Na osnovu člana 5. stav (1) tačka h) i člana 19. stav (1) tačka c) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", broj: 75/17) i čl. 81. i 248. Zakona o bankama ("Službene novine Federacije BiH", broj: 27/17), Upravni odbor Agencije za bankarstvo Federacije Bosne i Hercegovine, na sjednici održanoj 13.10.2017. godine donosi

O D L U K U
O UPRAVLJANJU INFORMACIONIM SISTEMOM U BANCI

Član 1.
Opće odredbe

Odlukom o upravljanju informacionim sistemom u banci utvrđuju se zahtjevi i kriteriji koje je banka dužna da osigura i provodi u procesu upravljanja informacionim sistemom i rizicima koji proističu iz korištenja informacionih sistema.

Član 2.
Definicije

Definicije koje se koriste u ovoj odluci imaju sljedeća značenja:

a) **Informacioni sistem** – sveobuhvatan skup resursa organizovan u svrhu prikupljanja, spremanja, obrade, održavanja, korištenja, distribucije i raspolaganja informacijama.
b) **Povjerljivost** – osobina da informacija nije dostupna ili otkrivena neovlaštenim licima ili procesima.
c) **Integritet** – osobina informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.
d) **Dostupnost** – osobina da informacija bude pravovremeno dostupna i iskoristiva na zahtjev od strane ovlaštenog lica.
e) **Kontrole** – politike, procedure, prakse, tehnologije i organizacione strukture dizajnirane kako bi obezbijedile razumno uvjerenje da će poslovni ciljevi biti dostignuti i da će neželjeni događaji biti spriječeni ili detektovani. Kontrole se dijele na upravljačke, logičke i fizičke. Upravljačke kontrole uključuju donošenje internih akata vezanih uz informacioni sistem i uspostavljanje odgovarajuće organizacijske strukture, te obezbjeđuju primjenu internih akata vezanih uz informacioni sistem u cilju obezbjeđivanja funkcionalnosti i sigurnosti informacionog sistema. Logičke kontrole su kontrole implementirane na software-skim komponentama. Fizičke kontrole su kontrole koje štite resurse informacionog sistema od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja.
f) **Resursi informacionog sistema** – resursi koji uključuju informacionu imovinu, software-ske i hardware-ske komponente, ljude i procese.
g) **Analiza isplativosti** (eng. cost-benefit analiza) – metoda ekonomske analize kojom se upoređuju i vrednuju sve prednosti i svi nedostaci projekta analizom troškova i koristi.
h) **Sigurnost informacija** – osigurava da samo ovlašteni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).
i) **Princip višeslojne zaštite** – princip implementacije više slojeva sigurnosnih zaštita, gdje neefikasnost jednog sloja zaštite nadoknađuje sljedeći sloj zaštite.
j) **Penetracioni test –** proces koji upotrebom automatizovanih alata otkriva prisutne ranjivosti u informacionom sistemu i iskorištava ih sa ciljem otkrivanja mogućnosti vršenja neautorizovanog pristupa ili druge maliciozne aktivnosti, te dalje, identifikuje i utvrđuje nivoe uočenih rizika otkrivenih ranjivosti.

k) **Test ranjivosti** – proces koji upotrebom automatizovanih alata otkriva prisutne ranjivosti u informacionom sistemu, ali ih ne iskorištava.
l) **Korisnici informacionog sistema** – sva lica koja koriste informacioni sistem (uposlenici banke, uposlenici pružaoca usluga, korisnici elektronskog bankarstva, uposlenici pravnih lica koji koriste informacioni sistem banke i drugo).
m) **Rizik informacionog sistema** – rizik koji proizilazi iz korištenja informacione tehnologije odnosno informacionog sistema.
n) **Elektronsko bankarstvo** – sistem koji omogućava klijentima banke obavljanje bankarskih poslova sa udaljene lokacije putem javnih komunikacionih mreža ili slično.
o) **Rizik povezan sa integritetom podataka** – rizik da su podaci koji su skladišteni i procesirani u informacionom sistemu nepotpuni, netačni ili nekonzistentni kroz sistem odnosno različite sisteme.
p) **Evidentiranje korisničkih prava pristupa** – proces dodjele prava pristupa korisnicima informacionog sistema.
q) **Identifikacija i autentifikacija** – procesi identifikacije korisnika informacionog sistema i potvrde njegova identiteta prilikom prijave i tokom provođenja radnji na informacionom sistemu.
r) **Autorizacija** – proces kojim se provjerava ima li klijent pravo izvršiti određenu radnju.
s) **Autentifikacija** – proces potvrde identiteta korisnika/procesa od strane sistema.
t) **Nadzor korisničkih prava pristupa –** proces koji uključuje praćenje, izmjenu i reviziju prava pristupa korisnika informacionog sistema.
u) **Povlašteni pristup** – pristup resursima informacionog sistema koji omogućava korisnicima znatno veća prava, te zaobilaženje ugrađenih logičkih kontrola (na primjer, administrator mrežne opreme, baze podataka, sistemskog software-a, aplikativnog software-a i slično).
v) **Udaljeni pristup** – omogućava pristup resursima informacionog sistema sa udaljene lokacije putem telekomunikacionih linija nad kojima banka nema potpunu kontrolu odnosno nadzor.
w) **Software-ske komponente (software-ska imovina)** – uključuju aplikacijski software, sistemski software, baze podataka, software-ske razvojne alate, uslužne programe, te ostali software.
x) **Operativni i sistemski zapisi** – hronološki zapisi o aktivnostima na resursima informacionog sistema (zapisi operativnih sistema, aplikacijskog software-a, baza podataka, mrežnih uređaja i slično).
y) **Maliciozni kod** – bilo koji oblik programskog koda stvoren s namjerom da se neovlašteno ostvari pristup resursima informacionog sistema, prikupe ili unište informacije, izazove neočekivano ponašanje ili prekid u funkcionisanju ovog sistema bez znanja i odobrenja vlasnika, odnosno da se na drugi način naruši povjerljivost, integritet ili raspoloživost tih resursa (na primjer, računarski virusi, crvi, trojanski konji i drugo).
z) **Hardware-ske komponente (hardware-ska imovina)** – fizičke komponente informacionog sistema koje uključuju: računare i računarsku opremu, komunikacijsku opremu, medije za čuvanje podataka, te ostalu tehničku opremu koja podržava rad informacionog sistema.
aa) **Informaciona imovina** – sva materijalna ili nematerijalna imovina koja za banku ima neku vrijednost (serveri, mrežne komponente, podaci u bazama podataka, datoteke sa podacima, programski kod, sistemska i aplikacijska dokumentacija, korisnička dokumentacija, planovi, interni akti i slično).
bb) **Kritični/vitalni procesi** – poslovne aktivnosti ili procesi koji ne mogu biti prekinuti ili nedostupni, a da značajno ne ugroze poslovanje banke.
cc) **Vlasnik** – lica i/ili organizacioni dio kojem je odobrena upravljačka odgovornost za produkciju, razvoj, održavanje, korištenje i zaštitu imovine.

