PRINCIPI UPRAVLJANJA RIZIKOM U ELEKTRONSKOM BANKARSTVU

RISK MANAGEMENT PRINCIPLES FOR ELECTRONIC BANKING

Dr Rade Stankić, redovni profesor
Ekonomski fakultet, Beograd

Apstrakt. Upravljanje rizicima u bankarskom poslovanju obuhvata identifikovanje, merenje i procenu rizika s ciljem minimiziranja njihovih negativnih efekata na finansijski rezultat i kapital banke. Bazelski komitet za bankarsku superviziju je definisao četrnaest principa upravljanja rizikom u e-bankarstvu, a sve u skladu s velikim promenama vezanim za tehnološke inovacije i inovacije servisa, opšteprisutan i globalan karakter otvorenih elektronskih mreža, integraciju aplikacija e-bankarstva sa već postojećim računarskim sistemima i povećane zavisnosti banaka od informacionih tehnologija.

Ključne reči: e-bankarstvo, upravljanje rizikom

Abstract. Risk management in banking business includes identification, measurement and risk assessment with the aim of minimizing potential negative effects on the financial result and capital of the bank. Basel Committee on Banking Supervision has defined fourteen principles of risk management in e-banking, in accordance with major changes related to technology and service innovations, global character of open electronic networks, integration of e-banking applications with existing computer systems and increased bank dependence on information technology.

Key words: e-banking, risk management

UVOD

Svaka banka se u svom poslovanju neminovno susreće sa različitim vrstama rizika iz kojih mogu proisteći negativni efekti na poslovanje banke. Upravljanje rizicima u bankarskom poslovanju obuhvata identifikovanje, merenje i procenu rizika s ciljem minimiziranja njihovih negativnih efekata na finansijski rezultat i kapital banke. Tehnološki napredak i tržišna konkurencija učinili su da se asortiman bankarskih proizvoda i usluga stalno unapređuju, a jedan od najvažnijih modernih servisa je elektronsko bankarstvo. Uočivši da ovaj segment bankarskih proizvoda podrazumeva i određene rizike, Bazelski komitet za bankarsku superviziju je definisao principe upravljanja rizikom u e-bankarstvu. Bazelski komitet smatra da su uvođenjem elektronskog bankarstva neki od tradicionalnih rizika povećani i modifikovani. U skladu sa tim došlo se do zaključka da su postojeća opšta načela upravljanja rizikom primenljiva na poslove e-bankarstva, ali da ih je potrebno prepraviti i prilagoditi, i u nekim slučajevima – proširiti. Nakon definisanja novih načela, stanovište Komiteta je da uprave banaka moraju preduzeti mere za preispitivanje i modifikaciju svojih postojećih politika i postupaka upravljanja rizikom, kako bi se njima pokrili i tekući i planirani poslovi e-bankarstva. Integracija aplikacija e-bankarstva sa već postojećim sistemima podrazumeva integrisani pristup upravljanju rizikom za sve poslove u banci.

PREPORUKE BAZELSKOG KOMITETA

Bazelski komitet je utvrdio četrnaest principa upravljanja rizikom u elektronskom bankarstvu s ciljem da pomogne bankama u proširivanju postojećih politika i postupaka kontrole rizika tako da one obuhvate i poslove e-bankarstva. Principi nisu postavljeni kao apsolutni zahtevi, pa čak ni kao "najbolja praksa". Komitet je bio na stanovištu da utvrđivanje previše detaljnih zahteva za upravljanje rizikom može biti kontraproduktivno, zbog same činjenice da bi oni mogli ubrzo zastareti s obzirom na brzinu promena. Zato je opredeljenje Komiteta bilo da definiše generalna očekivanja i preporuke, koje će promovisati sigurnost poslovanja u e-bankarstvu, uz zadržavanje fleksibilnosti u primeni. Pored toga, rizični profil svake banke je drugačiji i zahteva posebno prilagođen pristup ublažavanju rizika, zavisno od obima poslova e-bankarstva, značaja prisutnih rizika, kao i spremnosti i sposobnosti institucije da njima upravlja. Cilj principa nije da se definišu posebna tehnička rešenja ili standardi koji se odnose na e-bankarstvo. Tehnička rešenja moraju doneti institucije i tela koja propisuju standarde uporedo sa razvojem tehnologije. Zbog toga je očekivanje Komiteta da nacionalna suprevizorska tela upotrebe principe kao osnovne smernice koje će prilagoditi posebnim nacionalnim zahtevima i pojedinačnim profilima rizika. Od najvišeg menadžmenta banke se

očekuje da definiše eksplicitne, obrazložene i dokumentovane strateške odluke, koje se tiču toga hoće li banka i na koji način pružati usluge e-bankarstva. Aktivnosti menadžmenta treba da pokriju i preispitivanje i odobravanje ključnih aspekata procesa kontrole sigurnosti banke, kao što je razvoj i održavanje infrastrukture kontrolnih mehanizama kojima je zaštićen sistem e-bankarstva.

