Na osnovu člana 81. Zakona o bankama ("Službene novine Federacije BiH", broj 27/17) i čl. 5. stav (1) tačka h) i 19. stav (1) tačka c) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", broj 75/17) i člana 12. stav (1) tačka d) Statuta Agencije za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj 3/18), Upravni odbor Agencije za bankarstvo Federacije Bosne i Hercegovine, na sjednici održanoj 25.02.2025. godine donosi

ODLUKU
O UPRAVLJANJU INFORMACIONO-KOMUNIKACIONIM SISTEMOM I IKT RIZIKOM U BANCI

I OPĆE ODREDBE

Član 1.
Predmet Odluke

(1) Odlukom o upravljanju informaciono-komunikacionim sistemom i IKT rizikom u banci propisuju se uslovi koje je banka dužna osigurati i provoditi u procesu upravljanja informaciono-komunikacionim sistemom, upravljanja rizicima informacione-komunikacione tehnologije, uključujući zahtjeve koji se odnose na ugovorne aranžmane i nadzor nad trećim stranama koje pružaju informaciono-komunikacione usluge, pravovremeno izvještavanje o značajnim informaciono-komunikacionim incidentima i cyber prijetnjama, testiranje digitalne operativne otpornosti i razmjenu informacija o cyber prijetnjama.
(2) Ova odluka se primjenjuje na banke sa sjedištem u Federaciji Bosne i Hercegovine (u daljem tekstu: FBiH) kojima je Agencija za bankarstvo Federacije Bosne i Hercegovine (u daljem tekstu: Agencija) izdala dozvolu za rad.
(3) Banka je dužna primjenjivati odluku na pojedinačnoj i konsolidovanoj osnovi.
(4) Na pitanja koja nisu regulirana ovom odlukom, a koja se odnose na upravljanje informaciono-komunikacionim sistemom i rizicima informaciono-komunikacionih tehnologija, primjenjuju se odredbe drugih važećih propisa.

Član 2.
Pojmovi - Definicije

Pojedini pojmovi koji se koriste u ovoj odluci imaju sljedeće značenje:

a) **Analiza isplativosti (eng. cost-benefit analysis)** – metoda ekonomske analize kojom se upoređuju i vrednuju sve prednosti i svi nedostaci projekta analizom troškova i koristi.
b) **Analiza utjecaja na poslovanje (eng. business impact analysis - BIA)** – analiza pomoću koje se ocjenjuju kvantitativni i kvalitativni efekti koji bi mogli nastati u slučaju nedostupnosti poslovnih procesa i resursa IKT sistema uslijed određenog incidenta, neželjenog događaja ili havarije. Cilj analize utjecaja na poslovanje je identifikacija prioritetnih poslovnih funkcija, procesa i resursa IKT sistema kao dijela procesa upravljanja kontinuitetom poslovanja.
c) **Autentičnost** – svojstvo koje osigurava tačnost identiteta korisnika ili podataka, potvrđujući da je osoba ili podatak tačan.
d) **Autentifikacija** – proces verifikacije identiteta korisnika, sistema ili uređaja, koji osigurava da lice ili objekat koji traži pristup podacima ili sistemima zaista jeste ono za koga se predstavlja.

e) **Ciljana tačka oporavka podataka (eng. recovery point objective (RPO)) –** određuje se na osnovu prihvatljivog gubitka podataka u slučaju prekida operacija; najduže prihvatljivo vrijeme gubitka podataka u slučaju incidenta; RPO efikasno kvantificira dozvoljenu količinu gubitka podataka u slučaju prekida.
f) **Ciljani nivo oporavka usluge (eng. service delivery objective (SDO))** – nivo usluga koji se mora osigurati alternativnim metodama procesiranja do povratka na normalno funkcioniranje.
g) **Ciljano vrijeme oporavka (eng. recovery time objective (RTO))** – najduže prihvatljivo vrijeme neraspoloživosti poslovnog procesa banke i resursa IKT sistema potrebnih za odvijanje poslovnog procesa, odnosno vrijeme tokom koga je potrebno obnoviti poslovni proces.
h) **Cyber napad** – zlonamjeran utjecaj sa ciljem ugrožavanja informacione sigurnosti koji može rezultirati IKT incidentom.
i) **Cyber sigurnost** – sve aktivnosti koje su neophodne za zaštitu od cyber prijetnji IKT sistema, korisnika tih sistema i drugih osoba na koje one utječu.
j) **Digitalna operativna otpornost** – sposobnost banke da izgradi, osigura i preispituje svoj operativni integritet, kontinuitet i pouzdanost svojih IKT sistema i procesa, tako da upotrebom usluga koje pružaju treće strane, pružaoci IKT usluga direktno ili indirektno osigura cijeli raspon IKT sposobnosti potrebnih za sigurnost IKT sistema kojima se banka koristi i kojima se podržava kontinuirano pružanje finansijskih usluga i njihova kvaliteta, među ostalim i tokom poremećaja.
k) **Dokazivost (sljedivost)** – osobina koja osigurava da svaka aktivnost u IKT sistemu može biti jednoznačno praćena do njenog izvora.
l) **Dostupnost** – osobina da informacija i proces bude pravovremeno dostupni i iskoristivi na zahtjev od strane ovlaštenog lica.
m) **Hardverske komponente (hardverska imovina)** – fizičke komponente IKT sistema koje uključuju: računare i računarsku opremu, komunikacijsku opremu, medije za čuvanje podataka, te ostalu tehničku opremu koja podržava rad IKT sistema.
n) **IKT imovina** – softverska ili hardverska imovina koja se nalazi u poslovnom okruženju.
o) **IKT proces** – skup aktivnosti koje se provode radi oblikovanja, razvoja, ostvarivanja ili održavanja IKT proizvoda ili IKT usluge.
p) **IKT proizvod** – element ili skupina elemenata IKT sistema.
q) **IKT projekat** – svaki projekat u kojem se IKT sistemi i/ili usluge mijenjaju, zamjenjuju, odbacuju ili implementiraju. IKT projekti mogu biti dio širih IKT programa ili programa transformacije poslovanja.
r) **IKT usluge** – usluge koje IKT sistem pruža korisnicima informacionog sistema. Primjeri obuhvataju unos, smještaj i obradu podataka, kao i usluge izvještavanja, te nadzor i usluge za potrebe podrške poslovanju i odlučivanju.
s) **Incident** – događaj koji ugrožava dostupnost, autentičnost, dokazivost, integritet ili povjerljivost snimljenih, prenesenih ili obrađenih podataka ili usluga koje IKT sistemi nude ili kojima omogućuju pristup.
t) **Informaciona imovina** – skup informacija u materijalnom i nematerijalnom obliku koje imaju vrijednost za organizaciju i koje je potrebno zaštititi.
u) **Informacioni i komunikacioni sistem (u daljem tekstu: IKT sistem) –** jeste informaciona i komunikaciona tehnologija koja je uređena kao dio mehanizma ili međusobno povezane mreže kojima se pruža podrška poslovanju banke.
v) **Informaciona i komunikaciona tehnologija (u daljem tekstu: IKT)** – jeste tehnologija koja omogućava automatizirano prikupljanje, obradu, generisanje, spremanje, prijenos, prikaz i distribuciju informacija te raspolaganje njima.
w) **Integritet** – osobina podataka i procesa da nisu neovlašteno ili nepredviđeno mijenjani, u svim fazama životnog ciklusa podataka.

x) **Izbjegnuti incident** – svaki događaj koji je mogao ugroziti dostupnost, autentičnost, dokazivost, integritet ili povjerljivost snimljenih, prenesenih ili obrađenih podataka ili usluga koje IKT sistemi nude ili kojima omogućuju pristup, ali je uspješno spriječen ili se nije ostvario.
y) **Kontrole** – politike, procedure, postupci, prakse, mehanizmi, tehnologije i organizacione strukture dizajnirane kako bi osigurale razumno uvjerenje da će poslovni ciljevi biti dostignuti i da će neželjeni događaji biti spriječeni ili detektovani.
z) **Sigurnosne kopije** – kopija izvornih podataka (informaciona imovina, softverske komponente) koji su potrebni za ponovno uspostavljanje poslovnih procesa banke, te ostalih podataka za koje banka procjeni da ih je potrebno čuvati.
aa) **Korisnici IKT sistema** – sva lica koja koriste IKT sistem (zaposlenici banke, pružalac usluga, klijenti banke i drugo).
bb) **Korisnički zahtjev** – zahtjev od strane korisnika IKT sistema za pristup određenim resursima IKT sistema ili IT uslugama, zahtjev za informacijama ili savjetom, te ostale vrste zahtjeva koji ne spadaju u kategoriju incidenata ili promjena unutar IKT sistema.
cc) **Lanac čuvanja svih povezanih dokaza –** proces korišten za praćenje kretanja i kontrolu resursa kroz njegov životni vijek na način dokumentovanja svake osobe i organizacije koja rukuje resursom, datum/vrijeme kada je skupljena ili prebačena i razlog prebacivanja.
dd) **Maksimalno prihvatljivo vrijeme zastoja (eng. maximum tolerable downtime (MTD))** – najduži vremenski period u kojem poslovni proces banke može biti nedostupan (u zastoju) prije nego što njegov utjecaj postane neprihvatljiv za banku.
ee) **Neporecivost** – osobina koja osigurava nemogućnost poricanja izvršene aktivnosti ili primanja informacija (podataka).
ff) **Operativni ili sigurnosni incident (u daljem tekstu: IKT incident) –** jedan događaj ili niz povezanih događaja koje banka nije planirala, a koji imaju ili će vjerovatno imati negativan utjecaj na integritet, dostupnost, dokazivost, povjerljivost i/ili autentičnost usluga.
gg) **Operativni i sistemski zapisi** – hronološki zapisi o aktivnostima na IKT imovini (na primjer: zapisi operativnih sistema, aplikativnog softvera, baza podataka, mrežnih uređaja i slično).
hh) **Organi banke u smislu ove odluke su:** „nadzorni odbor“ i „uprava banke“.
ii) **Ozbiljna cyber prijetnja –** cyber prijetnja za koju se na osnovu njezinih tehničkih karakteristika može pretpostaviti da može imati ozbiljan utjecaj na IKT sisteme banke ili korisnike usluga banke uzrokovanjem znatne materijalne ili nematerijalne štete.
jj) **Penetracijska testiranja vođena prijetnjama (TLPT) –** okvir koji oponaša taktike, tehnike i procedure stvarnih aktera prijetnje koje se smatraju stvarnom cyber prijetnjom, koji omogućuje kontrolisano, prilagođeno testiranje ključnih produkcijskih sistema banke, vođeno saznanjima o prijetnjama („crveni tim”).
kk) **Postupanje s incidentom –** sve radnje i postupci čiji je cilj sprečavanje, otkrivanje, analiza, zaustavljanje incidenta ili odgovor na njega te oporavak od incidenta.
ll) **Pouzdanost** – označava da IKT sistem dosljedno i očekivano vrši predviđene funkcije i pruža tačne informacije.
mm) **Povjerljivost** – osobina da informacija nije dostupna ili otkrivena neovlaštenim licima ili procesima.
nn) **Prioritetni dio IKT sistema –** dio IKT sistema koji podržava prioritetnu funkciju i uslugu i provedbu kontrola od strane Agencije u slučaju rane intervencije ili restrukture.
oo) **Prioritetna funkcija –** funkcija čiji bi poremećaj bitno narušio finansijske rezultate banke ili pouzdanost ili kontinuitet njenih usluga i aktivnosti, odnosno funkcija čiji bi prestanak, neispravnost ili neizvršenje bitno narušili sposobnost banke da kontinuirano

ispunjava uslove i obaveze iz svog odobrenja za rad ili druge obaveze na osnovu primjenjivog prava o finansijskim uslugama.

pp) **Promjena** – izmjena podataka ili postojećih funkcionalnosti IKT sistema.

qq) **Pružalac IKT usluga unutar grupe –** društvo koje je dio finansijske grupe i koje uglavnom pruža IKT usluge finansijskim subjektima unutar iste grupe ili finansijskim subjektima koji pripadaju istom institucionalnom sistemu zaštite, među ostalim i njihovim matičnim društvima, društvima kćerima, podružnicama ili drugim subjektima koji su u zajedničkom vlasništvu ili pod zajedničkom kontrolom.

rr) **Ranjivost –** slabost, osjetljivost ili nedostatak IKT proizvoda ili IKT usluga koje cyber prijetnja može iskoristiti.

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

tt) **Razvoj** – uvođenje novih funkcionalnosti IKT sistema.

uu) **Resursi IKT sistema** – resursi koji uključuju informacionu imovinu, softverske i hardverske komponente, ljude i procese.

vv) **Rizik** – mogućnost gubitka ili poremećaja uzrokovana incidentom i treba ga izražavati kao kombinaciju obima takvog gubitka ili poremećaja i vjerovatnoće pojave tog incidenta.

ww) **Rizik informacionih i komunikacijskih tehnologija i sigurnosni rizik (u daljem tekstu: IKT rizik) -** rizik gubitka uslijed povrede povjerljivosti, gubitka integriteta sistema i podataka, neprikladnosti ili nedostupnosti sistema i podataka ili nemogućnosti promjene IKT unutar razumnog vremenskog roka i uz razumne troškove u slučaju promjene zahtjeva iz okruženja ili poslovanja (osobina prilagodljivosti). Navedeno obuhvata i sigurnosne rizike koji proizlaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući cyber napade ili neadekvatnu fizičku zaštitu.

xx) **Sigurnost IKT sistema** – sposobnost IKT sistema da na određenom nivou pouzdanosti odolijevaju svim događajima koji mogu ugroziti dostupnost, autentičnost, dokazivost, integritet ili povjerljivost snimljenih, prenesenih ili obrađenih podataka ili usluga koje ti IKT sistemi nude ili kojima omogućavaju pristup.

yy) **Sigurnost informacija** – osigurava da samo ovlašteni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).

zz) **Saznanja o prijetnjama** – znači informacije koje su agregirane, preoblikovane, analizirane, protumačene ili obogaćene kako bi se dobio kontekst potreban za donošenje odluka i kako bi se omogućilo relevantno i potrebno razumijevanje za ublažavanje utjecaja IKT incidenta ili cyber prijetnje, uključujući tehničke pojedinosti cyber napada, onih koji su odgovorni za napad te njihova načina rada i njihovih motiva.

aaa) **Softverske komponente (softverska imovina)** – uključuju aplikacijski softver, sistemski softver, baze podataka, softverske razvojne alate, uslužne programe, te ostali softver.

bbb) **Treća strana** – organizacija (pravno ili fizičko lice) koja je uspostavila poslovne odnose ili sklopila ugovore sa bankom u svrhu pružanja proizvoda ili usluge banci.

ccc) **Zastarjeli IKT sistem** – IKT sistem koji je na kraju svog životnog ciklusa, a koji zbog tehnoloških ili komercijalnih razloga nije pogodan za nadogradnju ili popravak ili za koji njegov dobavljač ili treća strana pružalac IKT usluga više ne pruža podršku, ali je još uvijek u upotrebi i podržava funkcije banke.

