REPUBLIKA E SHQIPËRISË
BANKA E SHQIPËRISË
KËSHILLI MBIKËQYRËS

VENDIM
Nr. 51, datë 6.11.2024

PËR

MIRATIMIN E RREGULLORES
"PËR ADMINISTRIMIN E RREZIKUT OPERACIONAL NGA BANKAT, INSTITUCIONET E PAGESAVE DHE INSTITUCIONET E PARASË ELEKTRONIKE"

Në bazë dhe për zbatim të nenit 12, shkronja "a" dhe nenit 43, shkronja "c" të ligjit nr. 8269, datë 23.12.1997 "Për Bankën e Shqipërisë", i ndryshuar; nenit 57, pika 4, nenit 58, pika 1, shkronja "c" dhe nenit 126 të ligjit nr. 9662, datë 18.12.2006 "Për bankat në Republikën e Shqipërisë", i ndryshuar; dhe të nenit 88, pika 3 të ligjit nr. 55/2020, datë 30.4.2020 "Për shërbimet e pagesave"; Këshilli Mbikëqyrës i Bankës së Shqipërisë, me propozim të Departamentit të Mbikëqyrjes,

VENDOSI:

1. Të miratojë rregulloren "Për administrimin e rrezikut operacional nga bankat, institucionet e pagesave dhe institucionet e parasë elektronike", sipas tekstit bashkëlidhur këtij vendimi.
2. Ngarkohen subjektet e rregullores për zbatimin e këtij vendimi.
3. Ngarkohet Departamenti i Mbikëqyrjes në Bankën e Shqipërisë për ndjekjen e zbatimit të këtij vendimi.
4. Ngarkohen Kabineti i Guvernatorit dhe Departamenti i Kërkimeve me publikimin e këtij vendimi, përkatësisht në Fletoren Zyrtare të Republikës së Shqipërisë dhe në Buletinin Zyrtar të Bankës së Shqipërisë.

Ky vendim hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

SEKRETARI **KRYETARI**

Elvis ÇIBUKU **Gent SEJKO**

KREU I
TË PËRGJITHSHME

Neni 1
Objekti

Objekti i kësaj rregulloreje është përcaktimi i kërkesave dhe rregullave minimale për administrimin e rrezikut operacional në veprimtarinë bankare dhe/ose financiare nga subjektet e kësaj rregulloreje.

Neni 2
Subjektet

1. Subjekte të kësaj rregulloreje janë bankat dhe degët e bankave të huaja, institucionet e pagesave dhe institucionet e parasë elektronike, të licencuara nga Banka e Shqipërisë për të ushtruar veprimtari bankare dhe financiare në Republikën e Shqipërisë, të cilat do të referohen në vijim në këtë rregullore, me termin "subjekte".
2. Banka e Shqipërisë, bazuar në vlerësimet e saj mbikëqyrëse lidhur me volumin dhe kompleksitetin e veprimtarisë, apo nivelin e ekspozimit ndaj rrezikut operacional, mund të vendosë që përveç subjekteve të parashikuara në pikën 1 të këtij neni, të përfshijë si subjekte të kësaj rregulloreje, edhe subjekte financiare jobanka apo shoqëri kursim-krediti të caktuara, që janë subjekte të rregullores nr. 3, datë 19.1.2011 "Për administrimin e rrezikut operacional nga subjektet financiare jobanka, shoqëritë e kursim-kreditit dhe unionet e tyre", e ndryshuar.
3. Në rastet e parashikuara në pikën 2 të këtij neni, Banka e Shqipërisë njofton subjektin financiar jobankë apo shoqërinë e kursim-kreditit, si dhe përcakton edhe afatin kohor brenda të cilit subjekti duhet të sigurojë plotësimin e kërkesave të kësaj rregulloreje.

Neni 3
Baza ligjore

Kjo rregullore nxirret në bazë dhe për zbatim të:

a) nenit 12, shkronja "a" dhe nenit 43, shkronja "c" të ligjit nr. 8269 datë 23.12.1997 "Për Bankën e Shqipërisë", i ndryshuar;
b) nenit 57, pika 4, nenit 58, pika 1, shkronja "c" dhe nenit 126 të ligjit nr. 9662, datë 18.12.2006 "Për bankat në Republikën e Shqipërisë", i cili këtu e më poshtë në këtë rregullore do të quhet ligji "Për bankat";
c) nenit 88, pika 3 të ligjit nr. 55/2020, datë 30.4.2020 "Për shërbimet e pagesave", i cili këtu e më poshtë në këtë rregullore do të quhet ligji "Për shërbimet e pagesave".

Neni 4
Përkufizime

1. Termat e përdorur në këtë rregullore kanë të njëjtin kuptim me termat e përkufizuar në ligjin "Për bankat" dhe në ligjin "Për shërbimet e pagesave", si dhe në akte të tjera nënligjore të Bankës së Shqipërisë.
2. Përveç sa parashikohet në pikën 1 të këtij neni, për qëllime të zbatimit të kësaj rregulloreje, termat e mëposhtëm kanë këtë kuptim:
   a) "rrezik operacional" - është mundësia që subjekti të pësojë humbje financiare, si rezultat i papërshtatshmërisë ose dështimit të proceseve të brendshme dhe të sistemeve, i gabimeve njerëzore, ose i ngjarjeve të jashtme. Rreziku operacional përfshin edhe rrezikun ligjor, por përjashton rrezikun reputacional dhe strategjik. Për qëllime të sistemit të brendshëm të administrimit të rrezikut operacional, subjekti mund të përcaktojë përkufizime më të specifikuara të këtij rreziku, me kusht që ato të përmbajnë minimalisht elementët e përkufizimit të kësaj rregulloreje;
   b) "rrezik ligjor" - është mundësia që subjekti të pësojë humbje financiare, si rezultat i moszbatimit ose i zbatimit në mënyrën jo të duhur të detyrimeve ligjore dhe/ose kontraktuale, duke përfshirë dhe procedura të tjera ligjore të cilat mund të ndikojnë negativisht në rezultatin financiar;
   c) "rrezik strategjik" - është mundësia që të cenohet arritja e objektivave strategjikë të subjektit, me pasojë fundore humbje financiare, për shkak të ndryshimeve në mjedisin e biznesit dhe nga vendimet e papërshtatshme të biznesit, zbatimi i gabuar i vendimeve ose mungesa e reagimit ndaj ndryshimeve në mjedisin e biznesit;
   d) "rrezik reputacional" - është mundësia që subjekti të pësojë humbje financiare të shkaktuara nga perceptimi negativ nga ana e klientëve, kundërpartive, aksionarëve, investitorëve, mbajtësve të borxhit, tregjeve, palëve të tjera të interesit, rregullatorëve, etj., që mund të ndikojnë negativisht në aftësinë e subjektit për të vazhduar të operojë/funksionojë apo për të krijuar marrëdhënie të reja biznesi dhe për të pasur akses të vazhdueshëm në burime financimi (p.sh nëpërmjet tregjeve ndërbankare, të kapitalit dhe borxhit apo në publikun e gjerë);
   e) "rrezik i sjelljes (*conduct risk*)" - është mundësia që subjekti të pësojë humbje financiare, si pasojë e ofrimit të papërshtatshëm të shërbimeve financiare, duke përfshirë rastet e një qasjeje të gabuar apo të qëllimtë ndaj klientit, ose për shkak të neglizhencës;
   f) "rrezik i modelit" - është mundësia që subjekti të pësojë humbje financiare, si pasojë e vendimeve të marra prej tij, bazuar kryesisht në rezultatet e modeleve të brendshme, të shkaktuara nga gabimet në zhvillimin, zbatimin ose përdorimin e këtyre modeleve;
   g) "rrezik i qenësishëm (*inherent risk*)" - është rreziku ndaj të cilit subjekti ekspozohet, pa marrë në konsideratë mjediset e kontrollit;
   h) "rrezik i mbetur (*residual risk*)" - është rreziku ndaj të cilit subjekti ekspozohet, pas zbatimit të teknikave të zbutjes së rrezikut dhe ndërveprimit me sistemet e kontrollit;
   i) "sistem i administrimit të rrezikut operacional (*operational risk framework*)" - është tërësia e politikave, procedurave, rregullave dhe strukturave të subjektit, si

dhe mekanizmave të përdorura prej tij, që shërbejnë për administrimin e rrezikut operacional;

j) "marrëveshje me të tretët (*outsourcing*)" - është një marrëveshje e çdo forme ndërmjet subjektit dhe një pale të tretë (ofruesi shërbimi), sipas së cilës pala e tretë (ofruesi i shërbimit) kryen një proces, një shërbim ose një funksion, që në rast të kundërt do të kryhej nga vetë subjekti;

k) "oreksi/toleranca ndaj rrezikut operacional (*operational risk appetite/tolerance*)" - oreksi për rrezik në kontekstin e rrezikut operacional, është i qenësishëm (*inherent*) në aktivitetin e subjektit dhe pranimi i tij nuk sjell përfitime të drejtpërdrejta, por ka vetëm efekt negativ financiar. Toleranca ndaj rrezikut operacional përbën vlerën maksimale të humbjes që pranohet kundrejt këtij rreziku;

l) "baza e të dhënave të ngjarjeve të rrezikut operacional" - është një regjistër, në të cilin grumbullohen, analizohen, mbahen dhe nga ku eksportohen/nxirren ngjarjet e rrezikut operacional. Baza e të dhënave të ngjarjeve të rrezikut operacional përmban informacion mbi ekspozimin ndaj rrezikut operacional, humbjet dhe efektivitetin e funksioneve të kontrollit të subjektit. Ky regjistër përmban të paktën të dhëna mbi datën e ngjarjes, humbjet bruto, shumën e rikuperuar dhe humbjen neto (pas rikuperimit), proceset/produktet e lidhura me humbjen, linjën e biznesit të lidhur me humbjen, llojin e humbjes, faktorët shkakësorë, etj.;

m) "tregues të paralajmërimit të hershëm (*early warning indicators*)" - janë tregues që ndihmojnë në identifikimin e hershëm të çështjeve, të cilat mund të ndikojnë në rritjen e ekspozimit ndaj rrezikut operacional. Treguesit mbulojnë të gjitha aktivitetet e subjektit, sipas prioritetit/rëndësisë dhe mund të jenë tregues performance, tregues rreziku dhe/ose tregues kontrolli. Treguesit shoqërohen me limite monitorimi të përshtatshëm dhe masa të përshkallëzuara, me qëllim zbutjen e rreziqeve dhe shërbejnë si pjesë e infrastrukturës së subjektit në drejtim të përcaktimit të oreksit për rrezik;

n) "hartëzimi dhe vetëvlerësimi i rreziqeve (*risk mapping and self-assessment*)" - është një mekanizëm i përdorur nga subjekti, i cili vlerëson proceset e punës në aktivitetet e tij, të ndarë sipas përgjegjësisë (*owner*) së procesit, kundrejt masës së ekspozimit të tyre ndaj rrezikut dhe llojit të rreziqeve, mjaftueshmërisë dhe llojit të sistemeve të kontrollit të aplikuar për çdo proces, rrezikut të mbetur dhe humbjes financiare të mundshme që buron nga materializimi i rrezikut;

o) "ngjarje kufitare (*boundary event*)" - janë ngjarje që burojnë nga incidente me natyrë rrezikun operacional, por që materializohen në humbje të lidhura me rrezikun e kredisë (*credit risk boundary event*) ose të lidhura me rrezikun e tregut (*market risk boundary event*);

p) "humbje efektive" – janë humbje me efekt ekonomik negativ të lidhura me ngjarje të rrezikut operacional, të cilat në përgjithësi nuk bien në kategoritë e parashikuara në shkronjat "q" deri në "y" të kësaj pike;

q) "provigjione specifike" – janë provigjionet që burojnë nga ngjarje të rrezikut operacional, që kanë një mundësi të lartë të materializimit të humbjes. Këto provigjione lidhen me ngjarje të tipit mashtrim i brendshëm/i jashtëm si pjesë e aktivitetit të kredidhënies; procese gjyqësore në kontekstin e ngjarjeve të tipit praktikat e punësimit dhe siguria në vendin e punës apo klientët, produktet dhe praktikat e biznesit; dëmtime të aktiveve fizike. Ato llogariten si diferencë ndërmjet

humbjes së mundshme dhe sipas rastit, vlerës neto të kolateralit, ose disbursimit të konfirmuar nga siguracioni, nëse këto të fundit ekzistojnë;

r) "humbje të mbetura pezull (*pending losses*)" – janë humbje që burojnë nga ngjarje të rrezikut operacional, me efekt negativ financiar, të regjistruara përkohësisht në llogari tranzitore/pezull dhe që nuk janë reflektuar ende në pasqyrën e të ardhurave dhe shpenzimeve (PASH);

s) "humbje të pamaterializuara (*near misses*)" - lidhen me ngjarje të rrezikut operacional, të cilat nuk shkaktojnë efekte me humbje financiare. Këto janë ngjarje që mund të kishin prodhuar një efekt negativ në pasqyrën e të ardhurave dhe shpenzimeve (PASH), por që nuk rezultuan të tilla për shkak të një kontrolli të momentit të fundit apo për arsye rastësore;

t) "humbjet në kohë (*timing losses*)" - janë humbje që burojnë nga ngjarje të rrezikut operacional, me efekte financiare negative në pasqyrën e flukseve të parasë ose pasqyrën e të ardhurave dhe shpenzimeve (PASH) të periudhave të mëparshme;

u) "kompensim" – janë pagesat ndaj palëve të treta, që kanë pësuar një humbje financiare për shkak të përfitimeve nga subjekti, në kundërshtim me kushtet kontraktuale. Çdo shumë e njohur për kompensim që nuk ndodh gjatë vitit fiskal, duhet të konsiderohet si humbje në kohë (*timing losses*);

v) "humbje të rikuperuara menjëherë (*rapidly recovered losses*)"- lidhen me ngjarje të rrezikut operacional, që shkaktojnë humbje të rikuperuara plotësisht brenda një harku kohor prej pesë ditë pune nga data e ndodhjes së ngjarjes;

x) "fitime/të ardhura operacionale" – lidhen me ngjarje të rrezikut operacional, të cilat mund të kishin prodhuar humbje, por për shkak të materializimit të një rrethane të favorshme, prodhuan fitime/të ardhura;

y) "kosto oportune/të ardhura të munguara" - janë të ardhura të parealizuara, që shkaktohen nga materializimi i ngjarjeve të rrezikut operacional.

