Na temelju članka 5. stavak (1) točka h) i članka 19. stavak (1) točka 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 INFORMACIJSKIM SUSTAVOM U BANCI

Članak 1.
Opće odredbe

Odlukom o upravljanju informacijskim sustavom u banci utvrđuju se zahtjevi i kriteriji koje je banka dužna osigurati i provoditi u procesu upravljanja informacijskim sustavom i rizicima koji proističu iz korištenja informacijskih sustava.

Članak 2.
Definicije

Definicije koje se koriste u ovoj odluci imaju sljedeća značenja:

a) **Informacijski sustav** – sveobuhvatan skup resursa organiziran u svrhu prikupljanja, spremanja, obrade, održavanja, korištenja, distribucije i raspolaganja informacijama.
b) **Povjerljivost** – osobina da informacija nije dostupna ili otkrivena neovlaštenim osobama ili procesima.
c) **Integritet** – osobina informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.
d) **Dostupnost** – osobina da informacija bude pravodobno dostupna i iskoristiva na zahtjev od strane ovlaštene osobe.
e) **Kontrole** – politike, procedure, prakse, tehnologije i organizacijske strukture dizajnirane kako bi osigurale razumno uvjerenje da će poslovni ciljevi biti dostignuti i da će neželjeni događaji biti spriječeni ili detektirani. Kontrole se dijele na upravljačke, logičke i fizičke. Upravljačke kontrole uključuju donošenje internih akata vezanih uz informacijski sustav i uspostavljanje odgovarajuće organizacijske strukture, te osiguravaju primjenu internih akata vezanih uz informacijski sustav u cilju osiguravanja funkcionalnosti i sigurnosti informacijskog sustava. Logičke kontrole su kontrole implementirane na softverskim komponentama. Fizičke kontrole su kontrole koje štite resurse informacijskog sustava od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja.
f) **Resursi informacijskog sustava** – resursi koji uključuju informatičku imovinu, softverske i hardverske komponente, ljude i procese.
g) **Analiza isplativosti** (eng. cost-benefit analiza) – metoda ekonomske analize kojom se uspoređuju i vrednuju sve prednosti i svi nedostaci projekta analizom troškova i koristi.
h) **Sigurnost informacija** – osigurava da samo ovlašteni korisnici (povjerljivost) imaju pristup točnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).
i) **Načelo višeslojne zaštite** – načelo implementacije više slojeva sigurnosnih zaštita, gdje neefikasnost jednog sloja zaštite nadoknađuje sljedeći sloj zaštite.
j) **Penetracijski test –** proces koji upotrebom automatiziranih alata otkriva prisutne ranjivosti u informacijskom sustavu i iskorištava ih s ciljem otkrivanja mogućnosti obavljanja neautoriziranog pristupa ili druge maliciozne aktivnosti, te dalje, identificira i utvrđuje razine uočenih rizika otkrivenih ranjivosti.
k) **Test ranjivosti** – proces koji upotrebom automatiziranih alata otkriva prisutne ranjivosti u informacijskom sustavu, ali ih ne iskorištava.

l) **Korisnici informacijskog sustava** – sve osobe koje koriste informacijski sustav (zaposlenici banke, zaposlenici pružatelja usluga, korisnici elektroničkog bankarstva, zaposlenici pravnih osoba koji koriste informacijski sustav banke i drugo).
m) **Rizik informacijskog sustava** – rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava.
n) **Elektroničko bankarstvo** – sustav koji omogućava klijentima banke obavljanje bankarskih poslova a udaljene lokacije putem javnih komunikacijskih mreža ili slično.
o) **Rizik povezan s integritetom podataka** – rizik da su podaci koji su skladišteni i procesirani u informacijskom sustavu nepotpuni, netočni ili nekonzistentni kroz sustav odnosno različite sustave.
p) **Evidentiranje korisničkih prava pristupa** – proces dodjele prava pristupa korisnicima informacijskog sustava.
q) **Identifikacija i autentifikacija** – procesi identifikacije korisnika informacijskog sustava i potvrde njegova identiteta prilikom prijave i tijekom provedbi radnji na informacijskom sustavu.
r) **Autorizacija** – proces kojim se provjerava ima li klijent pravo izvršiti određenu radnju.
s) **Autentifikacija** – proces potvrde identiteta korisnika/procesa od strane sustava.
t) **Nadzor korisničkih prava pristupa –** proces koji uključuje praćenje, izmjenu i reviziju prava pristupa korisnika informacijskog sustava.
u) **Povlašteni pristup** – pristup resursima informacijskog sustava koji omogućava korisnicima znatno veća prava, te zaobilaženje ugrađenih logičkih kontrola (na primjer, administrator mrežne opreme, baze podataka, sistemskog softvera, aplikativnog softvera i slično).
v) **Udaljeni pristup** – omogućava pristup resursima informacijskog sustava s udaljene lokacije putem telekomunikacijskih linija nad kojima banka nema potpunu kontrolu odnosno nadzor.
w) **Software-ske komponente (software-ska imovina)** – uključuju aplikacijski softver, sistemski softver, baze podataka, softverske razvojne alate, uslužne programe, te ostali softver.
x) **Operativni i sistemski zapisi** – kronološki zapisi o aktivnostima na resursima informacijskog sustava (zapisi operativnih sustava, aplikacijskog softvera, baza podataka, mrežnih uređaja i slično).
y) **Maliciozni kod** – bilo koji oblik programskog koda stvoren s namjerom da se neovlašteno ostvari pristup resursima informacijskog sustava, prikupe ili unište informacije, izazove neočekivano ponašanje ili prekid u funkcioniranju ovog sustava 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 informacijskog sustava koje uključuju: računala i računalnu opremu, komunikacijsku opremu, medije za čuvanje podataka, te ostalu tehničku opremu koja podržava rad informacijskog sustava.
aa) **Informacijska imovina** – sva materijalna ili nematerijalna imovina koja za banku ima neku vrijednost (serveri, mrežne komponente, podaci u bazama podataka, datoteke s 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** – osobe i/ili organizacijski dio kojem je odobrena upravljačka odgovornost za produkciju, razvoj, održavanje, korištenje i zaštitu imovine.