Posebnu pažnju trebalo bi posvetiti dodeli prava autorizacije i merama provere identiteta, kontroli logičkog i fizičkog pristupa, adekvatnoj infrastrukturi sigurnosti radi uspostavljanja ograničenja za interne i eksterne poslove korisnika, kao i verodostojnosti podataka o transakcijama, dokumentacije i informacija. Potrebno je obezbediti postojanje jasnih pisanih revizorskih tragova za sve transakcije e-bankarstva, a nivo mera za očuvanje poverljivosti informacija e-bankarstva treba da odgovara osetljivosti takvih informacija. Iako se zaštita klijenata i propisi o zaštiti privatnosti razlikuju od jedne države do druge, banke svakako imaju jasnu odgovornost da pruže svojim klijentima određeni nivo sigurnosti u pogledu objavljivanja informacija, zaštite privatnih podataka i mogućnosti upotrebe tih podataka u poslovne svrhe. Taj nivo treba biti sličan onom koji se klijentima pruža kada se koriste tradicionalni bankarski metodi. Kako bi banke svele na najmanju moguću meru pravne i reputacione rizike, vezane za poslove e-bankarstva u zemlji i u inostranstvu, one moraju nivo zaštite privatnosti uskladiti sa zakonima zemlje u kojoj banka pruža usluge e-bankarstva.

Da bi se banka zaštitila od poslovnog, pravnog i reputacionog rizika, usluge e-bankarstva moraju se pružati dosledno i pravovremeno, u skladu sa očekivanjima klijenata. Zbog toga su efikasni mehanizmi za vanredne slučajeve isto tako važni za minimiziranje operativnog, pravnog i reputacionog rizika, koji proizlaze iz neočekivanih događaja, kao što su interni i eksterni upadi u sistem. Banke bi morale izraditi odgovarajuće planove za incidentne slučajeve, uključujući strategiju komunikacije koja obezbeđuje kontinuitet poslovanja, kontroliše reputacioni rizik i locira odgovornost, ali i rezultate kod poremećaja u uslugama e-bankarstva.

Karakteristike e-bankarstva predstavljaju novi izazov za upravljanje rizikom. Pre svega, to je brzina promena povezanih s tehnološkim inovacijama. Nekada je uvođenje novih aplikacija trajalo dugo i sprovodilo se tek nakon opsežnog testiranja. Danas, međutim, banke, pod pritiskom konkurencije, u vrlo kratkom vremenu realizuju nove servise. Generalno posmatrano, e-bankarstvo povećava zavisnost banaka o informacionoj tehnologiji, povećavajući tehničku složenost mnogih operativnih i bezbednosnih pitanja. Ono, takođe, povećava ulogu eksternalizacije uz pomoć trećih strana, nebankarskih subjekata, poput pružaoca usluga Interneta, telekomunikacionih kompanija i drugih preduzeća koja se bave tehnologijom. Internet je svima dostupan i globalan po svojoj prirodi. To je otvorena mreža kojoj subjekti imaju pristup s bilo kog mesta u svetu. Zbog toga postaju veoma važni: bezbednosna kontrola, tehnika provere identiteta klijenata, zaštita podataka, postupak ostavljanja pisanog revizorskog traga i standardi zaštite privatnosti klijenata. Iako su tradicionalna načela upravljanja rizikom u bankarstvu primenjiva i na poslove e-bankarstva, složene karakteristike Interneta, kao distribucionog kanala, zahtevaju da primena tih načela bude organizovana tako da odgovara različitim on-line bankarskim poslovima i sa njima povezanim izazovima upravljanja rizikom.

Ove preporuke koriste definiciju operativnog rizika koju je dao Bazelski odbor, koja navodi da je to rizik gubitka koji proizlazi iz neadekvatnih ili neuspešnih internih procesa, ljudi i sistema ili zbog eksternih događaja. Dokument preporučuje integralni pristup upravljanja rizikom za sve bankarske poslove, a upravljanje rizikom u poslovima e-bankarstva mora biti sastavni deo celokupnog sistema upravljanja rizikom banke.

Načela upravljanja rizikom u elektronskom bankarstvu mogu se razvrstati u tri kategorije, koje se često preklapaju:

A) Nadzor kojim rukovodi odbor i menadžment

1. Delotvoran nadzor poslova e-bankarstva od strane menadžmenta;
2. Uspostavljanje sveobuhvatnih procesa kontrole sigurnosti;
3. Temeljna analiza poslovanja (*due diligence*) i proces nadzora kojim rukovodi menadžment pri eksternalizaciji i ostalim oblicima zavisnosti o uslugama trećih strana.

B) Kontrola sigurnosti

4. Provera identiteta klijenata koji koriste usluge e-bankarstva;
5. Neporicanje obaveza i odgovornost za transakcije e-bankarstva;
6. Odgovarajuće mere koje obezbeđuju raspodelu dužnosti;
7. Odgovarajuće kontrole provere identiteta unutar sistema e-bankarstva, baza podataka i aplikacija;

8. Integritet podataka, dokumentacije i informacija koji se odnose na transakcije e-bankarstva;
9. Uspostavljanje jasnih pisanih revizorskih tragova za transakcije e-bankarstva;
10. Poverljivost ključnih informacija banke.

C) Upravljanje pravnim i reputacionim rizikom

11. Odgovarajuće izveštavanje za usluge e-bankarstva;
12. Poverljivost informacija o klijentu;
13. Kapacitet, poslovni kontinuitet i planiranje za slučaj nepredviđenih okolnosti kako bi se osigurala raspoloživost sistema i usluga e-bankarstva;
14. Planiranje postupaka za incidente.

