На основу члана 5. став 1. тачка б, члана 20. став 2. тачка б. и члана 37. Закона о Агенцији за банкарство Републике Српске („Службени гласник Републике Српске“, бр. 59/13 и 4/17), члана 6. став 1. тачка б. и члана 19. став 1. тачка б. Статута Агенције за банкарство Републике Српске („Службени гласник Републике Српске“ број 63/17), Управни одбор Агенције за банкарство Републике Српске, на 16. сједници, одржаној 13.05.2025. године, доноси

О Д Л У К У
О УПРАВЉАЊУ ИНФОРМАЦИОНИМ СИСТЕМОМ И РИЗИЦИМА ИНФОРМАЦИОНЕ И КОМУНИКАЦИОНЕ ТЕХНОЛОГИЈЕ У БАНЦИ

I ОПШТЕ ОДРЕДБЕ

Члан 1.

(1) Овом одлуком се ближе дефинишу обавезе банке које се односе на управљање информационим системом, управљање ризицима информационе и комуникационе технологије, укључујући и захтјеве који се односе на уговоре и надзор пружаоца услуга информационих и комуникационих технологија од стране банке, извјештавање о значајним инцидентима у оквиру информационих и комуникационих технологија, као и сајбер пријетњама, тестирање дигиталне оперативне отпорности и размјена информација о сајбер пријетњама.

(2) Одредбе ове одлуке примјењују се на банке са сједиштем у Републици Српској, којима је Агенција за банкарство Републике Српске (у даљем тексту: Агенција) издала дозволу за рад.

(3) Одредбе ове одлуке банка је дужна примјењивати на појединачној и консолидованој основи.

(4) На питања у вези са управљањем информационим системом и управљањем ризицима информационе и комуникационе технологије која нису регулисана овом одлуком, а која су регулисана законом или другим подзаконским прописима, примјењују се одредбе тог закона или другог подзаконског прописа.

Члан 2.

(1) Појмови који се користе у овој одлуци имају сљедећа значења:

1) **Информациона и комуникациона технологија** (у даљем тексту: ИКТ) – технологија која омогућава аутоматизовано прикупљање, обраду, генерисање, складиштење, пренос, приказ и дистрибуцију информација, те располагање њима.
2) **Информациони систем** (у даљем тексту: ИКТ систем) - информациона и комуникациона технологија која је уређена као дио механизма или међусобно повезане мреже којима се пружа подршка пословању банке.
3) **Информациона имовина** – скуп информација у материјалном и нематеријалном облику коју вриједи заштитити.
4) **ИКТ имовина** – софтверска или хардверска имовина у мрежним и информационим системима које користи банка.
5) **Ресурси ІКТ система** – се односе на информациону имовину, ИКТ имовину, људе и процесе.
6) **Софтверска имовина** - обухвата апликативни и системски софтвер, базе података, алате за развој и тестирање, услужне програме и све друге софтверске производе који су инсталирани или лиценцирани за употребу унутар банке.
7) **Хардверска имовина** - физичке компоненте информационог система које укључују: рачунаре и рачунарску опрему, комуникациону опрему, медије за чување података, те осталу техничку опрему која подржава рад информационог система.
8) **Корисници ИКТ система** – сва лица која користе ИКТ систем (запослени банке, пружаоци услуга, клијенти банке и други).

9) **ИКТ услуге** - услуге које ИКТ системи пружају корисницима. Примјери укључују услуге уноса података, складиштење и обраду података, као и услуге извјештавања, праћења и подршке пословању и одлучивању.
10) **ИКТ пројекат** - сваки пројекат у којем се ИКТ системи и/или услуге мијењају, укидају или имплементирају. ИКТ пројекти могу бити дио ширих ИКТ програма или програма трансформације пословања.
11) **ИКТ производ** - елемент или скуп елемената ИКТ система.
12) **ИКТ процес** - скуп активности које се проводе ради обликовања, развоја, остваривања или одржавања ИКТ производа или ИКТ услуге.
13) **Критичне функције** – у складу са чланом 2. став 1. тачка 34. Закона о банкама Републике Српске (у даљем тексту: Закон о банкама).
14) **Кључне пословне активности** – у складу са чланом 2. став 1. тачка 35. Закона о банкама.
15) **Повјерљивост** - особина која подразумијева да подаци и информације нису доступни или откривени неовлашћеним лицима или процесима.
16) **Интегритет** - особина која подразумијева да подаци, информације и процеси нису неовлашћено или непредвиђено мијењани.
17) **Доступност** - особина која обезбјеђује да су подаци, информације и процеси увијек доступни и употребљиви на захтјев овлашћеног лица.
18) **Аутентичност** - особина која обезбјеђује да је идентитет лица заиста онај за који се тврди да јесте.
19) **Непорецивост** - особина која обезбјеђује немогућност порицања активности извршене у информационом систему или пријема информација.
20) **Доказивост** - особина која обезбјеђује да свака активност у ИКТ систему може једнозначно бити праћена до њеног извора.
21) **Поузданост** - означава да ИКТ систем досљедно и очекивано врши предвиђене функције и пружа тачне информације.
22) **Информациона безбједност** – представља скуп мјера неопходних за очување повјерљивости, доступности и интегритета информација и ИКТ система.
23) **Безбједност ИКТ система** - способност ИКТ система да на одређеном нивоу поузданости одолијева свим догађајима који могу угрозити доступност, аутентичност, интегритет или повјерљивост складиштених, пренесених или обрађених података или услуга које ти ИКТ системи нуде или којима омогућују приступ.
24) **Ризик** - могућност губитка или поремећаја узрокованог инцидентом, која се изражава као комбинација обима тог губитка или поремећаја и вјероватноће појаве инцидента.
25) **ИКТ ризик** – представља ризик од губитка услијед нарушавања повјерљивости, губитка интегритета система и података, неприкладности или недоступности система и података или немогућности промјене ИКТ-а у разумном временском периоду и уз разумне трошкове у случају промјене захтјева из окружења или пословања (особина прилагодљивости). Овај ризик обухвата и безбједносне ризике који произилазе из неадекватних или неуспјешних интерних поступака или спољних догађаја, укључујући сајбер нападе или неадекватну физичку заштиту.
26) **Дигитална оперативна отпорност** – значи способност банке да изгради, обезбиједи и преиспитује свој оперативни интегритет и поузданост тако да употребом услуга које пружају треће стране директно или индиректно обезбиједи цијели распон ИКТ способности потребних за безбједност ИКТ система које банка користи и којима се подржава континуирано пружање финансијских услуга и њихов квалитет, међу осталим и током поремећаја.
27) **Рањивост** – значи слабост, осјетљивост или недостатак ИКТ производа или ИКТ услуга које сајбер пријетња може да искористи.
28) **Контроле** – обухватају политике, процедуре, праксе, технологије и организационе структуре које се односе на ІКТ систем утврђене, како би се обезбиједило разумно увјерење

да ће пословни циљеви бити остварени и да ће нежељени догађаји бити спријечени или откривени.

29) **Запис** – хронолошка евиденција о активностима на ИКТ имовини (на примјер: записи оперативних система, апликативног софтвера, база података, мрежних уређаја, система за откривање неовлашћеног приступа и активности на ИКТ систему и слично).
30) **Оперативни или безбједносни инцидент** (у даљем тексту: ИКТ инцидент) – један догађај или низ повезаних догађаја које банка није планирала, а који имају или ће вјероватно имати негативан утицај на интегритет, доступност, повјерљивост података и/или аутентичност услуга.
31) **Избјегнути инцидент** – означава сваки догађај који је могао да угрози интегритет, доступност, повјерљивост података и/или аутентичност услуга, али је успјешно спријечен да се реализује или се није остварио.
32) **Поступање с инцидентом** - све радње и поступци чији је циљ спречавање, откривање, анализа, заустављање инцидента или одговор на њега те опоравак од инцидента.
33) **Сајбер безбједност** - све активности које су неопходне за заштиту од сајбер пријетњи ИКТ система, корисника тих система и других особа на које оне утичу.
34) **Сајбер напад**- злонамјеран утицај са циљем угрожавања информационе безбједности који може проузроковати ИКТ инцидент.
35) **Сајбер пријетња** - свака могућа околност, догађај или дјеловање које би могло оштетити, пореметити или на други начин негативно утицати на ИКТ систем, кориснике ИКТ система и друге особе.
36) **Озбиљна сајбер пријетња** - сајбер пријетња за коју се на основу њених техничких карактеристика може претпоставити да може имати озбиљан утицај на ИКТ системе банке или кориснике услуга банке узроковањем знатне материјалне или нематеријалне штете.
37) **Сазнања о пријетњама** - информације које су прикупљене, преобликоване анализиране, протумачене или обогаћене како би се добио контекст неопходан за доношење одлука и како би се омогућило релевантно и неопходно разумијевање за ублажавање утицаја ИКТ инцидента или сајбер пријетње, укључујући техничке појединости сајбер напада, оних који су одговорни за напад, те њиховог начина рада и њихових мотива.
38) **Пенетрациона тестирања вођена пријетњама (TLPT)** подразумијева оквир који опонаша тактике, технике и процедуре стварних актера пријетњи, које се сматрају стварном сајбер пријетњом и који пружа контролисано, прилагођено тестирање критичних продукционих система банке, вођено сазнањима о пријетњама („црвени тим“).
39) **Ланац чувања повезаних доказа** - процес који обезбјеђује да се све информације и материјали који су прикупљени као докази правилно документују, чувају и преносе тако да се одржи њихов интегритет, аутентичност и непромијењеност. Овај поступак омогућава да се прати свако кретање и руковање доказима од тренутка њиховог прикупљања до тренутка када се користе у судским поступцима или другим формама ревизије.
40) **Застарјели ИКТ систем** - означава ИКТ систем који је на крају свог животног циклуса, а који због технолошких или комерцијалних разлога није погодан за надоградњу или поправак или за којег његов добављач или пружалац ИКТ услуга више не пружа подршку, али је још увијек у употреби и подржава функције банке.
41) **Резервна копија података** (енгл. backup) - копија изворних података који су потребни за поновно успостављање пословних процеса банке, те осталих података за које банка процијени да их је потребно чувати.
42) **Анализа утицаја на пословање** (енгл. business impact analyses BIA) – процес који обухвата процјену квантитативних и квалитативних ефеката који би могли настати у случају недоступности пословних процеса и ресурса ИКТ система услијед одређеног инцидента, нежељеног догађаја или хаварије. Циљ анализе утицаја на пословање је идентификација кључних пословних активности, процеса и ресурса ИКТ система као дијела процеса управљања континуитетом пословања.

43) **Захтијевано вријеме опоравка – RTO** (енгл. recovery time objective) - најдуже прихватљиво вријеме недоступности пословног процеса банке и ресурса ИКТ система потребних за одвијање пословног процеса, тј. вријеме током кога је потребно обновити (опоравити) пословни процес.

44) **Циљана тачка опоравка – RPO** (енгл. recovery point objective) - најдужи прихватљиви период од посљедње резервне копије података до наступања недоступности пословног процеса, тј. најдужи прихватљив период губитка података у случају инцидента.

45) **Циљани ниво опоравка услуге** - SDO (енгл. service delivery objective) – ниво услуга које треба постићи током алтернативног начина процесирања док се не изврши повратак на нормалан рад.

46) **Промјена** – захтјев за промјеном (енгл. Change Request) или измјеном било ког аспекта ИКТ сервиса, система, инфраструктуре, процеса или документације.

47) **Кориснички захтјев** - захтјев корисника ИКТ система (енгл. User Request) за приступ одређеним ресурсима ИКТ система или услугама, захтјев за информације или савјет, те остали стандардни захтјев (нпр. ресетовање лозинке, захтјев за опрему и др.) који не спадају у категорију инцидената или промјена.