II ODGOVORNOSTI

Član 3.
Interni akti

(1) Banka je dužna donijeti i primjenjivati interne akte, u vidu strategija, politika, metodologija, procedura i radnih uputa, kojima se uređuje upravljanje IKT sistemom, uključujući upotrebu, praćenje i nadzor IKT sistema.
(2) Interni akti iz stava (1) ovog člana, kao minimum, trebaju biti:
   a) usklađeni sa važećim propisima, standardima i pravilima struke, te međusobno usklađeni kako bi se osigurala konzistentnost i cjelovitost,
   b) redovno pregledani i ažurirani,
   c) potpuni, detaljni i primjenjivi.
(3) Potrebno je osigurati da su svi korisnici IKT sistema upoznati sa sadržajem internih akata vezanim uz IKT sistem, u skladu sa potrebama i ovlaštenjima svakog korisnika.
(4) Ugovori, nalazi revizije, izvještaji koje razmatraju organi banke, uputstva i ostali dokumenti trebaju biti sačinjeni odnosno prevedeni na jedan od jezika u zvaničnoj upotrebi u Federaciji Bosne i Hercegovine.

Član 4.
Odgovornosti nadzornog odbora

(1) Nadzorni odbor banke dužan je, kao minimum, da:
   a) uspostavi, održava i unapređuje efikasan proces upravljanja IKT sistemom, u cilju implementacije sigurnog, pouzdanog i efikasnog IKT sistema u banci,
   b) uspostavi, održava i unapređuje proces upravljanja IKT rizikom, kao dio jedinstvenog procesa upravljanja rizicima banke,
   c) odlučuje o adekvatnoj organizacionoj strukturi banke sa jasnom i preciznom podjelom nadležnosti, dužnosti i odgovornosti, a kako bi se osiguralo efikasno i sigurno upravljanje IKT sistemom i IKT rizicima, uključujući upravljanje sigurnošću IKT sistema, upravljanje rizicima trećih strana pružaoca IKT usluga, upravljanje IKT incidentima, upravljanje kontinuitetom poslovanja i internom revizijom IKT sistema, te efikasnu i pravovremenu komunikaciju, saradnju i koordinaciju među navedenim funkcijama,
   d) u okviru organizacione strukture banke, utvrđuje jasne uloge i odgovornosti, stručne kvalifikacije i potrebne kompetencije, osiguravajući da su broj i potrebne vještine zaposlenika banke adekvatni za pružanje podrške efikasnom i sigurnom funkcioniranju IKT sistema i upravljanju IKT rizicima, uključujući i rizike upravljanja trećim stranama, na kontinuiranoj osnovi,
   e) donosi i periodično preispituje odgovarajući budžet za ispunjavanje potreba banke za osiguravanje efikasnog, sigurnog i pouzdanog IKT sistema, te adekvatnog nivoa digitalne operativne otpornosti, u pogledu svih vrsta resursa, uključujući i relevantne programe za podizanje svijesti o sigurnosti IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti, te sticanja znanja i vještina u području IKT i IKT sigurnosti,
   f) usvaja ključne strateške akte i politike koje se odnose na IKT sistem i upravljanje IKT rizicima, a najmanje:
      1) Strategiju IKT sistema,
      2) Strategiju kontinuiteta poslovanja,
      3) Politiku za upravljanje IKT rizicima,
      4) Politiku informacione sigurnosti,
      5) Politiku upravljanja IKT incidentima,
      6) Politiku za testiranje digitalne operativne otpornosti,
      7) Politiku o korištenju IKT usluga trećih strana,

uslove za njihovo provođenje, nadzire njihovo provođenje i najmanje jednom godišnje analizira iste, te ih prilagođava promjenama, uzimajući u obzir poslovni model banke, kompleksnost IKT sistema i sklonost ka preuzimanju rizika.

g) propiše sadržaj i periodičnost izvještavanja nadzornog odbora u vezi sa:
   1) upravljanjem IKT sistemom, uključujući izvještavanje o realizaciji operativnih planova, te najmanje o značajnim IKT incidentima, kao i odgovorima, oporavku i korektivnim mjerama,
   2) upravljanjem IKT rizicima, uključujući izvještaje o sigurnosti IKT sistema i stepenu digitalne operativne otpornosti,
   3) ugovorima sklopljenim sa trećim stranama, pružaocima IKT usluga, svim relevantnim planiranim materijalnim promjenama u vezi sa njima, te potencijalnom utjecaju tih promjena na prioritetne funkcije koje su podložne tim ugovorima, uključujući sažetak analize rizika za procjenu utjecaja tih promjena.

(2) U zavisnosti od veličine i ukupnog profila rizičnosti, te prirode, obima i složenosti svojih usluga, aktivnosti i poslovanja, unutrašnje organizacije, veličine i kompleksnosti IKT sistema, funkcija upravljanja IKT rizicima uspostavlja se kao izdvojena funkcija ili u okviru funkcije kontrole rizika.

Član 5.
Odgovornosti uprave banke

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

a) osigura uslove za provođenje efikasnog procesa upravljanja IKT sistemom, u skladu sa članom 4. tačka a) i strategijama i politika koje donosi nadzorni odbor,
b) osigura uslove za provođenje procesa upravljanja IKT rizikom, u skladu sa članom 4. tačka b),
c) priprema prijedloge strategija i politika iz člana 4. tačka f) ove odluke za usvajanje od strane nadzornog odbora, osigura provođenje usvojenih strategija i politika na svim nivoima odlučivanja i u poslovnim procesima, te redovno izvještava nadzorni odbor o njihovom provođenju,
d) donosi i provodi procedure upravljanja IKT sistemom i IKT rizicima, u skladu sa poslovnim ciljevima i poslovnom strategijom banke, a koje osiguravaju održavanje standarda dostupnosti, autentičnosti, integriteta, povjerljivosti i dokazivosti podataka, definiranih Strategijom IKT sistema,
e) sprovodi uspostavljeni proces upravljanja IKT rizikom, osigurava njegovo održavanje i kontinuirano unapređenje u skladu s politikama i strategijama koje je usvojio Nadzorni odbor, te integriše upravljanje IKT rizikom u jedinstveni proces upravljanja rizicima banke,
f) na osnovu procjene ukupnog profila rizičnosti banke, te obima i složenosti njenih poslovnih operacija, redovno preispituje rizike koji su utvrđeni u vezi sa ugovornim aranžmanima o upotrebi IKT usluga kojima se podržavaju prioritetne funkcije,
g) prati izvršenje operativnih planova provođenja Strategije IKT sistema, kao i bitnih izmjena,
h) implementira organizaciju i odgovornosti vezane uz upravljanje IKT sistemom, osiguravajući da su uloge jasno definirane i dodijeljene u skladu sa smjernicama koje je uspostavio Nadzorni odbor, pri čemu se posebna pažnja posvećuje adekvatnoj segregaciji dužnosti radi minimiziranja rizika i osiguravanja efikasnog upravljanja,
i) efikasno upravlja resursima za upravljanje IKT sistemom i IKT rizicima, uključujući i IKT rizike povezane sa trećim stranama pružaocima IKT usluga, te osigura optimalno korištenje ljudskih, finansijskih i tehničkih resursa u skladu s poslovnim potrebama, kao i osigurava da dostupni resursi budu adekvatno raspoređeni za realizaciju operativnih zadataka i implementaciju Strategije IKT sistema,

j) uspostavi i implementira odgovarajući sistem izvještavanja o upravljanju IKT sistemom, IKT rizicima i rizicima povezanim sa trećim stranama pružaocima IKT usluga,
k) uspostavi funkciju za praćenje aranžmana o upotrebi IKT usluga sklopljenih sa trećim stranama pružaocima IKT usluga ili imenuju člana višeg rukovodstva koji će biti odgovoran za nadzor nad povezanim izloženostima rizicima i relevantnom dokumentacijom,
l) osigura da svi članovi osoblja, uključujući i nositelje ključnih funkcija, prođu odgovarajuće osposobljavanje o IKT rizicima, uključujući i sigurnost informacija i IKT sistema, na godišnjoj osnovi ili češće, ako je to potrebno i
m) donosi procedure i interne akte vezane uz upravljanje IKT sistemom i IKT rizicima, a najmanje:
   1) Operativne planove provođenja Strategije IKT sistema,
   2) Procedure za upravljanje IKT rizicima,
   3) Procedure za testiranje digitalne operativne otpornosti,
   4) Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, te Analizu utjecaja na poslovanje (eng. BIA),
   5) Procedure upravljanja IKT incidentima,
   6) Procedure upravljanja sigurnosnim i zaštitnim (regulatornim) kopijama,
   7) Procedure upravljanja pristupom IKT sistemu,
   8) Procedure za upravljanje ažuriranjima softvera,
   9) Procedure za upravljanje zaštitom od malicioznog softvera,
   10) Procedure upravljanja IKT imovinom,
   11) Metodologiju upravljanja IKT projektima,
   12) Procedure nabavke, razvoja i održavanja IKT sistema,
   13) Procedure upravljanja IKT promjenama,
   14) Procedure upravljanja zapisima IKT sistema,
   15) Plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema,
   16) Plan edukacije zaposlenika,
   17) Planove komunikacije u krizi

   i ostale interne akte koji se odnose na specifične oblasti upravljanja IKT sistemom.

(2) Član/članovi uprave banke odgovorni za upravljanje IKT sistemom i IKT rizikom dužni su posjedovati odgovarajući nivo znanja i vještina koji im omogućava razumijevanje i procjenu IKT rizika i njegovog utjecaja na poslovanje banke, kao i kontinuirano se educirati i pratiti specijalizirane obuke, razmjerno veličini i složenosti IKT rizika kojim upravljaju.

(3) Uprava banke je dužna srazmjerno veličini, vrsti, obimu i složenosti IKT sistema, kao i prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, procijeniti potrebni broj zaposlenika u funkciji upravljanja IKT rizicima.

(4) Uprava banke je dužna imenovati najmanje jedno lice zaduženo za provođenje komunikacijskih planova za IKT incidente koje u tu svrhu ispunjava funkciju komunikacije s javnošću i medijima.

(5) Uprava banke je dužna razmotriti potrebu formiranja posebnog tijela za potrebe koordinacije aktivnosti vezanih uz IKT sistem, uzimajući u obzir veličinu banke, prirodu, obim i složenosti svojih usluga, aktivnosti i poslovanja, unutrašnju organizaciju, te veličinu i kompleksnost IKT sistema.

Član 6.
Funkcija upravljanja IKT rizicima

(1) U okviru funkcije upravljanja IKT rizicima, banka je dužna osigurati zaposlenike sa odgovarajućim stručnim kvalifikacijama, specijalističkim znanjima i praktičnim iskustvima iz oblasti upravljanja i procjene IKT rizika i IKT sigurnosti, koji posjeduju relevantne,

međunarodno priznate certifikate iz oblasti upravljanja IKT rizicima i IKT sigurnosti, uz obavezu kontinuiranog stručnog usavršavanja i praćenja razvoja u oblasti IKT sigurnosti.

(2) Funkcija upravljanja IKT rizicima je dužna obavljati poslove kontrolne funkcije upravljanja rizicima u skladu sa propisom Agencije kojim se reguliraju obaveze i odgovornosti kontrolne funkcije upravljanja rizicima, uključujući i nadziranje i koordiniranje aktivnosti vezanih uz sigurnost IKT sistema, a što uključuje minimalno sljedeće:
   a) ispitivanje i ocjenu adekvatnosti, efikasnosti i usklađenosti internih kontrola sa ovom odlukom u procesu upravljanja IKT rizicima,
   b) nadzor i analizu IKT sistema, sa ciljem otkrivanja sigurnosnih prijetnji i ranjivosti,
   c) aktivnosti identifikacije i procjene IKT rizika, kao i pružanju prijedloga mjera za ovladavanje IKT rizicima, iz čl. 15. - 19. ove odluke,
   d) izradu Politike informacione sigurnosti, iz člana 17. ove odluke, te prijedloga za njeno unapređenje, u skladu sa razvojem IKT sistema i IKT rizika u banci,
   e) praćenje promjena u IKT sistemu i analizu utjecaja promjena u IKT sistemu na postojeće kontrole IKT sigurnosti, davanje prijedloga za uvođenje novih kontrola sigurnosti IKT sistema, uključujući i analizu utjecaja IKT projekata i razvoja novih funkcionalnosti,
   f) osiguravanje, praćenje i koordiniranje aktivnosti iz okvira za testiranje informacione sigurnosti,
   g) osiguravanje adekvatnih i pravovremenih aktivnosti razmjene informacija o IKT incidentima i cyber prijetnjama, definiranih članom 52. ove odluke,
   h) procjena IKT rizika i predlaganje mjera ovladavanja IKT rizicima u slučaju angažovanja trećih strana pružaoca IKT usluga,
   i) praćenje IKT rizika koji proizlaze iz korištenja usluga trećih strana pružaoca IKT usluga,
   j) osiguravanje, praćenje i koordiniranje aktivnosti vezanih uz realizaciju programa podizanja svijesti o sigurnosti IKT sistema,
   k) učestvovanje u radu odbora i radnih grupa koji su formirani za potrebe upravljanja IKT sistemom i IKT rizicima,
   l) redovno izvještavanje organa banke o aktivnostima vezanim uz stanje IKT rizika, a najmanje na kvartalnoj osnovi.

