Në bazë të nenit 35, paragrafi 1 nënparagrafi 1.1 dhe nenit 65 të Ligjit nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës (Gazeta Zyrtare e Republikës së Kosovës , Nr. 77/16 gusht 2010), të ndryshuar dhe plotësuar me Ligjin Nr. 05/L –150 (Gazeta Zyrtare e Republikës së Kosovës / Nr. 10 /03 Prill 2017) dhe në bazë të nenit 135, nenit 95, paragrafit 3 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave dhe neni 51 të Ligjit Nr.08/L-304 për Bankat, Bordi i Bankës Qendrore të Republikës së Kosovës, në mbledhjen e mbajtur më 17 dhjetor 2024 miratoi këtë:

RREGULLORE PËR TEKNOLOGJINË E INFORMACIONIT DHE KOMUNIKIMIT DHE MENAXHIMIN E RREZIKUT TË SIGURISË

KAPITULLI I
DISPOZITAT E PËRGJITHSHME

Neni 1
Qëllimi dhe fushëveprimi

1. Qëllimi i kësaj rregulloreje është të përcaktojë kërkesat për vendosjen e masave rregullatore, rregullave dhe udhëzimeve për zbatimin e menaxhimit të rrezikut operacional dhe të sigurisë.
2. Kjo rregullore aplikohet në lidhje me menaxhimin e TIK-ut dhe rrezikut të sigurisë brenda institucioneve financiare, siç përcaktohet në nenin 2 të kësaj rregulloreje.
3. Kjo Rregullore aplikohet për institucionet financiare, të cilat për qëllim të kësaj rregulloreje i referohen ofruesve për shërbimet e pagesave, siç përcaktohet në paragrafin 1 të nenit 1 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.
4. Për institucionet financiare të ndryshme nga ofruesit e shërbimeve të pagesave, siç përcaktohet në nenet 2 dhe 3, kjo rregullore aplikohet për të gjitha aktivitetet që ato ofrojnë.
5. Kjo rregullore aplikohet tërësisht ose pjesërisht për institucionet mikrofinanciare dhe institucionet financiare jobankare, siç përcaktohet në nenin 3 të Ligjit Nr.08/L-304 për Bankat, duke marrë parasysh madhësinë dhe profilin e rrezikut të tyre.

Neni 2
Përkufizimet

1. Termat dhe përkufizimet e përdorura në këtë Rregullore kanë të njëjtin kuptim si në Ligjin Nr. 08/L-328 për Shërbimet e Pagesave dhe Ligjin nr. 08/L-304 për Bankat.
2. Përveç paragrafit 1 të këtij neni, për qëllime të zbatimit të kësaj Rregulloreje, termat dhe shkurtesat e mëposhtme kanë këto kuptime:

2.1. **BQK -** nënkupton Bankën Qendrore të Kosovës;

2.2. **Institucion financiar -** nënkupton një bankë, një institucion mikrofinanciar, një institucion financiar jo-bankar, një OSHP të referuar në nënparagrafët 1.4, 1.5 dhe 1.6 të nenit 1 të Ligjit për Shërbimet e Pagesave, një institucion pagese ose një institucion i parasë elektronike, objekt i kësaj Rregulloreje në pajtim me nenin 2 të kësaj rregulloreje;

2.3. **TIK -** nënkupton teknologjinë e informacionit dhe komunikimit, siç përcaktohet në Ligjin Nr. 04/L-145 për Organet Qeveritare për Shoqërinë e Informacionit;

2.4. Rreziqet e TIK-ut dhe të sigurisë trajtojnë rreziqet operacionale dhe të sigurisë të përcaktuara në nenin 95 të Ligjit nr. 08/L-328 për shërbimet e pagesave për ofrimin e shërbimeve të pagesave.

2.5. **Rreziku i TIK-ut dhe i sigurisë -** nënkupton rrezikun e humbjes për shkak të shkeljes së konfidencialitetit, dështimit të integritetit të sistemeve dhe të dhënave, papërshtatshmërisë ose mosdisponueshmërisë së sistemeve dhe të dhënave ose pamundësisë për të ndryshuar teknologjinë e informacionit dhe komunikimit brenda një kohe të arsyeshme dhe me kosto të arsyeshme kur ndryshojnë kërkesat e mjedisit ose biznesit (p.sh. shkathtësia). Kjo përfshin rreziqet e sigurisë që rrjedhin nga proceset e brendshme të pamjaftueshme ose të dështuara ose ngjarjet e jashtme, duke përfshirë sulmet kibernetike ose sigurinë fizike të pamjaftueshme;

2.6. **Organ menaxhues -** nënkupton:

2.6.1. për bankat, institucionet mikrofinanciare dhe institucionet financiare jobankare, ky term ka të njëjtin kuptim si në nenin 36, të Ligjit Nr. 08/L-304 për Bankat;

2.6.2. për institucionet e pagesave ose institucionet e parasë elektronike, ky term nënkupton drejtorët ose personat përgjegjës për menaxhimin e institucioneve të pagesave dhe institucioneve të parasë elektronike dhe, sipas rastit, personat përgjegjës për menaxhimin e aktiviteteve të shërbimeve të pagesave të institucioneve të pagesave dhe institucioneve të parasë elektronike;

2.6.3. për OSHP-të e përmendura në nënparagrafët 1.4, 1.5 dhe 1.6 të nenit 1 të Ligjit për Shërbimet e Pagesave, ky term ka kuptimin që i jep ligji në fuqi.

2.7. **Incident operacional ose i sigurisë -** nënkupton një ngjarje të vetme ose një seri ngjarjesh të lidhura të paplanifikuara nga institucioni financiar që ka ose ndoshta do të ketë një ndikim negativ në integritetin, disponueshmërinë, konfidencialitetin dhe/ose vërtetësinë e shërbimeve;

2.8. **OSHP -** nënkupton ofruesin e shërbimit të pagesave. Në kontekstin e kësaj Rregulloreje, përveç rasteve kur specifikohet ndryshe ose evidentohet nga teksti përreth, termi i referohet institucioneve të pagesave dhe institucioneve të parasë elektronike të autorizuara ose të përjashtuara nga autorizimi sipas Ligjit për Shërbimet e Pagesave;

2.9. **Menaxhment i lartë -** nënkupton:

2.9.1. për bankat, institucionet mikrofinanciare dhe institucionet financiare jobankare, ky term ka të njëjtin kuptim me përkufizimin në nenin 47, të Ligjit 08/L-304 të Bankave;

2.9.2. për institucionet e pagesave dhe institucionet e parasë elektronike, ky term nënkupton personat fizikë që ushtrojnë funksione ekzekutive brenda një institucioni dhe që janë

përgjegjës dhe japin llogari para organit drejtues për menaxhimin e përditshëm të institucionit;

2.9.3. për OSHP-të e referuara në nënparagrafët 1.4, 1.5 dhe 1.6 të nenit 1 të Ligjit për Shërbimet e Pagesave, ky term ka kuptimin që i jep ligji në fuqi.

2.10. **Oreksi i rrezikut -** nënkupton nivelin e përgjithshëm dhe llojet e rrezikut që institucionet financiare janë të gatshme të marrin përsipër brenda kapacitetit të tyre të rrezikut, në përputhje me modelin e tyre të biznesit, për të arritur objektivat e tyre strategjikë;

2.11. **Funksion auditimi -** nënkupton:

2.11.1.për bankat, funksioni i auditimit i përcaktuar në nenin 49, të Ligjit 08/L-304 për Bankat si dhe për institucionet mikrofinanciare dhe institucionet financiare jobankare i përcaktuar në nenin 103 Ligjin nr. 04/L-093 për banka, imf dhe IFJB .

2.11.2. për OSHP-të e tjera nga bankat, funksioni i auditimit duhet të jetë i pavarur brenda ose nga OSHP dhe mund të jetë një funksion auditimi i brendshëm dhe/ose i jashtëm.

2.12. **Projekte të TIK-ut -** nënkupton çdo projekt, ose pjesë të tij, ku sistemet dhe shërbimet e TIK-ut ndryshohen, zëvendësohen, shkarkohen ose zbatohen. Projektet e TIK-ut mund të jenë pjesë e programeve më të gjera të TIK-ut ose të transformimit të biznesit;

2.13. **Palë e tretë -** nënkupton një organizatë që ka lidhur marrëdhënie biznesi ose kontrata me një njësi ekonomike për të ofruar një produkt ose shërbim;

2.14. **Asete të informacionit -** nënkupton një koleksion informacioni, qoftë të prekshëm apo të paprekshëm, që ia vlen të mbrohet;

2.15. **Asete të TIK-ut -** nënkupton një aset ose softuer ose harduer që gjendet në mjedisin e biznesit;

2.16. **Sisteme të TIK-ut -** nënkupton ngritjen e TIK-ut si pjesë e një mekanizmi ose një rrjeti ndërlidhës që mbështet operacionet e një institucioni financiar;

2.17. **Shërbime të TIK-ut -** nënkupton shërbimet e ofruara nga sistemet e TIK-ut për një ose më shumë përdorues të brendshëm ose të jashtëm. Shembujt përfshijnë futjen e të dhënave, ruajtjen e të dhënave, përpunimin e të dhënave dhe shërbimet e raportimit, por gjithashtu monitorimin dhe shërbimet e mbështetjes së biznesit dhe vendimeve;

2.18. **Ligji për Shërbimet e Pagesave -** nënkupton Ligjin Nr.08/L-328 për Shërbimet e Pagesave;

2.19. **PSHP -** nënkupton përdorues të shërbimit të pagesave siç përcaktohet në Ligjin për Shërbimet e Pagesave.