48) **Трећа страна** – физичко или правно лице које је успоставило пословни однос или склопило уговор са банком у сврху пружања производа или услуге, укључујући пружаоце екстернализованих услуга.

49) **ИКТ ризик повезан с трећим странама** - ИКТ ризик који може настати у вези с употребом ИКТ услуга које пружају треће стране или њихови подизвођачи у домену ИКТ-а.

50) **Пружалац ИКТ услуга** је трећа страна која обавља одређену активност из подручја ИКТ-а, дјелимично или у цјелини, на основу уговора закљученог са банком.

51) **Пружалац ИКТ услуга унутар групе** - друштво које је дио финансијске групе и које углавном пружа ИКТ услуге финансијским субјектима унутар исте групе.

52) **Општи подаци** – подаци који спадају у категорију личних или осјетљивих података.

53) **Органи управљања банке** - надзорни одбор и управа банке.

(2) Појмови који нису дефинисани овим чланом, а користе се у овој одлуци, имају значење у складу са законским прописима и другим подзаконским прописима.

II ОДГОВОРНОСТИ

Члан 3.

(1) Банка је дужна да донесе и примијени интерна акта, у виду стратегија, политика, методологија, процедура и радних упутстава, којима се уређује управљање ИКТ системом, укључујући употребу, праћење и надзор ИКТ система.

(2) Интерни акти из става 1. овог члана, као минимум требају бити:

1) усклађени са законским и подзаконским прописима, стандардима и правилима струке, захтјевима Агенције, као и међусобно,

2) редовно, а најмање једном годишње, прегледани и ревидирани, те ажурирани у случају значајних промјена у банци те окружењу у којем банка послује и

3) потпуни, детаљни и примјењиви.

(3) Банка је дужна обезбиједити да су сви корисници ИКТ система упознати са садржајем интерних аката која се односе на ИКТ систем, у складу са њиховим овлашћењима, одговорностима и потребама.

(4) Уговори, налази ревизије, извјештаји које разматрају органи банке, упутства и остали документи треба да буду сачињени, односно преведени на један од језика у званичној употреби у Републици Српској.

Члан 4.

Надзорни одбор банке дужан је, као минимум, да:

1) успостави адекватан систем управљања ИКТ системом, као и систем за мјерење, праћење, контролу и управљање ИКТ ризиком, као дио свеобухватног система управљања ризицима у банци, како би се постигао висок степен дигиталне оперативне отпорности,
2) успостави адекватну организациону структуру са јасно дефинисаним и разграниченим надлежностима, дужностима и одговорностима, стручним квалификацијама и потребним компетенцијама, укључујући улоге и одговорности чланова управе банке, водећи рачуна о томе да су број и потребне вјештине запослених адекватни за пружање подршке ефикасном и безбједном функционисању ИКТ система и управљању ИКТ ризицима на континуираној основи,
3) обезбиједи да управљање информационом безбједношћу у свом раду и линији извјештавања буде независно од управљања ИКТ системом,
4) усваја буџет за испуњење потреба банке у погледу дигиталне оперативне отпорности, у погледу свих врста ресурса, укључујући и релевантне програме за подизање свијести о информационој безбједности и оспособљавање за дигиталну оперативну отпорност, као и стицања знања и вјештина у области ИКТ-а за све запослене у складу са чланом 21. ове Одлуке,
5) усвоји стратегију ИКТ система, стратегију за дигиталну оперативну отпорност и политику информационе безбједности, те обезбиједи услове за њихово спровођење, надзире њихово спровођење и периодично их ревидира, а најмање једном годишње анализира и прилагођава промјенама, узимајући у обзир пословни модел банке, комплексност ИКТ система и склоност ка преузимању ризика,
6) пропише садржај и периодичност извјештавања надзорног одбора и других релевантних одбора, тијела или лица у вези са:
   1. управљањем ИКТ системом, укључујући извјештавање о реализацији оперативних планова,
   2. управљање ИКТ ризицима, укључујући извјештај о степену дигиталне оперативне отпорности,
   3. значајним ИКТ инцидентима, укључујући план одговора, активности опоравка и корективне мјере,
   4. свим уговорима склопљеним са трећим странама у домену ИКТ-а, те процјеном ризика трећих страна,
   5. свим релевантним промјенама материјално значајних активности, процјеном ризика, потенцијалним утицајем тих промјена на критичне функције и/или кључне пословне активности, укључујући закључке анализе ризика и процјене утицаја тих промјена.

Члан 5.

(1) Управа банке је дужна, као минимум, да:

1) припрема приједлоге стратегија и политика из члана 4. тачка 5) ове одлуке које усваја надзорни одбор, обезбиједи њихово спровођење на свим нивоима одлучивања и у пословним процесима, те редовно извјештава надзорни одбор о њиховом спровођењу,
2) осигура адекватан оквир за управљање ИКТ ризицима, како би се постигао висок степен дигиталне оперативне отпорности, који је потребно ревидирати најмање на годишњем нивоу,
3) осигура да су све улоге и одговорности у вези са управљањем ИКТ системом, ИКТ ризиком, информационом безбједношћу и континуитетом пословања, укључујући органе управљања, адекватно успостављене, јасно дефинисане и додијељене, водећи рачуна о адекватној сегрегацији дужности, ефикасној и благовременој комуникацији, међусобној сарадњи и координацији,
4) осигура потребне и адекватне ресурсе за управљање ИКТ системом и ИКТ ризицима, укључујући и ИКТ ризике повезане са трећим странама. Ово подразумијева:
   1. довољан број запослених са одговарајућим стручним квалификацијама и вјештинама за пружање подршке оперативним потребама ИКТ-а и процесима управљања ИКТ

ризицима на континуираној основи, како би се обезбиједило спровођење стратегије ИКТ система и

2. довољан буџет за претходно наведено,

5) на основу процјене ризичног профила банке, као и обима и сложености њених активности и услуга, редовно преиспитује ризике који су утврђени у вези са уговорима о употреби ИКТ услуга којима се подржавају критичне функције и кључне пословне активности,

6) усваја и прати реализацију оперативних планова којима је подржано спровођење стратегије ИКТ система, као и значајне измјене ових планова,

7) периодично преиспитује начин на који банка проводи политику континуитета пословања у подручју ИКТ-а, те планова одговора и опоравка,

8) успостави одговарајући систем извјештавања о управљању ИКТ системом, ИКТ ризицима и ризицима повезаним са трећим странама,

9) припрема и периодично преиспитује буџет за испуњење потреба банке у погледу дигиталне оперативне отпорности, за све врсте имовина, укључујући и релевантне програме за подизање свијести о информационој безбједности и оспособљавање за дигиталну оперативну отпорност, као и стицања знања и вјештина у области ИКТ-а за све запослене у складу са чланом 21.,

10) успостави функцију за праћење уговора о употреби ИКТ услуга склопљених са трећим странама или именује члана вишег руководства који ће бити одговоран за надзор над повезаним ризицима и релевантном документацијом,

11) осигура да сви запослени, укључујући носиоце кључних функција, прођу одговарајуће оспособљавање о ИКТ ризицима и информационој безбједности, на годишњем нивоу или чешће ако је потребно и

12) доноси и проводи планове и процедуре у вези са управљањем ИКТ системима и информационом безбједношћу, укључујући, али не ограничавајући се на, оперативне планове, процедуре за управљање ИКТ ризицима, управљање ИКТ инцидентима, управљање резервним копијама података, управљање приступом ИКТ системима, управљање безбједносним исправкама и ажурирањем софтвера, заштита од злонамјерног софтвера и других безбједносних пријетњи, управљање ИКТ имовином, управљање ИКТ пројектима, управљање набавком и одржавањем ИКТ система, управљање ИКТ промјенама, управљање записима, као и планове континуитета пословања у подручју ИКТ-а, планове одговора и опоравка ИКТ система, анализу утицаја на пословања и планове комуникације у кризним ситуацијама.

(2) Чланови управе банке одговорни за управљање ИКТ системом и ИКТ ризицима треба да посједују адекватан ниво знања и вјештина за разумијевање и процјену ИКТ ризика и његов утицај на пословање банке. Такође, дужни су да редовно учествују у обукама из овог домена, сразмјерно нивоу ИКТ ризика којима управљају.

(3) Управа банке је дужна успоставити функцију управљања информационом безбједношћу, укључујући именовање лица одговорног за информациону безбједност и дефинисање његових овлашћења, одговорности и обима рада. При том је дужна обезбиједити независност и објективност ове функције тако што ће осигурати да она буде адекватно одвојена од оперативних процедура везаних за ИКТ. Такође, у складу са величином, врстом, обимом и сложеношћу ИКТ система, као и природом, обимом и сложеношћу својих услуга, активности и пословања, управа банке је дужна проценити потребан број запослених у функцији управљања информационом безбједношћу.

(4) Управа банке је дужна да именује најмање једно лице задужено за спровођење планова комуникације у случају ИКТ инцидента, која ће у ту сврху обављати функцију комуникације са јавношћу и медијима.

(5) Управа банке је дужна размотрити потребу формирања посебног тијела које ће координисати активности које се односе на ИКТ систем, узимајући у обзир величину банке, природу, обим и сложености својих услуга, активности и пословања, унутрашњу организацију, те величину и комплексност ИКТ система.

Члан 6.

(1) Лице одговорно за информациону безбједност треба бити компетентно лице с одговарајућим стручним квалификацијама, специјалистичким знањима и искуством у области управљања информационом безбједношћу и при том посједује релевантне међународно признате сертификате из ове области.

(2) Лице из става 1. овог члана треба да надзире и координише активности у вези са информационом безбједношћу, а што укључује најмање сљедеће:

1) координише и спроводи интерне контроле у складу са овом одлуком и релевантним стандардима,
2) врши надзор и анализу ИКТ система, с циљем откривања безбједносних пријетњи и рањивости,
3) учествује у активностима идентификације и процјене ИКТ ризика и пружању приједлога мјера за управљање ИКТ ризицима из чланова 15. – 19. ове одлуке,
4) учествује у изради политике информационе безбједности, из члана 17. ове одлуке, те даје приједлоге за њено унапређење, у складу са развојем ИКТ система и ИКТ ризика у банци,
5) прати промјене које се спроводе на ИКТ системима, укључујући ИКТ пројекте и развој нових функционалности, те анализира утицај ових промјена на постојећи ниво информационе безбједности и предлаже мјере заштите и безбједносне контроле,
6) учествује у изради и имплементацији планова одговора на ИКТ инцидент, укључујући опоравак,
7) обезбјеђује, прати и координише активности повезане са спровођењем програма тестирања дигиталне оперативне отпорности, дефинисаног чланом 35. ове одлуке,
8) обезбјеђује адекватну и благовремену размјену информација о ИКТ инцидентима и сајбер пријетњама, у складу са члановима 34. и 50. ове одлуке,
9) учествује у процјени ИКТ ризика и предлаже мјере за третман ових ризика у случају ангажовања пружаоца ИКТ услуга, као и њихове усклађености са захтјевима ове одлуке
10) прати безбједносне ризике који произилазе из коришћења услуга и производа трећих страна;
11) обезбјеђује, прати и координише активности повезане са спровођењем програма подизања свијести о информационој безбједности,
12) учествује у раду одбора и радних група задужених за управљање информационом безбједношћу.

(3) Лице из става 1. овог члана је дужно да најмање квартално, извјештава управу банке о стању и активностима које се односе на информациону безбједност.

