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“, број 59/13 и 4/17), те 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 44. сједници, одржаној 11.12.2017. године, д о н о с и

О Д Л У К У
О УПРАВЉАЊУ ИНФОРМАЦИОНИМ СИСТЕМИМА У БАНКАМА

1. Опште одредбе

Члан 1.

Овом одлуком утврђују се захтјеви и критеријуми које је банка дужна да обезбиједи и проводи, а који се односе на управљање информационим системима у банкама и ризицима информационих система.

Члан 2.

Поједини појмови који се користе у овој одлуци имају сљедеће значење:

1) Информациони систем је свеобухватан скуп технолошке инфраструктуре, организације, људи и поступака за прикупљање, чување, обраду, одржавање, коришћење, дистрибуцију и располагање информацијама.
2) Ресурси информационог система обухватају софтверске компоненте, хардверске компоненте и информациону имовину.
3) Софтверске компоненте обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер.
4) Хардверске компоненте обухватају рачунарску опрему, комуникациону опрему, медије за чување података, као и осталу техничку опрему која служи као подршка функционисању информационог система.
5) Информациона имовина обухвата податке у датотекама и базама података, програмски код, конфигурацију хардверских компонената, стручна знања, кључно особље, техничку и корисничку документацију, интерне акте и сл.
6) Корисници информационог система су сва лица која су овлашћена да користе информациони систем (запослени у банци, запослени код пружаоца услуга, корисници електронског банкарства и др.).
7) Ризик информационог система је ризик који произилази из коришћења информационе технологије, односно информационог система.
8) Информациона технологија обухвата сву технологију која се користи за прикупљање, обраду, чување, дистрибуцију и заштиту информација. Односи се на софтверске и хардверске компоненте.
9) Безбједност информационог система подразумијева очување повјерљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информационом систему.
10) Повјерљивост је особина која подразумијева да подаци и информације нису доступни или откривени неовлашћеним лицима или процесима.
11) Интегритет је особина која подразумијева да подаци, информације и процеси нису неовлашћено или непредвиђено мијењани.
12) Расположивост је особина која обезбјеђује да су подаци, информације и процеси увијек доступни и употребљиви на захтјев овлашћеног лица.

13) Аутентичност је особина која обезбјеђује да је идентитет лица заиста онај за који се тврди да јесте.
14) Доказивост је особина која обезбјеђује да свака активност у информационом систему може једнозначно бити праћена до њеног извора.
15) Непорецивост је особина која обезбјеђује немогућност порицања активности извршене у информационом систему или пријема информација.
16) Поузданост означава да информациони систем досљедно и очекивано врши предвиђене функције и пружа тачне информације.
17) Осјетљиви подаци/информације јесу они подаци/информације код којих би нарушавање особина повјерљивости, интегритета и расположивости изазвало негативне посљедице на пословање банке.
18) Контроле обухватају политике, процедуре, праксе, технологије и организационе структуре које се односе на информациони систем утврђене да би се обезбиједило разумно увјерење да ће пословни циљеви бити остварени и да ће нежељени догађаји бити спријечени или откривени, а према начину примјене дијеле се на управљачке, логичке и физичке.
19) Управљачке контроле обухватају доношење интерних аката која се односе на информациони систем и успостављање одговарајуће организационе структуре, те осигуравају примјену ових аката ради обезбјеђивања функционалности и безбједности информационог система.
20) Логичке контроле су контроле имплементиране на софтверском нивоу компонената информационог система.
21) Физичке контроле су контроле којима се штите ресурси информационог система од неовлашћеног физичког приступа, крађе, физичког оштећења или уништења.
22) Идентификација је процес представљања корисника информационог система приликом пријављивања и у току извођења активности у том систему.
23) Аутентификација је процес провјере и потврде корисничког идентитета коришћењем једног од сљедећих елемената или њихове комбинације:
    1. нешто што само корисник зна (нпр. лозинка, лични идентификациони број и сл.),
    2. нешто што само корисник посједује (нпр. паметна картица, токен, криптографски кључ и сл.) и
    3. нешто што само корисник јесте (биометријске карактеристике као што су отисак прста, очна дужица, глас, рукопис и сл.).
24) Ауторизација је процес додјеле права приступа корисницима информационог система.
25) Надзор корисничких права приступа јесте процес који укључује праћење, измјену и ревидирање права корисника информационог система.
26) Повлашћени приступ је приступ ресурсима информационог система који овлашћеним корисницима (администратори мреже, системског софтвера, база података и др.) омогућава заобилажење уграђених логичких контрола.
27) Удаљени приступ је приступ ресурсима информационог система са удаљене локације путем телекомуникационе инфраструктуре над којом банка нема потпуну контролу.
28) Кориснички захтјев је захтјев корисника информационог система за приступ одређеним ресурсима информационог система или ИТ услугама, захтјев за информације или савјет, те остали стандардни захтјеви (нпр. ресетовање лозинке, захтјев за опрему и др.).