(3) Zaposlenici u funkciji upravljanja IKT rizicima su dužni:
   a) svoju profesionalnu kompetentnost održavati putem sistemske i kontinuirane obuke, te se pravovremeno educirati o rizicima IKT sistema i tehnologijama koje se koriste u banci,
   b) poznavati relevantne međunarodne standarde i smjernice koje se odnose na uspostavu i nadzor upravljanja rizicima i sigurnosti IKT sistema,
   c) biti upućeni u najnovije prakse upravljanja sigurnosnim IKT incidentima, kako bi bili u mogućnosti efikasno odgovoriti na trenutne ili nove oblike cyber napada,
   d) pratiti relevantna tehnološka dostignuća kako bi bolje razumjeli mogući utjecaj koje bi uvođenje novih tehnologija moglo imati na zahtjeve u pogledu IKT sigurnosti.

Član 7.
Interna revizija IKT sistema

(1) Banka je dužna provoditi internu reviziju IKT sistema i sistema upravljanja IKT rizicima, u skladu sa propisima Agencije koji reguliraju sistem internog upravljanja u banci, a na osnovu definiranog programa rada interne revizije.

(2) Banka je dužna planirati i provoditi internu reviziju IKT sistema u skladu sa metodologijom procjene IKT rizika interne revizije, imajući u vidu da u određenim vremenskim intervalima budu detaljno revidirani svi elementi okvira za upravljanje IKT rizicima i svi IKT procesi, a naročito oni koji podržavaju prioritetne funkcije, te kontrole kojima se osigurava visoka digitalna otpornost banke, a proporcionalno IKT rizicima banke.

(3) Lica koja obavljaju internu reviziju IKT sistema banke trebaju posjedovati adekvatna stručna znanja i vještine neophodne za obavljanje revizije IKT sistema i upravljanja IKT rizicima, a uzimajući u obzir veličinu i kompleksnost IKT sistema u banci.
(4) Funkcija interne revizije je dužna na adekvatan način prikupljati i dokumentovati revizorske dokaze na osnovu kojih je donesena ocjena adekvatnosti i efikasnosti kontrola u okviru oblasti koja je predmet revizije, uključujući i podatke o revidiranim internim aktima, IKT procesima, efikasnosti uspostavljenih mjera i testiranim uzorcima.
(5) Banka je dužna propisati postupke za upravljanje u vezi sa kašnjenjem u izvršavanju naloženih mjera od strane interne revizije IKT sistema.

Član 8.
Eksterna revizija IKT sistema

(1) Banka je dužna obavljati eksternu reviziju IKT sistema u skladu sa propisima Agencije koji reguliraju oblast eksterne revizije u bankama, ukoliko odredbama ove odluke nije drugačije definirano.
(2) Ako Agencija utvrdi da eksterna revizija IKT sistema nije adekvatno provedena ili da revizorski izvještaj nije sačinjen u skladu sa zakonom, podzakonskim aktima donesenim na osnovu zakona, propisa kojim se uređuje računovodstvo i revizija i pravilima revizorske struke ili ako obavljenom supervizijom poslovanja banke ili na drugi način se utvrdi da revizorska ocjena nije zasnovana na istinitim i objektivnim činjenicama, Agencija može odbiti revizorski izvještaj i zahtijevati od banke da reviziju obave ovlašteni revizori drugog društva za reviziju ili, kada to ocijeni potrebnim, sama direktno imenuje revizora na trošak banke.
(3) Društvo za reviziju banke i ovlašteni revizor koji obavlja reviziju banke ne može biti lice čiji izvještaj o obavljenoj reviziji IKT sistema Agencija nije prihvatila za prethodnu poslovnu godinu.
(4) Izvještaj o obavljenoj reviziji IKT sistema je poseban izvještaj, te je banka dužna dostaviti Agenciji navedeni izvještaj najkasnije do 31. marta tekuće godine.
(5) Banka je dužna da reviziju IKT sistema obavlja na godišnjem nivou.
(6) Agencija zadržava pravo da nalaže mjere propisane Zakonom o bankama i propisima Agencije koji reguliraju eksternu reviziju u bankama.

III UPRAVLJANJE IKT SISTEMOM

Član 9.
Strategija IKT sistema

(1) Banka je dužna:
   a) razviti i nadzirati provođenje Strategije IKT sistema,
   b) definirati operativne planove koji podržavaju provođenje Strategije IKT sistema,
   c) uspostaviti postupke praćenja i mjerenja efikasnosti provođenja Strategije IKT sistema.
(2) Strategija IKT sistema iz stava (1) ovog člana, treba da:
   a) definira povezanost i usklađenost strateških ciljeva IKT sistema sa poslovnim ciljevima banke,
   b) definira dugoročne i kratkoročne inicijative unapređenja IKT sistema banke, koje opisuju način na koji bi se IKT sistem banke trebao razvijati radi efikasnog pružanja podrške i sudjelovanja u realizaciji poslovne strategije banke, uključujući razvoj organizacione strukture, promjene IKT sistema, uključujući i IKT arhitekturu, te ključne zavisnosti o trećim stranama,
   c) izloži pristup upravljanju IKT incidentima, uključujući odgovorne osobe i specifične timove zadužene za provođenje tih aktivnosti,

d) sadrži opis planova komunikacije u slučaju IKT incidenata,
e) definira kako se okvirom za upravljanje IKT rizicima podržava poslovna strategija banke i njeni ciljevi,
f) utvrdi toleranciju na IKT rizik, u skladu sa sklonošću preuzimanja rizika banke, te analizira utjecaj tolerancije prilikom poremećaja u radu IKT sistema,
g) definira jasne ciljeve u području informacione i IKT sigurnosti, uključujući dostupnost, povjerljivost, integritet, dokazivost podataka i IKT sistema, kao i ključne pokazatelje uspješnosti i ključne parametre rizika,
h) definira pristup banke vezan za IKT rizik povezan sa trećim stranama, pružaocima IKT usluga, uključujući procjenu sigurnosnih i operativnih rizika povezanih sa trećim stranama.

(3) Banka je dužna Strategiju IKT sistema periodično ažurirati, a posebno prilikom izmjene poslovne strategije banke i značajnih promjena u strategiji za upravljanje rizicima, uključujući i IKT rizike, a kako bi se osigurala kontinuirana usklađenost između poslovnih ciljeva i ciljeva IKT sistema, kao i odgovarajućih planova i aktivnosti.

Član 10.
Operativni planovi

(1) Operativni planovi iz člana 9. stav (1) tačka b) ove odluke treba da:
a) detaljnije definiraju aktivnosti koje će banka poduzeti kako bi se postigli ciljevi strategije iz člana 9. stav (2) ove odluke,
b) sadrže kao minimum sljedeće elemente: opis aktivnosti i projekata IKT sistema, uključujući i implementaciju mjera koje proizlaze iz procjene IKT rizika, planirane ugovore sa trećim stranama pružaocima IKT usluga, ljudske resurse, budžet, vremenske rokove i odgovorna lica,
c) budu predmetom redovnog praćenja i preispitivanja, a kako bi se osigurala njihova relevantnost i adekvatnost.

(2) Uprava banke treba biti obaviještena o realizaciji i statusu aktivnosti definiranih operativnim planovima jasno, detaljno i pravovremeno, a najmanje na kvartalnom nivou.

Član 11.
IKT sistemi

(1) Banka je dužna uspostaviti, implementirati, nadzirati, održavati, redovno revidirati i poboljšavati proces upravljanja IKT sistemom.

(2) Banka je dužna upotrebljavati i održavati ažurnim IKT sisteme i alate koji su:
a) primjereni veličini poslovnih funkcija banke koje podržava, a u skladu sa principom proporcionalnosti, uzimajući u obzir svoju veličinu i ukupni profil rizičnosti, kao i prirodu, obim i složenost usluga, aktivnosti i poslovanja banke,
b) pouzdani,
c) opremljeni dovoljnim kapacitetima za:
1) tačnu i pouzdanu obradu podataka neophodnih za obavljanje aktivnosti i pravovremeno pružanje usluga banke,
2) periode visoke opterećenosti sistema,
3) uvođenje novih tehnologija.
d) tehnološki otporni kako bi se na adekvatan način nosili sa dodatnim potrebama za obradom informacija u stresnim okolnostima na tržištu ili drugim nepovoljnim situacijama.

(3) Pored internih akata iz člana 3. ove odluke, banka je dužna pribavljati i čuvati i drugu dokumentaciju (tehničku, funkcionalnu, korisničku i drugu) i informacije koje se odnose na IKT sistem i njegove specifične dijelove. Navedena dokumentacija treba biti tačna, potpuna i ažurna.

IV UPRAVLJANJE IKT RIZICIMA

Član 12.
Uspostava okvira za upravljanje IKT rizicima

(1) Banka je dužna da, kao dio sveukupnog okvira i mehanizama interne kontrole i procesa upravljanja rizicima, uspostavi pouzdan, sveobuhvatan i dokumentovan okvir za upravljanje IKT rizicima, s ciljem efikasnog upravljanja IKT rizicima, donošenja adekvatnih odluka o preuzimanju rizika, te provođenja mjera za osiguranje visoke digitalne operativne otpornosti radi brzog, efikasnog i sveobuhvatnog odgovora na IKT rizike.
(2) Okvir za upravljanje IKT rizicima banke treba biti u potpunosti integrisan i usklađen sa sveukupnim okvirom upravljanja rizicima banke, a u skladu sa propisom Agencije kojim se regulira sistem internog upravljanja u banci.
(3) U skladu sa propisom Agencije kojim se regulira sistem internog upravljanja u banci, banka je dužna odgovornost za kontrolu i nadzor nad IKT rizicima dodijeliti kontrolnoj funkciji upravljanja rizicima, odnosno, u slučaju da je funkcija upravljanja IKT rizicima izdvojena funkcija, a u skladu sa članom 4. stav (2) ove odluke, banka je dužna osigurati koordiniran i usaglašen rad ove funkcije sa kontrolnom funkcijom upravljanja rizicima.

Član 13.
Princip proporcionalnosti

Okvir za upravljanje IKT rizicima, kao i pravila utvrđena u ovoj odluci, banka je dužna primijeniti u skladu sa načelom proporcionalnosti, uzimajući u obzir svoju veličinu i ukupni profil rizičnosti te prirodu, obim i složenost svojih usluga, aktivnosti i poslovanja, unutrašnju organizaciju, te veličinu i kompleksnost IKT sistema.

Član 14.
Sadržaj okvira za upravljanje IKT rizicima

(1) Okvir za upravljanje IKT rizicima treba da obuhvati najmanje strategije, politike, metodologije, programe, procedure i planove, kao i IKT kontrole koje su potrebne za propisnu i primjerenu zaštitu cjelokupne informacione i IKT imovine, u cilju svođenja utjecaja IKT rizika na najmanju moguću mjeru, a u skladu sa ciljevima definiranim strategijom.
(2) U okviru Politike za upravljanje IKT rizicima i procedura za upravljanje IKT rizicima, banka je dužna uključiti i sljedeće:
   a) postupke za redovno i pravovremeno identifikovanje i mjerenje, odnosno procjenu IKT rizika kojima je banka izložena ili bi mogla biti izložena,
   b) postupke za uspostavu mjera za ublažavanje IKT rizika, te pravila za primjenu tih mjera,
   c) postupke praćenja efikasnosti uspostavljenih mjera, a uključujući i praćenje na bazi broja prijavljenih IKT incidenata, te, ako je to potrebno, poduzimanje radnji za ispravljanje mjera,
   d) postupke za kontrolu rizika, uključujući i postupke provođenja testiranja digitalne operativne otpornosti,
   e) postupke za izvještavanje organa banke o IKT rizicima,
   f) postupke praćenja nivoa digitalne operativne otpornosti sa jasnim prikazom aktuelne situacije u pogledu digitalne operativne otpornosti na bazi broja prijavljenih značajnih IKT incidenata i efikasnosti preventivnih kontrola,
   g) postupke za utvrđivanje i procjenjivanje postojanja IKT rizika koji proizlaze iz bilo kakvih većih promjena u IKT sistemu ili uslugama, IKT procesima i/ili nakon svakog značajnijeg operativnog ili IKT incidenta.
(3) Banka je dužna adekvatno dokumentovati proces upravljanja IKT rizicima.

Član 15.
Identifikovanje rizika

(1) Banka je dužna kontinuirano identifikovati IKT rizike.
(2) U okviru identifikacije IKT rizika, banka je dužna:
   a) identifikovati i dokumentovati svoje poslovne funkcije, uloge i podržavajuće procese,
   b) identifikovati, uspostaviti, dokumentovati i redovno ažurirati mapiranje informacione i IKT imovine kojom se pruža podrška identifikovanim poslovnim funkcijama i podržavajućim procesima iz tačke a) ovog stava, kao što su IKT sistemi, zaposlenici, izvođači i treće strane, te njihove međusobne povezanosti,
   c) identifikovati i dokumentovati sve poslovne funkcije i podržavajuće procese zavisne o trećim stranama pružaocima IKT usluga i identifikovati međusobne zavisnosti pružaoca usluga.
(3) U okviru mapiranja iz stava (2) tačka b) ovog člana, banka je dužna mapirati svu IKT imovinu, uključujući IKT imovinu na udaljenim lokacijama, mrežne resurse i hardversku opremu, te mapirati i konfiguracije IKT imovine, kao i veze između različite IKT imovine te njihove međusobne zavisnosti.
(4) Banka je dužna izvršiti klasifikaciju identifikovanih poslovnih funkcija, podržavajućih procesa i informacionu i IKT imovinu iz stava (2) ovog člana, uzimajući u obzir zahtjeve u pogledu povjerljivosti, integriteta i dostupnosti, kao i dokazivosti i autentičnosti.
(5) Prilikom procjene rizika, banka je dužna preispitati adekvatnost klasifikacije informacione i IKT imovine.
(6) Banka je dužna odrediti jasnu internu odgovornost za upravljanje informacionom i IKT imovinom, uključujući precizno definiranje nadležnosti i odgovornosti za svaku komponentu.
(7) Banka je dužna osigurati relevantnu evidenciju za potrebe stava (1) i (2) ovog člana, te ih održavati ažurnom, a naročito nakon svake značajne izmjene.