(4) Професионалну компетентност лице из става 1. овог члана одржава кроз систематску и континуирану обуку, при том:

1) се благовремено едукује о ризицима ИКТ система и технологијама које се користе у банци,
2) прати и познаје релевантне међународне стандарде и смјернице који се односе на успостављање и надзор информационе безбједности,
3) је у току са најновијим праксама управљања ИКТ инцидентима, како би могао да обезбиједи ефикасан одговор на актуелне или нове облике сајбер напада,
4) прати релевантна технолошка достигнућа како би боље разумио потенцијални утицај који би увођење нових технологија могло имати на захтјеве информационе безбједности.

Члан 7.

(1) Функција интерне ревизије дужна је у складу са захтјевима прописаним Одлуком о систему управљања у банци, спроводити редовне ревизије у подручју ИКТ-а, а на основу дефинисаног програма рада интерне ревизије.

(2) Учесталост активности функције интерне ревизије у подручју ИКТ-а треба бити сразмјерна ИКТ ризицима у банци, при чему сви елементи оквира за управљање ИКТ ризицима и сви ИКТ процеси морају бити детаљно прегледани унутар дефинисаног ревизијског циклуса.

(3) Лица која проводе ревизије у подручју ИКТ-а треба да посједују адекватна стручна знања и вјештине у овом подручју.

Члан 8.

(1) Банка је у обавези да спроводи спољну ревизију ИКТ система на годишњем нивоу, у складу са Законом и подзаконским актима Агенције који регулишу област спољне ревизије у банкама, уколико одредбама ове одлуке није другачије дефинисано.

(2) Ако Агенција утврди да привредно друштво за ревизију (у даљем тексту: спољни ревизор) није обавило ревизију IKT система банке или да извјештај о ревизији није у складу са законом, подзаконским актима донесеним на основу закона, прописима из области ревизије и правилима ревизорске струке или ако се обављеним надзором пословања банке у овом сегменту или на други начин утврди да ревизорска оцјена о стању ИКТ система и адекватности управљања ИКТ системом није заснована на истинитим и објективним чињеницама, може одбити ревизорски извјештај и захтијевати од банке да ревизију обави друго привредно друштво за ревизију о трошку банке или, када то оцијени потребним, директно именује привредно друштво за ревизију о трошку банке.

(3) Спољни ревизор не може бити лице чији извјештај о обављеној ревизији ИКТ система за претходну пословну годину Агенција није прихватила.

(4) Спољни ревизор је дужан да Агенцији, најмање 30 дана прије почетка обављања ревизије ИКТ система, достави план обављања ревизије, из којег су видљива подручја која су предмет ревизије, назначена имена лица која ће обављати ревизију и њихов ангажман, те вријеме трајања ревизије.

(5) Приликом обављања ревизије ИКТ система спољни ревизор је дужан узети у обзир екстернализоване услуге и њихов значај и утицај на ИКТ систем, те у складу с тим развити план ревизије и ефикасан приступ ревизији.

(6) Спољни ревизор је дужан сачинити ревизорски извјештај о обављеној ревизији информационог система, те дати оцјену о стању ИКТ система и адекватности управљања њиме.

(7) Извјештај о обављеној ревизији ИКТ система је посебан извјештај, који је банка дужна доставити Агенцији најкасније до 30. априла текуће године.

(8) Агенција задржава право налагања мјера прописаних Законом о банкама и прописима Агенције који регулишу спољну ревизију у банкама.

III УПРАВЉАЊЕ ИКТ СИСТЕМОМ

Члан 9.

(1) Банка је дужна:
   1) донијети стратегију ИКТ система,
   2) дефинисати оперативне планове који подржавају провођење стратегије ИКТ система и
   3) успоставити поступке праћења и мјерења ефикасности провођења стратегије ИКТ система.

(2) Стратегија ИКТ система из става 1. тачка 1) овог члана, треба да:
   1) дефинише повезаност и усклађеност стратешких циљева ИКТ система са пословним циљевима банке,
   2) садржи опис постојеће ИКТ архитектуре, као и начин на који би се ИКТ систем банке требао развијати ради ефикасног пружања подршке и реализације пословне стратегије банке, укључујући и развој организационе структуре, промјене у ИКТ системима и кључне зависности са трећим странама и

3) дефинише јасне циљеве у погледу информационе безбједности, укључујући кључне показатеље успјешности и кључне параметре ризика.

(3) Банка је дужна стратегију ИКТ система периодично ажурирати, посебно у случају промјена у пословној стратегији банке или значајних промјена у стратегији за управљање ризицима, како би се осигурала усклађеност између пословних циљева и циљева ИКТ система, као и одговарајућих планова и активности.

Члан 10.

(1) Оперативним плановима из члана 9. став 1. тачка 2) ове одлуке банка је дужна дефинисати активности које ће предузети како би се постигли циљеви из стратегије из члана 9. став 2. ове одлуке. Планови садрже најмање сљедеће: опис активности и ИКТ пројекте, укључујући активности за имплементацију корективних мјера које произилазе из процјене ИКТ ризика, финансијска средства, људске ресурсе, временске рокове и податке о одговорним лицима.

(2) Банка је дужна редовно пратити и преиспитивати оперативне планове како би осигурала њихову релевантност и прикладност.

(3) Управа банке треба бити јасно, детаљно и благовремено обавијештена о реализацији и статусу активности дефинисаних оперативним плановима, а најмање на кварталном нивоу.

Члан 11.

(1) Банка је дужна да успостави, имплементира, надзире, одржава, редовно ревидира и континуирано унапрјеђује процес управљања ИКТ системом у складу са релевантним стандардима, регулаторним захтјевима и интерним политикама.

(2) Банка је дужна да користи и одржава ажурним ИКТ системе, протоколе и алате који су:

1) примјерени обиму операција које подржавају пословне активности банке, у складу са принципом пропорционалности из члана 13. ове одлуке,
2) поуздани,
3) опремљени довољним капацитетима за:
   1. тачну и поуздану обраду података неопходних за обављање пословних активности и благовремено пружање услуга,
   2. периоде повећаног оптерећења система (обрада највећег броја налога, порука или трансакција),
   3. увођење нових технологија и
4) технолошки отпорни како би се на адекватан начин носили са додатним потребама за обрадом података у условима стресног тржишта или других неповољних ситуација.

(3) Поред интерних аката из члана 3. ове одлуке, банка је дужна прибављати и чувати сву релевантну документацију (техничку, функционалну, корисничку и другу), као и информације које се односе на ИКТ систем и његове специфичне компоненте. Наведена документација треба бити тачна, потпуна и ажурна.

IV УПРАВЉАЊЕ ИКТ РИЗИЦИМА

Члан 12.

(1) Банка је дужна, у складу са Одлуком о систему управљања, да као дио свог свеобухватног система управљања ризицима успостави поуздан, свеобухватан и документован оквир за управљање ИКТ ризицима.

(2) Оквир из става 1. овог члана треба да омогући банци ефикасно управљање ИКТ ризицима, што обухвата доношење адекватних одлука о третману ИКТ ризика, спровођење одговарајућих мјера за управљање тим ризиком и осигурање високог степена дигиталне оперативне отпорности, у циљу брзог, ефикасног и свеобухватног одговора на ИКТ ризик.

Члан 13.

Оквир за управљање ИКТ ризицима, као и правила утврђена у овој одлуци, банка је дужна примијенити у складу са принципом пропорционалности, узимајући у обзир величину и ризични профил банке, те врсту, обим и сложеност својих услуга, активности и пословања, унутрашњу организацију, те величину и комплексност ИКТ система.

Члан 14.

(1) Оквир за управљање ИКТ ризицима, треба да обухвати најмање: стратегије, политике, методологије, програме, процедуре и планове, те ИКТ протоколе и алате који су неопходни за адекватну заштиту информационе имовине и ИКТ имовине, како би се утицај ИКТ ризика свео на најмању могућу мјеру.

(2) Банка је дужна донијети стратегију за дигиталну оперативну отпорност, која обухвата методе одговора на ИКТ ризик и постизање конкретних ИКТ циљева и којом се:

1) објашњава како оквир за управљање ИКТ ризицима подржава пословну стратегију банке и њене циљеве,
2) утврђује ниво толеранције на ИКТ ризик, у складу са склоношћу банке да преузме ризик, те анализира утицај толеранције на поремећаје у раду ИКТ-а,
3) описује референтна ИКТ архитектура и све промјене које потребно спровести како би се остварили специфични пословни циљеви,
4) описују успостављени механизми за откривање ИКТ инцидената, спречавање њиховог утицаја и пружања заштите од тих утицаја,
5) приказује се актуелна ситуација у погледу дигиталне оперативне отпорности и то на основу броја пријављених значајних ИКТ инцидената и ефикасности превентивних мјера,
6) дефинишу поступци тестирања дигиталне оперативне отпорности,
7) описују планови комуникације у случају значајног ИКТ инцидента и
8) дефинише стратегија за набавку ИКТ-а од различитих пружалаца ИКТ услуга.

Члан 15.

(1) У оквиру система за управљање ИКТ ризицима банка је дужна идентификовати, класификовати и адекватно документовати све пословне функције које подржава ИКТ, улоге и одговорности, информациону имовину и ИКТ имовину која подржава те функције, као и њихове улоге и зависности у односу на ИКТ ризик. Банка је дужна према потреби, а најмање на годишњем нивоу, преиспитати примјереност класификације и релевантне документације.

(2) Приликом провођења класификације из става 1. банка је дужна размотрити захтјеве у погледу повјерљивости, интегритета и доступности.

(3) Банка је дужна идентификовати сву информациону имовину и ИКТ имовину, укључујући и ону на удаљеним локацијама, мрежне ресурсе и хардверску опрему те мапирати критичну и кључну информациону и ИКТ имовину и јасно одредити одговорност за имовину. Такође, неопходно је мапирати конфигурацију информационе и ИКТ имовине, као и везе и међузависности између различитих информационих и ИКТ ресурса.

(4) У оквиру система за управљање ИКТ ризицима, банка је дужна идентификовати и документовати све процесе који зависе од пружаоца ИКТ услуга, те утврдити међусобну повезаност са пружаоцима ИКТ услуга који пружају услуге којима су подржане критичне функције или кључне пословне активности.

(5) Банка је дужна континуирано идентификовати све изворе ИКТ ризика, посебно изложеност ризицима од других финансијских субјеката и према њима, те процјењивати сајбер пријетње и рањивости ІКТ-а које су релевантне за њихове пословне функције подржане ИКТ-ом, информациону и ИКТ имовину. Банка је дужна редовно, а најмање једном годишње, преиспитати сценарије ризика који утичу на њих.

(6) Банка је дужна да успостави адекватну евиденцију за потребе ставова 1.,3. и 4., те је редовно ажурирати, а обавезно након значајних промјена.

Члан 16.

(1) Банка је дужна проводити и документовати процјену ИКТ ризика најмање на годишњем нивоу или чешће, а обавезно након сваке значајне промјене у ИКТ систему, процесима или поступцима који утичу на њене пословне функције које су подржане ИКТ-ом, информациону имовину или ИКТ имовину.

(2) Банка је дужна најмање једном годишње проводити посебну процјену ИКТ ризика за све застарјеле ИКТ системе, а обавезно прије и након интегрисања технологија, апликација или система.

(3) На основу процјене ИКТ ризика из става 1. овог члана, банка је дужна утврдити које су мјере потребне како би се ИКТ ризици свели на прихватљив ниво, те да ли су потребне промјене у постојећим пословним процесима, примијењеним мјерама заштите, ИКТ систему и ИКТ услугама. При том је банка дужна узети у обзир вријеме потребно за провођење тих промјена и вријеме потребно за предузимање одговарајућих привремених мјера за смањење ИКТ ризика, како би ризици остали у прихватљивим границама у складу са апетитом банке за преузимање ризика.

