

VENDIM
Nr. 30, datë 1.7.2026

**PËR MIRATIMIN E RREGULLORES “PËR QËNDRUESHMËRINË
OPERACIONALE DIGJITALE”**

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

VENDOSI:

1. Të miratojë rregulloren “Për qëndrueshmërinë operationale digjitale”, sipas tekstit bashkëlidhur këtij vendimi.
 2. Ngarkohen subjektet e rregullores për zbatimin e këtij vendimi.
 3. Ngarkohet Departamenti i Mbikëqyrjes së Bankës së 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.
 5. Me hyrjen në fuqi të kësaj rregulloreje, shfuqizohet udhëzimi “Për raportimin e incidenteve madhore”, miratuar me vendimin nr. 10, datë 7.2.2024, të Këshillit Mbikëqyrës të Bankës së Shqipërisë.
- Ky vendim hyn në fuqi 15 ditë pas botimit në Fletoren Zyrtare.

KRYETAR
Gent Sejko

RREGULLORE¹

¹ Kjo rregullore përaftron aktet e mëposhtme të Bashkimit Evropian:

PËR QËNDRUESHMËRINË OPERACIONALE DIGJITALE

KREU I KËRKESA TË PËRGJITHSHME

Neni 1

Objekti

1. Objekti i kësaj rregulloreje është përcaktimi i kërkesave të unifikuara në lidhje me sigurinë e rrjetit dhe sistemeve të informacionit që mbështesin veprimtarinë e subjekteve financiare, me qëllim arritjen e një niveli të lartë të përbashkët të qëndrueshmërisë operationale digjitale, për:

a) kërkesat e zbatueshme për subjektet financiare në lidhje me:

i. administrimin e rrezikut të teknologjisë së informacionit dhe komunikimit (TIK);
ii. raportimin e incidenteve madhore të lidhura me TIK-un dhe njoftimin mbi baza vullnetare për kërcënimet kibernetike të rëndësishme, në Bankën e Shqipërisë;

iii. raportimin në Bankën e Shqipërisë, të incidenteve madhore operationale ose të sigurisë të lidhura me pagesat, nga subjektet financiare të parashikuara në shkronjat “a” deri në “d” të pikës 1 të nenit 2 të kësaj rregulloreje;

iv. testimin e qëndrueshmërisë operationale digjitale;

v. shkëmbimin e informacionit dhe inteligjencës, në lidhje me kërcënimet dhe vulnerabilitetet kibernetike;

vi. masat për një administrim të shëndoshë nga subjektet financiare të rrezikut të TIK-ut nga palët e treta;

b) kërkesat në lidhje me marrëveshjet kontraktuale të lidhura ndërmjet ofruesve të shërbimeve të palëve të treta të TIK-ut dhe subjekteve financiare;

c) rregullat për ngritjen dhe funksionimin e kuadrit të mbikëqyrjes për ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, kur ofrojnë shërbime për subjektet financiare;

d) rregullat për bashkëpunimin ndërmjet Bankës së Shqipërisë dhe autoriteteve të tjera përgjegjëse, si dhe rregullat për mbikëqyrjen dhe ndjekjen e zbatimit nga Banka e Shqipërisë, të kërkesave të kësaj rregulloreje.

- Rregulloren (BE) 2022/2554 e Parlamentit Evropian dhe të Këshillit, e datës 14 dhjetor 2022, për qëndrueshmërinë operationale digjitale të sektorit financiar dhe për ndryshimin e Rregulloreve (KE) nr. 1060/2009, (BE) Nr. 648/2012, (BE) nr. 600/2014, (BE) nr. 909/2014 dhe (BE) 2016/1011.

- Rregulloren e Deleguar të Komisionit (BE) 2024/1772 që plotëson Rregulloren (BE) 2022/2554 në lidhje me standardet teknike, rregullatore që specifikojnë kriteret për klasifikimin e incidenteve të lidhur me TIK-un dhe kërcënimet kibernetike, duke caktuar kufijtë e materialitetit dhe specifikuar detajet e raporteve të incidenteve madhore.

- Rregulloren e Deleguar të Komisionit (BE) 2024/1773 që plotëson Rregulloren (BE) 2022/2554 në lidhje me standardet teknike, rregullatore që specifikojnë përmbajtjen e detajuar të politikës për marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut.

- Rregulloren e Deleguar të Komisionit (BE) 2025/301 që plotëson Rregulloren (BE) 2022/2554 në lidhje me standardet teknike, rregullatore që specifikojnë përmbajtjen dhe afatet kohore për njoftimin fillestar dhe raportin e ndërmjetëm dhe përfundimtar mbi incidentet madhore të lidhur me TIK-un dhe për përmbajtjen e njoftimit vullnetar të kërcënimeve kibernetike të rëndësishme.