Član 16.
Procjena rizika

(1) Banka je dužna redovno mjeriti, odnosno procjenjivati IKT rizike koje je identifikovala.
(2) U okviru procjene IKT rizika, banka je dužna identifikovati IKT rizike koji utječu na klasifikovane poslovne funkcije, podržavajuće procese i informacionu i IKT imovinu, iz člana 15. ove odluke.
(3) Banka je dužna provoditi i dokumentovati procjenu IKT rizika na godišnjoj osnovi ili češće, a obavezno u slučaju važnije promjene u IKT sistemu, postupcima ili procedurama koje utječu na poslovne funkcije, podržavajuće procese ili IKT imovinu.
(4) Banka je dužna najmanje jednom godišnje provoditi posebnu procjenu IKT rizika za sve zastarjele IKT sisteme, a obavezno prije i nakon povezivanja tehnologija, aplikacija ili sistema.
(5) Banka je dužna osigurati kontinuiranu identifikaciju svih izvora IKT rizika, posebno izloženost riziku drugih finansijskih subjekata i od drugih finansijskih subjekata, te procjenjivati prijetnje, uključujući i cyber prijetnje, i ranjivosti IKT sistema koje su relevantne za poslovne funkcije, podržavajuće procese i informacionu i IKT imovinu banke. Banka je dužna redovno, a najmanje jednom godišnje, preispitivati scenarije rizika koji utječu na njih, uključujući cyber rizike.

Član 17.
Ovladavanje rizicima

(1) Banka je dužna jasno i precizno odrediti i primjenjivati kriterije za odlučivanje i postupke za ovladavanje IKT rizicima, uzimajući u obzir rizični profil banke, odnosno sklonost banke ka preuzimanju IKT rizika, određenu strategijom rizika banke.

(2) Na osnovu procjene IKT rizika iz člana 16. ove odluke, banka je dužna identifikovati i implementirati potrebne kontrole za ovladavanje IKT rizicima, uključujući i potrebne promjene u postojećim poslovnim procesima, kontrolnim mjerama, IKT sistemu i IKT uslugama, osigurati svođenje IKT rizika na prihvatljivi nivo rizika, te zaštititi informacionu i IKT imovinu u skladu sa njenom klasifikacijom.
(3) Banka je dužna uzeti u obzir vrijeme potrebno za provođenje identifikovanih kontrola iz stava (2) ovog člana, kao i vrijeme potrebno za poduzimanje odgovarajućih privremenih kontrola za smanjenje IKT rizika, a kako bi ti rizici ostali unutar ograničenja sklonosti za preuzimanje IKT rizika banke.
(4) Kontrolama iz stava (2) ovog člana, banka je dužna najmanje:
   a) osigurati sigurnost u prijenosu podataka,
   b) na najmanju moguću mjeru svesti rizik od oštećenja ili gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje,
   c) spriječiti umanjenje dostupnosti, narušavanje autentičnosti i integriteta, kršenje povjerljivosti i gubitka podataka,
   d) osigurati da su podaci zaštićeni od rizika koji proizlaze iz upravljanja podacima, uključujući propuste u administraciji, rizika vezanih uz obradu podataka i ljudske greške.
(5) U sklopu okvira za upravljanje IKT rizicima, banka je dužna:
   a) propisati, provoditi i redovno ažurirati Politiku informacione sigurnosti, kojom se definiraju pravila za zaštitu dostupnosti, autentičnosti, integriteta, dokazivosti i povjerljivosti podataka, informacione i IKT imovine, kako bi se postigli ciljevi u području informacione sigurnosti,
   b) primjenom pristupa koji se zasniva na procjeni rizika, uspostaviti pouzdanu strukturu za upravljanje mrežom i infrastrukturom pomoću odgovarajućih tehnika, metoda i protokola, koji mogu uključivati automatizovane mehanizme za izolaciju zahvaćene informacione i IKT imovine u slučaju cyber napada (mogućnost trenutnog prekida ili segmentiranja kako bi se u najvećoj mogućoj mjeri spriječila zaraza),
   c) propisati i provoditi procedure, postupke i kontrole kojima se ograničava fizički ili logički pristup informacionoj i IKT imovini samo na ono što je nužno za legitimne i odobrene funkcije i aktivnosti, te u tu svrhu implementirati postupke i kontrole koji se odnose na prava pristupa i osiguravaju dobro upravljanje njima,
   d) propisati i provoditi procedure, postupke i kontrole za pouzdane mehanizme autentifikacije, na osnovu relevantnih standarda i namjenskih kontrolnih sistema, te mjere za zaštitu kriptografskih ključeva, kojima se podaci, u mirovanju i prijenosu, šifriraju, a na osnovu rezultata klasifikacije podataka i procjene IKT rizika,
   e) propisati i provoditi procedure za upravljanje IKT promjenama, a u skladu sa članom 40. ove odluke,
   f) propisati i provoditi odgovarajuće i sveobuhvatne dokumentovane postupke za upravljanje ažuriranjima softvera, kao i upravljanje zaštitom od malicioznog koda,
   g) propisati i provoditi procedure upravljanja IKT imovinom, a u skladu sa članom 37. ove odluke,
   h) propisati i provoditi odgovarajuće procedure izrade i upravljanja sigurnosnim kopijama, a u skladu sa članom 35. ove odluke,
   i) propisati i provoditi odgovarajuće planove kontinuiteta poslovanja u području IKT sistema, te planove odgovora i oporavka IKT sistema, a u skladu sa članom 30. i 31. ove odluke,
   j) propisati i provoditi odgovarajuće programe i planove osposobljavanje i podizanja svijesti o sigurnosti IKT sistema, u skladu sa članom 21. ove odluke.

Član 18.
Praćenje, nadzor i izvještavanje o IKT rizicima

(1) Banka je dužna uspostaviti sistem redovnog praćenja, nadzora i izvještavanja o IKT rizicima.
(2) U okviru redovnog praćenja IKT rizika, banka je dužna uspostaviti kontrole za kontinuiran nadzor IKT sistema i pravovremeno otkrivanje neuobičajenih aktivnosti, u skladu sa članom 41. ove odluke, a što uključuje i probleme sa performansama IKT sistema i IKT incidente, te identifikaciju mogućih važnih jedinstvenih tačaka prekida.
(3) Banka je dužna kontrole iz stava (2) ovog člana osigurati na višestrukim nivoima, definirati pragove upozorenja i kriterije za aktiviranje i pokretanje procesa odgovora na IKT incidente, uključujući mehanizme za automatsko pravovremeno upozoravanje relevantnog osoblja zaduženog za odgovor na IKT incidente.
(4) Banka je dužna osigurati adekvatno razdvajanje dužnosti zaposlenika u procesu nadzora i procesima koji su predmet nadzora.
(5) Pri obavljanju praćenja efikasnosti i kontrole IKT rizika, banka je dužna provjeravati uspostavljene kontrole za ovladavanje IKT rizicima, te vršiti ocjenu njihove efektivnosti i efikasnosti, uključujući i kontrole testiranja digitalne operativne otpornosti definirane čl. 23. - 27. ove odluke.
(6) Banka je dužna kontinuirano pratiti i utvrđivati utječu li promjene u postojećem operativnom okruženju na implementirane kontrole, te da li je potrebno uvođenje dodatnih kontrola radi smanjivanja povezanih IKT rizika, osiguravajući da su takve promjene dio formalnog procesa upravljanja promjenama.
(7) Banka je dužna osigurati dovoljno adekvatnih resursa, uključujući i osposobljene zaposlenike za:
   a) praćenje aktivnosti korisnika, nastanka neuobičajenih pojava u IKT sistemu i IKT incidenata, a naročito cyber napada,
   b) prikupljanje informacija o ranjivostima, cyber prijetnjama i IKT incidentima, a naročito cyber napadima, te za analizu njihovog vjerovatnog utjecaja na digitalnu operativnu otpornost banke.
(8) Banka je dužna uključiti izvještavanje o IKT rizicima, u okviru izvještavanja o rizicima, te u okviru izvještaja dati jasan prikaz aktuelne situacije u pogledu digitalne operativne otpornosti, i to na bazi broja prijavljenih značajnih IKT incidenata i efikasnosti preventivnih kontrola.

Član 19.
Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima

(1) Banka je dužna osigurati i dokumentovati proces preispitivanja okvira za upravljanje IKT rizicima, najmanje jednom godišnje, kao i
   a) nakon značajnih IKT incidenata, cyber napada, iskustava iz testova (npr. penetracijski testovi, TLPT, testovi kontinuiteta poslovanja IKT-a, planovi za odgovor i oporavak i slično), uputa iz revizija i drugo,
   b) bez odgađanja u slučaju identifikacije značajnih slabosti i nedostataka u okviru prioritetnih IKT sistema,
   c) obavezno nakon svake značajne promjene u IKT sistemu, procesima ili procedurama koje utječu na poslovne funkcije koje se podržavaju IKT sistemom, te IKT imovinu i
   d) kontinuirano ga poboljšavati na osnovu iskustava stečenih tokom njegovog provođenja i praćenja.
(2) Banka je dužna kontinuirano uključivati iskustva iz testiranja digitalne operativne otpornosti, stvarnih IKT incidenata (posebno cyber napada), problema s aktivacijom planova kontinuiteta i oporavka IKT sistema, razmjene informacija s partnerskim finansijskim subjektima, te nalaze revizije i supervizije u procjenu IKT rizika, te na osnovu toga preispitivati i prilagođavati komponente okvira za upravljanje IKT rizikom.

(3) Banka je dužna pratiti razvoj IKT rizika tokom vremena, analizirati učestalost, vrste, veličinu i razvoj IKT incidenata, a naročito cyber napada i njihovih obrazaca, a u svrhu razumijevanja nivoa izloženosti IKT riziku i unapređenja cyber zrelosti i spremnosti banke.
(4) Banka je dužna propisati, provoditi i na adekvatan način dokumentovati:
   a) redovno praćenje relevantnih novih tehnologija kako bi bolje razumjela mogući utjecaj tih tehnologija na zahtjeve u pogledu IKT sigurnosti i digitalne operativne otpornosti,
   b) redovno praćenje najnovijih praksi upravljanja IKT rizikom, kako bi bila u mogućnosti efikasno odgovoriti na trenutne ili nove oblike cyber napada.

Član 20.
Komunikacija

(1) U sklopu okvira za upravljanje IKT rizicima, banka je dužna definirati planove komunikacije u krizi, kojima će se uspostaviti jasni postupci za upravljanje internom i eksternom komunikacijom u slučaju aktiviranja planova kontinuiteta poslovanja iz oblasti IKT sistema ili planova odgovora i oporavka IKT sistema, uključujući i značajne IKT incidente.
(2) U okviru planova komunikacije u krizi, banka je dužna uzeti u obzir različite potrebe komunikacije za interne zaposlenike i eksterne učesnike, kao i razlike u potrebama zaposlenika uključenih u upravljanje IKT incidentom, posebno osoblja nadležnog za odgovor i oporavak, od osoblja koje je potrebno samo informisati.
(3) Banka je dužna odgovorno obavještavati klijente, javnost i partnerske finansijske subjekte o značajnim IKT incidentima ili ranjivostima, u zavisnosti od vrste i prirode IKT incidenta, a obavezno u slučaju značajnih IKT incidenata ili ranjivosti.

Član 21.
Osposobljavanje i podizanje nivoa svijesti o sigurnosti IKT sistema

(1) Banka je dužna uspostaviti i provoditi program za osposobljavanje, uključujući program podizanja svijesti o sigurnosti IKT sistema i digitalnoj operativnoj otpornosti, za sve svoje zaposlenike, a kako bi osigurala da su pravovremeno osposobljeni za izvršavanje dužnosti i odgovornosti u skladu sa politikom informacione sigurnosti i postupcima u cilju smanjenja ljudskih grešaka, krađa, prevara, zloupotreba ili gubitaka.
(2) Programom osposobljavanja trebaju biti pravovremeno obuhvaćeni svi zaposlenici, uključujući i više rukovodeće osoblje, a nivo njihove složenosti treba biti srazmjeran nadležnostima njihovih funkcija i odgovornosti, dok je, prema potrebi, banka dužna u programe osposobljavanja uključiti i treće strane pružaoce IKT usluga u odgovarajućem obimu.
(3) Banka je dužna osigurati da se programom osposobljavanja osigura osposobljavanje zaposlenika redovno, a najmanje jednom godišnje, vodeći posebno računa o pravovremenom osposobljavanju u pogledu prepoznatih IKT prijetnji.
(4) Programom osposobljavanja trebaju se predvidjeti i provoditi periodične provjere znanja i procjene svjesnosti o IKT prijetnjama.

Član 22.
Edukacija

(1) Banka je dužna da osigura stručno osposobljavanje i kontinuiranu edukaciju zaposlenika u organizacionoj jedinici IKT-a i upravljanja IKT rizicima, kao i internog revizora IKT sistema, kako bi osigurala da su navedeni zaposlenici pravovremeno i adekvatno osposobljeni za obavljanje svojih funkcija, a uzimajući u obzir razvoj IKT sistema i IKT rizika, veličinu i kompleksnost IKT sistema, kao i poslovni model banke.
(2) Banka je dužna definirati potrebne kompetencije za svaku funkciju, analizirati potrebe za dodatnom edukacijom zaposlenika u navedenim funkcijama, osigurati potrebnu edukaciju,

osigurati da su postignute potrebne kompetencije, te održavati dokumentaciju o edukaciji i kompetencijama.

(3) Banka je dužna izraditi detaljni godišnji plan edukacije zaposlenika, definirati vremenske rokove, dokumentovati njegovu realizaciju, te kvartalno izvještavati o realizaciji plana.

(4) Banka je dužna kontinuirano ispitivati efikasnost svojih planova edukacije i, ako je potrebno, ažurirati ih, kako bi osigurala da su obuke adekvatne i primjerene veličini i kompleksnosti IKT sistema, IKT rizicima, kao i da prate razvoj novih IKT i IKT rizika, uključujući i cyber rizike.

V TESTIRANJE DIGITALNE OPERATIVNE OTPORNOSTI

Član 23.
Testiranje digitalne operativne otpornosti
(eng. digital operational resilience testing)

(1) U okviru za upravljanje IKT rizicima, banka je dužna definisati, provoditi i redovno ažurirati Politiku za testiranje digitalne operativne otpornosti i procedure za testiranje digitalne operativne otpornosti, a u svrhu procjene pouzdanosti i efikasnosti implementiranih kontrola i spremnosti na postupanje prilikom IKT incidenata.

(2) Politika i procedure za testiranje digitalne operativne otpornosti iz stava (1) ovog člana trebaju uključiti niz procjena, testova, metodologija, postupaka i alata koji se primjenjuju u skladu sa čl. 23. - 27. ove odluke, te njihovo adekvatno dokumentovanje.

