, najmanje. Kao prvo, bankama će se isplatiti sredstva koja su uložile u materijalne i ljudske resurse, jer će konačno imati izveštaje koji ne ispunjavaju samo formu, već su zaista od velike koristi za donošenje odluka o iznosu kapitala koji će se izdvajati. Sa druge strane, regulator će na bazi ovakvog izveštavanja imati u vidu pravu sliku stanja u bankarskom sektoru, te će i sa njegove strane biti postignuta optimizacija kod donošenja odluka. Naravno, ove koristi će biti ostvarene samo uz podršku adekvatnog kadra i tehnologije, na obe strane, kako kod banaka tako i kod NBS kao regulatora. Ohrabruje činjenica da su neke banke već krenule sa izradom sopstvenih modela radi povećanja preciznosti izveštavanja prema svojim maticama, čije je sedište najvećim brojem u zemljama EU.

4.2.1. Bankarski sektor u Srbiji – razvoj i aktuelno stanje⁸⁰

Osnovni cilj Narodne banke Srbije, pored održavanja stabilnosti cena, je održavanje finansijske stabilnosti. Jedan od instrumenata NBS za ostvarivanje ovog cilja je obavljanje funkcije supervizora nad najvećim delom finansijskog sistema Srbije, uključujući i banke.

Bankarski sektor, koji ima dominantan položaj na rastućem finansijskom tržištu Srbije⁸¹, krajem 2007. godine činilo je 35 banaka, što je za 5 manje nego krajem 2005. godine. Trend smanjenja broja banaka rezultat je dalje konsolidacije bankarskog sektora. U prethodnom periodu priveden je kraju i postupak privatizacije najvećih banaka u većinskom vlasništvu države, što je uz ulazak novih reputabilnih finansijskih institucija iz Evropske Unije, izvršena spajanja i pripajanja, izmenilo vlasničku strukturu bankarskog sektora.

Imajući u vidu da na duži rok profitabilnost i održivost poslovanja banaka zavisi od efikasnosti i efektivnosti procesa upravljanja rizicima i kapitalom, interes banaka je da na adekvatan način upravljaju rizicima inherentnim bankarskom poslovanju. S druge strane, zbog izuzetnog značaja bankarskog sektora, specifičnosti delatnosti banaka u smislu njihovog uticaja na celokupnu ekonomsku aktivnost zemlje, kao i radi zaštite interesa deponenata i drugih korisnika finansijskih usluga, NBS ima ne samo interes, već i odgovornost da procenjuje adekvatnost upravljanja rizicima i kapitalom od strane banaka.

U skladu sa tim, NBS kontinuirano usavršava regulativu iz oblasti supervizije banaka⁸² i edukuje i stvara kompetentan kadar koji će biti sposoban da odgovori izazovima koji predstoje, prateći pri tom dostignuća i iskustva država članica Evropske Unije, kao i država iz regiona.

4.2.2. Svrha i ciljevi uvođenja standarda Bazelskog komiteta za bankarsku superviziju⁸³

U cilju daljeg jačanja stabilnosti finansijskog sistema, unapređenja funkcije supervizije u skladu sa razvojem i rastom aktivnosti banaka, kao i harmonizacije sa propisima Evropske unije, Narodna banka Srbije, kao supervizor banaka, će usvojiti i omogućiti primenu standarda Bazelskog komiteta za bankarsku superviziju – Bazel II.

Bazelski komitet za bankarsku superviziju, osnovan 1975. godine, čine supervizori banaka iz 13 zemalja. Imajući u vidu značaj poslovanja i supervizije banaka u kontekstu očuvanja stabilnosti finansijskog sistema i posredno čitave ekonomije, kako na

⁸⁰ www.nbs.rs

⁸¹ Ukupna bilansna suma finansijskog sistema Srbije, nakon značajnih reformi u bankarskom sektoru u periodu od 2001. do 2007. godine, kontinuirano raste i na kraju 2007. godine iznosila je 1.563 milijarde dinara (u 2004. godini ista je iznosila 564 milijarde dinara), pri čemu i bilansna suma banaka ostvaruje odgovarajući rast, tako da je njeno učešće u ukupnoj bilansnoj sumi finansijskog sistema iz godine u godinu stabilno i na visokom nivou od približno 90%.

⁸² Donet je novi Zakon o bankama „Službeni Glasnik RS“ br. 107/2005 a u skladu sa njim i prateća podzakonska regulativa iz oblasti supervizije banaka

⁸³ www.nbs.rs

nacionalnom, tako i na međunarodnom nivou, osnovni cilj Komiteta je unapređenje kvaliteta supervizije banaka u svetu. U svrhu ostvarivanja ovog cilja, Komitet razvija i unapređuje preporuke i standarde supervizije.

Nakon velikih finansijskih kriza tokom osamdesetih godina, uz težnju da relevantna regulativa i uslovi poslovanja banaka na globalnom bankarskom tržištu budu izjednačeni, 1988. godine Komitet je formulisao Bazel I standarde. Osnovna novina Bazela I bilo je uvođenje pojma adekvatnosti kapitala kao funkcije kreditnim rizikom ponderisane aktive banaka.

Iako je Bazel I predstavljao značajan pomak u upravljanju rizicima i superviziji banaka, vremenom su njegovi nedostaci došli do izražaja: baziran je na knjigovodstvenim, a ne na tržišnim vrednostima; akcenat je na kreditnom riziku, dok su tržišni rizici i operativni rizik izostavljeni iz analize; u oceni kreditnog rizika nema razlike između dužnika različitog kvaliteta i rejtinga i, konačno, Bazel I nije adekvatno sagledavao rizičnost i efekte upotrebe modernih finansijskih instrumenata.