dd) **Skrbnik** – lica i/ili organizacioni dio, koji logički ili fizički raspolaže resursima, a koji za potrebe i interes vlasnika obavlja operativne poslove i implementaciju odgovarajućih kontrola, koji su mu dodijeljeni, u skladu sa važećim politikama, procedurama i uputstvima.

ee) **Razvoj** – zahtjev za razvojem novih funkcionalnosti informacionog sistema.

ff) **Promjena** – zahtjev za izmjenom podataka ili izmjenama nad postojećim funkcionalnostima informacionog sistema.

gg) **Korisnički zahtjev** – zahtjev od strane korisnika informacionog sistema za pristup određenim resursima informacionog sistema ili IT uslugama, zahtjev za informacijama ili savjetom, te ostale vrste zahtjeva koji ne spadaju u kategoriju incidenata ili promjena unutar informacionog sistema.

hh) **Incident** – svaki neplanirani i neželjeni događaj koji može narušiti sigurnost i funkcionalnost resursa informacionog sistema koji podržavaju odvijanje poslovnih procesa banke.

ii) **Korisnički identitet** – identitet koji je moguće potvrditi korištenjem jednog ili kombinacijom sljedećih načina:
   1) pomoću nečega što samo korisnik zna (na primjer lozinka, PIN, kriptografski ključ),
   2) pomoću nečega što samo korisnik posjeduje (na primjer magnetna kartica, čip kartica, token) i
   3) pomoću nečega što korisnik jeste (korištenjem biometrijskih metoda, kao što su provjera otiska prsta ili karakteristika šarenice oka, prepoznavanje glasa, rukopisa i slično).

jj) **Kopije** – kopija izvornih podataka (informaciona imovina, software-ske komponente) koji su potrebni za ponovno uspostavljanje poslovnih procesa banke, te ostalih podataka za koje banka procjeni da ih je potrebno čuvati.

kk) **Teži incident** – incident koji ima ili može imati značajan uticaj na kontinuitet poslovanja banke i/ili na sigurnost osjetljivih podataka i/ili materijalno značajan uticaj na veliki broj korisnika usluga.

ll) **Raspoloživost** – svojstvo imovine da je pravovremeno dostupna i upotrebljiva na zahtjev ovlaštenog lica.

mm) **Informaciona tehnologija** – hardware, software, komunikacije i drugi uređaji koji se koriste za unos, spremanje, procesiranje (obradu), prijenos i izlaz podataka, u bilo kojem obliku.

nn) **Autentičnost** – osobina koja obezbjeđuje da je identitet lica zaista onaj za koji se tvrdi da jeste.

oo) **Neporecivost** – osobina koja osigurava nemogućnost poricanja izvršene aktivnosti ili primanja informacija (podataka).

pp) **Dokazivost** – osobina koja obezbjeđuje da svaka aktivnost u informacionom sistemu može jednoznačno biti praćena do njenog izvora.

qq) **Pouzdanost** – označava da informacioni sistem dosljedno i očekivano vrši predviđene funkcije i pruža tačne informacije.

rr) **Analiza uticaja na poslovanje** – analiza pomoću koje se ocjenjuju kvantitativni i kvalitativni efekti koji bi mogli nastati u slučaju nedostupnosti poslovnih procesa i resursa informacionog sistema uslijed određenog incidenta, neželjenog događaja ili havarije. Cilj analize uticaja na poslovanje je identifikacija ključnih poslovnih procesa i resursa informacionog sistema kao dijela procesa upravljanja kontinuitetom poslovanja.

ss) **Recovery time objective (RTO) –** najduže prihvatljivo vrijeme neraspoloživosti poslovnog procesa banke i resursa informacionog sistema potrebnih za odvijanje poslovnog procesa, odnosno vrijeme tokom koga je potrebno obnoviti poslovni proces.

tt) **Recovery point objective (RPO) –** određuje se na osnovu prihvatljivog gubitka podataka u slučaju prekida operacija; naznačava najraniju tačku u vremenu koja je prihvatljiva za

oporavak podataka; RPO efikasno kvantificira dozvoljenu količinu gubitka podataka u slučaju prekida.

uu) **Service delivery objective (SDO) –** nivo usluga koje treba postići tokom alternativnog načina procesiranja dok se ne izvrši povratak na normalan rad.

Član 3.

Okvir za upravljanje informacionim sistemom

(1) Banka je dužna uspostaviti, implementirati, nadzirati, održavati, redovno revidirati i poboljšavati proces upravljanja informacionim sistemom u cilju smanjenja izloženosti rizicima, osiguranja povjerljivosti, integriteta i dostupnosti informacija i cjelokupnog informacionog sistema, primjereno veličini, složenosti i obimu poslovanja banke, te kompleksnosti informacionog sistema.

(2) Banka je dužna uspostaviti adekvatan sistem koji uključuje identifikaciju, mjerenje, praćenje i kontrolu upravljanja rizicima koji proističu iz korištenja informacionog sistema.

Član 4.

Nadzorni odbor

Nadzorni odbor banke je dužan i odgovoran, kao minimum, da:

a) na osnovu prijedloga uprave, donosi strategiju informacionog sistema, koja treba biti sastavni dio ukupne poslovne strategije banke,
b) na osnovu prijedloga uprave, donosi politike za upravljanje informacionim sistemom, a posebno politiku sigurnosti informacionog sistema i nadzire njihovu implementaciju,
c) aktuelizira usvojene politike u skladu sa promjenama ekonomskih, tržišnih, tehnoloških i drugih uslova, a najmanje jednom godišnje,
d) uspostavi sistem za mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim uz informacioni sistem, prati efikasnost i unapređuje dati sistem,
e) donese i osigura uspostavu adekvatne organizacione strukture i odgovarajućih funkcija i ovlasti kako bi osigurala efikasno i sigurno upravljanje informacionim sistemom, sa obavezom definiranja stručnih kvalifikacija i potrebnih kompetencija,
f) osigura selekciju i imenovanje kvalifikovanog i kompetentnog člana uprave koji će biti nadležan za uspostavu i nadzor procesa upravljanja informacionim sistemom,
g) na osnovu prijedloga uprave, propiše sadržaj i periodičnost izvještavanja nadzornog odbora banke o relevantnim činjenicama vezanim uz upravljanje informacionim sistemom, a najmanje jednom godišnje i
h) osigura uslove za uspostavu efikasnog sistema internih kontrola u segmentu upravljanja informacionim sistemom i vrši nadzor nad tim sistemom.