(3) Politikom i procedurama za testiranje digitalne operativne otpornosti, banka je dužna primijeniti pristup zasnovan na procjeni rizika, a uzimajući u obzir razvoj IKT rizika, sve konkretne rizike kojima je banka izložena ili bi mogla biti izložena, kritičnost informacione i IKT imovine i usluga, kao i ostale faktore koje banka smatra odgovarajućim. Politikom i procedurama za testiranje digitalne operativne otpornosti potrebno je uzeti u obzir i prijetnje i ranjivosti utvrđene praćenjem prijetnji te postupcima procjene IKT rizika.

(4) Banka je dužna osigurati da testiranja provode nezavisne interne ili eksterne osobe sa dovoljno znanja, vještina i stručnosti u testiranju mjera sigurnosti IKT sistema, osiguravajući izbjegavanje sukoba interesa u fazama dizajna i provođenja testa, te osiguravajući dovoljna sredstva u tu svrhu.

(5) Banka je dužna uspostaviti postupke za prioritizaciju, klasifikaciju, otklanjanje i praćenje svih slabosti i nedostataka otkrivenih izvođenjem testova iz stava (2) ovog člana, te metodologiju interne provjere kako bi se utvrdilo da su sve identifikovane slabosti i nedostaci u potpunosti otklonjeni, te bez odgađanja otkloniti identifikovane slabosti i nedostatke u prioritetnim IKT sistemima.

(6) Banka je dužna osigurati obavljanje primjerenih testova IKT sistema:

a) najmanje jednom godišnje za sve IKT sisteme i aplikacije kojima se podržavaju prioritetne funkcije,

b) najmanje jednom u intervalu od tri godine za IKT sisteme koji nisu prioritetni, proporcionalno rizicima,

c) prije svake izmjene postojeće ili dodavanja nove komponente IKT sistema i usluga, u slučaju da se radi o podržavanju prioritetnih funkcija, kao i u slučaju značajnih izmjena IKT procesa i infrastrukture, uključujući promjene provedene zbog IKT incidenata,

d) u slučaju implementacije novih ili značajno izmijenjenih aplikacija u IKT sistemu banke, a koje su dostupne putem interneta.

Član 24.
Sadržaj testiranja digitalne operativne otpornosti

(1) Politikom i procedurama za testiranje digitalne operativne otpornosti iz člana 23. ove odluke, banka je dužna obuhvatiti izvođenje odgovarajućih testova, kao što su procjene i skeniranja ranjivosti, analize javno dostupnih izvora, procjene mrežne sigurnosti, analize odstupanja, preispitivanja fizičke sigurnosti, upitnici i softverska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvodivo, testiranja na osnovu scenarija, testiranje kompatibilnosti, testiranje performansi, integralno testiranje (eng. end-to-end testing) i penetracijsko testiranje.
(2) Testiranja na osnovu scenarija trebaju obuhvatiti i scenarije relevantnih i poznatih potencijalnih napada, a na osnovu uočenih sigurnosnih prijetnji.

Član 25.
Napredno testiranje sigurnosti IKT sistema (TLPT)

(1) Banka je dužna provoditi napredno testiranje sigurnosti IKT sistema u obliku penetracijskog testiranja vođenim prijetnjama (TLPT) najmanje jednom u intervalu od tri godine, a uzimajući u obzir rizik banke i operativne okolnosti, Agencija može, kada je to potrebno, tražiti od banke da smanji ili poveća učestalost TLPT-a.
(2) TLPT-jem iz stava (1) ovog člana je potrebno obuhvatiti više ili sve prioritetne funkcije banke. TLPT je potrebno provoditi na produkcijskom sistemu koji podržava te funkcije.
(3) Banka je dužna identifikovati sve relevantne IKT sisteme, procese i tehnologije, kojima se podržavaju prioritetne funkcije, kao i IKT usluge, uključujući i one koje su eksternalizovane ili ugovorene sa IKT pružaocima usluga, a kojima se podržavaju prioritetne funkcije.
(4) Banka je dužna procijeniti koje prioritetne funkcije će biti obuhvaćene TLPT-om, te rezultat procjene dostaviti Agenciji.
(5) Ako su treće strane pružaoci IKT usluga obuhvaćeni TLPT-om, banka je dužna poduzeti sve potrebne i zaštitne mjere kako bi osigurala učešće takvih trećih strana pružaoca IKT usluga u TLPT-u, s tim da banka u svakom trenutku zadržava potpunu odgovornost za osiguravanje usklađenosti sa ovom odlukom.
(6) U slučaju kada postoji opravdana sumnja da će sudjelovanje treće strane pružaoca IKT usluga iz stava (5) ovog člana, negativno utjecati na kvalitet, sigurnost usluga ili povjerljivost podataka koji su povezani sa takvim uslugama, a koji se odnose na klijente treće strane pružaoca IKT usluga koji nisu obuhvaćeni primjenom ove odluke, banka se može pismeno dogovoriti sa trećom stranom pružaocem IKT usluga da treća strana pružalac IKT usluga direktno angažuje eksterne provoditelje testiranja.
(7) TLPT se u okolnostima iz stava (6) ovog člana provodi pod vodstvom jedne imenovane banke iz udruženog TLPT-a, u kojem učestvuje nekoliko banaka (eng. pooled testing) kojima treća strana pružalac IKT usluga pruža iste usluge, pri čemu navedeno ne dovodi u pitanje aktivnosti iz st. (2) i (3) ovog člana.
(8) Udruženim TLPT-jem iz stava (6) ovog člana potrebno je obuhvatiti relevantan obim IKT usluga koje podržavaju prioritetne funkcije koje su banke ugovorile sa trećom stranom pružaocem IKT usluga.
(9) Udruženi TLPT smatra se TLPT-jem koji provode banke koje učestvuju u udruženom TLPT-ju i na njega se primjenjuju odredbe ove odluke.
(10) Banka je dužna, u saradnji sa trećim stranama pružaocima IKT usluga i drugim uključenim stranama, uključujući provoditelje testiranja, ali isključujući Agenciju, primjenjivati adekvatne kontrole upravljanja rizicima kako bi ublažila rizike od mogućeg utjecaja na podatke, od oštećenja imovine i od poremećaja u radu prioritetnih funkcija, usluga ili operacija u samoj banci, njenim partnerima ili finansijskom sektoru.
(11) Banka je dužna, na kraju testiranja, nakon što su usaglašeni izvještaji i planovi za ispravljanje nedostataka, dostaviti Agenciji sažetak relevantnih nalaza, planove za

ispravljanje nedostataka i dokumentaciju kojom se potvrđuje da je TLPT proveden u skladu sa zahtjevima.

(12) U slučaju da banka učestvuje u grupnom testiranju, u okviru kojeg je uključeno drugo nadležno tijelo izvan Bosne i Hercegovine, banka je dužna pravovremeno obavijestiti Agenciju o navedenome, te dostaviti potvrdu, sažetak relevantnih nalaza i planova za ispravljanje nedostataka.

(13) Banka u svakom slučaju ostaje potpuno odgovorna za utjecaje/posljedice testiranja iz st. (5), (6), (7) i (12) ovog člana.

Član 26.
Provoditelji testiranja TLPT

(1) Banka je dužna angažovati provoditelje testiranja za potrebe obavljanja TLPT, a u skladu sa članom 27. ove odluke. U slučaju kada banka angažuje interne provoditelje testiranja za potrebe obavljanja TLPT-a, dužna je angažovati eksterne provoditelje testiranja za svaki treći test.

(2) Agencija će odrediti banke koje su dužne obavljati TLPT, na osnovu principa proporcionalnosti, a uzimajući u obzir sljedeće:
   a) faktore povezane sa utjecajem, posebno mjere u kojoj usluge i aktivnosti koje banka pruža imaju na finansijski sektor u cjelini,
   b) moguće probleme u pogledu finansijske stabilnosti, što uključuje sistemsku prirodu banke na nivou finansijskog sistema,
   c) specifični profil IKT rizičnosti i nivo IKT zrelosti banke ili korištenih tehnoloških karakteristika.

Član 27.
Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT

(1) Banke su dužne angažovati provoditelje testiranja za izvođenje TLPT-a koji:
   a) imaju zadovoljavajući nivo stručnosti i adekvatno iskustvo i reference, te su među najadekvatnijim i najuglednijim provoditeljima testiranja,
   b) posjeduju tehničke, organizacijske sposobnosti i posebno stručno znanje u području saznanja o prijetnjama, penetracijskom testiranju i testiranju „crvenog tima“ (eng. red team),
   c) su akreditovani u oblasti obavljanja penetracijskih testiranja međunarodno priznatim akreditacijama, te se pridržavaju formalnih kodeksa ponašanja ili etičkih okvira,
   d) pružaju nezavisno uvjerenje ili revizorski izvještaj u vezi sa adekvatnim upravljanjem rizicima povezanim sa provođenjem TLPT-a, uključujući odgovarajuću zaštitu povjerljivih informacija banke i pravnu zaštitu s obzirom na poslovne rizike banke,
   e) su propisno i u potpunosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, uključujući i rizike od protupravnog i nemarnog postupanja.

(2) U slučaju angažovanja internih provoditelja testiranja, banka je dužna osigurati da, pored uslova iz stava (1) ovog člana, budu ispunjeni i sljedeći uslovi:
   a) izbjegavanje sukoba interesa prilikom dizajniranja i provođenja testa,
   b) pružalac informacija o prijetnjama nije dio banke.

(3) Banka je dužna osigurati da se ugovorom sklopljenim sa eksternim provoditeljima testiranja osigura adekvatno upravljanje rezultatima TLPT-a i da niti jedna obrada podataka s tim u vezi, uključujući proizvodnju, izradu, smještaj, obradu, izvještavanje, obavještavanje ili uništavanje, ne stvara rizike po banku.

VI UPRAVLJANJE KONTINUITETOM POSLOVANJA

Član 28.
Kontinuitet poslovanja u području IKT sistema

(1) Banka je dužna donijeti Strategiju kontinuiteta poslovanja koja treba da sadrži ciljeve upravljanja kontinuitetom poslovanja sa jasnim kvantitativnim i kvalitativnim zahtjevima koji se odnose na dostupnost poslovnih funkcija i podržavajućih procesa banke, a vodeći računa o veličini i ukupnom profilu banke, kao i prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja.

(2) Na osnovu Strategije kontinuiteta poslovanja iz stava (1) ovog člana, banka je dužna donijeti Plan kontinuiteta poslovanja u području IKT sistema (Plan kontinuiteta IKT-a) koji je sastavni dio Plana kontinuiteta poslovanja banke uzimajući u obzir identifikovane poslovne funkcije, procese i resurse IKT sistema iz člana 15. ove odluke.

Član 29.
Analiza utjecaja na poslovanje

(1) Banka je dužna provoditi analizu utjecaja na poslovanje (eng. BIA) analiziranjem svoje izloženosti znatnijim prekidima poslovanja i procjenom njihovih potencijalnih efekata (uključujući povjerljivost, integritet i dostupnost), kvantitativno i kvalitativno, upotrebom internih i/ili eksternih podataka uz analizu scenarija koji uzimaju u obzir različite rizike.

(2) Analizom utjecaja na poslovanje potrebno je uzeti u obzir kritičnost utvrđenih i mapiranih poslovnih funkcija, podržavajućih procesa, trećih strana, informacione i IKT imovine, kao i njihove međusobne zavisnosti, a u skladu sa članom 15. ove odluke.

(3) U okviru analize utjecaja na poslovanje potrebno je kao minimum:
   a) navesti prioritetne funkcije i podržavajuće procese, a u skladu sa članom 15. stav (2) tačka a) ove odluke,
   b) navesti IKT imovinu potrebnu za odvijanje pojedinačnih poslovnih funkcija, kao i njihove međusobne zavisnosti i povezanosti, a u skladu sa članom 15. stav (2) tačka b) ove odluke,
   c) odrediti, kao minimum, RTO, RPO, SDO i MTD za svaku pojedinačnu poslovnu aktivnost, imajući u vidu eksternalizaciju i zavisnost od trećih strana.

(4) Pri utvrđivanju parametara RTO, RPO i MTD, banka je dužna uzeti u obzir i mogući opći utjecaj na cjelokupno finansijsko tržište. Navedenim parametrima banka je dužna osigurati da se u ekstremnim scenarijima postigne dogovoreni nivo usluga (SDO), a u skladu sa Strategijom IKT sistema i ciljevima informacione sigurnosti.

(5) Banka je dužna osigurati da su IKT resursi i IKT usluge uspostavljeni i usklađeni sa analizom utjecaja na poslovanje, a posebno u pogledu adekvatnog osiguranja redundantnosti ključnih IKT komponenti, a kako bi se spriječili prekidi izazvani događajima koji utječu na te komponente.

Član 30.
Plan kontinuiteta IKT-a

(1) Na osnovu analize utjecaja na poslovanje banka je dužna donijeti Plan kontinuiteta IKT-a.

(2) Planom kontinuiteta IKT-a banka je dužna osigurati:
   a) kontinuitet prioritetnih funkcija banke u okviru definiranih RTO i RPO parametara,
   b) brze, adekvatne i efikasne odgovore na sve IKT incidente i njihovo rješavanje, na način kojim se ograničava šteta, a daje prioritet nastavku poslovanja i mjerama oporavka,
   c) aktivaciju, bez odlaganja, ciljanih planova kojima se omogućavaju kontrole, procesi i tehnologije za suzbijanje širenja IKT incidenta i sprječavanja dalje štete, a koje su prilagođene svakoj vrsti IKT incidenta, kao i prilagođene postupke odgovora i oporavka uspostavljenih u skladu sa članom 31. ove odluke,

d) procjenu preliminarnog utjecaja, štete i gubitka,
e) definiranje komunikacijskih mjera i mjera za upravljanje kriznim situacijama kojima se osigurava prijenos ažurnih informacija svim relevantnim članovima banke i eksternim zainteresovanim stranama, a u skladu sa članom 20. ove odluke, i izvještavanje Agencije u skladu sa članom 44. ove odluke.

(3) Planom kontinuiteta IKT-a banka je dužna podržati ciljeve za zaštitu, i ako je potrebno, ponovnu uspostavu povjerljivosti, integriteta i dostupnosti poslovnih procesa, podržavajućih procesa i IKT imovine.

