RREGULLORE
"PËR MBIKËQYRJEN E TRANSAKSIONEVE BANKARE NË RRUGË ELEKTRONIKE"

(miratuar me vendimin nr.28, datë 30.03.2005 të Këshillit Mbikëqyrës të Bankës së Shqipërisë).

Neni 1
Baza ligjore

Kjo rregullore nxirret në zbatim të ligjit nr.8269, datë 23.12.1997 "Për Bankën e Shqipërisë" dhe të ligjit nr.8365, datë 2.07.1998 "Për bankat në Republikën e Shqipërisë".

Neni 2
Qëllimi

Kjo rregullore ka për qëllim të përcaktojë:

a) kushtet organizative, kushtet në lidhje me personelin dhe kushtet teknike për realizimin e veprimtarisë bankare në rrugë elekronike (*e-banking)*;
b) kërkesat lidhur me verifikimin e kryer nga Banka e Shqipërisë për shërbimin *e- banking;*
c) parimet e administrimit të rrezikut të shërbimit *e-banking*.

Neni 3
Subjektet

Subjekt i kësaj rregulloreje janë të gjitha bankat dhe degët e bankave të huaja (më poshtë, bankat), që kryejnë veprimtari bankare në Republikën e Shqipërisë dhe që synojnë kryerjen e veprimtarisë bankare në rrugë elektronike.

Neni 4
Përcaktime

E-banking **është** shërbimi në distancë, nëpërmjet kanaleve elektronike të shpërndarjes dhe të komunikimit, i produkteve dhe i shërbimeve tradicionale dhe të reja bankare, brenda veprimtarive të lejuara për bankat e nivelit të dytë.

Neni 5
Ndalimet

a) Bankat nuk lejohet të hapin llogari *e-banking* pa praninë fizike të klientit në bankë dhe pa kryer identifikimin e tij ose të përfaqësuesit të tij të autorizuar ligjërisht, mbështetur edhe në rregulloret e brendshme të miratuara. Banka ruan dokumentacionin që provon identifikimin e klientit, të paktën për një periudhë 5 vjeçare.
b) Bankat nuk lejohet të kryejnë shërbimin *e-banking,* pa u verifikuar më parë për kushtet e kryerjes së tij nga Banka e Shqipërisë.

Neni 6
E drejta për kryerjen e veprimtarisë *e-banking*

Bankat mund të kryejnë *e-banking* vetëm pas verifikimit për plotësimin e kushteve nga ana e Bankës së Shqipërisë. Pas përgatitjeve, banka njofton Bankën e Shqipërisë për kryerjen e verifikimit. Njoftimi, shoqërohet me:

a) vendimin e këshillit drejtues të bankës për përdorimin e *e-banking* në kryerjen e veprimtarive të bankës;

b) *curriculum vitae* të përgjegjësit direkt dhe të personelit teknik që do të mbështesë bankën në realizimin e veprimtarisë së *e-banking,* e cila duhet të përmbajë edhe kualifikimet dhe përvojën e punës së tyre*;*

c) të dhënat që tregojnë kërkesat teknike të nevojshme për drejtimin dhe kontrollin e *e-banking;*

d) vlerësimin e efekteve të përdorimit të *e-banking* në rezultatin e bankës nëpërmjet pasqyrave financiare për tre vitet e ardhshme;

e) prodedurat e funksionimit të *e-banking* dhe programi i kontrollit të brendshëm për këtë qëllim;

f) marrëveshjen e nënshkruar me shoqërinë për realizimin e mbështetjes informatike të bankës, nëse ka të tillë ose nëse lidhet pas marrjes së autorizimit;

g) listën e transaksioneve bankare që do të kryejnë së bashku me kanalet e komunikimit do të përdorin.

