Radni nacrt
Odluke o upravljanju informacionim sistemom u banci
V1.0

Sadržaj

Na osnovu člana 81. Zakona o bankama ("Službene novine Federacije BiH", broj: 27/17) i člana 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 xx.xx.xxxx godine donosi

ODLUKU
O UPRAVLJANJU INFORMACIONIM SISTEMOM U BANCI

I OPŠTE ODREDBE

Član 1.
Predmet Odluke

(1) Odlukom o upravljanju informacionim sistemom u banci propisuju se uslovi koje je banka dužna da osigura i provodi u procesu upravljanja informaciono-komunikacionim sistemom, upravljanja rizicima informacione i komunikacione tehnologije, uključujući i zahtjeve (uslove) koji se odnose na ugovorne aranžmane i uspostavu nadzora od strane banke nad trećim stranama pružaocima informaciono-komunikacionih usluga, izvještavanje o značajnim informaciono-komunikacionim incidentima i cyber prijetnjama, testiranje digitalne operativne otpornosti i razmjena informacija o cyber prijetnjama.

(2) Ova odluka primjenjuje se 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 vezana uz upravljanje informaciono-komunikacionim sistemom i rizicima informaciono-komunikacionih tehnologija koja nisu regulisana ovom odlukom, a regulisana su drugim propisima, primjenjivati će se odredbe tog propisa.

Član 2.
Pojmovi - Definicije

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

a) **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.
b) **Informaciono-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.
c) **Software-ske komponente (software-ska imovina)** – uključuju aplikacijski software, sistemski software, baze podataka, software-ske razvojne alate, uslužne programe, te ostali software.
d) **Hardware-ske komponente (hardware-ska imovina)** – fizičke komponente informacionog sistema koje uključuju: računare i računarsku opremu, komunikacijsku opremu, medije za čuvanje podataka, te ostalu tehničku opremu koja podržava rad informacionog sistema.
e) **Informaciona imovina** – skup informacija u materijalnom i nematerijalnom obliku koje vrijedi zaštiti.
f) **IKT imovina** – je software-ska ili hardware-ska imovina koja se nalazi u poslovnom okruženju.
g) **Resursi informacionog sistema** – resursi koji uključuju informacionu imovinu, software-ske i hardware-ske komponente, ljude i procese.
h) **Korisnici informacionog sistema** – sva lica koja koriste IKT sistem (zaposlenici banke, pružaoca usluga, klijenti banke i drugo).
i) **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.
j) **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.
k) **IKT proizvod** - element ili skupina elemenata IKT sistema.
l) **IKT proces** - skup aktivnosti koje se provode radi oblikovanja, razvoja, ostvarivanja ili održavanja IKT proizvoda ili IKT usluge.
m) **Prioritetna ili važna funkcija** znači funkcija čiji bi poremećaj bitno narušio finansijske rezultate banke ili pouzdanost ili kontinuitet njegovih 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.
n) **Prioritetni ili važni dio informacionog sistema** znači dio informacionog sistema koji podržava prirotetnu ili važnu funkciju i uslugu i provedbu kontrola od strane Agencije u slučaju rane intervencije ili restrukture.
o) **Povjerljivost** – osobina da informacija nije dostupna ili otkrivena neovlaštenim licima ili procesima.
p) **Integritet** – osobina informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.
q) **Dostupnost** – osobina da informacija i proces bude pravovremeno dostupna i iskoristiva na zahtjev od strane ovlaštenog lica.
r) **Autentičnost** – osobina koja obezbjeđuje da je identitet lica zaista onaj za koji se tvrdi da jeste, odnosno tačnost, ažurnost u slučaju podataka.

s) **Neporecivost** – osobina koja osigurava nemogućnost poricanja izvršene aktivnosti ili primanja informacija (podataka).
t) **Dokazivost (sljedivost)**– osobina koja obezbjeđuje da svaka aktivnost u IKT sistemu može biti jednoznačno praćena do njenog izvora.
u) **Pouzdanost** – označava da IKT sistem dosljedno i očekivano vrši predviđene funkcije i pruža tačne informacije.
v) **Raspoloživost** – osobina imovine da je pravovremeno dostupna i upotrebljiva na zahtjev ovlaštenog lica.
w) **Sigurnost informacija** – osigurava da samo ovlašteni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).
x) **Sigurnost IKT sistema** - sposobnost IKT sistema da na određenom nivou pouzdanosti odolijevaju svim događajima koji mogu ugroziti dostupnost, autentičnost, integritet ili povjerljivost snimljenih, prenesenih ili obrađenih podataka ili usluga koje ti IKT sistemi nude ili kojima omogućuju pristup.
y) **Rizik** - mogućnost gubitka ili poremećaja uzrokovana incidentom i treba ga izražavati kao kombinaciju opsega takvog gubitka ili poremećaja i vjerovatnosti pojave tog incidenta.
z) **Rizik informaciono-komunikacijskih tehnologija i sigurnosni rizik (u daljem tekstu: IKT rizik)** predstavlja 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 obuhvaća i sigurnosne rizike koji proizilaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući cyber napade ili neadekvatnu fizičku zaštitu.
aa) **Ranjivost** znači slabost, osjetljivost ili nedostatak IKT proizvoda ili IKT usluga koje cyber prijetnja može iskoristiti.
bb) **Digitalna operativna otpornost** znači sposobnost banke da izgradi, osigura i preispituje svoj operativni integritet i pouzdanost 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.
cc) **Kontrole** – politike, procedure, postupci, prakse, tehnologije i organizacione strukture dizajnirane kako bi obezbijedile razumno uvjerenje da će poslovni ciljevi biti dostignuti i da će neželjeni događaji biti spriječeni ili detektovani.
dd) **Operativni i sistemski zapisi** – hronološki zapisi o aktivnostima na IKT imovini (na primjer: zapisi operativnih sistema, aplikacijskog software-a, baza podataka, mrežnih uređaja i slično).
ee) **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 uticaj na integritet, dostupnost, povjerljivost i/ili autentičnost usluga.
ff) **Izbjegnuti incident** - svaki događaj koji je mogao ugroziti dostupnost, autentičnost, 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.
gg) **Incident** - događaj koji ugrožava dostupnost, autentičnost, integritet ili povjerljivost snimljenih, prenesenih ili obrađenih podataka ili usluga koje IKT sistemi nude ili kojima omogućuju pristup.
hh) **Postupanje s incidentom** - sve radnje i postupci čiji je cilj sprečavanje, otkrivanje, analiza, zaustavljanje incidenta ili odgovor na njega te oporavak od incidenta.
ii) **Cyber napad –** zlonamjeran uticaj sa ciljem ugrožavanja informacione sigurnosti koji može rezultirati IKT incidentom.
jj) **Cyber sigurnost** - sve aktivnosti koje su neophodne za zaštitu od cyber prijetnji IKT sistema, korisnika tih sistema i drugih osoba na koje one utiču.

kk) **Ozbiljna cyber prijetnja -** cyber prijetnja za koju se na osnovu njezinih tehničkih karakteristika može pretpostaviti da može imati ozbiljan uticaj na IKT sisteme banke ili korisnike usluga banke uzrokovanjem znatne materijalne ili nematerijalne štete.

ll) **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 uticaja IKT incidenta ili cyber prijetnje, uključujući tehničke pojedinosti cyber napada, onih koji su odgovorni za napad te njihova načina rada i njihovih motiva.

mm) **Penetracijska testiranja vođena prijetnjama (TLPT)** znači 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").

nn) **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.