3. Termat e përdorur në këtë rregullore "këshill drejtues" dhe "drejtori", të cilët i referohen formës së organizimit juridik të bankave nuk kushtëzojnë ose kufizojnë zbatimin e kërkesave të kësaj rregullore për subjektet e tjera të rregullores. Këto terma në rastin e subjekteve të tjera, të cilat nuk janë të organizuara si banka, do të nënkuptojnë organet përkatëse të subjektit, të cilat ushtrojnë funksionet analoge të "këshillit drejtues" dhe "drejtorisë", në varësi të organizimit juridik të tyre.

KREU II
DREJTIMI I RREZIKUT OPERACIONAL

Neni 5
Sistemi i administrimit të rrezikut operacional

1. Sistemi i administrimit të rrezikut operacional është tërësia e politikave, procedurave, rregullave, strukturave dhe mekanizmave të subjektit, që shërbejnë për administrimin e rrezikut operacional.
2. Subjekti krijon dhe zhvillon sistemin e administrimit të rrezikut operacional, në përputhje me natyrën, vëllimin dhe kompleksitetin e veprimtarisë së tij bankare dhe/ose financiare.

3. Sistemi i administrimit të rrezikut operacional ka për qëllim të sigurojë identifikimin dhe vlerësimin, matjen, kontrollin dhe zbutjen, monitorimin në vazhdimësi, si dhe raportimin periodik te strukturat e brendshme drejtuese, të rrezikut operacional.

Neni 6
Struktura organizative për administrimin e rrezikut operacional

1. Subjekti krijon një strukturë të përshtatshme organizative për administrimin e rrezikut operacional, duke përcaktuar qartë kompetencat dhe përgjegjësitë e organeve drejtuese, si dhe të gjitha strukturave/njësive të përfshira në administrimin e rrezikut operacional, sipas tre linjave të kontrollit.
2. Në veçanti, subjekti siguron që struktura/njësia e administrimit të rrezikut operacional si pjesë e linjës së dytë të mbrojtjes dhe si pjesë e rëndësishme e sistemit të administrimit të rrezikut operacional, të jetë e ndarë qartë nga pikëpamja organizative dhe operacionale prej linjave të biznesit dhe funksioneve të tjera mbështetëse operacionale.
3. Struktura/njësia e administrimit të rrezikut operacional, në varësi të zgjedhjes së strukturave drejtuese të subjektit dhe parimit të proporcionalitetit, mund të jetë pjesë e strukturës së përgjithshme të administrimit të rreziqeve, ose një njësi që mund të qëndrojë jashtë kësaj strukture.
4. Struktura/njësia e parashikuar në pikën 3 të këtij neni, në çdo rast funksionon si linjë e dytë e kontrollit dhe duhet të raportojë drejtpërdrejt te këshilli drejtues, drejtoria apo struktura/komitete të tjera të përcaktuara sipas rastit, për qëllime të administrimit të rrezikut operacional.

Neni 7
Këshilli drejtues

1. Këshilli drejtues, pa rënë ndesh me përcaktimet e përgjegjësive dhe rolit të tij të përcaktuar në kuadrin ligjor e rregullativ, është përgjegjës për:
   a) të krijuar një kulturë të administrimit të rrezikut dhe për të siguruar që subjekti ka procese të përshtatshme, për të kuptuar natyrën e rrezikut operacional që buron nga strategjitë dhe aktivitetet aktuale dhe të planifikuara të subjektit;
   b) të siguruar që proceset e administrimit të rrezikut operacional i nënshtrohen një monitorimi/mbikëqyrjeje gjithëpërfshirëse dhe dinamike dhe janë plotësisht të integruar ose të koordinuar me sistemin e përgjithshëm të administrimit të të gjitha rreziqeve të subjektit;
   c) miratimin e politikave për administrimin e rrezikut operacional dhe monitorimin e zbatimit të tyre;
   d) ngritjen e një strukture administrimi të aftë dhe të përshtatshme për zbatimin e akteve rregullative të brendshme të subjektit për administrimin e rrezikut operacional;
   e) të siguruar që sistemi i administrimit të rrezikut operacional është subjekt i shqyrtimit/kontrollit të pavarur nga ana e njësisë së kontrollit të brendshëm. Për këtë, këshilli drejtues përcakton linja/ndarje të qarta të detyrave dhe përgjegjësive që ndihmojnë në ngritjen e funksioneve të përshtatshme të kontrollit të brendshëm

të rrezikut operacional. Kontrollet duhet të rishikohen, monitorohen dhe testohen rregullisht, për të siguruar efektivitet të vazhdueshëm. Mjedisi i kontrollit duhet të sigurojë pavarësinë dhe ndarjen e duhur të detyrave ndërmjet funksioneve të administrimit të rrezikut operacional, njësive të biznesit dhe funksioneve mbështetëse;

f) rishikimin dhe vlerësimin në mënyrë periodike të efektivitetit të sistemit të administrimit të rrezikut operacional dhe miratimin e tij, për të siguruar identifikimin dhe administrimin nga subjektet, të rrezikut operacional që rrjedh nga ndryshimet e jashtme të tregut dhe faktorë të tjerë të mjedisit, si dhe të rreziqeve operacionale që lidhen me produktet, veprimtaritë, proceset ose sistemet e reja, përfshirë ndryshimet në profilin e rrezikut dhe në prioritetet e subjektit. Procesi i rishikimit duhet të synojë vlerësimin dhe përzgjedhjen e praktikave më të mira të administrimit të rrezikut operacional, të përshtatshme për veprimtaritë, sistemet dhe proceset e subjektit;

g) miratimin dhe rishikimin në mënyrë periodike të deklaratës së oreksit/tolerancës ndaj rrezikut operacional, në përputhje me strategjinë e subjektit, rezultatet financiare, si dhe llojet dhe nivelet e rrezikut që subjekti është i gatshëm të pranojë.

2. Këshilli drejtues siguron që sistemi i administrimit të rrezikut operacional i nënshtrohet një procesi efektiv dhe gjithëpërfshirës të kontrollit të brendshëm nga një personel i pavarur, i kualifikuar dhe i përgjegjshëm.

Neni 8
Drejtoria

1. Drejtoria, në funksion të administrimit të rrezikut operacional, është përgjegjëse për zbatimin e politikave, proceseve dhe sistemeve për administrimin e rrezikut operacional në të gjitha shërbimet/produktet, veprimtaritë, proceset dhe sistemet me rëndësi për subjektin, në përputhje me deklaratën e oreksit/tolerancës ndaj rrezikut.
2. Drejtoria, në funksion të administrimit të rrezikut operacional është përgjegjëse për:
   a) zbatimin e akteve të brendshme rregullative për administrimin e rrezikut operacional të subjektit, të miratuara nga këshilli drejtues;
   b) përcaktimin e përgjegjësive dhe zhvillimin e linjave të raportimit për të inkurajuar dhe për të ruajtur llogaridhënien, si dhe për të siguruar burimet financiare dhe njerëzore të duhura për administrimin efektiv të rrezikut operacional, në përputhje me deklaratën e oreksit/tolerancës ndaj rrezikut;
   c) komunikimin në mënyrë të qartë te punonjësit e të gjitha niveleve mbi sistemin e administrimit të rrezikut operacional të aplikuar nga subjekti;
   d) ushtrimin e veprimtarisë bankare dhe/ose financiare të subjektit nga personel i kualifikuar, me përvojë dhe aftësi teknike të nevojshme;
   e) sigurimin që personeli përgjegjës për monitorimin e zbatimit të sistemit të administrimit të rrezikut operacional dhe përputhshmërisë së tij me politikën e rrezikut të subjektit, të jetë i pavarur nga njësitë që mbikëqyr.

Neni 9
Linjat e mbrojtjes

1. Subjekti administron rrezikun operacional, duke zbatuar modelin e tre linjave të mbrojtjes, ku:
   a) në linjën e parë përfshihen njësitë e biznesit dhe funksionet ndihmëse/operacionale;
   b) në linjën e dytë përfshihet funksioni i pavarur përgjegjës për administrimin e rrezikut operacional dhe funksioni/njësia e përputhshmërisë; dhe
   c) në linjën e tretë përfshihet funksioni i pavarur i kontrollit.
2. Subjekti zbaton modelin e tre linjave të mbrojtjes në varësi të natyrës, madhësisë, kompleksitetit dhe të profilit të rrezikut të tij.
3. Subjekti sigurohet që secila nga linjat e mbrojtjes:
   a) ka burime financiare dhe njerëzore dhe mjete të mjaftueshme;
   b) ka detyra dhe përgjegjësi të përcaktuara qartë;
   c) trajnohet në mënyrë të vazhdueshme dhe të mjaftueshme;
   d) promovon një kulturë të shëndoshë të administrimit të rrezikut në gjithë organizatën (subjektin);
   e) komunikon me linjat e tjera të mbrojtjes, për zbatimin e sistemit të administrimit të rrezikut operacional.
4. Në rastet kur në një njësi biznesi përfshihen funksione të linjës së parë dhe të dytë të mbrojtjes, subjekti dokumenton dhe dallon përgjegjësitë e këtyre funksioneve sipas linjave të mbrojtjes, duke theksuar pavarësinë e linjës së dytë të mbrojtjes nga njësitë e biznesit.
5. Për qëllime të administrimit të rrezikut operacional, në linjën e parë të mbrojtjes përfshihet administrimi i njësive të biznesit dhe funksioneve ndihmëse/operacionale të subjektit. Punonjësit e linjës së parë të mbrojtjes janë përgjegjës për identifikimin dhe administrimin e vazhdueshëm të rreziqeve të qenësishme (*inherent*) në produktet, aktivitetet, proceset dhe sistemet, për të cilat janë përgjegjës gjatë punës së përditshme.
6. Për qëllime të pikës 5 të këtij neni, përgjegjësitë e linjës së parë të mbrojtjes përfshijnë:
   a) identifikimin dhe vlerësimin e materialitetit të rreziqeve operacionale të qenësishme (*inherent*) në njësitë e tyre të biznesit, nëpërmjet përdorimit të sistemeve të kontrollit, manuale apo automatike, në përputhje me procedurat e brendshme dhe parimin e ndarjes së detyrave;
   b) vendosjen e sistemeve të përshtatshme të kontrollit, në bashkëpunim me strukturat e tjera të kontrollit dhe funksionin e administrimit të rrezikut operacional, për të zbutur rrezikun operacional të qenësishëm (*inherent*), si edhe vlerësimin dhe raportimin e efektivitetit të këtyre kontrolleve nëpërmjet përdorimit të mekanizmave të administrimit të rrezikut operacional;
   c) identifikimin, monitorimin dhe raportimin e ngjarjeve të rrezikut operacional, në përputhje me sistemin e administrimit të rrezikut operacional;
   d) raportimin e rreziqeve operacionale të mbetura (*residual*), të cilat nuk janë zbutur nga kontrollet, mangësitë e kontrollit dhe pamjaftueshmëritë e proceseve;
   e) trajnimin e duhur për të siguruar identifikimin dhe vlerësimin e rreziqeve operacionale, si dhe raportimin në rastet kur njësitë e biznesit kanë mungesa në burime, mekanizma apo trajnime që mundësojnë identifikimin dhe vlerësimin e rreziqeve operacionale.

7. Për qëllime të administrimit të rrezikut operacional, në linjën e dytë të mbrojtjes përfshihen funksionet e pavarura nga njësitë e biznesit për administrimin e rrezikut operacional, si pjesë e sistemit të administrimit të rrezikut. Kjo linjë është përgjegjëse për monitorimin e vazhdueshëm dhe periodik dhe zhvillimin e sistemit të administrimit të rrezikut operacional dhe raportimin e çështjeve të lidhura me këtë rrezik, te drejtoria dhe këshilli drejtues.
8. Për qëllime të pikës 7 të këtij neni, përgjegjësitë e linjës së dytë të mbrojtjes përfshijnë minimalisht:
   a) zhvillimin e një opinioni të pavarur nga njësitë e tjera të biznesit mbi:
      i. ngjarjet materiale të rrezikut operacional të identifikuara,
      ii. hartimin/përcaktimin dhe efektivitetin e kontrolleve kyçe, dhe
      iii. tolerancën ndaj rrezikut operacional;
   b) sigurimin dhe dokumentimin e zbatimit të drejtë nga linja e parë e kontrollit të përgjegjësive, mekanizmave dhe sistemeve të raportimit të administrimit të rrezikut operacional;
   c) zhvillimin dhe mirëmbajtjen e politikave, standardeve, metodologjive dhe udhëzimeve për administrimin dhe matjen e rrezikut operacional;
   d) rishikimin dhe kontributin në monitorimin dhe raportimin e profilit të rrezikut operacional;
   e) hartimin dhe zhvillimin e trajnimeve të punonjësve për çështje të rrezikut operacional si dhe nxitjen e ndërgjegjësimit ndaj rreziqeve/promovimin e kulturës së rreziqeve.
9. Për qëllime të administrimit të rrezikut operacional, në linjën e tretë të mbrojtjes përfshihet njësia e kontrollit të brendshëm. Kjo linjë siguron këshillin drejtues për përshtatshmërinë e sistemit të administrimit të rrezikut operacional, duke rishikuar në mënyrë të pavarur dhe duke i raportuar këshillit drejtues mbi bazën e një periodiciteti të caktuar të mbështetur mbi një qasje të bazuar në rrezik. Punonjësit e njësisë së kontrollit të brendshëm nuk duhet të përfshihen në zhvillimin, zbatimin dhe funksionimin e proceseve të administrimit të rrezikut operacional nga dy linjat e tjera të mbrojtjes.