A) Nadzor kojim rukovodi odbor i menadžment (1. do 3. načela)

Menadžment višeg nivoa je odgovoran za razvoj poslovne strategije bankarske institucije i on donosi eksplicitnu stratešku odluku o pružanju usluga e-bankarstva. Menadžment treba da osigura da svi planovi vezani za e-bankarstvo budu jasno integrisani u korporativne strateške ciljeve, kao i da se sprovede analiza rizika kod predloženih poslova e-bankarstva, uspostave odgovarajući procesi ublažavanja i praćenja rizika za utvrđene rizike, te da se sprovodi kontinuirano preispitivanje, kako bi se ocenili rezultati poslovanja e-bankarstva u odnosu na poslovne planove i ciljeve institucije. Pružanje finansijskih usluga preko Interneta može značajno modifikovati ili čak povećati tradicionalne bankarske rizike (npr. strateški, reputacioni, kreditni, operativni i rizik likvidnosti). Stoga je potrebno preduzeti mere za modifikaciju postojećih procesa upravljanja rizikom banke, u svrhu njihovog prilagođavanja uslugama e-bankarstva.

1. načelo: Odbor direktora i menadžment višeg nivoa treba da uspostave delotvoran nadzor upravljanja rizicima koji su vezani za poslove e-bankarstva, uključujući jasno alociranje odgovornosti, politika i kontrola za upravljanje tim rizicima.

Sledeći aspekti e-bankarstva mogu biti značajani za procese upravljanja rizikom:

- Glavni elementi distribucionih kanala izvan su direktne kontrole banke;
- Internet omogućava globalno pružanje usluga nezavisno od toga da li ta institucija posluje u konkretnim zemljama;
- Složenost pitanja koja su povezana sa e-bankarstvom, koja uključuju posebna znanja, kao i tehnički jezik i pojmove koji neretko prelaze okvire tradicionalnog menadžmenta viših nivoa.

Menadžment treba da obezbedi da se banka ne upušta u nove poslove e-bankarstva ili u usvajanje novih tehnologija ako nema potrebnu stručnost za sprovođenje kompetentnog nadzora nad upravljanjem rizikom. Stručnost uprave i zaposlenih treba da odgovara tehničkom karakteru i složenosti aplikacija e-bankarstva. Značajan reputacioni rizik povezan s e-bankarstvom zahteva kontinuirano praćenje operativne sposobnosti sistema i zadovoljstva klijenata, kao i odgovarajuće izveštavanje o incidentnim slučajevima. Menadžment treba da osigura da procesi upravljanja rizikom u e-bankarstvu budu integrisani u sveukupni pristup upravljanja rizikom banke.

Mere za upravljanja rizikom treba da uključuju:

- Jasno utvrđenu sklonost riziku institucije u odnosu na e-bankarstvo;
- Uspostavljanje ključnih mehanizama podele dužnosti i izveštavanja, uključujući postupke za nepredviđene okolnosti, zdravo poslovanje i održavanje reputacije (npr. upad u mrežu, narušavanje sigurnosti od strane zaposlenih, zloupotreba sistema i sl.);
- Uzimanje u obzir svih jedinstvenih faktora rizika povezanih sa obezbeđivanjem sigurnosti, integriteta i raspoloživosti proizvoda i usluga e-bankarstva, kao i obezbeđivanje da treće strane, kojima je banka eksternalizovala svoj sistem i aplikacije, preduzmu sliče mere;
- Obezbeđivanje sprovođenja odgovarajućih temeljnih analiza poslovanja i analize rizika pre nego što banka počne obavljati poslove e-bankarstva u inostranstvu.

Internet omogućava distribuciju proizvoda i usluga globalno. Eventualni prekogranični poslovi e-bankarstva, posebno ako se obavljaju bez ikakve odobrene fizičke prisutnosti u "državi domaćinu", mogu izložiti banku povećanom pravnom i regulatornom riziku, zbog razlika koje mogu postojati između država u odnosu na izdavanje dozvole za rad bankama, nadzor i zahteve za zaštitu privatnosti klijenata. Resursi potrebni za

nadzor usluga e-bankarstva treba da odgovaraju osobinama i važnosti sistema, osetljivosti mreže i osetljivosti informacija koje se prenose.

2. načelo: Menadžment višeg nivoa treba da odobri sve ključne aspekte procesa kontrole bezbednosti.
Odbor direktora i menadžment višeg nivoa treba da nadziru razvoj i kontinuirano sprovođenje sigurnosnih mera, čiji je zadatak da štiti sisteme i podatke vezane za e-bankarstvo od internih i eksternih pretnji. To uključuje uspostavljanje odgovarajućih prava autorizacije, kontrole logičkog i fizičkog pristupa, i adekvatnu infrastrukturu za ograničavanje aktivnosti internih i eksternih korisnika. Menadžment mora utvrditi da li banka ima sveobuhvatne procese sigurnosti, uključujući politike i procedure koje se odnose na moguće interne i eksterne pretnje sigurnosti. Ključni elementi delotvornog procesa sigurnosti uključuju:

- Dodeljivanje eksplicitnih odgovornosti menadžmentu/zaposlenima u pogledu nadzora nad uspostavljenom politikom sigurnosti i njenim sprovođenjem;
- Fizičku kontrolu za sprečavanje neautoriziranog fizičkog pristupa računarskom okruženju;
- Adekvatnu logičku kontrolu i procese praćenja za sprečavanje neautoriziranog internog i eksternog pristupa aplikacijama i bazama podataka e-bankarstva;
- Redovno preispitivanje i testiranje sigurnosnih mera i kontrola, uključujući kontinuirano praćenje aktuelnog razvoja sigurnosti u bankarstvu, kao i instalaciju odgovarajućih dograđenih softvera, uslužnih paketa i ostalih potrebnih mera.