(4) Банка је дужна усвојити план примјене мјера и континуирано пратити реализацију овог плана. Овај план најмање укључује преглед свих идентификованих ризика, опис корективних мјера, приоритете и рокове за провођење, одговорна лица. Уколико банка пролонгира рок за неприхватљиве ризике дужна је о томе благовремено обавијестити Агенцију.

Члан 17.

(1) Банка је дужна да, ради постизања и одржавања адекватног нивоа безбједности ИКТ система, континуирано прати и контролише функционисање и безбједност ИКТ система и алата, те утицај ИКТ ризика своди на најмању могућу мјеру, тако да ризици буду у складу са апетитом банке за преузимање ризика.

(2) Банка је дужна дефинисати, израдити и проводити политике, поступке, протоколе и алате за безбједност ИКТ-а, како би обезбиједила отпорност, континуитет и доступност ИКТ система, посебно оних којима се подржавају критичне функције и кључне пословне активности, те одржавати високе стандарде доступности, аутентичности, интегритета и повјерљивости података приликом складиштења, употребе и преноса.

(3) Како би остварила циљеве из става 2, банка је дужна примијенити ИКТ рјешења и процесе како би:

1) осигурала безбједност средстава за пренос података,
2) на најмању могућу мјеру свела ризик од оштећења или губитка података, неовлашћеног приступа и техничких недостатака који могу нарушити пословање;
3) спријечила смањење доступности, нарушавање аутентичности и интегритета, кршења повјерљивости и губитка података и
4) осигурала заштиту података од ризика који произилазе из управљања подацима, укључујући пропусте у администрацији, ризике повезане са обрадом података и људске грешке.

(4) У склопу оквира за управљање ИКТ ризицима, банка је дужна:

1) да усвоји и имплементира политику информационе безбједности, којом се дефинишу правила за заштиту доступности, аутентичности, интегритета и повјерљивости података, те информационе и ИКТ имовине, како би се постигли циљеви у области информационе безбједности,
2) да примјеном приступа који се заснива на процјени ризика, успостави поуздану структуру за управљање ИКТ системом користећи одговарајуће технике, методе и протоколе, који могу укључивати аутоматизоване механизме за изолацију погођене информационе и ИКТ имовине у случају сајбер напада (могућност тренутног прекида или сегментације како би се највећој могућој мјери смањио и спријечио пренос ризика);

3) да проводи политике којима се ограничава физички или логички приступ информационој и ИКТ имовини на принципу најмањих привилегија, укључујући и удаљени приступ и у ту сврху имплементира политике, поступке и контроле који се односе на права приступа и осигуравају адекватно управљање правима приступа,
4) да имплементира политике и протоколе за јаке механизме аутентификације, засноване на релевантним стандардима и намјенским системима за контролу, као и мјере заштите криптографских кључева, којима се подаци шифрују, на основу резултата класификације података и процеса процјене ИКТ ризика и
5) да успостави процедуре за управљање промјенама ИКТ-а, а у складу са чланом 31. ове одлуке.

Члан 18.

(1) У оквиру редовног праћења ИКТ ризика, Банка је дужна да успостави механизме за континуиран надзор ИКТ система и благовремено откривање необичних активности у складу са чланом 32. ове одлуке, што обухвата проблеме са перформансама ИКТ система и ИКТ инциденте, као и идентификацију потенцијално критичних тачака прекида.

(2) Механизми за откривање из става 1. треба да омогуће више слојева контроле, дефинишу прагове упозорења и критеријуме за активирање и покретање процеса одговора на ИКТ инциденте, укључујући аутоматске механизме за обавјештавање релевантног особља задуженог за одговор на ИКТ инциденте.

(3) Банка је дужна осигурати адекватну сегрегацију дужности запослених у процесу надзора и процесима који су предмет надзора.

(4) Банка је дужна да редовно провјерава имплементиране мјере заштите и контроле за овладавање ИКТ ризицима, те врши оцјену њихове ефективности и ефикасности, укључујући и оквир за тестирање дигиталне оперативне отпорности дефинисан члановима 35. до 39.

(5) Банка је дужна континуирано утврђивати да ли промјене у постојећем оперативном окружењу утичу на примијењене мјере безбједности или је потребно имплементирати додатне мјере за адекватно ублажавање повезаних ризика. Ове промјене треба да буду саставни дио формалног процеса управљања промјенама.

(6) Банка је дужна обезбиједити довољно ресурса и капацитета за:
1) праћење активности корисника, откривање необичних појава у ИКТ системима и ИКТ инцидената, посебно сајбер напада и
2) прикупљање информација о рањивостима и сајбер пријетњама, ИКТ инцидентима, посебно сајбер нападима и анализу утицаја који они могу имати на дигиталну оперативну отпорност банке.

Члан 19.

(1) Банка је дужна адекватно документовати оквир за управљање ИКТ ризицима и преиспитивати га најмање на годишњем нивоу или по настанку значајних ИКТ промјена, као и у складу са налазима ревизијских и надзорних прегледа.

(2) Банка је дужна лекције стечене из тестирања дигиталне оперативне отпорности, као и из стварних ИКТ инцидената, посебно сајбер напада, заједно са изазовима са којима се суочава при активирању планова за континуитет пословања у подручју ИКТ-а и планова одговора и опоравка ИКТ система, као и релевантне информације размијењене са финансијским субјектима и налазе ревизијских и надзорних прегледа, адекватно и континуирано укључити у процес процјене ИКТ ризика. На основу наведеног, банка је дужна проводити одговарајућа преиспитивања релевантних компоненти оквира за управљање ИКТ ризиком и њихове адекватности.

(3) Банка је дужна пратити развој ИКТ ризика током времена, анализирати учесталост, врсте, утицај и развој ИКТ инцидената, посебно сајбер напада и њихове обрасце, с циљем разумијевања нивоа изложености ИКТ ризику, посебно у односу на критичне функције и кључне пословне активности, побољшања сајбер зрелости и спремности банке.

(4) Банка је дужна да континуирано прати релевантна технолошка достигнућа, с циљем разумијевања могућег утицаја примјене нових технологија на захтјеве у погледу информационе безбједности и дигиталне оперативне отпорности. Такође, мора бити у току са најновијим процесима управљања ИКТ ризицима, како би могла да ефикасно реагује на актуелне или нове облике сајбер напада.

Члан 20.

(1) У склопу оквира за управљање ИКТ ризицима, банка је дужна усвојити планове комуникације у кризи, којима ће се дефинисати поступци за управљање интерном и вањском комуникацијом у случају активирања плана континуитета пословања у подручју ИКТ-а или планова одговора и опоравка ИКТ система, укључујући и значајне ИКТ инциденте.

(2) Приликом дефинисања планова из става 1. овог члана, банка је дужна проводити политике комуникације за запослене и вањске учеснике. Политике комуникације за запослене треба да узму у обзир потребу за разликовањем између запослених који су укључени у управљање ИКТ ризицима, посебно запослених који су задужени за одговор и опоравак, и запослених које треба обавијестити.

(3) Банка је дужна осигурати одговорно обавјештавање клијената и партнера, најмање о значајним ИКТ инцидентима или рањивостима, као и јавности кад је то релевантно.

Члан 21.

(1) Банка је дужна да програме за подизање свијести о безбједности ИКТ система и обуке о дигиталној оперативној отпорности, укључи као обавезне модуле у оквиру програма обуке запослених. Програми и обуке се проводе за све запослене, укључујући и више руководство, а ниво сложености је сразмјеран обиму њихових дужности и одговорности. Банка према потреби у ове програме и обуке може укључити пружаоце ИКТ услуга у складу са чланом 27. став 3. тачка 4.

(2) Банка је дужна обезбиједити да се програми и обуке редовно проводе, а најмање једном годишње, при чему се посебно мора водити рачуна о благовременом оспособљавању у погледу препознатих ИКТ пријетњи.

V УПРАВЉАЊЕ ИКТ РИЗИЦИМА ПОВЕЗАНИМ СА ТРЕЋИМ СТРАНАМА

Члан 22.

(1) Независно од одредби Одлуке о управљању екстернализацијом, банка је дужна управљати ИКТ ризицима повезаним са трећим странама, као саставним дијелом оквира за управљање ИКТ ризицима из члана 12. ове одлуке.

(2) Управљање ИКТ ризицима повезаним са трећим странама банка је дужна да успостави у складу са следећим принципима:

1) банка која има склопљене уговоре о употреби ИКТ услуга за потребе свог пословања у сваком тренутку сноси потпуну одговорност за поштовање и извршавање свих обавеза из ове одлуке и примјењивог законског оквира,

2) принципом пропорционалности и узимајући у обзир:

1. природу, обим, сложеност и важност зависности у подручју ИКТ-а и
2. ризике који произилазе из уговора о употреби ИКТ услуга склопљених са пружаоцима ИКТ услуга, водећи рачуна о критичности или значају уговорене услуге, процеса или функције, те о могућем утицају на континуитет и доступност финансијских услуга и активности на нивоу банке и на нивоу групе.

(3) Банка је дужна оквиром за управљање ИКТ ризицима обухватити политику о употреби ИКТ услуга, а посебно ИКТ услуга којима се подржавају критичне функције и кључне пословне

активности, а које пружају треће стране у подручју ИКТ-а, те је примјењивати на појединачној и према потреби консолидованој основи.

(4) Банка је дужна благовремено обавијестити Агенцију о свим планираним уговорима о употреби ИКТ услуга којима се подржавају критичне функције и кључне пословне активности, као и томе да је одређена функција или активност постала критична (кључна) у складу са члановима 14., 15. и 16. Одлуке о управљању екстернализацијом.

Члан 23.

Банка је дужна да води и редовно ажурира, како на нивоу банке, тако и на консолидованом нивоу, регистар информација у вези са свим уговорима о употреби ИКТ услуга које пружају треће стране.

Члан 24.

(1) Прије склапања уговора о употреби ИКТ услуга банка је дужна:
   1) проценити да ли уговор обухвата употребу ИКТ услуга којима се подржава критична функција или кључна пословна активност,
   2) проценити да ли су испуњени регулаторни захтјеви у погледу уговарања,
   3) утврдити и проценити све релевантне ризике у вези са уговором, а у складу са чланом 8. став 1. Одлуке о управљању екстернализацијом, укључујући и могућност да тај уговор допринесе јачању ризика концентрације, у складу са чланом 26. ове одлуке,
   4) проводити дубинске анализе потенцијалних пружаоца ИКТ услуга и обезбиједити прикладност пружаоца ИКТ услуга током цијелог процеса избора и процеса процјене и
   5) утврдити и проценити сукобе интереса које би уговор могао изазвати.

(2) Банка је дужна склапати уговоре искључиво са пружаоцима ИКТ услуга који примјењују одговарајуће стандарде ИКТ безбједности. Уколико се уговор односи на услуге које подржавају критичне функције или кључне пословне активности, банка је дужна, прије склапања уговора утврдити да пружалац услуга примјењује релевантне и признате стандарде ИКТ безбједности.

(3) Банка је дужна континуирано пратити да ли пружалац ИКТ услуга поштује одговарајуће стандарде ИКТ безбједности, који су у складу са безбједносним циљевима и мјерама банке и тражити независну оцјену усклађености (нпр. релевантни сертификати, извјештаји о независним провјерама и друго).

(4) Банка је дужна осигурати и примјењивати право приступа подацима и право на ревизију пружаоца ИКТ услуга у складу са члановима 12.,13. и 17. Одлуке о управљању екстернализацијом.

Члан 25.