Neki od nedostataka Bazela I, posebno oni koji se tiču tržišnog rizika, otklonjeni su kroz izmene i dopune preporuka 1993. i 1996. godine i to kroz uvođenje novog instrumenta za ocenu tržišnog rizika banke – VaR (*Value at Risk*). Međutim, neotklonjeni nedostaci i dalji razvoj delatnosti banaka uslovili su višegodišnji rad Komiteta i nastanak novih preporuka i standarda 2004. godine (*International Convergence of Capital Measurement and Capital Standards*), poznatih pod nazivom Bazel II.

Osnovne ideje Bazela I uglavnom su inkorporirane u aktuelne domaće propise i praksu iz oblasti supervizije⁸⁴ a doneti novi propisi, koji su stupili na snagu 1. jula 2008. godine⁸⁵, predstavljaju i značajan korak ka primeni Bazel II standarda.

⁸⁴ Odluka o adekvatnosti kapitala banke „Službeni glasnik RS“ br. 57/2006, 116/2006, 56/2007; Odluka o upravljanju rizicima „Službeni glasnik RS“ br. 57/2006, 86/2007; Odluka o klasifikaciji bilansne aktive i vanbilansnih stavki banke „Službeni glasnik RS“ br. 57/2006, 116/2006.

⁸⁵ Odluka o adekvatnosti kapitala banke „Službeni glasnik RS“ br. 129/2007; Odluka o upravljanju rizicima banke „Službeni glasnik RS“ br. 129/2007; Odluka o klasifikaciji bilansne aktive i vanbilansnih stavki banke „Službeni glasnik RS“ br. 129/2007; Odluka o upravljanju rizikom likvidnosti banke „Službeni glasnik RS“ br. 129/2007.

4.3. ISO STANDARDI

U savremenom načinu poslovanja postizanje visokog stepena kvaliteta sve više dobija na značaju zbog sve veće konkurentnosti na globalnom svetskom tržištu. Kvalitet proizvoda i usluga danas predstavlja dominantan faktor konkurentnosti i prestiža na svetskom tržištu. Da bi se postigao kvalitet u bilo kom segmentu tržišta kako svetskog tako i domaćeg neophodna je primena savremenog koncepta poslovanja koji uključuje standardizaciju poslovnih procesa i uspostavljanje Sistema menadžmenta kvalitetom. Sistem menadžmenta kvaliteta obuhvata sve poslovne funkcije i ima za cilj stalno poboljšanje svih procesa koji utiču na kvalitet proizvoda i usluga.

Sistem menadžmenta kvalitetom ujedno predstavlja i ulaznicu na tržište koje traži međunarodno priznat dokaz kvaliteta u vidu sertifikata iz serije ISO 9000 standarda. Sistem menadžmenta kvaliteta uspostavlja se uvođenjem standarda ISO 9000 serije odnosno standarda ISO 9001 i 9004 kao opšte prihvaćenog opredeljenja za kvalitet u svim oblastima poslovanja. Standardi iz serije ISO 9000 mogu da se primene na sve vrste organizacija (proizvodne, uslužne, neprofitne idr.) i na sve veličine organizacija (velika, srednja, mala). Standardi sadrže spisak delatnosti na koje se mogu primeniti a to su: ugostiteljske usluge, komunikacije, zdravstvene usluge, trgovina, finansije, administracija itd.

ISO 9000 standardi su međunarodno priznati i širom sveta poznati standardi o upravljanju i obezbeđenju kvaliteta poslovanja. Odmah nakon donošenja, 1987 godine postali su svetski model savremenih sistema kvaliteta. Do sada ih je usvojilo ili sa njima usaglasilo svoje nacionalne standarde 90 zemalja širom sveta: ISO 9000 - ISO 9004 predstavljaju međunarodnu osnovu za razvoj koncepcije «borbe za kvalitet».

Bivša SFRJ Jugoslavija je veoma brzo nakon usvajanja u ISO-u, izradila odgovarajuće analogne standarde sa oznakom JUS ISO⁸⁶. Danas se primenjuju **svi** standardi ove serije i ne zaostaje se za najrazvijenijim zemljama sveta u tome. S obzirom na to da se sve veći broj organizacija iz oblasti finansijskih usluga odlučuje da uvede sistem kvaliteta prema standardima serije ISO 9000, predstavnici tri nacionalne certifikacione organizacije Nemačke, Austrije i Švajcarske (DQS, OQS i SQS) u saradnji sa finansijskim stručnjacima, izradili su smernice sa ciljem da pomognu u tumačenju i praktičnoj primeni zahteva standarda ISO 9000 u oblasti finansijskih usluga.

Pod finansijskim uslugama u smislu ovih smernica podrazumevaju se: bankarstvo, osiguranje, poštanski poslovi i druge srodne usluge. Srpski⁸⁷ standardi za bankarstvo i finansijske delatnosti se donose na osnovu Zakona o standardizaciji⁸⁸. Domaći standardi uglavnom čine prevode međunarodnih ISO standarda. Pored tih standarda izrađuju se i "čisto" domaći standardi. Kod izrade ovih standarda ne prevode se međunarodni standardi, već se u skladu sa određenim pravilima izrađuju sopstveni tekstovi. Standardi izrađeni na ovaj način upotrebljavaju se samo na području naše zemlje. Njih izrađuje Komisija koju je formirao Instituta za standardizaciju Srbije.

⁸⁶ SRPS ISO - Izrađuju se u Institutu za standardizaciju Srbije

⁸⁷ U oblasti standardizacije i dalje se koristi izraz "srpski" koji označava da se radi o domaćim standardima i Ustavima koje se bave standardizacijom.