Član 5.

Uprava banke

(1) Uprava banke je dužna i odgovorna, kao minimum, da:

a) imenuje odbor za upravljanje informacionim sistemom, sastavljen od predstavnika različitih poslovnih funkcija, koji će se sastajati periodično i izvještavati upravu o svojim aktivnostima najmanje na kvartalnom nivou, a čija uloga treba biti koordinacija inicijativa i praćenje razvojnih aktivnosti informacionog sistema, kao i usklađenosti ciljeva informacionog sistema sa poslovnim ciljevima i poslovnom strategijom banke,
b) predlaže i implementira politike, te donosi i provodi procedure upravljanja informacionim sistemom u skladu sa poslovnim ciljevima i poslovnom strategijom banke,
c) implementira sistem za identifikaciju, mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim za informacioni sistem,
d) osigura da su sve dužnosti vezane uz upravljanje informacionim sistemom jasno definirane i dodijeljene, vodeći računa o adekvatnoj segregaciji dužnosti,

e) donosi plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema,
f) osigura potrebne resurse za upravljanje informacionim sistemom i
g) usvoji i primjeni metodologiju upravljanja projektima kojom će se definirati kriteriji, načini i postupci upravljanja projektima vezanim uz informacioni sistem.

(2) Uprava banke je dužna pravovremeno obavijestiti Agenciju za bankarstvo Federacije Bosne i Hercegovine (u daljem tekstu: Agencija) o svakoj značajnoj i kompleksnoj promjeni koja može imati uticaja na informacioni sistem banke, te dostaviti odgovarajuću dokumentaciju (na primjer, projektni plan, projektne timove, planirani budžet, analizu isplativosti projekta, procjenu rizika projekta i slično).

Član 6.

Strategija informacionog sistema

(1) Banka je dužna razviti i nadzirati implementaciju strategije informacionog sistema koja, kao minimum, treba da:
a) obuhvati dugoročne i kratkoročne inicijative vezane za informacioni sistem,
b) definira povezanost i usklađenost ciljeva informacionog sistema sa poslovnim ciljevima banke,
c) se periodično ažurira, a posebno prilikom izmjene poslovne strategije, kako bi se osigurala kontinuirana usklađenost između poslovnih ciljeva i ciljeva informacionog sistema, te odgovarajućih planova i aktivnosti i
d) se detaljnije razradi kroz donošenje operativnih planova.

(2) Uprava banke je dužna usvojiti operativni plan informacionog sistema na godišnjem nivou, a koji proizlazi iz strategije informacionog sistema.

(3) Operativni plan informacionog sistema treba, kao minimum, sadržavati sljedeće elemente: opis aktivnosti i projekata informacionog sistema, ljudske resurse, budžet, vremenske rokove i odgovorna lica.

(4) Banka je dužna osigurati da je identifikacija, procjena i smanjenje rizika povezanih sa implementacijom strategije informacionog sistema, kao i efikasna uspostava okvira za upravljanje informacionim sistemom, pod kontinuiranim nadzorom kontrolnih funkcija banke.

Član 7.

Politika sigurnosti informacionog sistema

(1) Banka je dužna usvojiti i implementirati politiku sigurnosti informacionog sistema, koja predstavlja osnov za upravljanje sigurnošću informacionog sistema banke, i koja kao minimum treba da:
a) sadrži načela i principe upravljanja sigurnošću resursa informacionog sistema i, gdje god je moguće, pridržavati se međunarodno priznatih sigurnosnih standarda i principa (poput principa najmanjih privilegija, princip višeslojne zaštite i slično),
b) definira odgovornosti koje se odnose na područje upravljanja sigurnošću informacionog sistema, uključujući odgovornost za dizajn, implementaciju i nadzor nad kontrolama sigurnosti,
c) obuhvati područja upravljačke, logičke i fizičke zaštite resursa informacionog sistema, u skladu sa veličinom i kompleksnošću informacionog sistema,
d) definira mjere u slučaju odgovornosti korisnika informacionog sistema za narušavanje sigurnosti informacionog sistema i
e) obuhvati kontrole koje su identifikovane procjenom i analizom rizika informacionog sistema banke.

(2) Politika sigurnosti informacionog sistema treba da bude usklađena sa promjenama u okruženju i informacionom sistemu banke.

(3) Banka je dužna da proces upravljanja sigurnošću informacionog sistema uspostavi kao kontinuirani proces identifikovanja potreba za ovom sigurnošću i postizanja i održavanja adekvatnog nivoa te sigurnosti, na osnovu rezultata procjene rizika i obaveza koje proizlaze iz propisa, ugovornih odnosa i slično.

Član 8.

Banka je dužna, na godišnjem nivou, pregledati i testirati sigurnosne mjere i kontrole informacionog sistema banke (na primjer, test ranjivosti, penetracioni test i slično), utvrditi obim testiranja u skladu sa procjenom rizika, te izvještavati upravu i nadzorni odbor o rezultatima testiranja.

Član 9.

Interni akti

(1) Banka je dužna propisati i primijeniti detaljne procedure kojima se uređuje upravljanje informacionim sistemom, te osigurati provođenje tih procedura.
(2) Interni akti trebaju, kao minimum, biti:
   a) usklađeni sa propisima, standardima i pravilima struke,
   b) redovno pregledani i ažurirani i
   c) potpuni, detaljni i primjenjivi.
(3) Potrebno je osigurati da su svi korisnici informacionog sistema upoznati sa sadržajem internih akata, vezanih uz informacioni sistem, u skladu sa potrebama svakog korisnika.
(4) Ugovori, nalazi revizije, uputstva i ostali dokumenti trebaju biti sačinjeni odnosno prevedeni na jedan od jezika u zvaničnoj upotrebi u Federaciji Bosne i Hercegovine.