   Kjo strukturë vlerëson në mënyrë të pavarur efektivitetin e proceseve të krijuara në linjën e parë dhe të dytë të kontrollit, si dhe siguron mbarëvajtjen e këtyre proceseve.
10. Për qëllime të pikës 9 të këtij neni, përgjegjësitë e linjës së tretë të mbrojtjes përfshijnë:
    a) rishikimin e hartimit dhe zbatimit të sistemit të administrimit të rrezikut operacional, si dhe proceset shoqëruese të drejtimit/qeverisjes nga linja e parë dhe e dytë e mbrojtjes (përfshirë edhe pavarësinë e linjës së dytë të mbrojtjes);
    b) rishikimin e proceseve të vlerësimit për t'u siguruar që ato janë të pavarura dhe të zbatuara në përputhje me kuadrin rregullativ të subjektit;
    c) sigurimin që modelet/mekanizmat e matjeve të përdorura nga subjekti janë mjaftueshëm të fortë/të qëndrueshëm, për të siguruar integritet të lartë për të dhënat hyrëse, supozimet, proceset dhe metodologjitë e përdorura, si dhe për të rezultuar në vlerësime të rrezikut operacional, të cilat pasqyrojnë në mënyrë të besueshme profilin e rrezikut operacional të subjektit;
    d) sigurimin që drejtuesit e njësive të biznesit përgjigjen në mënyrë të shpejtë, të saktë dhe adekuate për çështjet e ngritura, si dhe raportimin rregullisht në këshillin

drejtues ose në komitetet në varësi të tij, mbi çështjet e rrezikut operacional të mbetura pezull ose të zgjidhura;

e) vlerësimin në tërësi të mjaftueshmërisë dhe përshtatshmërisë së sistemit të administrimit të rrezikut operacional dhe proceseve shoqëruese të qeverisjes/drejtimit të subjektit. Përtej kontrollit të përputhshmërisë me politikat dhe procedurat në fuqi, linja e tretë e kontrollit vlerëson në mënyrë të pavarur nëse sistemi i administrimit të rrezikut operacional plotëson nevojat dhe objektivat e subjektit, si dhe nëse është në përputhje me dispozitat ligjore dhe statutore, marrëveshjet kontraktore, rregullat e brendshëm të subjektit dhe kodin e etikës.

Neni 10
Politika për administrimin e rrezikut operacional

1. Subjekti harton një politikë për administrimin e rrezikut operacional, e cila komunikohet në mënyrë efektive në tërë subjektin dhe në veçanti te strukturat e linjës së parë dhe të dytë të kontrollit të përfshira në administrimin e rrezikut operacional.
2. Politika për administrimin e rrezikut operacional rishikohet në baza të rregullta, të paktën një herë në vit dhe miratohet nga këshilli drejtues.
3. Politika për administrimin e rrezikut operacional përfshin të paktën elementet e mëposhtme:
   a) qëllimin e politikës për administrimin e rrezikut operacional;
   b) kuadrin ligjor dhe rregullativ për rrezikun operacional dhe përputhshmërinë me këtë kuadër;
   c) përkufizimin e termave të përdorur nga subjekti në politikën për administrimin e rrezikut operacional;
   d) objektivat në lidhje me identifikimin, vlerësimin, kontrollin dhe zbutjen e rrezikut operacional të subjektit;
   e) elementët e sistemit të administrimit të rrezikut operacional që përfshijnë:
      i. qeverisjen,
      ii. kulturën e rrezikut dhe ndërgjegjësimin,
      iii. raportimin/mbledhjen e ngjarjeve të rrezikut operacional,
      iv. hartëzimin dhe vetëvlerësimin e rreziqeve dhe kontrolleve në fuqi,
      v. analizën e skenarëve,
      vi. treguesit e paralajmërimit të hershëm,
      vii. matjen dhe modelimin,
      viii. raportimin,
      ix. oreksin dhe tolerancën ndaj rrezikut;
   f) kuadrin rregullativ mbështetës në zbatimin e politikës, të përbërë nga procedura, udhëzime dhe manuale të subjektit.

Neni 11
Identifikimi dhe vlerësimi i rrezikut operacional

1. Subjekti identifikon dhe vlerëson rrezikun operacional në të gjitha shërbimet/produktet, veprimtaritë, proceset dhe sistemet me rëndësi.

2. Subjekti, përpara hedhjes në treg të shërbimeve/produkteve të reja, kryerjes së veprimtarive apo proceseve të ndryshme, dhe/ose krijimit të sistemeve të reja, përpara dhe gjatë marrjes së shërbimeve/funksioneve nga palë të treta, të cilat mbartin potencialisht rrezik për subjektin, siguron zbatimin e procedurave të mjaftueshme dhe të përshtatshme për vlerësimin paraprak të rrezikut operacional që mund të lidhet me to.
3. Subjekti identifikon dhe vlerëson në mënyrë efektive rrezikun operacional, duke konsideruar mjediset e biznesit dhe kontrollet në fuqi.
4. Subjekti vlerëson impaktin e ngjarjeve të rrezikut operacional, duke iu referuar deklaratës së oreksit/tolerancës ndaj rrezikut operacional, e cila miratohet dhe rishikohet çdo vit nga këshilli drejtues.

Neni 12
Matja e rrezikut operacional

1. Subjekti mat ekspozimin ndaj rrezikut operacional, nëpërmjet informacionit të mbledhur dhe të dhënave që burojnë nga zbatimi i mekanizmave të administrimit të rrezikut operacional, të tilla si:
   a) të dhëna historike të bazës së të dhënave të ngjarjeve të rrezikut operacional të subjektit;
   b) të dhëna të jashtme të marra nga burime të hapura apo nga baza të dhënash të industrisë;
   c) rezultatet e vetëvlerësimit të rreziqeve të subjektit;
   d) rezultatet e analizës së skenarëve;
   e) treguesit e paralajmërimit të hershëm.
2. Për sa parashikohet në pikën 1 të këtij neni, subjekti duhet të sigurohet për plotësinë dhe saktësinë e të dhënave hyrëse, kushtet e përpunimit të informacionit, si dhe vlerësimin periodik të rezultateve.
3. Me matjen e rrezikut operacional, subjekti përcakton profilin e tij të rrezikut, me qëllim përdorimin efikas të burimeve njerëzore dhe teknike për administrimin e këtyre rreziqeve.
4. Matja e rrezikut operacional në terma të kërkesave për kapital, trajtohet sipas përcaktimeve të rregulloreve respektive në fuqi të Bankës së Shqipërisë.

Neni 13
Monitorimi i rrezikut operacional

1. Subjekti zhvillon një proces monitorimi periodik të profilit të rrezikut operacional dhe ekspozimeve kryesore ndaj këtij rreziku.
2. Subjekti përfshin në procesin e monitorimit periodik, edhe shërbimet e ofruara nga palë të treta (*outsourcing*), të cilat mbartin rrezik për subjektin, duke monitoruar cilësinë e shërbimeve të ofruara prej tyre dhe përmbushjen e detyrimeve kontraktuale.
3. Subjekti, në realizimin e procesit të monitorimit efektiv dhe të vazhdueshëm të rrezikut operacional:
   a) përcakton tregues të përshtatshëm që sigurojnë paralajmërim të hershëm të rritjes së rrezikut operacional, i cili mund të sjellë humbje në të ardhmen;

b) vendos kufij për këta tregues, kur është e mundur, me qëllim krijimin e një procesi efektiv monitorimi, që mund të ndihmojë për të identifikuar rreziqet kryesore dhe me rëndësi për subjektin dhe për t'i mundësuar këtij të fundit monitorimin në kohë dhe parandalimin e materializimit të këtyre rreziqeve;
c) përcakton periodicitetin e procesit të monitorimit, duke marrë në konsideratë shkallën e rrezikut dhe natyrën e ndryshimeve në mjedisin në të cilin operon;
d) siguron përfshirjen e rezultateve të monitorimit në raportet e rregullta për këshillin drejtues, drejtorinë si dhe përfaqësuesit e linjave të biznesit, të cilët ndikohen nga problematikat e ngritura në raport.

Neni 14
Kontrolli dhe zbutja e rrezikut operacional

1. Subjekti duhet të ketë një mjedis të përshtatshëm kontrolli, të përbërë nga një kuadër i brendshëm rregullativ i plotë dhe i përshtatshëm, procese dhe sisteme të forta dhe gjithëpërfshirëse, kontrolle të brendshme të duhura, si dhe strategji për zbutjen dhe/ose transferimin e rrezikut.
2. Subjekti në funksion të kontrollit dhe zbutjes së rrezikut operacional:
   a) harton sisteme procedurash dhe procesesh kontrolli, për të siguruar zbatimin e politikave të brendshme për administrimin e rrezikut operacional;
   b) siguron, që praktikat/proceset e brendshme të jenë të përshtatshme për kontrollin e rrezikut operacional dhe të përfshijnë të paktën:
      i. përcaktimin e qartë të autoriteteve/proceseve për miratim dhe ndarjen e detyrave,
      ii. monitorimin nga afër të respektimit të kufijve të caktuar ose kufijve të rrezikut,
      iii. marrjen e masave mbrojtëse për përdorimin e të dhënave dhe të aktiveve të subjektit, përfshirë përdorimin e kontratave të sigurimit, duke e transferuar rrezikun jashtë subjektit,
      iv. sigurimin se personeli është i kualifikuar dhe ka ekspertizën e duhur,
      v. identifikimin e linjave të biznesit ose të produkteve, ku fitimet duket të jenë jashtë pritshmërive të arsyeshme,
      vi. heqjen dorë nga linjat e biznesit, aktivitetet dhe produktet me potencial të lartë ekspozimi dhe humbjeje për shkak të rrezikut operacional, që shoqërohen me një probabilitet të lartë ndodhjeje;
   c) përdor mjete ose programe për uljen e ekspozimit ndaj ngjarjeve me probabilitet të ulët, por që mund të shkaktojnë ndikim të madh në rezultatin financiar të tij;
   d) i kushton vëmendje të veçantë veprimtarive dhe/ose krijimit të produkteve të reja, sidomos kur këto të fundit nuk janë në përputhje me planin e biznesit të subjektit;
   e) i kushton vëmendje të veçantë hyrjes në tregje të panjohura dhe/ose ndërmarrjes së veprimtarive tregtare gjeografikisht larg zyrës qendrore të subjektit;
   f) tregon kujdesin e duhur në lidhje me rritjen e shkallës së automatizimit të shërbimeve, e cila duhet të bashkërendohet me forcimin e sigurisë në drejtim të informacionit dhe teknologjisë;
   g) krijon politika dhe praktika për administrimin e rrezikut operacional që rrjedh nga transferimi i proceseve, shërbimeve ose funksioneve të subjektit te palë të treta nëpërmjet kontraktimit (*outsourcing*).

3. Subjekti siguron reagim dhe administrim të përshtatshëm ndaj ngjarjeve të rrezikut operacional, duke u bazuar edhe në kuadrin e tolerancës ndaj rrezikut. Administrimi i ngjarjeve të rrezikut operacional duhet të bjerë në një nga kategoritë e mëposhtme:
   a) pranimi i ndikimit të ngjarjes, për ngjarje me rrezik dhe ndikim të papërfillshëm, të materializuara në frekuencë të ulët dhe ndikim/humbje të vogël (humbje të pritshme);
   b) zbutja e ndikimit të ngjarjes me sisteme kontrolli dhe parandaluese, për ngjarje me rrezik të pranueshëm, të materializuar në frekuencë të lartë dhe ndikim/humbje të vogël (humbje të pritshme);
   c) zbutja e ndikimit të ngjarjes nëpërmjet transferimit/përdorimit të kontratave të sigurimit, për ngjarje me rrezik të lartë, të materializuar në frekuencë të ulët por ndikim/humbje të madhe;
   d) heqja dorë nga aktivitete të caktuara, të cilat gjenerojnë ngjarje me rrezik të lartë, të materializuara në frekuencë të lartë dhe ndikim/humbje të madhe.