dd) **Skrbnik** – osobe i/ili organizacijski 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, sukladno važećim politikama, procedurama i uputama.

ee) **Razvoj** – zahtjev za razvojem novih funkcionalnosti informacijskog sustava.

ff) **Promjena** – zahtjev za izmjenom podataka ili izmjenama nad postojećim funkcionalnostima informacijskog sustava.

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

hh) **Incident** – svaki neplanirani i neželjeni događaj koji može narušiti sigurnost i funkcionalnost resursa informacijskog sustava 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)
   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 (informacijska imovina, softverske komponente) koji su potrebni za ponovno uspostavljanje poslovnih procesa banke, te ostalih podataka za koje banka procijeni da ih je potrebno čuvati.

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

ll) **Raspoloživost** – svojstvo imovine da je pravodobno dostupna i upotrebljiva na zahtjev ovlaštene osobe.

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

nn) **Autentičnost** – osobina koja osigurava da je identitet osobe 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 osigurava da svaka aktivnost u informacijskom sustavu može jednoznačno biti praćena do njenog izvora.

qq) **Pouzdanost** – označava da informacijski sustav dosljedno i očekivano obavlja predviđene funkcije i pruža točne informacije.

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

ss) **Recovery time objective (RTO) –** najduže prihvatljivo vrijeme neraspoloživosti poslovnog procesa banke i resursa informacijskog sustava potrebnih za odvijanje poslovnog procesa, odnosno vrijeme tijekom kojega je potrebno obnoviti poslovni proces.

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

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

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

Članak 3.

Okvir za upravljanje informacijskim sustavom

(1) Banka je dužna uspostaviti, implementirati, nadzirati, održavati, redovno revidirati i poboljšavati proces upravljanja informacijskim sustavom u cilju smanjenja izloženosti rizicima, osiguranja povjerljivosti, integriteta i dostupnosti informacija i cjelokupnog informacijskog sustava, primjereno veličini, složenosti i opsegu poslovanja banke, te kompleksnosti informacijskog sustava.

(2) Banka je dužna uspostaviti adekvatan sustav koji uključuje identifikaciju, mjerenje, praćenje i kontrolu upravljanja rizicima koji proističu iz korištenja informacijskog sustava.

Članak 4.

Nadzorni odbor

Nadzorni odbor banke je dužan i odgovoran, kao minimum:

a) na temelju prijedloga uprave, donijeti strategiju informacijskog sustava, koja treba biti sastavni dio ukupne poslovne strategije banke;
b) na temelju prijedloga uprave, donijeti politike za upravljanje informacijskim sustavom, a posebno politiku sigurnosti informacijskog sustava i nadzirati njihovu implementaciju;
c) aktualizirati usvojene politike u skladu s promjenama ekonomskih, tržišnih, tehnoloških i drugih uvjeta, a najmanje jednom godišnje;
d) uspostaviti sustav za mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim uz informacijski sustav, pratiti efikasnost i unapređivati dani sustav;
e) donijeti i osigurati uspostavu adekvatne organizacijske strukture i odgovarajućih funkcija i ovlasti kako bi osigurala efikasno i sigurno upravljanje informacijskim sustavom, s obvezom definiranja stručnih kvalifikacija i potrebnih kompetencija;
f) osigurati selekciju i imenovanje kvalificiranog i kompetentnog člana uprave koji će biti nadležan za uspostavu i nadzor procesa upravljanja informacijskim sustavom;
g) na temelju prijedloga uprave, propisati sadržaj i periodičnost izvješćivanja nadzornog odbora banke o relevantnim činjenicama vezanim uz upravljanje informacijskim sustavom, a najmanje jednom godišnje;
h) osigurati uvjete za uspostavu efikasnog sustava unutarnjih kontrola u segmentu upravljanja informacijskim sustavom i obavljati nadzor nad tim sustavom.