Član 10.

Upravljanje rizicima iz ugovornih odnosa

Banka je dužna kontinuirano procjenjivati i adekvatno upravljati rizicima koji proizlaze iz ugovornih odnosa sa pravnim i fizičkim licima, a čije su aktivnosti vezane uz informacioni sistem banke.

Član 11.

Upravljanje rizicima informacionog sistema

(1) Banka je dužna uspostaviti proces upravljanja rizicima informacionog sistema koji treba biti sastavni dio sistema upravljanja rizicima na nivou banke, u skladu sa propisima Agencije koji regulišu oblast upravljanja rizicima u bankama.
(2) Uprava banke je dužna usvojiti metodologiju kojom će se definirati kriteriji, načini i postupci upravljanja rizicima koji proizlaze iz upotrebe informacionog sistema, te odrediti odgovornosti upravljanja rizicima i prihvatljive nivoe rizika za identifikovane značajne rizike informacionog sistema.
(3) U okviru upravljanja rizicima informacionog sistema, banka je dužna, kao minimum:
   a) identifikovati ključne dijelove i servise informacionog sistema,
   b) procijeniti prijetnje, ranjivosti, posljedice i implementirane kontrole identifikovanih ključnih dijelova i servisa informacionog sistema,
   c) preporučiti mjere za tretiranje rizika, donijeti plan tretmana rizika i kontinuirano pratiti realizaciju ovog plana,
   d) redovno, a najmanje jednom godišnje izvještavati upravu i nadzorni odbor banke o rezultatima procjene rizika.
(4) Upravljanje rizicima informacionog sistema treba da obuhvati informacioni sistem banke u potpunosti sa posebnom pažnjom na sljedeće:

a) dijelove informacionog sistema i servise koji podržavaju ključne poslovne operacije i distribucijske kanale (na primjer, bankomati, elektronsko bankarstvo, kartično poslovanje i slično),
b) dijelove informacionog sistema i servise koji podržavaju osnovne procese upravljanja i korporativne funkcije, uključujući upravljanje rizicima,
c) dijelove informacionog sistema i servise koji potpadaju pod specijalne pravne ili regulatorne zahtjeve, a koji nameću pojačane/povećane zahtjeve za dostupnost, fleksibilnost, povjerljivost i sigurnost,
d) dijelove informacionog sistema i servise koji procesiraju ili skladište povjerljive ili osjetljive podatke, pri čemu neovlašten pristup tim podacima može značajno utjecati na reputaciju banke, finansijske rezultate ili stabilnost, te kontinuitet njenog poslovanja,
e) dijelove informacionog sistema i servise koji osiguravaju osnovne funkcionalnosti vitalne za adekvatno funkcionisanje banke i
f) dijelove informacionog sistema i servise koji su procijenjeni kao materijalno značajne eksternalizovane aktivnosti.

(5) Svi navedeni ključni dijelovi informacionog sistema i servisi trebaju biti ocijenjeni sa stanovišta utjecaja i izloženosti riziku dostupnosti i kontinuiteta poslovanja, riziku sigurnosti informacionog sistema, riziku promjena u informacionom sistemu, riziku povezanom sa integritetom podataka i riziku eksternalizacije.

(6) Banka je dužna osigurati da je identifikacija, procjena i smanjenje rizika povezanih sa informacionim sistemom, kao i efikasna uspostava okvira za upravljanje rizicima informacionog sistema, pod kontinuiranom nadzorom interne i eksterne revizije.

Član 12.

Odgovorno lice za sigurnost informacionog sistema

(1) Uprava banke dužna je imenovati odgovorno lice (voditelj/oficir) za funkciju sigurnosti informacionog sistema, te definirati njegova ovlaštenja, odgovornosti i obim rada. Funkcija sigurnosti informacionog sistema treba biti nezavisna od funkcije organizacione jedinice za upravljanje informacionim sistemom. Lice odgovorno za sigurnost informacionog sistema treba biti kompetentno lice sa odgovarajućim stručnim kvalifikacijama, specijalističkim znanjima i iskustvom.

(2) Lice odgovorno za funkciju sigurnosti informacionog sistema treba, kao minimum, da nadzire i koordinira aktivnosti vezane uz sigurnost informacionog sistema, te da redovno izvještava upravu banke o stanju i aktivnostima vezanim uz sigurnost informacionog sistema, a minimalno na kvartalnom nivou.

Član 13.

Interna revizija

(1) Banka je dužna provoditi internu reviziju informacionog sistema u skladu sa propisima Agencije koji regulišu oblast interne revizije banke, a na osnovu definiranog programa rada interne revizije.

(2) Banka je dužna planirati i provoditi internu reviziju informacionog sistema u skladu sa metodologijom procjene rizika, imajući u vidu da u određenim vremenskim intervalima budu redovno pregledane (obuhvaćene) sve kritične i ključne funkcije informacionog sistema banke.

(3) Banka je dužna osigurati da se interna revizija informacionog sistema provodi na kontinuiranoj osnovi tokom cijele godine.

(4) Lica koja obavljaju internu reviziju informacionog sistema banke trebaju posjedovati stručna znanja i vještine o informacionim sistemima.

(5) U slučaju eksternalizacije aktivnosti interne revizije informacionog sistema, banka treba osigurati da pružalac usluga interne revizije informacionog sistema istovremeno (u toj godini)

ne pruža usluge eksterne revizije informacionog sistema banci, te treba osigurati da ne postoji sukob interesa u skladu sa profesijom interne revizije.

(6) U slučaju eksternalizacije aktivnosti interne revizije informacionog sistema, banka treba osigurati da pružalac usluga posjeduje međunarodno priznate certifikate za reviziju informacionog sistema.

Član 14.

Eksterna revizija

(1) Agencija daje prethodnu saglasnost za imenovanje društva za reviziju za obavljanje revizije informacionog sistema.

(2) Banka je dužna Agenciji podnijeti zahtjev za izdavanje odobrenja za imenovanje društva za reviziju informacionog sistema.

(3) Banka je dužna, uz zahtjev iz stava (2) ovog člana, dostaviti Agenciji sljedeće dokumente:
   a) nacrt odluke o imenovanju društva za reviziju informacionog sistema,
   b) nacrt ugovora ili pisma namjere sa društvom za reviziju informacionog sistema,
   c) reference društva za reviziju informacionog sistema o obavljenim revizijama informacionih sistema,
   d) dokaze o stručnim kvalifikacijama lica koja će obavljati reviziju i njihove biografije i
   e) izjavu o nepostojanju sukoba interesa između društva za reviziju (odnosno lica koja operativno provode reviziju) i banke.