⁸⁸ Prvi Zakon o standardizaciji donet je 2008.godine, a kasnije su doneti podzakonski propisi

Zahtevi savremenog tržišta su za stabilnom, pouzdanom, efikasnom i racionalnom bankom i u tom pravcu banke treba da postave organizaciju koja je tržišno orijentisana, efikasna i fleksibilna, da neposredno i adekvatno reaguje na promene i zadovoljenje zahteva tržišta. Banke treba da stalno podstiču aktivnosti istraživanja tržišta i razvoja, kako bi unapredile svoju poziciju i ugled na tržištu, da projektuju nove vrste usluga prema potrebama i zahtevima korisnika. Uspešne će biti samo one banke u kojima svi zaposleni na svim nivoima razumeju i realizuju "orijentaciju ka kvalitetu", prihvataju i sprovode zahteve standarda ISO 9000⁸⁹ i teže ka uspostavljanju i održavanju procesa totalnog menadžmenta kvaliteta (TQM)⁹⁰. Da bi ostvarile svoje ciljeve banke treba da obezbede odgovarajući sistem kvaliteta, u skladu sa zahtevima serije standarda ISO 9000 za banakrske usluge i posebno ISO 15.000 za poslove sa HOV.

Osnovni elementi sistema kvaliteta su: ispunjenje zahteva korisnika usluga, neophodnost planiranja svih procesa od značaja za kvalitet, neophodnost permanentnog unapređenja kvaliteta usluga, obaveznost kontrolisanja i proveravanja usluga, kao i smanjenje troškova poslovanja. U ispunjenju ovih elemenata bitnu ulogu imaju standardi, jer u standardima se nalaze zahtevi za usluge, poznavanjem standarda se može delovati na isporučioc, standardizuju se dokumentacija i postupci komuniciranja, putem standarda se najbolje vrši obuka u vezi sa savremenim sredstvima i metodama.

Standardizacija obezbeđuje nove usluge koje nude veće koristi i za pružaoca usluge i za korisnika. Standardizacija u bankama prema sistemu kvaliteta ISO 9000 i ISO 15000 ima tri osnovne uloge:

- da obezbedi specifikacije za proizvode/ usluge;
- da obezbedi ispitivanja koja predstavljaju osnovu za kontrolu kvaliteta;
- da obezbedi informacije o tehnici upravljanja i elementima sistema kvaliteta, odnosno kriterijume po kojima treba ocenjivati upravljanje kvalitetom u banci.

Standardi serije ISO 9000 govore kako se može uspostaviti, dokumentovati i održavati efikasan sistem kvaliteta koji će dokazati kupcima da je banka sposobna da zadovolji njihove potrebe za kvalitetom. Upotreba standarda omogućava da se sačini tačan pregled svih pojedinačnih usluga banke, da se utiče na kvalitet usluga i da se utvrdi odgovornost za otklanjanje svake greške.

Prema Zakonu o standardizaciji⁹¹, standardizacija u Republici Srbiji zasniva se na sledećim načelima:

- 1) pravu na dobrovoljno učešće svih zainteresovanih strana prilikom donošenja srpskih standarda;
- 2) koncenzus zainteresovanih strana;
- 3) sprečavanju prevladavanja pojedinačnih interesa nad zajedničkim interesom zajedničkih strana;
- 4) preglednosti postupaka standardizacije i dostupnosti javnosti srpskih standarda i srodnih dokumenata;
- 5) međusobnoj usklađenosti srpskih standarda i srodnih dokumenata;
- 6) uzimanju u obzir stanja razvijenosti tehnike i pravila međunarodnih i evropskih organizacija za standardizaciju i odgovarajućih međunarodnih sporazuma;

⁸⁹ ISO - The International Organization for Standardization, je svetska federacija sastavljena od nacionalnih tela (ISO članica).

⁹⁰ Ralph L. Meisner, H.: Total Quality Management, WEKA Fachverlag, 1995.

⁹¹ Službeni glasnik Republike Srbije br. 36/09, od 15.05.2009. godine, str. 169

7) jednakom tretmanu inostranih proizvoda ili usluga i istih ili sličnih domaćih proizvoda ili usluga, u skladu sa potvrđenim međunarodnim sporazumima čiji je potpisnik Republika Srbija.

Srpski standardi donose se i objavljuju u skladu sa Zakonom o standardizaciji i pravilima Instituta koja su usklađena sa pravilima međunarodnih i evropskih organizacija za standardizaciju. Kao osnov za donošenje srpskih standarda koriste se po pravilu međunarodni standardi i srodni dokumenti. Srpski standard, odnosno srodni dokument, označava se oznakom koja počinje skraćenicom SRPS. Srpski standardi donose se i objavljuju na srpskom jeziku i pismu. Primena srpskih standarda i srodnih dokumenata je dobrovoljna.

Dokumentovan sistem kvaliteta mora da uzima u obzir obavezne standarde i druge propise, da se bazira na uputstvima koja su propisana za vršenje finansijskih i bankarskih poslova i na drugim standardima koji su prihvaćeni na širem planu, a u vezi su sa obavljanjem bankarskih poslova. To je, sa jedne strane neophodno, kada se radi o obaveznim dokumentima, sa druge strane racionalno, jer ne treba izmišljati ono što je provereno u praksi i, najzad, to je garancija da će se bolje postići saradnja i razumevanje sa klijentima, kao i sa drugim finansijskim institucijama u zemlji i svetu. Međunarodni i evropski standardi ne pokrivaju sve oblasti bankarskog poslovanja naše zemlje. U oblastima koje nisu pokrivene odgovarajućim međunarodnim standardima izraženi su jugoslovenski standardi koji nose oznaku SRPS ISO⁹². Oni su potrebni zbog tipizacije i unifikacije činioca bankarskog poslovanja, racionalizacije i modernizacije bankarskog poslovanja uvođenjem novih tehnologija.

Usvajanjem specijalizovanog ISO 9004-2⁹³ za usluge stvaraju se uslovi za pojašnjenja i olakšava se rad na razvoju sistema kvaliteta i u uslužnim delatnostima. Ovaj standard prikazuje i spisak uslužnih delatnosti na koje se on može primeniti: ugostiteljske usluge, komunikacije, zdravstvene usluge, trgovina, finansije, administracija itd. U međunarodnom standardu se proces pružanja usluga deli na četiri stepena:

1. Izrada koncepta pružanja usluga: Ovaj proces obuhvata istraživanje tržišta, prikazivanje potreba kupaca, *feedback* od strane kupaca, interne popise zaliha, pravne i komercijalne obaveze kao i druge, za koncept korisne informacije.