Neni 7
E drejta e kryerjes së shërbimit dhe pezullimi i shërbimit

a) Pas njoftimit në Bankën e Shqipërisë sipas nenit 6, si edhe pas kryerjes së një verifikimi nga inspektorët e Bankës së Shqipërisë mbi vlerësimin e kushteve teknike, banka ka të drejtë të kryejë shërbimin e *e-banking*.

b) Banka e Shqiperise mund të urdhërojë bankën të pezullojë në mënyrë të pjesshme ose të plotë shërbimin e *e-banking*, nëse gjatë procesit të mbikëqyrjes nga Banka e Shqipërisë vërehet se banka nuk ka respektuar kërkesat e kësaj rregulloreje.

c) Në rastin e pezullimit të pjesshëm, banka ndërpret brenda 60 ditësh shërbimin *e-banking* të pezulluar dhe njofton për këtë Bankën e Shqipërisë. Banka nuk mund të rifillojë këtë shërbim pa kaluar një periudhë prej 6 muajsh nga pezullimi i tij. Kushtet e rifillimit, janë të njëjta si në nenin 6.

d) Në rastin e pezullimit të plotë, banka ndërpret brenda 60 ditësh shërbimin *e-banking* dhe njofton për këtë Bankën e Shqipërisë. Banka nuk mund të rifilloje këtë shërbim pa kaluar një periudhe prej 18 muajsh nga pezullimi i tij. Kushtet e rifillimit, janë të njëjta si ne nenin 6.

Neni 8
Kërkesa pas fillimit të shërbimit

a) Banka njofton paraprakisht Bankën e Shqipërisë për të gjitha shtesat në listën e kanaleve te komunikimit dhe në transaksionet bankare që kryen në rrugë elektronike, të cilat ndodhin pas fillimit të shërbimit *e-banking*.

b) Banka e Shqipërisë ka të drejtë të kërkojë plotësimin e dokumentacionit të nenit 6 për të gjitha ndryshimet dhe të kryejë verifikime të kushteve teknike, kur e gjykon të arsyeshme.

Neni 9
Kontabiliteti

Bankat bëjnë regjistrimet kontabël për veprimet e kryera edhe për *e-banking*, duke zbatuar ligjin "Për kontabilitetin dhe pasqyrat financiare" dhe "Manualin e kontabilitetit bankar".

PARIMET E ADMINISTRIMIT TË RREZIKUT TË *E-BANKING*

Neni 10
Mbikëqyrja efektive

Këshilli drejtues dhe drejtuesit e lartë ekzekutivë duhet të krijojnë një mbikëqyrje efektive të administrimit të rreziqeve që shoqërojnë veprimtaritë e *e-banking*, duke përfshirë vendosjen e përgjegjësive, të politikave dhe të kontrolleve specifike për të administruar këto rreziqe. Për këtë ata duhet, që në mënyrë të dokumentuar:

a) të përcaktojnë qartë rrezikun e bankës në lidhje me *e-banking;*
b) të pëcaktojnë autoritetet, kompetencat e tyre dhe mekanizmat e raportimit, duke përfshirë procedurat e nevojshme të veprimit sipas shkallëve të përgjegjësisë në raste thyerjeje të sigurisë (si penetrimi nëpërmjet rrjetit, shkelje të kërkesave sigurisë nga të punësuarit, ndonjë keqpërdorim serioz i pajisjeve të kompjuterave etj.) që ndikojnë në sigurinë e shërbimit, në gjendjen dhe në reputacionin e bankës;
c) të vlerësojnë faktorët unikë të rrezikut për garantimin e sigurisë, të integritetit dhe të disponueshmërisë së produkteve dhe të shërbimeve *e-banking,* dhe të zbatojnë kërkesën që palët e treta, me të cilat banka ndan/përdor sistemet apo aplikimet kryesore, të marrin të njëjtat masa;
d) të garantojnë që *due diligence* dhe analiza e rrezikut janë realizuar para kryerjes së veprimtarive me jashtë (*cross-border*);
e) të përcaktojnë burimet që kërkohen për të mbikëqyrur shërbimet e *e-banking* në përpjesëtim me funksionimin operacional dhe me rrezikshmërinë e sistemeve, dobësitë e rrjeteve dhe ndjeshmëritë (natyrën) e informacioneve që transmetohen.

Neni 11
Infrastruktura e kontrollit të cilësisë

Këshilli drejtues dhe drejtuesit e lartë ekzekutivë duhet të rishikojnë dhe të miratojnë orientimet kryesore të procesit të kontrollit të sigurisë së bankës.

a) Këshilli drejtues dhe drejtuesit e lartë ekzekutivë, duhet të mbikëqyrin zhvillimin dhe mirëmbajtjen e vazhdueshme të infrastrukturës së kontrollit të cilësisë, që mbron në mënyrë të mjaftueshme sistemet dhe të dhënat e *e-banking* nga kërcënimet e jashtme dhe të brendshme. Ky proces përfshin dhënien e të drejtave të autorizuara, të drejtave për kontrollet logjike dhe fizike, si edhe percaktimin e sigurisë të mjaftueshme të infrastrukturës për të ruajtur kufijtë dhe kufizimet e duhura në veprimtaritë e brendshme dhe të jashtme.