Neni 3
Proporcionaliteti

Të gjitha institucionet financiare duhet të respektojnë dispozitat e përcaktuara në këtë Rregullore në mënyrë të tillë që të jetë proporcionale me dhe të marrë parasysh madhësinë e institucioneve financiare, organizimin e tyre të brendshëm, si dhe natyrën, shtrirjen, kompleksitetin dhe rrezikshmërinë e shërbimeve dhe produkteve që institucionet financiare ofrojnë ose synojnë të ofrojnë.

KAPITULLI II
TIK DHE MENAXHIMI I RREZIKUT TË SIGURISË

Qeverisja dhe Strategjia

Neni 4
Qeverisja

1. Organi menaxhues duhet të sigurojë që institucionet financiare të kenë kornizën e duhur të qeverisjes së brendshme dhe të kontrollit të brendshëm për rreziqet e tyre të TIK-ut dhe sigurisë.

   1.1. organi menaxhues duhet të përcaktojë role dhe përgjegjësi të qarta për funksionet e TIK-ut, menaxhimin e rrezikut të sigurisë së informacionit dhe vazhdimësinë e biznesit, duke përfshirë ato për organin menaxhues dhe komitetet e tij.

2. Organi menaxhues duhet të sigurojë që sasia dhe aftësitë e stafit të institucioneve financiare janë të mjaftueshme për të mbështetur nevojat e tyre operacionale për TIK-un dhe proceset e tyre të menaxhimit të rrezikut të TIK-ut dhe sigurisë në baza të vazhdueshme dhe për të siguruar zbatimin e strategjisë së tyre TIK.

   2.1. organi menaxhues duhet të sigurojë që buxheti i ndarë është i përshtatshëm për ta përmbushur siç u cek më lartë. Për më tepër, institucionet financiare duhet të sigurojnë që të gjithë anëtarët e stafit, duke përfshirë bartësit e funksioneve kryesore, të marrin trajnimin e duhur mbi TIK-un dhe rreziqet e sigurisë, duke përfshirë sigurinë e informacionit, në baza vjetore, ose më shpesh nëse kërkohet

3. Organi menaxhues ka përgjegjësi të përgjithshme për përcaktimin, miratimin dhe mbikëqyrjen e zbatimit të strategjisë së TIK-ut të institucioneve financiare si pjesë e strategjisë së tyre të përgjithshme të biznesit, si dhe për krijimin e një kornize efektive të menaxhimit të rrezikut për TIK-un dhe rreziqet e sigurisë për të siguruar përputhjen me legjislacionin në fuqi.

Neni 5
Strategjia

1. Strategjia e TIK-ut duhet të përafrohet me strategjinë e përgjithshme të biznesit të institucioneve financiare dhe duhet të përmbajë kërkesa minimale si më poshtë:

   1.1. si duhet të evoluojë TIK-u i institucioneve financiare për të mbështetur në mënyrë efektive dhe për të marrë pjesë në strategjinë e tyre të biznesit, duke përfshirë evolucionin e strukturës organizative, ndryshimet e sistemit të TIK-ut dhe varësitë kryesore me palët e treta;

   1.2. strategjinë e planifikuar dhe evolucionin e arkitekturës së TIK-ut, duke përfshirë varësitë nga palët e treta;

   1.3. objektiva të qarta të sigurisë së informacionit, duke u fokusuar në sistemet dhe shërbimet e TIK-ut, stafin dhe proceset.

2. Institucionet financiare duhet të krijojnë grupe planesh veprimi që përmbajnë masat që duhen marrë për të arritur objektivin e strategjisë së TIK-ut.

2.1. këto duhet t'i komunikohen të gjithë stafit përkatës (duke përfshirë kontraktorët dhe ofruesit e palëve të treta kur është e zbatueshme dhe e përshtatshme);

2.2. planet e veprimit duhet të rishikohen periodikisht për të siguruar rëndësinë dhe përshtatshmërinë e tyre;

2.3. institucionet financiare duhet gjithashtu të krijojnë procese për të monitoruar dhe matur efektivitetin e zbatimit të strategjisë së tyre TIK.

Neni 6
Përdorimi i ofruesve të palëve të treta

1. Në varësi të Rregullores për aranzhmanet e kontraktimit të jashtëm dhe nenit 21 të Ligjit për Shërbimet e Pagesave, institucionet financiare duhet të sigurojnë efektivitetin e masave për zbutjen e rrezikut siç përcaktohet në kornizën e tyre të menaxhimit të rrezikut, duke përfshirë kërkesat e përcaktuara në këtë Rregullore, kur Funksionet operacionale të shërbimeve të pagesave dhe/ose shërbimeve të TIK-ut dhe sistemeve të TIK-ut të çdo aktiviteti kontraktohen nga jashtë, duke përfshirë subjektet e grupit ose kur përdoren palë të treta.
2. Për të siguruar vazhdimësinë e shërbimeve të TIK-ut dhe sistemeve të TIK-ut, dhe pa paragjykuar kërkesat e tjera të aplikueshme në përputhje me Rregulloren për aranzhmanet e kontraktimit të jashtëm, institucionet financiare duhet të sigurojnë që kontratat dhe marrëveshjet e nivelit të shërbimit (si për rrethana normale ashtu edhe në rast të ndërprerjes së shërbimit - shih gjithashtu Nenin 28) me ofruesit (ofruesit e jashtëm, subjektet e grupit ose ofruesit e palëve të treta) përfshijnë në vijim:

   2.1. objektivat dhe masat e duhura dhe proporcionale të lidhura me sigurinë e informacionit, duke përfshirë kërkesa të tilla si kërkesat minimale të sigurisë kibernetike; specifikimet e ciklit jetësor të të dhënave të institucionit financiar; çdo kërkesë në lidhje me enkriptimin e të dhënave, sigurinë e rrjetit dhe proceset e monitorimit të sigurisë dhe vendndodhjen e qendrave të të dhënave;

   2.2. procedurat e trajtimit të incidenteve operacionale dhe të sigurisë duke përfshirë përshkallëzimin dhe raportimin.

3. Institucionet financiare duhet të monitorojnë dhe të kërkojnë siguri për nivelin e përputhshmërisë së këtyre ofruesve me objektivat e sigurisë, masat dhe objektivat e performancës së institucionit financiar.

KAPITULLI III
KORNIZA E TIK DHE E MENAXHIMIT TË RREZIKUT TË SIGURISË

Neni 7
Organizimi dhe objektivat

1. Institucionet financiare duhet të identifikojnë dhe menaxhojnë rreziqet e tyre të TIK-ut dhe sigurisë. Funksionet e TIK-ut përgjegjës për sistemet, proceset dhe operacionet e sigurisë së TIK-ut duhet të kenë procese dhe kontrolle të përshtatshme për të siguruar që të gjitha rreziqet identifikohen, analizohen, maten, monitorohen, menaxhohen, raportohen dhe mbahen brenda

kufijve të oreksit të rrezikut të institucionit financiar dhe që projektet dhe sistemet që ata ofrojnë dhe aktivitetet që ata kryejnë janë në përputhje me kërkesat e jashtme dhe të brendshme.

2. Institucionet financiare duhet të caktojnë përgjegjësinë për menaxhimin dhe mbikëqyrjen e TIK-ut dhe rreziqeve të sigurisë në një funksion kontrolli, duke iu përmbajtur kërkesave të nenit 9 paragrafi 5 të Rregullores për qeverisjen korporative të bankave. Institucionet financiare duhet të sigurojnë pavarësinë dhe objektivitetin e këtij funksioni të kontrollit duke e ndarë atë në mënyrë të përshtatshme nga proceset e operacioneve të TIK-ut;

   2.1. ky funksion kontrolli duhet t'i përgjigjet drejtpërdrejt organit menaxhues dhe përgjegjës për monitorimin dhe kontrollin e respektimit të kornizës së TIK-ut dhe menaxhimit të rrezikut të sigurisë.

   2.2. ai duhet të sigurojë që rreziqet e TIK-ut dhe të sigurisë janë identifikuar, matur, vlerësuar, menaxhuar, monitoruar dhe raportuar.

   2.3. institucionet financiare duhet të sigurojnë që ky funksion kontrolli të mos jetë përgjegjës për ndonjë auditim të brendshëm.

3. Funksioni i auditimit të brendshëm, duke ndjekur një qasje të bazuar në rrezik, duhet të ketë kapacitetin për të rishikuar në mënyrë të pavarur dhe për të ofruar siguri objektive për përputhshmërinë e të gjitha aktiviteteve dhe njësive të TIK-ut dhe sigurisë të një institucioni financiar me politikat dhe procedurat e institucionit financiar dhe me kërkesat e jashtme, duke iu përmbajtur kërkesave të nenit 17 për Rregullores së për qeverisjen korporative të bankave.

4. Institucionet financiare duhet të përcaktojnë dhe caktojnë rolet dhe përgjegjësitë kryesore, dhe linjat përkatëse të raportimit, në mënyrë që kuadri i menaxhimit të rrezikut të TIK-ut dhe sigurisë të jetë efektiv. Kjo kornizë duhet të integrohet plotësisht dhe të përafrohet me proceset e përgjithshme të menaxhimit të rrezikut të institucioneve financiare.