(4) U okviru Plana kontinuiteta IKT-a banka je dužna razmotriti niz različitih scenarija kojima bi mogla biti izložena, uključujući ekstremne, ali moguće scenarije, te procijeniti njihov potencijalni utjecaj. Na osnovu tih scenarija, banka je dužna opisati način osiguravanja kontinuiteta IKT sistema i usluga, kao i informacionu sigurnost banke.

(5) Pri procesu planiranja kontinuiteta poslovanja u području IKT-a, banka je dužna definirati procese, resurse, uloge i odgovornosti, a kako bi osigurala da su eksternalizovani dijelovi IKT sistema i servisi adekvatno pokriveni planovima kontinuiteta poslovanja. Banka je dužna uzeti u obzir zavisnost o uslugama trećih strana.

(6) U slučaju aktivacije planova kontinuiteta IKT-a ili planova odgovora i oporavka IKT-a, uključujući i značajne IKT incidente, banka je dužna voditi evidenciju aktivnosti prije i nakon poremećaja u radu, koja treba biti lako dostupna.

Član 31.
Planovi odgovora i oporavka IKT sistema

(1) Na osnovu analize utjecaja na poslovanje iz člana 29. ove odluke i Plana kontinuiteta IKT-a iz člana 30. ove odluke, banka je dužna da definira i usvoji planove odgovora i oporavka IKT sistema.

(2) Planovima odgovora i oporavka IKT sistema, banka je dužna definirati uslove za aktiviranje planova, kao i mjere koje je potrebno poduzeti kako bi se osigurala dostupnost, kontinuitet i oporavak minimalno prioritetnih funkcija odnosno ključnih IKT sistema i usluga. Planovi za oporavak IKT sistema trebaju biti usmjereni prema postizanju ciljeva oporavka poslovanja banke.

(3) Banka je dužna da u slučaju nastanka okolnosti koje zahtijevaju primjenu plana odgovora i oporavka IKT sistema odmah po saznanju o navedenom obavijesti Agenciju sa svim relevantnim činjenicama i okolnostima koje se na to odnose.

(4) Banka je dužna ažurirati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema najmanje jednom godišnje, a na osnovu rezultata testiranja, saznanja o aktuelnim prijetnjama, kao i iskustvima stečenim iz prethodnih događaja, kao i nalaza/preporuka revizija, te obavezno prilikom promjene ciljeva oporavka, poslovnih funkcija, podržavajućih procesa ili IKT imovine.

Član 32.
Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema

(1) Banka je dužna testirati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema:
a) kojima se podržavaju sve funkcije, najmanje jednom godišnje,
b) u slučaju svih bitnih promjena u IKT sistemima koji podržavaju prioritetne funkcije.

(2) Banka je dužna testirati i odgovarajuće planove kontinuiteta IKT-a, u slučaju da su prioritetne funkcije eksternalizovane ili ugovorene sa trećim stranama pružaocima IKT usluga.

(3) Banka je dužna testirati planove komunikacije u krizi.

(4) U okviru testiranja iz stava (1) ovog člana, banka je dužna obavezno uključiti scenarije cyber napada i prebacivanja sa primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i rezervni informatički centar.

(5) Banka je dužna:
   a) dokumentovati rezultate testiranja, sa svim popratnim detaljima i dokazima o testiranju,
   b) analizirati i otkloniti sve utvrđene nedostatke koji proizlaze iz testiranja, te o njima izvijestiti upravljačke organe banke,
   c) preispitati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema, uzimajući u obzir rezultate testova iz stava (1) ovog člana, kao i preporuke iz revizijskih ili supervizijskih pregleda.

Član 33.
Rezervni informatički centar

(1) Banka je dužna osigurati rezervni informatički centar koji:
   a) je lociran na odgovarajućoj geografskoj udaljenosti od lokacije primarnog informatičkog centra, uzimajući u obzir rizik da pojedinačni scenario, incident ili katastrofa ne mogu istovremeno utjecati na primarni i rezervni informatički centar i sisteme oporavka,
   b) osigurava kontinuitet prioritetnih funkcija na isti način kao i primarni informatički centar ili pruža nivo usluga neophodnih da banka obavlja svoje prioritetne funkcije u okviru definiranih ciljeva oporavka (RTO, RPO, SDO i MTD),
   c) je odmah dostupan zaposlenicima banke kako bi se osigurao kontinuitet prioritetnih funkcija u slučaju nedostupnosti primarnog informatičkog centra,
   d) je zaštićen od neovlaštenog pristupa ili oštećenja u području IKT sistema.
(2) Efektivna funkcionalnost rezervnog informatičkog centra treba biti potvrđena najmanje jednom godišnje, kao i poslije implementiranih značajnih promjena u IKT sistemu banke. Banka je dužna, 30 dana prije planiranog testiranja funkcionalnosti rezervnog informatičkog centra, obavijestiti Agenciju.
(3) Rezultate testiranja iz stava (2) ovoga člana, banka je dužna detaljno dokumentovati i osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke.

Član 34.
Eksternalizacija IKT sistema izvan Bosne i Hercegovine

(1) U slučaju eksternalizacije cjelokupnog ili dijela IKT sistema izvan teritorije Bosne i Hercegovine, banka je dužna:
   a) definirati prioritetne funkcije banke sa stanovišta kontinuiteta poslovanja i odvijanja istih u zemlji, uzimajući u obzir analizu utjecaja na poslovanje, kao i važeće zakonske propise,
   b) definirati odgovarajuće RTO, RPO, SDO i MTD parametre za funkcije definirane tačkom a) ovog stava, osiguravajući adekvatne nivoe usluge,
   c) definirati ključne resurse IKT sistema banke koji podržavaju prioritetne definirane poslovne funkcije iz tačke a) ovog stava, uzimajući pri tome u obzir i podržavajuće resurse, te napredak i primjenu IKT u poslovnim procesima banke,
   d) definirati Plan kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema u zemlji,
   e) osigurati lokalni informatički centar na teritoriji Bosne i Hercegovine kako bi osigurala kontinuitet prioritetnih funkcija u zemlji na isti način kao i u okviru primarnog informatičkog centra odnosno pružanje nivoa usluga neophodnih da banka obavlja svoje prioritetne funkcije u okviru definiranih ciljeva oporavka (RTO, RPO i SDO),
   f) provoditi testiranje funkcionalnosti lokalnog informatičkog centra najmanje na godišnjem nivou, te osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke,
   g) osigurati osposobljenost zaposlenika banke za izvođenje navedenih aktivnosti,
   h) analizirati i definirati vrstu podataka koje je potrebno osigurati u lokalnom informatičkom centru odnosno zemlji, kako bi se zadovoljile poslovne potrebe banke, uzimajući u obzir tačku a) i e) ovog stava, kao i važeće zakonske propise,

i) osigurati stalnu ažurnost podataka definiranih tačkom h) u lokalnom informatičkom centru.

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

Član 35.
Sigurnosne kopije podataka i sistema

(1) Banka je dužna uspostaviti proces upravljanja sigurnosnim kopijama (eng. backup) koji uključuje procedure izrade, smještaja, testiranja kopija podataka i sistema, te ponovne uspostave i oporavka, kao i adekvatan transport i predaju kopija, a kako bi se osigurala raspoloživost podataka i sistema u slučaju potrebe, te omogućio adekvatan oporavak odnosno ponovna uspostava prioritetnih procesa u zahtijevanom vremenu i raspoloživosti.

(2) U okviru procesa upravljanja sigurnosnim kopijama, banka je dužna propisati za sve resurse IKT sistema:
   a) vrstu,
   b) način izrade,
   c) obim,
   d) frekvenciju izrade,
   e) frekvenciju odlaganja,
   f) period čuvanja sigurnosnih kopija.

   Obim i frekvenciju izrade sigurnosnih kopija, banka je dužna definirati u skladu sa zahtjevima Analize utjecaja na poslovanje i Planovima za odgovor i oporavak IKT sistema, te procjenjivati u skladu s provedenom procjenom IKT rizika.

(3) Banka je dužna osigurati sigurnosne kopije na jednoj ili više sekundarnih lokacija, pri čemu najmanje jedna mora biti dovoljno udaljena od primarne lokacije, na kojoj se nalaze izvorni podaci, kako ne bi bile izložene istim rizicima, te ih održavati ažurnima i adekvatno zaštićenima od odgovarajućih IKT rizika (cyber rizici, rizici prilikom prijenosa, nedostupnost primarne lokacije i drugo), a kako bi se osigurao integritet, dokazivost i autentičnost izvornih podataka.

(4) Banka je dužna da, u slučaju odgovora i oporavka od cyber napada, putem povrata podataka sa sigurnosne kopije podataka, koristi IKT sisteme koji su fizički i logički odvojeni od izvornog IKT sistema, a koji su zaštićeni od neovlaštenog pristupa ili oštećenja, te koji omogućavaju pravovremenu ponovnu uspostavu funkcija banke.

(5) U slučaju primjene stava (4) ovog člana, banka je dužna razmotriti i potrebu korištenja sigurnosnih kopija sistema.

Član 36.
Zaštitne (regulatorne) kopije podataka

Banka je dužna osigurati zaštitne (regulatorne) kopije podataka:
   a) koje sadrže minimalni set podataka neophodan za nastavak poslovanja banke i pružanje prioritetnih funkcija i usluga, kao i provedbu kontrola od strane Agencije u slučaju rane intervencije ili restrukture,
   b) u lako dostupnom formatu kojem je moguće pristupiti, pročitati i obraditi koristeći standardne, uobičajene, sveprisutne dostupne alate, nezavisno od izvornih sistema u kojima su podaci nastali, te u skladu sa zahtjevima Agencije,
   c) ažurne u skladu sa zahtjevima Agencije,
   d) dostupne na teritoriji Bosne i Hercegovine i u skladu sa zahtjevima Agencije.

VII UPRAVLJANJE IKT OPERACIJAMA

Član 37.
IKT operacije

(1) Banka je dužna upravljati svojim IKT operacijama na osnovu dokumentovanih, usvojenih i implementiranih procesa i procedura. Tim dokumentima, banka je dužna definirati način upotrebe, praćenja i kontrole svojih IKT sistema i usluga.
(2) Banka je dužna osigurati da je izvršavanje IKT operacija usklađeno sa zahtjevima poslovanja banke, uključujući i zahtjevima informacione sigurnosti.
(3) Banka je dužna održavati i unapređivati efikasnost svojih IKT operacija, naročito svođenja pogrešaka koje proizlaze iz izvršavanja ručnih zadataka na najmanju moguću mjeru.
(4) Banka je dužna evidentirati, pratiti i čuvati zapise za kritične IKT operacije kako bi se omogućilo otkrivanje, analiza i ispravljanje grešaka.
(5) Banka je dužna:
   a) definirati i provoditi procedure upravljanja IKT imovinom, tokom cijelog njenog životnog ciklusa, od nabavke ili razvoja do povlačenja iz upotrebe, sa ciljem osiguranja dostupnosti, autentičnosti, integriteta i povjerljivosti podataka,
   b) provoditi postupke planiranja, te praćenja performansi i kapaciteta kako bi pravovremeno spriječila, otkrila i odgovorila na značajne probleme u radu IKT sistema i nedostatke kapaciteta IKT sistema.

Član 38.
Upravljanje projektima

(1) Banka je dužna uspostaviti proces upravljanja projektima kojima su definirane uloge i odgovornosti potrebne za efikasnu podršku provođenju Strategije IKT sistema.
(2) Banka je dužna na odgovarajući način pratiti i smanjivati rizike koji proizlaze iz IKT projekata, a uzimajući u obzir i rizike koji mogu proizaći iz međusobne zavisnosti različitih projekata i zavisnosti višestrukih projekata o istim resursima i/ili stručnostima. Banka je dužna uključiti projektni rizik u okvir upravljanja IKT rizicima.
(3) Banka je dužna propisati i usvojiti metodologiju upravljanja projektima.
(4) Metodologijom upravljanja projektima, banka je dužna osigurati da zahtjeve informacione sigurnosti analizira i odobrava funkcija upravljanja IKT rizicima.
(5) Upravljanje rizicima značajnog IKT projekta treba biti predmetom interne revizije IKT sistema banke, u cilju identifikovanja, procjene odnosno mjerenja, praćenja, kontrole, izvještavanja i poduzimanja odgovarajućih mjera za ograničavanje i ublažavanje rizika u banci.
(6) U zavisnosti od važnosti i veličine IKT projekta, te utjecaja na prioritetne funkcije, banka je dužna redovno, kao i dodatno po potrebi, izvještavati upravu banke o uspostavi i napretku IKT projekta, te povezanim rizicima.

Član 39.
Nabavka i razvoj IKT sistema

(1) Banka je dužna definirati i provoditi procedure kojima se propisuje način nabavke, razvoja i održavanja IKT sistema.
(2) Banka je dužna osigurati da se prije svake kupovine ili razvoja IKT sistema jasno i na odgovarajućem nivou upravljanja definiraju i odobre funkcionalni i nefunkcionalni zahtjevi, uključujući zahtjeve u pogledu informacione sigurnosti.
(3) Banka je dužna uspostaviti kontrole za ovladavanje rizikom od nenamjernih promjena ili namjerne manipulacije IKT sistemom tokom razvoja i uvođenja u produkcijsko okruženje.
(4) Banka je dužna:

a) osigurati odvojena IKT okruženja kako bi osigurala adekvatnu segregaciju dužnosti i ublažila efekat neprovjerenih promjena u produkcionim okruženjima,
b) odvojiti produkciona okruženja od razvojnih, testnih i drugih neprodukcionih okruženja,
c) zaštititi integritet i povjerljivost produkcijskih podataka u neprodukcionim okruženjima, te pristup produkcijskim podacima ograničiti na ovlaštene korisnike,
d) zaštititi integritet izvornog koda interno razvijenih IKT sistema.

(5) Banka je dužna detaljno dokumentovati razvoj, implementaciju, rad i konfiguraciju IKT sistema.

(6) U skladu s procjenom rizika, banka je dužna primjenjivati postupke nabavke i razvoja IKT sistema i na IKT sisteme koje razvijaju ili kojima upravljaju krajnji korisnici poslovne funkcije izvan IKT organizacije. Banka je dužna voditi registar ovakvih sistema.

Član 40.
Upravljanje IKT promjenama

(1) Banka je dužna definirati i provoditi procedure upravljanja IKT promjenama kako bi se izbjeglo da promjene dovedu do neočekivanog i neželjenog ponašanja IKT sistema, odnosno naruše njegovu sigurnost ili funkcionalnost.