Članak 5.

Uprava banke

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

a) imenovati odbor za upravljanje informacijskim sustavom, sastavljen od predstavnika različitih poslovnih funkcija, koji će se sastajati periodično i izvješćivati upravu o svojim aktivnostima najmanje na kvartalnoj razini, a čija uloga treba biti koordinacija inicijativa i praćenje razvojnih aktivnosti informacijskog sustava, kao i usklađenosti ciljeva informacijskog sustava s poslovnim ciljevima i poslovnom strategijom banke;
b) predlagati i implementirati politike te donositi i provoditi procedure upravljanja informacijskim sustavom sukladno poslovnim ciljevima i poslovnoj strategiji banke;
c) implementirati sustav za identifikaciju, mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim za informacijski sustav;
d) osigurati da su sve dužnosti vezane uz upravljanje informacijskim sustavom jasno definirane i dodijeljene, vodeći računa o adekvatnoj segregaciji dužnosti;

e) donositi plan i program za uspostavu i podizanje svijesti o sigurnosti informacijskog sustava;
f) osigurati potrebne resurse za upravljanje informacijskim sustavom;
g) usvojiti i primijeniti metodologiju upravljanja projektima kojom će se definirati kriteriji, načini i postupci upravljanja projektima vezanim uz informacijski sustav.

(2) Uprava banke je dužna pravodobno obavijestiti Agenciju za bankarstvo Federacije Bosne i Hercegovine (u daljnjem tekstu: Agencija) o svakoj značajnoj i kompleksnoj promjeni koja može imati utjecaja na informacijski sustav banke, te dostaviti odgovarajuću dokumentaciju (na primjer, projektni plan, projektne timove, planirani proračun, analizu isplativosti projekta, procjenu rizika projekta i slično).

Članak 6.
Strategija informacijskog sustava

(1) Banka je dužna razviti i nadzirati implementaciju strategije informacijskog sustava koja, kao minimum, treba:
a) obuhvatiti dugoročne i kratkoročne inicijative vezane za informacijski sustav;
b) definirati povezanost i usklađenost ciljeva informacijskog sustava s poslovnim ciljevima banke;
c) se periodično ažurirati, a posebno prilikom izmjene poslovne strategije, kako bi se osigurala kontinuirana usklađenost između poslovnih ciljeva i ciljeva informacijskog sustava, te odgovarajućih planova i aktivnosti;
d) se detaljnije razraditi kroz donošenje operativnih planova.

(2) Uprava banke je dužna usvojiti operativni plan informacijskog sustava na godišnjoj razini, a koji proizlazi iz strategije informacijskog sustava.

(3) Operativni plan informacijskog sustava treba, kao minimum, sadržavati sljedeće elemente: opis aktivnosti i projekata informacijskog sustava, ljudske resurse, proračun, vremenske rokove i odgovorne osobe.

(4) Banka je dužna osigurati da je identifikacija, procjena i smanjenje rizika povezanih s implementacijom strategije informacijskog sustava, kao i efikasna uspostava okvira za upravljanje informacijskim sustavom, pod kontinuiranim nadzorom kontrolnih funkcija banke.

Članak 7.
Politika sigurnosti informacijskog sustava

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

(2) Politika sigurnosti informacijskog sustava treba biti usklađena s promjenama u okruženju i informacijskom sustavu banke.

(3) Banka je dužna proces upravljanja sigurnošću informacijskog sustava uspostaviti kao kontinuirani proces identificiranja potreba za ovom sigurnošću i postizanja i održavanja adekvatne razine te sigurnosti, na temelju rezultata procjene rizika i obveza koje proizlaze iz propisa, ugovornih odnosa i slično.

Članak 8.

Banka je dužna, na godišnjoj razini, pregledati i testirati sigurnosne mjere i kontrole informacijskog sustava banke (na primjer, test ranjivosti, penetracijski test i slično), utvrditi opseg testiranja sukladno procjeni rizika, te izvješćivati upravu i nadzorni odbor o rezultatima testiranja.

Članak 9.

Interni akti

(1) Banka je dužna propisati i primijeniti detaljne procedure kojima se uređuje upravljanje informacijskim sustavom, te osigurati provedbu tih procedura.
(2) Interni akti trebaju, kao minimum, biti:
   a) usklađeni s propisima, standardima i pravilima struke;
   b) redovito pregledani i ažurirani;
   c) potpuni, detaljni i primjenjivi.
(3) Potrebno je osigurati da su svi korisnici informacijskog sustava upoznati sa sadržajem internih akata, vezanih uz informacijski sustav, sukladno potrebama svakog korisnika.
(4) Ugovori, nalazi revizije, upute i ostali dokumenti trebaju biti sačinjeni odnosno prevedeni na jedan od jezika u službenoj upotrebi u Federaciji Bosne i Hercegovine.

Članak 10.