Këshilli drejtues dhe drejtuesit e lartë ekzekutivë duhet:
b) të përcaktojnë përgjegjësitë eksplicite të personelit për zbatimin dhe kontrollin e zbatimit të politikave të sigurisë së bankës;
c) të mundësojnë kryerjen e kontrolleve të mjaftueshme fizike për t'u mbrojtur nga hyrjet fizike të paautorizuara në ambientin kompjuterik;
d) të mundësojnë kryerjen e kontrolleve të mjaftueshme logjike dhe të proceseve monitoruese për t'u mbrojtur nga hyrjet e jashtme apo të brendshme të paautorizuara në aplikimet dhe në bazën e të dhënave të *e-banking*;
e) të mundësojnë kryerjen e rishikimeve të rregullta dhe të testimeve të masave dhe të kontrolleve të sigurisë, duke përfshirë ndjekjen e vazhdueshme të zhvillimeve aktuale të industrisë së sigurisë dhe instalimin e *software* të përmirësuar, të paketave të shërbimit dhe të masave të tjera.

Neni 12
Mbikëqyrja e burimeve të jashtme

Këshilli drejtues dhe drejtuesit e lartë ekzekutivë duhet të vendosin nje proces mbikëqyrjeje dhe të zbatojnë kujdes të plotë dhe të vazhdueshëm për administrimin e marrëdhënieve të bankës me palët e tjera të jashtme që mbështesin *e-banking* dhe për përdorimin e burimeve të tjera të jashtme në këtë fushë.

Këshilli drejtues dhe drejtuesit e lartë ekzekutivë duhet të sigurojnë që:
a) banka kupton plotësisht rreziqet që shoqërohen me përfshirjen në një marrëveshje partneriteti apo burimi të jashtëm (psh. me një kompani të pavarur që ofron shërbimin e internetit, etj.) për sistemet dhe aplikimet e saj të *e-banking*;
b) është kryer një rishikim i kujdesshëm dhe i përshtatshëm i aftësisë profesionale dhe i mundësisë financiare të dhënësit të shërbimit si palë e tretë, para nënshkrimit të kontratës për shërbimet e *e-banking;*
c) është përcaktuar qartë përgjegjësia kontraktuale e të gjitha palëve në marrëdhënien e

partneritetit, duke përfshirë edhe një palë të jashtme. Veçanërisht, përgjegjësitë për dhënien dhe për marrjen e informacionit tek dhe nga dhënësi i shërbimit, përgjegjësitë për mbajtjen e *backupeve* dhe të kopjeve të transaksioneve të kryera nëpërmjet *e-banking,* duhet të përcaktohen qartë*;*

d) të gjitha sistemet dhe operacionet e *e-banking* të dhëna nga burime të jashtme janë subjekt i administrimit të rrezikut, të politikave të sigurisë dhe të ruajtjes së fshehtësisë që përputhen me standardet e vetë bankës;

e) janë kryer kontrolle periodike të brendshme dhe/ose të jashtme ndaj operacioneve të burimeve të jashtme, të paktën në të njëjtën shtrirje që kërkohet kur këto të jenë kryer nga burimet e brendshme;

f) ekzistojnë plane për burime rezervë në raste incidentesh për aktivitetet e *e-banking* nga burimet e jashtme.