(4) Skupština banke, uz prethodnu saglasnost Agencije, imenuje društvo za reviziju najkasnije do 30. septembra tekuće godine, koje će obaviti reviziju informacionog sistema za tu godinu.

(5) Odluku o imenovanju društva za reviziju banka je dužna dostaviti Agenciji u roku od osam dana od dana donošenja odluke.

(6) Ugovor o obavljanju revizije informacionog sistema mora biti zaključen između banke i društva za reviziju u pisanoj formi, koji je banka dužna dostaviti Agenciji u roku od osam dana od dana potpisivanja ugovora.

(7) Prilikom obavljanja eksterne revizije informacionog sistema, društvo za reviziju je dužno uzeti u obzir eksternalizovane usluge i njihovu značajnost i utjecaj na informacioni sistem, te u skladu s tim razviti plan revizije i efikasni pristup reviziji.

(8) Društvo za reviziju je dužno sačiniti revizorski izvještaj o obavljenoj reviziji informacionog sistema, te dati ocjenu o stanju informacionog sistema i adekvatnosti upravljanja informacionim sistemom.

(9) Izvještaj o obavljenoj reviziji informacionog sistema je poseban izvještaj, te je banka dužna dostaviti Agenciji navedeni izvještaj najkasnije do 31.05. tekuće godine.

(10) Banka je dužna da reviziju informacionog sistema obavlja na godišnjem nivou.

(11) Agencija zadržava pravo nalaganja mjera propisanih Zakonom o bankama i propisima Agencije koji regulišu eksternu reviziju u bankama.

Član 15.

Upravljanje kontrolama pristupa

Banka je dužna da uspostavi adekvatan sistem upravljanja pristupom resursima informacionog sistema koji, kao minimum, treba da obuhvati:

a) definiranje odgovarajućih upravljačkih, logičkih i fizičkih kontrola,
b) definiranje politika lozinki računa za pristup resursima informacionog sistema u skladu sa dobrim praksama,
c) upravljanje korisničkim pravima pristupa koji obuhvata procese evidentiranja, identifikacije, autorizacije i autentifikacije, te nadzora prava pristupa,
d) upravljanje povlaštenim i udaljenim pristupom,
e) upravljanje generičkim i servisnim računima i
f) reviziju prava pristupa resursima informacionog sistema, a najmanje jednom godišnje.

Član 16.

Cyber sigurnost

Banka je dužna uspostaviti mjere zaštite informacionog sistema od napada putem internetske mreže ili drugih eksternih mreža (na primjer, tradicionalne telekom konekcije ili konekcije sa povjerljivim partnerima), koje trebaju, kao minimum, da uključe sljedeće:

a) proces ili rješenja za održavanje kompletnog i ažurnog registra i pregled svih vanjskih mrežnih tačaka konekcije (na primjer, web stranice, internet aplikacije, wi-fi, udaljeni pristup i slično) kroz koje treća lica mogu upasti u interni informacioni sistem banke,
b) upravljanje i nadzor nad sigurnosnim mjerama (na primjer, firewall, proxy serveri, antivirus, skeniranje sadržaja i slično) uspostavljenim u cilju zaštite dolaznog i odlaznog mrežnog saobraćaja i vanjskih mrežnih konekcija kroz koje treća lica mogu upasti u interni informacioni sistem banke,
c) procese i rješenja za zaštitu web stranica i aplikacija koje mogu biti direktno napadnute sa interneta i/ili izvana, a koje mogu služiti kao ulazna tačka u interni informacioni sistem banke (na primjer, princip osnaživanja sistema – hardening, IPS/IDS sistemi i slično),
d) segmentiranje mreže, redovno praćenje mrežnog prometa i analize zapisa, kao i provjere integriteta softvera i
e) periodično sigurnosno penetraciono testiranje kako bi se procijenila efikasnost implementiranih cyber i internih sigurnosnih mjera i procesa.

Član 17.

Operativni i sistemski zapisi

(1) Banka je dužna da, u skladu sa procjenom rizika, osigura izradu, redovno praćenje i čuvanje operativnih i sistemskih zapisa u svrhu pravovremenog otkrivanja neovlaštenih pristupa i radnji u informacionom sistemu, identifikovanja problema, rekonstruiranja događaja, te utvrđivanja odgovornosti.
(2) Banka je dužna definirati resurse informacionog sistema i vrste operativnih i sistemskih zapisa koji se prate, njihov sadržaj, vrste i frekvenciju analize i nadzora operativnih i sistemskih zapisa, period čuvanja zapisa, te odgovorna lica.
(3) Banka je dužna da uspostavi adekvatnu zaštitu zapisa, osigura njihov integritet i povjerljivost u skladu sa klasifikacijom informacija, te razdvoji dužnosti lica koja administriraju resurse informacionog sistema sa kojih se zapisi prikupljaju od lica koja administriraju zapise.

Član 18.

Maliciozni kod

Banka je dužna da uspostavi proces za upravljanje zaštitom od malicioznog koda koji treba da, kao minimum, obuhvati sljedeće:

a) jasne uloge i odgovornosti lica nadležnih za upravljanje zaštitom od malicioznog koda,
b) kontrole prevencije, detekcije i oporavka informacionog sistema (sprječavanje izvršavanja malicioznog programskog koda, kontinuirano ažuriranje softvera za otkrivanje malicioznog koda, upravljanje ranjivostima i provjerama informacionog sistema i slično), sa ciljem zaštite resursa od malicioznog programskog koda,
c) definira postupke u slučaju otkrivanja malicioznog programskog koda i
d) podizanje svijesti korisnika informacionog sistema o rizicima od posljedica djelovanja malicioznog programskog koda kroz redovne programe edukacije.

Član 19.

Aplikativne kontrole

Banka je dužna da osigura da aplikativni softver ima ugrađene kontrole ispravnosti, potpunosti i konzistentnosti podataka koji se unose, mijenjaju, obrađuju i generišu.

Član 20.