29) Оперативни и системски записи обухватају хронолошке записе о активностима на ресурсима информационог система (записи оперативних система, апликативног софтвера, база података, мрежних уређаја и сл.).

30) Малициозни кôд је било који облик програмског кода створен с намјером да се неовлашћено оствари приступ ресурсима информационог система, прикупе или униште информације, изазове неочекивано понашање или прекид у функционисању овог система, односно да се на други начин наруши повјерљивост, интегритет или расположивост тих ресурса (нпр. рачунарски вируси, црви, тројански коњи и др.).

31) Инцидент је сваки непланирани и нежељени догађај који може нарушити безбједност или функционалност ресурсâ информационог система који подржавају одвијање пословних процеса банке.

32) Тежи инцидент јесте инцидент који има или може имати значајан утицај на континуитет пословања банке и/или на безбједност осјетљивих података и/или материјално значајан утицај на велики број корисника услуга.

33) Електронско банкарство је систем који клијентима банака омогућава коришћење услуга које банке пружају (приступ финансијским информацијама, електронско плаћање и сл.) с удаљене локације путем јавних комуникационих мрежа или сл.

34) Критични/кључни пословни процеси јесу они пословни процеси или функције чије неадекватно функционисање може значајно угрозити, тј. нарушити пословање банке.

35) Резервна копија података (енгл. backup) јесте копија изворних података који су потребни за поновно успостављање пословних процеса банке, те осталих података за које банка процијени да их је потребно чувати.

36) Захтијевано вријеме опоравка – RTO (енгл. recovery time objective) јесте најдуже прихватљиво вријеме нерасположивости пословног процеса банке и ресурса информационог система потребних за одвијање пословног процеса, тј. вријеме током кога је потребно обновити пословни процес.

37) Циљана тачка опоравка – RPO (енгл. recovery point objective) јесте најдужи прихватљив период од посљедње резервне копије података до наступања нерасположивости пословног процеса, тј. најдужи прихватљив период за који подаци могу бити изгубљени.

2. Оквир за управљање информационим системом

Члан 3.

(1) Банка је дужна да, у складу са природом, сложеношћу и обимом пословања, као и сложеношћу информационог система успостави, надзире, редовно ревидира и унапређује процес управљања информационим системом у циљу смањења изложености ризицима, очувања безбједности и функционалности овог система.

(2) Банка је дужна успоставити адекватан систем који укључује идентификацију, мјерење, праћење и контролу управљања ризицима информационог система.

Члан 4.

Надзорни одбор банке дужан је и одговоран, као минимум, да:

1) на основу приједлога управе банке доноси стратегију информационог система, која мора бити у складу са пословном стратегијом банке,
2) на основу приједлога управе банке доноси политике за управљање информационим системом, а посебно политику безбједности информационог система, и надзире њихову имплементацију,

3) усвојене политике разматра најмање једном годишње, тј. правовремено врши њихово прилагођавање економским, тржишним, технолошким и другим условима (у складу са промјенама у окружењу),
4) успостави систем за мјерење, праћење, контролу и управљање ризицима информационог система, те редовно прати и процјењује ефикасност овог система,
5) успостави одговарајућу организациону структуру, с јасно утврђеном подјелом послова, дужностима запослених, као и њихових стручних квалификација и потребних компетенција, како би се обезбиједило адекватно управљање информационим системом,
6) обезбиједи избор и именовање квалификованог и компетентног члана управе банке који ће бити надлежан за успостављање и надзор процеса управљања информационим системом,
7) на приједлог управе пропише садржај и периодичност извјештавања надзорног одбора о релевантним чињеницама везаним за управљање информационим системом, а најмање на годишњем нивоу и
8) обезбиједи услове за успостављање ефикасног система унутрашњих контрола у сегменту управљања информационим системом и врши надзор над тим системом.

Члан 5.

