Rad primljen: 18.12.2009.
UDK: 005.334:[004.738.5:339

UPRAVLJANJE RIZICIMA U ELEKTRONSKOM BANKARSTVU

MANAGING RISKS OF ELECTRONIC BANKING

Tijana Radojević

Rezime: Primena informacione tehnologije u bankarstvu donosi, s jedne strane, snažan porast organizacionih i ekonomskih potencijala, a sa druge strane, otvara prostor za pojavu novih oblika rizika. Znači, brzi razvoj potencijala e-bankinga nosi i rizike i koristi. Zbog toga se adekvatno obezbeđenje sigurnosti, pojavljuje kao poseban kritičan faktor u funkcionisanju elektronskog bankarstva. Suština problema bezbednosti savremenih sistema elektronskog bankarstva svodi se na rizike narušavanja bezbednosti podataka i identiteta subjekata, pri čemu se relativni odnos značaja pomenutih elemenata menja sa tehnološkim razvojem.

Ključne reči: bankarski rizici, rizik menadžment, elektronsko bankarstvo.

Abstract: *Application of information technology in banking brings, with one hand, strong organizational and economic growth potential, and on the other hand, opens space for the emergence of new forms of risk. So, rapid development potential of e-banking carries risks and benefits. Therefore, the provision of adequate security, appear as a separate critical factor in the functioning of electronic banking. The essence of security problems of modern electronic banking system reduced the risks of data security breaches and identity of entities, whereby the relative importance of these elements changes with technological development.*

Key words*: banking risks, risk management, electronic banking.*

1. UVOD

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 konkurentske 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.

2. POJAM BANKARSKIH RIZIKA

Rizici kao mogućnost apsolutnog ili relativnog gubitka u odnosu na očekivanja u poslovanju banaka su karakteristika svakog bankarskog posla, a osvajanjem novih instrumenata, tehnika i strategija, finansijskog inženjeringa, novih bankarskih proizvoda, a naročito finansijskih derivata, lista rizika se neprestano širi. Neizvesnost raste sa promenama u kamatnim stopama, promenama depozita i sa nesposobnošću dužnika da vrati kredit, ali i pod dejstvom takvih faktora kao što su deregulacija, moralni hazard, kao i ulaskom banaka u poslove koji ranije nisu bili tradicionalno bankarski.

Globalizacija bankarskog poslovanja i trendovi spajanja i pripajanja velikih banaka, nagone menadžment banke da identifikuju najvažnije rizike. To se odnosi, pre svega, na sistemske rizike, i posebno na rizike koji proizilaze iz zaostajanja bankarskog menadžmenta u praćenju poslovanja na nepoznatim, geografski udaljenim tržištima [1]. Banke, saglasno Bazelu II, imaju pravo da razviju sopstevnu internu metodologiju za merenje rizika. Generalni cilj svake banke je optimizacija odnosa rizika i prinosa. Na osnovu njega banke mogu da izaberu najprofitabilnije proizvode i grane bankarstva, kao i najbolji način za određivanje cene proizvoda.

Konačno, banke će morati da ulože značajne materijalne i ljudske resurse kako bi postavile na kvalitativno viši nivo upravljanje rizicima.

Slika 1. Izloženost banke rizicima

3. RIZICI U ELEKTRONSKOM BANKARSTVU

Banke se tokom pružanja usluga elektronskog bankarstva i upotrebe elektronskog novca suočavaju sa određenim setom specifičnih rizika, a to su: [2]

- operativni rizik,
- reputacioni rizik,
- pravni rizik,
- rizik internacionalnog poslovanja,
- ostali rizici.

3.1. Operativni rizik

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:

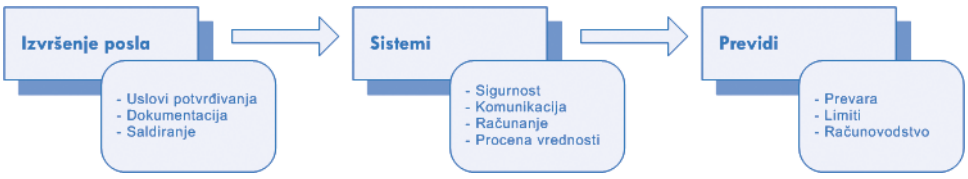
- rizici sigurnosti (pouzdanosti i integriteta sistema),
- rizici dizajniranja, implementacije i održavanja sistema,
- rizici zloupotrebe proizvoda ili usluga od strane klijenata.