Upravljanje rizicima iz ugovornih odnosa

Banka je dužna kontinuirano procjenjivati i adekvatno upravljati rizicima koji proizlaze iz ugovornih odnosa s pravnim i fizičkim osobama, a čije su aktivnosti vezane uz informacijski sustav banke.

Članak 11.

Upravljanje rizicima informacijskog sustava

(1) Banka je dužna uspostaviti proces upravljanja rizicima informacijskog sustava koji treba biti sastavni dio sustava upravljanja rizicima na razini banke, sukladno propisima Agencije koji reguliraju 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 informacijskog sustava, te odrediti odgovornosti upravljanja rizicima i prihvatljive razine rizika za identificirane značajne rizike informacijskog sustava.
(3) U okviru upravljanja rizicima informacijskog sustava, banka je dužna, kao minimum:
   a) identificirati ključne dijelove i servise informacijskog sustava;
   b) procijeniti prijetnje, ranjivosti, posljedice i implementirane kontrole identificiranih ključnih dijelova i servisa informacijskog sustava;
   c) preporučiti mjere za tretiranje rizika, donijeti plan tretmana rizika i kontinuirano pratiti realizaciju ovoga plana;
   d) redovito, a najmanje jednom godišnje izvješćivati upravu i nadzorni odbor banke o rezultatima procjene rizika.
(4) Upravljanje rizicima informacijskog sustava treba obuhvatiti informacijski sustav banke u potpunosti s posebnom pažnjom na sljedeće:

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

(5) Svi navedeni ključni dijelovi informacijskog sustava i servisi trebaju biti ocijenjeni sa stanovišta utjecaja i izloženosti riziku dostupnosti i kontinuiteta poslovanja, riziku sigurnosti informacijskog sustava, riziku promjena u informacijskom sustavu, riziku povezanom s integritetom podataka i riziku eksternalizacije.

(6) Banka je dužna osigurati da je identifikacija, procjena i smanjenje rizika povezanih s informacijskim sustavom, kao i efikasna uspostava okvira za upravljanje rizicima informacijskog sustava, pod kontinuiranom nadzorom unutarnje i vanjske revizije.

Članak 12.

Odgovorna osoba za sigurnost informacijskog sustava

(1) Uprava banke dužna je imenovati odgovornu osobu (voditelj/oficir) za funkciju sigurnosti informacijskog sustava, te definirati njegove ovlasti, odgovornosti i opseg rada. Funkcija sigurnosti informacijskog sustava treba biti nezavisna od funkcije organizacijske jedinice za upravljanje informacijskim sustavom. Osoba odgovorna za sigurnost informacijskog sustava treba biti kompetentna osoba s odgovarajućim stručnim kvalifikacijama, specijalističkim znanjima i iskustvom.

(2) Osoba odgovorna za funkciju sigurnosti informacijskog sustava treba, kao minimum, nadzirati i koordinirati aktivnosti vezane uz sigurnost informacijskog sustava, te da redovito izvješćuje upravu banke o stanju i aktivnostima vezanim uz sigurnost informacijskog sustava, a minimalno na kvartalnoj razini.

Članak 13.

Unutarnja revizija

(1) Banka je dužna provoditi unutarnju reviziju informacijskog sustava sukladno propisima Agencije koji reguliraju oblast unutarnje revizije banke, a na temelju definiranog programa rada unutarnje revizije.

(2) Banka je dužna planirati i provoditi unutarnju reviziju informacijskog sustava sukladno metodologiji procjene rizika, imajući u vidu da u određenim vremenskim intervalima budu redovno pregledane (obuhvaćene) sve kritične i ključne funkcije informacijskog sustava banke.

(3) Banka je dužna osigurati da se unutarnja revizija informacijskog sustava provodi na kontinuiranoj osnovi tijekom cijele godine.

(4) Osobe koja obavljaju unutarnju reviziju informacijskog sustava banke trebaju posjedovati stručna znanja i vještine o informacijskim sustavima.

(5) U slučaju eksternalizacije aktivnosti unutarnje revizije informacijskog sustava, banka treba osigurati da pružatelj usluga unutarnje revizije informacijskog sustava istodobno (u toj

godini) ne pruža usluge vanjske revizije informacijskog sustava banci, te treba osigurati da ne postoji sukob interesa u skladu s profesijom unutarnje revizije.

(6) U slučaju eksternalizacije aktivnosti unutarnje revizije informacijskog sustava, banka treba osigurati da pružatelj usluga posjeduje međunarodno priznate certifikate za reviziju informacijskog sustava.

Članak 14.

Vanjska revizija

(1) Agencija daje prethodnu suglasnost za imenovanje društva za reviziju za obavljanje revizije informacijskog sustava.