- Rregulloren Implementuese të Komisionit (BE) 2025/302 që përcakton standardet teknike implementuese për zbatimin e Rregulloreve (BE) 2022/2554 në lidhje me format, formularët dhe procedurat standarde për subjektet financiare për raportimin e incidenteve madhore të lidhur me TIK-un dhe për njoftimin e kërcënimeve kibernetike të rëndësishme.

- Udhëzimet e Përbashkëta 2024 34 mbi vlerësimin e kostove të agreguara vjetore dhe humbjeve të shkaktuara nga incidentet madhore të lidhura me TIK-un, sipas Rregulloreve (BE) 2022/2554.

Neni 2 **Subjektet**

1. Subjekte të kësaj rregulloreje janë:
 - a) bankat, të cilat në vijim do të referohen si institucione të kreditit, sipas parashikimeve në legjislacionin e zbatueshëm për bankat;
 - b) institucionet e pagesave, përfshirë edhe ato që përjashtohen sipas parashikimeve të nenit 27 të ligjit “Për shërbimet e pagesave”;
 - c) ofruesit e shërbimit të informimit të llogarisë, siç parashikohen në nenit 28 të ligjit “Për shërbimet e pagesave”;
 - d) institucionet e parasë elektronike, përfshirë edhe ato që përjashtohen sipas parashikimeve të ligjit “Për shërbimet e pagesave”;
 - e) emetuesit e tokenave të aseteve dhe emetuesit e tokenave të parasë elektronike, sipas parashikimeve të legjislacionit për tregjet e kryptoaseteve;
 - f) ofruesit e shërbimeve të palëve të treta të TIK-un.
2. Për qëllime të kësaj rregulloreje, subjektet e parashikuara në shkronjat “a” deri në “e” të pikës 1 të këtij neni, do të referohen në vijim në këtë rregullore, me termin “subjekte financiare”.
3. Kjo rregullore nuk zbatohet për institucionet e shërbimeve postare të parashikuara në nenin 2(5), pika 3, të Direktivës (BE) 2013/36.
4. Banka e Shqipërisë mund të përjashtojë nga fusha e zbatimit të kësaj rregulloreje subjektet e parashikuara në nenin 2 (5), pikat 4 deri në 23, të Direktivës (BE) 2013/36 që ndodhen brenda territorit të Republikës së Shqipërisë. Banka e Shqipërisë informon Komisionin Evropian kur vendos përjashtimin e një subjekti sipas kësaj pike, si dhe për çdo ndryshim pasues. Komisioni Evropian publikon informacionin në faqen e tij të internetit ose në mënyra të tjera lehtësisht të aksesueshme.

Neni 3 **Baza ligjore**

Kjo rregullore nxirret në bazë dhe për zbatim të nenit 3, pika 3, nenit 12, shkronja “a”, dhe nenit 43, shkronja “c”, të ligjit nr. 8269, datë 23.12.1997, “Për Bankën e Shqipërisë”, i ndryshuar; nenit 58 të ligjit nr. 9662, datë 18.12.2006, “Për bankat në Republikën e Shqipërisë”, i ndryshuar, dhe të nenit 88 të ligjit nr. 55/2020, datë 30.4.2020, “Për shërbimet e pagesave”.

Neni 4 **Përkufizime**

1. Termat e përdorur në këtë rregullore kanë të njëjtin kuptim me ata të përdorur në ligjin nr. 9662, datë 18.12.2006, “Për bankat në Republikën e Shqipërisë”, i ndryshuar (i cili për thjeshtësi në këtë rregullore do të quhet ligji “Për bankat”) dhe në ligjin nr. 55/2020, datë 30.4.2020, “Për shërbimet e pagesave” (i cili për thjeshtësi në këtë rregullore do të quhet ligji “Për shërbimet e pagesave”).
2. Përveç sa parashikohet në pikën 1 të këtij neni, për qëllime të zbatimit të kësaj rregulloreje, termat e mëposhtëm kanë këtë kuptim:
 - 1) “qëndrueshmëri operationale digjitale” – nënkupton aftësinë e një subjekti financiar për të ndërtuar, siguruar dhe rishikuar integritetin dhe besueshmërinë operationale, duke siguruar, drejtpërdrejt ose tërthorazi, nëpërmjet përdorimit të ofruesve të shërbimeve të palëve të treta të teknologjisë së informacionit dhe komunikimit (TIK), aftësitë e lidhura me TIK-un, të

nevojshme për të adresuar sigurinë e rrjetit dhe sistemeve të informacionit që përdor subjekti financiar dhe që mbështesin ofrimin e vazhdueshëm të shërbimeve financiare dhe cilësinë e tyre, përfshirë edhe gjatë ndërprerjeve;