Neni 15
Raportimi i rrezikut operacional

1. Funksioni i pavarur i administrimit të rrezikut operacional siguron raportime periodike dhe joperiodike (*ad-hoc*), sipas nevojave, për drejtorinë/komitetin e administrimit të rrezikut, këshillin drejtues si dhe përfaqësuesit e linjave të biznesit, të cilat ndikohen nga problematikat e ngritura në raport.
2. Raportet e rrezikut operacional zakonisht përmbajnë informacion mbi:
   a) ngjarjet e rrezikut operacional të subjektit;
   b) ngjarjet e jashtme/të tregut të rëndësishme;
   c) ndjekjen e vendimeve të marra;
   d) rezultatet e vetëvlerësimit të rreziqeve;
   e) rezultatet e treguesve të paralajmërimit të hershëm;
   f) kapitalin për mbulimin e rrezikut operacional;
   g) çështje të cilat kërkojnë vendimmarrje ose përshkallëzim;
   h) profilin e rrezikut operacional të subjektit.
3. Subjekti, për qëllime të kësaj rregulloreje, përveç raportimeve të brendshme, raporton çdo tremujor në Bankën e Shqipërisë, të dhënat e treguesve të paralajmërimit të hershëm sipas aneksit nr. 1 dhe ngjarjet e rrezikut operacional sipas aneksit nr. 3 të kësaj rregulloreje, me informacionet e regjistruara gjatë periudhës raportuese.
4. Gjithashtu, subjekti raporton në Bankën e Shqipërisë, në mënyrë joperiodike dhe jashtë raportimeve normale (*ad hoc*), ngjarjet e rrezikut operacional të vlerësuara nga vetë subjekti si kritike [1], sipas matricës së brendshme të tolerancës ndaj rreziqeve, pavarësisht materializimit të efektit financiar, dhe në çdo rast ato ngjarje të rrezikut operacional, humbja bruto e të cilave tejkalon vlerën prej 2% të kapitalit rregullator të subjektit, përfshirë shkakun e humbjes dhe masat korrigjuese për mos përsëritjen e tyre.
5. Klasifikimi i ngjarjes si ngjarje kritike kryhet brenda një kohe të arsyeshme, pasi është zbuluar, por jo më vonë se 24 orë. Nëse nevojitet një kohë më e gjatë për të klasifikuar

[1] Vlerësimi i kritikalitetit të ngjarjeve të rrezikut operacional bëhet sipas matricës së frekuencës dhe impaktit nga ushtrimi i hartëzimit dhe vetëvlerësimit të rreziqeve dhe kontrolleve në fuqi, referuar nenit 22 të kësaj rregulloreje.

ngjarjen, subjekti shpjegon arsyet në raportimin fillestar në Bankën e Shqipërisë. Raportimi i ngjarjes kritike në Bankën e Shqipërisë realizohet në tre faza, si më poshtë:

a) **raportimi fillestar**, realizohet brenda një afati prej 4 orësh nga momenti i klasifikimit të ngjarjes si kritike. Në këtë raportim subjekti përfshin një informacion të përgjithshëm dhe paraqet karakteristikat kryesore të ngjarjes dhe pasojave të pritshme të saj, bazuar në informacionin e disponueshëm;
b) **raportimi i ndërmjetëm**, realizohet në çdo rast brenda 3 ditë pune nga data e paraqitjes së raportit fillestar dhe përmban një përshkrim më të detajuar të ngjarjes dhe pasojave të saj. Subjekti paraqet pranë Bankës së Shqipërisë, raportin e ndërmjetëm kur veprimtaria e tij e rregullt (e zakonshme) është rikuperuar dhe biznesi është kthyer në normalitet, duke njoftuar Bankën e Shqipërisë për këtë rrethanë, gjithashtu edhe në rastin kur veprimtaria e rregullt (e zakonshme) nuk është rikuperuar;
c) **raportimi përfundimtar**, realizohet brenda një afati prej 20 ditësh pune, pasi biznesi të konsiderohet si i rikthyer në normalitet. Subjekti përfshin në raportin përfundimtar informacion të plotë mbi të dhënat/shifrat reale mbi ndikimin e ngjarjes, në vend të vlerësimeve të tij, si dhe informacion mbi shkakun bazë, nëse dihet, dhe një përmbledhje të masave të zbatuara ose të planifikuara të zbatohen, për të mënjanuar problemin dhe për të parandaluar ndodhjen (përsëritjen) e tij në të ardhmen.

6. Në rastin kur veprimtaria e rregullt e subjektit është rikuperuar përpara se të kenë kaluar 4 orë nga klasifikimi i ngjarjes si kritike dhe subjekti është në gjendje të sigurojë të gjithë informacionin e kërkuar në raportin përfundimtar brenda këtij intervali kohor, subjekti mund të realizojë një raportim të vetëm në Bankën e Shqipërisë, i cili përmban njëkohësisht informacionin lidhur me raportimin fillestar, të ndërmjetëm dhe përfundimtar.
7. Pa rënë ndesh me kërkesat e kësaj rregulloreje, për ngjarjet (incidentet) e vlerësuara si kritike (madhore), që lidhen me shërbimet e pagesave, subjekti zbaton kërkesat e kuadrit rregullativ në fuqi për raportimin e incidenteve madhore.

Neni 16
Plani i vazhdimësisë së veprimtarisë

1. Subjekti harton plane të vazhdimësisë së veprimtarisë, të cilat kanë për qëllim të sigurojnë ushtrimin në mënyrë të pandërprerë të veprimtarisë dhe kufizimin e humbjeve të lidhura me rrezikun operacional.
2. Subjekti siguron që planet për vazhdimësinë e veprimtarisë të jenë pjesë përbërëse e sistemit të administrimit të rrezikut operacional dhe/ose të rreziqeve të tjera.
3. Subjekti, për hartimin dhe miratimin e këtyre planeve, përcakton:
   a) veprimtaritë kryesore;
   b) skenarë/ngjarje, të cilat mund të shkaktojnë ndërprerjen e proceseve dhe/ose veprimtarive kryesore;
   c) zgjidhje alternative për të ruajtur vazhdimësinë e ushtrimit të veprimtarive kryesore;

d) veprimet dhe radhën e tyre për të rivendosur funksionimin e rregullt të veprimtarive, veçanërisht për të siguruar informacionin e sistemeve elektronike dhe kthimin e këtyre sistemeve në gjendje funksionale;
e) strategjitë e komunikimit në rastet e problemeve serioze dhe/ose ndërprerjeve të veprimtarisë.

4. Subjekti shqyrton dhe rishikon periodikisht planet për sigurimin e vazhdimësisë së veprimtarisë, në mënyrë që ato të jenë në përputhje me veprimtarinë aktuale, rreziqet dhe strategjinë e tij të biznesit.
5. Subjekti, për kërkesa të detajuara të planit të vazhdimësisë së veprimtarisë i referohet rregulloreve përkatëse në fuqi të Bankës së Shqipërisë.

Neni 17
***Stress test*-et**

1. Në përputhje me përcaktimet e kuadrit rregullativ në fuqi për *stress test*-et për bankat, në procesin e hartimit dhe kryerjes së *stress test*-eve për rrezikun operacional, banka harton dhe zhvillon një program për *stress test*-et e rrezikut operacional, si pjesë integrale e programit të *stress test*-eve për rreziqet kryesore.
2. Banka përcakton qartë rolet e strukturave në hartimin dhe zbatimin e *stress test*-eve për rrezikun operacional, raportimin efektiv dhe në kohë të rezultateve të tij, dokumentimin e procesit dhe marrjen e masave korrigjuese sipas rastit.

Neni 18
Mekanizmat për administrimin e rrezikut operacional

1. Subjekti, për administrimin e rrezikut operacional bazohet në mekanizmat kryesorë të mëposhtëm, të cilët konsiderohen si shtylla e administrimit të këtij rreziku:
   a) identifikimi dhe raportimi i ngjarjeve të rrezikut operacional;
   b) baza e të dhënave të ngjarjeve të rrezikut operacional;
   c) treguesit e paralajmërimit të hershëm;
   d) hartëzimi dhe vetëvlerësimi i rreziqeve dhe kontrolleve në fuqi; dhe
   e) analiza e skenarëve.
2. Subjekti, në përputhje me madhësinë dhe kompleksitetin e tij, përdor sisteme informacioni të përshtatshme dhe të mjaftueshme për mbarëvajtjen dhe mirëfunksionimin e proceseve të parashikuara në pikën 1 të këtij neni.

Neni 19
Identifikimi dhe raportimi i ngjarjeve të rrezikut operacional

1. Subjekti harton një kuadër të brendshëm rregullativ apo procedurë për administrimin e ngjarjeve të rrezikut operacional, ku përcaktohen të gjitha hapat në ciklin e administrimit të tyre, afatet, si dhe rolet e strukturave të përfshira në këtë proces.
2. Ngjarjet e rrezikut operacional, pasi identifikohen, përpunohen dhe raportohen sipas rastit nga struktura e subjektit që e identifikon dhe në përputhje me kërkesat minimale të përcaktuara sipas formularit të standardizuar në aneksin nr. 16 të kësaj rregullore.

Në varësi të madhësisë dhe kompleksitetit të subjektit dhe infrastrukturës teknologjike, të dhënat regjistrohen direkt në bazën e të dhënave të ngjarjeve të rrezikut operacional të subjektit, ose regjistrohen nga njësia e administrimit të rrezikut operacional.

3. Raportimi i ngjarjeve të rrezikut operacional, në varësi të organizimit të procesit, kryhet nga çdo punonjës i subjektit i cili e ka identifikuar ngjarjen, ose nëpërmjet një punonjësi përgjegjës për rrezikun operacional, i përcaktuar për çdo strukturë të subjektit.

Neni 20
Baza e të dhënave të ngjarjeve të rrezikut operacional

1. Subjekti harton një kuadër të brendshëm rregullativ/metodologji për administrimin e bazës së të dhënave të ngjarjeve të rrezikut operacional, ku përcaktohet qëllimi, hapat, afatet dhe rolet e strukturave të përfshira në këtë proces.
2. Subjekti zbaton mekanizma të përshtatshëm që sigurojnë përdorimin e një baze të dhënash cilësore për ngjarjet e rrezikut operacional, të mbështetur në sisteme informatike.
3. Baza e të dhënave të ngjarjeve të rrezikut operacional të subjektit plotëson kërkesat e mëposhtme:
   a) të dhënat e ngjarjeve të rrezikut operacional duhet të jenë gjithëpërfshirëse, në mënyrë që të përfshijnë të gjitha veprimtaritë e subjektit;
   b) për mbledhjen e të dhënave që lidhen me ngjarjet e rrezikut operacional, subjekti përcakton kufij sasiorë minimalë të përshtatshëm;
   c) baza e të dhënave të ngjarjeve të rrezikut operacional të subjektit duhet të përmbajë të paktën:
      i. numrin e identifikimit të ngjarjes,
      ii. përshkrimin e ngjarjes,
      iii. njësinë raportuese të ngjarjes,
      iv. datën e ndodhjes së ngjarjes (d.m.v),
      v. datën e identifikimit të ngjarjes (d.m.v),
      vi. datën e raportimit të ngjarjes (d.m.v),
      vii. datën e kontabilizimit të ngjarjes (d.m.v),
      viii. vlerën e humbjes bruto/fillestare (në lekë),
      ix. vlerën e rikuperuar dhe datën e rikuperimit,
      x. klasifikimin e çdo ngjarjeje sipas llojit të ngjarjes, linjës së biznesit, efektit financiar, shkakut dhe informacion mbi ngjarjet kufitare (*boundary events*);
   d) subjekti duhet të jetë në gjendje të identifikojë humbjet e rrezikut operacional që shkaktohen nga ngjarjet e lidhura me rrezikun e kredisë dhe atë të tregut (*boundary events*) dhe t'i regjistrojë në bazën e të dhënave të ngjarjeve të rrezikut operacional, të shoqëruara me shënimet përkatëse[2];
   e) subjekti duhet të jetë në gjendje të kategorizojë ngjarjet e rrezikut operacional, të paktën sipas efekteve financiare të mëposhtme:
      i. humbje financiare efektive,
      ii. provigjione specifike për rrezikun operacional,
      iii. humbje të mbetura pezull (*pending losses*),
      iv. humbje të pamaterializuara (*near misses*),

[2] Shembuj të ngjarjeve kufitare (*boundary events*) paraqiten në aneksin nr. 17 të rregullores.

v. humbje në kohë (*timing losses*),
vi. kompensim,
vii. humbje të rikuperuara menjëherë (*rapidly recovered loss*),
viii. fitime/të ardhura operacionale,
ix. kosto oportune/të ardhura të munguara;

f) subjekti duhet të jetë në gjendje të kategorizojë çdo ngjarje sipas shkakut/faktorit që e shkakton. Kategorizimi sipas shkakut, i ndarë në 2 nivele detajimi, paraqitet në aneksin nr. 5 të kësaj rregulloreje;
g) subjekti duhet të jetë në gjendje të hartëzojë/kategorizojë (*mapping*) çdo ngjarje sipas llojit dhe linjës së biznesit, sipas anekseve nr. 6-14 të kësaj rregullore. Kategorizimi i ngjarjeve kryhet duke përdorur kritere objektive dhe të dokumentuara.