Upravljanje resursima

(1) Banka je dužna da uspostavi proces upravljanja hardverskom i softverskom imovinom, koja je neophodna za obavljanje kritičnih (vitalnih) procesa, tokom cijelog životnog ciklusa, od nabavke ili razvoja do povlačenja iz upotrebe.
(2) Proces upravljanja hardverskom i softverskom imovinom treba da obuhvata postupke identifikacije, evidentiranja, određivanja vlasnika i skrbnika, načina raspolaganja, utvrđivanje pravila njihovog prihvatljivog korištenja, praćenja, obnavljanja i odlaganja te imovine.
(3) Banka je dužna da osigura adekvatno održavanje hardverske i softverske imovine informacionog sistema prema preporukama proizvođača, te da čuva zapise o tom održavanju.
(4) Banka je dužna da klasifikuje i zaštiti informacije, te definira način upravljanja istim prema njihovoj vrijednosti, pravnim zahtjevima, osjetljivosti i kritičnosti za banku.

Član 21.

Upravljanje razvojem

(1) Banka je dužna da definira i implementira procedure koje propisuju upravljanje razvojem informacionog sistema, vodeći računa o funkcionalnim i sigurnosnim aspektima, a koje uključuju, kao minimum:
   a) način iniciranja i odobravanja zahtjeva za razvojem (na primjer, nova funkcionalnost, modul, aplikacija i slično),
   b) planiranje, analizu i formalnu organizaciju,
   c) postupke komunikacije i izvještavanja,
   d) proces razvoja, adekvatnog testiranja i edukacije osoblja,
   e) uvođenje u produkcioni rad, vodeći računa o adekvatnoj segregaciji dužnosti,
   f) dokumentovanje procesa razvoja i isporuke informacionog sistema i
   g) plana povratka na 'staro' stanje,
(2) Banka je dužna osigurati adekvatno razdvajanje razvojnog, testnog i produkcionog okruženja.
(3) Banka je dužna osigurati odgovarajuću analizu i testiranje sigurnosti i ranjivosti sistema prije implementacije u produkciono okruženje, te osigurati da promjene komponenata informacionog sistema ne narušavaju sigurnost i funkcionalnost informacionog sistema.

Član 22.

Upravljanje promjenama

(1) Banka je dužna uspostaviti procedure procesa upravljanja promjenama u informacionom sistemu, kako bi se izbjeglo da one dovedu do neočekivanog i neželjenog ponašanja ovog sistema, odnosno naruše njegovu sigurnost ili funkcionalnost, a koji treba da uključe, kao minimum, sljedeće:
   a) iniciranje, analizu i odobravanje zahtjeva za promjenama (na primjer, promjene u aplikacijama, konfiguracijama i slično), te način utvrđivanja prioriteta,
   b) testiranje, odobrenje i dokumentovanje, prije uvođenja u produkcioni rad,
   c) upravljanje 'hitnim' promjenama,
   d) implementaciju promjena, uključujući i plan povratka na 'staro' stanje,
   e) segregaciju dužnosti vezano za razvoj i implementaciju promjena i
   f) praćenje i izvještavanje.
(2) Banka je dužna osigurati testno okruženje koje adekvatno odražava produkciono okruženje, vodeći računa o povjerljivosti informacija.
(3) Banka je dužna utvrditi procedure za upravljanje sigurnosnim ispravkama (eng. patch) u okviru kojih će definirati na koji način se prate informacije o sigurnosnim ispravkama, najduži period u kojem se ove ispravke moraju primjeniti u zavisnosti od kritičnosti i procjene rizika za banku, te način primjene.

(4) Banka je dužna osigurati odgovarajuću analizu i testiranje sigurnosti i ranjivosti sistema prije implementacije značajnih promjena u produkciono okruženje, te osigurati da promjene komponenata informacionog sistema ne narušavaju sigurnost i funkcionalnost informacionog sistema.
(5) Banka je dužna da utvrdi početne verzije softverskih komponenata informacionog sistema, te evidentira i dokumentuje sve promjene komponenata informacionog sistema onim slijedom kako su nastajale, zajedno sa vremenom nastanka promjene.
(6) Procedure navedene u stavu (1) ovog člana se odnose na promjene osnovnih operativnih sistema, aplikativnog softvera, konfiguracionih datoteka, hardvera i ostalih dijelova informacionog sistema.

Član 23.
Dokumentacija

Banka je dužna da definira i implementira procedure upravljanja dokumentacijom (tehničkom, funkcionalnom, korisničkom i drugom) koja se odnosi na informacioni sistem, a koja, kao minimum, treba da uključi sljedeće:
a) osiguranje tačne, potpune i ažurne dokumentacije i
b) osiguranje pristupa zaposlenika dokumentaciji, u skladu sa njihovim poslovnim potrebama i klasifikaciji.

Član 24.
Upravljanje korisničkim zahtjevima

Banka je dužna da uspostavi proces upravljanja korisničkim zahtjevima koji, kao minimum, treba da obuhvati procedure za prijavljivanje, klasificiranje, određivanje prioriteta, obradu i izvještavanje o korisničkim zahtjevima.

Član 25.
Upravljanje incidentima

(1) Banka je dužna da uspostavi proces upravljanja incidentima, koji obuhvata, kao minimum, identifikaciju, klasifikaciju, eskalaciju, odgovor na incident, oporavak, analizu, te izvještavanje, a koji treba omogućiti brz, efektivan i propisan odgovor u slučaju narušavanja sigurnosti i funkcionalnosti informacionog sistema.
(2) Banka je dužna da, kao minimum, evidentira sljedeće vrste incidenata: prekidi u radu hardverskih i softverskih komponenti, smanjenje performansi servisa, neautorizovani pristup resursima informacionog sistema, odliv podataka, krađa identiteta, maliciozni kod, krađa, neuspješan proces izrade rezervne kopije podataka, narušavanje integriteta podataka i slično.
(3) Banka je dužna osigurati izvještavanje uprave o incidentima vezanim uz informacioni sistem na periodičnoj osnovi.
(4) Banka je dužna da odmah po saznanju o težem incidentu, kako u dijelu informacionog sistema koji se nalazi u banci, tako i u dijelu informacionog sistema koji je eksternalizovan (ključna bankarska aplikacija, sistem elektronskog bankarstva, sistem kartičnog poslovanja i drugo) obavijesti Agenciju, te nakon rješavanja incidenta dostavi kompletnu analizu incidenta zajedno sa posljedicama i poduzetim aktivnostima.