Neni 13
Identiteti dhe autorizimi i klientëve

Bankat duhet të marrin masat e nevojshme për të vërtetuar identitetin dhe autorizimin e klientëve me të cilët ato kryejnë biznes nëpërmjet internetit.

a) Bankat duhet të përdorin metoda të sigurta për verifikimin e identitetit dhe autorizimin e klientëve të rinj si edhe vërtetimin e identitetit të klientëve ekzistues që kërkojnë të ndërmarrin transaksione elektronike.

b) Bankat mund të përdorin metoda të ndryshme, në mënyrë të veçantë ose të kombinuara mes tyre, për të vendosur identifikimin, përfshirë PIN-et, *password-et, smart cards*, *biometrics* dhe çertifikatat digitale. Bankat duhet të monitorojnë dhe adoptojnë praktikat e shëndosha të industrisë në këtë fushë për të siguruar që:

i) Bazat e të dhënave për verifikim, që sigurojnë hyrjen në llogaritë *e-banking* të klientëve ose hyrjen në sistemet sensitive, janë të mbrojtura nga manipulimet dhe korruptimi. Këto manipulime duhet të jenë të zbulueshme dhe duhet të vendosen kontrolle gjurmimi për të dokumentuar përpjekje të tilla.

ii) Shtesat, fshirjet ose ndryshimet për individin, për agjentin ose për sistemin në bazën e të dhënave të verifikimit, janë të autorizuara vetëm nga një burim i verifikuar.

iii) Janë vendosur masat e duhura për të kontrolluar lidhjet e sistemit të *e-banking,* me qëllim që palë të treta të panjohura të mos kenë mundësi të zhvendosin ose të zëvendësojnë klientët e njohur.

iv) Sesionet e verifikuara të *e-banking* të mbeten të sigurta gjatë gjithë zgjatjes së seancës ose në rast të një gabimi sigurie, sistemi kërkon riverifikimin.

Neni 14
Verifikimi i transaksioneve

Bankat duhet të përdorin metoda të verifikimit të transaksionit, të cilat nxisin njohjen reale të fakteve dhe vendosin përgjegjësitë për transaksionet e *e-banking*.

Bankat duhet të bëjnë përpjekje të arsyeshme, në përputhje me tipin e transaksionit *e-banking* dhe vlerën që ai ka ose mund të ketë për bankën, për t'u siguruar që:

a) Sistemet e *e-banking* janë projektuar për të reduktuar mundësinë që përdoruesit e autorizuar do të ndërmarrin transaksione të pamenduara dhe që klientët i kuptojnë plotësisht rreziqet që lidhen me transaksionet që ata ndërmarrin.

b) Të gjitha palët në transaksion janë të verifikuara pozitivisht dhe është kryer kontrolli për kanalet e verifikimit.

c) Të dhënat e transaksioneve financiare janë të mbrojtura nga modifikimet dhe nëse ndodhin, këto modifikime të jenë të kapshme.

Neni 15
Ndarja e detyrave

Bankat duhet të sigurojnë që janë vendosur masat e përshtatshme për ndarjen e duhur të detyrave brenda sistemeve, bazave të të dhënave dhe aplikimeve të *e-banking*.

Praktikat për vendosjen dhe për ruajtjen e ndarjes së detyrave brenda ambientit të *e-banking* përfshijnë:

a) proceset dhe sistemet, të cilat sigurojnë që asnjë punonjës/dhënës i shërbimit nga jashtë të mund të hyjë, të autorizojë dhe të plotësojë një transaksion;
b) ndarjen e detyrave midis atyre që organizojnë të dhënat statike (përfshirë përmbajtjen e faqes së *web*-it) dhe atyre që janë përgjegjës për verifikimin e integritetit të tyre;
c) testimin e sistemeve *e-banking* duke siguruar që ndarja e detyrave nuk mund të kapërcehet ose të anashkalohet;
d) ndarjen e detyrave midis atyre që zhvillojnë dhe atyre që administrojnë sistemet e e-banking.

Neni 16
Kontrolli dhe e drejta e hyrjes në sistem

Bankat duhet të sigurojnë që janë vendosur kontrollet për autorizimet dhe privilegjet për të drejtat e hyrjes në sisteme, në bazën e të dhënave dhe aplikimet e *e-banking*.

Me qëllim që të ruajnë ndarjen e detyrave, bankat duhet të kontrollojnë në mënyrë strikte privilegjet e autorizimit dhe të hyrjes. Në sistemet e *e-banking*, autorizimet dhe të drejtat për hyrje mund të vendosen në mënyrë të centralizuar ose të shpërndarë brenda një banke dhe në përgjithësi janë të ruajtura në bazat e të dhënave. Mbrojtja e ketyre bazave të të dhënave nga ndërhyrja e të tjerëve apo korruptimi, është themelore për kontrollin e autorizuar dhe efektiv.