2) “rrjet dhe sistem i informacionit” – është një rrjet dhe sistem informacioni, siç përcaktohet në nenin 5, pika 35, të ligjit 25/2024 “Për sigurinë kibernetike”;

3) “sistem i vjetër i TIK-ut (*legacy ICT system*)” - nënkupton një sistem TIK që ka arritur fundin e ciklit të tij jetësor, që nuk është më i përshtatshëm për përmirësime ose rregullime, për arsye teknologjike ose tregtare, ose që nuk mbështetet më nga ofruesi i tij ose nga një ofrues shërbimi i palëve të treta të TIK-ut, por që është ende në përdorim dhe mbështet funksionet e subjektit financiar;

4) “siguri e rrjetit dhe e sistemeve të informacionit” – nënkupton sigurinë e rrjetit dhe sistemeve të informacionit, siç përcaktohet në nenin 5, pika 42, të ligjit 25/2024, “Për sigurinë kibernetike”;

5) “rrezik i TIK” – nënkupton çdo rrethanë të identifikueshme në mënyrë të arsyeshme, në lidhje me përdorimin e rrjetit dhe sistemeve të informacionit, e cila, nëse materializohet, mund të rrezikojë sigurinë e rrjetit dhe sistemeve të informacionit, të çdo mjeti apo procesi të varur nga teknologjia, të operacioneve dhe proceseve, ose të ofrimit të shërbimeve, duke prodhuar efekte të kundërta në mjedisin digjital ose fizik;

6) “aset informacioni” – nënkupton një koleksion informacioni, të prekshëm ose të paprekshëm, që ia vlen të mbrohet;

7) “aset i TIK-ut” – nënkupton një aset *software* ose *hardware* në rrjetin dhe sistemet e informacionit të përdorur nga subjekti financiar;

8) “incident i lidhur me TIK-un” – nënkupton një ngjarje të vetme ose një seri ngjarjesh të lidhura, të paplanifikuara nga subjekti financiar, që kompromenton sigurinë e rrjetit dhe të sistemeve të informacionit, dhe që ka një ndikim negativ në disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave ose mbi shërbimet e ofruara nga subjekti financiar;

9) “incident madhor i lidhur me TIK-un” – nënkupton një incident të lidhur me TIK-un, që ka një ndikim negativ të lartë në rrjet dhe sistemet e informacionit që mbështesin funksionet kritike ose të rëndësishme të subjektit financiar;

10) “incident operacional ose i sigurisë i lidhur me pagesat” – është një ngjarje e vetme ose një seri ngjarjesh të lidhura, të paplanifikuara nga subjektet financiare të parashikuara në shkronjat “a” deri në “d” të pikës 1 të nenit 2 të kësaj rregulloreje, pavarësisht nëse është ose jo i lidhur me TIK-un, që ka një ndikim negativ në disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave të lidhura me pagesat ose mbi shërbimet e lidhura me pagesat, të ofruara nga subjekti financiar;

11) “incident madhor operacional ose i sigurisë i lidhur me pagesat” – nënkupton një incident operacional ose të sigurisë të lidhur me pagesat, që ka një ndikim negativ të lartë në shërbimet e lidhura me pagesat të ofruara nga subjekti financiar;

12) “kërcënim kibernetik” – ka të njëjtin kuptim siç përcaktohet në nenin 5, pika 16, të ligjit 25/2024 “Për sigurinë kibernetike”;

13) “kërcënim i rëndësishëm kibernetik” – është një kërcënim kibernetik, karakteristikat teknike të të cilit tregojnë se ka mundësinë që të rezultojë në një incident madhor të lidhur me TIK-un, ose në një incident madhor operacional ose të sigurisë të lidhur me pagesat;

14) “sulm kibernetik” – nënkupton një incident me synime keqdashëse të lidhur me TIK-un, të shkaktuar me anë të një përpjekjeje të kryer nga çdo aktor kërcënues, për të shkatërruar, ekspozuar, ndryshuar, çaktivizuar, vjedhur ose për të fituar akses të paautorizuar në një aset ose për të përdorur në mënyrë të paautorizuar një aset;

15) “inteligjencë kërcënimi” – nënkupton informacionin që është grumbulluar, transformuar, analizuar, interpretuar ose pasuruar për të ofruar kontekstin e nevojshëm për vendimmarrje dhe

për të mundësuar të kuptuarit e përshtatshëm dhe të mjaftueshëm, për zbutjen e efektit të një incidenti të lidhur me TIK-un, ose të një kërcënimi kibernetik, duke përfshirë detajet teknike të një sulmi kibernetik, personat përgjegjës për sulmin, mënyrën specifike që përdoret nga këta persona për të kryer sulmin, si dhe motivimet e tyre;