3. načelo: Odbor direktora i menadžment višeg nivoa trebalo bi da uspostave opsežnu, kontinuiranu i temeljnu analizu poslovanja (*due diligence*) i procese nadzora za upravljanje eksternalizovanim procesima banke, odnosno svim oblicima oslanjanja na treće strane kod pružanja servisa e-bankarstva.

Povećano oslanjanje na spoljne partnere, koji deluju kao treće strane u obavljanju važnih funkcija e-bankarstva, smanjuje direktnu kontrolu menadžmenta banke. U skladu s tim, potrebno je razraditi sveobuhvatan proces upravljanja rizicima povezanim s eksternalizacijom i ostalim vrstama oslanjanja na treće strane. U prošlosti je eksternalizacija često bila ograničena na jednog pružaoca usluga - za jednu određenu funkciju. Međutim, poslednjih godina eksternalizovani servisi povećali su se i po broju i složenosti, što je direktna posledica napretka u informacionoj tehnologiji. Složenost se kod e-bankarstva još više povećava zbog činjenice da izdvojene usluge e-bankarstva mogu pružati i dodatni podugovarači ili se mogu pružati u stranoj zemlji. Kako aplikacije i usluge e-bankarstva postaju tehnološki naprednije i strateški značajnije, određena funkcionalna područja e-bankarstva zavise od malog broja specijalizovanih pružaoca usluga. Takva kretanja mogu dovesti do povećane koncentracije rizika, implicirajući potrebu za dodatnim oprezom i sa strane pojedinačne banke, ali i sistema u celini.

Menadžment višeg nivoa trebalo bi da se posebno usmeri na ostvarivanje sledećeg:

- Banka u potpunosti treba biti svesna rizika povezanih sa eksternalizacijom;
- Pre sklapanja takvih ugovora potrebno je sprovesti detaljno preispitivanje kompetentnosti i finansijske snage pružaoca usluga, odnosno treće strane;
- Potrebno je jasno definisati odgovornost svih strana;
- Svi eksternalizovani sistemi i poslovi e-bankarstva trebalo bi da budu usklađeni s politikama upravljanja rizikom, sigurnosnim politikama i politikama o zaštiti privatnosti koje zadovoljavaju standarde same banke;
- Povremene nezavisne interne i/ili eksterne revizije eksternalizovanih poslova trebalo bi sprovoditi makar u onoj meri koja bi bila potrebna kada bi se takvi poslovi obavljali interno;
- Neophodno je definisati planove za slučaj nepredviđenih okolnosti za eksternalizovane poslove e-bankarstva.

B) Kontrola sigurnosti (4. do 10. načela)

Kod definisanja procesa i postupka u okviru kontrole bezbednosti sledeća pitanja su od posebnog značaja:

- Provera identiteta;
- Neporecivost odgovornosti;
- Integritet podataka i transakcija;
- Razdvajanje dužnosti;

- Kontrola autorizacije;
- Postojanje pisanih revizorskih tragova;
- Poverljivost ključnih bankarskih informacija.

4. načelo: Banke treba da preduzmu odgovarajuće mere za proveru identiteta i autorizacije prilikom transakcija preko Interneta.

Dakle, važno je obezbediti da određena komunikacija, transakcija ili zahtev za pristupom budu legitimni. U skladu s tim, banke treba da koriste pouzdane metode provere identiteta i autorizacije novih klijenata, kao i utvrđivanje identiteta i ovlašćenja postojećih klijenata koji iniciraju elektronsku transakciju. Na primer, utvrđivanje identiteta klijenta, prilikom otvaranja računa, važno je za smanjivanje rizika krađe identiteta, lažnih prijava za otvaranje računa i pranja novca. U slučaju kada su poslovi e-bankarstva autsorsovani, mora se osigurati da se provajderi servisa prema tim pitanjima odnose barem zadovoljavajući standarde same banke. Identifikacija se odnosi na postupke, tehnike i procese koji se koriste za utvrđivanje identiteta klijenta. Autorizacija označava postupke, tehnike i procese koji se koriste kako bi se utvrdilo da klijent ima legitiman pristup određenom bankarskom računu ili ovlašćenje za obavljanje transakcija vezanih za taj račun. Utvrđivanje i provera identiteta pojedinca i ovlašćenja za pristup bančinom informacionom sistemu, u elektronski otvorenom mrežnom okruženju, može biti težak zadatak. Legitimna autorizacija korisnika može biti simulirana pomoću nekoliko tehnika poznatih pod nazivom "oponašanje" (engl. *spoofing*). Hakeri mogu presresti transakcije putem Interneta pomoću tehnika tzv. "njuškanja" (engl. *sniffer*).