(1) Управа банке дужна је и одговорна, као минимум, да:
1) именује одбор за управљање информационим системом, састављен од представника различитих пословних функција, који ће се састајати периодично и извјештавати управу о својим активностима најмање на кварталном нивоу, а чија улога треба бити координација иницијатива и праћење развојних активности информационог система које се тичу усклађености са пословним циљевима и пословном стратегијом банке,
2) предлаже и имплементира политике, те доноси и проводи процедуре које се односе на управљање информационим системом,
3) успостави процесе и поступке за управљање ризицима информационог система који обухватају идентификацију, мјерење, мјере за ограничавање и ублажавање, праћење, анализирање и контролу ризика,
4) обезбиједи да су све дужности везане за управљање информационим системом јасно дефинисане и додијељене, водећи рачуна о адекватној сегрегацији дужности,
5) обезбиједи потребне ресурсе за управљање информационим системом,
6) донесе план и програм за успостављање и подизање свијести о безбједности информационог система и
7) усвоји и примијени методологију управљања пројектима, којом ће се дефинисати критеријуми, начин и поступци управљања пројектима који се односе на информациони систем.

(2) Управа банке дужна је правовремено обавијестити Агенцију за банкарство Републике Српске (у даљем тексту: Агенција) о значајним и комплексним промјенама на информационом систему банке, те доставити одговарајућу документацију (детаљан опис промјене, план активности, пројектне тимове, планирани буџет, анализу исплативости пројекта, резултате процјене ризика и сл.).

Члан 6.

(1) Банка је дужна развити и надзирати имплементацију стратегије информационог система која као минимум треба да:
1) обухвати дугорочне и краткорочне иницијативе везане за информациони систем,

2) дефинише повезаност и усклађеност циљева информационог система с пословним циљевима банке.

(2) Банка је дужна да периодично ажурира стратегију информационог система, а посебно приликом измјена пословне стратегије банке, како би се обезбиједила усклађеност између циљева информационог система и пословних циљева, планова и активности.

(3) Управа банке дужна је усвојити оперативни план активности везан за информациони систем на годишњем нивоу, који произилази из стратегије информационог система.

(4) План из става 3. овог члана треба, као минимум, садржавати сљедеће: опис активности и пројеката информационог система, финансијске и људске ресурсе, временске рокове и податке о одговорним особама.

(5) Контролне функције банке дужне су, у складу са својим надлежностима, обезбиједити да су ризици повезани с имплементацијом стратегије информационог система адекватно идентификовани, процијењени и ублажени, као и да је успостављено ефикасно управљање информационим системом.

Члан 7.

(1) Банка је дужна да донесе и примијени интерна акта која се односе на информациони систем, те обезбиједи провођење тих аката.

(2) Интерни акти морају, као минимум, бити:
1) усклађени са прописима, стандардима и правилима струке,
2) редовно прегледани и ажурирани и
3) потпуни, детаљни и примјењиви.

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

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

Члан 8.

(1) Управа банке дужна је именовати лице одговорно за функцију безбједности информационог система, те дефинисати његова овлашћења, одговорности и обим рада. Ова функција треба бити независна од функције организационе јединице за управљање информационим системом. Лице одговорно за функцију безбједности информационог система треба бити компетентно лице с одговарајућим стручним квалификацијама, специјалистичким знањима и искуством.

(2) Лице одговорно за функцију безбједности информационог система треба, као минимум, да надзире и координише активности везане за безбједност информационог система, те да редовно, најмање на кварталном нивоу, извјештава управу банке о стању и активностима везаним за безбједност информационог система.

3. Управљање ризицима из уговорних односа

Члан 9.

Банка је дужна континуирано процјењивати ризике и адекватно управљати оним ризицима који произилазе из уговорних односа са правним и физичким лицима чије су активности везане за информациони систем банке.

4. Управљање ризицима информационог система

Члан 10.

(1) Банка је дужна успоставити процес управљања ризицима информационог система, који треба бити саставни дио система управљања ризицима у банци, у складу с Одлуком о управљању ризицима у банкама.

(2) Управа банке дужна је усвојити методологију којом ће се дефинисати критеријуми, начин и поступци управљања ризицима информационог система, те одредити одговорности управљања ризицима и прихватљиве нивое ризика.

(3) У оквиру управљања ризицима информационог система банка је дужна:
1) проценити ризик укључујући сљедеће елементе: ресурсе информационог система, пријетње и рањивости, примијењене мјере заштите и контроле,
2) препоручити мјере за поступање с процијењеним ризицима, донијети план примјене мјера и континуирано пратити реализацију овог плана и
3) редовно, а најмање једном годишње, извјештавати управу и надзорни одбор банке о резултатима процјене ризика.