Član 26.
Kopije

(1) Banka je dužna uspostaviti proces upravljanja kopijama (eng. backup) koji uključuje procedure izrade, smještaja, testiranja kopija podataka, te restauracije podataka sa kopija podataka, kao i adekvatan transport i predaju kopija, kako bi se osigurala raspoloživost podataka u slučaju potrebe, te omogućio oporavak odnosno ponovna uspostava kritičnih (vitalnih) poslovnih procesa u zahtijevanom vremenu.

(2) U okviru procesa upravljanja kopijama, banka je dužna propisati za sve resurse informacionog sistema vrstu, način izrade, frekvenciju izrade, frekvenciju odlaganja na udaljenu lokaciju, te period čuvanja kopija.
(3) Kopije trebaju biti ažurne i čuvane na primjeren način, na jednoj ili više sekundarnih lokacija, od kojih najmanje jedna mora biti dovoljno udaljena od primarne lokacije na kojoj se nalaze izvorni podaci, a na osnovu urađene analize rizika.
(4) Banka je dužna osigurati rezervnu kopiju podataka na jednom od medija (na primjer, eksterni hard disk, trake i slično) na jednoj ili više sekundarnih lokacija, te adekvatno zaštititi rezervne kopije podataka prilikom prijenosa i voditi ažurnu evidenciju o istim.

Član 27.
Edukacija

(1) Banka je dužna da osigura stručno osposobljavanje i kontinuiranu edukaciju zaposlenika zaduženih za upravljanje informacionim sistemom, odgovornog lica za sigurnost informacionog sistema i internog revizora informacionog sistema, kao i primjerenu, pravovremenu i kontinuiranu edukaciju korisnika informacionog sistema.
(2) Banka je dužna da provodi programe podizanja svijesti korisnika informacionog sistema, vezane za sigurnost informacionog sistema u banci, vodeći računa o aktuelnim trendovima (na primjer, cyber prijetnje i slično).

Član 28.
Elektronsko bankarstvo

(1) Banka je dužna da uspostavi proces upravljanja rizikom elektronskog bankarstva, koji treba biti sastavni dio cjelokupnog upravljanja rizicima kojima je banka izložena, a u okviru kojeg je potrebno dokumentovati detaljne procjene rizika vezane uz obavljanje elektronskog bankarstva, uzimajući u obzir minimalno: tehnološka rješenja koja se koriste, napredak tehnologije i nove rizike, usluge koje su eksternalizovane, kao i tehničko okruženje klijenta.
(2) Banka je dužna uspostaviti mehanizme nadzora transakcija u svrhu sprječavanja, otkrivanja i blokiranja sumnjivih platnih transakcija u okviru sistema elektronskog bankarstva, pri čemu bi visokorizične transakcije trebale biti predmetom posebnog postupka ispitivanja i procjene.
(3) U sklopu upravljanja rizicima elektronskog bankarstva, banka je, kao minimum, dužna:
   a) uspostaviti, redovno pregledati i testirati sigurnosne mjere i kontrole, a koje proizlaze iz analize rizika,
   b) uspostaviti proces za nadziranje, rješavanje i praćenje sigurnosnih incidenata i pritužbi klijenata vezanih uz sigurnost, te redovno izvještavanje o navedenom,
   c) primijeniti sigurne i efikasne metode autentifikacije za potvrdu identiteta i ovlaštenja lica, procesa i sistema,
   d) osigurati da autentifikacija korisnika uključuje najmanje dva međusobno nezavisna elementa za potvrđivanja korisničkog identiteta,
   e) osigurati odgovarajuću potvrdu svog identiteta na distribucijskom kanalu elektronskog bankarstva, kako bi korisnici elektronskog bankarstva mogli provjeriti identitet i autentičnost banke,
   f) osigurati sigurne komunikacijske kanale između strana koje učestvuju u razmjeni osjetljivih podataka, za cijelo vrijeme trajanja sesije, a u svrhu osiguranja povjerljivosti i integriteta podataka,
   g) osigurati kontrole ograničenja maksimalnog broja prijave na sistem (autentifikacije, autorizacije i slično), pravilo vremenskog ograničavanja trajanja sesije, kao i vremensko ograničavanje validnosti autentifikacije i
   h) osigurati generisanje, čuvanje i redovnu analizu operativnih i sistemskih zapisa, uključujući i podatke o pristupima podacima o transakcijama i ovlaštenjima, a kako bi osigurala neporecivost i dokazivost radnji povezanih sa elektronskim bankarstvom.

(4) Izuzetno od stava (3) tačka d) banka može primijeniti autentifikaciju korisnika koja se vrši korištenjem jednog elementa za potvrđivanje korisničkog identiteta, u slučaju:
   a) plaćanja male novčane vrijednosti, pod uslovom da se rizicima koji se odnose na ukupan iznos ovih transakcija upravlja na odgovarajući način,
   b) prijenos novčanih sredstava između dva računa istog korisnika kod iste banke i
   c) plaćanja prema pouzdanim primaocima, odnosno primaocima koje je korisnik unaprijed odredio (tzv. bijele liste primaoca).

(5) Banka je dužna da za primjenu autentifikacije iz stava (4) ovog člana dokumentuje sveobuhvatnu i detaljnu analizu rizika i načina upravljanja rizicima koji proizlaze iz pružanja usluga utvrđenih u odredbama stava (4) tačke a) do c) ovog člana.

Član 29.
Fizičke kontrole

(1) Banka je dužna da implementira procedure kojim se definiraju mjere zaštite i kontrole pristupa prostorijama u kojima su smješteni resursi informacionog sistema (prostorije sa serverima, prostorije sa komunikacijskom opremom i slično), kao i prostorijama u kojima se nalaze sistemi za podršku funkcionisanju informacionog sistema, u cilju zaštite od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja resursa informacionog sistema.
(2) Banka je dužna da definira i implementira adekvatne mjere zaštite od statičkog elektriciteta, požara, poplave, zemljotresa, eksplozije i drugih oblika prirodnih katastrofa ili šteta uzrokovanih ljudskim djelovanjem, a na bazi procjene rizika.
(3) Banka je dužna da periodično kontroliše ispravnost implementiranih mjera zaštite.