(1) Банка је дужна осигурати могућност раскида и/или отказа уговора о употреби ИКТ услуга, у складу са чланом 9. став 7. Одлуке о управљању екстернализацијом, укључујући и сљедеће ситуације:
   1) праћењем ИКТ ризика повезаног са трећим странама идентификоване су околности за које се сматра да би могле довести до промјена у обављању активности које се пружају на основу уговора, укључујући и значајне промјене које утичу на уговор или стање пружаоца ИКТ услуга и
   2) документоване су слабости пружаоца ИКТ услуга које се односе на његово управљање ИКТ ризицима, а посебно у начину на који осигурава доступност, аутентичност, интегритет и повјерљивост података, било да се ради о личним или другим осјетљивим подацима или општим подацима.

(2) Уколико се уговор односи на активности које подржавају критичне функције или кључне пословне активности, банка је дужна да усвоји излазну стратегију и поступке, који су у складу са политиком о употреби ИКТ услуга и плановима континуитета пословања банке, поштујући одредбе члана 10. Одлуке о управљању екстернализацијом.

(3) Банка је дужна у излазним стратегијама узети у обзир ризике који се могу појавити на нивоу пружаоца ИКТ услуга, посебно ризик од прекида пружања њихових услуга, нарушавање квалитета ИКТ услуге, поремећаја у пословању због неприкладног или неуспјешног пружања ИКТ услуге или било који значајан ризик који би могао настати из неадекватног и непрекидног обезбјеђивања ИКТ услуге или раскида/отказа уговора са пружаоцима ИКТ услуга.

(4) Банка је дужна осигурати могућност раскида и/или отказа уговора без прекида својих пословних активности, ограничења у постизању усклађености са регулаторним захтјевима и без негативних посљедица по континуитет и квалитет услуга које се пружају клијентима.

Члан 26.

Уколико се уговор односи на активности које подржавају критичне функције или кључне пословне активности, банка је дужна приликом утврђивања и процјене ризика из члана 24. ове одлуке, размотрити сљедеће:

1) утицај ризика концентрације који произилазе из већег броја склопљених уговора са истим пружаоцем ИКТ услуга или уско повезаним пружаоцима ИКТ услуга,

2) ниво замјењивости пружаоца ИКТ услуга,

3) користи и трошкове алтернативних рјешења, као што је ангажман различитих пружалаца ИКТ услуга, узимајући у обзир да ли и на који начин предвиђена рјешења одговарају пословним потребама и циљевима дефинисаним у стратегији за дигиталну оперативну отпорност,

4) потенцијалне користи и ризике подуговарања, уколико је уговором предвиђена могућност да пружалац ИКТ услуга може ИКТ услуге којима се подржавају критичне функције или кључне пословне активности подуговорити неком другом пружаоцу ИКТ услуга, посебно ако је подизвођач изван територије Босне и Херцеговине,

5) законске одредбе које би се примјењивале у случају стечаја пружаоца ИКТ услуга, као и било која ограничења која могу настати при хитном опоравку података банке,

6) усклађеност са законским и регулаторним захтјевима који се односе на заштиту података а примјењују се на банку, уколико се пружалац ИКТ услуга или локација за складиштење и обраду података налази изван територије Босне и Херцеговине,

7) утицај потенцијално дугих и сложених ланаца подуговарања на способност банке да у потпуности прати уговорене активности, као и на способност Агенције да ефикасно надзире банку у том случају.

Члан 27.

(1) Банка је дужна са пружаоцем ИКТ услуга склопити уговор у писаној форми, којим ће јасно дефинисати све релевантне појмове, услове, права, обавезе и одговорности уговорних страна. Уговор укључује и споразуме о нивоу услуга и доступан је у материјалном или електронском облику, у складу са релевантним и важећим прописима.

(2) Банка је дужна осигурати усклађеност уговора из става 1. овог члана са чланом 9. став 3. Одлуке о управљању екстернализацијом.

(3) Уговори о употреби ИКТ услуга, поред услова из става 2. овог члана, требају укључити и сљедеће:

1) одредбе о доступности, аутентичности, интегритету и повјерљивости у вези са заштитом података, укључујући и личне податке,

2) одредбе о осигуравању приступа личним и осталим подацима банке, те о осигуравању њиховог опоравка и враћања у лако доступном формату у случају несолвентности, реструктурирања или престанка пословања пружаоца ИКТ услуга или у случају раскида уговора,

3) обавезу пружаоца ИКТ услуга да пружи помоћ банци без додатних трошкова или уз унапријед утврђене трошкове у случају ИКТ инцидента који је повезан с ИКТ услугом коју пружа банци,

4) услове за учествовање пружаоца ИКТ услуга у програмима за подизање свијести о безбједности у подручју ИКТ-а и оспособљавањима о дигиталној оперативној отпорности које проводи банка, а у складу са чланом 21. ове одлуке,
5) спецификације животног циклуса података банке и
6) поступке рјешавања инцидената, укључујући поступке ескалације и извјештавања.

(4) Уговори о употреби ИКТ услуга које подржавају критичне функције и кључне пословне активности, требају бити усаглашени са чланом 9. ставом 4. Одлуке о управљању екстернализацијом и ставом 3. овог члана, а укључују и сљедеће:
1) рокове за претходна обавјештења и обавезу извјештавања пружаоца ИКТ услуга према банци, укључујући обавјештење о свакој промјени који би могла имати значајан утицај на способност пружаоца ИКТ услуга да ефективно пружа ИКТ услуге које подржавају критичне функције или кључне пословне активности у складу са договореним нивоима услуга,
2) захтјеве да пружалац ИКТ услуга успостави мјере, алате и политике за безбједност ИКТ система и које пружају адекватан ниво безбједности за пружање услуга банци у складу са њеним регулаторним оквиром, укључујући захтјеве за енкрипцију података, безбједност мреже и процедуре праћења безбједности,
3) обавезу пружаоца ИКТ услуга да учествује у TLPT-у банке, а у складу са чланом 38. ове одлуке, те његову пуну кооперативност,
4) право на континуирано праћење рада пружаоца ИКТ услуге, што укључује следеће:
   1. одредбе дефинисане чланом 9. став 4. тачка 1) Одлуке о управљању екстернализацијом, укључујући и право да се на лицу мјеста узму копије релевантне документације ако су кључне за рад пружаоца ИКТ услуга, при чему ефективно остваривање ових права не смије бити спријечено или ограничено другим уговорима или политикама,
   2. право уговарања алтернативних нивоа осигурања ако су обухваћена права других клијената,
   3. обавезу пружаоца ИКТ услуга да у потпуности сарађује током непосредних надзора и ревизија које проводи Агенција, банка, укључујући и треће стране које оне именују и
   4. обавезу достављања појединости о обиму, поступцима којих се треба придржавати и учесталости таквих надзора и ревизија,
5) излазне стратегије, посебно дефинисање обавезног прелазног периода:
   1. током којег ће пружалац ИКТ услуга наставити пружати предметне активности или ИКТ услуге банци како би се смањио ризик од поремећаја у раду банке или како би се осигурао њен ефикасан опоравак и реструктурирање и
   2. у којем банка може изабрати другог пружаоца ИКТ услуга или враћање предметне активности у банку, у складу са сложеношћу услуге која је предмет уговора.

VI УПРАВЉАЊЕ ИКТ ОПЕРАЦИЈАМА

Члан 28.

(1) Банка је дужна да управља својим ИКТ операцијама на основу документованих, усвојених и имплементираних процеса и процедура. Тим документима је потребно дефинисати како банка користи, прати и контролише своје ИКТ системе и услуге.

(2) Банка је дужна обезбиједити да је извршавање ИКТ операција у складу са захтјевима пословања банке, укључујући и захтјеве информационе безбједности.

(3) Банка је дужна одржавати и унапређивати ефикасност својих ИКТ операција, обухватајући, али не ограничавајући се на потребу разматрања начина за смањење потенцијалних грешака насталих током извршавања ручних задатака.

(4) Банка је дужна евидентирати, пратити и чувати записе за критичне ИКТ операције како би се омогућило откривање, анализа и исправљање грешака.

(5) Банка је дужна да успостави процес управљања ИКТ имовином, у свим фазама њеног животног циклуса – од набавке или развоја до повлачења из употребе, водећи рачуна о ризицима посебно оним који произилазе из употребе застарјеле или неподржане ИКТ имовине и система, укључујући и ИКТ имовину пружалаца услуга.

(6) Банка је дужна да проводи поступке планирања и праћења перформанси и капацитета како би благовремено спријечила, открила и одговорила на значајне проблеме у раду ИКТ система и недостатке капацитета ИКТ система.

Члан 29.

(1) Банка је дужна успоставити процес управљања пројектима којим су дефинисане улоге и одговорности потребне за ефикасну подршку провођењу стратегије ИКТ система.

(2) Банка је дужна на одговарајући начин пратити и смањивати ризике који произлазе из ИКТ пројеката, а узимајући у обзир и ризике који могу произаћи из међусобне зависности различитих пројеката и зависности вишеструких пројеката о истим ресурсима и/или стручности. Банка је дужна укључити пројектни ризик у оквир управљања ИКТ ризицима.

(3) Методологијом управљања пројектима, банка је дужна да осигура да захтјеве у погледу информационе безбједности анализира и одобрава функција управљања информационом безбједношћу.

(4) Банка је дужна осигурати да чланови пројектног тима располажу одговарајућим знањима за сигурно и успјешно провођење пројекта у свим подручјима на која утиче ИКТ пројекат.

(5) У зависности од важности и величине ИКТ пројекта, те утицаја на критичне функције и кључне пословне активности, банка је дужна редовно, као и додатно по потреби, извјештавати управу банке о успостављању и напретку ИКТ пројекта, те повезаним ризицима.

Члан 30.

(1) Банка је дужна дефинисати и проводити процедуре којима се прописује начин набавке, развоја и одржавање ИКТ система.

(2) Банка је дужна осигурати да се прије сваке набавке или развоја ИКТ система јасно дефинишу и на одговарајућем нивоу управљања одобре функционални и нефункционални захтјеви, укључујући и захтјеве у погледу информационе безбједности.

(3) Банка је дужна осигурати да су успостављене мјере за смањење ризика од ненамјерних промјена или намјерних манипулација ИКТ система током развоја и увођења у продукционо окружење.

(4) Банка је дужна утврдити поступке за тестирање и прихватање ИКТ система и услуга прије њихове прве употребе или значајне промјене.

(5) Банка је дужна:

1) успоставити одвојена ИКТ окружења како би се осигурала адекватна сегрегација дужности и ублажио ефекат неконтролисаних промјена у продукционим окружењима,
2) одвојити продукциона окружења од развојних, тестних и других непродукционих окружења,
3) заштитити интегритет и повјерљивост продукционих података у непродукционим окружењима, те приступ продукционим подацима ограничити на овлашћене кориснике и
4) заштитити интегритет изворног кода интерно развијених ИКТ система.

(6) Банка је дужна детаљно документовати развој, имплементацију, функционисање и конфигурацију ИКТ система. При том документација садржи најмање, корисничку и техничку документацију ИКТ системе, те оперативне процедуре.

(7) У складу са процјеном ризика, банка је дужна примјењивати поступке набавке и развоја ИКТ система и на оне ИКТ системе које развијају или којима управљају крајњи корисници у пословним функцијама изван ИКТ организације. Банка је дужна водити регистар оваквих система који су подршка критичним пословним функцијама или процесима.

Члан 31.

(1) Банка је дужна да успостави процес управљања промјенама у ИКТ систему, како би се избјегло да оне доведу до неочекиваног и нежељеног понашања ИКТ система, односно да наруше његову безбједност или функционалност.