(4) Управљање ризицима информационог система мора да обухвати све ресурсе информационог система који подржавају значајне пословне процесе, те да с посебном пажњом процијени значај дијелова информационог система и сервиса који:
1) подржавају кључне пословне операције и дистрибуционе канале,
2) подржавају кључне процесе управљања и корпоративне функције, укључујући управљање ризицима,
3) подлијежу специфичним правним или регулаторним захтјевима, који намећу веће захтјеве за расположивост, опоравак, повјерљивост и безбједност,
4) врше обраду или складиште осјетљиве податке, при чему неовлашћен приступ тим подацима може знатно утицати на репутацију, финансијске резултате или континуитет пословања банке, и
5) обезбјеђују основне функционалности које су кључне за адекватно функционисање банке (нпр. телекомуникационе услуге).

(5) Банка је дужна да за потребе процјене ризика материјално значајних екстернализованих активности обезбиједи извјештаје о процјени ризика информационог система пружаоца услуга.

(6) Банка је дужна обезбиједити да интерна и спољна ревизија редовно врше оцјену ефикасности система за управљање ризицима информационог система, те да су ризици информационог система адекватно идентификовани, процијењени и ублажени.

5. Интерна ревизија

Члан 11.

(1) Банка је дужна спроводити интерну ревизију информационог система у складу са прописима Агенције којима се регулише област интерне ревизије у банкама, а на основу дефинисаног програма рада интерне ревизије.

(2) Банка је дужна планирати и проводити интерну ревизију информационог система у складу са процјеном ризика појединих подручја информационог система, при чему мора дефинисати временски интервал у којем ће бити прегледана (обухваћена) сва подручја информационог система банке.

(3) Банка је дужна обезбиједити да се интерна ревизија информационог система проводи континуирано током цијеле године.

(4) Лица која обављају интерну ревизију информационог система треба да посједују стручна знања и вјештине о информационим системима.

(5) У случају екстернализације интерне ревизије информационог система, банка треба обезбиједити да пружалац услуга интерне ревизије информационог система истовремено (у тој години) не пружа услуге спољне ревизије информационог система банци, те треба да обезбиједи да не постоји сукоб интереса. Лица која оперативно обављају ревизију морају посједовати међународно признате сертификате за ревизију информационих система.

6. Спољна ревизија

Члан 12.

(1) Агенција даје претходну сагласност за именовање привредног друштва за ревизију ради обављања ревизије информационог система (у даљем тексту: спољни ревизор ИС).

(2) Банка је дужна Агенцији поднијети захтјев за издавање сагласности за именовање спољног ревизора ИС ради ревизије информационог система.

(3) Банка је дужна, уз захтјев из става 2. овог члана, доставити Агенцији сљедеће документе:

1) нацрт одлуке о именовању спољног ревизора ИС,
2) нацрт уговора или писма намјере са спољним ревизором ИС,
3) референце спољног ревизора ИС о обављеним ревизијама информационих система,
4) доказе о стручним квалификацијама лица која ће обављати ревизију и њихове биографије и
5) изјаву о непостојању сукоба интереса између спољног ревизора ИС (тј. лица која оперативно проводе ревизију) и банке.

(4) Скупштина банке, уз претходну сагласност Агенције, најкасније до 30. септембра текуће године доноси одлуку о именовању спољног ревизора ИС, који ће обавити ревизију информационог система за ту годину.

(5) Банка је дужна доставити одлуку о именовању спољног ревизора ИС у року од осам дана од дана усвајања одлуке и уговор о обављању ревизије информационог система у писаној форми у року од осам дана од дана потписивања уговора.

(6) Спољни ревизор ИС дужан је да Агенцији 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 најмање 30 дана прије почетка ревизије информационог система банке.

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

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

(9) Извјештај о обављеној ревизији информационог система јесте посебан извјештај, који је банка дужна доставити Агенцији најкасније до 31. маја текуће године.

(10) Банка је дужна да ревизију информационог система обавља на годишњем нивоу.

7. Безбједност информационог система

Члан 13.

(1) Банка је дужна да усвоји и имплементира политику безбједности информационог система, која представља основ за управљање безбједношћу информационог система банке и која као минимум треба да:
   1) садржи начела и принципе управљања безбједношћу ресурса информационог система и притом се придржава међународно признатих стандарда и принципа у мјери којој је то могуће,
   2) дефинише овлашћења и одговорности који се односе на подручје управљања безбједношћу информационог система,
   3) обухвати подручја управљачке, логичке и физичке заштите ресурса информационог система, у складу са величином и комплексношћу информационог система и
   4) дефинише мјере у случају одговорности корисника информационог система за нарушавање безбједности информационог система.

(2) Политика безбједности информационог система мора бити усклађена са промјенама у окружењу и информационом систему банке.

