Na osnovu člana 17 stav 1 tačka 2 Zakona o Centralnoj banci Crne Gore (»Sl. list RCG«, br, 52/00 i 47/01) i člana 64 stav 3 Zakona o bankama (»Sl. list RCG«, br. 52/00 i 32/02), Savjet Centralne banke Crne Gore, na sjednici održanoj 23. i 24. februara 2009. godine, donio je

ODLUKU
o minimalnim standardima za upravljanje operativnim rizikom u bankama

1. Opšta odredba

Predmet regulisanja

Član 1

Ovom odlukom se utvrđuju minimalni standardi za upravljanje operativnim rizikom u bankama.

2. Upravljanje operativnim rizikom

Identifikacija izvora operativnog rizika

Član 2

U postupku identifikacije izvora operativnog rizika, banka je dužna da naročito identifikuje rizike koji proizilaze iz:

1) neadekvatnog informacionog i drugih sistema u banci;
2) poremećaja u poslovanju i kvara sistema (na primjer: kvarovi vezani za informacionu tehnologiju, telekomunikacioni problemi, prekidi u radu i sl.) ;
3) nemogućnosti adekvatnog integrisanja ili održivosti informacionih i drugih sistema, u slučaju statusnih promjena banke;
4) protivpravnog i neadekvatnog postupanja zaposlenih u banci, kao što je pronevjera, pranje novca, neovlašćeni pristup računima klijenata, zloupotreba povjerljivih informacija, davanje lažnih ili pogrešnih informacija o stanju banke, neažurnost u izvršavanju poslova, greške pri unosu podataka, nepridržavanje dobrih poslovnih praksi u radu i sl.;
5) angažovanja lica izvan banke za obavljanje poslova za banku;
6) radnji, odnosno nečinjenja koja mogu uzrokovati sudske i druge sporove protiv banke (pravni rizik);

7) spoljnih protivpravnih radnji, kao što su krađa, neovlašćeni prenos sredstava, neovlašćeno ulaženje u bazu podataka, nezakonito pribavljanje dokumenata banke i sl.;
8) događaja koji se ne mogu predvidjeti, kao što su elementarne i druge nepogode, terorizam i sl.

Mjerenje i kontrolisanje rizika

Član 3

Banka je dužna da nakon identifikacije konkretnog izvora operativnog rizika, primjenom adekvatnih metoda mjerenja, procijeni nivo tog rizika.

Banka je dužna da, u zavisnosti od prirode i nivoa konkretnog operativnog rizika, primijeni odgovarajuće metode za njegovo smanjenje odnosno eliminisanje, ili za njegovo praćenje i kontrolisanje.

Banka koja izračunava potrebni kapital za operativni rizik primjenom standardizovanog metoda dužna je da prati i mjeri operativni rizik po svim poslovnim linijama.

Identifikacija novih izvora rizika

Član 4

Banka je dužna da prije uvođenja novih proizvoda, procesa i sistema ili prije preduzimanja novih poslovnih aktivnosti, identifikuje i procijeni operativni rizik koji je sa njima povezan.

Definisanje ovlašćenja i odgovornosti

Član 5

Banka je dužna da u svojim aktima jasno definiše ovlašćenja i odgovornosti za upravljanje operativnim rizikom.

Banka je dužna da obezbijedi da svi zaposleni budu upoznati sa obavezama u procesu upravljanja operativnim rizikom.

Interno izvještavanje

Član 6

Banka je dužna da u svojim aktima utvrdi obavezu i način internog izvještavanja o funkcionisanju sistema upravljanja operativnim rizikom i njegovog periodičnog preispitivanja.

Operativni rizik koji proizilazi iz informacionog sistema banke

Član 7

Banka je dužna, da u cilju obezbjeđenja adekvatnog upravljanja operativnim rizikom koji proizilazi iz informacionog sistema, kao minimum:

1) usvoji strategiju informacionog sistema koja mora biti u skladu sa poslovnom strategijom banke;
2) usvoji interni akt koji će biti okvir za upravljanje bezbjednošću informacionog sistema, a kojim se obezbjeđuje:
   - klasifikacija i zaštita informacija prema stepenu njihove osjetljivosti, s obzirom na moguće posljedice narušavanja povjerljivosti, integriteta i raspoloživosti informacija;
   - kontrolisanje pristupa resursima informacionog sistema, prostorijama sa resursima informacionog sistema, kao i sistemima koji su podrška funkcionisanju informacionog sistema i primjena odgovarajuće upravljačke, logičke i fizičke kontrole pristupa;
   - uspostavljanje sistema upravljanja korisničkim pravima pristupa, koji obuhvata procese evidentiranja, autorizacije, identifikacije, potvrde autentičnosti i nadzora korisničkih prava pristupa;
   - zaštita nematerijalnih resursa informacionog sistema od malicioznog programskog koda primjenom odgovarajućih upravljačkih, logičkih i fizičkih kontrola;
   - izrada i čuvanje operativnih i sistemskih zapisa koji omogućavaju rekonstruisanje događaja, otkrivanje neovlašćenih pristupa i radnji na informacionom sistemu, identifikovanje problema i utvrđivanje odgovornosti;
   - uspostavljanje procesa upravljanja incidentima, koji omogućavaju pravovremeni i efektivan odgovor u slučaju narušavanja bezbjednosti i funkcionalnosti resursa informacionog sistema koji podržavaju odvijanje poslovnih procesa;
   - odgovarajući način testiranja i odobravanja, prije uvođenja u produkcioni rad, razvijenih softverskih komponenti informacionog sistema, kao i novih hardverskih komponenti informacionog sistema.