(2) Банка треба осигурати да се све промјене из става 1. овог члана евидентирају, процјењују, одобравају, проводе, тестирају и провјеравају на контролисан начин. Ово укључује најмање:

1) иницирање, анализу, процјену ризика и одобравање захтјева за промјену, те начин утврђивања приоритета и реализације,
2) тестирање, одобравање и документовање прије имплементације промјене у продукцији,
3) план имплементације, који укључује и план повратка на претходно стање,
4) раздвајање дужности везаних за развој и имплементацију промјена и
5) информисање корисника информационог система о детаљима извршених промјена.

(3) Банка је дужна да утврди поступке за управљање тзв. хитним промјенама (тј. промјене које се морају провести у најкраћем могућем року) који укључују и поступке који обезбјеђују одговарајуће мјере заштите.

(4) Банка је дужна да утврди почетне верзије софтверских компоненти ИКТ система, те евидентира и хронолошки документује све промјене ових компонената и архитектуре база података.

(5) Банка је дужна утврдити процедуре за управљање безбједносним и функционалним исправкама (енгл. *patch*) у оквиру којих ће дефинисати на који се начин прате информације о безбједносним исправкама, најдужи период у којем се ове исправке морају примијенити у зависности од критичности и процјене ризика за банку, те начин њихове примјене.

VII УПРАВЉАЊЕ ИКТ ИНЦИДЕНТИМА

Члан 32.

(1) Банка је дужна да дефинише, успостави и проводи процес управљања ИКТ инцидентима ради благовременог откривања ИКТ инцидената, управљања њима и обавјештавања о истим.

(2) Банка је дужна у оквиру процеса управљања ИКТ инцидентима из става 1. овог члана:

1) успоставити показатеље за рано упозорење,
2) успоставити поступке за идентификацију, праћење, евидентирање, категоризацију и класификацију ИКТ инцидената према њиховом приоритету и степену озбиљности, као и према критичности погођених услуга, у складу са критеријумима утврђеним у члану 33. ове одлуке,
3) додијелити улоге и одговорности за управљање различитим врстама ИКТ инцидената (нпр. грешке, неисправан рад, сајбер напади и слично) и сценарија,
4) утврдити планове за комуникацију са запосленим, ванјским заинтересованим странама и медијима у складу са чланом 20. ове одлуке, као и планове за обавјештавање клијената, поступке повезане са интерном ескалацијом, а што укључује приговоре корисника повезане са ИКТ-ом и према потреби информисање других субјеката финансијског сектора,
5) осигурати да се барем значајни ИКТ инциденти пријављују релевантном вишем руководству, те обавијесте органи управљања о овим инцидентима, уз објашњење њиховог утицаја, одговора на инцидент и додатних контрола које је потребно имплементирати због таквих инцидената,
6) успоставити поступке одговора на ИКТ инциденте како би се ублажио њихов утицај и обезбиједило да услуге банке благовремено постану доступне и сигурне,
7) успоставити одговарајуће процедуре и поступке како би се осигурало досљедно и интегрисано праћење ИКТ инцидената, те поступања и предузимања даљњих мјера како би се осигурало утврђивање и документовање њихових основних узрока и спријечило

понављање таквих инцидената, те ажурирање безбједносних мјера ИКТ система у складу са стеченим знањима.

(3) Банка је дужна евидентирати све ИКТ инциденте и значајне сајбер пријетње.

(4) У оквиру поступка одговора на инциденте из става 2. тачка 7) овог члана банка је дужна имплементирати поступке за адекватно управљање доказима, кад год је то могуће, узимајући у обзир сљедеће:

1) одржавање ланца чувања доказа (енг. chain of custody),
2) приликом покретања дигиталне форензичке истраге, размотрити могуће правне посљедице,
3) осигурати да критични аспекти задржавања доказа нису занемарени и
4) осигурати да су прикупљени докази прихватљиви пред надлежним судом.

Члан 33.

(1) Банка је дужна да класификује ИКТ инциденте и утврди њихов утицај на основу сљедећих критеријума:

1) број и/или релевантност обухваћених клијената или трећих страна и, ако је примјењиво, износ или број трансакција обухваћених ИКТ инцидентом, као и чињенице да ли је ИКТ инцидент имао утицај на репутацију банке;
2) трајање ИКТ инцидента, укључујући вријеме прекида услуга,
3) географска распрострањеност у вези са подручјима обухваћеним ИКТ инцидентом;
4) губитак података које ИКТ инцидент проузроковао, у односу на доступност, аутентичност, интегритет или повјерљивост података;
5) критичност обухваћених услуга, укључујући трансакције и операције банке и
6) економски утицај ИКТ инцидента, посебно директни и индиректни трошкови и губици у апсолутном и релативном смислу.

(2) Банка је дужна да класификује сајбер пријетњу као значајну на основу критичности услуге која је изложена ризику, укључујући трансакције и операције банке, број и/или релевантност захваћених клијената или трећих страна, као и географску распрострањеност подручја изложеног ризику.

Члан 34.

(1) Банка је дужна одмах по сазнању о значајном ИКТ инциденту, обавијестити Агенцију у складу са ставом 6. овог члана.

(2) За потребе става 1. овог члана, банка је дужна, након прикупљања и анализе свих релевантних информација, саставити иницијално обавјештење и извјештаје из става 6. овог члана.

(3) Иницијално обавјештење и извјештаји из става 6. овог члана треба да садрже све информације које су Агенцији потребне да утврди озбиљност значајног ИКТ инцидента и његов утицај на финансијски сектор.

(4) Банка је дужна одмах по сазнању о значајним сајбер пријетњама обавијестити Агенцију, уколико сматра да је пријетња релевантна за финансијски сектор, кориснике услуга или клијенте.

(5) У случају значајног ИКТ инцидента који има утицај на финансијске интересе клијената, банка је дужна, без непотребног одлагања, чим постане свјесна инцидента, обавијестити своје клијенте о том значајном ИКТ инциденту и мјерама које су предузете за ублажавање негативних посљедица таквог инцидента. Ако се ради о значајној сајбер пријетњи, банка је дужна, ако је примјењиво, благовремено обавијестити своје клијенте, који су потенцијално погођени, о свим одговарајућим мјерама заштите које они могу узети у обзир.

(6) Банка је дужна Агенцији доставити сљедеће:

1) иницијално обавјештење,

2) прелазни извјештај, након иницијалног обавјештења из тачке 1) овог става, чим се статус изворног инцидента значајно промијени или се поступање у вези са значајним ИКТ инцидентом промијени на основу нових доступних информација, а након тога према потреби ажурирана обавјештења сваки пут кад се појаве релевантне новости о статусу, као и на изричит захтјев Агенције и
3) коначни извјештај, када је анализа основног узрока ИКТ инцидента завршена, независно од тога да ли су мјере за ублажавање утицаја већ проведене и када се процијењене вриједности утицаја могу замијенити стварним подацима о утицају ИКТ инцидента.

(7) Након што прими обавјештење, Агенција ће према потреби предузети све потребне мјере у сврху заштите стабилности банкарског система.

VIII ТЕСТИРАЊЕ ДИГИТАЛНЕ ОПЕРАТИВНЕ ОТПОРНОСТИ

Члан 35.

(1) За потребе процјене спремности за поступање са ИКТ инцидентима, утврђивања слабости, недостатака и одступања у дигиталној оперативној отпорности банка је дужна дефинисати, проводити и редовно ажурирати програм тестирања дигиталне оперативне отпорности, као саставни дио оквира за управљање ИКТ ризицима.

(2) Програм тестирања дигиталне отпорности из става 1. овог члана укључује различите процјене, тестове, методологије, поступке и алате који се примјењују у складу са чланом 37. и 38. ове одлуке.

(3) Приликом спровођења програма тестирања дигиталне отпорности из става 1. овог члана банке је дужна примијенити приступ који се заснива на процјени ризика, узимајући у обзир развој ИКТ ризика, конкретне ризике којима је банка изложена или би могла бити изложена, критичност информационе имовине и услуга које пружа, као и све остале факторе које банка сматра релевантним.

(4) Банка је дужна успоставити поступке за утврђивање приоритета, класификацију и отклањање свих слабости и недостатака идентификованих извођењем тестова из става 2. овог члана, те утврдити интерне методологије провјере како би се увјерила да су све идентификоване слабости и недостаци у потпуности отклоњени.

(5) Банка је дужна обезбиједити да се одговарајући тестови редовно проводе, поштујући сљедеће:
1) најмање једном годишње за све ИКТ системе и апликације који подржавају критичне функције и кључне пословне активности,
2) за остале ИКТ системе и апликације, у складу са процјеном ризика, најмање једном у три године,
3) прије било какве измјене постојеће или додавања нових апликација и инфраструктурних компоненти система и ИКТ услуга, којима се подржавају критичне функције и кључне пословне активности, укључујући и апликације доступне путем интернета.

Члан 36.

Програм тестирања дигиталне отпорности из члана 35. ове одлуке, треба да обухвати извођење одговарајућих тестова, као што су процјене и скенирања рањивости, анализе отвореног кода, процјене мрежне безбједности, анализа одступања, провјера физичке безбједности, упитнике и софтверска рјешења за скенирање, преглед изворног кода уколико је примјењиво, тестирања на бази сценарија, тестирање компатибилности, тестирање перформанси, интегрално тестирање (енг. *end-to-end testing*) и пенетрационо тестирање. Тестирања на основу сценарија требају обухватити и сценарије релевантних и познатих потенцијалних напада, а на основу уочених безбједносних пријетњи.

Члан 37.

(1) Банке, које су утврђене у складу са чланом 38. став 2., су дужне проводити напредно тестирање TLPT (пенетрационо тестирање вођено пријетњама) најмање једном у 3 године. Узимајући у обзир ризични профил банке и оперативне околности, Агенција може, када је то потребно, тражити од банке да смањи или повећа ову учесталост.

(2) Сваки пенетрациони тест из става 1. овог члана треба да обухвати више критичних функција банке и кључних пословних активности или све такве функције и активности и при том се проводи на продукционим системима који подржавају те функције и активности.

(3) Банка је дужна идентификовати све релевантне ИКТ системе, процесе и технологије, којима су подржане критичне функције и кључне пословне активности, као и ИКТ услуге, укључујући и оне које су екстернализоване или уговорене са пружаоцима ИКТ услуга.

(4) Банка је дужна проценити које критичне функције и кључне пословне активности морају бити обухваћене TLPT-ом, те резултате процјене доставити Агенцији.

(5) Ако су пружаоци ИКТ услуга обухваћени TLPT-ом, банка је дужна предузети неопходне мјере како би обезбиједила учешће тих пружаоца услуга у TLPT-у, укључујући и мјере заштите. При том је банка у сваком тренутку у потпуности одговорна за усклађеност са одредбама ове одлуке.

(6) Не доводећи у питање ставове 2. и 3. овог члана уколико се оправдано може очекивати да ће учешће пружаоца ИКТ услуга из става 5. овог члана, негативно утицати на квалитет или безбједност услуга које овај пружалац ИКТ услуга пружа другим корисницима, на које се не примјењује ова одлука или на повјерљивост података повезаних са таквим услугама, банка и пружалац ИКТ услуга се могу у писаном облику договорити да пружалац ИКТ услуга директно ангажује трећу страну за провођење заједничког TLPT-а, који укључује више банака (заједничко тестирање), под вођством једне одређене банке, а којима пружа ИКТ услуге, а поштујући одредбе ове одлуке.

(7) Заједничким тестирањем из става 6. овог члана потребно је обухватити релевантан обим ИКТ услуга које подржавају критичне функције и кључне пословне активности које су банке уговориле са пружаоцем ИКТ услуга. Број банака који учествују у овом тестирању треба бити сразмјеран сложености и врсти обухваћених услуга.