(3) Банка је дужна да процес управљања безбједношћу информационог система успостави као континуирани процес идентификовања потреба за овом безбједношћу и постизања и одржавања адекватног нивоа те безбједности, на основу резултата процјене ризика и обавеза које произилазе из прописа, уговорних односа и сл.

(4) Банка је дужна да, ради постизања и одржавања адекватног нивоа безбједности информационог система, редовно провјерава имплементиране мјере заштите и контроле информационог система банке, у зависности од резултата ових провјера и процјене ризика обезбиједи независне провјере (нпр. пенетрациони тест), те извјештава управу и надзорни одбор о резултатима ових тестирања.

Члан 14.

(1) Банка је дужна да успостави адекватан систем управљања приступом ресурсима информационог система, који као минимум обухвата:
   1) дефинисање одговарајућих управљачких, логичких и физичких контрола,
   2) дефинисање политика лозинки у складу са добрим праксама, али и властитом процјеном ризика и важности ресурса којима се приступа,
   3) управљање корисничким правима приступа, које обухвата процес евидентирања, идентификације, аутентификације и ауторизације, те надзор над корисничким правима приступа,
   4) управљање повлашћеним и удаљеним приступом,
   5) управљање генеричким и сервисним налозима и
   6) редовну провјеру адекватности одобрених права приступа ресурсима информационог система, а најмање на годишњем нивоу.

(2) Банка је дужна обезбиједити да се ауторизација корисника информационог система заснива на принципу додјеле најмањих могућих права приступа ресурсима тог система, која омогућавају ефикасно обављање послова.

Члан 15.

Банка је дужна да успостави адекватне мјере заштите информационог система од злоупотреба или неовлашћеног приступа извана, као минимум укључујући сљедеће:

1) управљање и надзор над механизмима заштите (нрп. фајервол, филтрирање веб-саобраћаја, антивирусна рјешења, системи за детекцију и спречавање неовлашћеног приступа и сл.),
2) сегментацију рачунарске мреже, редовно праћење мрежног саобраћаја и анализу записа,
3) провјеру интегритета софтвера,
4) периодичне провјере рањивости и пенетрациона тестирања,
5) ојачавање система (примјеном безбједносних препорука),
6) заштиту комуникационих канала и
7) адекватну обуку корисника информационог система, посебно у погледу препознавања напада.

Члан 16.

(1) Банка је дужна да, у складу са процјеном ризика, обезбиједи генерисање, редовно праћење и чување оперативних и системских записа у сврху благовременог откривања неовлашћених приступа и радњи у информационом систему, идентификовања проблема, реконструисања догађаја, те утврђивања одговорности.

(2) Банка је дужна да утврди листу ресурса информационог система са којих се записи прикупљају, врсту записа, структуру и период чувања, начин праћења и анализе, те извјештавање о резултатима анализа.

(3) Банка је дужна да успостави адекватну заштиту записа, обезбиједи њихов интегритет и повјерљивост у складу са класификацијом информација, те раздвоји дужности лица која администрирају ресурсе информационог система са којих се записи прикупљају од лица која администрирају записе.

Члан 17.

(1) Банка је дужна да донесе и имплементира процедуре којим се дефинишу мјере заштите и контроле приступа просторијама у којима су смјештени ресурси информационог система (просторије са серверском инфраструктуром, комуникационом опремом и сл.), као и просторијама у којима се налазе системи за подршку функционисању информационог система, с циљем заштите од неовлашћеног физичког приступа, крађе, физичког оштећења или уништења ресурса информационог система.

(2) Банка је дужна да дефинише и имплементира адекватне мјере заштите од статичког електрицитета, пожара, поплаве, земљотреса, експлозије и других облика природних катастрофа или штета узрокованих људским дјеловањем, а на бази процјене ризика.

(3) Банка је дужна да редовно контролише исправност имплементираних мјера заштите из става 2. овог члана.

Члан 18.

Банка је дужна да примјеном одговарајућих контрола заштити ресурсе информационог система од малициозног програмског кода, те да као минимум обухвати сљедеће:

1) дефинише улоге и одговорности лица задужених за провођење мјера заштите,
2) успостави контроле превенције и детекције (спречавање извршавања малициозног програмског кода, континуирано ажурирање софтвера за откривање малициозног кода, управљање рањивостима и провјерама информационог система и сл.),
3) дефинише поступке у случају откривања малициозног програмског кода и

4) подизање свијести корисника информационог система о ризицима од посљедица дјеловања малициозног програмског кода кроз редовне програме едукације.

Члан 19.

Банка је дужна обезбиједити да апликативни софтвер има уграђене контроле исправности, комплетности и конзистентности података који се уносе, мијењају, обрађују и генеришу.