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

pp) **Analiza isplativosti (engl. cost-benefit analyses)** – metoda ekonomske analize kojom se upoređuju i vrednuju sve prednosti i svi nedostaci projekta analizom troškova i koristi.

qq) **Analiza uticaja na poslovanje (engl. business impact analyses 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 uticaja na poslovanje je identifikacija prioritetnih poslovnih funkcija, procesa i resursa IKT sistema kao dijela procesa upravljanja kontinuitetom poslovanja.

rr) **Ciljano vrijeme oporavka (engl. 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.

ss) **Ciljana tačka oporavka podataka (engl. 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.

tt) **Ciljani nivo oporavka usluge (engl. service delivery objective (SDO))** – nivo usluga koje treba postići tokom alternativnog načina procesiranja dok se ne izvrši povratak na normalan rad.

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

vv) **Promjena** – zahtjev za izmjenom podataka ili izmjenama nad postojećim funkcionalnostima IKT sistema.

ww) **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 informacionog sistema.

xx) **Zastarjeli IKT sistem** znači 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.

yy) **Treća strana** jeste organizacija - pravno ili fizičko lice koje je uspostavilo poslovne odnose ili sklopilo ugovore sa bankom u svrhu pružanja proizvoda ili usluge banci.

zz) **Pružatelj 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.

aaa) **Organi banke u smislu ove odluke su:** „nadzorni odbor“ i „uprava banke“.

II ODGOVORNOSTI

Član 3.
Interni akti

(1) Banka je dužna propisati i primijeniti 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), kao minimum, trebaju biti:
   a) usklađeni sa propisima, standardima i pravilima struke, te međusobno,
   b) redovno pregledani i ažurirani i
   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 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

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, te osigurava da uprava banke osigura uslove za njegovo provođenje,
b) uspostavi, održava i unapređuje proces upravljanja IKT rizikom, kao dio jedinstvenog procesa upravljanja rizicima banke, te osigurava da uprava banke osigura uslove za njegovo provođenje,
c) odlučuje o adekvatnoj organizacionoj strukturi banke sa jasnom i preciznom podjelom nadležnosti, dužnosti i odgovornosti, a kako bi osigurala 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 internu reviziju 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 uposlenika banke adekvatni za pružanje podrške efikasnom i sigurnom funkcionisanju IKT sistema i upravljanju IKT rizicima na kontinuiranoj osnovi,
e) osigurava da organizacija upravljanja sigurnošću IKT sistema bude nezavisna od organizacije upravljanja IKT sistemom u svom radu i izvještajnoj liniji,

f) 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.
g) usvaja:
   i. Strategiju IKT sistema,
   ii. Strategiju kontinuiteta poslovanja,
   iii. Politiku za upravljanje IKT rizicima,
   iv. Politiku informacione sigurnosti,
   v. Politiku upravljanja IKT incidentima,
   vi. Politiku za testiranje digitalne operativne otpornosti i
   vii. Politiku o korištenju IKT usluga trećih strana,

te osigura uslove za njihovo provođenje, nadzire njihovo provođenje i periodično ih revidira, a najmanje jednom godišnje analizira i prilagođava promjenama, uzimajući u obzir poslovni model banke, kompleksnost IKT sistema i sklonost ka preuzimanju rizika i
h) propiše sadržaj i periodičnost izvještavanja nadzornog odbora u vezi sa:
   i. upravljanjem IKT sistemom, uključujući izvještavanje o realizaciji operativnih planova, te najmanje o značajnim IKT incidentima, kao i odgovorima, oporavku i korektivnim mjerama,
   ii. upravljanjem IKT rizicima, uključujući izvještaj o stepenu digitalne operativne otpornosti i
   iii. ugovorima sklopljenim sa trećim stranama pružaocima IKT usluga, svim relevantnim planiranim materijalnim promjenama u vezi sa njima te potencijalnom uticaju tih promjena na prioritetne ili važne funkcije koje su podložne tim ugovorima, uključujući sažetak analize rizika za procjenu uticaja tih promjena.

Član 5.
Odgovornosti uprave banke

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

a) priprema prijedloge strategija i politika iz člana 4. tačka g) ove odluke za usvajanje nadzornom odboru, osigura provođenje istih na svim nivoima odlučivanja i u poslovnim procesima, te izvještava nadzorni odbor o njihovom provođenju,
b) 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 sljedivosti podataka, definisanih Strategijom IKT sistema,
c) uspostavi i osigura adekvatan okvir za upravljanje IKT rizicima, a koji je potrebno najmanje jednom godišnje analizirati i prilagoditi promjenama,
d) 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 (važne) funkcije,
e) prati izvršenje operativnih planova provođenja Strategije IKT sistema, kao i bitne izmjene,
f) osigura da su sve uloge i odgovornosti vezane uz upravljanje IKT sistemom adekvatno uspostavljene, jasno definirane i dodijeljene, vodeći računa o adekvatnoj segregaciji dužnosti,
g) osigura potrebne i adekvatne resurse za upravljanje IKT sistemom i IKT rizicima, uključujući i IKT rizike povezane sa trećim stranama pružaocima IKT usluga, uključujući dovoljan broj i

stručnu osposobljenost zaposlenika za pružanje podrške operativnim potrebama u procesu upravljanja IKT sistemom i upravljanju IKT rizicima, kao i za provođenje Strategije IKT sistema, te dovoljna finansijska sredstva za osiguravanje navedenog,

h) uspostavi i implementira odgovarajući sistem izvještavanja o upravljanju IKT sistemom, IKT rizicima i rizicima povezanim sa trećim stranama pružaocima IKT usluga,
i) 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 povezanom izloženosti rizicima i relevantnom dokumentacijom,
j) osigura da svi članovi osoblja, uključujući i nositelje ključnih funkcija, prođu odgovarajuće osposobljavanje o IKT rizicima, uključujući i o informacionoj sigurnosti, na godišnjoj osnovi ili češće, ako je to potrebno i
k) donosi sljedeće procedure i interne akte:
    i. Operativne planove provođenja Strategije IKT sistema,
    ii. Procedure za upravljanje IKT rizicima,
    iii. Procedure za testiranje digitalne operativne otpornosti,
    iv. Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, te Analizu uticaja na poslovanje (eng. BIA),
    v. Procedure upravljanja IKT incidentima,
    vi. Procedure upravljanja sigurnosnim i zaštitnim (regulatornim) kopijama,
    vii. Procedure upravljanja pristupom IKT sistemu,
    viii. Procedure za upravljanje ažuriranjima software-a,
    ix. Procedure za upravljanje zaštitom od malicioznog software-a,
    x. Procedure upravljanja IKT imovinom,
    xi. Metodologiju upravljanja IKT projektima,
    xii. Procedure nabave, razvoja i održavanja IKT sistema,
    xiii. Procedure upravljanja IKT promjenama,
    xiv. Procedure upravljanja zapisima IKT sistema,
    xv. Plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema,
    xvi. Plan edukacije uposlenika i
    xvii. Planove komunikacije u krizi.