2. Dizajn pružanja usluge: Ako je koncept pružanja usluga (koji definiše šta kupac hoće) jednom napravljen, onda se koncept u sledećem koraku realizuje u specifikacijama za kreiranje pružanja usluga i oblik njegove pripreme. Dizajn pružanja usluga uključuje raspodelu odgovornosti za pojedinačne stepene procesa pružanja usluga i razvoj postupaka za obezbeđenje kvaliteta, koji se zasnivaju na minimalnim standardima za svaku pojedinačnu karakteristiku pružanja usluge.

3. Vršanje usluge: Kod vršenja usluge treba obratiti pažnju na specifikaciju, pri čemu bi trebalo nadgledati ispunjenje specifikacije, kao i odstupanja. To zahteva

⁹² SRPS ISO standardi su srpski standardi koje su izradile Komisije Instituta za standardizaciju.

Komisija nosi oznaku KSI 068 – Bankarstvo i srodne finansijske delatnosti. Područje rada je identično sa područjima ISO TC 68 i ISO/IEC JTC 1/SC 17. Zadaci Komisije u okviru svog područja rada da planira izradu standarda, izrađuje prednacrt u okviru radnih grupa, nacrt i definitivne tekstove standarda – predloge Instituta za standardizaciju koji donosi propise o srpskim standardima.

⁹³ ISO 9004-2 je serija standarda koja je pripremljena tako da se odnosi i na uslužne delatnosti i definiše specifičnosti upravljanja i elemente sistema obezbeđenja kvaliteta usluga što olakšava primenu čitave serije u ovoj oblasti.

kontinuelni nadzor preko internih instanci i kupaca, kao i uređenje efikasnog sistema za korektivne mere, da bi se obezbedilo isključenje neprikladnih postupaka iz sistema.

4. Analiza i poboljšanje pružanja usluge: Sistem za korektivne mere indicira moguće probleme, koji ne mogu odmah da se reše. One mogu da učine potrebnim temeljnije provere procesa. Centralni sastavni deo svakog sistema kvaliteta je strategija ka kontinualnom poboljšanju. Trebalo bi težiti ka tome da se indetifikuju i pronađu centralne karakteristike usluge, koje mogu da se poboljšaju.

Osam kategorija, prikazanih u ISO 9004, su:

- Utvrdjivanje potreba i ocekivanja kupca u odnosu na ponudenu uslugu;
- Istraživanje dopunskih usluga i njihovog mogućeg uticaja na karakter i kvalitet ponudene usluge;
- Istraživanje mogućeg uticaja aktivnosti konkurencije na uslugu;
- Zakonske regulative kao relevantni nacionalni i međunarodni standardi i smernice;
- Uzimanje u obzir zahteva klijenata interno sakupljenih podataka o usluzi;
- Informacija iz pojedinačnih odnosnih funkcionalnih područja uslužne organizacije, da bi se obezbedila njihova odlučnost za ispunjenje zahteva kvaliteta usluge. Važno je, uveriti se u operativne kapacitete funkcionalnih područja;
- Istraživanja o promenljivim zahtevima tržišta, novim tehnologijama i dejstvu konkurencije;
- Pouke, izvučene iz sistema za obezbeđenje kvaliteta i rezultata kontrola kvaliteta.

Ovih osam izvora informacija se analizira i u koncentrisanom obliku ulazi u koncept usluge. On se sastoji iz sledećih elemenata:

1. Utvrđivanje potreba kupaca. Osnovu predstavljaju informacije, koje su dobijene istraživanjem tržišta, internom analizom potreba kupaca i istraživanjem potreba, koje se menjaju.

2. Procena dometa sopstvene organizacije i prilagođenje sopstvenog načina rada. Oni se zasnivaju na informaciji, koja je dobijena od samih vršilaca usluge i iz rezultata obezbeđenja kvaliteta.

3. Utvrđivanje instrukcija za operativni sistem. Ona se dobija, kao prvo, oba gore navedena elementa, a kao drugo iz saznanja, koja su dobijena iz posmatranja aktivnosti sličnih ili konkurentskih firmi, a kao treće iz zakonskih obaveza.

Moderni sistemi obezbeđenja kvaliteta se uobičajeno zasnivaju na seriji ISO 9000⁹⁴, koja se sastoji od pet glavnih elemenata ISO 9000 do ISO 9004, kao i od niza dopunskih. Ako banka na pažljiv način stvara radne sisteme, beleži rezultate i razvija poboljšanja, ona može sprovesti postojeće i stalno poboljšavane. Ključ za to je u pisanim procedurama.

Uvođenje sistema kvaliteta u banku je veoma složen i zahtevan projekat, zahteva širok vidik, odličan menadžment projekta, visokokvalifikovane saradnike i dobro osmišljen proces komunikacije. Na prvom mestu važan je top menadžment banke – ako glavni menadžer banke ne podstiče program kvaliteta i ne podržava ga ima malo izgleda na uspeh.

Merenje kvaliteta usluga se vrši kroz proces:

- 1) definišu se usluge koje se pružaju klijentima banke,

⁹⁴ Standardi serije ISO 9000 namenjeni su proizvodnji i uslugama.

2) razvija se merenje učinaka za svaki pojedinačni elemenat usluge prema tačnosti, savesnosti i predusretljivosti,

3) utvrđuje se mereni nivo usluge,

4) razvija se obiman merni sistem,

5) metodologija obezbeđenja kvaliteta definiše mogućnost poboljšanja.