8. Развој и одржавање информационог система

Члан 20.

(1) Банка је дужна да успостави процес развоја информационог система у складу са релевантним пословним промјенама у банци и окружењу, имајући у виду функционалне и безбједносне аспекте, који као минимум укључује:
   1) планирање и формалну организацију пројеката у складу са методологијом управљања пројектима,
   2) успостављање и документовање процеса програмског развоја и испоруке, који обухвата поступке анализе и пројектовања, програмирања, тестирања, те увођења у продукциони рад,
   3) едукацију запослених и
   4) поступке комуникације и извјештавања.

(2) Банка је дужна обезбиједити адекватно раздвајање развојног, тестног и продукционог окружења.

Члан 21.

(1) Банка је дужна да успостави процес управљања хардверским и софтверским компонентама у свим фазама њиховог животног циклуса – од набавке или развоја до повлачења из употребе.

(2) Процес управљања хардверским и софтверским компонентама треба да обухвати: поступке идентификације, одржавања детаљне и ажурне евиденције, именовање једног или више лица запослених у банци који су одговорни за управљање и заштиту тих компонената, те утврђивање правила њиховог прихватљивог коришћења и безбједног одлагања при повлачењу из употребе.

(3) Банка је дужна да обезбиједи адекватно одржавање хардверских и софтверских компонената информационог система према препорукама произвођача, те да чува записе о том одржавању.

(4) Банка је дужна да класификује и заштити информације, те дефинише начин управљања истим према њиховој важности, правним захтјевима, осјетљивости и критичности за банку.

Члан 22.

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

(2) Процес из става 1. овог члана као минимум треба да обухвати:
   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,
5) информисање корисника информационог система о детаљима извршених промјена и
6) управљање хитним промјенама.

(3) Банка је дужна да утврди почетне верзије софтверских и хардверских компонената информационог система, те да евидентира и хронолошки документује све промјене ових компонената.

(4) Банка је дужна утврдити процедуре за управљање безбједносним 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.

(5) Банка је дужна обезбиједити да тестно окружење у највећој могућој мјери одражава продукционо окружење, а да притом није нарушена повјерљивост информација.

Члан 23.

Банка је дужна успоставити процес управљања корисничким захтјевима, који као минимум треба да обухвати процедуре за пријављивање, класификацију, одређивање приоритета, обраду и извјештавање о корисничким захтјевима.

Члан 24.

Банка је дужна да дефинише и имплементира процедуре управљања документацијом у вези с информационим системом, које као минимум треба да обезбиједе:
1) постојање тачне, потпуне и ажурне документације и
2) приступ запослених документацији у складу са њиховим пословним потребама.

Члан 25.

(1) Банка је дужна да обезбиједи адекватну и континуирану едукацију запослених која се односи на коришћење ресурса информационог система, као и специјалистичке едукације администратора система, лица одговорног за функцију безбједности информационог система и интерног ревизора који обавља ревизију информационог система.

(2) Банка је дужна да проводи програме подизања свијести корисника информационог система о безбједности информационог система, водећи рачуна о актуелним трендовима.

(3) Банка је дужна да спроводи тестирање корисника информационог система из области безбједности информационог система, те да анализира и документује резултате овог тестирања.

9. План опоравка информационог система

Члан 26.

(1) С циљем обезбјеђења континуираног одвијања критичних (кључних) пословних процеса, банка је дужна да донесе план континуитета пословања и план опоравка информационог система у складу с Одлуком о управљању ризицима у банкама.

(2) На основу спроведене анализе утицаја на пословање, банка је дужна да дефинише и усвоји план опоравка информационог система, који ће примијенити у случају ванредних ситуација, да утврди приоритете опоравка пословних процеса, као и потребне ресурсе и системе, те да детаљно опише поступке које је потребно

слиједити како би се у захтијеваном времену опоравка и са захтијеваним функционалностима опоравили критични (кључни) пословни процеси.

(3) У оквиру анализе утицаја на пословање потребно је, као минимум:
1) утврдити критичне (кључне) пословне процесе и активности,
2) утврдити ресурсе и системе потребне за одвијање појединачних пословних процеса, као и њихове међузависности и повезаности,
3) проценити ризик у вези са појединачним пословним процесима,
4) утврдити прихватљиви ниво ризика за појединачне пословне процесе и
5) одредити RTO и RPO појединачних пословних процеса, имајући у виду екстернализацију и зависност од трећих лица.