Neni 21
Treguesit e paralajmërimit të hershëm

1. Subjekti harton një kuadër të brendshëm rregullativ/metodologji/procedurë për hartimin dhe administrimin e treguesve të paralajmërimit të hershëm, ku përcaktohet qëllimi, hapat, afatet dhe rolet e strukturave të përfshira në këtë proces.
2. Subjekti përdor tregues të paralajmërimit të hershëm, të cilët shërbejnë për identifikimin e hershëm të çështjeve që mund të ndikojnë në rritjen e ekspozimit ndaj rrezikut operacional.
3. Treguesit e paralajmërimit të hershëm mbulojnë të gjitha aktivitetet e subjektit, sipas prioritetit/rëndësisë dhe mund të jenë tregues performance, tregues rreziku dhe/ose tregues kontrolli.
4. Treguesit e paralajmërimit të hershëm në përgjithësi duhet të jenë të matshëm, të krahasueshëm në kohë dhe transparentë.
5. Në varësi të kompleksitetit dhe madhësisë, subjekti harton treguesit e tij të brendshëm, të cilët përfshijnë edhe treguesit e aneksit nr.1 të kësaj rregullore, ose përdor vetëm treguesit e përcaktuar në atë aneks.
6. Treguesit e paralajmërimit të hershëm identifikohen dhe rishikohen në mënyrë të vazhdueshme. Në identifikimin e treguesve të përshtatshëm shërben edhe procesi i vetëvlerësimit të rreziqeve, ku identifikohen rreziqe për të cilat duhen vendosur tregues të monitorimit të tyre.
7. Çdo tregues i paralajmërimit të hershëm shoqërohet të paktën me të dhënat e mëposhtme:
   a) emrin e treguesit;
   b) përshkrimin e treguesit;
   c) objektivin e treguesit dhe rrezikun që monitoron;
   d) mënyrën e përllogaritjes;
   e) strukturën përgjegjëse (*owner*) dhe veprimtarinë ku bie treguesi;
   f) frekuencën e raportimit;
   g) limitin e monitorimit (i kuq, portokalli, i gjelbër ose i lartë, i mesëm, i ulët).
8. Thyerja e limiteve shoqërohet me monitorim dhe masa të mëtejshme, të cilat kanë si qëllim zbutjen e rreziqeve.

Neni 22
Hartëzimi dhe vetëvlerësimi i rreziqeve dhe kontrolleve në fuqi

1. Subjekti zhvillon një metodologji të përshtatshme për hartëzimin e rreziqeve për proceset/nënproceset e punës/aktivitetet, për të gjitha linjat e biznesit dhe funksionet operacionale dhe mbështetëse të tyre, ku përcaktohen qartë hapat, rolet dhe përgjegjësitë e strukturave të përfshira në këtë proces, me qëllim monitorimin e proceseve dhe funksioneve me rreziqe të qenësishme (*inherent*), parandalimin e materializimit të tyre dhe vlerësimin e mjaftueshmërisë së eficiencës të kontrolleve në fuqi.
2. Hartëzimi dhe vetëvlerësimi i rreziqeve kryhet të paktën një herë në vit. Ky proces mban në konsideratë të gjitha ndryshimet materiale në strukturën organizative, aktivitetet, sistemet dhe kuadrin rregullativ që kanë ndodhur përgjatë periudhës së rishikimit, duke konfirmuar vlefshmërinë e vlerësimeve të një periudhe më parë, të pandikuara nga ndryshimet dhe duke siguruar përfshirjen e vlerësimeve të reja të ndikuara nga këto ndryshime.
3. Hartëzimi dhe vetëvlerësimi i rreziqeve dhe kontrolleve në fuqi materializohet në katër hapa si vijon:
   a) inventari i proceseve - Hartëzimi i rreziqeve konsiston në ndarjen e çdo aktiviteti në procese dhe nënprocese. Çdo proces/nënproces përmban minimalisht informacionin e mëposhtëm:
      i. emrin e procesit/nënprocesit, qëllimin dhe llojin e aktivitetit ku bën pjesë,
      ii. strukturën përgjegjëse (*owner*) të procesit/nënprocesit,
      iii. frekuencën e procesit/nënprocesit,
      iv. maksimumin e kohës që pranohet për moskryerjen e procesit/nënprocesit;
   b) hartëzimi i rreziqeve - Çdo proces/nënproces i përcaktuar në inventar identifikohet në një prej ngjarjeve të rrezikut, në përputhje me anekset nr. 6-13 të kësaj rregulloreje dhe shoqërohet nga një kod unik;
   c) vlerësimi i rrezikut - Për çdo proces/nënproces kryhet vlerësimi i rrezikut me qëllim identifikimin e dobësive dhe përcaktimin e mënyrës së veprimit për administrimin e rrezikut sipas skenarëve të mëposhtëm:
      i. njohje dhe pranim i rrezikut,
      ii. parandalim i rrezikut duke zvogëluar frekuencën e materializimit të tij,
      iii. zbutje e rrezikut duke zvogëluar ndikimin e tij,
      iv. transferim i rrezikut te një palë e tretë,
      v. mospranim i rrezikut;
   d) niveli i kontrollit - Çdo proces/nënproces i identifikuar në inventarin e proceseve si pjesë e hartëzimit dhe vlerësimit të rreziqeve, është subjekt i kontrolleve të ndryshme, në nivel të linjës së parë dhe linjës së dytë të mbrojtjes, që variojnë në formë dhe frekuencë. Çdo kontroll duhet të përmbajë minimalisht elementet e mëposhtme:
      i. përshkrimin e kontrollit,
      ii. tipologjinë e kontrollit (autorizim, rikonsilim, akses në sistem, konfigurim sistemi, akses fizik, etj.),
      iii. strukturën përgjegjëse (*owner*) për zbatimin e kontrollit,
      iv. frekuencën e kryerjes së kontrollit.

4. Vlerësimi i rrezikut i parashikuar në shkronjën "c" të pikës 3 të këtij neni, konsiston të paktën në vlerësimin e:
   a) humbjes së pritshme vjetore;
   b) humbjes maksimale të mundshme sipas skenarit të rënduar;
   c) frekuencës së humbjes maksimale të mundshme sipas skenarit të rënduar;
   d) ndikimit jofinanciar (humbjes reputacionale, sipas klasave të përcaktuara në metodologji);
   e) cilësisë së kontrollit (sipas klasave të përcaktuara në metodologji).
5. Kontrollet e parashikuara në shkronjën "d" të pikës 3 të këtij neni, për çdo proces/nënproces, i nënshtrohen një procesi raportimi të formalizuar. Raportimet dhe rezultatet e kontrolleve duhet të përmbajnë minimalisht informacionin e mëposhtëm:
   a) rezultatin e kontrollit sipas një vlerësimi metodologjik të përshkallëzuar në disa klasa (p.sh. e gjelbër/e verdhë/portokalli/e kuqe);
   b) vlerën e rezultatit, nëse është e aplikueshme (p.sh. 100%, diferencë 0, ditë në vonesë, po/jo, etj.);
   c) një koment të qartë dhe të shkurtër mbi kontrollin e kryer;
   d) dokumentacionin që mbështet rezultatin e kontrollit dhe ndihmon eventualisht në hartimin e një plani korrigjues.
6. Efektiviteti i kontrolleve dhe cilësia e ekzekutimit të tyre është objekt i procesit të kontrollit të vazhdueshëm, në mënyrë që subjekti të ushtrojë veprimtarinë e tij në mënyrë të sigurt, në përputhje me kuadrin e brendshëm rregullativ dhe kuadrin ligjor e rregullativ të Bankës së Shqipërisë.
7. Struktura e pavarur e administrimit të rrezikut operacional planifikon dhe ndjek realizimin e procesit të hartëzimit dhe vetëvlerësimit të rreziqeve dhe kontrolleve në fuqi, me mbështetjen e organeve drejtuese të subjektit.
8. Procesi i hartëzimit dhe vetëvlerësimit të rreziqeve dhe kontrolleve realizohet nga vetë strukturat përgjegjëse (*owner*) për proceset/nënproceset, në bashkëpunim me strukturën e pavarur të administrimit të rrezikut operacional.
9. Çdo proces/nënproces i nënshtrohet një vlerësimi përfundimtar të rrezikut, të diferencuar në disa klasa dhe të përcaktuar sipas një metodologjie të brendshme të subjektit. Në vlerësimin përfundimtar të shkallës së rrezikut, subjekti mban në konsideratë të paktën kombinimin e elementeve të mëposhtëm:
   a) nivelin e humbjeve të pritshme;
   b) shkallën e ndikimit jofinanciar;
   c) cilësinë e kontrollit.
10. Proceset/nënproceset të cilat vlerësohen me rrezik të lartë (kritik), sipas metodologjisë së brendshme të subjektit, janë pjesë e kontrollit të vazhdueshëm. Ata janë objekt i kontrolleve shtesë dhe efektive nga strukturat përgjegjëse (*owner*) të procesit, në bashkëpunim me njësinë e administrimit të rrezikut operacional. Subjekti sigurohet për zbatimin dhe efektivitetin e kontrolleve nëpërmjet raportimeve sipas një frekuence të bashkërenduar.

Neni 23
Analiza e skenarëve

1. Subjekti përdor analiza skenarësh për të vlerësuar ekspozimin ndaj rreziqeve, kryesisht atyre me impakt të lartë financiar dhe probabilitet të ulët për të ndodhur. Nëpërmjet

analizës së skenarëve subjekti merr informacion të vlefshëm për shkaqet dhe pasojat e materializimit të ngjarjeve të rëndësishme, rezultate të cilat mund të përdoren në planin e vazhdimësisë së veprimtarisë gjatë testimit të qëndrueshmërisë operacionale (*operational resilience*).

2. Analiza e skenarëve bazohet në vlerësime subjektive, të cilat prodhohen nëpërmjet takimeve të zhvilluara midis strukturës përgjegjëse për administrimin e rrezikut operacional dhe ekspertëve të ndryshëm të aktivitetit të subjektit.
3. Zakonisht analizat e skenarëve përdorin si të dhëna, informacione nga:
   a) baza e të dhënave të ngjarjeve të rrezikut operacional të subjektit;
   b) informacione të jashtme, nga tregu;
   c) procesi i vetëvlerësimit të rreziqeve;
   d) sistemi i kontrollit të brendshëm;
   e) treguesit e paralajmërimit të hershëm;
   f) analiza e shkakut kryesor (*root-cause*);
   g) analiza e proceseve.

KREU III
TË TJERA

Neni 24
Masat mbikëqyrëse dhe ndëshkimore

Banka e Shqipërisë, në rast të mosplotësimit të kërkesave të kësaj rregulloreje, zbaton masat mbikëqyrëse dhe/ose ndëshkimore të parashikuara në ligjin "Për bankat" dhe në ligjin "Për shërbimet e pagesave".

Neni 25
Fillimi i efekteve

1. Kjo rregullore i fillon efektet nga data 1 mars 2025.
2. Subjektet, deri në datën 1 mars 2025, marrin masa për plotësimin e kërkesave të rregullores.

Neni 26
Dispozitë e fundit

Anekset bashkëlidhur kësaj rregulloreje janë pjesë përbërëse e saj.

KRYETARI I KËSHILLIT MBIKËQYRËS

Gent SEJKO

ANEKSET

Për raportimin e treguesve të paralajmërimit të hershëm në Bankën e Shqipërisë, subjekti plotëson aneksin nr.1, duke ndjekur udhëzimet e parashikuara në aneksin nr.2 të kësaj rregulloreje.

Aneksi nr.1

Treguesit e paralajmërimit të hershëm

<table>
<tr><th>Nr.</th><th>Treguesi</th><th>Vlera</th><th>Komente</th></tr>
<tr><td>1</td><td>Numri i çështjeve të reja ligjore</td><td>Numër</td><td></td></tr>
<tr><td>2</td><td>Kostoja e çështjeve ligjore</td><td>Vlerë (ALL)</td><td></td></tr>
<tr><td>3</td><td>Ankesat e reja të klientëve</td><td>Numër</td><td></td></tr>
<tr><td>4</td><td>Ankesat e hapura të klientëve</td><td>Numër</td><td></td></tr>
<tr><td>5</td><td>Numri i gjobave nga autoritetet</td><td>Numër</td><td></td></tr>
<tr><td>6</td><td>Vlera e gjobave nga autoritetet</td><td>Vlerë (ALL)</td><td></td></tr>
<tr><td>7</td><td>Qarkullimi i punonjësve</td><td>Përqindje (%)</td><td></td></tr>
<tr><td>8</td><td>Avari/Ndërprerje të programit bazë (core system)</td><td>(orë:minuta:sekonda)</td><td></td></tr>
<tr><td>9</td><td colspan="3">Numri i tentativave për hacking/ incidenteve kibernetike
<table>
<tr><th>Niveli 1 i detajimit</th><th>Niveli 2 i detajimit</th><th>Numër</th></tr>
<tr><td rowspan="5">Software/program i dëmshëm (Malware)</td><td>Ransomware</td><td></td></tr>
<tr><td>Trojan horse</td><td></td></tr>
<tr><td>Virus</td><td></td></tr>
<tr><td>Worm</td><td></td></tr>
<tr><td>Spyware/Adware</td><td></td></tr>
<tr><td>Mobile malware</td><td></td></tr>
<tr><td rowspan="4">Sulmet e inxhinierisë sociale (Social Engineering)</td><td>Phishing</td><td></td></tr>
<tr><td>Spear Phishing</td><td></td></tr>
<tr><td>Pretexting</td><td></td></tr>
<tr><td>Cyber squatting</td><td></td></tr>
<tr><td rowspan="4">Sulme nga punonjës ose palë të treta që aksidentalisht dhe/ose qëllimisht keqpërdorin të drejtat e aksesit (Insider/Third Party Provider Event and/or Misuses of access rights)</td><td>Accidental misuse of access rights</td><td></td></tr>
<tr><td>Intentional misuse of access rights by service provider</td><td></td></tr>
<tr><td>Intentional misuse of access rights by insider</td><td></td></tr>
<tr><td>Policy violation (Insider/ TPP)</td><td></td></tr>
<tr><td rowspan="5">Akses i paautorizuar i qëllimshëm (Unauthorised Access intentional)</td><td>Brute force attack</td><td></td></tr>
<tr><td>Malicious script injection and/or OS commanding</td><td></td></tr>
<tr><td>SQL Injection</td><td></td></tr>
<tr><td>Other exploited vulnerability</td><td></td></tr>
<tr><td>Information exposure</td><td></td></tr>
<tr><td>Sulm me shërbim të refuzuar/mohim shërbimi (Denial of Service Attack)</td><td>DoS attack</td><td></td></tr>
</table></td></tr>
</table>