Za sve usluge koje banka vrši se utvrđuju stanadardi učinka i ciljevi, pri čemu se uzimaju u obzir sledeći faktori: očekivanje kupca, konkurencija, zakonski okviri i uslovi, ekonomičnost i kapacitet obrade.

Kvalitet u bankarskom poslovanju može da se posmatra preko modifikovanja početaka definicije pojma kvaliteta specifičnog za banku koji uključuje:

a) operativni i tehnički kvalitet:

- vreme obrade,

- prosečno vreme realizacije,

- učešće grešaka,

- vreme raspoloživosti tehničkog osoblja,

b) Strateški kvalitet:

- stepen zadovoljstva kupca,

- odnos poverenja banaka – kupac,

- stepen motivacije saradnika,

- sposobnost za inovacije i

- strateška osetljivost.

Uobičajeno je postojanje univerzalne bankarske institucije. Početni korak u pripremi za izradu projekta uvođenja sistema kvaliteta se sastoji u sagledavanju poslova koje banka obavlja. Realizacija Projekta uvođenja sistema kvaliteta u banku uključuje sledeće faze:

1) Utvrđivanje zadatog koncepta – rukovodstvo banke mora da utvrdi i dokumentuje svoju načelnu obavezu za kvalitet;

2) Analiza stvarnog stanja – interni audit – podrazumeva naročito snimanje i analizu postojeće organizacije rada i toka aktivnosti i prenosa informacija u banci;

3) Analiza slabih mesta – analiza slabih mesta je od ključnog značaja zato što otklanjanjem slabih mesta se najpre može uticati na poboljšanje sistema kvaliteta;

4) Strukturiranje projekta – podrazumeva pripremu, planiranje realizaciju projekta sa nosiocima pojedinih funkcija u realizaciji i opredeljivanje načina pristupa i vremena za njihovo izvršenje;

5) Kontinuirano poboljšanje sistema kvaliteta – obezbeđenje ove funkcije znači uvođenje u praksu banke organizacije koja uči putem uvođenja mehanizama koji analiziraju pružanje usluga i ukazuju na slabosti i način otklanjanja grešaka i slabosti;

6) Priprema za sertifikaciju – priprema podrazumeva privođenje izradi celokupne dokumentacije i obuku ljudi i

7) Sertifikacija – na osnovu analize dokumenata i stvarnog stanja obezbeđuje se sertifikat od strane ovlašćene institucije.

ZAKLJUČNA RAZMATRANJA

ZAKLJUČNA RAZMATRANJA

Najvažniji razlog zbog kog se upravljanju rizicima u bankarstvu, poklanja izuzetno velika pažnja jeste priznanje ekonomskog i društvenog doprinosa bankarstva u razvoju društva. Kroz poslovanje banke se manifestuju ne samo interesi njenih neposrednih vlasnika, već i interesi nacionalne ekonomije. Javni karakter banke podrazumeva njen doprinos stabilnosti nacionalnog finansijskog sistema.

Savremene banke se shvataju kao multifunkcionalni, multiorganizovani i multiadaptivni sistemi, koji mogu da usmeravaju privredna i investiciona kretanja. Putem kreditiranja novih poslova, investicija, inovacija i stvaranju mogućnosti zapošljavanja, zdravo bankarstvo doprinosi ekonomskom rastu.

Poseban značaj bankarstvo ima u zemljama u tranziciji, kao što je i naša, jer od njihovog kreditnog potencijala zavisi dinamika i kvalitet privrednih i društvenih reformi.

1. Regulisanje kapitala je započeto 1988. godine sa formalnim sporazumom poznatijim kao Bazel I, koji je bio prevashodno usmeren ka najvećim međunarodnim bankama. Ovaj set međunarodnih pravila zahtevao je od mnogih najvećih komercijalnih banaka da odvoje svoje knjigovodstvene i vanknjigovodstvene bilanse i da svoje obaveze svrstaju u određene kategorije rizika, kao i da pomnože svoju aktivu pojedinačno sa odgovarajućim stepenom rizika da bi se utvrdio ukupan rizik, kojoj je izložena aktiva. Koeficijent ukupnog zakonskog neisplaćenog kapitala u odnosu na ukupan stepen rizika aktive i obaveza iz vanknjigovodstvenog bilansa, ključni je pokazatelj visine kapitala u jednoj banci, tj. pokazatelj njene snage. Postoje najniži koeficijenti adekvatnog nivoa kapitala koje svaka banka mora da ispuni, odnosno prevaziđe.

Ubrzo su se pokazale slabosti Bazelskog sporazuma I, među kojima je i njegova nesposobnost da reaguje na promene i nova otkrića na finansijskom tržištu. Sve to je dovelo do pisanja nacrtu novog sporazuma poznatog kao Bazel II ili Drugi bazelski sporazum. Ovaj novi pristup u upravljanju kapitalom, zahteva od najvećih bankarskih kompanija da sprovedu kontinuiranu unutrašnju procenu izloženosti riziku, uključujući i kontrolu osetljivosti i da obračunavaju sopstveni nivo potrebnog kapitala. U tom slučaju, svaka banka potpisnik imaće sopstvene jedinstvene procene potreba kapitala baziranih na sopstvenoj jedinstvenoj proceni profila rizika. Manje banke će verovatno koristiti jednostavnije, standardizovane pristupe da bi odredile da je njihov minimalni nivo kapitala identičan, ili u najmanju ruku sličan pravilima iz Prvog bazelskog sporazuma.

Osnovni cilj Bazelskog sporazuma II je povećanje osetljivosti na rizike, tj. visinu potrebnog kapitala dovesti u vezu sa visinom izloženosti riziku. Prema tome, Bazel II bi trebalo da dovede do povećanja nužnog kapitala u slučaju povećane izloženosti rizicima, odnosno do smanjenja pri niskoj izloženosti riziku. Stoga, njegova namera nije da se generalno smanji nivo potrebnog kapitala za kreditni rizik, već da se taj nivo dovede u vezu s rizicima.