Član 30.
Plan oporavka informacionog sistema

(1) U cilju osiguranja odvijanja kritičnih (vitalnih) poslovnih procesa u odgovarajućem vremenskom okviru, banka je dužna da donese plan oporavka informacionog sistema koji je sastavni dio plana kontinuiteta poslovanja banke, a u skladu sa propisima Agencije koji regulišu oblast upravljanja rizicima.
(2) Odgovarajući vremenski okvir oporavka banka je dužna da odredi provedbom analize utjecaja na poslovanje.
(3) U okviru analize utjecaja na poslovanje potrebno je kao minimum:
   a) definirati kritične (ključne) poslovne procese i aktivnosti,
   b) definirati resurse i sisteme potrebne za odvijanje pojedinačnih poslovnih procesa, kao i njihove međuzavisnosti i povezanosti,
   c) procijeniti rizik u vezi sa pojedinačnim poslovnim procesima,
   d) utvrditi prihvatljivi nivo rizika za pojedinačne poslovne procese i
   e) odrediti, kao minimum, RTO, RPO i SDO za svaki pojedinačni poslovni proces, imajući u vidu eksternalizaciju i zavisnost od trećih lica.
(4) Pri procesu planiranja kontinuiteta poslovanja, banka je dužna da definira procese, uloge i odgovornosti, a kako bi osigurala da su eksternalizovani dijelovi informacionog sistema i servisi adekvatno pokriveni planovima kontinuiteta poslovanja. Banka je dužna uzeti u obzir zavisnost o uslugama trećih lica.
(5) Na osnovu analize utjecaja na poslovanje, banka je dužna da definira i usvoji plan(ove) oporavka informacionog sistema kojim će omogućiti raspoloživost resursa, definira prioritete oporavka poslovnih procesa, kao i potrebne resurse i sisteme, te detaljno opiše postupke koje je potrebno slijediti kako bi se u zahtijevanom vremenskom roku i sa zahtijevanim funkcionalnostima oporavili kritični (vitalni) poslovni procesi i podaci.
(6) Plan oporavka informacionog sistema treba, kao minimum, da sadrži:

a) detaljne procedure i uputstva za oporavak resursa informacionog sistema potrebnih za odvijanje kritičnih (ključnih) poslovnih procesa u slučaju vanrednih situacija,
b) definirane prioritete oporavka resursa informacionog sistema, kao i spisak svih resursa potrebnih za ponovno uspostavljanje kritičnih (ključnih) poslovnih procesa,
c) podatke o timovima koji će biti odgovorni za oporavak informacionog sistema, njihovim članovima sa jasno definiranim dužnostima i odgovornostima,
d) podatke o lokaciji za oporavak informacionog sistema i
e) podatke o ključnim pružaocima usluga.

(7) Uprava banke treba da osigura da je plan oporavka informacionog sistema ažuran.

Član 31.

(1) Banka je dužna da, u skladu sa procjenom rizika i na osnovu rezultata analize utjecaja na poslovanje, osigura raspoloživost rezervnog informatičkog centra koji je na odgovarajućoj udaljenosti od primarnog informatičkog centra, uzimajući u obzir rizik da pojedinačni scenario, incident ili katastrofa ne mogu istovremeno utjecati na produkcioni sistem banke i sisteme oporavka.
(2) Efektivna funkcionalnost rezervnog informatičkog centra treba biti potvrđena najmanje jednom godišnje, kao i poslije implementiranih značajnih promjena u informacionom sistemu banke. Rezultate navedenog testiranja je potrebno dokumentovati i osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke. U okviru navedenog testiranja, banka je dužna uzeti u obzir različite realne scenarije uključujući cyber napade, prekide komunikacionih veza, nedostupnost primarnog informatičkog centra, testove kopija za kritični softver i podatke i slično. Banka je dužna, 30 dana prije planiranog testiranja funkcionalnosti rezervnog informatičkog centra, obavijestiti Agenciju.
(3) Banka je dužna da u slučaju nastanka okolnosti koje zahtijevaju primjenu plana oporavka informacionog sistema odmah obavijesti Agenciju o svim relevantnim činjenicama i okolnostima koje se na to odnose.

Član 32.

(1) U slučaju eksternalizacije cjelokupnog ili dijela informacionog sistema izvan teritorije Bosne i Hercegovine, banka je dužna sljedeće:
a) da definira kritične (vitalne) procese sa stanovišta kontinuiteta poslovanja i odvijanja istih u zemlji,
b) da osigura lokalni informatički centar na teritoriji Bosne i Hercegovine kako bi osigurala raspoloživost podataka i mogućnost odvijanja kritičnih (vitalnih) procesa u zemlji definiranih u okviru stava (1) tačka a) ovog člana,
c) da provodi testiranje funkcionalnosti lokalnog informatičkog centra najmanje na godišnjem nivou, te osigura da je izvještaj o rezultatima testiranja usvojen od strane uprave banke,
d) da osigura ažurnost podataka u lokalnom informatičkom centru na dnevnoj osnovi i
e) da osigura podatke u lokalnom informatičkom centru, u skladu sa važećim zakonskim propisima.

(2) Banka je dužna, 30 dana prije planiranog testiranja funkcionalnosti lokalnog informatičkog centra, obavijestiti Agenciju.

Član 33.

Prijelazne i završne odredbe

(1) Direktor Agencije će u roku od 60 (šezdeset) dana od dana stupanja na snagu ove odluke donijeti Uputstvo za izvještavanje o upravljanju informacionim sistemima, kojim će se detaljnije propisati izvještavanje, način i metodologija popunjavanja obrazaca, koji su sastavni dio navedenog Uputstva.

(2) Banka je dužna da uskladi svoje poslovanje sa odredbama ove odluke u skladu sa članom 250. stav (1) Zakona o bankama, izuzev člana 17. stav (2), člana 28. st. (2), (3) i (4), koji se počinju primjenjivati 180 dana od dana stupanja na snagu ove odluke, čl. 8., 11. st. (3), (4), (5) i (6) i člana 16., koji se primjenjuju 360 dana od dana stupanja na snagu ove odluke.

(3) Banka je dužna da sačini prve kvartalne izvještaje za I. kvartal 2018. godine i prve godišnje izvještaje za 2017. godinu i dostavi ih Agenciji u skladu sa Uputstvom iz stava (1) ovog člana.

(4) Stupanjem na snagu ove odluke, prestaje da važi Odluka o minimalnim standardima upravljanja informacionim sistemima u bankama („Službene novine Federacije BiH“, broj: 1/12).

Član 34.

Stupanje na snagu

Ova odluka stupa na snagu osmog dana od dana objavljivanja u „Službenim novinama Federacije BiH“.

Broj: U.O.-08-25/17
Sarajevo, 13.10.2017. godine

PREDSJEDNICA
UPRAVNOG ODBORA

mr. sc. Ljerka Marić, dipl.ecc., s.r.