(8) Банке је дужна, у сарадњи са пружаоцима ИКТ услуга и осталим укљученим странама, укључујући треће стране које проводе тестирање, али не и Агенцију, примијенити ефикасне контроле управљања ризицима како би ублажила ризике од потенцијалног утицаја на податке, оштећења имовине и поремећаја у раду критичне функције и кључне пословне активности, услуга или операција у самој банци, њеним партнерима или у финансијском сектору.

(9) На крају тестирања, након што су извјештаји и планови за корективне мјере завршени, банка је дужна доставити Агенцији сажетак релевантних налаза, планове за корективне мјере и осталу документацију којем се потврђује да је TLPT проведен у складу са одредбама ове одлуке.

(10) Надлежна тијела банкама издају потврду да је тест спроведен у складу с захтјевима, како је наведено у документацији, како би се омогућило да надлежна тијела узајамно признају TLPT. Уколико банка учествује у заједничком тестирању под вођством банке која није под надзором Агенције, дужна је Агенцији доставити потврду, сажетак релевантних налаза и планове за корективне мјере. Без обзира на ову потврду, банка је и даље у потпуности одговорна за утицај и посљедице које могу настати током спровођења тестова.

Члан 38.

(1) Банка је дужна извршиоце за провођење TLPT-а ангажовати у складу са чланом 39. ове одлуке. Ако је банка за потребе провођења TLPT-а ангажовала интерне ресурсе, дужна је за сваки трећи тест ангажовати ванјске извршиоце.

(2) Агенција ће утврдити које банке су дужне проводити TLPT, узимајући у обзир принцип пропорционалности, а имајући у виду сљедеће:
   1) факторе које утичу на финансијски сектор, с посебним освртом на степен у којем услуге и активности које банка пружа утичу на финансијски сектор у цјелини,
   2) потенцијални утицај на стабилност финансијског сектора, укључујући системски значај банке,
   3) специфични ИКТ профил ризика, ниво ИКТ зрелости банке или карактеристика коришћених технологија.

Члан 39.

(1) За провођење TLPT-а Банка је дужна ангажовати само извршиоце који:
   1) су високог угледа и репутације,
   2) посједују техничке и организационе способности, стручна знања у домену прикупљања и анализе сајбер пријетњи, провођења пенетрационих тестирања и вјежби црвеног тима (енг. red team testing),
   3) посједују међународно признате сертификате/акредитације за провођење пенетрационих тестирања, те се придржавају формалних кодекса понашања или етичких норми,
   4) пружају независно увјерење или извјештај о ревизији који се односи на квалитет управљања ризицима повезаним спровођењем TLPT-а, укључујући одговарајућу заштиту повјерљивих информација банке и правну заштиту у погледу ризика којима је банка изложена у свом пословању,
   5) су адекватно и у потпуности покривени релевантним осигурањем од одговорности, укључујући ризике од непримјереног и немарног поступања.

(2) Уколико банка интерно проводи тестирање, дужна је да, поред услова из става 1. овог члана, испуни и сљедеће услове:
   1) ангажман лица која проводе тестирање је одобрен од стране Агенције,
   2) Агенција је потврдила да банка располаже адекватним ресурсима, те да не постоји сукоб интереса приликом планирања и провођења тестирања и
   3) банка користи ванјске изворе информација о пријетњама.

(3) Банка је дужна обезбиједити да се уговором са трећом страном која проводи тестирање обухвати адекватно управљање резултатима TLPT-а, те да никаква обрада података у вези с тим, укључујући генерисање, складиштење, обраду, извјештавање, пренос или уништавање, не ствара ризике за банку.

IX УПРАВЉАЊЕ КОНТИНУИТЕТОМ ПОСЛОВАЊА

Члан 40.

(1) Банка је дужна успоставити процес за управљање континуитетом пословања како би у највећој могућој мјери обезбиједила континуирано пружање услуга, те ограничила губитке у случају озбиљних поремећаја у пословању. На процес управљања континуитетом пословања примјењују се одредбе Одлуке о систему управљања у банци осим ако овом одлуком није другачије прописано.

(2) У склопу оквира за управљање ИКТ ризицима, банка је дужна донијети план континуитета пословања у подручју ИКТ-а (у даљем тексту: План континуитета ИКТ), која може бити усвојен као посебан документ и чини саставни дио плана континуитета пословања банке.

Члан 41.

(1) Банка је дужна да редовно проводи анализу утицаја на пословање (енг. BIA) с обзиром на своју изложеност озбиљнијим прекидима у пословању и њоме обухватити процјену потенцијалног утицаја таквих прекида на повјерљивост, интегритет и доступност, помоћу квантитативних и квалитативних критеријума, користећи интерне и/или екстерне податке, као и анализом сценарија.

(2) Анализу утицаја на пословање треба спроводити с обзиром на критичност идентификованих и мапираних пословних функција, подржавајућих процеса, зависност од трећих страна и информациону имовину, као и њихову међузависност, а у складу са чланом 15. ове одлуке.

(3) У оквиру анализе утицаја на пословање потребно је као минимум:
   1) навести критичне функције и кључне пословне активности, као и процесе који их подржавају, а у складу са чланом 15. став 1. ове одлуке,

2) навести ИКТ имовину потребну за одвијање појединачних пословних процеса, као и њихове међусобне зависности и повезаности, а у складу са чланом 15. став 3. ове одлуке,

3) одредити, као минимум, RTO, RPO и SDO за сваку појединачну пословну активност, имајући у виду екстернализацију и зависност од трећих страна.

(4) Банка је дужна обезбиједити да су њени ИКТ системи и ИКТ услуге успостављени и усклађени са анализом утицаја на пословање, а посебно у погледу редундантности критичних и кључних ИКТ компоненти како би се спријечили прекиди изазваним догађајима који утичу на те компоненте.

Члан 42.

(1) На основу анализе утицаја на пословање банка је дужна донијети План континуитета ИКТ како би у случају озбиљног прекида у пословању или ванредне ситуације обезбиједила поновно успостављање својих критичних функција и кључних пословних активности након прекида унутар захтијеваног времена опоравка (*RTO*) и циљане тачке опоравка података (*RPO*).

(2) План из става 1. овог члана, као и други намјенски планови, поступци и механизми, релевантни за процес континуитета пословања, имају за циљ:

1) обезбиједити континуитет критичних функција и кључних пословних активности банке у складу са дефинисаним параметрима за RTO и RPO,

2) брз, адекватан и ефикасан одговор на све ИКТ инциденте и њихово рјешавање, на начин којим се ограничава штета, а приоритет даје наставку пословања и мјерама опоравка,

3) активацију, без одлагања, намјенских планова којима се омогућавају мјере, процеси и технологије за сузбијање ширења и који су прилагођени свакој врсти ИКТ инцидента и спречавања даљих штета, као и прилагођене поступке одговора и опоравка дефинисане у складу са чланом 43. ове одлуке,

4) процјену прелиминарног утицаја, штете и губитака,

5) утврдити комуникацијске мјере, као и мјере за управљање кризним ситуацијама како би све релевантне стране (запослени, органи управљања, ванјски актери, пружаоци услуга) били благовремено и адекватно информисани, а у складу са чланом 20. ове одлуке, укључујући и извјештавање Агенције у складу са чланом 43. ове одлуке.

(3) Планом континуитета ИКТ-а банка је дужна подржати циљеве за заштиту, и ако је потребно, поновно успостављање повјерљивости, интегритета и доступности пословних процеса, подржавајућих процеса и информационе имовине.

(4) У оквиру Плана континуитета ИКТ банка је дужна размотрити низ различитих сценарија којима би могла бити изложена, укључујући екстремне, али могуће сценарије, те процијенити њихов потенцијални утицај. На основу тих сценарија банка је дужна описати на који начин ће обезбиједити континуитет ИКТ система и услуга, као и информациону безбједност банке.

(5) У оквиру процеса управљања планом континуитета пословања у подручју ИКТ-а банка је дужна да:

1) утврди методологију за процјену штета и дефинише коефицијенте за максимално дозвољено вријеме нефункционисања критичних пословних процеса, као и да одреди појединачне вриједности за RPO, RTO и SDO,

2) утврди приоритете опоравка пословних процеса,

3) одреди резервну локацију за опоравак критичних пословних процеса на којој ће подаци бити заштићени, која треба да буде на одговарајућој географској удаљености од примарне локације, како би се смањио ризик да обе локације буду истовремено изложене истом ризику,

4) идентификује алтернативне механизме за континуитет пословних процеса у случају прекида примарних механизама,

5) идентификује начин заштите и опоравак података који су потребни за наставак пословног процеса на резервној локацији,

6) узме у обзир физичке мјере за заштиту критичне инфраструктуре банке на примарној и резервној локацији и да обезбиједи одговарајуће услове за њихово непрекидно и сигурно функционисање и

7) узме у обзир улоге и одговорности лица одговорних за ИКТ инфраструктуру у условима коришћења услуга од трећих страна, кроз одговарајуће планове и активности за осигурање континуитета пословања и дигиталне отпорности.

Члан 43.

(1) На основу анализе утицаја на пословање из члана 41. ове одлуке и Плана континуитета ИКТ из члана 42. ове одлуке, банка је дужна донијети планове одговора и опоравка ИКТ система, који ће омогућити опоравак и доступност ИКТ система и услуга неопходних за рад критичних функција и кључних пословних активности унутар захтијеваног времена опоравка и циљане тачке опоравка података.

(2) Плановима одговора и опоравка ИКТ система потребно је дефинисати услове за активирање планова, као и мјере које је потребно предузети како би се обезбиједила доступност, континуитет и опоравак најмање, критичних и кључних ИКТ система и услуга. Ови планови требају бити усмјерени према постизању циљева опоравка пословања банке .

(3) Банка је дужна ажурирати План континуитета ИКТ и планове одговора и опоравка ИКТ система најмање једном годишње, а на основу резултата тестирања, сазнања о актуелним пријетњама, као и искуствима стеченим из претходних догађаја, те налазима ревизијских и надзорних прегледа, а обавезно приликом промјене циљева опоравка, пословних функција, подржавајућих процеса или информационе имовине.

(4) У случају покретања Плана континуитета ИКТ или планова одговора и опоравка ИКТ система, укључујући и значајне ИКТ инциденте, банка је дужна да води евиденцију активности прије и након поремећаја у раду, која мора бити лако доступна. При том је дужна одмах по сазнању обавијестити Агенцију о свим релевантним чињеницама и околностима које се на то односе.

Члан 44.

(1) У склопу оквира за управљање ИКТ ризицима, Банка је дужна:

1) редовно тестирати План континуитета ИКТ, те планове одговора и опоравка ИКТ система којима се подржавају све функције, најмање једном годишње, као и у случају настанка значајних промјена у ИКТ системима који подржавају критичне функције и кључне пословне активности и
2) тестирати планове комуникације у кризи.

(2) У оквиру планова одговора и опоравка банка је дужна успоставити и проводити мјере за осигурање континуитета пословања кључних ИКТ услуга које су уговорене са пружаоцима ИКТ услуга.

(3) У оквиру тестирања из става 1. тачка 1) овог члана банка је дужна обавезно укључити сценарије сајбер напада и пребацивања са примарне ИКТ инфраструктуре на редундантне капацитете, резервне копије и локацију резервног рачунарског центра.

(4) Банка је дужна:

1) документовати резултате тестирања,
2) анализирати и отклонити све утврђене недостатке уочене током тестирања, те извијестити органе управљања банке и
3) редовно преиспитивати План континуитета ИКТ и планове одговора и опоравка ИКТ система, узимајући у обзир резултате тестирања из става 1. тачка 1) овог члана, као и налазе ревизијских и надзорних прегледа.

Члан 45.