2. Pojavom globalizacije tržišta poslovanje jedne banke postaje sve rizičnije. Prateći deo poslovanja jedne banke su rizici. Rizik se može svesti na najmanju moguću meru adekvatnim upravljanjem rizika i pažljivim analiziranjem svih kredita pre nego što se odobre, a potom i savesnim vođenjem kredita sve dok ne bude otplaćen.

Nekoliko je objektivnih razloga koji ovu temu čine posebno aktuelnom, poželjnom i naučno interesantnom:

- *prvo*, razumevanje značaja upravljanjem rizicima i njihovim analiziranjem, dolazi se do mogućnosti svođenja rizika na najmanju moguću meru. Samim tim banke ostvaruju manje gubitke u poslovanju a veće kreditne potencijale za kreditiranje privrede i stanovništva, što je od izuzetne važosti za ekonomski razvoj i prosperitet jednog društva;
- *drugo*, uočavanje rizika, slabosti, negativnih kretanja i propusta po planu transformacije bankarskog sektora omogućice da se blagovremeno zaustave nepovoljne tendencije i onemogućići dovođenje u pitanje strategije razvoja zdravog bankarskog sistema;
- *treće*, operativni rizik je izraz opasnosti od direktnih ili indirektnih gubitaka koji su rezultat neadekvatnih internih procesa, ljudi i sistema ili zbog spoljašnjih događaja;
- *četvrti*, prema operativnom riziku u bankarstvu mora se imati kritički odnos, zbog izuzetne važnosti kojim ga definiše Basel II.

3. Rizik upravljanja je operativni rizik broj jedan, mišljenje je vodećih bankarskih stručnjaka u svetu danas i u bliskoj vezi sa još dva vodeća slučaja operativnih rizika – rizikom događaja (uključujući interne i eksterne prevare) i rizik tehnologije (stabilnost sistema, analize/programiranje)

Značajni finansijski gubici, i do određenog nivoa reputacioni gubici, vrlo dugo nisu bili viđeni i tretirani kao gubici zbog operativnih propusta. Uzrokovani propustima u razumevanju ili kontroli izloženosti u odnosu na tržište ili klijente, oni su se realizovali i bili dokumentovani kao tržišni ili kreditni rizici, a u osnovi ovih gubitaka i rizika, bili su operativni rizici. Ceo proces, međutim, pospešili su konkurencija, razvoj finansijskog inženjeringa i tehnike za ublažavanje izloženosti drugim rizicima (kreditni, tržišni) koje su istovremeno ukazivale na značaj rastućih operativnih rizika. Sve ozbiljnije suočavanje sa operativnim rizikom, bila je realnost koja je podsticalo delovala na razvoj discipline upravljanja ovim rizikom u bankama, u smislu da se ona našla u samom fokusu svetske bankarske industrije i postala predmet kontinuiranog testiranja i usavršavanja. Mnoge tehnike koje se koriste za upravljanje kreditnim i tržišnim rizicima, vrlo brzo su ocenjene kao prihvatljive i za operativne rizike.

4. Proces je brzo evoluirao u praksi od momenta kada je Bazelski komitet za bankarsku superviziju odlučio da u novi okvir Međunarodne saglasnosti za merenje kapitala i kapitalne standarde (Bazelski sporazum II) , pored kreditnog i tržišnog rizika, uključi i operativne rizike u osnovicu za kalkulaciju ekonomskog kapitala, a za potrebe utvrđivanja nivoa kapitalne adekvatnosti banaka.

Ovim značajnim dokumentom, koji već ima dimenziju međunarodnih standarda u oblasti merenja kapitalne adekvatnosti banaka i preventivne supervizije njihovog poslovanja, rešio je neke suštinske dileme vezano za operativni rizik i ponudio ih stručnoj javnosti , kao standardizovana rešenja-od definicije pojma operativnog rizika, osnovne strukture okvira za upravljanje operativnim rizikom, do kvalitativnih standarda za faze u procesu upravljanja, odnosno kvalitativne standarde za najvišu fazu ovog procesa-merenje izloženosti operativnom riziku i kalkulaciju optimalnog ekonomskog kapitala.

Banke u Srbiji nesporno se nalaze pred strateški važnim zadatkom da razvijaju efikasne okvire za upravljanje operativnim rizikom. Faktor koji može otežati put ka ovome cilju je činjenica da je reč o riziku, koji je slabo poznat domaćoj bankarskoj industriji, što podrazumeva neophodno vreme za edukaciju zaposlenih u smislu svesti o postojanju ovog rizika , kao i potrebne edukacije na planu podizanja kultura ponašanja na svim nivoima u banci u odnosu na izloženost operativnom riziku. U tom kontekstu, pristup koji je odredio nacionalni regulator dobro je osmišljen , jer obezbeđuje potrebno vreme, a ono je neophodan element uspešnog ishoda procesa.

Potrebno vreme, faktor je koji se ne može zaobići i kada je u pitanju priprema Upravnog i Izvršnog odbora , za njihovo puno uključenje u procese kreiranja strategija, politika i procesa upravljanja operativnim rizikom , u smislu podizanja nivoa svesti o postojanju ovog rizika kao posebne kategorije, kojom se mora pažljivo upravljati i to na svim nivoima u banci. Ovaj momenat bitan je za odobravanje i nadzor jednog efikasnog okvira za upravljanje operativnim rizikom od strane Upravnog odbora i odgovornost za njegovu konzistentnu i efikasnu primenu od strane Izvršnog odbora, a što su i zahtevi standarda iz Bazelskog sporazuma II.