5. Korniza e menaxhimit të rrezikut të TIK-ut dhe sigurisë duhet të përfshijë të paktën proceset e mëposhtme:

   5.1. të përcaktojë oreksin e rrezikut për rreziqet e TIK-ut dhe të sigurisë, në përputhje me oreksin e rrezikut të institucionit financiar;

   5.2. të identifikojë dhe vlerësojë rreziqet e TIK-ut dhe të sigurisë ndaj të cilave është i ekspozuar një institucion financiar;

   5.3. të përcaktojë masat zbutëse, duke përfshirë kontrollet, për të zbutur rreziqet e TIK-ut dhe të sigurisë;

   5.4. të monitorojë efektivitetin e këtyre masave si dhe numrin e incidenteve të raportuara, duke përfshirë për OSHP-të incidentet e raportuara në përputhje me nenin 96 të Ligjit për Shërbimet e Pagesave që prekin aktivitetet e lidhura me TIK-un, dhe të ndërmarrë veprime për korrigjimin e masave kur është e nevojshme;

   5.5. t'i raportojë organit menaxhues për rreziqet dhe kontrollet e TIK-ut dhe sigurisë;

   5.6. të identifikojë dhe vlerësojë nëse ka ndonjë rrezik TIK dhe të sigurisë që rezulton nga ndonjë ndryshim i madh në sistemin e TIK-ut ose shërbimet, proceset ose procedurat e TIK-ut, dhe/ose pas ndonjë incidenti të rëndësishëm operacional ose të sigurisë.

6. Institucionet financiare duhet të sigurojnë që korniza e TIK-ut dhe e menaxhimit të rrezikut të sigurisë dokumentohet dhe përmirësohet vazhdimisht, bazuar në 'mësimet e nxjerra' gjatë zbatimit dhe monitorimit të tij.

   6.1. kuadri i menaxhimit të rrezikut të TIK-ut dhe sigurisë duhet të miratohet dhe rishikohet, të paktën një herë në vit, nga organi menaxhues.

Neni 8
Identifikimi i funksioneve, proceseve dhe aseteve

1. Institucionet financiare duhet të identifikojnë, krijojnë dhe mbajnë të përditësuar listën e funksioneve të tyre të biznesit, roleve dhe proceseve mbështetëse për të identifikuar rëndësinë e secilit dhe ndërvarësitë e tyre në lidhje me TIK-un dhe rreziqet e sigurisë.
2. Përveç kësaj, institucionet financiare duhet të identifikojnë, krijojnë dhe mbajnë hartën e përditësuar të aseteve të informacionit që mbështesin funksionet e tyre të biznesit dhe proceset mbështetëse, të tilla si sistemet e TIK-ut, stafi, kontraktorët, palët e treta dhe varësitë nga sistemet dhe proceset e tjera të brendshme dhe të jashtme, për të qenë në gjendje, të paktën të menaxhojnë asetet e informacionit që mbështesin funksionet dhe proceset e tyre kritike të biznesit.

Neni 9
Klasifikimi dhe vlerësimi i rrezikut

1. Institucionet financiare duhet të klasifikojnë funksionet e identifikuara të biznesit, proceset mbështetëse dhe asetet e informacionit të përcaktuara në këtë nen për sa i përket kritikës.
2. Për të përcaktuar kritikën e këtyre funksioneve të identifikuara të biznesit, proceset mbështetëse dhe asetet e informacionit, institucionet financiare duhet, së paku, të marrin në konsideratë kërkesat e konfidencialitetit, integritetit dhe disponueshmërisë. Llogaridhënia dhe përgjegjësia për asetet e informacionit duhet të caktohet qartë.
3. Institucionet financiare duhet të rishikojnë përshtatshmërinë e klasifikimit të aseteve të informacionit dhe dokumentacionit përkatës, kur kryhet vlerësimi i rrezikut.
4. Institucionet financiare duhet të identifikojnë rreziqet e TIK-ut dhe të sigurisë që ndikojnë në funksionet e identifikuara dhe të klasifikuara të biznesit, duke mbështetur proceset dhe asetet e informacionit, sipas kritikës së tyre.

   4.1. ky vlerësim i rrezikut duhet të kryhet dhe dokumentohet çdo vit ose në intervale më të shkurtra nëse kërkohet;

   4.2. vlerësime të tilla të rrezikut duhet të kryhen edhe për çdo ndryshim të madh në infrastrukturë, procese ose procedura që prekin funksionet e biznesit, proceset mbështetëse ose asetet e informacionit, dhe për rrjedhojë vlerësimi aktual i rrezikut të institucioneve financiare duhet të përditësohet.

5. Institucionet financiare duhet të sigurojnë që ata të monitorojnë vazhdimisht kërcënimet dhe dobësitë që lidhen me proceset e tyre të biznesit, funksionet mbështetëse dhe asetet e informacionit dhe duhet të rishikojnë rregullisht skenarët e rrezikut që ndikojnë në to.

Neni 10
Zbutja e rrezikut

1. Bazuar në vlerësimet e rrezikut, institucionet financiare duhet të përcaktojnë se cilat masa kërkohen për të zbutur rreziqet e identifikuara të TIK-ut dhe sigurisë në nivele të pranueshme dhe nëse janë të nevojshme ndryshime në proceset ekzistuese të biznesit, masat e kontrollit, sistemet e TIK-ut dhe shërbimet e TIK-ut.

   1.1. një institucion financiar duhet të marrë parasysh kohën e nevojshme për zbatimin e këtyre ndryshimeve dhe kohën për të marrë masat e duhura zbutëse të ndërmjetme për të minimizuar rreziqet e TIK-ut dhe të sigurisë për të qëndruar brenda oreksit të TIK-ut dhe rrezikut të sigurisë së institucionit financiar.

2. Institucionet financiare duhet të përcaktojnë dhe zbatojnë masa për të zbutur rreziqet e identifikuara të TIK-ut dhe të sigurisë dhe për të mbrojtur asetet e informacionit në përputhje me klasifikimin e tyre.

Neni 11
Raportimi

Institucionet financiare duhet t'i raportojnë organit menaxhues rezultatet e vlerësimit të rrezikut në mënyrë të qartë dhe me kohë. Një raportim i tillë është pa paragjykim ndaj obligimit të OSHP-ve për t'i ofruar BQK-së një vlerësim të përditësuar dhe gjithëpërfshirës të rrezikut, siç parashihet në nenin 95 paragrafin 2 të Ligjit për Shërbimet e Pagesave.

Neni 12
Auditimi

1. Qeverisja, sistemet dhe proceset e një institucioni financiar për TIK-un e tij dhe rreziqet e sigurisë duhet të auditohen në baza periodike nga auditorë me njohuri, aftësi dhe kompetenca të mjaftueshme në TIK dhe rreziqet e sigurisë dhe në pagesat (për OSHP-të) për të ofruar siguri të pavarur të tyre. efektiviteti ndaj organit menaxhues.

   1.1. auditorët duhet të jenë të pavarur brenda ose nga institucioni financiar;

   1.2. shpeshtësia dhe fokusi i auditimeve të tilla duhet të jetë në përpjesëtim me rreziqet përkatëse të TIK-ut dhe të sigurisë.

2. Organi menaxhues i një institucioni financiar duhet të miratojë planin vjetor të auditimit, duke përfshirë çdo auditim të TIK-ut dhe çdo modifikim material të tij.

   2.1. plani i auditimit dhe ekzekutimi i tij, duke përfshirë shpeshtësinë e auditimit, duhet të reflektojnë dhe të jenë në proporcion me rreziqet e qenësishme të TIK-ut dhe të sigurisë në institucionin financiar dhe duhet të përditësohen rregullisht.

3. Duhet të krijohet një proces formal përcjellës, duke përfshirë dispozita për verifikimin dhe korrigjimin në kohë të gjetjeve kritike të auditimit të TIK-ut.

KAPITULLI IV
SIGURIA E INFORMACIONIT

Neni 13
Politika e sigurisë së informacionit

1. Institucionet financiare duhet të zhvillojnë dhe dokumentojnë një politikë të sigurisë së informacionit që duhet të përcaktojë parimet dhe rregullat e nivelit të lartë për të mbrojtur konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave dhe informacionit të institucioneve financiare dhe klientëve të tyre.

   1.1. për OSHP-të kjo politikë është identifikuar në dokumentin e politikës së sigurisë që do të miratohet në përputhje me nenin 12 nënparagrafi 1.10 të Ligjit për Shërbimet e Pagesave;

   1.2. politika e sigurisë së informacionit duhet të jetë në përputhje me objektivat e sigurisë së informacionit të institucionit financiar dhe të bazuar në rezultatet përkatëse të procesit të vlerësimit të rrezikut

   1.3. politika duhet të miratohet nga organi menaxhues.

2. Politika duhet të përfshijë një përshkrim të roleve dhe përgjegjësive kryesore të menaxhimit të sigurisë së informacionit, dhe duhet të përcaktojë kërkesat për personelin dhe kontraktorët, proceset dhe teknologjinë në lidhje me sigurinë e informacionit, duke pranuar që stafi dhe kontraktorët në të gjitha nivelet kanë përgjegjësi për të siguruar sigurinë e informacionit të institucioneve financiare.