		DDoS attack	
	Ngjarje të tjera të sigurisë kibernetike (*Other Cyber Security Event*)	*Defacement*	
		Brand Abuse on Mass and Social Media	
		Libel of persons on Mass and Social Media	
		Vulnerability Scan	

10

Numri i tentativave të suksesshme për incidente me natyrë kibernetike të *hacking*/incidenteve kibernetike

Niveli 1 i detajimit	**Niveli 2 i detajimit**	**Numër**
Software/program i dëmshëm (*Malware*)	*Ransomware*	
	Trojan horse	
	Virus	
	Worm	
	Spyware/Adware	
	Mobile malware	
Sulmet e inxhinierisë sociale (*Social Engineering*)	*Phishing*	
	Spear Phishing	
	Pretexting	
	Cyber squatting	
Sulme nga punonjës ose palë të treta që aksidentalisht dhe/ose qëllimisht keqpërdorin të drejtat e aksesit (*Insider/Third Party Provider Event and/or Misuses of access rights*)	*Accidental misuse of access rights*	
	Intentional misuse of access rights by service provider	
	Intentional misuse of access rights by insider	
	Policy violation (Insider/ TPP)	
Akses i paautorizuar i qëllimshëm (*Unauthorised access intentional*)	*Brute force attack*	
	Malicious script injection and/or OS commanding	
	SQL Injection	
	Other exploited vulnerability	
	Information exposure	
Sulm me shërbim të refuzuar/mohim shërbimi (*Denial of Service Attack*)	*DoS attack*	
	DDoS attack	

	Ngjarje të tjera të sigurisë kibernetike (*Other Cyber Security Event*)	*Defacement*	
		Brand Abuse on Mass and Social Media	
		Libel of persons on Mass and Social Media	
		Vulnerability Scan	
11	Disponueshmëria e ATM-ve (*uptime ratio*)	*Përqindje (%)*	
12	Karta nën investigim	*Numër*	
13	Rekomandimet e kontrollit të brendshëm të pa përmbushura brenda afatit	*Numër*	
14	Procedura, politika dhe rregullore të papërditësuara	*Përqindje (%)*	
15	Projekte që nuk janë mbyllur brenda afatit të përcaktuar nga subjekti	*Përqindje (%)*	
16	Numri i rasteve të identifikuara si mashtrim	*Numër*	
17	Thyerja e limiteve të brendshme të mbajtjes së *cash*-it në degë	*Numër*	
18	Numri i transfertave të gabuara në nisje (*outgoing*)	*Numër*	
19	Numri i kolateraleve hipotekare të regjistruar të cilëve iu ka mbaruar afati i sigurimit	*Numër*	
20	Kredi të reja me probleme	*Përqindje (%)*	
21	*Outsourcing* kritik pa kryer vlerësim vjetor të rrezikut të sigurisë së informacionit dhe vazhdimësisë së biznesit	*Numër*	
22	Numri i ngjarjeve kur mbulimi i fondeve të klientëve bie nën nivelin 100%*	*Numër*	
23	Vlera maksimale e shumës së fondeve të klientëve, e pambrojtur (*safeguarding*) sipas kërkesave ligjore e rregullative*	*Vlerë (ALL)*	

** Kërkesë e aplikueshme vetëm për institucionet e pagesave dhe institucionet e parasë elektronike.*

Aneksi nr.2

Udhëzime për plotësimin e treguesve të paralajmërimit të hershëm

<table>
<tr><th>Nr.</th><th>Treguesi</th><th>Përshkrimi</th></tr>
<tr><td>1</td><td>Numri i çështjeve të reja ligjore</td><td>Numri i çështjeve të reja ligjore të hapura gjatë periudhës raportuese, në të cilat përfshihet subjekti dhe të cilat përmbajnë elementë të rrezikut operacional. Përjashtohen çështjet e tjera ligjore, të cilat nuk përmbajnë elementë të rrezikut operacional.</td></tr>
<tr><td>2</td><td>Kostoja e çështjeve ligjore</td><td>Vlera e humbjes së pritshme e vlerësuar nga vetë subjekti në lidhje me çështjet ligjore të treguesit nr. 1. Përjashtohen kostot e çështjeve të tjera ligjore, të cilat nuk përmbajnë elementë të rrezikut operacional.</td></tr>
<tr><td>3</td><td>Ankesat e reja të klientëve</td><td>Numri i ankesave të ngritura kundër subjektit nga klientët apo palë të treta gjatë tremujorit, të marra nëpërmjet të gjitha kanaleve të komunikimit të vëna në dispozicion nga subjekti (shkresë formale, email, rrjete sociale etj.). Përfshihen të gjitha ankesat e marra gjatë tremujorit, qofshin ato të mbyllura, të refuzuara apo të hapura në fund të periudhës raportuese (tremujorit).</td></tr>
<tr><td>4</td><td>Ankesat e hapura të klientëve</td><td>Numri i ankesave të ngritura kundër subjektit nga klientët, grupet e klientëve apo publiku, që rezultojnë ende të hapura në fund të periudhës raportuese (tremujorit).</td></tr>
<tr><td>5</td><td>Numri i gjobave nga autoritetet</td><td>Numri i gjobave të vendosura subjektit nga autoritetet e ndryshme gjatë tremujorit, të cilat lidhen me veprimtarinë bankare dhe/ose financiare.</td></tr>
<tr><td>6</td><td>Vlera e gjobave nga autoritetet</td><td>Vlera e gjobave të vendosura nga autoritetet e ndryshme gjatë tremujorit, të cilat lidhen me veprimtarinë bankare dhe/ose financiare.</td></tr>
<tr><td>7</td><td>Qarkullimi i punonjësve</td><td>Përqindja e qarkullimit të punonjësve të të gjitha kategorive gjatë periudhës raportuese. Përfshihen punonjësit me kohë të plotë dhe kohë të pjesshme.
$Q=L/(P)*100$, $(P)=(P_0+P_1)/2$
ku:
Q – qarkullimi i punonjësve;
L – numri i punonjësve të larguar gjatë periudhës së raportimit;
(P) – numri mesatar i punonjësve gjatë periudhës së raportimit;
P_0 – numri i punonjësve në fillim të periudhës së raportimit;
P_1 – numri i punonjësve në fund të periudhës së raportimit.</td></tr>
<tr><td>8</td><td>Avari/Ndërprerje të programit bazë (core system)</td><td>Kohëzgjatja e ndërprerjeve të paplanifikuara të programit bazë të subjektit gjatë tremujorit, e shprehur sipas formatit (orë:minuta:sekonda).</td></tr>
<tr><td>9</td><td colspan="2">Numri i tentativave për hacking/ incidenteve kibernetike
<table>
<tr><th>Niveli 2 i detajimit</th><th>Përshkrimi</th></tr>
<tr><td>Ransomware</td><td>Lloj malware që kufizon aksesin në pajisjen e infektuar dhe kërkon shpërblim për të hequr kufizimin.</td></tr>
<tr><td>Trojan horse</td><td>Lloj malware që funksionimin e tij e fsheh brenda një programi tjetër, në dukje i dobishëm dhe i padëmshëm.</td></tr>
<tr><td>Virus</td><td>Lloj malware që është në gjendje të kopjojë veten e vet dhe të përhapet në kompjuterë të tjerë. Viruset mund të përdoren për të vjedhur informacione, për të dëmtuar kompjuterët, për të vjedhur para, për të dhënë më shumë reklama etj.</td></tr>
<tr><td>Worm</td><td>Një program që përsëritet dhe shkatërron të dhënat dhe skedarët në kompjuter. Në ndryshim nga virusi, ai nuk ka nevojë të lidhet me programe të tjera të ekzekutueshme për t'u përhapur.</td></tr>
</table></td></tr>
</table>

	Spyware/Adware	Është një lloj *malware* që gjeneron reklama automatikisht. *Adware* mund të lidhet me *spyware* dhe të gjurmojnë aktivitetin e përdoruesit dhe të vjedhin informacion.
	Mobile malware	*Software* keqdashës që sulmon pajisjet celulare ose mundëson teknologjinë me valë (*wireless*), duke shkaktuar bllokim të pajisjes, humbje të të dhënave ose vjedhje të informacionit.
	Phishing	Përpjekja për të marrë informacione të ndjeshme si emrat e përdoruesve, fjalëkalimet dhe informacionet e kartës së kreditit, duke pretenduar se është subjekt i besueshëm në një komunikim elektronik (p.sh. përmes një *e-mail*).
	Spear Phishing	Përpjekje/Sulme të drejtpërdrejta për të mashtruar individë ose kompani specifike.
	Pretexting	Krijimi dhe përdorimi i një skenari të shpikur (preteksti) për të përfshirë një përdorues të caktuar, në mënyrë të tillë që të rrisë shanset për të zbuluar informacionin ose për të vepruar në mënyra të pamundura në rrethana normale.
	Cyber squatting	Një regjistrim spekulativ i një domeni interneti që korrespondon me emrin e markës, shërbimit ose produktit të dikujt tjetër.
	Accidental misuse of access rights	Shkelje aksidentale/e paqëllimshme e të drejtave të aksesit në sistem me mundësi rrjedhjeje të mundshme të të dhënave dhe/ose korrupsion të të dhënave.
	Intentional misuse of access rights by service provider	Keqpërdorim i qëllimshëm i të drejtave të aksesit nga ofruesi i shërbimit.
	Intentional misuse of access rights by insider	Keqpërdorim i qëllimshëm i të drejtave të aksesit nga personat e brendshëm.
	Policy violation (Insider/ TPP)	Shkelje e politikës (personat e brendshëm/ofrues nga palë të treta).
	Brute force attack	Sulm i sforcuar.
	Malicious script injection and/or OS commanding	Futja e një skripti me qëllim të dëmshëm dhe/ose komandimi i OS.
	SQL Injection	Injeksioni SQL.
	Other exploited vulnerability	Dobësi e ekspozuar e *software* për të marrë akses të paautorizuar në sistemet e informacionit.
	Information exposure	Ekspozimi i informacionit.
	DoS attack	Sulm i krijuar për pamundësi përdorimi, për të mbyllur ose ndërprerë një rrjet, *website* ose shërbim.
	DDoS attack	Sulmi DoS në të cilin burimi i sulmit përbëhet nga adresa të shumta IP.
	Defacement	Sulm në një faqe interneti që ndryshon pamjen vizuale të faqes së internetit.
	Brand Abuse on Mass and Social Media	Një lloj ngjarjeje ku sulmuesit regjistrojnë profile të rreme në mediat sociale me emrin e kompanisë dhe/ose të drejtuesve.
	Libel of persons on Mass and Social Media	Lloji i ngjarjes në të cilën sulmuesit përhapin informacion të rremë/shpifës në mediat sociale me qëllim dëmtimin e imazhit dhe reputacionit të individit (p.sh. drejtuesve) dhe të kompanisë.
	Vulnerability Scan	Teknikë e përdorur për të identifikuar dobësitë e sigurisë në një sistem kompjuterik (nganjëherë cënueshmëria e aktiviteteve të skanimit mund të çojë në një shërbim ose një mosfunksionim/kohë të mosfunksionimit të procesit).
10	Numri i tentativave të suksesshme për incidente me natyrë kibernetike të *hacking*/incidentev e kibernetike	Sipas shpjegimit të dhënë në treguesin nr.9.