Neni 17
Mbrojtja e integritetit

Bankat duhet të sigurojnë që janë vendosur masat e duhura për të mbrojtur integritetin e të dhenave të transaksioneve, të regjistrimeve dhe të informacioneve të *e-banking*.

a) Bankat duhet të sigurojnë që janë vendosur masat e përshtatshme për të përcaktuar saktësinë, plotësinë dhe sigurinë e transaksioneve, të regjistrimeve dhe të informacionit të *e-banking* që transmetohet nëpërmjet internetit, rezident në bazën e brendshme të të dhënave të bankës, ose që transmetohet/ruhet nga një dhënës shërbimi i tretë në emër të bankës.
b) Praktikat për ruajtjen e integritetit të të dhënave brenda ambientit të *e-banking* përfshijnë:
    i) kryerjen e transaksioneve të *e-banking* në një mënyrë që i bën ato shumë rezistente ndaj ndërhyrjeve gjatë gjithë procesit;
    i) ruajtjen, aksesimin dhe modifikimin e regjistrimeve të *e-banking,* në një mënyrë që i bën ato shumë rezistente ndaj ndërhyrjeve;
    ii) projektimin e transaksionet të *e-banking* dhe të proceseve të mbajtjes së regjistrimeve, në një menyrë që e bën të pamundur shmangien e zbulimit të ndryshimeve të paautorizuara;
    iii) vendosjen e politikave të mjaftueshme të kontrollit të ndryshimeve, duke përfshirë procedurat e monitorimit dhe të testimit, që vendosen për t'u mbrojtur kundër ndryshimeve të sistemit të e-banking dhe që mund të kompromentojnë gabimisht kontrollet ose sigurinë e të dhënave;
    iv) zbulimin e ndërhyrjeve në transaksionet ose në regjistrimet e *e-banking* nëpërmjet procesimit të transaksionit, të funksioneve të monitorimit dhe të mbajtjes së regjistrimeve.

Neni 18
Kontrolli i transaksioneve *e-banking*

Bankat duhet të sigurohen që ekzistojnë kontrolle të sigurta për të gjitha transaksionet e *e-banking*.

Shpërndarja e shërbimeve financiare nëpërmjet internetit mund ta bëjë më të vështirë për bankat që të aplikojnë dhe të vënë në zbatim kontrollet e brendshme dhe të mbajnë gjurmimin e sigurtë të kontrollit, nëse këto masa nuk janë përshtatur për një mjedis *e-banking*. Në procesin e përcaktimit se ku duhet të kryhen gjurmimet e kontrollit, duhet të merren në konsideratë elementët e mëposhtëm të transaksioneve të *e-banking*:

a) hapja, modifikimi ose mbyllja e llogarisë së klientit;
b) pasojat financiare të transaksionit;
c) një autorizim i dhënë një klienti që kalon kufirin e lejuar;
d) një dhënie, një ndryshim ose një revokim i të drejtave dhe i privilegjeve për hyrjen në sisteme.

Neni 19
Ruajtja e informacionit

Bankat duhet të marrin masat e duhura për të ruajtur konfidencialitetin e informacionit themelor të *e-banking*. Masat e marra për ruajtjen e konfidencialitetit, duhet të jenë në përpjesëtim me ndjeshmërinë e informacionit që transmetohet dhe/ose ruhet në bazën e të dhënave.

Për këtë bankat duhet të sigurohen që:

a) të gjitha të dhënat dhe regjistrimet konfidenciale të bankës të jenë të arritshme vetëm nga individë, nga agjentë dhe nga sisteme të autorizuara dhe të vërtetuara;
b) të gjitha të dhënat konfidenciale të bankës, të ruhen në mënyrë të sigurtë dhe të mbrohen nga shikimi ose nga ndryshimi, gjatë transmetimit nëpërmjet rrjeteve publike, private ose të brendshme;
c) standardet dhe kontrollet e bankës për përdorimin dhe për mbrojtjen e të dhënave, të zbatohen edhe kur palët e treta kanë akses tek të dhënat nëpërmjet marrëdhënieve të burimit të jashtëm;
d) të gjitha hyrjet tek të dhënat e kufizuara të jenë të gjurmueshme dhe të kërkojnë konfirmim (të jenë të *log*-uara), edhe pas një numri të caktuar përpjekjesh jo të suksesshme për t'u loguar.