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

(2) Član/članovi uprave banke odgovorni za upravljanje IKT sistemom i IKT rizikom dužni su posjedovati adekvatan nivo znanja i vještina da razumiju i procijene IKT rizik i njegov uticaj na poslovanje banke, kao i kontinuirano se educirati i pratiti posebne obuke, razmjerno veličini IKT rizika kojim se upravlja.

(3) Uprava banke je dužna uspostaviti funkcije upravljanja sigurnošću IKT sistema, što uključuje imenovanje lica zaduženog za sigurnost IKT sistema, te definisati ovlaštenja, odgovornosti i obim rada. 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 funkcijama upravljanja sigurnošću IKT sistema.

(4) Uzimajući u obzir princip proporcionalnosti naveden u čl. 13 ove odluke, funkcija upravljanja sigurnošću IKT sistema može biti dodijeljena kontrolnoj funkciji upravljanja IKT rizicima. Lice zaduženo za sigurnost IKT sistema odgovara članu uprave zaduženom za upravljanje rizicima ili upravljanje rizicima IKT sistema, ukoliko je drugo imenovano.

(5) 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.

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

Član 6.
Lice zaduženo za sigurnost IKT sistema (CISO)

(1) Lice zaduženo za sigurnost IKT sistema (CISO) treba biti kompetentno lice sa odgovarajućim stručnim kvalifikacijama, specijalističkim znanjima i iskustvom iz oblasti upravljanja IKT sigurnosti, te posjedovati relevantne međunarodno priznate certifikate iz oblasti IKT sigurnosti.

(2) CISO treba, kao minimum, da nadzire i koordinira aktivnosti vezane uz sigurnost IKT sistema, a što uključuje minimalno sljedeće:
   a) koordinira i sprovodi interne kontrole usklađene sa ovom odlukom,
   b) vrši nadzor i analizu IKT sistema, u cilju otkrivanja sigurnosnih prijetnji i ranjivosti,
   c) učestvuje u aktivnostima identifikacije i procjene IKT rizika i pružanju prijedloga mjera ovladavanja IKT rizicima, iz članova 15. – 19. ove odluke,
   d) učestvuje u izradi Politike informacione sigurnosti, iz člana 17. ove odluke, te daje prijedloge za njeno unapređenje, u skladu sa razvojem IKT sistema i IKT rizika u banci,
   e) prati promjene IKT sistema i analizira uticaj promjena IKT sistema na postojeće kontrole IKT sigurnosti, daje prijedlog uvođenja novih kontrola sigurnosti IKT sistema, uključujući i razvoj novih funkcionalnosti i IKT projekte,
   f) osigurava, prati i koordinira aktivnosti iz okvira za testiranje informacione sigurnosti,
   g) osigurava adekvatne i pravovremene aktivnosti razmjene informacija o IKT incidentima i cyber prijetnjama, definisane članom 51. ove odluke,
   h) učestvuje u procjeni IKT rizika i pružanju mjera ovladavanja IKT rizicima u slučaju angažovanja trećih strana pružaoca IKT usluga,
   i) prati sigurnosne rizike koji proizilaze iz korištenja usluga trećih strana pružaoca IKT usluga,
   j) osigurava, prati i koordinira aktivnosti vezane uz realizaciju programa podizanja svijesti o sigurnosti IKT sistema,
   k) učestvuje u radu odbora i radnih grupa koji su formirani za potrebe upravljanja sigurnošću IKT sistema i
   l) izvještava redovno upravu banke o aktivnostima vezanim uz stanje sigurnosti IKT sistema, a najmanje na kvartalnoj osnovi.

(3) CISO je dužan da redovno izvještava upravu banke o stanju i aktivnostima vezanim uz sigurnost IKT sistema, a minimalno na kvartalnom nivou.

(4) CISO je dužan:
   a) svoju profesionalnu kompetentnost održavati putem sistemske i stalne obuke, te pravovremeno se educirati o rizicima IKT sistema i tehnologija koje se koriste u banci,
   b) poznavati relevantne međunarodne standarde i smjernice koje se odnose na uspostavu i nadzor sigurnosti IKT sistema,

c) biti u toku sa najnovijim praksama upravljanja sigurnosnim IKT incidentima, kako bi bilo u mogućnosti efikasno odgovoriti na trenutne ili nove oblike cyber napada i
d) pratiti relevantna tehnološka dostignuća kako bi bolje razumijela mogući uticaj koji bi uvođenje novih tehnologija moglo imati na zahtjeve u pogledu IKT sigurnosti.

Član 7.
Interna IKT revizija

(1) Banka je dužna provoditi internu reviziju IKT sistema i sistema upravljanja IKT rizicima, u skladu sa zahtjevima propisanim Odlukom o sistemu internog upravljanja u banci, a na osnovu definisanog programa rada interne revizije.

(2) Banka je dužna planirati i provoditi internu reviziju IKT sistema u skladu sa metodologijom procjene IKT rizika, imajući u vidu da u određenim vremenskim intervalima budu redovno detaljno pregledani (obuhvaćeni) svi elementi okvira za upravljanje IKT rizicima i svi IKT procesi, a naročito oni koji podupiru prioritetne (važne) 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 neophodna 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 dokumentovati informacije na osnovu kojih je donesena ocjena adekvatnosti i efikasnosti kontrola u okviru oblasti koja je predmetom revizije, uključujući i podatke o revidiranim internim aktima, IKT procesima i testiranim uzorcima.

(5) Banka je dužna propisati postupke za upravljanje kašnjenjem u izvršenju naloženih mjera.

Član 8.
Eksterna revizija IKT sistema

(1) Banka je dužna obavljati eksternu reviziju IKT sistema na godišnjem nivou, u skladu sa propisima Agencije koji regulišu oblast eksterne revizije u bankama, ukoliko odredbama ove Odluke nije drugačije definisano.

(2) Ako Agencija utvrdi da eksterna revizija IKT sistema nije obavljena ili da revizorski izvještaj nije sastavljen 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 utvrdi da revizorska ocjena nije zasnovana na istinitim i objektivnim činjenicama, 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, a 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 za prethodnu poslovnu godinu Agencija nije prihvatila.