L I T E R A T U R A

LITERATURA

1. Avery R. and Milton P. Insures to the rescue? Operational Risk, Special Edition of Risk Professional, (2000)
2. Aleksić V.: "Banka i moć", Stubovi kulture, Beograd, 2002.
3. А.Д.Урсул, Т.Н. Цырдя, Информационная безопасность, сущность, содержание и принципы ее обеспечения, журнал Факт № 2, 2000
4. Barać S., Stakić B., Hadžić M., Ivaniš M.: "Praktikum za bankarstvo", Fakultet za finansijski menadžment i bankarstvo, Beograd, 2005.
5. Barać S.: "Restruktuiranje bankarskog sektora u svetu i kod nas ", časopis "Finansije, Bankarstvo, Revizija i Osiguranje" br. 4/2004, Fakultet za finansijski menadžment i osiguranje, Beograd.
6. Barać S., Stakić B., Hadžić M., Ivaniš M.: "Organizacija bankarstva", Fakultet za finansijski menadžment i bankarstvo, Beograd, 2005.
7. Barać S., Stakić B.: " Osnovi ekonomije ", Fakultet za finansijski menadžment i osiguranje, Beograd, 2006.
8. Barać S., Stakić B., Ivaniš M.: " Praktikum za finansije i bankarstvo ", Fakultet za finansijski menadžment i osiguranje, Beograd, 2003.
9. Barać S., Stakić B., Hadžić M., Ivaniš M.: " Poslovno bankarstvo ", Fakultet za finansijski menadžment i osiguranje, Beograd, 2005.
10. Barać S., Stakić B.: " Praktikum za osnove ekonomije ", Fakultet za finansijski menadžment i osiguranje, Beograd, 2006.
11. Barać S., Stakić B., Hadžić M., Jeremić Z.: " Pojmovnik finansija i bankarstva ", Fakultet za finansijski menadžment i osiguranje, Beograd, 2006.
12. Basel Committee on Banking Supervision: "An internal model-based approach to market risk capital requirements ", Consultative Proposal, Basel 1995.
13. Basel Committee on Banking Regulation and Supervisory Practices: " International convergence of capital measurement and capital standards ", Basel 1988.
14. Basel Committee on Banking Supervision " Framework for international control systems in banking organizations ", Basel 1998.
15. Basel Committee on Banking Supervision : "Operational risk management" Basel 1998.
16. Basel Committee on Banking Supervision: "A new capital adequacy framework: Consultative Paper", Basel 1999.
17. Basel Committee on Banking Supervision : " Enhancing corporate governance for banking organisations " Basel 1999.
18. Basel Committee on Banking Supervision : " Update on work on a new capital adequacy framework " Basel 1999.
19. Basel Committee on Banking Supervision Risk Management Group : " Other risks preliminary survey " , Basel 2000.
20. Basel Committee on Banking Supervision : " The new basel capital accord ", Basel 2001.
21. Basel Committee on Banking Supervision : " International convergence on capital measurement and capital standards – a revised framework ", June 2004.

22. Bazelski komitet za bankarski nadzor : " Međunarodna saglasnost o obimu kapitala i standardima za kapital – važeći bazelski sporazum - Bazel I ", prevod Udruženje banaka Jugoslavije,1988.
23. Bazelski komitet za bankarski nadzor : " Novi bazelski sporazum o kapitalu : Uvodno objašnjenje ", prevod Udruženje banaka Jugoslavije,2001.
24. Bazelski komitet za bankarski nadzor : " Prikaz novog bazelskog sporazuma o kapitalu ", prevod Udruženje banaka Srbije, 2003.
25. BIS: "Overview of the amendment of the capital accord to incorporate market risks ", Amendment to the Capital Accord to incorporate market risks, January 1996.
26. Bjelica, V.: " Bankarstvo " , Stilos , Novi Sad, 2001.
27. Барсуков Д., Интегральная защита информации, "Электроника. Наука, технология, бизнес" № 3-4,1998г.
28. Cvetinović M.: " Upravljanje rizicima u finansijskom poslovanju " , Univerzitet Singidunum, Beograd, 2008.
29. Cascarino Richard, Information Systems Auditing, John Wiley & Sons Inc., USA, 2007
30. Coghlan R.: " Money, credit and the economy " , George Allen and Unwin, London, 1994.
31. Cow D. : " Succes in elements of banking " , John Murray, London, 1992.
32. Ćirović M.: " Bankarski menadžment ", Ekonomski institut Beograd, Beograd, 1995.
33. Duff and Phelps Credit Rating Co.,: "A new capital adequacy framework Consultative Paper Issued by the Basel Committee on banking Supervision ", June 1999.
34. D. K. Hsiao, D.S. Kerr, S.E. Madnik, Computer security, Academic Press, New York, san Francisko, 1979
35. Đukić Đ., Bjelica V., Ristić Ž,: " Bankarstvo " , Centar za izdavačku delatnost Ekonomskog fakulteta, Beograd, 2004.
36. Đukić Đ.: " Centralna banka i finansijski sistem " , Litopapir, Čačak, 1991.
37. Erić - Jović M.: "Bazelski sporazum II – kreditni rizik: standardni pristup", časopis " Bankarstvo " br. 5-6/2003, Beograd,
38. Greuning van H. and S. Brajovic-Bratanovic: "Analyzing and managing banking risk " , Second Edition, The World Bank, 2003.
39. Horne C. Van James: Financial Management and Policy, Prentice-Hall Inc, New York, 1999
40. Icon Institute Gmbh: " Priručnik o upravljanju kreditnim rizikom " , Beograd, 2004.
41. ISO 27001:2005 ISMS Implementation, BSI Management Systems, 2007.
42. Information Risk Management in Corporate Governance, ISF Workshop, 2003.
43. Ivan Vukadinović: Uspostavljanje sistema za upravljanje informatičkom bezbednošću, Infotech 2006.
44. IRAM Training Presentation Pack, ISF, 2007.
45. Jaffee D. and J. Stiglitz : "Credit rationing in handbook of monetary economics " , Chapter 16, North-Holland 1990,
46. Jović S.: " Bankarstvo " , Naučna knjiga, Beograd, 1990.