(1) Банка је дужна успоставити резервни рачунарски центар који:

1) је на одговарајућој географској удаљености од локације примарног рачунарског центра, како би се осигурало да примарни и резервни рачунарски центар нису истовремено изложени истим ризицима,

2) осигурава континуитет критичних функција или кључних пословних активности на исти начин као и примарни рачунарски центар или пружа ниво услуга који је потребан како би се осигурао континуитет критичних функција и кључних пословних активности унутар дефинисаних циљних вриједности (RTO, RPO и SDO) и
3) је доступан запосленима банке како би се осигурао континуитет критичних функција и кључних пословних активности у случају недоступности ИКТ ресурса на примарној локацији.

(2) Ефективна функционалност резервног рачунарског центра мора бити потврђена најмање једном годишње, а обавезно послије значајних промјена у ИКТ систему банке. Банка је дужна, најмање 30 дана прије тестирања функционалности резервног рачунарског центра обавијестити Агенцију.

(3) Банка је дужна документовати резултате тестирања из става 2. овог члана, те осигурати да је извјештај о резултатима тестирања усвојен од стране управе банке.

Члан 46.

(1) Уколико је банка екстернализовала ИКТ системе и услуге, који подржавају обављање критичних функција и кључних пословних активности, изван мјеста сједишта банке, дужна је за ове ИКТ системе и услуге:
1) утврдити одговарајуће RTO, RPO и SDO параметре како би обезбиједила адекватан ниво услуга и усклађеност са законским прописима,
2) дефинисати план континуитета ИКТ-а и планове одговора и опоравка у мјесту сједишта банке,
3) обезбиједити у локалном рачунарском центру у мјесту сједишта банке ИКТ ресурсе који су потребни за њихов опоравак у захтијеваном времену опоравка, имајући у виду оспособљеност запослених у банци за опоравак ових система, као и ажурност података у складу са дефинисаним RPO из тачке 1) овог става,укључујући и системе за генерисање извјештаја у складу са овом ставом.

(2) Банка је дужна тестирати функционалности у мјесту сједишта банке у складу са одредбама члана 45.

Члан 47.

(1) Банка је дужна да успостави процес управљања резервним копијама података (енг. backup), како би осигурала опоравак ИКТ система и података у захтијеваном времену опоравка и доступност података, који укључује:
1) процедуре и поступке за израду резервних копија података, у којима се утврђује обим података за који се израђују, те минимална учесталост израде у складу са процјеном ризика, резултатима анализе утицаја на пословање и критичношћу ИКТ система и података и
2) поступке и методе за обнављање и опоравак података.

(2) Банка је дужна имплементирати системе за израду резервних копија података, који се могу активирати у складу са процедурама и поступцима за израду резервних копија података, те поступцима и методама за обнављање и опоравак података. Активацијом система за израду резервних копија података не смије се угрозити безбједност ИКТ система, као ни доступност, аутентичност, интегритет или повјерљивост података. Банка је дужна, периодично тестирати, процедуре за израду резервних копија, као и поступке и методе за обнављање и опоравак података.

(3) ИКТ системи који се користе за обнављање и опоравак података, морају бити физички и логички одвојени од изворних ИКТ система, те заштићени од неовлашћеног приступа или оштећења у подручју ИКТ система.

(4) Банка је дужна обезбиједити да се резервне копије података чувају на једној или више секундарних локација, од којих најмање једна мора бити довољно удаљена од примарне локације, на којој се налазе изворни подаци, тако да нису изложене истим ризицима. Резервне копије података морају бити ажурне и адекватно заштићене од релевантних ризика (сајбер напади, ризици приликом преноса и друго).

Члан 48.

(1) Банка је дужна обезбиједити заштитне (регулаторне) копије података:

1) које садрже минимални сет података неопходан за пружање критичних функција и обављање кључних пословних активности, као и провођење поступка реструктурирања банке од стране Агенције,
2) у лако доступном формату, који омогућује преносивост података, независно од изворних система у којима су подаци настали, коришћењем алата који су широко доступни на тржишту, уз документацију која прецизира на који начин се може приступити подацима,
3) ажурне у складу са регулаторним захтјевима Агенције и
4) доступне у мјесту сједишта банке.

X УПРАВЉАЊЕ ОДНОСИМА СА КОРИСНИЦИМА ПЛАТНИХ УСЛУГА

Члан 49.

(1) Банка је дужна успоставити и проводити процесе за јачање свијести корисника платних услуга о безбједносним ризицима повезаним са платним услугама, који укључују пружање помоћи и смјерница корисницима платних услуга.

(2) Помоћ и смјернице које се нуде корисницима платних услуга треба редовно ажурирати с обзиром на нове пријетње и рањивости, а кориснике платних услуга треба благовремено информисати о овим промјенама.

(3) Банка је дужна да корисницима платних услуга дозволи да онемогуће одређене платне функционалности везане за платне услуге које банка пружа кориснику платних услуга, уколико таква опција постоји у оквиру функционалности производа.

(4) Ако је банка сагласна са корисником у вези са ограничењима потрошње за платне трансакције извршене путем одређених платних инструмената, банка је дужна да кориснику омогући опцију прилагођавања ових ограничења до износа највишег договореног ограничења.

(5) Банка је дужна омогућити да корисници платних услуга примају упозорења о иницирању и/или неуспјелим покушајима иницирања платних трансакција, како би били у могућности да благовремено открију лажно или злонамјерно коришћење њихових рачуна.

(6) Банка је дужна да информише кориснике платних услуга о измјенама у безбједносним процедурама које утичу на кориснике платних услуга у вези са пружањем платних услуга.

(7) Банка је дужна са својим корисницима платних услуга да комуницира на такав начин да их увјери у аутентичност примљених порука.

(8) Банка је дужна да корисницима платних услуга пружи помоћ у вези са свим питањима, захтјевима за подршку и обавјештењима о неправилностима или проблемима у погледу безбједносних питања повезаних са платним услугама. Корисници платних услуга треба да буду адекватно информисани о томе како је могуће добити наведену помоћ.

XI РАЗМЈЕНА ИНФОРМАЦИЈА

Члан 50.

(1) Банке су дужне са Агенцијом размијењивати информације и сазнања о сајбер пријетњама, укључујући показатеље компромитовања, тактике, технике и поступке, упозорења о сајбер безбједности и алате за конфигурацију. Агенција ће размијенити информације и сазнања са банкама у мјери у којој таква размјена информација и сазнања има за циљ: побољшати дигиталну оперативну отпорност банака, посебно кроз подизање свијести у вези са сајбер пријетњама, ограничавање или спречавање могућности ширења сајбер пријетњи, јачање

одбрамбених капацитета и техника откривања пријетњи, стратегија ублажавања или одговора и опоравка.

(2) У сврху става 1. овог члана Агенција ће успоставити протокол о размјени информација и обезбиједити платформу за размјену информација.

(3) Протоколом о размјени информација из става 1. се дефинише најмање сљедеће: учесници и њихове улоге, учесталост и начин размјене, обим информација, мјере за заштиту потенцијално осјетљивих информација којима се у потпуности поштују пословна тајна и заштита личних података, услове за укључивање других заинтересованих страна.

XII ИЗВЈЕШТАВАЊЕ И ОБАВЈЕШТАВАЊЕ АГЕНЦИЈЕ

Члан 51.

(1) Банка је дужна Агенцији доставити сљедеће интерне акте и извјештаје:
   1) Стратегију ИКТ система и оперативни планови дефинисани чланом 5. ове одлуке,
   2) Политику информационе безбједности,
   3) политике које се односе на управљање ИКТ ризицима, дефинисане чланом 14. ове одлуке,
   4) политике које се односе на управљање ИКТ инцидентима, дефинисане чланом 32. ове одлуке,
   5) програм тестирања дигиталне оперативне отпорности, дефинисан чланом 35. ове одлуке,
   6) политике које се односе на коришћење ИКТ услуга трећих страна, дефинисане чланом 22. ове одлуке,
   7) Анализу утицаја на пословање, План континуитета ИКТ и планове одговора и опоравка ИКТ система, дефинисане чланом 41., 42. и 43. ове одлуке,
   8) Програм подизања свијести о информационој безбједности, дефинисан чланом 21. ове одлуке,
   9) Регистар информација дефинисан чланом 23. ове одлуке,
   10) извјештај о броју нових уговора о употреби ИКТ услуга, категорије пружаоца ИКТ услуга и врсти уговора
   11) извјештај о резултатима процјене ИКТ ризика, дефинисане чланом 16. ове одлуке, укључујући план корективних мјера
   12) извјештаје о управљању ИКТ ризицима и примјени корективних мјера, као и извјештај степену дигиталне оперативне отпорности
   13) извјештаје о реализацији оперативног плана из тачке 1) овог става,
   14) извјештаје о проведеним тестирањима дигиталне оперативне отпорности дефинисане чланом 35. ове одлуке,
   15) извјештаје о тестирању планова дефинисаних чланом 44.-46. ове одлуке.

(2) Банка је дужна интерна акта из става 1. тачке 1) – 8) достављати годишње, најкасније 90 дана по завршетку календарске године који су усвојени или ажурирани током извјештајног периода.

(3) Банка је дужна извјештаје из става 1. тачке 9) – 15) достављати 15 дана по усвајању од стране органа управљања.

(4) Банка је дужна правовремено обавијестити Агенцију о свакој значајној и комплексној промјени која може имати утицај на ИКТ систем банке и при том доставити одговарајућу документацију (детаљан опис промјене, план активности, пројектне тимове, планирани буџет, резултате процјене ИКТ ризика и сл.), укључујући и промјене кључног особља (руководилац организационе јединице за управљање ИКТ, лице одговорно за информациону безбједност, главни администратори,..).

(5) Банка која планира миграцију података на нови систем кључне банкарске апликације (core business application) или у други рачунарски центар, односно која врши промјену локације

рачунарског центра, а претходно је обавијестила Агенцију у складу са ставом 4. дужна је најкасније 30 дана прије почетка тестирања планираног да о томе обавијести Агенцију.

Обавјештење из овог става садржи најмање:

1) детаљне описе система између којих се подаци преносе;
2) план, динамику и опис активности у вези с миграцијом података, укључујући и методологију тестирања;
3) резултате процјене ризика и опис контрола које ће се примијенити током миграције података с циљем очувања повјерљивости, интегритета и доступности података;
4) план враћања на стање прије миграције података, који укључује динамику тог враћања и опис активности, као и критеријуме за доношење одлуке за примјену овог плана.

XIII ОБЈАВА ИНФОРМАЦИЈА ЗНАЧАЈНИХ ЗА ЈАВНОСТ

Члан 52.

Агенција може објавити информације, укључујући и мјере, за које процијени да су од значаја за јавност, а које се односе на управљање ИКТ системима, безбједношћу ИКТ система, сајбер ризицима, као и другим специфичним областима повезаним са употребом ИКТ-а.

XIV ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Додатна упутства о примјени Одлуке

Члан 53.

Агенција ће посебним упутствима детаљније прописати захтјеве у сврху примјене одредаба ове Одлуке.

Прелазне и завршне одредбе

Члан 54.

(1) Ова Одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске”, а примјењује се од 01.04.2026. године.

(2) Даном почетка примјене ове одлуке престаје да важи Одлука о управљању информационим системима у банкама („Службени гласник Републике Српске“, број 116/17).

(3) Банка је дужна уговоре о употреби ИКТ услуга, склопљене са пружаоцима ИКТ услуга прије ступања на снагу ове одлуке, ускладити са одредбама ове одлуке, најкасније у року од 3 мјесеца од дана примјене ове одлуке.

Број: УО-159/25

Датум, 13.05.2025. год.

ПРЕДСЈЕДНИК
УПРАВНОГ ОДБОРА

Дејан Кустурић