(4) Izvještaj o obavljenoj reviziji IKT sistema je poseban izvještaj, te je banka dužna dostaviti Agenciji navedeni izvještaj najkasnije do 31.03. tekuće godine.

(5) Banka je dužna da reviziju IKT sistema obavlja na godišnjem nivou.

(6) Agencija zadržava pravo nalaganja mjera propisanih Zakonom o bankama i propisima Agencije koji regulišu 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) definisati operativne planove koji podržavaju provođenje strategije IKT sistema i
c) uspostaviti postupke praćenja i mjerenja efikasnosti provođenja strategije IKT sistema.

(2) Strategija IKT sistema iz stava (1) ovog člana, treba da:
a) definiše povezanost i usklađenost strateških ciljeva IKT sistema sa poslovnim ciljevima banke,
b) definiše dugoročne i kratkoročne inicijative unapređenja IKT sistema banke, koje sadrže 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 ovisnosti o trećim stranama,
c) izloži pristup upravljanju IKT incidentima,
d) sadrži opis planova komunikacije u slučaju IKT incidenata,
e) definiše kako se okvirom za upravljanje IKT rizicima podupire poslovna strategija banke i njeni ciljevi,
f) utvrdi toleranciju na IKT rizik, u skladu sa sklonošću preuzimanja rizika banke, te analizirati uticaj tolerancije prilikom poremećaja u radu IKT sistema,
g) definiše jasne ciljeve u području informacione sigurnosti, uključujući dostupnost, povjerljivost, integritet i sljedivost podataka i IKT sistema, kao i ključne pokazatelje uspješnosti i ključne parametre rizika i
h) definiše strategiju banke vezanu za IKT rizik povezan sa trećim stranama pružaocima IKT usluga.

(3) Banka je dužna strategiju IKT sistema periodično ažurirati, a posebno prilikom izmjene poslovne strategije banke i značajnih promjena u strategiji za upravljanje IKT rizicima, 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 definišu aktivnosti koje će poduzeti kako bi se postigao cilj 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 proizilaze iz procjene IKT rizika, planirane

ugovore sa trećim stranama pružaocima IKT usluga, ljudske resurse, budžet, vremenske rokove i odgovorna lica i

c) budu predmetom redovnog praćenja i preispitivanja, a kako bi se osigurala njihova relevantnost i adekvatnost.

(2) Uprava banke treba biti jasno, detaljno i pravovremeno obaviještena o realizaciji i statusu aktivnosti definisanih operativnim planovima, 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:
   i. tačnu i pouzdanu obradu podataka neophodnih za obavljanje aktivnosti i pravovremeno pružanje usluga banke,
   ii. periode visoke opterećenosti sistema,
   iii. uvođenje novih tehnologija i
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 pohranjivati 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.

(2) Okvir za upravljanje IKT rizicima banke treba biti u potpunosti integrisan i usklađen sa sveukupnim okvirom upravljanja rizicima banke, a u skladu sa Odlukom o sistemu internog upravljanja u banci („Službene novine FBiH“, br. 39/21).

(3) Ispunjavanje uslova iz stava (1) ovog člana omogućava banci efikasno upravljanje IKT rizikom i donošenje adekvatnih odluka o preuzimanju IKT rizika, te osigurava provođenje

adekvatnih mjera za upravljanje tim rizikom, uključujući i osiguranje visokog nivoa digitalne operativne otpornosti, a u cilju brzog, efikasnog i sveobuhvatnog odgovara na IKT rizik.

(4) U skladu sa članom 36. stav 1. tačka a) Odluke o sistemu internog upravljanja, banka je dužna odgovornost za kontrolu i nadzor nad IKT rizicima dodijeliti kontrolnoj funkciji 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, te IKT kontrole koje su potrebne za propisnu i primjerenu zaštitu sve informacione i IKT imovine, u cilju svođenja uticaja IKT rizika na najmanju moguću mjeru, a u skladu sa ciljevima definisanim 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 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 i
   g) postupke za utvrđivanje i procjenjivanje postojanja IKT rizika koji proizilaze 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 (funkcija, procesa i imovine)

(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 i uspostaviti 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, uposlenici, izvođači i treće strane, te njihove međusobne povezanosti, te dokumentovati i redovno ažurirati,
   c) identifikovati i dokumentovati sve procese ovisne o trećim stranama pružaocima IKT usluga i identifikovati međusobne ovisnosti pružaoca usluga.

(3) U okviru mapiranja iz stava (2) tačka b) ovog člana, banka je dužna mapirati svu IKT imovinu, uključujući i onu na udaljenim lokacijama, mrežne resurse i hardware-sku opremu, te mapirati i konfiguracije IKT imovine, te veze između različite IKT imovine i njihove međuovisnosti.

(4) Banka je dužna klasifikovati identifikovane poslovne funkcije, podržavajuće procese i informacionu i IKT imovinu iz stava (2) ovog člana, uzimajući u obzir zahtjeve u pogledu povjerljivosti, integriteta i dostupnosti.

(5) Prilikom procjene rizika, banka je dužna preispitati adekvatnost klasifikacije informacione i IKT imovine.

(6) Banka je dužna odrediti jasnu odgovornost za informacionu i IKT imovinu.

(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 utiču na klasifikovane poslovne funkcije, podržavajuće procese i informacionu 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 koji utiču na poslovne funkcije, podržavajuće procese ili IKT imovinu.

(4) Banka je dužna najmanje jedanput 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 utiču 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.

(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 njezinom 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 preuzimanju IKT rizika banke.

(4) Kontrolama iz stava (2) ovog člana, banka je dužna:
a) osigurati sigurnost sredstava za prenos 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 i
d) osigurati da su podaci zaštićeni od rizika koji proizilaze iz upravljanja podacima, uključujući propuste u administraciji, rizike vezane 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 definišu pravila za zaštitu dostupnosti, autentičnosti, integriteta 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 promjenama IKT-a, a u skladu sa članom 40. ove odluke,
f) propisati i provoditi odgovarajuće i sveobuhvatne dokumentovane postupke za upravljanje ažuriranjima software-a, 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 iz oblasti IKT sistema, te planove odgovora i oporavka, a u skladu sa članom 32. ove Odluke i
j) propisati i provoditi odgovarajuće programe i planove osposobljavanje i podizanja svijesti o informacionoj sigurnosti, 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 neobičnih 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, definisati pragove upozorenja i kriterije za aktiviranje i pokretanje procesa odgovora na IKT incidente, uključujući mehanizme za automatsko upozoravanje relevantnog osoblja zaduženog za odgovor na IKT incidente.

(4) Banka je dužna osigurati adekvatno razdvajanje dužnosti uposlenika u procesu nadzora i procesima koji su predmet nadzora.