(4) План опоравка информационог система обавезно садржи:
1) детаљне процедуре и упутства за опоравак ресурса информационог система потребних за одвијање критичних (кључних) пословних процеса у случају ванредних ситуација,
2) дефинисане приоритете опоравка ресурса информационог система, као и списак свих ресурса потребних за поновно успостављање критичних (кључних) пословних процеса,
3) податке о тимовима који ће бити одговорни за опоравак информационог система и њиховим члановима, са јасно утврђеним дужностима и одговорностима,
4) податке о локацији за опоравак информационог система и
5) податке о кључним пружаоцима услуга.

(5) Банка је дужна, ради ефикасног спровођења планова из става 1. овог члана, обезбиједити да сви запослени буду упознати са својим улогама и одговорностима у случају наступања ванредних ситуација. За спровођење и усклађивање ових планова са пословним промјенама одговорна је управа банке.

Члан 27.

(1) Банка је дужна да на основу анализе утицаја на пословање и процјене ризика обезбиједи резервну локацију за опоравак информационог система, која је на одговарајућој удаљености од примарне локације, узимајући у обзир да примарна и резервна локација не могу истовремено бити изложене истом утицају ризика.

(2) Банка је дужна да планове из члана 26. став 1. ове одлуке тестира периодично и послије значајних промјена, а најмање једном годишње, те да документује резултате ових тестирања и обезбиједи да је извјештај о резултатима тестирања усвојен од стране управе банке. Тестирања треба проводити на бази различитих сценарија (нпр. сајбер напад, прекид комуникационих веза, недоступност примарне локације, губитак критичних података и др.).

(3) Банка је дужна најмање 30 дана прије тестирања плана опоравка информационог система обавијестити Агенцију о томе.

(4) Банка је дужна да у случају настанка околности које захтијевају примјену плана опоравка информационог система одмах обавијести Агенцију о свим релевантним чињеницама и околностима које се на то односе.

Члан 28.

Уколико је банка екстернализовала информациони систем, у потпуности или дјелимично, изван територије Босне и Херцеговине, дужна је да:

1) у оквиру плана опоравка информационог система дефинише критичне (кључне) пословне процесе са становишта континуитета пословања и њиховог одвијања у земљи,
2) обезбиједи ресурсе информационог система на територији Босне и Херцеговине који су потребни за опоравак пословних процеса дефинисаних у тачки 1. овог става, у захтијеваном времену опоравка,
3) обезбиједи резервне копије података на годишњем нивоу на територији Босне и Херцеговине у складу са важећим законским прописима и
4) проводи тестирање плана опоравка информационог система у земљи у складу с одредбама члана 27. ове одлуке.

Члан 29.

(1) Банка је дужна да успостави процес управљања резервним копијама података, који укључује детаљне процедуре и одговорности везане за начин и учесталост израде, начин и вријеме чувања, провјеру исправности, као и опоравак података, како би се обезбиједила расположивост података, те омогућио опоравак, тј. поновно успостављање критичних (кључних) пословних процеса у захтијеваном времену опоравка у случају непредвиђених догађаја и ванредних ситуација.

(2) Резервне копије података морају бити ажурне, периодично тестиране и адекватно заштићене на једној или више секундарних локација, од којих најмање једна мора бити довољно удаљена од локације на којој се налазе изворни подаци, а на основу урађене анализе ризика. Притом је банка дужна обезбиједити резервне копије података на неком од екстерних медија.

(3) Банка је дужна адекватно заштитити резервне копије података приликом њиховог преноса и одлагања, те обезбиједити ажурну евиденцију о њима.

Члан 30.

(1) Банка је дужна да успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбједности или функционалности ресурса информационог система.

(2) Банка је дужна, као минимум, да пропише процедуре за пријављивање, класификацију, обраду, опоравак и праћење, као и анализу и извјештавање о инцидентима.

(3) Банка је дужна, као минимум, да евидентира сљедеће врсте инцидената: грешку или прекид у раду хардверских и софтверских компонената, смањење перформанси сервиса, неауторизовани приступ ресурсима информационог система, одлив података, крађу идентитета, малициозни код, крађу, неуспјешан процес израде резервне копије података, те нарушавање интегритета података.

(4) Банка је дужна да одмах по сазнању о тежем инциденту, било да се односи на дио информационог система који се налази у банци или је екстернализован (кључна банкарска апликација, систем електронског банкарства, систем картичног пословања и сл.), обавијести Агенцију, те да након рјешавања инцидента достави комплетну документацију у вези с инцидентом, која обавезно садржи податке о врсти инцидента, опис инцидента, вријеме његовог трајања, посљедице које је изазвао, те предузете активности.

10. Електронско банкарство

Члан 31.