   2.1. politika duhet të sigurojë konfidencialitetin, integritetin dhe disponueshmërinë e aseteve kritike logjike dhe fizike të një institucioni financiar, burimeve dhe të dhënave të ndjeshme qofshin ato në pushim, në tranzit ose në përdorim;

   2.2. politika e sigurisë së informacionit duhet t'i komunikohet të gjithë stafit dhe kontraktorëve të institucionit financiar.

3. Bazuar në politikën e sigurisë së informacionit, institucionet financiare duhet të vendosin dhe zbatojnë masa sigurie për të zbutur rreziqet e TIK-ut dhe të sigurisë ndaj të cilave janë të ekspozuara. Këto masa duhet të përfshijnë:

   3.1. organizimi dhe qeverisja në përputhje me paragrafët 1, 2 dhe 3 të nenit 8;

   3.2. siguria logjike (neni 14);

   3.3. siguria fizike (neni 15);

   3.4. siguria e operacioneve TIK-ut (neni 16);

   3.5. monitorimi i sigurisë (neni 17);

   3.6. rishikimet, vlerësimi dhe testimi i sigurisë së informacionit (neni 18);

   3.7. trajnimi dhe vetëdijësimi për sigurinë e informacionit (neni 19).

Neni 14
Siguria logjike

1. Institucionet financiare duhet të përcaktojnë, dokumentojnë dhe zbatojnë politika dhe procedura për kontrollin logjik të qasjes (menaxhimi i identitetit dhe qasja).

   1.1. Këto procedura duhet të zbatohen, vendosen, monitorohen dhe rishikohen periodikisht.

   1.2. procedurat duhet të përfshijnë gjithashtu kontrolle për monitorimin e anomalive

   1.3. këto procedura duhet, të paktën, të zbatojnë elementët e mëposhtëm, ku termi 'përdorues' përfshin edhe përdoruesit teknikë:

      1.3.1. **duhet ta dinë, privilegjin më të vogël dhe ndarjen e detyrave**: institucionet financiare duhet të menaxhojnë të drejtat e qasjes në asetet e informacionit dhe sistemet e tyre mbështetëse mbi një bazë "nevoja për të ditur", duke përfshirë qasjen në distancë. Përdoruesve duhet t'u jepen të drejta minimale qasjeje që kërkohen rreptësisht për të kryer detyrat e tyre (parimi i "privilegjit më të vogël"), dmth. për të parandaluar qasjen e pajustifikuar në një grup të madh të dhënash ose për të parandaluar ndarjen e kombinimeve të të drejtave të qasjes që mund të përdoren për të anashkaluar kontrollet (parimi i "ndarjes së detyrave");

      1.3.2. **llogaridhënia e përdoruesve**: institucionet financiare duhet të kufizojnë, sa më shumë që të jetë e mundur, përdorimin e llogarive të përgjithshme dhe të përbashkëta të përdoruesve dhe të sigurojnë që përdoruesit të mund të identifikohen për veprimet e kryera në sistemet e TIK-ut;

      1.3.3. **të drejta të privilegjuara të qasjes**: institucionet financiare duhet të zbatojnë kontrolle të forta mbi qasjen e privilegjuar të sistemit duke kufizuar dhe mbikëqyrur rreptësisht llogaritë me të drejta të larta të qasjes në sistem (p.sh. llogaritë e administratorit). Për të siguruar komunikim të sigurt dhe për të zvogëluar rrezikun, qasja administrative në distancë në sistemet kritike të TIK-ut duhet të jepet vetëm në bazë të nevojës për t'u ditur dhe kur përdoren zgjidhje të forta vërtetimi;

      1.3.4. **regjistrimi i aktiviteteve të përdoruesve**: të paktën, të gjitha aktivitetet nga përdoruesit e privilegjuar duhet të regjistrohen dhe monitorohen. Regjistrat e qasjes duhet të sigurohen për të parandaluar modifikimin ose fshirjen e paautorizuar dhe të mbahen për një periudhë proporcionale me kritikën e funksioneve të identifikuara të biznesit, proceset mbështetëse dhe asetet e informacionit, në përputhje me nenin 10, pa paragjykuar kërkesat e ruajtjes të përcaktuara në ligje ose rregullore të tjera në fuqi. Një institucion financiar duhet ta përdorë këtë informacion për të lehtësuar identifikimin dhe hetimin e aktiviteteve anormale që janë zbuluar në ofrimin e shërbimeve;

      1.3.5. **menaxhimi i qasjes**: të drejtat e qasjes duhet të jepen, tërhiqen ose modifikohen në kohën e duhur, sipas rrjedhave të miratimit të paracaktuara që përfshijnë pronarin e biznesit të informacionit që qaset (pronari i aseteve të informacionit). Në rast të përfundimit të punësimit, të drejtat e qasjes duhet të tërhiqen menjëherë;

1.3.6. **Ricertifikimi i qasjes**: të drejtat e qasjes duhet të rishikohen periodikisht për t'u siguruar që përdoruesit nuk kanë privilegje të tepërta dhe se të drejtat e qasjes tërhiqen kur nuk kërkohen më;

1.3.7. **metodat e vërtetimit**: institucionet financiare duhet të zbatojnë metoda të vërtetimit që janë mjaftueshëm të fuqishme për të siguruar në mënyrë adekuate dhe efektive që politikat dhe procedurat e kontrollit të qasjes janë në përputhje. Metodat e vërtetimit duhet të jenë në proporcion me kritikën e sistemeve të TIK-ut, informacionit ose procesit që qaset. Kjo duhet, së paku, të përfshijë fjalëkalime komplekse ose metoda më të forta vërtetimi (siç është vërtetimi me dy faktorë), bazuar në rrezikun përkatës.

2. Qasja elektronike nga aplikacionet në të dhëna dhe sistemet e TIK-ut duhet të kufizohet në minimumin e kërkuar për të ofruar shërbimin përkatës.

Neni 15
Siguria fizike

1. Masat e sigurisë fizike të institucioneve financiare duhet të përcaktohen, dokumentohen dhe zbatohen për të mbrojtur ambientet e tyre, qendrat e të dhënave dhe zonat e ndjeshme nga qasja e paautorizuar dhe nga rreziqet mjedisore.

2. Qasja fizike në sistemet e TIK-ut duhet t'u lejohet vetëm individëve të autorizuar.

   2.1. autorizimi duhet të caktohet në përputhje me detyrat dhe përgjegjësitë e individit dhe të kufizohet tek individët të cilët janë të trajnuar dhe monitoruar siç duhet.

   2.2. qasja fizike duhet të rishikohet rregullisht për të siguruar që të drejtat e panevojshme të qasjes të revokohen menjëherë kur nuk kërkohet.

3. Masat adekuate për të mbrojtur nga rreziqet mjedisore duhet të jenë në proporcion me rëndësinë e ndërtesave dhe kritikën e operacioneve ose sistemeve të TIK-ut të vendosura në këto ndërtesa.

Neni 16
Siguria e operacioneve të TIK-ut

1. Institucionet financiare duhet të zbatojnë procedura për të parandaluar shfaqjen e çështjeve të sigurisë në sistemet e TIK-ut dhe shërbimet e TIK-ut dhe duhet të minimizojnë ndikimin e tyre në ofrimin e shërbimeve të TIK-ut. Këto procedura duhet të përfshijnë masat e mëposhtme:

   1.1. identifikimin e dobësive të mundshme, të cilat duhet të vlerësohen dhe korrigjohen duke u siguruar që softueri dhe firmware janë të përditësuar, duke përfshirë softuerin e ofruar nga institucionet financiare për përdoruesit e tyre të brendshëm dhe të jashtëm, duke vendosur arna " patches " kritike të sigurisë ose duke zbatuar kontrolle kompensuese;

   1.2. zbatimi i linjave bazë të konfigurimit të sigurt të të gjithë komponentëve të rrjetit;

   1.3. zbatimi i segmentimit të rrjetit, sistemeve të parandalimit të humbjes së të dhënave dhe kriptimi i trafikut të rrjetit (në përputhje me klasifikimin e të dhënave);

1.4. zbatimi i mbrojtjes së pikave fundore duke përfshirë serverët, stacionet e punës dhe pajisjet mobile; institucionet financiare duhet të vlerësojnë nëse pikat fundore përmbushin standardet e sigurisë të përcaktuara prej tyre përpara se t'u jepet qasje në rrjetin e korporatës;

1.5. duke siguruar që mekanizmat janë të vendosur për të verifikuar integritetin e softuerit, firmware dhe të dhënave;

1.6. kriptimi i të dhënave në pushim dhe në tranzit (në përputhje me klasifikimin e të dhënave).

2. Për më tepër, në mënyrë të vazhdueshme, institucionet financiare duhet të përcaktojnë nëse ndryshimet në mjedisin ekzistues operacional ndikojnë në masat ekzistuese të sigurisë ose kërkojnë miratimin e masave shtesë për të zbutur siç duhet rreziqet përkatëse.

2.1. këto ndryshime duhet të jenë pjesë e procesit formal të menaxhimit të ndryshimeve të institucioneve financiare, i cili duhet të sigurojë që ndryshimet janë planifikuar, testuar, dokumentuar, autorizuar dhe zbatuar siç duhet.