Neni 20
Informimi i klientëve

Bankat duhet të sigurohen që është dhënë informacioni i mjaftueshëm në *website,* për t'iu lejuar klienteve që të kenë një konkluzion të informuar mbi identitetin e bankës dhe statusin rregullator të saj, para se të hyjnë në transaksionet e *e-banking*.

Informacionet që banka duhet të sigurojë në *website*-in e saj janë:

a) emri i bankës dhe vendndodhja e zyrës qendrore të saj (dhe e zyrave lokale në qoftë se është e aplikueshme);
b) identiteti i autoritetit kryesor mbikëqyrës bankar, i cili është përgjegjës për mbikëqyrjen e zyrës qendrore të bankës;
c) mënyra si mund të kontaktojnë klientet me qendrën e shërbimit të klientit të bankës në lidhje me problemet e shërbimit, me ankesat, me keqpërdorimin e dyshimtë të llogarive etj.;
d) si mund të kenë klientët akses për informacionin mbi kompensimin e aplikueshëm, mbulimin e depozitave të siguruara dhe nivelin e mbrojtjes që këta përballojnë (ose lidhjet në website-et që japin një informacion të tillë);
e) informacione të tjera që mund të jenë të përshtatshme ose që kërkohen nga situata të vecanta.

Neni 21
Kërkesa në lidhje me fshehtësinë e klientit

Bankat duhet të marrin masat e duhura për të siguruar besnikërinë ndaj kërkesave të fshehtësisë

për klientin, të aplikueshme në juridiksionet në të cilat banka ofron produktet dhe shërbimet e *e-banking*.

Bankat duhet të bëjnë përpjekje të arsyeshme për t'u siguruar që:

a) politikat dhe standardet e fshehtësisë së klientit të bankës marrin parasysh përputhshmërinë me të gjitha ligjet dhe rregulloret për fshehtësinë, në juridiksionin në të cilin ajo ofron produktet dhe sherbimet e *e-banking;*

b) klientet janë njohur me politikat dhe me çështjet që lidhen me fshehtësinë në lidhje me përdorimin e produkteve dhe të shërbimeve të *e-banking*;

c) klientët mund të heqin dorë nga lejimi i bankës që të ndajë me palë të treta për qëllime *cross-marketing* informacionin mbi kërkesat, mbi interesat, mbi pozitën financiare ose veprimtarinë bankare personale të klientit;

d) të dhënat për klientin nuk përdoren për qëllime të tjera, përvec atyre që janë lejuar specifikisht ose të cilat janë lejuar prej klientit;

e) standardet e bankës për përdorimin e të dhënave të klientëve duhet të zbatohen edhe kur palët e treta kanë akses në të dhënat e klientit nëpërmjet marrëdhënieve me burime të jashtme.

Neni 22
Sigurimi i vazhdimësisë së aktiviteteve *e-banking*

Bankat duhet të kenë kapacitete efektive, të sigurojnë vazhdimësi të biznesit dhe procese efektive të planifikimit të rezervave, për të ndihmuar në sigurimin e disponueshmërisë së sistemeve dhe të shërbimeve të *e-banking*.

a) Për të mbrojtur bankat kundrejt rrezikut të biznesit, rrezikut ligjor dhe atij reputacional, shërbimet e *e-banking* duhet të kryhen në mënyrë të vazhdueshme dhe t'i përgjigjen në kohë pritjeve të klientit.

b) Për të arritur këtë, banka duhet të ketë aftësinë të japë shërbimet *e-banking* tek përdoruesit e fundit, si nga burimet parësore (si sistemet dhe aplikimet e brendshme të bankës) ashtu edhe nga ato dytësore (si: sistemet dhe aplikimet e ofruesve të shërbimit).

Për t'iu ofruar klientëve vazhdimësinë e shërbimeve të *e-banking* që ata presin, bankat duhet të sigurohen që:

d) kapacitetet aktuale dhe zhvillimi i ardhshëm i sistemeve të *e-banking* janë analizuar në kuadër të zhvillimit të të gjitha tregjeve për tregtinë elektronike dhe të shkallës së pritshme të pranimit nga klienti të produkteve dhe të shërbimeve *e-banking;*

e) llogaritjet e kapacitetit të procesimit të transaksioneve të *e-banking,* janë vërtetuar, janë testuar (stress tested) dhe janë rishikuar periodikisht;

f) planet për vazhdimësinë e veprimtarisë normale për sistemet dhe procesimet kritike të *e-banking,* janë në fuqi dhe të testuara rregullisht.