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

(3) Banka je dužna, uz zahtjev iz stavka (2) ovoga člana, dostaviti Agenciji sljedeće dokumente:
   a) nacrt odluke o imenovanju društva za reviziju informacijskog sustava;
   b) nacrt ugovora ili pisma namjere s društvom za reviziju informacijskog sustava;
   c) reference društva za reviziju informacijskog sustava o obavljenim revizijama informacijskih sustava;
   d) dokaze o stručnim kvalifikacijama osoba koje će obavljati reviziju i njihove životopise;
   e) izjavu o nepostojanju sukoba interesa između društva za reviziju (odnosno osobe koje operativno provode reviziju) i banke.

(4) Skupština banke, uz prethodnu suglasnost Agencije, imenuje društvo za reviziju najkasnije do 30. rujna tekuće godine, koje će obaviti reviziju informacijskog sustava 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 informacijskog sustava 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 vanjske revizije informacijskog sustava, društvo za reviziju je dužno uzeti u obzir eksternalizirane usluge i njihovu značajnost i utjecaj na informacijski sustav, te sukladno tomu razviti plan revizije i efikasni pristup reviziji.

(8) Društvo za reviziju je dužno sačiniti revizorsko izvješće o obavljenoj reviziji informacijskog sustava, te dati ocjenu o stanju informacijskog sustava i adekvatnosti upravljanja informacijskim sustavom.

(9) Izvješće o obavljenoj reviziji informacijskog sustava je posebno izvješće, te je banka dužna dostaviti Agenciji navedeno izvješće najkasnije do 31. svibnja tekuće godine.

(10) Banka je dužna reviziju informacijskog sustava obavljati na godišnjoj razini.

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

Članak 15.

Upravljanje kontrolama pristupa

Banka je dužna uspostaviti adekvatan sustav upravljanja pristupom resursima informacijskog sustava koji, kao minimum, treba obuhvatiti:

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

Članak 16.

Cyber sigurnost

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

a) proces ili rješenja za održavanje kompletnog i ažurnog registra i pregled svih vanjskih mrežnih točaka konekcije (na primjer, web stranice, internet aplikacije, wi-fi, udaljeni pristup i slično) kroz koje treće osobe mogu upasti u interni informacijski sustav 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 prometa i vanjskih mrežnih konekcija kroz koje treće osobe mogu upasti u interni informacijski sustav banke;
c) procese i rješenja za zaštitu web stranica i aplikacija koje mogu biti izravno napadnute s interneta i/ili izvana, a koje mogu služiti kao ulazna točka u interni informacijski sustav banke (na primjer, princip osnaživanja sustava – hardening, IPS/IDS sustavi i slično),
d) segmentiranje mreže, redovito praćenje mrežnog prometa i analize zapisa, kao i provjere integriteta softvera;
e) periodično sigurnosno penetracijsko testiranje kako bi se procijenila efikasnost implementiranih cyber i internih sigurnosnih mjera i procesa.

Članak 17.

Operativni i sistemski zapisi

(1) Banka je dužna, sukladno procjenu rizika, osigurati izradu, redovito praćenje i čuvanje operativnih i sistemskih zapisa u svrhu pravodobnog otkrivanja neovlaštenih pristupa i radnji u informacijskom sustavu, identificiranja problema, rekonstruiranja događaja, te utvrđivanja odgovornosti.
(2) Banka je dužna definirati resurse informacijskog sustava i vrste operativnih i sistemskih zapisa koji se prate, njihov sadržaj, vrste i frekvenciju analize i nadzora operativnih i sistemskih zapisa, razdoblje čuvanja zapisa, te odgovorne osobe.
(3) Banka je dužna uspostaviti adekvatnu zaštitu zapisa, osigurati njihov integritet i povjerljivost sukladno klasifikaciji informacija, te razdvojiti dužnosti osoba koje administriraju resurse informacijskog sustava s kojih se zapisi prikupljaju od osoba koje administriraju zapise.

Članak 18.

Maliciozni kod

Banka je dužna uspostaviti proces za upravljanje zaštitom od malicioznog koda koji treba, kao minimum, obuhvatiti sljedeće:

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

Članak 19.

Aplikativne kontrole

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

Članak 20.

Upravljanje resursima

(1) Banka je dužna uspostaviti proces upravljanja hardverskom i softverskom imovinom, koja je neophodna za obavljanje kritičnih (vitalnih) procesa, tijekom cijelog životnog ciklusa, od nabave ili razvoja do povlačenja iz upotrebe.
(2) Proces upravljanja hardverskom i softverskom imovinom treba obuhvatiti postupke identifikacije, evidentiranja, određivanja vlasnika i skrbnika, načina raspolaganja, utvrđivanje pravila njihovog prihvatljivog korištenja, praćenja, obnavljanja i odlaganja te imovine.
(3) Banka je dužna osigurati adekvatno održavanje hardverske i softverske imovine informacijskog sustava prema preporukama proizvođača, te čuvati zapise o tom održavanju.
(4) Banka je dužna klasificirati i zaštititi informacije, te definirati način upravljanja istim prema njihovoj vrijednosti, pravnim zahtjevima, osjetljivosti i kritičnosti za banku.

Članak 21.