Neni 17
Monitorimi i sigurisë

1. Institucionet financiare duhet të krijojnë dhe zbatojnë politika dhe procedura për të zbuluar aktivitetet anormale që mund të ndikojnë në sigurinë e informacionit të institucioneve financiare dhe për t'iu përgjigjur në mënyrë të përshtatshme këtyre ngjarjeve.

1.1. si pjesë e këtij monitorimi të vazhdueshëm, institucionet financiare duhet të zbatojë aftësitë e duhura dhe efektive për zbulimin dhe raportimin e ndërhyrjeve fizike ose logjike, si dhe shkeljet e konfidencialitetit, integritetit dhe disponueshmërisë së aseteve të informacionit;

1.2. proceset e vazhdueshme të monitorimit dhe zbulimit duhet të përfshijnë:

1.2.1. faktorët përkatës të brendshëm dhe të jashtëm, duke përfshirë biznesin dhe funksionet administrative të TIK-ut;

1.2.2. transaksionet për zbulimin e keqpërdorimit të qasjes nga palët e treta ose subjektet e tjera dhe keqpërdorimi i brendshëm i qasjes;

1.2.3. kërcënimet e mundshme të brendshme dhe të jashtme.

2. Institucionet financiare duhet të krijojnë dhe zbatojnë procese dhe struktura organizative për të identifikuar dhe monitoruar vazhdimisht kërcënimet e sigurisë që mund të ndikojnë materialisht në aftësitë e tyre për të ofruar shërbime.

2.1. institucionet financiare duhet të monitorojnë në mënyrë aktive zhvillimet teknologjike për të siguruar që ata janë të vetëdijshëm për rreziqet e sigurisë

2.2. institucionet financiare duhet të zbatojnë masa detektive, për shembull për të identifikuar rrjedhjet e mundshme të informacionit, kodin me qëllim të keq dhe kërcënime të tjera të sigurisë, dhe dobësitë e njohura publikisht në softuer dhe harduer dhe duhet të kontrollojnë për përditësime të reja të sigurisë përkatëse.

3. Procesi i monitorimit të sigurisë duhet të ndihmojë gjithashtu një institucion financiar për të kuptuar natyrën e incidenteve operacionale ose të sigurisë, për të identifikuar tendencat dhe për të mbështetur hetimet e organizatës.

Neni 18
Rishikimet, vlerësimi dhe testimi i sigurisë së informacionit

1. Institucionet financiare duhet të kryejnë një sërë rishikimesh, vlerësimesh dhe testesh të sigurisë së informacionit për të siguruar identifikimin efektiv të cenueshmërisë në sistemet e tyre të TIK-ut dhe shërbimet e TIK-ut.

   1.1. për shembull, institucionet financiare mund të kryejnë analiza të mangësive kundrejt standardeve të sigurisë së informacionit, rishikimeve të pajtueshmërisë, auditimeve të brendshme dhe të jashtme të sistemeve të informacionit ose rishikimeve të sigurisë fizike

   1.2. për më tepër, institucioni financiar duhet të marrë parasysh praktikat e mira të tilla si rishikimet e kodit burimor, vlerësimet e cenueshmërisë, testet e depërtimit dhe ushtrimet stimuluese "red team exercises".

2. Institucionet financiare duhet të krijojnë dhe zbatojnë një kornizë testimi të sigurisë së informacionit që vërteton qëndrueshmërinë dhe efektivitetin e masave të tyre të sigurisë së informacionit dhe të sigurojë që kjo kornizë të marrë parasysh kërcënimet dhe dobësitë, të identifikuara përmes monitorimit të kërcënimeve dhe procesit të vlerësimit të rrezikut të TIK-ut dhe sigurisë.

3. Korniza e testimit të sigurisë së informacionit duhet të sigurojë që testet:

   3.1. kryhen nga testues të pavarur me njohuri, aftësi dhe ekspertizë të mjaftueshme në testimin e masave të sigurisë së informacionit dhe që nuk janë të përfshirë në zhvillimin e masave të sigurisë së informacionit;

   3.2. përfshijnë skanimet e cenueshmërisë dhe testet e depërtimit (përfshirë testimin e penetrimit të udhëhequr nga kërcënimi kur është e nevojshme dhe e përshtatshme) në proporcion me nivelin e rrezikut të identifikuar me proceset dhe sistemet e biznesit.

4. Institucionet financiare duhet të kryejnë teste të vazhdueshme dhe të përsëritura të masave të sigurisë.

   4.1. për të gjitha sistemet kritike të TIK-ut (neni 10 paragrafi 1), këto teste duhet të kryhen të paktën në baza vjetore dhe, për OSHP-të, ato do të jenë pjesë e vlerësimit gjithëpërfshirës të rreziqeve të sigurisë në lidhje me shërbimet e pagesave që ofrojnë, në përputhje me nenin 95 paragrafi 2 të Ligjit për Shërbimet e Pagesave;

   4.2. Sistemet jokritike duhet të testohen rregullisht duke përdorur një qasje të bazuar në rrezik, por të paktën çdo 3 vjet.

5. Institucionet financiare duhet të sigurojnë që testet e masave të sigurisë të kryhen në rast të ndryshimeve në infrastrukturë, procese ose procedura dhe nëse ndryshimet bëhen për shkak të incidenteve të mëdha operacionale ose të sigurisë ose për shkak të lëshimit të aplikacioneve kritike të reja ose të ndryshuara dukshëm të internetit.

6. Institucionet financiare duhet të monitorojnë dhe vlerësojnë rezultatet e testeve të sigurisë dhe të përditësojnë masat e tyre të sigurisë në përputhje me rrethanat pa vonesa të panevojshme në rastin e sistemeve kritike të TIK-ut.

7. Për OSHP-të, korniza e testimit duhet të përfshijë gjithashtu masat e sigurisë që lidhen me: (i) terminalet dhe pajisjet e pagesave të përdorura për ofrimin e shërbimeve të pagesave, (ii) terminalet e pagesave dhe pajisjet e përdorura për vërtetimin e njësive të furnizimit me energji elektrike, dhe

(iii) pajisjet dhe softuerin e ofruar nga OSHP-ja tek PSHP-ja për të gjeneruar/marrë një kod vërtetimi.

8. Bazuar në kërcënimet e sigurisë të vëzhguara dhe ndryshimet e bëra, testimi duhet të kryhet për të inkorporuar skenarë të sulmeve të mundshme përkatëse dhe të njohura.

Neni 19
Trajnimi dhe vetëdijesimi për sigurinë e informacionit

1. Institucionet financiare duhet të krijojnë një program trajnimi, duke përfshirë programe periodike vetëdijesimi për sigurinë, për të gjithë stafin dhe kontraktorët për të siguruar që ata janë të trajnuar për të kryer detyrat dhe përgjegjësitë e tyre në përputhje me politikat dhe procedurat përkatëse të sigurisë për të reduktuar gabimet njerëzore, vjedhjet, mashtrimet, keqpërdorimet ose humbje dhe si të adresohen rreziqet që lidhen me sigurinë e informacionit.

   1.1. institucionet financiare duhet të sigurojnë që programi i trajnimit të ofrojë trajnime për të gjithë anëtarët e stafit dhe kontraktorët të paktën çdo vit.

KAPITULLI V
MENAXHIMI I OPERACIONEVE TË TIK

Neni 20
Menaxhimi i operacioneve të TIK

1. Institucionet financiare duhet të menaxhojnë operacionet e tyre të TIK-ut duke u bazuar në proceset dhe procedurat e dokumentuara dhe të zbatuara (të cilat, për OSHP-të, përfshijnë dokumentin e politikës së sigurisë në përputhje me nënparagrafin 1.10 të nenit 12 të Ligjit për Shërbimet e Pagesave) të miratuara nga organi menaxhues.

   1.1. ky grup dokumentesh duhet të përcaktojë se si institucionet financiare operojnë, monitorojnë dhe kontrollojnë sistemet dhe shërbimet e tyre të TIK-ut, duke përfshirë dokumentimin e operacioneve kritike të TIK-ut dhe duhet t'u mundësojë institucioneve financiare të mbajnë inventar të përditësuar të aseteve të TIK-ut.

2. Institucionet financiare duhet të sigurojnë që performanca e operacioneve të tyre të TIK-ut të jetë në përputhje me kërkesat e tyre të biznesit.

   2.1. institucionet financiare duhet të ruajnë dhe përmirësojnë, kur është e mundur, efikasitetin e operacioneve të tyre të TIK-ut, duke përfshirë, por pa u kufizuar në nevojën për të marrë në konsideratë mënyrën e minimizimit të gabimeve të mundshme që rrjedhin nga ekzekutimi i detyrave manuale.

3. Institucionet financiare duhet të zbatojnë procedurat e regjistrimit dhe monitorimit për operacionet kritike të TIK-ut për të lejuar zbulimin, analizën dhe korrigjimin e gabimeve.

4. Institucionet financiare duhet të mbajnë një inventar të përditësuar të aseteve të tyre të TIK-ut (përfshirë sistemet e TIK-ut, pajisjet e rrjetit, bazat e të dhënave, etj.).

4.1. inventari i aseteve të TIK-ut duhet të ruajë konfigurimin e aseteve të TIK-ut dhe lidhjet dhe ndërvarësitë ndërmjet aseteve të ndryshme të TIK-ut, për të mundësuar një proces të duhur konfigurimi dhe menaxhimi të ndryshimeve.