(5) Pri obavljanju 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 definisane članom 23. – 27. ove odluke.

(6) Banka je dužna kontinuirano pratiti i utvrđivati utiču li promjene u postojećem operativnom okruženju na implementirane kontrole, te da li je potrebno uvođenje dodatnih kontrola radi smanjivanja povezanih IKT rizika. Navedene promjene trebaju biti sastavnim dijelom formalnog procesa upravljanja promjenama.

(7) Banka je dužna osigurati dovoljno adekvatnih resursa, uključujuči i osposobljene uposlenike za:
a) praćenje aktivnosti korisnika, nastanka neobičnih pojava u IKT sistemu i IKT incidenata, a naročito cyber napada i
b) prikupljanje informacija o ranjivostima, cyber prijetnjama i IKT incidentima, a osobito cyber napadima, te za analizu njihovog vjerovatnog uticaja 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 penetracioni testovi, TLPT, testovi kontinuiteta poslovanja IKT-a, planovi za odgovor i oporavak i sl.), uputa iz revizija i drugo,
   b) bez odgađanja u slučaju identifikacije značajnih slabosti i nedostataka u okviru kritičnih (vitalnih) IKT sistema i
   c) obavezno nakon svake značajne promjene u IKT sistemu, procesima ili procedurama koje utiču na poslovne funkcije koje se podržavaju IKT sistemom, te IKT imovinu,

te ga kontinuirano poboljšavati na osnovu „naučenih lekcija" tokom njegovog provođenja i praćenja.

(2) Banka je dužna lekcije stečene iz testiranja digitalne operativne otpornosti, te iz stvarnih IKT incidenata, posebno cyber napada, kao i problema pri aktivaciji planova kontinuiteta poslovanja IKT-a, te planova odgovora i oporavka u području IKT-a, zajedno sa relevantnim informacijama razmijenjenim sa partnerskim finansijskim subjektima i procjenama prilikom revizije i supervizije, adekvatno i kontinuirano uključiti u proces procjene IKT rizika. Na osnovu navedenog, banka je dužna provoditi odgovarajuća preispitivanja relevantnih komponenti okvira za upravljanje IKT rizikom i njihove adekvatnosti.

(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 uticaj tih tehnologija na zahtjeve u pogledu IKT sigurnosti i digitalne operativne otpornosti. i
   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 definisati planove komunikacije u krizi, kojima će se uspostaviti jasni postupci za upravljanje internom i eksternom komunikacijom u slučaju aktiviranja planova kontinuiteta IKT-a 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 uposlenike i eksterne učesnike, kao i razlike u potrebama uposlenika uključenih u upravljanje IKT incidentom, posebno osoblja nadležnog za odgovor i oporavak, od osoblja koje je potrebno samo informisati.

(3) Banka je dužna osigurati odgovornu objavu barem značajnih IKT incidenata ili ranjivosti, klijentima, javnosti i partnerskim finansijskim subjektima, ovisno o IKT incidentu.

(4) 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 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 uposlenike, 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 pogrešaka, 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. Banka je dužna, prema potrebi, u programe osposobljavanja, uključiti i treće strane pružaoce IKT usluga.

(3) Banka je dužna osigurati da se programom osposobljavanja obezbijedi osposobljavanje uposlenika redovno, a najmanje jednom godišnje, vodeći posebno računa o pravovremenom osposobljavanju u pogledu prepoznatih IKT prijetnji.

Član 22.
Edukacija

(1) Banka je dužna da osigura stručno osposobljavanje i kontinuiranu edukaciju zaposlenika u organizacionoj jedinici IKT-a i upravljanja sigurnošću IKT sistema, kao i internog revizora IKT sistema, a kako bi osigurala da su navedeni uposlenici pravovremeno i adekvatno osposobljeni za obavljanje svojih funkcija, uzimajući u obzir razvoj IKT i IKT rizika, te veličinu i kompleksnost IKT sistema u banci.

(2) Banka je dužna izraditi detaljni godišnji plan edukacije uposlenika, definisati vremenske rokove, dokumentovati njegovu realizaciju, te kvartalno izvještavati o realizaciji plana.

(3) 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
(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 članom 23.- 27. ove odluke.

(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. Programom testiranja 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 neovisne interne ili vanjske osobe s 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 i otklanjanje 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. U slučaju prioritetnih (važnih) IKT sistema, Banka je dužna bez odgađanja otkloniti identifikovane slabosti i nedostatke.

(6) Banka je dužna osigurati obavljanje primjerenih testova IKT sistema, pri čemu:
   a) za sve IKT sisteme i aplikacije kojima se podupiru prioritetne (važne) funkcije banke se testiranje provodi barem jedanput godišnje,
   b) za IKT sisteme koji nisu kritični, proporcionalno rizicima, testiranje se provodi barem jedanput svake tri godine,
   c) prije svake izmjene postojeće ili dodavanja nove komponente IKT sistema i usluga, u slučaju da se radi o podržavanju prioritetnih (važnih) funkcija, kao i u slučaju značajnih izmjena IKT procesa i infrastrukture, uključujući promjene provedene zbog IKT incidenata, i
   d) u slučaju implementacije novih ili znatno izmijenjenih aplikacija dostupnih putem interneta.

Član 24.
Sadržaj testiranja informacione sigurnosti
(digital operational resilience testing)

Politikom i procedurama za testiranje digitalne operativne otpornosti iz člana 23. ove odluke, treba da obuhvataju izvođenje odgovarajućih testova, kao što su procjene i skeniranja ranjivosti, analize javno dostupnih izvora, procjene mrežne sigurnosti, analize odstupanja, preispitivanja fizičke sigurnosti, upitnici i software-ska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvedivo, testiranja na osnovu scenarija, testiranje kompatibilnosti, testiranje performansi, integralno testiranje (eng. end-to-end testing) i penetracijsko testiranje. 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 3 godine. Uzimajući u obzir rizik banke i operativne okolnosti, Agencija može, kada je to potrebno, tražiti od banke da smanji ili poveća ovu učestalost.

(2) TLPT-jem iz stava (1) ovog člana je potrebno obuhvatiti više ili sve prioritetne (važne) 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 (važne) funkcije, kao i IKT usluge, uključujući i one koje su eksternalizovane/ugovorene sa IKT pružaocima usluga, a kojima se podržavaju prioritetne (važne) funkcije.

(4) Banka je dužna procijeniti koje prioritetne (važne) 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 pružaoca usluga u TLPT-u. Banka u svakom trenutku zadržava potpunu odgovornost za osiguravanje usklađenosti sa ovom odlukom.

(6) Ne dovodeći u pitanje stav (2) i (3), u slučaju kada se opravdano može očekivati da će sudjelovanje treće strane pružaoca IKT usluga iz stava (5) ovog člana, negativno uticati na kvalitet ili sigurnost usluga odnosno povjerljivost podataka povezanih 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. U tom slučaju, TLPT se provodi pod vodstvom jedne imenovane banke, udruženog TLPT-a, u kojem učestvuje nekoliko banaka (eng. pooled testing) kojima treća strana pružalac IKT usluga pruža iste usluge.