Upravljanje razvojem

(1) Banka je dužna definirati i implementirati procedure koje propisuju upravljanje razvojem informacijskog sustava, 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 izvješćivanja;
   d) proces razvoja, adekvatnog testiranja i edukacije osoblja;
   e) uvođenje u produkcijski rad, vodeći računa o adekvatnoj segregaciji dužnosti;
   f) dokumentiranje procesa razvoja i isporuke informacijskog sustava;
   g) plana povratka na 'staro' stanje,
(2) Banka je dužna osigurati adekvatno razdvajanje razvojnog, testnog i produkcijskog okruženja.
(3) Banka je dužna osigurati odgovarajuću analizu i testiranje sigurnosti i ranjivosti sustava prije implementacije u produkcijsko okruženje, te osigurati da promjene komponenata informacijskog sustava ne narušavaju sigurnost i funkcionalnost informacijskog sustava.

Članak 22.

Upravljanje promjenama

(1) Banka je dužna uspostaviti procedure procesa upravljanja promjenama u informacijskom sustavu, kako bi se izbjeglo da one dovedu do neočekivanog i neželjenog ponašanja ovog sustava, 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 dokumentiranje, prije uvođenja u produkcijski rad;
   c) upravljanje 'hitnim' promjenama;
   d) implementaciju promjena, uključujući i plan povratka na 'staro' stanje;
   e) segregaciju dužnosti vezano za razvoj i implementaciju promjena;
   f) praćenje i izvješćivanje.
(2) Banka je dužna osigurati testno okruženje koje adekvatno odražava produkcijsko 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, najdužr razdoblje 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 sustava prije implementacije značajnih promjena u produkcijsko okruženje, te osigurati da promjene komponenata informacijskog sustava ne narušavaju sigurnost i funkcionalnost informacijskog sustava.
(5) Banka je dužna utvrditi početne verzije softverskih komponenata informacijskog sustava, te evidentirati i dokumentirati sve promjene komponenata informacijskog sustava onim slijedom kako su nastajale, zajedno s vremenom nastanka promjene.
(6) Procedure navedene u stavku (1) ovoga članka se odnose na promjene osnovnih operativnih sustava, aplikativnog softvera, konfiguracijskih datoteka, hardvera i ostalih dijelova informacijskog sustava.

Članak 23.
Dokumentacija

Banka je dužna definirati i implementirati procedure upravljanja dokumentacijom (tehničkom, funkcionalnom, korisničkom i drugom) koja se odnosi na informacijski sustav, a koja, kao minimum, treba uključiti sljedeće:

a) osiguranje točne, potpune i ažurne dokumentacije;
b) osiguranje pristupa zaposlenika dokumentaciji, u skladu s njihovim poslovnim potrebama i klasifikaciji.

Članak 24.
Upravljanje korisničkim zahtjevima

Banka je dužna uspostaviti proces upravljanja korisničkim zahtjevima koji, kao minimum, treba obuhvatiti procedure za prijavljivanje, klasificiranje, određivanje prioriteta, obradu i izvješćivanje o korisničkim zahtjevima.

Članak 25.
Upravljanje incidentima

(1) Banka je dužna uspostaviti proces upravljanja incidentima, koji obuhvaća, kao minimum, identifikaciju, klasifikaciju, eskalaciju, odgovor na incident, oporavak, analizu, te izvješćivanje, a koji treba omogućiti brz, efektivan i propisan odgovor u slučaju narušavanja sigurnosti i funkcionalnosti informacijskog sustava.
(2) Banka je dužna, kao minimum, evidentirati sljedeće vrste incidenata: prekidi u radu hardverskih i softverskih komponenti, smanjenje performansi servisa, neautorizirani pristup resursima informacijskog sustava, odljev podataka, krađa identiteta, maliciozni kod, krađa, neuspješan proces izrade rezervne kopije podataka, narušavanje integriteta podataka i slično.
(3) Banka je dužna osigurati izvješćivanje uprave o incidentima vezanim uz informacijski sustav na periodičnoj osnovi.
(4) Banka je dužna odmah po saznanju o težem incidentu, kako u dijelu informacijskog sustava koji se nalazi u banci, tako i u dijelu informacijskog sustava koji je eksternaliziran (ključna bankarska aplikacija, sustav elektroničkog bankarstva, sustav kartičnog poslovanja i drugo) obavijestiti Agenciju, te nakon rješavanja incidenta dostaviti kompletnu analizu incidenta zajedno s posljedicama i poduzetim aktivnostima.

Članak 26.
Kopije

(1) Banka je dužna uspostaviti proces upravljanja kopijama (eng. backup) koji uključuje procedure izrade, smještaja, testiranja kopija podataka, te restauracije podataka s 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 informacijskog sustava vrstu, način izrade, frekvenciju izrade, frekvenciju odlaganja na udaljenu lokaciju, te razdoblje 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 temelju urađene analize rizika.
(4) Banka je dužna osigurati rezervnu kopiju podataka na jednom od medija (na primjer, vanjski 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.