5. Inventari i aseteve të TIK-ut duhet të jetë mjaft i detajuar për të mundësuar identifikimin e menjëhershëm të aseteve të TIK-ut, vendndodhjen e tij, klasifikimin e sigurisë dhe pronësinë. Ndërvarësia ndërmjet aseteve duhet të dokumentohet për të ndihmuar në përgjigjen ndaj incidenteve të sigurisë dhe operacioneve, duke përfshirë sulmet kibernetike.

6. Institucionet financiare duhet të monitorojnë dhe menaxhojnë ciklet jetësore të aseteve të TIK-ut, për të siguruar që ato të vazhdojnë të përmbushin dhe mbështesin kërkesat e biznesit dhe të menaxhimit të rrezikut.

   6.1. Institucionet financiare duhet të monitorojnë nëse asetet e tyre të TIK-ut mbështeten nga shitësit dhe zhvilluesit e tyre të jashtëm ose të brendshëm dhe nëse të gjitha korrigjimet dhe përmirësimet përkatëse zbatohen bazuar në proceset e dokumentuara.

   6.2. rreziqet që rrjedhin nga ciklet jetësore të aseteve ose të pambështetura të TIK-ut duhet të vlerësohen dhe të zvogëlohen.

7. Institucionet financiare duhet të zbatojnë proceset e planifikimit dhe monitorimit të performancës dhe kapaciteteve për të parandaluar, zbuluar dhe reaguar ndaj çështjeve të rëndësishme të performancës së sistemeve të TIK-ut dhe mungesave të kapaciteteve të TIK-ut në kohën e duhur.

8. Institucionet financiare duhet të përcaktojnë dhe zbatojnë procedurat e rezervimit dhe restaurimit të të dhënave dhe sistemeve të TIK-ut për të siguruar që ato të mund të rikuperohen sipas nevojës.

   8.1. fushëveprimi dhe shpeshtësia e kopjeve rezervë duhet të përcaktohet në përputhje me kërkesat e rimëkëmbjes së biznesit dhe kritikitetin e të dhënave dhe sistemeve të TIK-ut dhe të vlerësohet sipas vlerësimit të rrezikut të kryer;

   8.2. testimi i procedurave rezervë dhe restaurimit duhet të ndërmerret në baza periodike.

9. Institucionet financiare duhet të sigurojnë që kopjet rezervë të të dhënave dhe të sistemit të TIK-ut të ruhen në mënyrë të sigurt dhe të jenë mjaft të largëta nga faqja kryesore, në mënyrë që të mos ekspozohen ndaj të njëjtave rreziqe.

Neni 21
Menaxhimi i incidenteve dhe problemeve të TIK

1. Institucionet financiare duhet të krijojnë dhe zbatojnë një proces të menaxhimit të incidenteve dhe problemeve për të monitoruar dhe regjistruar incidentet operacionale dhe të sigurisë së TIK-ut për t'u mundësuar institucioneve financiare që të vazhdojnë ose rifillojnë, në kohën e duhur, funksionet dhe proceset kritike të biznesit kur ndodhin ndërprerje.

   1.1. institucionet financiare duhet të përcaktojnë kriteret dhe kufijtë e duhur për klasifikimin e ngjarjeve si incidente operacionale ose të sigurisë, siç përcaktohet në nenin 3, si dhe treguesit e paralajmërimit të hershëm që duhet të shërbejnë si alarme për të mundësuar zbulimin e hershëm të këtyre incidenteve;

   1.2. kriteret dhe kufijtë e tillë, për OSHP-të, nuk paragjykojnë klasifikimin e incidenteve madhore në përputhje me nenin 96 të Ligjit për Shërbimet e Pagesave dhe Rregulloren për

ta njoftuar Bankën Qendrore të Republikës së Kosovës për incidente madhore operacionale apo të sigurisë.

2. Për të minimizuar ndikimin e ngjarjeve të padëshiruara dhe për të mundësuar rikuperimin në kohë, institucionet financiare duhet të krijojnë procese dhe struktura organizative të përshtatshme për të siguruar një monitorim të qëndrueshëm dhe të integruar, trajtimin dhe ndjekjen e incidenteve operacionale dhe të sigurisë dhe për t'u siguruar që shkaqet kryesore janë identifikuar dhe eliminuar për të parandaluar shfaqjen e incidenteve të përsëritura. Procesi i menaxhimit të incidentit dhe problemit duhet të përcaktojë:

   2.1. procedurat për identifikimin, gjurmimin, regjistrimin, kategorizimin dhe klasifikimin e incidenteve sipas një prioriteti, bazuar në kritikën e biznesit;

   2.2. rolet dhe përgjegjësitë për skenarë të ndryshëm incidentesh (p.sh. gabime, keqfunksionime, sulme kibernetike);

   2.3. procedurat e menaxhimit të problemeve për të identifikuar, analizuar dhe zgjidhur shkakun kryesorë pas një ose më shumë incidenteve një institucion financiar duhet të analizojë incidentet operacionale ose të sigurisë që mund të prekin institucionin financiar që janë identifikuar ose kanë ndodhur brenda dhe/ose jashtë organizatës dhe duhet të marrë parasysh mësimet kryesore të nxjerra nga këto analiza dhe përditësimi i masave të sigurisë në përputhje me rrethanat;

   2.4. plane efektive të komunikimit të brendshëm, duke përfshirë njoftimin e incidentit dhe procedurat e përshkallëzimit - duke mbuluar gjithashtu ankesat e klientëve në lidhje me sigurinë - për të siguruar që:

      2.4.1. incidentet me një ndikim negativ potencialisht të lartë në sistemet kritike të TIK-ut dhe shërbimet e TIK-ut i raportohen menaxhmentit të lartë përkatës dhe menaxhmentit të lartë të TIK-ut;

      2.4.2. organi menaxhues informohet ad hoc në rast incidentesh të rëndësishme dhe, të paktën, informohet për ndikimin, reagimin dhe kontrollet shtesë që do të përcaktohen si rezultat i incidenteve.

   2.5. procedurat e reagimit ndaj incidenteve për të zvogëluar ndikimet që lidhen me incidentet dhe për të siguruar që shërbimi të bëhet funksional dhe i sigurt në kohën e duhur;

   2.6. plane specifike të komunikimit të jashtëm për funksionet dhe proceset kritike të biznesit me qëllim që:

      2.6.1. të bashkëpunojë me palët përkatëse të interesit për t'iu përgjigjur në mënyrë efektive dhe për t'u rikuperuar nga incidenti;

      2.6.2. të sigurojë informacion në kohë për palët e jashtme (p.sh. klientët, pjesëmarrësit e tjerë të tregut, autoritetin mbikëqyrës) sipas rastit dhe në përputhje me rregullore në fuqi.

KAPITULLI VI
PROJEKTI I TIK DHE MENAXHIMI I NDRYSHIMEVE

Neni 22
Menaxhimi i projektit të TIK

1. Një institucion financiar duhet të zbatojë një program dhe/ose një proces të qeverisjes së projektit që përcakton rolet, përgjegjësitë dhe llogaridhëniet për të mbështetur në mënyrë efektive zbatimin e strategjisë së TIK-ut.
2. Një institucion financiar duhet të monitorojë dhe të zbusë në mënyrë të përshtatshme rreziqet që rrjedhin nga portofoli i tyre i projekteve të TIK-ut (menaxhimi i programit), duke marrë parasysh gjithashtu rreziqet që mund të rezultojnë nga ndërvarësia midis projekteve të ndryshme dhe nga varësia e projekteve të shumta nga të njëjtat burime dhe/ose ekspertizë.
3. Një institucion financiar duhet të krijojë dhe zbatojë një politikë të menaxhimit të projektit të TIK-ut që përfshin si minimum:
   3.1. objektivat e projektit;
   3.2. rolet dhe përgjegjësitë;
   3.3. një vlerësim të rrezikut të projektit;
   3.4. një plan projekti, afat kohor dhe hapa;
   3.5. piketa kryesore;
   3.6. ndryshimet e kërkesave të menaxhimit.
4. Politika e menaxhimit të projektit të TIK-ut duhet të sigurojë që kërkesat e sigurisë së informacionit të analizohen dhe miratohen nga një funksion që është i pavarur nga funksioni i zhvillimit.
5. Një institucion financiar duhet të sigurojë që të gjitha fushat e ndikuara nga një projekt i TIK-ut të përfaqësohen në ekipin e projektit dhe që ekipi i projektit të ketë njohuritë e nevojshme për të siguruar zbatimin e sigurt dhe të suksesshëm të projektit.
6. Krijimi dhe ecuria e projekteve të TIK-ut dhe rreziqet e lidhura me to duhet t'i raportohen organit menaxhues, individualisht ose në grup, në varësi të rëndësisë dhe madhësisë së projekteve të TIK-ut, rregullisht dhe në baza ad hoc sipas rastit.
   6.1. institucionet financiare duhet të përfshijnë rrezikun e projektit në kornizën e tyre të menaxhimit të rrezikut.