(7) Udruženim TLPT-jem iz stava (6) ovog člana potrebno je obuhvatiti relevantan obim IKT usluga koje podržavaju prioritetne (važne) funkcije koje su banke ugovorile sa trećom stranom pružaocem IKT usluga. Broj banaka koje učestvuju u udruženom TLPT-ju treba biti srazmjeran složenosti i vrsti uključenih usluga.

(8) Udruženi TLPT smatra se TLPT-jem koji provode banke koje učestvuju u udruženom TLPT-ju i na njega se primjenjuju odredbe ove odluke.

(9) Banka je dužna, u saradnji sa trećim stranama pružaocima IKT usluga i drugim uključenim stranama, uključujući provoditelje testiranja, ali isključujući Agenciju, primjenjivati efektivne (adekvatne) kontrole upravljanja rizicima kako bi ublažila rizike od mogućeg uticaja na podatke, od oštećenja imovine i od poremećaja u radu prioritetnih (važnih) funkcija, usluga ili operacija u samoj banci, njenim partnerima ili finansijskom sektoru.

(10) 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.

(11) U slučaju da banka učestvuje u grupnom testiranju, prilikom čega drugo nadležno tijelo izvan zemlje izdaje potvrdu iz stava (9), banka je dužna Agenciji dostaviti potvrdu, sažetak relevantnih nalaza i planova za ispravljanje nedostataka.

(12) Ne dovodeći u pitanje takvu potvrdu, banka u svakom slučaju ostaje potpuno odgovorna za uticaje/posljedice testiranja iz stava (5).

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, kao i banke koje mogu koristiti interne provoditelje testiranja, na osnovu principa proporcionalnosti, a uzimajući u obzir sljedeće:
a) faktore povezane sa uticajem, posebno mjeru 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 i
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) koji imaju zadovoljavajući nivo stručnosti i adekvatno iskustvo i reference, te su među najadekvatnijim i najuglednijim provoditeljima testiranja,
b) posjeduju tehničke i organizacijske sposobnosti i posebno stručno znanje u području saznanja o prijetnjama, penetracionom testiranju i testiranju „red 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 i
e) su propisno i u potpunosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, uključujući i rizike od protupravnog i nemarnog postupanja.

(2) U slučaju anažovanja internih provoditelja testiranja, banka je dužna osigurati da, pored uslova iz stava (1) ovog člana, budu ispunjeni i sljedeći uslovi:

a) angažovanje internih provoditelja testiranja je odobreno od strane Agencije,
b) Agencija je potvrdila da banka ima dovoljno adekvatnih resursa, te da je osigurala izbjegavanje sukoba interesa prilikom dizajniranja i provođenja testa i
c) pružatelj 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) U sklopu okvira za upravljanje IKT rizicima, banka je dužna donijeti Strategiju upravljanja kontinuitetom 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 upravljanja kontinuitetom poslovanja iz stava (1) ove odluke, 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 uticaja na poslovanje

(1) Banka je dužna provoditi analizu uticaja na poslovanje (eng. BIA) analiziranjem svoje izloženosti znatnijim prekidima poslovanja i procjenom njihovih potencijalnih efekata (uključujući na povjerljivost, integritet i dostupnost), kvantitativno i kvalitativno, upotrebom internih i/ili eksternih podataka i analizom scenarija.

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

(3) U okviru analize uticaja na poslovanje potrebno je kao minimum:
a) navesti prioritetne (važne) funkcije i podržavajuće procese, a u skladu sa članom 15. stav (1) 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) ove odluke,
c) odrediti, kao minimum, RTO, RPO i SDO za svaku pojedinačnu poslovnu aktivnost, imajući u vidu eksternalizaciju i zavisnost od trećih strana.

(4) Pri utvrđivanju parametara RTO i RPO, banka je dužna uzeti u obzir i mogući opšti uticaj na cjelokupno finansijsko tržište. Navedenim parametrima banka je dužna osigurati da se u

ekstremnim scenarijima postigne dogovoreni nivo usluga., a u skladu sa strategijom IKT- i ciljevima informacione sigurnosti.

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

Član 30.
Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema

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

(2) Planom kontinuiteta IKT-a banka je dužna osigurati:
a) kontinuitet prioritetnih (važnih) funkcija banke u okviru definisanih 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 uticaja, štete i gubitka i
e) definisanje komunikacijskih mjera i mjera za upravljanje kriznim situacijama kojima se osigurava prenos 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 uticaj. 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 definisati procese, 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.

Član 31.
Planovi odgovora i oporavka IKT sistema

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

(2) Planovima odgovora i oporavka IKT sistema je potrebno definisati uslove za aktiviranje planova, kao i mjere koje je potrebno poduzeti kako bi se osigurala dostupnost, kontinuitet i oporavak minimalno prioritetnih (važnih) funkcija odnosno ključnih (važnih) 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 barem jedanput 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 i
   b) u slučaju svih bitnih promjena u IKT sistemima koji podržavaju prioritetne (važne) funkcije.

(2) Banka je dužna testirati i odgovarajuće planove kontinuiteta IKT-a, u slučaju da su prioritetne (važne) 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) 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 i
   c) preispitati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema, uzimajući u obzir rezultate testova iz stava (1), 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 uticati na primarni i rezervni informatički centar i sisteme oporavka,

b) osigurava kontinuitet prioritetnih (važnih) funkcija na isti način kao i primarni informatički centar ili pruža nivo usluga neophodnih da banka obavlja svoje prioritetne (važne) funkcije u okviru definisanih ciljeva oporavka (RTO, RPO i SDO),
c) je odmah dostupan zaposlenicima banke kako bi se osigurao kontinuitet prioritetnih (važnih) funkcija u slučaju nedostupnosti primarnog informatičkog centra i
d) je logički odvojen od primarnog informatičkog centra, 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 potrebno je detaljno dokumentovati i osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke.

Član 34.
Eksternalizacija IKT sistema izvan države

(1) U slučaju eksternalizacije cjelokupnog ili dijela IKT sistema izvan teritorije Bosne i Hercegovine, banka je dužna:
a) definisati prioritetne (važne) funkcije banke sa stanovišta kontinuiteta poslovanja i odvijanja istih u zemlji, uzimajući u obzir analizu uticaja na poslovanje, kao i važeće zakonske propise,
b) definisati odgovarajuće RTO, RPO i SDO parametre za funkcije definisane tačkom a) ovog stava, osiguravajući adekvatne nivoe usluge,
c) definisati ključne resurse IKT sistema banke koji podržavaju prioritetne (važne) definisane poslovne procese iz tačke a) ovog stava, uzimajući pri tome u obzir i podržavajuće resurse, te napredak i primjenu IKT u poslovnim procesima banke,
d) definisati plan kontinuiteta IKT-a i planove oporavka IKT sistema u zemlji,
e) osigurati lokalni informatički centar na teritoriji Bosne i Hercegovine kako bi osigurala kontinuitet prioritetnih (važnih) funkcija u zemlji na isti način kao i u okviru primarnog informatičkog centra odnosno pružanje nivoa usluga neophodnih da banka obavlja svoje prioritetne (važne) funkcije u okviru definisanih 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 definisati 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 važeći zakonski propisi i
i) osigurati ažurnost podataka definisanih tačkom h) u lokalnom informatičkom centru na dnevnoj osnovi.