Neni 23
Administrimi i ngjarjeve të papritura

Bankat duhet të kenë plane të përshtatshme në përgjigje të incidenteve, për të administruar, për të mbajtur dhe për të minimizuar problemet që dalin nga ngjarjet e papritura (duke përfshirë goditjet e brendshme dhe të jashtme), që mund të vështirësojnë ofrimin e sistemeve dhe të shërbimeve të *e-banking*.

Për të siguruar një reagim efektiv ndaj ngjarjeve të parashikuara, bankat duhet të përgatisin:

a) planet e reagimit ndaj ngjarjeve të parashikuara, për të adresuar rivendosjen në punë të sistemeve dhe të shërbimeve të *e-banking*. Analiza e skenarëve duhet të marrë në konsideratë mundësinë e ndodhjes së rrezikut dhe ndikimin e tij tek banka. Sistemet e *e-banking* që shërbehen nga ofrues të jashtëm, duhet të jenë pjesë integrale e këtyre planeve;

b) mekanizmat për të identifikuar një incident apo një krizë sapo të ndodhë, për të vlerësuar materialitetin e tyre dhe për të kontrolluar rrezikun e reputacionit që lidhet me ndonjë ndërprerje në shërbim;

c) një strategji komunikimi për të adresuar mjaftueshmërisht shqetësimet e tregjeve te jashtme dhe të mjeteve të komunikimit, që mund të dalin në rast të dështimeve të sistemeve të *e-banking;*

d) një proces të qartë për njoftimin e autoriteteve mbikëqyrëse, në rastet e thyerjeve materiale të sigurisë ose të ndodhjes së incidenteve të ndërprerjeve;

e) skuadrat e reagimit ndaj incidenteve, të cilat duhet të jenë të trainuara në mënyrë të mjaftueshme dhe të kenë autoritetin për të vepruar në emergjencë, për të analizuar sistemet e reagimit/zbulimit të incidenteve dhe për të interpretuar domethënien e rezultatit;

f) një zinxhir të qartë komandash, që përfshin si operacionet e brendshme ashtu edhe ato nga burimet e jashtme, për t'u siguruar që janë marrë veprimet e menjëhershme sipas rëndësisë së incidentit. Shkallëzimi dhe procedurat e komunikimit të brendshëm, duhet të përcaktohen dhe të përfshijnë njoftimin e këshillit drejtues kur është e nevojshme;

g) një proces që të sigurojë që të gjitha palët relevante të jashtme, duke përfshirë klientët e bankës, korrespondentët dhe mjetet e komunikimit, janë informuar në kohë dhe në mënyrën e duhur për ndërprerjet e *e-banking* dhe zhvillimet e rifillimit të veprimtarisë;

h) një proces për grumbullimin dhe ruajtjen e evidencës së ligjshme, për të lehtësuar rishikimet e nevojshme pas ndodhjes të ndonjë incidenti të *e-banking,* si edhe për të ndihmuar në ngritjen e akuzës ndaj ndërhyrësve të paligjshëm.

Neni 24
Penalizimet

Mosrespektimi i kërkesave të kësaj rregulloreje, përbën shkelje të kushteve për kryerjen e veprimtarisë bankare në mënyrë të shëndoshë dhe të sigurtë dhe trajtohet sipas përcaktimeve të nenit 44, të ligjit nr. 8365, datë 02.07.1998, "Për bankat në Republikën e Shqipërisë".

Neni 25
Kalimtare

Bankat që kanë filluar kryerjen e transaksioneve *e-banking* para hyrjes në fuqi të kësaj rregulloreje, duhet që brenda një periudhe gjashtëmujore nga hyrja në fuqi e saj, të plotësojnë kushtet e parashikuara në këtë rregullore.

Neni 26
Hyrja në fuqi

Kjo rregullore hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare të Republikës së Shqipërisë.

KRYETARI I KËSHILLIT MBIKËQYRËS
Adrian FULLANI