Banke mogu koristiti različite metode utvrđivanja identiteta, uključujući PIN-ove, lozinke, "pametne" (engl. *smart*) kartice, biometrijske metode, digitalne potvrde itd. Sve te metode mogu biti jednofaktorske ili multifaktorske – pružaju veći stepen bezbednosti (npr. istovremena upotreba lozinke i biometrijskih tehnologija). Koje će metode provere identiteta banka koristiti – odlučuje se na osnovu procena rizika. U analizi rizika potrebno je oceniti i tipove transakcionih mogućnosti sa aspekta rizika koji su im imanentni (prenos sredstava, plaćanje računa, uzimanje kredita, pregled stanja računa,...), odnosno osetljivost i vrednost podataka i jednostavnost metoda pristupa. Robusni postupci identifikacije i provere identiteta klijenata posebno su važni kod prekograničnih poslova e-bankarstva, uključuju veći rizik i teže obavljanje provere kreditne sposobnosti potencijalnih klijenata. Efikasne mere provere identiteta smanjuju mogućnosti da autorizovani korisnik naknadno poriče da je autorizovao i izvršio određenu transakciju. Svako dodavanje, brisanje ili promena sistema ili baze podataka mora biti dokumentovano i zabeleženo. Isto tako, potvrđena sesija e-bankarstva treba biti zaštićena tokom celokupnog trajanja povezanosti, a u slučaju prekida za novu sesiju neophodno je zahtevati ponovnu proveru identiteta.

5. načelo: Potrebno je koristiti metode provere autentičnosti koje obezbeđuju neporecivost i uspostavljaju odgovornost za izvršene transakcije.

Rizik poricanja transakcije postoji i kod „tradicionalnih transakcija“, kao što su transakcije kreditnim karticama, međutim, e-bankarstvo povećava taj rizik zbog poteškoća utvrđivanja identiteta, zbog mogućnosti menjanja ili presretanja elektronskih transakcija, kao i mogućnosti tvrdnje korisnika e-bankarstva da su transakcije prevarom izmenjene. Sistemi e-bankarstva treba da budu strukturirani tako da smanjuju verovatnoću da korisnici obave nenameravanu transakciju, odnosno da u potpunosti razumeju rizike povezane sa bilo kojom transakcijom koju započinju. Za sve strane uključene u transakciju sa sigurnošću treba biti utvrđen identitet, a kanale komunikacije držati pod kontrolom. Tehnike koje pomažu da se ostvari neporicanje, odnosno da se osigura poverljivost i verodostojnost transakcija e-bankarstva su digitalne potvrde koje se koriste u infrastrukturi javnog ključa i sl. Izdavanjem digitalne potvrde klijentu se obezbeđuje jedinstvena identifikacija/provera identiteta i smanjuje rizik poricanja transakcije. U nekim državama zakonom je regulisana pravna obaveznost digitalnog potpisa. U infrastrukturi javnog ključa svaka strana ima par ključeva: jedan privatni i jedan javni ključ. Privatni ključ je tajni, tako da ga upotrebljava samo jedna strana. Sve strane se koriste javnim ključem. Privatnim ključem stvara se elektronski potpis na dokumentu, a parovi ključeva napravljeni su tako da je poruku šifrovanu privatnim ključem moguće pročitati samo korišćenjem drugog ključa. Kada je reč o digitalnim sertifikatima, banka može delovati kao samostalno telo za izdavanje ili se može osloniti na neku proverenu treću stranu. U tom slučaju, banka treba da utvrdi da li je ta institucija prilikom izdavanja potvrde koristila isti nivo provere identiteta koji bi i banka koristila.

6. načelo: Banke treba da obezbede postojanje odgovarajućih mera za adekvatno razdvajanje dužnosti unutar sistema e-bankarstva, baza podataka i aplikacija.

Razdvajanje dužnosti osnovna je mera interne kontrole i svrha joj je smanjivanje rizika prevare u operativnim procesima i sistemima, kao i obezbeđivanje ispravne autorizacije, knjiženja i zaštite transakcija i imovine. Razdvajanje dužnosti važno je za postizanje tačnosti i verodostojnosti podataka u smislu sprečavanja prevara od strane pojedinca. Ako su dužnosti adekvatno raspodeljene, prevaru je moguće počiniti samo u međusobnom dosluhu pojedinaca. Usluge e-bankarstva mogu zahtevati modifikovanje načina razdvajanja dužnosti, s obzirom na to da se transakcije odvijaju preko elektronskih sistema gde se identiteti mogu lakše prikriti ili lažirati. Budući da je loše zaštićenim bazama podataka moguće lako pristupiti preko internih ili eksternih mreža, potrebno je dati naglasak važnosti strogih postupaka autorizacije i identifikacije, sigurne strukture obrade, i postojanja adekvatnih pisanih revizorskih tragova. Proces za izvršenje transakcija i pripadajući sistemi treba da budu strukturirani tako da jedan isti zaposleni/eksterni pružalac usluga ne može pristupiti, autorizovati i dovršiti transakciju. Podelu dužnosti treba uspostaviti između onih koji iniciraju statične podatke (uključujući sadržaj web-stranice) i onih koji su odgovorni za proveru njihovog integriteta. Sistemi e-bankarstva treba da budu testirani tako da se onemogući zaobilaženje podele dužnosti. Podelu treba održavati i između onih koji ih razvijaju i onih koji upravljaju sistemima e-bankarstva.

7. načelo: Banke moraju obezbediti postojanje odgovarajućih kontrola autorizacije i prava pristupa sistemima e-bankarstva, bazama podataka i aplikacijama.