11	Disponueshmëria e ATM-ve (*uptime ratio*)	Përqindja e ATM-ve funksionale. Kërkohet të raportohet mesatarja e funksionimit/disponueshmërisë në përqindje të ATM-ve gjatë periudhës së raportimit, pavarësisht se periodiciteti i matjes mund të jetë i ndryshëm ndërmjet subjekteve. *Shembull indikativ*: Nëse një ATM është funksionale për 23 orë nga 24 orë në ditë, koeficienti i disponueshmërisë do të jetë (23/24)*100=95.83%. E njëjta logjikë ndiqet për raportimin tremujor. Për qëllime të këtij treguesi do të llogaritet disponueshmëria e të gjitha ATM-ve të subjektit për periudhën e raportimit (tremujorin).
12	Karta nën investigim	Numri i kartave të raportuara që janë nën një investigim të justifikuar nga subjekti, për shkak të arsyeve të mashtrimit që lidhen me to gjatë tremujorit (të gjitha llojet e kartave). Nuk përfshihen kartat e humbura, të vjedhura apo ato të riprintuara për arsye të tjera (për shembull riprintime për arsye dëmtimi).
13	Rekomandimet e kontrollit të brendshëm të papërmbushura brenda afatit	Rekomandime të njësisë së kontrollit të brendshëm, të cilat kanë kaluar afatin përfundimtar të plotësimit/përmbushjes në periudhën e raportimit.
14	Procedura, politika dhe rregullore të papërditësuara	Numri i procedurave që iu ka kaluar afati i rishikimit sipas politikave të brendshme të bankës ndaj totalit të procedurave dhe rregulloreve (në %).
15	Projekte që nuk janë mbyllur brenda afatit të përcaktuar nga subjekti	Numri i projekteve të cilave iu ka kaluar afati, ndaj totalit të projekteve në vazhdimësi (në %). Në numërues përfshihet numri i projekteve të cilat e kanë kaluar afatin përfundimtar të përmbushjes, për shkak të vonesave, joefikasitetit apo mosmonitorimit të projekteve, etj. dhe kostoja aktuale e të cilave tejkalon buxhetin vjetor për projektet >20%. *Shënim:* Në raportim do të përfshihen edhe ato projekte që subjekti i konsideron që kanë impakt direkt në drejtim të sistemeve të kontrollit dhe efektivitetit të saj, edhe pse impakti financiar mund të jetë < 20%.
16	Numri i rasteve të identifikuara si mashtrim	Numri i rasteve të identifikuara si mashtrim nga subjekti gjatë periudhës së raportimit. Nga ky tregues përjashtohen mashtrimet me kartat.
17	Thyerja e limiteve të brendshme të mbajtjes së *cash*-it në degë	Numri i rasteve të identifikuara të thyerjes së limiteve në fund të ditës për *cash*-in e mbajtur në degë gjatë periudhës së raportimit.
18	Numri i transfertave të gabuara në nisje (*outgoing*)	Numri total i transfertave (kombëtare dhe ndërkombëtare) në nisje, të kthyera mbrapsht ose të sistemuara, për shkak të gabimeve të realizuara gjatë periudhës raportuese. Në raportim do të përfshihen të gjitha rastet e procesuara gabim nga subjekti, përjashtuar rastet kur gabimi vjen nga klienti.
19	Numri i kolateraleve hipotekare të regjistruar të cilëve iu ka mbaruar afati i sigurimit	Numri i kolateraleve hipotekare për individë dhe biznese të cilëve iu ka mbaruar afati i sigurimit dhe janë të detyrueshëm për t'u siguruar.
20	Kredi të reja me probleme	Numri i kredive të reja me probleme ndaj numrit total të kredive të reja të disbursuara gjatë periudhës raportuese (në %).

		Në numërues përfshihen kreditë e reja me probleme për të cilat nuk kanë kaluar 90 ditë nga momenti i pagesës.
21	*Outsourcing* kritik pa kryer vlerësim vjetor të rrezikut të sigurisë së informacionit dhe vazhdimësisë së biznesit	Numri i ofruesve të shërbimeve me palë të treta (*outsourcing*) të vlerësuara si kritike nga subjekti, për të cilët nuk është kryer vlerësim vjetor i sigurisë së informacionit dhe vazhdimësisë së biznesit, në datën e mbylljes së periudhës raportuese.
22	Numri i ngjarjeve kur mbulimi i fondeve të klientëve bie nën nivelin 100%*	Numri i ngjarjeve kur mbulimi i fondeve të klientëve bie nën nivelin 100%. Llogaritja e treguesit për qëllime të këtij raportimi realizohet në bazë ditore për periudhën e raportimit.
23	Vlera maksimale e shumës së fondeve të klientëve, e pambrojtur (*safeguarding*) sipas kërkesave ligjore e rregullative*	Vlera maksimale e shumës së fondeve të klientëve, e pambrojtur (*safeguarding*) sipas kërkesave ligjore e rregullative, pra vlera më e lartë e fondeve e pambrojtur, që është evidentuar gjatë periudhës raportuese.

* *Kërkesë e aplikueshme vetëm për institucionet e pagesave dhe institucionet e parasë elektronike.*

Për raportimin e ngjarjeve të rrezikut operacional në Bankën e Shqipërisë, subjekti plotëson regjistrin sipas aneksit nr. 3, duke ndjekur udhëzimet e aneksit nr.4 dhe njëkohësisht zbaton parashikimet e pikës 3 të nenit 20 të rregullores.
Për ngjarje të cilat kanë zgjatur për më shumë se një periudhë raportuese dhe për rrjedhojë janë raportuar në periudha të mëparshme, subjekti përdor të njëjtin numër identifikimi në qelizën përkatëse të regjistrit dhe informacionin për ngjarjen e paraqet për periudhën raportuese.
Plotësimi i të gjitha fushave të aneksit është i detyrueshëm për çdo ngjarje të regjistruar, përveç fushës "data e rikuperimit" dhe "vlera e rikuperuar", plotësimi i të cilave do të kryhet kur ka informacion në lidhje me to. Fusha e komenteve rekomandohet, por nuk është e detyrueshme për t'u plotësuar.
Plotësimi i fushave të datës së rikuperimit dhe vlerës së rikuperimit do të shoqërohet me plotësimin e detyrueshëm edhe të fushave "numri i identifikimit të ngjarjes" dhe "përshkrimi i ngjarjes".

Aneksi nr. 3

Regjistri i ngjarjeve të rrezikut operacional

Numri i identifikimit	Përshkrimi	Njësia raportuese	Data e ndodhjes (d.m.v)	Data e identifikimit (d.m.v)	Data e kontabilizimit (d.m.v)	Lloji i ngjarjes (Niveli 1)	Lloji i ngjarjes (Niveli 2)	Lloji i ngjarjes (Niveli 3)	Linja e biznesit (Niveli 1)	Linja e biznesit (Niveli 2)	Efekti financiar	Shkaku (Niveli 1)	Shkaku (Niveli 2)	Vlera e humbjes bruto/fillestare (lekë)	*Data e rikuperimit*	*Vlera e rikuperuar*	*Ngjarje kufitare*	*Komente*

Aneksi nr. 4

Udhëzime për plotësimin e regjistrit të ngjarjeve të rrezikut operacional

Kolona	Udhëzime për plotësimin
Numri i identifikimit	Plotësohet numri i identifikimit të ngjarjes i përdorur nga subjekti në regjistrin e brendshëm të ngjarjeve të rrezikut operacional.
Përshkrimi	Plotësohet përshkrimi i çdo ngjarje të regjistruar në këtë regjistër. Subjekti nuk duhet të përfshijë informacione të cilat janë subjekt i ligjit "Për mbrojtjen e të dhënave personale".
Njësia raportuese	Plotësohet emri i njësisë që ka raportuar ngjarjen.
Data e ndodhjes	Plotësohet data e ndodhjes ose data e fillimit të ndodhjes së ngjarjes, për ato ngjarje të cilat kanë zgjatur efektin e tyre në kohë.
Data e identifikimit	Plotësohet data e identifikimit të ngjarjes nga punonjësit e subjektit.
Data e kontabilizimit	Plotësohet data në të cilën ngjarja është regjistruar në pasqyrat financiare të subjektit.
Lloji i ngjarjes (Niveli 1)	Klasifikimi i llojit të ngjarjes sipas nivelit 1 të detajimit, siç paraqitet në aneksin nr. 6 të kësaj rregulloreje.
Lloji i ngjarjes (Niveli 2)	Klasifikimi i llojit të ngjarjes sipas nivelit 2 të detajimit, siç paraqitet në anekset nr. 7-13 të kësaj rregulloreje.
Lloji i ngjarjes (Niveli 3)	Klasifikimi i llojit të ngjarjes sipas nivelit 3 të detajimit, siç parashikohet në anekset nr. 7-13 të kësaj rregulloreje. Subjekti, duke ndjekur udhëzimet sipas kuadrit të brendshëm rregullativ, mund të përdorë edhe ndarje të tjera për nivelin e tretë të llojit të ngjarjeve.
Linja e biznesit (Niveli 1)	Klasifikimi i ngjarjes sipas linjës së biznesit të nivelit 1 të detajimit, siç paraqitet në aneksin nr. 14 të kësaj rregulloreje.
Linja e biznesit (Niveli 2)	Klasifikimi i ngjarjes sipas linjës së biznesit të nivelit 2 të detajimit, siç paraqitet në aneksin nr. 14 të kësaj rregulloreje. Subjekti, duke ndjekur udhëzimet sipas kuadrit të brendshëm rregullativ, mund të përdorë edhe ndarje të tjera për nivelin e dytë të linjës së biznesit.
Efekti financiar	Efekti financiar plotësohet me një nga opsionet e parashikuar në aneksin nr. 15 të rregullores. Efektet e tjera financiare të parashikuara në nenin 20, pika 3, shkronja "e" të rregullores, vlejnë vetëm për qëllime të brendshme të subjektit.
Shkaku (Niveli 1)	Plotësohet një nga opsionet e kolonës *"Shkaku i ngjarjes, ndarje sipas nivelit 1"* të aneksit nr. 5 të kësaj rregulloreje.
Shkaku (Niveli 2)	Plotësohet një nga opsionet e kolonës *"Shkaku i ngjarjes, ndarje sipas nivelit 2"* të aneksit nr. 5 të kësaj rregulloreje.
Vlera e humbjes bruto/fillestare (lekë)	Plotësohet humbja fillestare/bruto e çdo ngjarje të ndodhur në këtë regjistër. Regjistrohet vlera absolute/pozitive dhe në asnjë rast nuk plotësohen vlera negative.
Data e rikuperimit	Plotësohet data në të cilën është kontabilizuar vlera e rikuperimit.
Vlera e rikuperuar	Plotësohet çdo vlerë e rikuperuar nga humbja fillestare. Vlera e rikuperuar regjistrohet në këtë qelizë dhe nuk prek vlerën e regjistruar në qelizën e humbjes bruto/fillestare.
Ngjarje kufitare (*boundary event)*	Plotësohet me një nga fjalët: "JO" ose "Rreziku i kredisë" ose "Rreziku i tregut". *Sqarim*: me shënimin "rreziku i kredisë" ose "rreziku i tregut" plotësohet vetëm kur ngjarja operacionale vjen nga ngjarje të lidhura me rrezikun e kredisë ose atë të tregut (*boundary events*). Në çdo rast tjetër do regjistrohet "JO".
Komente	Plotësohet me çdo koment të vlefshëm mbi ngjarjen.

Aneksi nr. 5
Klasifikimi i ngjarjes sipas shkakut, niveli 1 dhe 2 i detajimit

Shkaku i ngjarjes, ndarje sipas nivelit 1	**Shkaku i ngjarjes, ndarje sipas nivelit 2**
Njerëzit/punonjësit	Shkaqe aksidentale (njerëz)
	Mungesë e trajnimit/kompetencës së mjaftueshme
	Nivel i pamjaftueshëm i burimeve njerëzore
	Role dhe përgjegjësi joefektive
	Komunikim i gabuar
	Kulturë joefektive
	Keqdashje
Dështim i proceseve	Dështim në dizenjimin e procedurës/procesit
	Dështim në implementimin e procedurës/procesit
	Keqadministrim i projekteve/ndryshimeve
	Dështim i qeverisjes
Faktorë të jashtëm	Fatkeqësi natyrore
	Keqdashje
	Terrorizëm/sulme të jashtme (me përjashtim të sulmeve kibernetike)
	Mjedisi (me përjashtim të fatkeqësive natyrore)
	Destabilizim gjeopolitik/ekonomik/social
	Mjedisi rregullator dhe legjislativ
Sistemet	Probleme me funksionalitetin
	Probleme me performancën/kapacitetin
	Mungesë mirëmbajte/suporti
	Padisponueshmëri
	Testim/zhvillim i papërshtatshëm
	Probleme gjatë lancimit/nxjerrjes në përdorim
	Probleme konfigurimi
	Probleme me ruajtjen/memorien dhe shkatërrimin e të dhënave
	Shfrytëzimi i vulnerabiliteteve të lidhura me sigurinë e informacionit
	Çështje të lidhura me teknologjinë
	Probleme planifikimi

Aneksi nr. 6
Klasifikimi i ngjarjes sipas llojit, niveli 1 i detajimit

Kodi	Ndarje sipas nivelit 1	Përshkrimi
EL1	Mashtrimi i brendshëm	Mashtrimi i brendshëm lidhet me ushtrimin e veprimtarive të paautorizuara, vjedhje dhe/ose mashtrime që përfshijnë të paktën një punonjës të subjektit.
EL2	Mashtrimi i jashtëm	Mashtrimi i jashtëm i referohet mashtrimeve dhe/ose vjedhjeve që kryhen nga një palë e tretë jashtë subjektit.
EL3	Praktikat e punësimit dhe të sigurisë në punë	Kjo kategori i referohet ngjarjeve që lidhen me marrëdhëniet e punonjësve, sigurisë së mjediseve të punës, si dhe diversitetit/diskriminimit.
EL4	Klientët, produktet dhe praktika të veprimtarive	Në këtë kategori, humbjet operacionale lindin si pasojë e një dështimi për të përmbushur një detyrim të klientit, ose nga natyra dhe projektimi i produktit.
EL5	Dëmtime fizike të aktiveve	Kjo kategori i referohet ngjarjeve të cilat lidhen me humbjen apo dëmtimin e aktiveve nga fatkeqësitë natyrore apo ngjarje të tjera.
EL6	Ndërprerja e aktivitetit dhe dështimi i sistemeve	Kjo kategori i referohet humbjeve që vijnë nga ndërprerja e biznesit ose dështimet e sistemit.
EL7	Ekzekutimi, shpërndarja dhe administrimi i proceseve	Kjo kategori përfshin ngjarjet e rrezikut që lidhen me përpunimin e transaksioneve ose me administrimin e proceseve dhe të marrëdhënieve me palë të treta.