Članak 27.
Edukacija

(1) Banka je dužna osigurati stručno osposobljavanje i kontinuiranu edukaciju zaposlenika zaduženih za upravljanje informacijskim sustavom, odgovorne osobe za sigurnost informacijskog sustava i unutarnjeg revizora informacijskog sustava, kao i primjerenu, pravodobnu i kontinuiranu edukaciju korisnika informacijskog sustava.
(2) Banka je dužna provoditi programe podizanja svijesti korisnika informacijskog sustava, vezane za sigurnost informacijskog sustava u banci, vodeći računa o aktualnim trendovima (na primjer, cyber prijetnje i slično).

Članak 28.
Elektroničko bankarstvo

(1) Banka je dužna uspostaviti proces upravljanja rizikom elektroničkog bankarstva, koji treba biti sastavni dio cjelokupnog upravljanja rizicima kojima je banka izložena, a u okviru kojeg je potrebno dokumentirati detaljne procjene rizika vezane uz obavljanje elektroničkog bankarstva, uzimajući u obzir minimalno: tehnološka rješenja koja se koriste, napredak tehnologije i nove rizike, usluge koje su eksternalizirane, kao i tehničko okruženje klijenta.
(2) Banka je dužna uspostaviti mehanizme nadzora transakcija u svrhu sprječavanja, otkrivanja i blokiranja sumnjivih platnih transakcija u okviru sustava elektroničkog bankarstva, pri čemu bi visokorizične transakcije trebale biti predmetom posebnog postupka ispitivanja i procjene.
(3) U sklopu upravljanja rizicima elektroničkog bankarstva, banka je, kao minimum, dužna:
   a) uspostaviti, redovito 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 izvješćivanje o navedenom;
   c) primijeniti sigurne i efikasne metode autentifikacije za potvrdu identiteta i ovlaštenja osoba, procesa i sustava;
   d) osigurati da autentifikacija korisnika uključuje najmanje dva međusobno neovisna elementa za potvrđivanja korisničkog identiteta;
   e) osigurati odgovarajuću potvrdu svog identiteta na distribucijskom kanalu elektroničkog bankarstva, kako bi korisnici elektroničkog bankarstva mogli provjeriti identitet i autentičnost banke;
   f) osigurati sigurne komunikacijske kanale između strana koje sudjeluju 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 sustav (autentifikacije, autorizacije i slično), pravilo vremenskog ograničavanja trajanja sesije, kao i vremensko ograničavanje validnosti autentifikacije;
   h) osigurati generiranje, čuvanje i redovitu analizu operativnih i sistemskih zapisa, uključujući i podatke o pristupima podacima o transakcijama i ovlastima, a ako bi osigurala neporecivost i dokazivost radnji povezanih s elektroničkim bankarstvom.

(4) Iznimno od stavka (3) točka d) banka može primijeniti autentifikaciju korisnika koja se vrši korištenjem jednog elementa za potvrđivanje korisničkog identiteta, u slučaju:
   a) plaćanja male novčane vrijednosti, pod uvjetom 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;
   c) plaćanja prema pouzdanim primateljima, odnosno primateljima koje je korisnik unaprijed odredio (tzv. bijele liste primatelja).

(5) Banka je dužna da za primjenu autentifikacije iz stavka (4) ovoga članka dokumentira sveobuhvatnu i detaljnu analizu rizika i načina upravljanja rizicima koji proizlaze iz pružanja usluga utvrđenih u odredbama stavka (4) točke a) do c) ovoga članka.

Članak 29.
Fizičke kontrole

(1) Banka je dužna implementirati procedure kojim se definiraju mjere zaštite i kontrole pristupa prostorijama u kojima su smješteni resursi informacijskog sustava (prostorije sa serverima, prostorije s komunikacijskom opremom i slično), kao i prostorijama u kojima se nalaze sustavi za podršku funkcioniranju informacijskog sustava, u cilju zaštite od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja resursa informacijskog sustava.
(2) Banka je dužna definirati i implementirati 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 periodično kontrolirati ispravnost implementiranih mjera zaštite.