Da bi očuvale podelu dužnosti, banke moraju strogo kontrolisati autorizaciju i pravo pristupa. Ako se ne obezbedi adekvatna kontrola autorizacije, pojedinac može izmeniti svoja ovlašćenja, zaobići podelu dužnosti i steći pristup sistemima e-bankarstva, bazama podataka i aplikacijama na koje nema pravo. Autorizacije i prava pristupa mogu se unutar banke uspostaviti ili na centralizovani ili na distribuirani način, i najčešće se smeštaju u baze podataka. Zaštita tih baza podataka od nameštanja ili iskrivljavanja nužna je za delotvornu kontrolu autorizacije.

8. načelo: Banke treba da obezbede postojanje odgovarajućih mera zaštite verodostojnosti podataka o transakcijama e-bankarstva, dokumentaciji i informacijama.

Verodostojnost podataka odnosi se na to da informacija koja se prenosi, ili koja je uskladištena, ne bude izmenjena bez autorizacije. Nenarušavanje verodostojnosti podataka o transakcijama, dokumentaciji i informacijama može izložiti banku finansijskim gubicima, i značajnom pravnom i reputacionom riziku. Direktna obrada naloga u e-bankarstvu može otežati otkrivanje programskih grešaka ili nedozvoljenih radnji u ranoj fazi. Budući da se e-bankarstvo obavlja preko javnih mreža, transakcije su izložene dodatnom riziku iskrivljivanja podataka, prevare i lažiranja. U skladu s time, potrebno je postojanje odgovarajućih mera za postizanje tačnosti, potpunosti i pouzdanosti transakcija e-bankarstva, dokumentacije i informacija koje se prenose preko Interneta, i koje ostaju u internim bazama podataka banke ili ih prenose/skladište pružaoci usluga - treće strane u ime banke.

Opšte prakse koje se koriste za očuvanje integriteta podataka unutar okruženja e-bankarstva su sledeće:

- Transakcije e-bankarstva potrebno je sprovoditi tako da budu u velikoj meri otporne na promenu tokom celog trajanja obrade;
- Dokumentaciju vezanu za e-bankarstvo treba skladištiti tako da bude otporna na iskrivljavanje;
- Transakcije e-bankarstva i postupci vođenja dokumentacije treba da su tako strukturirani da bude gotovo nemoguće zaobići otkrivanje neautoriziranih promena;
- Pored toga, moraju postojati adekvatne politike kontrole promena, uključujući postupke praćenja i testiranja, u svrhu zaštite od promena, koje mogu pogrešno ili nenamerno dovesti u pitanje kontrole ili pouzdanost podataka;
- Bilo kakvo iskrivljavanje transakcija e-bankarstva ili dokumentacije trebalo bi biti moguće otkriti pomoću funkcija obrade transakcija, praćenja i vođenja dokumentacije.

9. načelo: Banke moraju obezbediti postojanje jasnih pisanih revizorskih tragova za sve transakcije e-bankarstva.

Kod pružanja ovog servisa, pred bankama je izazov da obezbede ne samo sprovođenje delotvornih internih kontrola u visokoautomatizovanom okruženju već i nezavisnu reviziju tih kontrola, posebno za sve ključne događaje i aplikacije e-bankarstva. Interna kontrola banke može biti oslabljena ako se ne mogu sačuvati jasni pisani revizorski tragovi za poslove e-bankarstva. To zbog toga što je veliki deo, ako ne i sva dokumentacija i dokazi koji prate transakcije e-bankarstva u elektronskom obliku.

Jasni pisani revizorski tragovi potrebni su za:

- Otvaranje, promene ili gašenje računa klijenta;
- Svaku transakciju s finansijskim posledicama;
- Svaku autorizaciju koju dobije klijent za prekoračenje računa;
- Svako dodeljivanje, modifikovanje ili opoziv prava pristupa sistemu.

10. načelo: Banke treba da preduzmu i odgovarajuće mere za očuvanje poverljivosti ključnih informacija e-bankarstva. Mere koje se preduzimaju za očuvanje poverljivosti treba da odgovaraju osetljivosti informacija koje se prenose i/ili skladište u bazama podataka.

Banke moraju obezbediti da sistemi za vođenje dokumentacije budu strukturirani i konfigurisani tako da omogućavaju ponovno dobijanje dokumentacije koja je možda iskrivljena ili uništena. Poverljivost je obezbeđivanje da ključne informacije banke ostanu tajne, te da ih neće moći pregledavati ili koristiti neovlašćena lica. Zloupotreba ili neautorizovano objavljivanje podataka izlaže banku reputacionom i pravnom riziku. Pojava e-bankarstva je na tom polju dodatni izazov za sigurnost banke, jer povećava rizik da informacije koje se prenose preko javne mreže ili smeštaju u baze podataka postanu dostupne neovlašćenim osobama, ili iskorišćene onako kako to klijent koji daje informacije ne namerava i želi. Isto tako, povećana upotreba usluga spoljnih pružaoca usluga može izložiti ključne bančine podatke drugim stranama.

U tom smislu, banke moraju obezbediti sledeće:

- Da svi poverljivi podaci budu dostupni samo pojedincima ili sistemima koji su prošli propisanu autorizaciju i proveru identiteta;
- Da se svi poverljivi podaci čuvaju na siguran način i da budu zaštićeni od neautorizovanog pregledavanja i modifikovanja tokom prenosa preko javnih, privatnih ili internih mreža;
- Da se standardi i kontrole banke za korišćenje i zaštitu podataka poštuju kada treće strane imaju pristup podacima na osnovi eksternalizacije poslovanja;
- Da se svaki pristup podacima do kojih je pristup ograničen beleži, te da se ulaže odgovarajući napor kako bi se postiglo da ti zapisi budu otporni na iskrivljavanja.