Aneksi nr. 7
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL1) Mashtrimi i brendshëm

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL1.1	Veprime të paautorizuara	EA1.1.1	Transaksione të paraportuara (qëllimisht)
		EA1.1.2	Shpërdorim i detyrës, aktivitete të paautorizuara
		EA1.1.3	Ngatërresë/Mospërputhje e pozicionit (qëllimisht)
EL1.2	Vjedhje dhe mashtrim (i brendshëm)	EA1.2.1	Mashtrim/mashtrim me kreditë/mashtrim me depozitat
		EA1.2.2	Vjedhje/zhvatje/përvetësim/grabitje
		EA1.2.3	Keqpërdorim i pronës së subjektit
		EA1.2.4	Shkatërrim i qëllimshëm i aseteve
		EA1.2.5	Falsifikim
		EA1.2.6	Mashtrim me çeqet
		EA1.2.7	Korrupsion
		EA1.2.8	Falsifikim/përvetësim i llogarisë
		EA1.2.9	Mospërputhshmëri me taksat/evazion fiskal
		EA1.2.10	Shantazhe/ryshfete ose dështim për t'iu përmbajtur rregullave në rastet e përfitimeve (dhurata dhe ftesat e dhëna dhe të marra)
		EA1.2.11	Keqpërdorim i llogarive (qëllimisht)

Aneksi nr. 8
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL2) Mashtrimi i jashtëm

Kodi	**Ndarje sipas nivelit 2**	**Kodi**	**Ndarje sipas nivelit 3**
EL2.1	Vjedhje dhe mashtrim (i jashtëm)	EA2.1.1	Vjedhje/grabitje
		EA2.1.2	Falsifikim
		EA2.1.3	Mashtrim me çeqet
EL2.2	Siguria e sistemit (mashtrim i jashtëm)	EA2.2.1	Dëmtime nga sulmet kibernetike (*hacking)*
		EA2.2.2	Vjedhje dhe publikim i të dhënave konfidenciale

Aneksi nr. 9
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL3) Praktikat e punësimit dhe të sigurisë në punë

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL3.1	Marrëdhëniet me punonjësit	EA3.1.1	Problematika lidhur me kompensime, përfitime dhe shkëputje nga puna
		EA3.1.2	Aktivitete (greva, protesta) të organizuara të punonjësve
EL3.2	Mjedis i sigurt	EA3.2.1	Detyrime/përgjegjësi të përgjithshme lidhur me sigurinë në punë
		EA3.2.2	Problematika të rregullores së sigurisë dhe shëndetit
		EA3.2.3	Kompensime për punonjësit
EL3.3	Diversiteti dhe diskriminimi	EA3.3.1	Të gjitha llojet e diskriminimit

Aneksi nr. 10
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL4) Klientët, produktet dhe praktika të veprimtarive

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL4.1	Përshtatshmëria, publikimi dhe mirëbesimi	EA4.1.1	Thyerje të rregullave, të mirëbesimit
		EA4.1.2	Problematika në përshtatshmërinë dhe zbulimin e të dhënave të klientit, etj.
		EA4.1.3	Shkelje e masave mbrojtëse për publikimin e të dhënave të klientëve
		EA4.1.4	Shkelje e privatësisë
		EA4.1.5	Praktika të papërshtatshme shitjeje
		EA4.1.6	Abuzim me të drejtat e llogarisë
		EA4.1.7	Shpërdorim i informacionit konfidencial
		EA4.1.8	Detyrim/përgjegjësi e huadhënësit (*lender liability*)
EL4.2	Praktika të papërshtatshme biznesi dhe tregu	EA4.2.1	*Antitrust*
		EA4.2.2	Praktika të papërshtatshme të biznesit
		EA4.2.3	Reklamim manipulues
		EA4.2.4	Tregtim i brendshëm (*insider trading*)
		EA4.2.5	Aktivitet i palicencuar
		EA4.2.6	Pastrim parash
EL4.3	Mangësitë e produktit	EA4.3.1	Produkte defektive
		EA4.3.2	Gabime në modele
EL4.4	Seleksionimi, sponsorizimi/financimi dhe ekspozimi	EA4.4.1	Dështim për të investiguar klientin sipas udhëzimeve/rregulloreve/mungesë e njohjes së klientit
		EA4.4.2	Tejkalim i limiteve të ekspozimit të klientëve
EL4.5	Aktivitete këshilluese	EA4.5.1	Mosmarrëveshje mbi performancën e aktiviteteve këshilluese

Aneksi nr. 11
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL5) Dëmtime fizike të aktiveve

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL5.1	Ngjarje katastrofike dhe të tjera	EA5.1.1	Humbje nga katastrofa natyrore
		EA5.1.2	Humbje njerëzore nga ngjarje madhore si terrorizëm, vandalizëm etj.

Aneksi nr. 12
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL6) Ndërprerja e aktivitetit dhe dështimi i sistemeve

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL6.1	Sistemet	EA6.1.1	*Hardware*
		EA6.1.2	*Software*
		EA6.1.3	Telekomunikacioni
		EA6.1.4	Dështime të utiliteteve (energjia, transporti...)

Aneksi nr. 13
Klasifikimi i ngjarjes sipas llojit, niveli 2 dhe 3 i detajimit
Lloji i ngjarjes: (EL7) Ekzekutimi, shpërndarja dhe administrimi i proceseve

Kodi	Ndarje sipas nivelit 2	Kodi	Ndarje sipas nivelit 3
EL7.1	Njohja, ekzekutimi dhe mirëmbajtja e transaksioneve	EA7.1.1	Komunikim i gabuar
		EA7.1.2	Gabime në regjistrimin e të dhënave, mirëmbajtje dhe gabime në ngarkim (*loading*)
		EA7.1.3	Dështim në përmbushjen e afateve apo përgjegjësive
		EA7.1.4	Keqfunksionim i modeleve/sistemeve
		EA7.1.5	Gabime në kontabilizim
		EA7.1.6	Keqfunksionim i detyrave të tjera
		EA7.1.7	Dështim gjatë vendosjes në përdorim (*delivery failure*)
		EA7.1.8	Dështim në administrimin e kolateralit
		EA7.1.9	Mangësi në mirëmbajtjen e të dhënave referuese
EL7.2	Monitorimi dhe raportimi	EA7.2.1	Dështim në përputhshmërinë me kërkesat për raportim (raporte financiare ose rregullatore)
		EA7.2.2	Raportime të jashtme të papërshtatshme (humbje të ndodhura)
EL7.3	Regjistrimi i klientëve dhe dokumentimi	EA7.3.1	Pëlqimi i klientit/mungesa e refuzimit
		EA7.3.2	Mungesa e dokumenteve ligjore/të paplotësuara
EL7.4	Menaxhimi i llogarive të klientëve	EA7.4.1	Akses i paaprovuar dhënë llogarive të klientëve
		EA7.4.2	Regjistrim i pasaktë i klientëve
		EA7.4.3	Humbje apo dëmtim i aseteve të klientëve si pasojë e neglizhencës
EL7.5	Palët e treta tregtare	EA7.5.1	Keqperformancë e palëve të treta joklientë
		EA7.5.2	Mosmarrëveshje të ndryshme kundrejt palëve të treta joklientë
EL7.6	Shitësit dhe furnitorët	EA7.6.1	Mosmarrëveshje me shitësit dhe furnitorët

Aneksi nr. 14

Klasifikimi i ngjarjes sipas linjës së biznesit. Niveli 1 dhe 2 i detajimit

Kodi	Ndarje sipas nivelit 1	Kodi	Ndarje sipas nivelit 2
BL1	Financat e korporatave	BL1.1	Financat e korporatave
		BL1.2	Financat lokale dhe të qeverisë qendrore
		BL1.3	Shërbime bankare tregtare (*merchant banking*)
		BL1.4	Shërbime këshilluese
BL2	Veprime me thesarin	BL2.1	Tregtimi
		BL2.2	Tregtimi për llogari të vet (*market making*)
		BL2.3	Pozicioni i pronarit (*proprietary positions*)
		BL2.4	Veprime me thesarin
BL3	Veprimtari bankare me pakicë (*retail*)	BL3.1	Veprimtari bankare me pakicë (*retail*)
		BL3.2	Shërbime bankare të personalizuara (*private banking*)
		BL3.3	Shërbimet e kartave
BL4	Veprimtari bankare e financiare	BL4.1	Ndërmjetësim në tregjet ndërbankare
BL5	Pagesat dhe shlyerjet	BL5.1	Klientë të jashtëm
BL6	Shërbime si agjent	BL6.1	Ruajtje e instrumenteve financiare
		BL6.2	Administrim dhe marrje në kujdestari e instrumenteve financiare
BL7	Administrim aktivesh	BL7.1	Administrim i fondeve
		BL7.2	Forma të tjera të administrimit të aktiveve
BL8	Ndërmjetësim me pakicë	BL8.1	Ndërmjetës financiar me pakicë (*retail*)

Shënim: Subjekti duhet të përcaktojë kritere të veçanta në kuadrin e brendshëm rregullativ për kategorizimin e ngjarjeve sipas linjave të biznesit. Kriteret duhet të rishikohen dhe të përshtaten për aktivitetet e reja apo/dhe për çdo ndryshim të biznesit dhe të rreziqeve, që ndërmerr subjekti.

Parimet për kategorizimin e linjave të biznesit sipas aneksit nr.14 të kësaj rregulloreje janë:

a) të gjitha veprimtaritë duhet të kategorizohen/përfshihen plotësisht në linjat e biznesit të përcaktuara në aneksin nr.14;
b) çdo veprimtari e cila nuk mund të kategorizohet lehtë në kuadrin e linjave të biznesit, por që përbën një funksion ndihmës për një veprimtari të përfshirë në këtë kuadër linjash, duhet të përfshihet në atë linjë biznesi që mbështet. Subjekti duhet të vendosë kritere objektive për kategorizimin e veprimtarive, në rastin kur veprimtaria ndihmëse mbështet më shumë se një linjë biznesi;
c) nëse një veprimtari nuk mund të kategorizohet në një linjë të veçantë biznesi, subjekti duhet të përdorë njërën nga linjat e biznesit, siç veprohet në rastin e veprimtarive ndihmëse;
d) kategorizimi i veprimtarive në linjat e biznesit, për qëllime të rrezikut operacional, duhet të jetë në përputhje me kategoritë e përdorura për klasifikimin e aktiveve sipas rrezikut të kredisë dhe rreziqeve të tregut;
e) procesi i kategorizimit të veprimtarive sipas linjave të biznesit duhet të jetë subjekt i shqyrtimit të pavarur të kontrollit të brendshëm.

Aneksi nr. 15
Klasifikimi i ngjarjes sipas efektit

Kodi	Efekti financiar
ET1	Humbje efektive
ET2	Vendosje provigjionesh
ET3	Humbje të mbetura pezull (*pending losses*)*
ET4	Humbje të pamaterializuara (*near misses*)*
ET5	Humbje në kohë (*timing losses*)*
ET6	Kompensim*

** Këto ngjarje do të raportohen në Bankën e Shqipërisë vetëm nëse janë vlerësuar si kritike nga vetë subjekti. Për sa i përket rubrikës "Humbje në kohë (timing losses)", në Bankën e Shqipërisë do të raportohen vetëm ato ngjarje të vlerësuara si kritike dhe që kanë prekur/kanë efekt financiar në pasqyrat e të ardhurave dhe shpenzimeve të dy ose më shumë viteve.*

Aneksi nr. 16

Shembull i formularit standard për raportimin e ngjarjeve të rrezikut operacional nga punonjësit e subjektit

Emri i punonjësit që raporton ngjarjen	
Struktura e punonjësit që raporton ngjarjen	
Përshkrimi i ngjarjes	
Vendndodhja e ngjarjes	
Data e ndodhjes së ngjarjes	
Data e zbulimit të ngjarjes	
Data e kontabilizimit të ngjarjes	
Mënyra e zbulimit të ngjarjes (nga kontrolli, klientët, informuar nga punonjësit, të tjerë, duke specifikuar)	
Shkaku i ngjarjes	
Vlera bruto e humbjes	
Vlera e mundshme e rikuperimit	
Mënyra e rikuperimit (sigurimi, klienti, kundërpartia, tjetër, duke e specifikuar)	
Vlera e rikuperuar	
Data e rikuperimit	
Vlera neto e humbjes	
Efekti financiar (humbje efektive, humbje të pamaterializuara, etj.)	
Lloji i ngjarjes (sipas anekseve nr.6-13)	
Linja e biznesit (sipas aneksit nr.14)	
Masat e marra	

Aneksi nr. 17

Në vijim jepen disa shembuj të ngjarjeve kufitare (*boundary events*) të lidhura me rrezikun e kredisë dhe të tregut:

1. Mashtrim i brendshëm nëpërmjet falsifikimit të të dhënave të kredimarrësit (të dhënat personale, statusin e kredimarrësit, aftësinë paguese, etj.);
2. Aprovim i kredive tek persona të cilët nuk ekzistojnë;
3. Vjedhje e identitetit të klientit;
4. Mbivlerësim i qëllimshëm i kolateralit nga ekspertë të jashtëm;
5. Pamundësi për të mbledhur kreditë e këqija si pasojë e mungesës/mos arkivimit të saktë të dokumentacionit/kontratës;
6. Kolaterale të pasiguruara;
7. Thyerje e qëllimshme e limiteve të thesarit;
8. Gabime gjatë aktivitetit të thesarit (blerje e letrave me vlerë të gabuara, shitje në vend të blerjes, etj.).