(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 (važnih) 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 na udaljenu lokaciju,
f) te period čuvanja sigurnosnih kopija.

Obim i frekvenciju izrade sigurnosnih kopija, banka je dužna definisati u skladu sa zahtjevima analize uticaja na poslovanje i planovima za odgovor i oporavak IKT sistema, te procjenjivati u skladu s provedenom procjenom IKT rizika.

(3) Banka je dužna sigurnosne kopije osigurati na jednoj ili više sekundarnih lokacija, od kojih najmanje jedna mora biti dovoljno udaljena od primarne lokacije, na kojoj se nalaze izvorni podaci, na način da nisu izložene istim rizicima. Sigurnosne kopije trebaju biti ažurne i adekvatno zaštićene od odgovarajućih rizika (cyber napadi, rizici prilikom prijenosa i drugo).

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 (važnih) funkcija i usluga, kao i sprovedbu kontrola od strane Agencije u slučaju rane intervencije ili restrukture,
b) u lako dostupnom formatu kojem je moguće pristupiti/pročitati koristeći standardne, uobičajene, sveprisutne dostupne alate, neovisno od izvornih sistema u kojima su podaci nastali,
c) ažurne u skladu sa zahtjevima Agencije i
d) dostupne na centralnoj lokaciji banke.

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 potrebno je definisati kako banka

upotrebljava, prati i kontroliše svoje IKT sisteme i usluge. Navedene procedure trebaju biti potpune, ažurne i međusobno usklađene.

(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 pogrešaka.

(5) Banka je dužna:
   a) definisati i provoditi procedure upravljanja IKT imovinom, tokom cijelog njenog životnog ciklusa, od nabavke ili razvoja do povlačenja iz upotrebe, u cilju osiguranja dostupnosti, autentičnosti, integriteta i povjerljivosti podataka i
   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 kojim su definisane 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 sigurnošću IKT sistema.

(5) U zavisnosti od važnosti i veličine IKT projekta, te uticaju na prioritetne (važne) funkcije, banka je dužna redovno, kao i dodatno po potrebi, izvještavati upravu banke o uspostavi i napretku IKT projekta, te povezanim rizicima.

Član 39.
Nabava i razvoj IKT sistema

(1) Banka je dužna definisati i provoditi procedure kojima se propisuje način nabave, 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 definišu 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 i
   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 nabave 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 definisati 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 treba 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) i
   c) upravljanje sigurnosnim i funkcionalnim ispravkama (eng. patch).

(4) Banka je dužna da utvrdi početne verzije software-skih 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 da definiše, uspostavi i provodi 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 definiše i uspostavi Politiku upravljanja IKT incidentima i procedure upravljanja IKT incidentima koji 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 s 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 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. pogreške, neispravni rad, cyber napadi i sl.),
   h) planove za komunikaciju sa uposlenicima, 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 institucija,
   i) izvještavanje organa banke najmanje o značajnim IKT incidentima, uz objašnjenje njihovog uticaja, 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 i
   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 uticaj na osnovu sljedećih kriterija:
   a) broj i/ili relevantnost zahvaćenih klijenata ili finansijskih partnera, gdje je to primjenjivo, iznos ili broj transakcija na koje je uticao IKT incident, kao i činjenice da li je IKT incident imao uticaj 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 prouzročen IKT incidentom, u smislu dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka,
   e) kritičnost pogođenih usluga, uključujući transakcije i operacije banke i
   f) ekonomski uticaj IKT incidenta, posebno direktni i indirektni troškovi i gubici, u apsolutnom i relativnom smislu.

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

Član 43.
Učenje i razvoj

(1) Banka je dužna uspostaviti procedure analiza i pregleda nakon značajnih IKT incidenata i cyber prijetnji, analizirajući uzroke poremećaja i identificirajući potrebna poboljšanja u IKT procesima ili u okviru plana kontinuiteta IKT-a definisanog 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 preduzete kontrole bile efikasne, uključujući procjene sljedećeg:
a) brzinu u odgovoru na sigurnosna upozorenja i utvrđivanje uticaja IKT incidenta i njegove ozbiljnosti,
b) kvalitet i brzinu izvođenja forenzičke analize, gdje je to primjenjivo,
c) efikasnost eskalacije incidenta unutar banke i
d) efikasnost interne i eksterne komunikacije.

Član 44.
Izvještavanje o IKT incidentu i cyber napadu

(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, nakon prikupljanja i analize svih relevantnih informacija, dostaviti inicijalno obavještenje i izvještaj, a u skladu sa stavom (3) i (5) ovog člana.

(3) Inicijalno obavještenje i izvještaj iz stava (2) treba da sadrže sve potrebne informacije kako bi Agencija bila u mogućnosti procijeniti značaj IKT incidenta i njegov uticaj na cjelokupni finansijski sektor.

(4) 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.

(5) U slučaju značajnog IKT incidenta koji ima uticaj na finansijske interese klijenata, banka je dužna, bez nepotrebnog odlaganja, čim sazna za taj incident, obavijestiti svoje klijente o značajnom IKT incidentu i poduzetim mjerama za ublažavanje negativnih efekata incidenta. U slučaju značajne cyber prijetnje, banka je dužna, ako je to primjenjivo, pravovremeno obavijestiti svoje klijente koji bi mogli biti zahvaćeni tom cyber prijetnjom, te dostaviti informaciju o svim odgovarajućim zaštitnim mjerama koje bi klijenti mogli razmotriti.

(6) Banka je dužna Agenciji dostaviti sljedeće:
a) inicijalno obavještenje,
b) prelazni 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 i

c) konačni izvještaj, kada je analiza osnovnog uzroka IKT incidenta završena, neovisno o tome da li su mjere za ublažavanje uticaja već provedene i kada se procijenjene vrijednosti uticaja mogu zamijeniti stvarnim podacima o uticaju IKT incidenta.

(7) Nakon primanja informacije, Agencija će prema potrebi poduzeti sve potrebne mjere u svrhu zaštite stabilnosti finansijskog sistema.

(8) Ovisno o karakteristikama cyber incidenta, banka je dužna razmotriti obavezu obavještavanja ostalih relevantnih organa i institucija unutar države.