(2) Procedurama iz stava (1) ovog člana, banka je dužna osigurati da se sve promjene IKT sistema evidentiraju, testiraju, procjenjuju, odobravaju, provode i provjeravaju na kontrolisan način.

(3) Procedurama upravljanja IKT promjenama, banka je dužna obuhvatiti i sljedeće:
a) tzv. hitne promjene,
b) povratak na staro stanje (prije promjene),
c) upravljanje sigurnosnim i funkcionalnim ispravkama (eng. patch).

(4) Banka je dužna da utvrdi početne verzije softverskih komponenata IKT sistema, te evidentira i dokumentuje sve promjene komponenata IKT sistema onim slijedom kako su nastajale, zajedno sa vremenom nastanka promjene.

VIII UPRAVLJANJE IKT INCIDENTIMA

Član 41.
Upravljanje IKT incidentima i problemima

(1) Banka je dužna definirati, uspostaviti i provoditi proces upravljanja IKT incidentima radi pravovremenog otkrivanja IKT incidenata, upravljanja njima i obavještavanja o istim.

(2) U procesu upravljanja IKT incidentima, banka je dužna da definira i uspostavi Politiku upravljanja IKT incidentima i procedure upravljanja IKT incidentima koje obuhvataju:
a) pokazatelje za rano upozoravanje,
b) evidenciju svih IKT incidenata i ozbiljnih cyber prijetnji,
c) postupke za utvrđivanje i dosljedno i integrisano (centralizirano) praćenje i evidentiranje svih IKT incidenata i ozbiljnih cyber prijetnji,
d) kategorizaciju i klasifikaciju IKT incidenata u skladu sa njihovim prioritetom i ozbiljnosti te kritičnosti zahvaćenih usluga, a uzimajući u obzir kriterije utvrđene članom 42. ove odluke,
e) postupke odgovora na IKT incidente, uključujući utvrđivanje i dokumentovanje njihovih osnovnih uzroka (eng. root causes) i daljnje postupanje i poduzimanje mjera, u cilju ublažavanja njihovog efekta i osiguravanja pravovremene dostupnosti i sigurnosti poslovnih funkcija banke,

f) postupke upravljanja problemima, što uključuje utvrđivanje, analizu i rješavanje glavnih uzroka jednog ili više incidenata, kako bi se spriječilo ponavljanje incidenta, te u skladu sa stečenim znanjima ažuriranje sigurnosnih mjera IKT sistema,
g) uloge i odgovornosti za različite vrste IKT incidenata (npr. greške, neispravni rad, cyber napadi i slično),
h) planove za komunikaciju sa zaposlenicima, eksternim učesnicima i medijima, a u skladu sa članom 20. ove odluke, planove za obavještavanje klijenata, postupke povezane sa internom eskalacijom, a što uključuje prigovore korisnika povezane s IKT sistemom i prema potrebi informisanje partnerskih finansijskih subjekata,
i) izvještavanje organa banke najmanje o značajnim IKT incidentima, uz objašnjenje njihovog utjecaja, odgovora na njih i dodatnih kontrola koje je potrebno uvesti.

(3) Banka je dužna evidentirati sve IKT incidente i ozbiljne cyber prijetnje.

(4) U okviru postupaka odgovora na incidente iz stava (2) tačka e) ovog člana, banka je dužna implementirati postupke za adekvatno upravljanje potencijalnim dokazima, kad god je to moguće, vodeći računa o sljedećem:
a) održavanje lanca čuvanja svih povezanih dokaza (eng. chain of custody),
b) prilikom pokretanja digitalne forenzičke istrage, razmotriti moguće posljedice sa pravne tačke gledišta,
c) osigurati da nisu zanemareni kritični aspekti zadržavanja dokaza,
d) osigurati da su prikupljeni dokazi prihvatljivi na nadležnom sudu.

Član 42.
Klasifikacija incidenata

(1) Banka je dužna da klasifikuje IKT incidente i utvrdi njihov utjecaj na osnovu sljedećih kriterija:
a) broj i/ili relevantnost zahvaćenih klijenata ili partnerskih finansijskih subjekata, gdje je to primjenjivo, iznos ili broj transakcija na koje je utjecao IKT incident, kao i činjenice da li je IKT incident imao utjecaj na ugled banke,
b) trajanje IKT incidenta, uključujući vrijeme zastoja u pružanju usluge,
c) geografska rasprostranjenost u smislu područja pogođenih IKT incidentom,
d) gubitak podataka prouzročenih IKT incidentom, u smislu dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka,
e) kritičnost pogođenih usluga, uključujući transakcije i operacije banke,
f) ekonomski utjecaj IKT incidenta, posebno direktni i indirektni troškovi i gubici, u apsolutnom i relativnom smislu.

(2) Banka je dužna da klasifikuje cyber prijetnju kao ozbiljnu na osnovu kritičnosti usluge koja je izložena riziku, uključujući transakcije i operacije banke, broj i/ili relevantnost zahvaćenih klijenata ili partnerskih finansijskih subjekata, kao i geografsku rasprostranjenost područja izloženog riziku.

Član 43.
Učenje i razvoj

(1) Banka je dužna uspostaviti procedure analize i pregleda nakon značajnih IKT incidenata i ozbiljnih cyber prijetnji, analizirajući uzroke poremećaja i identificirajući potrebna poboljšanja u IKT procesima ili u okviru Plana kontinuiteta IKT-a definiranog članom 28. ove odluke.

(2) Pregledom iz stava (1) ovog člana, banka je dužna utvrditi da li su poštovani uspostavljeni procesi i da li su poduzete kontrole bile efikasne, uključujući procjene sljedećeg:
a) brzinu u odgovoru na sigurnosna upozorenja i utvrđivanje utjecaja IKT incidenta i njegove ozbiljnosti,
b) kvalitet i brzinu izvođenja forenzičke analize, gdje je to primjenjivo,

c) efikasnost eskalacije incidenta unutar banke,
d) efikasnost interne i eksterne komunikacije.

Član 44.
Izvještavanje o IKT incidentu i cyber prijetnji

(1) Banka je dužna da odmah po saznanju o značajnom IKT incidentu, kako u dijelu IKT sistema koji se nalazi u banci, tako i u dijelu IKT sistema koji je eksternalizovan/povjeren na obavljanje trećim stranama pružaocima IKT usluga, obavijesti Agenciju.
(2) Za potrebe stava (1) ovog člana, banka je dužna dostaviti inicijalno obavještenje i izvještaje, koji moraju sadržavati sve potrebne informacije kako bi Agencija mogla procijeniti značaj IKT incidenta i njegov utjecaj na cjelokupni finansijski sektor, u skladu sa stavom (5) ovog člana.
(3) Banka je dužna odmah po saznanju o ozbiljnoj cyber prijetnji obavijestiti Agenciju, ukoliko smatra da je prijetnja relevantna za finansijski sektor, korisnike usluga ili klijente.
(4) U slučaju značajnog IKT incidenta koji utječe na finansijske interese klijenata, banka je dužna bez odlaganja obavijestiti klijente o incidentu i mjerama za ublažavanje njegovih efekata, dok u slučaju ozbiljne cyber prijetnje, ako je primjenjivo, mora pravovremeno obavijestiti potencijalno ugrožene klijente i pružiti informacije o odgovarajućim zaštitnim mjerama.
(5) Banka je dužna Agenciji dostaviti sljedeće:
   a) inicijalno obavještenje,
   b) privremeni statusni izvještaj, nakon inicijalnog obavještenja iz tačke a) ovog stava, čim se status izvornog IKT incidenta značajno promijeni ili se postupanje u vezi sa značajnim IKT incidentom promijeni na osnovu novih dostupnih informacija, a nakon toga prema potrebi, ažurirana obavještenja svaki put kad se pojave relevantne novosti o statusu, kao i na poseban zahtjev Agencije,
   c) konačni izvještaj, kada je analiza osnovnog uzroka IKT incidenta završena, nezavisno o tome da li su mjere za ublažavanje utjecaja već provedene i kada se procijenjene vrijednosti utjecaja mogu zamijeniti stvarnim podacima o utjecaju IKT incidenta.
(6) U zavisnosti od karakteristika IKT/cyber incidenta, banka je dužna razmotriti obavezu obavještavanja ostalih relevantnih organa i institucija unutar Bosne i Hercegovine.
(7) Nakon primanja informacije, Agencija će prema potrebi poduzeti sve potrebne mjere u svrhu zaštite stabilnosti finansijskog sistema.

IX UPRAVLJANJE IKT RIZICIMA POVEZANIM SA TREĆIM STRANAMA

Član 45.
Uspostavljanje okvira upravljanja rizicima trećih strana

(1) Nezavisno o odredbama Odluke o upravljanju eksternalizacijom u banci, banka je dužna uspostaviti upravljanje IKT rizicima povezanim sa trećim stranama čije su aktivnosti vezane uz IKT usluge i IKT sisteme, kao sastavnim dijelom IKT rizika u okviru za upravljanje IKT rizicima, iz člana 12. ove odluke.
(2) Upravljanje IKT rizicima povezanim sa trećim stranama pružaocima IKT usluga, banka je dužna uspostaviti u skladu sa sljedećim principima:
   a) banka koja ima sklopljene ugovore o obavljanju IKT usluga sa trećim stranama za potrebe svog poslovanja u svakom trenutku snosi potpunu odgovornost za poštovanje i izvršavanje svih obaveza iz ove odluke i primjenjivog zakonskog okvira,
   b) principom proporcionalnosti i uzimajući u obzir:
      1) prirodu, obim, složenost i važnost zavisnosti u području IKT sistema,

2) rizike koji proizlaze iz ugovora o upotrebi IKT usluga sklopljenih sa trećim stranama pružaocima IKT usluga, vodeći računa o ključnosti predmetne usluge, procesa ili funkcije, te o mogućem utjecaju na kontinuitet i dostupnost usluga i aktivnosti na nivou banke i na nivou grupe.

(3) Banka je dužna propisati i provoditi Politiku o korištenju IKT usluga trećih strana, a posebno IKT usluga kojima se podržavaju prioritetne funkcije, te je primjenjivati na pojedinačnoj, i prema potrebi, na konsolidovanoj osnovi.

(4) Banka je dužna pravovremeno obavijestiti Agenciju o svim planiranim ugovorima o upotrebi IKT usluga kojima se podržavaju prioritetne funkcije, kao i o tome da je određena funkcija postala prioritetna, poštujući odredbe čl. 28., 29. i 30. Odluke o upravljanju eksternalizacijom u banci.

Član 46.
Registar informacija

Banka je dužna održavati i redovno ažurirati, kako na nivou banke, tako i na konsolidovanom nivou, registar informacija u vezi sa svim ugovorima o korištenju IKT usluga koje pružaju treće strane pružaoci IKT usluga.

Član 47.
Procjena rizika

(1) Prije sklapanja ugovora o pružanju IKT usluga banka je dužna:
a) procijeniti da li ugovor obuhvata upotrebu IKT usluga kojima se podržava prioritetna funkcija,
b) procijeniti da li su ispunjeni nadzorni uslovi u pogledu ugovaranja,
c) utvrditi i procijeniti sve relevantne rizike povezane sa ugovorom, a u skladu sa članom 9. stav (1) Odluke o upravljanju eksternalizacijom, uključujući i rizik da taj ugovor doprinese jačanju koncentracijskog IKT rizika, u skladu sa članom 48. ove odluke,
d) provoditi dubinske analize potencijalnih trećih strana pružaoca IKT usluga i osiguravati adekvatnost treće strane pružaoca IKT usluga tokom cijelog procesa odabira i procesa procjene,
e) utvrditi i procijeniti sukobe interesa koje bi ugovor mogao izazvati.

(2) Banka je dužna ugovarati IKT usluge isključivo sa trećim stranama pružaocima IKT usluga koji ispunjavaju odgovarajuće standarde IKT sigurnosti. U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne funkcije, banka je dužna, prije sklapanja ugovora, utvrditi da pružalac IKT usluga koristi najsavremenije i najviše standarde IKT sigurnosti.

(3) Banka je dužna kontinuirano pratiti i tražiti garancije nivoa usklađenosti trećih strana pružaoca IKT usluga sa sigurnosnim ciljevima, mjerama i ciljevima banke.

(4) Banka je dužna osigurati i primjenjivati pravo pristupa podacima i reviziju treće strane pružaoca IKT usluga u skladu sa čl. 25., 26. i 27. Odluke o upravljanju eksternalizacijom u banci.

(5) Banka je dužna, u okvir upravljanja IKT rizicima, uključiti i procjenu rizika sigurnosti lanca snabdijevanja, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih direktnih dobavljača ili pružaoca usluga.

Član 48.
Preliminarna procjena koncentracijskog IKT rizika

U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne funkcije, banka je dužna prilikom utvrđivanja i procjene rizika iz člana 47. ove odluke, razmotriti i sljedeće:
a) rizike definirane članom 16. tačka h) Odluke o upravljanju eksternalizacijom u banci, te koristi i troškove alternativnih rješenja, kao što je angažman različitih trećih strana pružaoca IKT usluga, uzimajući u obzir podudaraju li se predviđena rješenja sa

poslovnim potrebama i ciljevima utvrđenim u Strategiji IKT sistema i Politici za upravljanje IKT rizicima i u kojoj mjeri,

b) potencijalne koristi i rizike podugovaranja, naročito u slučaju da je podizvođač izvan Bosne i Hercegovine, ukoliko je ugovorom predviđena mogućnost da treća strana pružalac IKT usluga može podugovoriti IKT usluge kojima se podržavaju prioritetne funkcije banke nekoj drugoj trećoj strani pružaocu IKT usluga,
c) odredbe prava o nesolventnosti koje bi se primjenjivale u slučaju stečaja treće strane pružaoca IKT usluga, kao i o svim ograničenjima do kojih bi moglo doći pri hitnom oporavku podataka banke,
d) usklađenosti sa zakonskim okvirom u Bosni i Hercegovini, u slučaju da se treća strana pružalac IKT usluga nalazi izvan Bosne i Hercegovine,
e) utjecaj potencijalno dugih ili složenih lanaca podugovaranja na sposobnost banke da u potpunosti prati ugovorene aktivnosti, kao i na sposobnost Agencije za izvođenje efikasnog nadzora nad bankom u tom slučaju.