C) Upravljanje pravnim i reputacionim rizikom (11. do 14. načela)

Zaštita prava klijenata, odnosno propisi i zakoni koji se odnose na privatnost razlikuju se od države do države. Međutim, banke, uvek, bez obzira na sistem, imaju jasnu odgovornost da osiguraju svojim klijentima određeni nivo sigurnosti objavljivanja informacija, zaštite podataka o klijentu i njihove raspoloživosti u poslovanju, a koja treba da odgovara nivou koji bi imali da poslove obavljaju preko tradicionalnih bankarskih distribucionih kanala.

11. načelo: Banke moraju obezbediti postojanje adekvatnih informacija na svojim web-stranicama koje će potencijalnim klijentima omogućiti donošenje jasnog zaključka o identitetu i regulatornom statusu banke, pre upuštanja u transakcije e-bankarstva.

Među takvim informacijama su:

- Ime banke i lokacija njenog sedišta (i lokalnih filijala, ako je to potrebno);
- Identitet glavnog nadzornog tela banke, odgovornog za nadzor nad sedištem banke;
- Način na koji klijenti mogu kontaktirati s bančinom službom za korisnike po pitanjima problema vezanih za usluge, pritužbe, sumnje na zlopotrebu računa i dr.;
- Način na koji se klijenti mogu obratiti ombudsmanu ili telu koje se bavi zaštitom potrošača;

- Način na koji klijenti mogu ostvariti pristup informacijama o naknadama štete koje se primenjuju ili o programu osiguranja depozita, kao i o nivou zaštite koju oni mogu pružiti (ili linkovi na web-stranice koje pružaju takve informacije),
- Ostale informacije koje mogu biti korisne sa aspekta određene države.

12. načelo: Banke treba da preduzmu odgovarajuće mere za obezbeđenje usklađenosti sa zahtevima za poštovanje privatnosti klijenata, primenljivim u državama u kojima banka pruža proizvode i usluge e-bankarstva.

Očuvanje poverljivosti informacija o klijentu ključna je odgovornost banke. Zloupotreba ili neautorizovano objavljivanje poverljivih podataka o klijentu izlaže banku pravnom i reputacionom riziku. Da bi odgovorile na te izazove koji se tiču očuvanja poverljivosti informacija o klijentu, banke bi trebalo da ulažu adekvatne napore kako bi obezbedile sledeće:

- Bančina politika i standardi koji se odnose na privatnost klijenta trebalo bi da budu usklađeni sa svim propisima i zakonima o privatnosti koji se primenjuju u državama u kojima banka pruža proizvode i usluge e-bankarstva;
- Klijenti treba da budu upoznati sa politikama koje se odnose na privatnost i relevantnim pitanjima vezanim za privatnost, a kod korišćenja proizvoda i usluga e-bankarstva;
- Klijenti bi trebalo da imaju mogućnost da odbiju (ili povuku) ovlašćenje banci da deli s trećom stranom sve informacije o klijentovim ličnim potrebama, interesima, finansijskom položaju ili bankarskom poslovanju;
- Podaci o klijentima ne bi se smeli koristiti, osim u zakonom dopuštene svrhe, ili ako su klijenti autorizovali njihovu upotrebu;
- Standardi banke za upotrebu podataka o klijentu moraju se poštovati i onda kada treće strane na osnovi eksternalizacije poslovanja imaju pristup podacima o klijentu.

13. načelo: Banke bi trebalo da imaju odgovarajući kapacitet, poslovni kontinuitet i planiranje za slučaj nepredviđenih okolnosti kako bi i tada obezbedile raspoloživost sistema i usluga u e-bankarstvu.

Kako bi se banke zaštitile od poslovnog, pravnog i reputacionog rizika, usluge e-bankarstva moraju se pružati dosledno i pravovremeno, u skladu sa očekivanjima klijenata. Da bi se to postiglo, banka mora biti sposobna da pruža usluge e-bankarstva krajnjim korisnicima iz primarnih izvora (npr. interni bančini sistemi i aplikacije) ili sekundarnih izvora (npr. sistemi i aplikacije pružaoca usluga). Održavanje adekvatne raspoloživosti takođe zavisi od sposobnosti rezervnih sistema u slučaju nepredviđenih okolnosti za ublažavanje "napada" na usluge, ili ostalih događaja koji bi mogli izazvati poremećaje u poslovanju. Izazov održavanja kontinuiteta raspoloživosti sistema i aplikacija e-bankarstva može biti značajan, posebno u poslovno najaktivnijim periodima. Velika očekivanja klijenata što se tiče kratkog vremena ciklusa obrade transakcija i stalne raspoloživosti (24 sata na dan, 7 dana u nedelji) takođe impliciraju važnost planiranja za slučaj nepredviđenih okolnosti. Kako bi klijentima omogućile kontinuitet usluga e-bankarstva, banke treba da osiguraju:

- Da se trenutni kapacitet sistema e-bankarstva i budući razvoj analiziraju u svetlu sveukupne tržišne dinamike za e-trgovinu i predviđene stope prihvatanja proizvoda i usluga e-bankarstva od strane klijenata;
- Da se uvedu procene kapaciteta obrade transakcija u e-bankarstvu i da se sprovede testiranje na stres;
- Da postoje odgovarajući planovi za obezbeđenje kontinuiteta poslovanja za slučaj nepredviđenih okolnosti za ključne sisteme obrade i distribucije, kao i da se oni redovno testiraju.