IX UPRAVLJANJE IKT RIZICIMA POVEZANIM SA TREĆIM STRANAMA

Član 45.
Uspostavljanje okvira upravljanja rizicima trećih strana

(1) Neovisno o odredbama Odluke o upravljanju eksternalizacijom u banci („Službene novine FBiH“, 75/22), 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:

i. prirodu, obim, složenost i važnost ovisnosti u području IKT sistema i

ii. rizike koji proizilaze iz ugovora o upotrebi IKT usluga sklopljenih sa trećim stranama pružaocima IKT usluga, vodeći računa o ključnosti ili važnosti predmetne usluge, procesa ili funkcije, te o mogućem uticaju 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 (važne) 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 (važne) funkcije, kao i o tome da je određena funkcija postala prioritetna (važna), poštujući odredbe člana 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 i 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 ili važna 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 i
   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 (važne) funkcije, banka je dužna, prije sklapanja ugovora, utvrditi da pružalac 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 članom 25., 26. i 27. Odluke o upravljanju eksternalizacijom u banci.

Član 48.
Preliminarna procjena koncentracijskog IKT rizika

U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne (važne) funkcije, banka je dužna prilikom utvrđivanja i procjene rizika iz člana 47. ove odluke, razmotriti i sljedeće:
a) rizike definisane 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 ciljevim utvrđenim u strategiji digitalne otpornost i u kojoj mjeri,
b) potencijalne koristi i rizike podugovaranja, naročito u slučaju da je podizvođač izvan države Bosne i Hercegovine, ukoliko je ugovorom predviđena mogućnost da treća strana pružalac IKT usluga može podugovoriti IKT usluge kojima se podržavaju prioritetne (važne) 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 Zakonom o zaštiti podataka te o efikasnom izvršavanju zakonodavstva BiH, u slučaju da se treća strana pružalac IKT usluga nalazi izvan države Bosne i Hercegovine,
e) uticaj 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.
Izlazna strategija i raskid ugovora

(1) U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne (važne) funkcije, banka je dužna donijeti izlaznu strategiju i postupke koji su u skladu sa politikom o korištenju IKT usluga 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, uključujući i:
   a) praćenjem IKT rizika povezanih s 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 utiču na ugovor ili stanje treće strane pružaoca IKT usluga,
   b) uslijed slabosti pružaoca IKT usluga u vezi sa opštim upravljanjem IKT rizikom, a posebno u načinu na koji osigurava dostupnost, autentičnost, povjerljivost, integritet i sljedivost podataka, bilo da se radi o ličnim ili drugim osjetljivim podacima ili neosobnim podacima i
   c) Agencija zbog uslova ugovora ili okolnosti povezanih sa ugovorom ne može (više) efikasno nadzirati banku.

Član 50.
Ugovor sa pružaocima IKT usluga

(1) Banka je dužna prava i obaveze banke i treće strane pružaoca IKT usluga jasno definisati 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 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 i
g) postupke rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja.

(4) Ugovori o korištenju IKT usluga koje podržavaju prioritetne (važne) 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 definisane 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:
   i. odredbe definisane 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,
   ii. pravo ugovoranja alternativnih nivoa osiguranja ako su obuhvaćena prava drugih klijenata,
   iii. obavezu treće strane pružaoca IKT usluga da u potpunosti sarađuje tokom direktnih nadzora i revizija koje provodi Agencija, banka, uključujući i treće strane koje one imenuju i
   iv. obavezu dostavljanja pojedinosti o obimu, postupcima kojih se treba pridržavati i učestalosti takvih nadzora i revizija,
e) izlazne strategije, posebno određivanje obaveznog adekvatnog prelaznog razdoblja:
   i. tokom kojega 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 i
   ii. 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 koja su propisana zakonskom regulativom za konkretne usluge, a gdje je primjenjivo.

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 utiču 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 obavijesti o nepravilnostima ili problemima u pogledu sigurnosnih pitanja povezanih s 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 sa Agencijom razmjenjivati informacije i obavještajne podatke o cyber prijetnjama, uključujući indikatore kompromitovanja, taktike, tehnike i procedure, upozorenja

o cyber sigurnosti 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) odvija se u okviru bankarskog sistema, što uključuje i razmjenu informacija sa svim ostalim subjektima za koje je Agencije izdala dozvolu za rad i
c) provodi se 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), Agencija će osigurati platformu i aranžmane za razmjenu informacija.

(3) Aranžmanima za razmjenu informacija iz stava (1) potrebno je definisati 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, definisanu članom 9. i 10. ove odluke,
b) Politiku i procedure za upravljanje IKT rizicima, definisane članom 14. ove odluke,
c) Politiku informacione sigurnosti, definisanu članom 17. ove odluke,
d) Strategiju upravljanja kontinuitetom poslovanja, definisanu članom 28. ove odluke,
e) Politiku i procedure upravljanja IKT incidentima, definisane članom 41. ove odluke,
f) Politiku i procedure testiranja digitalne operativne otpornosti, definisane članom 23. ove odluke,
g) Politiku o korištenju IKT usluga trećih strana, definisane članom 45. ove odluke,
h) Analizu uticaja na poslovanje, Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, definisane članom 28., 29. i 30. ove odluke,
i) Planove komunikacije u krizi, definisane članom 20. ove odluke,
j) Program podizanja svijesti o informacionoj sigurnosti, definisan članom 21. ove odluke,
k) Registar informacija u vezi sa svim ugovorima povezanim sa trećim stranama pružaocima IKT usluga, definisan članom 46. ove odluke,
l) Rezultate procjene IKT rizika, definisane članom 16. ove odluke,
m) Izvještaje o upravljanju IKT rizicima, definisane članom 18. stav (8) ove odluke,
n) Izvještaje prema organima banke, definisane članom 5. stav (1) tačka h),
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 definisane članom 32.-34. ove odluke.

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

(3) Banka je dužna izvještaje iz tačke (1) l) – p) 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 uticaja na IKT sistem banke, te dostaviti odgovarajuću dokumentaciju (metodologiju upravljanja IKT projektima sa pratećom dokumentacijom, procjenu IKT rizika navedene promjene 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, sigurnošću IKT sistema, cyber rizicima, kao i drugim specifičnim oblastima vezanim uz upotrebu IKT sistema i IKT.

XIV PRELAZNE I ZAVRŠNE ODREDBE

Član 55.
Dodatna uputstva za primjenu odluke

U svrhu primjene odredbi ove odluke direktor Agencije će donijeti pripadajuća uputstva.

Član 56.
Prelazne i završne odredbe

(1) Danom početka primjene ove odluke prestaje da važi Odluka o upravljanju informacionim sistemom u banci („Službene novine Federnacije BiH“, broj 81/17).

(2) Banka je dužna uskladiti svoje poslovanje sa odredbama ove odluke do 01.06.2025. 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 31.12.2024. godine.