Centralna banka Crne Gore (u daljem tekstu: Centralna banka) može donijeti uputstvo za primjenu odredaba stava 1 ovog člana.

Operativni rizik koji proizilazi iz elektronskog bankarstva

Član 8

Banka koja pruža usluge elektronskog bankarstva dužna je da u cilju kontrolisanja operativnog rizika koji proizilazi iz vršenja tih usluga, kao minimum:

1) primijenjuje bezbjedne i efikasne mehanizme za potvrdu autentičnosti i ovlašćenja lica, procesa i sistema;
2) obezbijedi odgovarajuću potvrdu svog identiteta na distribucionom kanalu elektronskog bankarstva, kako bi korisnici elektronskog bankarstva mogli provjeriti identitet banke;

3) obezbijedi postojanje odgovarajućih operativnih i sistemskih zapisa na osnovu kojih se mogu nesporno dokazati radnje povezane sa elektronskim bankarstvom.

Zaštita podataka

Član 9

Banka je dužna da uspostavi proces upravljanja rezervnim kopijama podataka, koji obuhvata postupke izrade, smještanja i testiranja rezervnih kopija podataka i restauracije podataka sa rezervnih kopija podataka, kako bi se obezbijedila raspoloživost podataka u slučaju potrebe i omogućio oporavak, odnosno ponovno uspostavljanje vitalnih poslovnih procesa u zahtijevanom vremenu.

Rezervne kopije podataka moraju biti ažurne i smještene na primjeren način na jednoj ili više bezbjednih lokacija od kojih najmanje jedna mora biti, u skladu sa procjenom rizika, dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci.

Plan za vanredne situacije

Član 10

Banka je dužna da sačini plan za vanredne situacije u cilju obezbjeđivanja kontinuiranog rada banke u slučaju nastanka ozbiljnih poremećaja u poslovanju uzrokovanih situacijama koje su van kontrole banke.

Planom iz stava 1 ovog člana utvrđuju se:

1) ključne poslovne aktivnosti za koje je neophodno očuvati kontinuitet obavljanja i u vanrednim situacijama;
2) scenarija događaja koji mogu uzrokovati prekid ključnih poslovnih procesa u banci;
3) alternativna rješenja za očuvanje kontinuiteta obavljanja ključnih poslovnih aktivnosti u vanrednim situacijama;
4) aktivnosti za uspostavljanje redovnog funkcionisanja poslovanja, a posebno oporavka informacionog sistema koji će omogućiti oporavak i raspoloživost resursa informacionog sistema potrebnih za odvijanje vitalnih poslovnih procesa u zahtijevanom vremenu;

Plan iz stava 1 ovog člana testira se najmanje jednom godišnje, a rezultati tog testiranja prezentiraju se nadležnom organu banke.

Evidentiranje gubitaka

Član 11

Banka je dužna da formira bazu podataka o svim nastalim gubicima po osnovu operativnog rizika i utvrdi metodologiju za interno evidentiranje tih gubitaka, po kategorijama utvrđenim prema izvorima gubitaka.

Banka koja za izračunavanje potrebnog kapitala za operativni rizik primjenjuje standardizovani metod, dužna je da podatke o gubicima po osnovu operativnog rizika

raspoređuje po odgovarajućim poslovnim područjima i po kategorijama utvrđenim prema izvorima gubitaka.

Izvještavanje Centralne banke

Član 12

Banka je dužna da o gubicima koji su proistekli iz operativnog rizika, a koji prelaze 1% sopstvenih sredstava banke, obavijesti Centralnu banku i to najkasnije u roku od osam radnih dana od dana nastanka gubitka.

Izvještaj iz stava 2 ovog člana sadrži uzroke i iznos gubitka, radnje koje je banka preduzela da nadoknadi gubitak, kao i radnje koje je banka preduzela ili namjerava da preduzme u cilju sprječavanja nastanka sličnih gubitaka u budućnosti.

3. Završne odredbe

Član 13

Stupanjem na snagu ove odluke prestaje da važi Odluka o minimalnim standardima za upravljanje operativnim rizikom u bankama (»S.list RCG«, br. 08/05.)

Član 14

Ova odluka stupa na snagu osmog dana od dana objavljivanja u »Službenom listu Crne Gore«, izuzev čl. 7 i 8 koji će se primjenjivati od 1. januara 2010. godine.

SAVJET CENTRALNE BANKE CRNE GORE

P R E D S J E D N I K

Ljubiša Krgović s.r.

O.br. 0101-325/2-29
Podgorica, 24.02.2009.god.