Neni 23
Përvetësimi dhe zhvillimi i sistemeve të TIK

1. Institucionet financiare duhet të zhvillojnë dhe zbatojnë një proces që rregullon blerjen, zhvillimin dhe mirëmbajtjen e sistemeve të TIK-ut, të dizajnuara duke përdorur një qasje të bazuar në rrezik.
2. Një institucion financiar duhet të sigurojë që, përpara se të ndodhë ndonjë blerje ose zhvillim i sistemeve të TIK-ut, kërkesat funksionale dhe jofunksionale (përfshirë kërkesat e sigurisë së informacionit) të përcaktohen qartë dhe të miratohen nga menaxhmenti përkatës i biznesit.

3. Një institucion financiar duhet të sigurojë se janë marrë masa për të zvogëluar rrezikun e ndryshimit të paqëllimshëm ose manipulimit të qëllimshëm të sistemeve të TIK-ut gjatë zhvillimit dhe zbatimit në mjedisin e prodhimit.

4. Institucionet financiare duhet të kenë një metodologji për testimin dhe miratimin e sistemeve të TIK-ut përpara përdorimit të tyre të parë.

   4.1. kjo metodologji duhet të marrë në konsideratë kritikën e proceseve dhe aseteve të biznesit;

   4.2. testimi duhet të sigurojë që sistemet e reja të TIK-ut të funksionojnë siç synohet;

   4.3. ata gjithashtu duhet të përdorin mjedise testuese që pasqyrojnë në mënyrë adekuate mjedisin e prodhimit.

5. Institucionet financiare duhet të testojnë sistemet e TIK-ut, shërbimet e TIK-ut dhe masat e sigurisë së informacionit për të identifikuar dobësitë, shkeljet dhe incidentet e mundshme të sigurisë.

6. Një institucion financiar duhet të zbatojë mjedise të veçanta të TIK-ut për të siguruar ndarjen e duhur të detyrave dhe për të zvogëluar ndikimin e ndryshimeve të paverifikuara në sistemet e prodhimit.

   6.1. në mënyrë specifike, një institucion financiar duhet të sigurojë ndarjen e mjediseve të prodhimit nga mjediset e zhvillimit, testimit dhe mjediseve të tjera joprodhuese;

   6.2. një institucion financiar duhet të sigurojë integritetin dhe konfidencialitetin e të dhënave të prodhimit në mjedise joprodhuese. Qasja në të dhënat e prodhimit është e kufizuar për përdoruesit e autorizuar.

7. Institucionet financiare duhet të zbatojnë masa për të mbrojtur integritetin e kodeve burimore të sistemeve të TIK-ut që zhvillohen brenda vendit.

   7.1. institucionet financiare duhet gjithashtu të dokumentojnë zhvillimin, zbatimin, funksionimin dhe/ose konfigurimin e sistemeve të TIK-ut në mënyrë gjithëpërfshirëse për të reduktuar çdo varësi të panevojshme nga ekspertët e lëndës;

   7.2. dokumentacioni i sistemit TIK duhet të përmbajë, aty ku është e aplikueshme, të paktën dokumentacionin e përdoruesit, dokumentacionin teknik të sistemit dhe procedurat e funksionimit.

8. Proceset e një institucioni financiar për blerjen dhe zhvillimin e sistemeve të TIK-ut duhet të zbatohen gjithashtu për sistemet e TIK-ut të zhvilluara ose të menaxhuara nga përdoruesit fundorë të funksionit të biznesit jashtë organizatës së TIK-ut (p.sh. aplikacionet kompjuterike të përdoruesve fundorë) duke përdorur një qasje të bazuar në rrezik.

   8.1. institucioni financiar duhet të mbajë një regjistër të këtyre aplikacioneve që mbështesin funksionet ose proceset kritike të biznesit.

Neni 24
Menaxhimi i ndryshimeve të TIK

1. Institucionet financiare duhet të krijojnë dhe zbatojnë një proces të menaxhimit të ndryshimeve të TIK-ut për të siguruar që të gjitha ndryshimet në sistemet e TIK-ut regjistrohen, testohen, vlerësohen, miratohen, zbatohen dhe verifikohen në mënyrë të kontrolluar dhe në përputhje me politikat dhe procedurat në fuqi.

1.1. institucionet financiare duhet të trajtojnë ndryshimet gjatë emergjencave (d.m.th. ndryshimet që duhet të futen sa më shpejt të jetë e mundur) duke ndjekur procedurat që ofrojnë garanci të përshtatshme.

2. Institucionet financiare duhet të përcaktojnë nëse ndryshimet në mjedisin ekzistues operacional ndikojnë në masat ekzistuese të sigurisë ose kërkojnë miratimin e masave shtesë për të zvogëluar rreziqet e përfshira. Këto ndryshime duhet të jenë në përputhje me procesin formal të menaxhimit të ndryshimeve të institucioneve financiare.

KAPITULLI VII
MENAXHIMI I VAZHDIMËSISË SË BIZNESIT

Neni 25
Procesi i menaxhimit të vazhdimësisë së biznesit

Institucionet financiare duhet të krijojnë një proces të shëndoshë të menaxhimit të vazhdimësisë së biznesit (MVB) për të maksimizuar aftësitë e tyre për të ofruar shërbime në mënyrë të vazhdueshme dhe për të kufizuar humbjet në rast të ndërprerjes së rëndë të biznesit.

Neni 26
Analiza e ndikimit në biznes

1. Si pjesë e menaxhimit të shëndoshë të vazhdimësisë së biznesit, institucionet financiare duhet të kryejnë analizën e ndikimit në biznes (BIA) duke analizuar ekspozimin e tyre ndaj ndërprerjeve të rënda të biznesit dhe duke vlerësuar ndikimet e tyre të mundshme (përfshirë konfidencialitetin, integritetin dhe disponueshmërinë), në mënyrë sasiore dhe cilësore, duke përdorur të dhëna të brendshme dhe/ose të jashtme (p.sh. të dhënat e ofruesit të palës së tretë të rëndësishme për një proces biznesi ose të dhëna të disponueshme publikisht që mund të jenë të rëndësishme për BIA) dhe analiza e skenarit.

   1.1. BIA duhet gjithashtu të marrë në konsideratë kritikën e funksioneve të identifikuara dhe të klasifikuara të biznesit, proceset mbështetëse, palët e treta dhe asetet e informacionit, si dhe ndërvarësinë e tyre, në përputhje me nenin 10.

2. Institucionet financiare duhet të sigurojnë që sistemet e tyre të TIK-ut dhe shërbimet e TIK-ut të jenë të dizajnuara dhe të përafruara me BIA-n e tyre, për shembull me tepricë të disa komponentëve kritikë për të parandaluar ndërprerjet e shkaktuara nga ngjarjet që ndikojnë në ato komponentë.

Neni 27
Planifikimi i vazhdimësisë së biznesit

1. Në bazë të BIA-ve të tyre, institucionet financiare duhet të krijojnë plane për të siguruar vazhdimësinë e biznesit (planet e vazhdimësisë së biznesit, PVB), të cilat duhet të dokumentohen dhe miratohen nga organet e tyre menaxhuese.

   1.1. planet duhet të marrin në konsideratë në mënyrë specifike rreziqet që mund të ndikojnë negativisht në sistemet dhe shërbimet e TIK-ut;

1.2. planet duhet të mbështesin objektivat për të mbrojtur dhe, nëse është e nevojshme, të rivendosin konfidencialitetin, integritetin dhe disponueshmërinë e funksioneve të tyre të biznesit, duke mbështetur proceset dhe asetet e informacionit

1.3. institucionet financiare duhet të koordinohen me palët përkatëse të interesit të brendshëm dhe të jashtëm, sipas rastit, gjatë krijimit të këtyre planeve.

2. Institucionet financiare duhet të vendosin PVB-në për të siguruar që ata mund të reagojnë në mënyrë të përshtatshme ndaj skenarëve të mundshëm të dështimit dhe se janë në gjendje të rikuperojnë operacionet e aktiviteteve të tyre kritike të biznesit pas ndërprerjeve brenda një kohe të fundme të rimëkëmbjes (ang. Recovery Time Objective) (RTO, koha maksimale brenda së cilës një sistem ose procesi duhet të rikthehet pas një incidenti) dhe pika e fundme e kthimit (ang. Recovery Point Objective) (RPO, periudha maksimale kohore gjatë së cilës është e pranueshme që të dhënat të humbasin në rast incidenti).

2.1. në rastet e ndërprerjeve të rënda të biznesit që nxisin plane specifike të vazhdimësisë së biznesit, institucionet financiare duhet t'i japin përparësi veprimeve të vazhdimësisë së biznesit duke përdorur qasjen e bazuar në rrezik, e cila mund të bazohet në vlerësimet e rrezikut të kryera sipas nenit 10;

2.2. për OSHP-të kjo mund të përfshijë, për shembull, lehtësimin e përpunimit të mëtejshëm të transaksioneve kritike, ndërkohë që vazhdojnë përpjekjet për riparim.

3. Një institucion financiar duhet të marrë në konsideratë një sërë skenarësh të ndryshëm në PVB-në e tij, duke përfshirë ato ekstreme, por të besueshme ndaj të cilave mund të ekspozohet, duke përfshirë një skenar të sulmit kibernetik, dhe duhet të vlerësojë ndikimin e mundshëm që mund të kenë skenarë të tillë.

3.1. Bazuar në këta skenarë, një institucion financiar duhet të përshkruajë se si sigurohet vazhdimësia e sistemeve dhe shërbimeve të TIK-ut, si dhe siguria e informacionit të institucionit financiar.