(1) Банка је дужна да, као саставни дио управљања ризиком информационог система, успостави процес управљања ризицима који произилазе из пружања услуга

електронског банкарства, у оквиру којег је потребно проводити и документовати детаљне процјене ових ризика узимајући у обзир минимално: технолошка рјешења која се користе, услуге које су екстернализоване и техничко окружење клијента.

(2) У пословима електронског банкарства банка је, као минимум, дужна да:
1) успостави процес за надзирање, рјешавање и праћење безбједносних инцидената, укључујући и приговоре корисника који се односе на безбједност, те редовно извјештавање о овим инцидентима,
2) примијени безбједне и ефикасне методе аутентификације за потврду идентитета и овлашћења лица, процеса и система,
3) обезбиједи да аутентификација корисника електронског банкарства укључује комбинацију најмање два међусобно независна елемента за потврђивање корисничког идентитета,
4) обезбиједи одговарајућу потврду свог идентитета на дистрибутивном каналу електронског банкарства како би корисници електронског банкарства могли провјерити идентитет и аутентичност банке,
5) обезбиједи да се при размјени осјетљивих података примијени безбједно криптовање комуникационих канала између страна које учествују за вријеме трајања сесије, у сврху обезбјеђења повјерљивости и интегритета података,
6) утврди максималан број неуспјешних покушаја пријаве на систем или аутентификације, најдуже вријеме трајања сесије без активности корисника, као и временско ограничавање валидности аутентификације и
7) обезбиједи генерисање, чување и редовну анализу оперативних и системских записа, као и контроле приступа осјетљивим подацима о трансакцијама и критичним ресурсима, како би се осигурала непорецивост и доказивост радњи у вези с електронским банкарством.

(3) Изузетно од става 2. тачка 3. овог члана банка може примијенити аутентификацију корисника која се врши коришћењем једног елемента за потврђивање корисничког идентитета, у случају:
1) плаћања мале новчане вриједности, под условом да се ризицима који се односе на укупан износ ових трансакција управља на одговарајући начин,
2) преноса новчаних средстава између два рачуна истог корисника код исте банке и
3) плаћања према поузданим примаоцима, тј. примаоцима које је корисник унапријед одредио (тзв. бијеле листе прималаца).

(4) Банка је дужна да за примјену аутентификације из става 3. овог члана документује свеобухватну и детаљну анализу ризика и начин управљања ризицима који произилазе из пружања услуга утврђених у одредбама става 3. т. 1–3. овог члана.

(5) Банка је у оквиру система електронског банкарства дужна успоставити механизме праћења трансакција у сврху спречавања, откривања и блокирања сумњивих платних трансакција прије коначне ауторизације од стране банке, при чему сумњиве или високоризичне трансакције треба да буду предмет посебног поступка испитивања и процјене.

(6) Банка је дужна да у оквиру информација које пружа кориснику, а тичу се услуга електронског банкарства, обавезно наведе:
1) захтјеве који се односе на опрему корисника, софтверске или друге потребне алате (нпр. антивирусни софтвер, фајервол и др.),
2) упутства за исправно и безбједно коришћење софтверских и хардверских ресурса (нпр. токен, паметна картица, лозинка и др.), као и поступке у случају губитка или крађе ресурса који се користе за пријаву на систем или провођење трансакције,

3) поступке које треба слиједити у случају откривене злоупотребе или сумње на злоупотребу и
4) опис појединачних одговорности и обавеза пружаоца услуге електронског банкарства и корисника у вези са коришћењем услуге електронског банкарства.

11. Прелазне и завршне одредбе

Члан 32.

(1) Упутством за извјештавање о управљању информационим системима детаљније ће се прописати извјештавање, начин и методологија попуњавања образаца, који су саставни дио наведеног упутства.

(2) Банка је дужна да усклади своје пословање с одредбама ове одлуке у року од 90 дана, изузев члана 29. ст. 2–6, који се почиње примјењивати 180 дана од дана ступања на снагу ове одлуке, те члана 10. став 4, члана 13. став 4. и члана 15, који се почињу примјењивати 360 дана од дана ступања на снагу ове одлуке.

(3) Банка је дужна да Агенцији достави извјештаје у складу с Упутством из става 1. овог члана, почев од извјештајног датума 31.12.2017. године.

(4) Даном ступања на снагу ове одлуке престаје да важи Одлука о минималним стандардима управљања информационим системима у банкама („Службени гласник Републике Српске“ број 1/14).

Члан 33.

Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске“.

Број: УО-327/17

Датум: 11.12.2017. год.

ПРЕДСЈЕДНИК
УПРАВНОГ ОДБОРА
Мира Бјелац