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 razvoj 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 obezeđuje nesmetano odvijanje elektronskog bankarstva i poslove sa elektronskim novcem.

Jedan od mogućih rizika dizajniranja, implementacije i održavanja sistema, predstavljaju zaposleni i menadžment

Slika 2. Obuhvat operativnog rizika u bankama



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 toga je slaba implementacija novih tehnologija i nemogućnost da se obezbedi kontinuirana podrška razvoju. Neophodno je sprovoditi obuku, kao permanentni proces, i za menadžment i za zaposlene. [3]

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.

3.2. Reputacioni rizik

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.

3.3. Pravni rizik

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.

3.4. 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, 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.

3.5. 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 vremeneske periode, koji nisu propraćeni 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.

4. UPRAVLJANJE RIZICIMA

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.

4.1. PROCENA RIZIKA

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 emprijska 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 rizka, 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.

4.2. 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.

4.3. 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 sistema. [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.

5. 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 prudencijalan način. Ovaj razlog naveo je Bazelski komitet za bankarsku kontrolu [5] sprovede preliminarno istaživanje implikacija upravljanja rizikom na e-banking i e-novac. Ova rana studija pokazala je jasno potrebu za još mnogo 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).

5.1. IZAZOVI UPRAVLJANJA RIZIKOM

EGB 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 spreme 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 vebsajtovi 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 manuel-

nih 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 autsorsinga 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.

5.2. 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 način:[6]

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 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 e-bankinga, 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 odnostiti 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.

6. ZAKLJUČAK

Rizici u bankarskom poslovanju su sastavni deo posla. Novi komunikacioni kanal koji opštim imenom možemo nazvati elektronsko bankarstvo, donelo je značajne prednosti kako banci tako i njenim klijentima. Činjenica je da je elektronsko bankarstvo učinilo da banke, prvi put u svojoj istoriji, načine iskorak iz svog poslovnog prostora i dopuste da korisnici samostalno obavljaju svoje poslove vezane za banku. Ovaj iskorak doneo je, s jedne strane bankama značajne uštede i proširenje korisničke baze ali je, s druge strane, naterao banke da deo svojih poslova dislociraju u druge specijalizovane firme.[7]

Da bi se banke zaštitile od poslovnog, pravnog i reputacionog rizika, usluge e-bankinga moraju da se pružaju konziste-ntno i blagovremeno, u skladu sa visokim očekivanjima klijenata u pogledu stalne i brze raspoloživosti, ali i u skladu sa potencijalno visokom tražnjom za transakcijama. Banke mo-

raju da budu sposobne da pružaju usluge e-bankinga svim krajnjim korisnicima i da budu u stanju da održe takvu raspoloživost u svim okolnostima. Efektivni mehanizmi za reagovanje na incidente su takođe od ključnog značaja za umanjenje ope-rativnog, pravnog i reputacionog rizika koji nastaju kao posledica neočekivanih događaja, uključujući interne i eksterne napade, koji mogu da ugroze pružanje e-banking sistema i usluga. Da bi se odgovorilo očekivanjima klijenata, banke moraju da imaju efektivan kapacitet, poslovni kontinuitet i planove za svaku eventualnost. Banke treba da razviju odgovarajuće planove za reagovanje na incidente, uključujući komunikacione strategije, koje obezbeđuju kontinuitet poslovanja, kontrolu reputacionog rizika i limitiranje obaveza po osnovu poremećaja u njihovim uslugama e-bankinga.

Literatura

[1] Bjelica, V., *Bankarstvo*, Stylos, Novi Sad, 2001, str.265

[2] Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, mart 1998, www.bis.org/publ/bcbs35.pdf

[3] www.eccf.su.ac.yu/obaveštenja/inf_u_finansijama.htm

[4] Vunjak N.: *Finansijski menadžment*, Proleter Bečej, Subotica, 2005, str. 340

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

[6] Vuković D.: *Principi upravljanja rizikom za elektronsko bankarstvo*, prevod, Jugoslovenski pregled, Beograd, 2007, str.101

[7] Vasković V.: *Sistemi plaćanja u elektronskom poslovanju*, Fakultet oragizacionih nauka, Beograd, 2007, str.392

Autor

Mr Tijana Radojević
Univerzitet Singidunum,
Danijelova 32, Beograd
e-mail:
tradojevic@singidunum.ac.rs

Oblast istraživanja:
finansije i bankarstvo,
elektronsko poslovanje.