14. načelo: Banke bi trebalo da izrade odgovarajuće planove za incidentne slučajeve, kako bi upravljale, rešile ili minimizirale probleme koji nastaju zbog neočekivanih događaja, uključujući interne i eksterne prodore u sistem koji mogu sprečiti pružanje usluga e-bankarstva.

Delotvorni mehanizmi za incidentne slučajeve važni su za minimiziranje operativnog, pravnog i reputacionog rizika koji se javlja zbog neočekivanih događaja, kao što su interni ili eksterni prodori u sistem. Banke bi trebalo da izrade odgovarajuće planove za incidentne slučajeve, uključujući komunikacionu strategiju, kako bi omogućile poslovni kontinuitet, kontrolu reputacionog rizika, i ograničile odgovornost

vezanu za poremećaje u uslugama e-bankarstva, kao i one koji nastaju na osnovu eksternalizacije sistema ili poslova.

Da bi obezbedile efikasno delovanje u slučaju nepredviđenih incidenata, banke moraju da izrade:

- Planove za incidentne slučajeve, – kako bi bio omogućen oporavak sistema i usluga e-bankarstva u okviru različitih scenarija, poslovnih i geografskih lokacija. (Analiza scenarija trebalo bi da obuhvati razmatranje verovatnoće pojave rizika i njegovog uticaja na banku. Sistemi e-bankarstva koji su povereni trećim stranama trebali bi biti sastavni deo tih planova);
- Mehanizme za utvrđivanje incidentnog slučaja ili krize čim se ona pojavi, procenu njihove veličine i kontrolu reputacionog rizika povezanog sa bilo kakvim poremećajem u pružanju usluga;
- Komunikacionu strategiju za adekvatno rešavanje pitanja vezanih za spoljno tržište, a koja se mogu pojaviti u slučaju narušavanja sigurnosti, direktnih prodora u sistem ili pada sistema e-bankarstva;
- Jasan proces za uzbunjivanje odgovarajućih regulatornih tela u slučaju da dođe do značajnog narušavanja sigurnosti ili poremećaja;
- Timove za incidentne slučajeve, ovlašćene da deluju u hitnim slučajevima i dovoljno kvalifikovane za analizu sistema otkrivanja incidenta (delovanja u slučaju incidenta), te tumačenje važnosti odnosnog autputa;
- Jasan zapovedni lanac, koji obuhvata interne i eksternalizovane poslove kako bi se osiguralo preduzimanje odgovarajućih hitnih mera u skladu sa važnošću incidentnog slučaja. Osim toga, potrebno je razviti i intenzivirati procedure interne komunikacije i uključiti izveštavanje odbora, kada je to potrebno.
- Proces koji osigurava da sve relevantne eksterne strane – uključujući klijente banke, druge ugovorne strane i mediji, budu pravovremeno i na odgovarajući način informisani o značajnim poremećajima u e-bankarstvu i nastavku poslovanja.
- Proces za prikupljanje i čuvanje forenzičnih dokaza koji olakšavaju odgovarajuća naknadna preispitivanja svih incidentnih slučajeva u e-bankarstvu i pomažu u krivičnom gonjenju počinilaca.

Praćenje službe za pomoć i poslove podrške klijentima, i redovno preispitivanje pritužbi klijenata može pomoći u utvrđivanju nesklada između informacija koje su otkrivene i prijavljene putem uspostavljenih kontrola, u odnosu na stvarne aktivnosti ometanja.

ZAKLJUČAK

Očekivanje *Bazelskog komiteta* je da nadležna nacionalna nadzorna tela upotrebljavaju načela kao osnovu, koju će prilagoditi nacionalnim zahtevima, a sa ciljem da se promoviše sigurno i zdravo poslovanje u e-bankarstvu. Profil rizika svake banke je drugačiji i zahteva pristup upravljanju rizikom koji je prilagođen obimu njenih poslova e-bankarstva, važnosti prisutnih rizika, te spremnosti i sposobnosti institucije za upravljanje tim rizicima. Te razlike potvrđuju potrebu da načela upravljanja rizicima budu dovoljno fleksibilna. Preporuke, takođe, ne definišu posebna tehnička rešenja za eliminisanje pojedinih rizika, niti tehničke standarde za e-bankarstvo. Finansijske institucije u saradnji sa raznim telima za standardizaciju kontinuirano daju rešenja koja prate razvoj tehnologije. Svaka banka treba da razvije postupke upravljanja rizikom koji su prilagođeni njenom pojedinačnom profilu rizika, operativnoj strukturi i kulturi korporativnog upravljanja i koji su u skladu sa zahtevima i politikama upravljanja rizikom koje utvrdi supervizija banaka.

LITERATURA

1. *Živković, A., Stankić, R., Krstić B.: "Bankarsko poslovanje i platni promet", Ekonomski fakultet, Beograd, 2009.*
2. *Basel Committee on Banking Supervision, "Risk Management Principles for Electronic Banking", July 2003, http://www.bis.org/publ/bcbs98.htm*
3. *www.bis.org*
4. *www.ecb.int*