Neni 28
Planet e reagimit dhe rimëkëmbjes

1. Në bazë të BIA-ve (paragrafi 1 i nenit 27) dhe skenarëve të besueshëm (paragrafi 3 i nenit 27), institucionet financiare duhet të zhvillojnë plane reagimi dhe rimëkëmbjeje.

1.1. këto plane duhet të specifikojnë se cilat kushte mund të nxisin aktivizimin e planeve dhe çfarë veprimesh duhet të ndërmerren për të siguruar disponueshmërinë, vazhdimësinë dhe rimëkëmbjen e, të paktën, sistemeve kritike të TIK-ut të institucioneve financiare dhe shërbimeve të TIK-ut;

1.2. Planet e reagimit dhe rimëkëmbjes duhet të synojnë përmbushjen e objektivave të rimëkëmbjes së operacioneve të institucioneve financiare.

2. Planet e reagimit dhe rimëkëmbjes duhet të marrin në konsideratë opsionet e rimëkëmbjes afatshkurtër dhe afatgjatë. Planet duhet:

2.1. fokusohet në rikuperimin e operacioneve të funksioneve kritike të biznesit, proceseve mbështetëse, aseteve të informacionit dhe ndërvarësive të tyre për të shmangur efektet negative në funksionimin e institucioneve financiare dhe në sistemin financiar, duke

përfshirë sistemet e pagesave dhe përdoruesit e shërbimeve të pagesave, dhe për të siguruar ekzekutimin e transaksioneve të pagesave në pritje;

2.2. të jetë i dokumentuar dhe i disponueshëm për biznesin dhe njësitë mbështetëse dhe lehtësisht i qasshëm në rast emergjence;

2.3. të përditësohet në përputhje me mësimet e nxjerra nga incidentet, testet, rreziqet e reja të identifikuara dhe kërcënimet, dhe ndryshimi i objektivave dhe prioriteteve të rimëkëmbjes.

3. Planet duhet gjithashtu të marrin në konsideratë opsionet alternative ku rikuperimi mund të mos jetë i realizueshëm në afat të shkurtër për shkak të kostove, rreziqeve, logjistikës ose rrethanave të paparashikuara.

4. Për më tepër, si pjesë e planeve të reagimit dhe rimëkëmbjes, një institucion financiar duhet të marrë parasysh dhe zbatojë masat e vazhdimësisë për të zbutur dështimet e ofruesve të palëve të treta, të cilat janë të një rëndësie kyçe për vazhdimësinë e shërbimit të TIK-ut të një institucioni financiar (në përputhje me dispozitat e Rregullores për aranzhmanet e kontraktimit të jashtëm në lidhje me planet e vazhdimësisë së biznesit).

Neni 29
Testimi i planeve

1. Institucionet financiare duhet të testojnë PVB-të e tyre në mënyrë periodike. Në veçanti, ato duhet të sigurojnë që PVB-të e funksioneve të tyre kritike të biznesit, proceset mbështetëse, asetet e informacionit dhe ndërvarësitë e tyre (përfshirë ato të ofruara nga palët e treta, kur është e zbatueshme) të testohen të paktën çdo vit, në përputhje me paragrafin 3 të këtij neni.

2. PVB-të duhet të përditësohen të paktën çdo vit, bazuar në rezultatet e testimit, inteligjencën aktuale të kërcënimeve dhe mësimet e nxjerra nga ngjarjet e mëparshme. Çdo ndryshim në objektivat e rikuperimit (duke përfshirë RTO-të dhe RPO-të) dhe/ose ndryshim në funksionet e biznesit, proceset mbështetëse dhe asetet e informacionit, duhet të konsiderohet gjithashtu, aty ku është e përshtatshme, si bazë për përditësimin e PVB-ve.

3. Testimi i PVB-ve të tyre nga institucionet financiare duhet të tregojë se ato janë në gjendje të mbështesin qëndrueshmërinë e bizneseve të tyre derisa të rivendosen operacionet kritike. Në veçanti ato duhet:

3.1. Të përfshijnë testimin e një grupi adekuat skenarësh të rëndë por të besueshëm, duke përfshirë ato të konsideruara për zhvillimin e PVB-ve (si dhe testimin e shërbimeve të ofruara nga palë të treta, aty ku është e zbatueshme); kjo duhet të përfshijë kalimin e funksioneve kritike të biznesit, proceset mbështetëse dhe asetet e informacionit në mjedisin e rikuperimit nga fatkeqësitë dhe demonstrimin se ato mund të drejtohen në këtë mënyrë për një periudhë kohe mjaft përfaqësuese dhe se funksionimi normal mund të rikthehet më pas;

3.2. të jenë të dizajnuara për të sfiduar supozimet mbi të cilat mbështeten PVB-të, duke përfshirë marrëveshjet e qeverisjes dhe planet e komunikimit të krizës; dhe

3.3. të përfshijnë procedurat për të verifikuar aftësitë e stafit dhe kontraktorëve të tyre, sistemeve të TIK-ut dhe shërbimeve të TIK-ut për t'iu përgjigjur në mënyrë adekuate skenarëve të përcaktuar në nën-paragrafin 3.1.

4. Rezultatet e testit duhet të dokumentohen dhe çdo mangësi e identifikuar që rezulton nga testet duhet të analizohet, adresohet dhe raportohet te organi menaxhues.

Neni 30
Komunikimet e krizës

Në rast të një ndërprerjeje apo emergjence, dhe gjatë zbatimit të PVB-ve, institucionet financiare duhet të sigurojnë që të kenë masa efektive të komunikimit të krizës në mënyrë që të gjitha palët përkatëse të interesit të brendshëm dhe të jashtëm, përfshirë BQK-në, si dhe ofruesit përkatës (ofruesit e jashtëm , subjektet e grupit ose ofruesit e palëve të treta) të informohen në kohë dhe në mënyrën e duhur.

KAPITULLI VIII
MENAXHIMI I MARRËDHËNIEVE ME PËRDORUESIT E SHËRBIMIT TË PAGESAVE

Neni 31
Menaxhimi i marrëdhënieve me përdoruesit e shërbimit të pagesave

1. OSHP-të duhet të krijojnë dhe zbatojnë procese për të rritur vetëdijesimin e PSHP-ve për rreziqet e sigurisë që lidhen me shërbimet e pagesave, duke u ofruar PSHP-ve asistencë dhe udhëzime.
2. Ndihma dhe udhëzimet e ofruara për PSHP-të duhet të përditësohen në dritën e kërcënimeve dhe dobësive të reja dhe ndryshimet duhet t'i komunikohen PSHP-së.
3. Aty ku lejon funksionaliteti i produktit, OSHP-të duhet t'i lejojnë PSHP-të të çaktivizojnë funksionalitete specifike të pagesave që lidhen me shërbimet e pagesave të ofruara nga OSHP-ja për PSHP-në.
4. Kur, në përputhje me nenin 68 paragrafin 1 të Ligjit për Shërbimet e Pagesave, një OSHP ka rënë dakord me kufijtë e shpenzimeve të paguesit për transaksionet e pagesave të kryera përmes instrumenteve të veçanta të pagesës, OSHP duhet t'i ofrojë paguesit mundësinë për t'i rregulluar këto kufij deri në kufirin maksimal të rënë dakord.
5. OSHP-të duhet t'u ofrojnë PSHP-ve opsionin për të marrë sinjalizime për përpjekjet e inicuara dhe/ose të dështuara për të filluar transaksionet e pagesave, duke u mundësuar atyre të zbulojnë përdorimin mashtrues ose keqdashës të llogarive të tyre.
6. OSHP-të duhet t'i mbajnë PSHP-të të informuara për përditësimet në procedurat e sigurisë që prekin PSHP-të në lidhje me ofrimin e shërbimeve të pagesave.
7. OSHP-të duhet t'u ofrojnë PSHP-ve asistencë për të gjitha pyetjet, kërkesat për mbështetje dhe njoftimet për anomali ose çështje në lidhje me çështjet e sigurisë që lidhen me shërbimet e pagesave. PSHP-të duhet të informohen siç duhet për mënyrën se si mund të merret një ndihmë e tillë.

KAPITULLI IX

DISPOZITAT PËRFUNDIMTARE

Neni 32
Dispozitat kalimtare

Institucioneve financiare që i nënshtrohen kësaj rregulloreje kërkohet që t'i përshtatin plotësisht aktivitetet dhe operacionet e tyre me dispozitat e kësaj rregulloreje brenda 12 muaj nga data e hyrjes në fuqi, siç përcaktohet në nenin 34 të kësaj rregulloreje.

Neni 33
Zbatim, masa përmirësuese dhe ndëshkimeve

Çdo shkelje e dispozitave të kësaj Rregulloreje do t'i nënshtrohet masave përmirësuese dhe ndëshkimeve administrative dhe gjobave civile të përcaktuara në Ligjin nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës, të ndryshuar dhe plotësuar me Ligjin nr. 05/ L –150, Ligji për Shërbimet e Pagesave Nr. 08/L-328 si dhe Ligji për Bankat.

Neni 34
Hyrja në fuqi

Kjo Rregullore hyn në fuqi 10 ditë pas hyrjes në fuqi të Ligjit Nr.08/L-328 për Shërbimet e Pagesave.

Dr.sc. Bashkim Nurboja
Kryetar i Bordit të Bankës Qendrore të Republikës së Kosovës