47. Labus M.: " Osnovi ekonomije ", Stubovi kulture, Beograd, 1999.
48. Luhmann N.: " Soziolog des risikos " Berlin , New York 1991.
49. Matić V.: " Upravljanje kreditnim rizikom u svetlu odredbi bazelskog sporazuma", časopis "Jugoslovensko bankarstvo" br. 7-8/2002, Beograd,
50. Matić V.: " Bazelski sporazum II ", časopis "Bankarstvo" br.1-2/2007, Beograd,
51. Matić V.: " Srpsko bankarstvo u 2006.godini ", časopis " Bankarstvo " specijalan broj 1/2007, Beograd,
52. Matten C.: " Managing bank capital ", Second Edition, John Wiley and Sons Ltd, Chichester 2000.
53. Mishkin S. Frederic: " Monetarna ekonomija, bankarstvo i finansijska tržišta ", prevod, Data status, Beograd, 2006.
54. Obradović G.: " Evropojmovnik -prevod", Institut za međunarodnu politiku i privredu, Beograd, 2005.
55. Pušara K.: " Bankarstvo i sistemi plaćanja ", Alef, Novi Sad, 1993.
56. П.В. Константинович, От информационных войн к управляемой конфронтации и сотрудничеству, журнал Факт № 9, 2001
57. Radojević T.: " Inteliktualna svojina i intelektualni kapital banke ", časopis "Spoljnotrgovinski savetnik" br.1/2007, Poslovni biro, Beograd,
58. Radovanović R. : " Bilansi preduzeća i banaka ", Bmg, Beograd, 1999.
59. Rajković S.: " Jugoslovenski bankarski standardi ", Bankinfo, 1996.
Rodić B., Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija (*doktorska disertacija*), Vojnotehnička akademija, Beograd, 2001
60. Rose S. Peter, Sylvia C. Hudgine : "Bankarski menadžment i finansijske usluge ", prevod, Data status, Beograd, 2005.
61. Rose S. Peter: Commercial Bank Management, Thind Edition, Irwin, 1995
62. Rose S. Peter: " Commercial bank management " , 5th Edition, McGraw-Hill Irwin, Boston 2002.
63. Risk Management for Eletronic Banking and Eletronic Money Activities, mart 1998. godine,
64. dostupno na Bank for Intrenational Settlements, <http://www.bis.org>
65. Stakić B., Radović R. : " Bankarsko poslovanje ", FST , Bijeljina ,1996.
66. Stakić B.: " Finansijski i devizni menadžment u turizmu ", Fakultet za turistički i hotelijerski menadžment, Beograd, 2005.
67. Stakić B.: " Bazel II ", časopis "Spoljnotrgovinski savetnik" br. 12/2002, Poslovni biro, Beograd,
68. Stakić B.: "Restruktuiranje bankarskog sektora u svetu ", časopis "Spoljnotrgovinski savetnik" br. 10/2004, Poslovni biro, Beograd,
69. Stojiljković V., Uzunović R., Veljković B., Stojiljković Lj., Stojanović N., Grandić D.: " ISO 9000 / ISO 14000 – Put ka TQM / ", CIM College, Mašinski fakultet Niš, 1996.
70. Standardi JUS ISO 9001/2/3, SZS, 1991.
71. Šuvakov T.: " Ekonomija ", Ofsetprint, Novi Sad , 1995.
72. Vasiljević B.: " Rizici u bankarskom poslovanju " Fokus, Beograd,1990.
73. Vuković D.: "Bazel II –značaj za banke ", Udruženje banaka Srbije, Beograd, 2006.

74. Vuković D.: Principi upravljanja rizikom za elektronsko bankarstvo, prevod, Jugoslovenski
75. pregled, Beograd, 2007, str.101
76. Vunjak N.: " Finansijski menadžment - bankarske finansije", Ekonomski fakultet, Subotica, 1999.
77. Vunjak N.: Finansijski menadžment, Proleter Bečej, Subotica, 2005, str. 340
78. Vučković M.: " Bankarstvo " , Naučna knjiga , Beograd, 1960.
79. Todorovic V.: " Uticaj finansijskih rizika na profitabilnost banaka " , Bankarstvo 2003
80. Živković A., Stankić R., Krstić B.,: " Bankarsko poslovanje i platni promet " , Ekonomski fakultet u Beogradu, 2006.

NEAUTORIZOVANI IZVORI

1. Zakon o bankama („Sl. glasnik RS“, br. 107/2005)
2. Odluka o bližim uslovima i načinu vršenja kontrole Narodne banke Srbije nad bankama ("Sl. glasnik RS", br. 51/06)
3. Odluka o sprovođenju odredaba Zakona o bankama koje se odnose na davanje preliminarnog odobrenja za osnivanje banke i dozvole za rad banke, kao i pojedinih odredaba koje se odnose na davanje saglasnosti NBS ("Sl. glasnik RS", br. 51/06)
4. Odluka o upravljanju rizicima ("Sl.glasnik RS", br.57/06)
5. Odluka o adekvatnosti kapitala banke ("Sl.glasnik RS",br.57/06 i 116/06)
6. Odluka o načinu i uslovima identifikacije i praćenja rizika usklađenosti poslovanja banke i upravljanja tim rizikom ("Sl.glasnik RS", br.57/06)
7. Uputstvo o izveštajima banaka ("Sl.glasnik RS", br. 57/06 i 116/06)
8. Usklađenost i funkcija kontrole usklađenosti u bankama – prevod, Bazelski komitet za bankarski nadzor, 2005.

ELEKTRONSKI IZVORI

www.worldbank.org

www.imf.org

www.ifc.org

www.miga.org

www.ecb.int

www.eib.org

www.ebrd.com

www.iadb.org

www.afdb.org

www.adb.org

www.wto.org

www.iso.org

www.iccwbo.org

www.clubdeparis.org

www.bis.org

www.oecd.org

www.nbs.rs

www.ekonomistonline.rs