Član 49.
Ugovor sa pružaocima IKT usluga

(1) Banka je dužna prava i obaveze banke i treće strane pružaoca IKT usluga jasno definirati u pisanoj formi. Potpuni ugovor, koji uključuje i sporazume o nivou usluga, je potrebno osigurati u pisanoj formi koja je ugovornim stranama dostupna u papirnom obliku ili u dokumentu u nekom drugom trajnom i pristupačnom formatu koji se može preuzeti.
(2) Banka je dužna osigurati usklađenost ugovora iz stava (1) ovog člana sa članom 19. stav (3) Odluke o upravljanju eksternalizacijom u banci.
(3) Ugovori o korištenju IKT usluga, pored uslova iz stava (2) ovog člana, trebaju uključiti i sljedeće:
   a) lokacije, posebno regije ili zemlje, na kojima će se pružati ugovorene ili podugovorene aktivnosti i IKT usluge, te na kojima će se obrađivati podaci, uključujući lokaciju čuvanja podataka, kao i zahtjev da treća strana pružalac IKT usluga unaprijed obavijesti banku ako namjerava promijeniti takve lokacije,
   b) odredbe o dostupnosti, autentičnosti, integritetu, dokazivosti i povjerljivosti u vezi sa zaštitom podataka, među ostalim i ličnih podataka,
   c) odredbe o osiguravanju pristupa ličnim i ostalim podacima koje obrađuje banka te o osiguravanju njihova oporavka i vraćanja u lako dostupnom formatu u slučaju nesolventnosti, sanacije ili prestanka poslovanja treće strane pružaoca IKT usluga ili u slučaju raskida ugovora,
   d) obavezu treće strane pružaoca IKT usluga da pruži pomoć banci bez dodatnih troškova ili uz unaprijed utvrđene troškove u slučaju IKT incidenta koji je povezan s IKT uslugom koju ta treća strana pruža banci,
   e) uslove za učestvovanje trećih strana pružaoca IKT usluga u programima za podizanje svijesti o sigurnosti u IKT i osposobljavanjima o digitalnoj operativnoj otpornosti koje provodi banke, a u skladu sa članom 21. ove odluke,
   f) specifikacije životnog ciklusa podataka banke,
   g) postupke rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja.
(4) Ugovori o korištenju IKT usluga koje podržavaju prioritetne poslovne funkcije, trebaju biti usaglašeni sa članom 19. stav (4) Odluke o upravljanju eksternalizacijom u banci i stavom (3) ovog člana, te trebaju uključiti i sljedeće:
   a) rokove za prethodne obavijesti i obaveze izvještavanja koje treća strana pružalac IKT usluga ima u odnosu na banku, uključujući i odredbe definirane članom 19. stav (3) tačka m) Odluke o upravljanju eksternalizacijom u banci,

b) zahtjeve da treća strana pružalac IKT usluga uvede i testira planove za nepredvidive situacije u poslovanju, kao i alate, politike i kontrole za sigurnost IKT sistema, uključujući i cyber sigurnost, kojima se banci osigurava odgovarajući nivo IKT sigurnosti za pružanje usluga, a u skladu sa prihvatljivim nivoom IKT rizika banke i primjenjivih regulatornih odredbi, a uključujući i zahtjeve u pogledu enkripcije podataka, mrežne sigurnosti i postupaka sigurnosnog praćenja,
c) obavezu treće strane pružaoca IKT usluga da učestvuje u TLPT-u banke, a u skladu sa članovima 25. – 27. ove odluke, te njegovu punu kooperativnost,
d) pravo kontinuiranog praćenja rada treće strane pružaoca IKT usluga, što uključuje sljedeće:
   1) odredbe definirane članom 19. stav (3) tačka g) Odluke o upravljanju eksternalizacijom u banci, uključujući i pravo na pristup i izradu kopija relevantne dokumentacije na licu mjesta pružaoca usluge, ako je prioritetna za poslovanje treće strane pružaoca IKT usluge, pri čemu drugi ugovorni aranžmani ili politike ne sprječavaju i ne ograničavaju efikasno ostvarivanje tih prava,
   2) pravo ugovaranja alternativnih nivoa osiguranja ako su obuhvaćena prava drugih klijenata,
   3) obavezu treće strane pružaoca IKT usluga da u potpunosti sarađuje tokom direktnih nadzora koje provodi Agencija i revizija koje provodi banka, uključujući i treće strane koje one imenuju,
   4) obavezu dostavljanja pojedinosti o obimu, postupcima kojih se treba pridržavati i učestalosti takvih nadzora i revizija,
e) izlazne strategije, posebno određivanje obaveznog adekvatnog prelaznog perioda:
   1) tokom kojeg će treća strana pružalac IKT usluga nastaviti pružati predmetne aktivnosti ili IKT usluge banci kako bi se smanjio rizik od poremećaja u radu banke ili kako bi se osigurala njena efikasna sanacija i restrukturiranje,
   2) u kojem banka može preći na usluge druge treće strane pružaoca IKT usluga ili se prebaciti na interna rješenja, u skladu sa složenošću usluge koja se pruža.

(5) Tokom pregovora o ugovorima sa pružaocem IKT usluga, banka je dužna razmotriti primjenu standardnih ugovornih klauzula koje su propisane zakonskom regulativom za konkretne usluge, a gdje je primjenjivo.

Član 50.
Izlazna strategija i raskid ugovora

(1) U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne funkcije, banka je dužna donijeti izlaznu strategiju i postupke koji su u skladu sa Politikom o korištenju IKT usluga trećih strana i planovima kontinuiteta poslovanja banke, poštujući odredbe člana 23. Odluke o upravljanju eksternalizacijom u banci.

(2) Banka je dužna osigurati mogućnost raskida ugovora o upotrebi IKT usluga, u skladu sa članom 21. Odluke o upravljanju eksternalizacijom u banci, uključujući i u sljedećim situacijama:
   a) praćenjem IKT rizika povezanih sa trećom stranom utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjena u izvršavanju aktivnosti koje se pružaju na osnovu ugovora, a što uključuje bitne promjene koje utječu na ugovor ili stanje treće strane pružaoca IKT usluga,
   b) uslijed slabosti pružaoca IKT usluga u vezi sa općim upravljanjem IKT rizikom, a posebno u načinu na koji osigurava dostupnost, autentičnost, povjerljivost, integritet i dokazivosti podataka, bilo da se radi o ličnim ili drugim osjetljivim podacima ili neosobnim podacima,
   c) Agencija zbog uslova ugovora ili okolnosti povezanih sa ugovorom ne može (više) efikasno nadzirati banku.

X UPRAVLJANJE ODNOSIMA SA KORISNICIMA PLATNIH USLUGA

Član 51.
Upravljanje odnosima s korisnicima platnih usluga

(1) Banka je dužna izraditi plan podizanja svijesti i nivoa razumijevanja korisnika platnih usluga o sigurnosnim rizicima povezanim s platnim uslugama, koji uključuje osiguravanje pomoći i uputstava korisnicima platnih usluga.
(2) Pomoć i uputstva koje se nude korisnicima platnih usluga trebali bi se pravovremeno ažurirati s obzirom na nove prijetnje i ranjivosti, a o promjenama bi trebalo pravovremeno obavještavati korisnike platnih usluga.
(3) Ako je to dopušteno u okviru funkcionalnosti proizvoda, banka je dužna dopustiti korisnicima platnih usluga da onemoguće određene platne funkcionalnosti povezane s platnim uslugama koje banka pruža korisniku platnih usluga.
(4) Ako je banka pristala na ograničenja potrošnje korisnika za platne transakcije izvršene putem određenog platnog instrumenta, banka je dužna korisniku omogućiti da prilagodi ta ograničenja do iznosa najvišeg dogovorenog ograničenja.
(5) Banka je dužna omogućiti da korisnici platnih usluga primaju upozorenja o iniciranju ili neuspjelim pokušajima iniciranja platnih transakcija čime im se omogućava da otkriju prevarno ili zlonamjerno korištenje njihovih računa.
(6) Banka je dužna informisati korisnike platnih usluga o ažuriranjima u pogledu sigurnosnih postupaka koja utječu na korisnike platnih usluga s obzirom na pružanje platnih usluga.
(7) Banka je dužna korisnicima platnih usluga pružiti pomoć s obzirom na sva pitanja, zahtjeve za podršku i obavještenja o nepravilnostima ili problemima u pogledu sigurnosnih pitanja povezanih sa platnim uslugama. Korisnici platnih usluga trebali bi biti primjereno informisani o tome kako je moguće dobiti navedenu pomoć.

XI RAZMJENA INFORMACIJA

Član 52.
Razmjena informacija

(1) Banka je dužna Agenciji dostavljati informacije i podatke o cyber prijetnjama, uključujući indikatore kompromitovanja, taktike, tehnike i procedure, upozorenja o cyber prijetnjama i alate za konfiguraciju, u mjeri u kojoj takve informacije i razmjena podataka:
   a) ima za cilj poboljšati digitalnu operativnu otpornost bankarskog sistema, posebno kroz podizanje svijesti u vezi sa cyber prijetnjama, ograničavanje ili ometanje mogućnosti širenja cyber prijetnji, podržavanje odbrambenih sposobnosti, tehnika otkrivanja prijetnji, strategija ublažavanja ili odgovora i oporavka,
   b) dalja razmjena informacije se odvija u okviru bankarskog sistema, što uključuje i razmjenu informacija sa svim ostalim subjektima za koje je Agencije izdala dozvolu za rad,
   c) razmjena informacija se provodi kroz aranžmane za razmjenu informacija koji štite potencijalno osjetljivu prirodu informacija koje se razmjenjuju i koji su uređeni pravilima poslovnog ponašanja u kojima se u potpunosti poštuju poslovna tajna, zaštita ličnih podataka i smjernica o politici tržišne konkurencije.
(2) U svrhu stava (1) ovog člana, Agencija će osigurati platformu i aranžmane za razmjenu informacija.
(3) Aranžmanima za razmjenu informacija iz stava (2) ovog člana, potrebno je definirati uslove za učešće i, prema potrebi, navesti detaljno, eventualno uključivanje javnih uprava i svojstvo u kojem oni mogu biti povezani na aranžmane za razmjenu informacija, uključivanje IKT pružaoca usluga, operativne elemente, uključujući i korištenje namjenskih IKT platformi.

XII IZVJEŠTAVANJE AGENCIJE

Član 53.
Obavještavanje i izvještavanje Agencije

(1) Banka je dužna Agenciji dostaviti sljedeće interne izvještaje i akte:
   a) Strategiju IKT sistema i operativne planove, definirane čl. 9. i 10. ove odluke,
   b) Politiku i procedure za upravljanje IKT rizicima, definirane članom 14. ove odluke,
   c) Politiku informacione sigurnosti, definiranu članom 17. ove odluke,
   d) Strategiju kontinuiteta poslovanja, definiranu članom 28. ove odluke,
   e) Politiku i procedure upravljanja IKT incidentima, definirane članom 41. ove odluke,
   f) Politiku i procedure testiranja digitalne operativne otpornosti, definirane članom 23. ove odluke,
   g) Politiku o korištenju IKT usluga trećih strana, definirane članom 45. ove odluke,
   h) Analizu utjecaja na poslovanje, Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, definirane čl. 29., 30. i 31. ove odluke,
   i) Planove komunikacije u krizi, definirane članom 20. ove odluke,
   j) Program podizanja svijesti o sigurnosti IKT sistema, definiran članom 21. ove odluke,
   k) Registar informacija u vezi sa svim ugovorima o korištenju IKT usluga koje pružaju treće strane pružaoci IKT usluga, definiran članom 46. ove odluke,
   l) Rezultate procjene IKT rizika, definirane članom 16. ove odluke,
   m) Izvještaje o upravljanju IKT rizicima, definirane članom 18. stav (8) ove odluke,
   n) Izvještaje prema organima banke, definirane članom 5. stav (1) tačka j) ove odluke,
   o) Izvještaje o obavljenim testovima digitalne operativne otpornosti iz člana 23. ove odluke,
   p) Izvještaje o testiranju planova kontinuiteta IKT-a, planova odgovora i oporavka, odnosno testiranja rezervnog i/ili lokalnog informatičkog centra definirane čl. 32.,33. i 34. ove odluke.

(2) Banka je dužna interne akte iz stava (1) tačke a) do k) dostavljati godišnje, odnosno odmah po njihovim izmjenama.

(3) Banka je dužna izvještaje iz stava (1) tačke l) do p) ovog člana dostavljati Agenciji 7 dana po usvajanju od strane organa upravljanja.

(4) Uprava banke je dužna pravovremeno obavijestiti Agenciju o svakoj značajnoj i kompleksnoj promjeni koja može imati utjecaja na IKT sistem banke, te dostaviti odgovarajuću dokumentaciju (procjenu IKT rizika navedene promjene, metodologiju upravljanja IKT projektima sa pratećom dokumentacijom i drugo).

XIII OBJAVA INFORMACIJA ZNAČAJNIH ZA JAVNOST

Član 54.
Objava informacija značajnih za javnost

Agencija može objaviti informacije, uključujući i mjere, za koje procijeni da su od značaja za javnost, a koje se odnose na upravljanje IKT sistemima, sigurnosti IKT sistema, cyber rizicima, kao i drugim specifičnim oblastima vezanim uz upotrebu IKT sistema.

XIV PRIJELAZNE I ZAVRŠNE ODREDBE

Član 55.
Dodatna uputstva za primjenu odluke

U svrhu primjene odredbi ove odluke direktor Agencije će donijeti pripadajuća uputstva u roku od 6 mjeseci od dana stupanja na snagu ove odluke.

Član 56.
Prijelazne i završne odredbe

(1) Danom početka primjene ove odluke prestaje da važi Odluka o upravljanju informacionim sistemom u banci („Službene novine Federacije BiH“, broj 81/17).
(2) Banka je dužna uskladiti svoje poslovanje sa odredbama ove odluke do 31.12.2025. godine.

Član 57.
Stupanje na snagu

Ova odluka stupa na snagu osmog dana od dana objavljivanja u „Službenim novinama Federacije BiH“, a primjenjuje se od 31.12.2025. godine.

Broj: U.O.-32-03/25
Sarajevo, 25.02.2025. godine

PREDSJEDNICA
UPRAVNOG ODBORA

Ivanka Galić, dipl. oec., s.r.