Članak 30.
Plan oporavka informacijskog sustava

(1) U cilju osiguranja odvijanja kritičnih (vitalnih) poslovnih procesa u odgovarajućem vremenskom okviru, banka je dužna donijeti plan oporavka informacijskog sustava koji je sastavni dio plana kontinuiteta poslovanja banke, a sukladno propisima Agencije koji reguliraju oblast upravljanja rizicima.
(2) Odgovarajući vremenski okvir oporavka banka je dužna odrediti 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 sustave potrebne za odvijanje pojedinačnih poslovnih procesa, kao i njihove međuovisnosti i povezanosti;
   c) procijeniti rizik u vezi s pojedinačnim poslovnim procesima;
   d) utvrditi prihvatljivu razinu rizika za pojedinačne poslovne procese;
   e) odrediti, kao minimum, RTO, RPO i SDO za svaki pojedinačni poslovni proces, imajući u vidu eksternalizaciju i ovisnost od trećim osobama.
(4) Pri procesu planiranja kontinuiteta poslovanja, banka je dužna definirati procese, uloge i odgovornosti, a kako bi osigurala da su eksternalizirani dijelovi informacijskog sustava i servisi adekvatno pokriveni planovima kontinuiteta poslovanja. Banka je dužna uzeti u obzir ovisnost o uslugama trećih osoba.
(5) Na temelju analize utjecaja na poslovanje, banka je dužna definirati i usvojiti plan(ove) oporavka informacijskog sustava kojim će omogućiti raspoloživost resursa, definirati prioritete oporavka poslovnih procesa, kao i potrebne resurse i sustave, te detaljno opisati 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 informacijskog sustava treba, kao minimum, sadržavati:
   a) detaljne procedure i upute za oporavak resursa informacijskog sustava potrebnih za odvijanje kritičnih (ključnih) poslovnih procesa u slučaju izvanrednih situacija;

b) definirane prioritete oporavka resursa informacijskog sustava, kao i popis svih resursa potrebnih za ponovno uspostavljanje kritičnih (ključnih) poslovnih procesa;
c) podatke o timovima koji će biti odgovorni za oporavak informacijskog sustava, njihovim članovima s jasno definiranim dužnostima i odgovornostima;
d) podatke o lokaciji za oporavak informacijskog sustava;
e) podatke o ključnim pružateljima usluga.

(7) Uprava banke treba osigurati da je plan oporavka informacijskog sustava ažuran.

Članak 31.

(1) Banka je dužna, sukladno procjeni rizika i na temelju rezultata analize utjecaja na poslovanje, osigurati raspoloživost rezervnog informatičkog centra koji je na odgovarajućoj udaljenosti od primarnog informatičkog centra, uzimajući u obzir rizik da pojedinačni scenarij, incident ili katastrofa ne mogu istodobno utjecati na produkcijski sustav banke i sustave oporavka.
(2) Efektivna funkcionalnost rezervnog informatičkog centra treba biti potvrđena najmanje jednom godišnje, kao i poslije implementiranih značajnih promjena u informacijskom sustavu banke. Rezultate navedenog testiranja je potrebno dokumentirati i osigurati da je izvješće o rezultatima testiranja usvojeno od strane uprave banke. U okviru navedenog testiranja, banka je dužna uzeti u obzir različite realne scenarije uključujući cyber napade, prekide komunikacijskih 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 u slučaju nastanka okolnosti koje zahtijevaju primjenu plana oporavka informacijskog sustava odmah obavijestiti Agenciju o svim relevantnim činjenicama i okolnostima koje se na to odnose.

Članak 32.

(1) U slučaju eksternalizacije cjelokupnog ili dijela informacijskog sustava izvan teritorija Bosne i Hercegovine, banka je dužna sljedeće:
a) definirati kritične (vitalne) procese sa stajališta kontinuiteta poslovanja i odvijanja istih u zemlji;
b) osigurati lokalni informatički centar na teritoriju Bosne i Hercegovine kako bi osigurala raspoloživost podataka i mogućnost odvijanja kritičnih (vitalnih) procesa u zemlji definiranih u okviru stavka (1) točka a) ovoga članka;
c) provoditi testiranje funkcionalnosti lokalnog informatičkog centra najmanje na godišnjoj razini, te osigurati da je izvješće o rezultatima testiranja usvojeno od strane uprave banke;
d) osigurati ažurnost podataka u lokalnom informatičkom centru na dnevnoj osnovi;
e) osigurati podatke u lokalnom informatičkom centru, u skladu s važećim zakonskim propisima.

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

Članak 33.

Prijelazne i završne odredbe

(1) Direktor Agencije će u roku od 60 (šezdeset) dana od dana stupanja na snagu ove odluke donijeti Uputu za izvješćivanje o upravljanju informacijskim sustavima, kojim će se detaljnije propisati izvješćivanje, način i metodologija popunjavanja obrazaca, koji su sastavni dio navedene Upute.
(2) Banka je dužna uskladiti svoje poslovanje s odredbama ove odluke sukladno članku 250. stavak (1) Zakona o bankama, izuzev članka 17. stavak (2), članka 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 članka 16., koji se primjenjuju 360 dana od dana stupanja na snagu ove odluke.

(3) Banka je dužna sačiniti prva kvartalna izvješća za I. kvartal 2018. godine i prva godišnja izvješća za 2017. godinu i dostaviti ih Agenciji sukladno Uputi iz stavka (1) ovoga članka.
(4) Stupanjem na snagu ove odluke, prestaje važiti Odluka o minimalnim standardima upravljanja informacijskim sustavima u bankama („Službene novine Federacije BiH“, broj: 1/12).

Članak 34.
Stupanje na snagu

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

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

PREDSJEDNICA
UPRAVNOG ODBORA

mr. sc. Ljerka Marić, dipl.oec., s.r.