16) “vulnerabilitet” – nënkupton një dobësi, ndjeshmëri ose defekt të një aseti, sistemi, procesi ose kontrolli që mund të shfrytëzohet nga një kërcënim;

17) “testimi i depërtueshmërisë i udhëhequr nga kërcënim (TLPT)” – nënkupton një kuadër që imiton taktikat, teknikat dhe procedurat e aktorëve të kërcënimit në jetën reale, të perceptuar sikur paraqesin një kërcënim të vërtetë kibernetik, që ofron një test të kontrolluar, të porositur, të udhëhequr nga inteligjenca (ekip i kuq) të sistemeve kritike *live* të prodhimit të subjektit financiar;

18) “rrezik i TIK-ut i palës së tretë” – nënkupton rrezikun e TIK-ut që mund të lindë për një subjekt financiar, në lidhje me përdorimin e shërbimeve të TIK-ut të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut ose nga nënkontraktorë të këtyre të fundit, përfshirë edhe nëpërmjet marrëveshjeve me palët e treta (*outsourcing*);

19) “ofrues shërbimi i palëve të treta të TIK-ut” – nënkupton një kompani që ofron shërbime të TIK-ut;

20) “ofrues shërbimesh të TIK-ut brenda grupit” – nënkupton një kompani që është pjesë e një grupi financiar dhe që ofron kryesisht shërbime të TIK-ut për subjektet financiare brenda të njëjtit grup ose subjektet financiare që i përkasin së njëjtës skemë të mbrojtjes institucionale, duke përfshirë bankat apo institucionet financiare mëmë, filialet, degët ose subjektet e tjera që janë nën pronësi ose kontroll të përbashkët;

21) “shërbime të TIK-ut” – janë shërbimet digjitale dhe të të dhënave, të ofruara në mënyrë të vazhdueshme nëpërmjet sistemeve TIK-ut, për një ose më shumë përdorues të brendshëm ose të jashtëm, duke përfshirë *hardware* si shërbim dhe shërbimet e *hardware*, që përfshijn ofrimin e mbështetjes teknike nëpërmjet përditësimeve të *software* ose *firmware* nga ofruesi i *hardware*, duke përfshirë shërbimet tradicionale telefonike analoge;

22) “funksion kritik ose i rëndësishëm” – është një funksion, ndërprerja e të cilit do të dëmtojte materialisht performancën financiare të subjektit financiar, ose qëndrueshmërinë apo vazhdimësinë e shërbimeve dhe aktiviteteve të tij, ose performanca e ndërprerë, e mangët ose e dështuar e atij funksioni do të dëmtojte materialisht pajtueshmërinë e vazhdueshme të subjektit financiar me kushtet dhe detyrimet e përcaktuara për licencimin e tij, ose me detyrime të tjera sipas legjislacionit përkatës për subjektet financiare;

23) “ofrues kritik i shërbimeve të palëve të treta të TIK-ut” – nënkupton një ofrues të shërbimeve të palëve të treta të TIK-ut, të caktuar si kritik në përputhje me nenin 31 të Rregullores (BE) 2022/2554 dhe sipas parashikimeve të nenit 60 të kësaj rregulloreje;

24) “ofrues shërbimi i palëve të treta të TIK-ut i themeluar në një shtet tjetër” – nënkupton një ofrues shërbimi të palëve të treta të TIK-ut që është një person juridik i themeluar në një shtet tjetër dhe që ka lidhur një marrëveshje kontraktuale me një subjekt financiar për ofrimin e shërbimeve të TIK-ut;

25) “nënkontraktor i TIK-ut i themeluar në një shtet tjetër” – nënkupton një nënkontraktor TIK që është një person juridik i themeluar në një shtet tjetër dhe që ka lidhur një marrëveshje kontraktuale me një ofrues shërbimi të palëve të treta TIK, ose me një ofrues shërbimi të palës së tretë të TIK-ut, të vendosur në një shtet tjetër;

26) “rrezik i përqendrimit të TIK-ut” – nënkupton një ekspozim ndaj një ose disa ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut të lidhur, duke krijuar një shkallë varësie nga ofruesit e tillë, në mënyrë që mosdisponueshmëria, dështimi ose çdo lloj tjetër mungese i këtyre të fundit, mund të rrezikojë potencialisht aftësinë e një subjekti financiar, për të kryer funksione kritike ose të rëndësishme, ose për të vuajtur efekte të tjera negative, duke përfshirë humbje të mëdha ose cenimin e stabilitetit financiar të vendit;

27) “organ drejtues” – nënkupton organin ose organet e subjektit financiar, të cilët kanë përgjegjësinë për të vendosur/përcaktuar strategjinë, objektivat dhe drejtimin e përgjithshëm të subjektit financiar dhe për të mbikëqyrur dhe monitoruar vendimmarrjen e administratorëve dhe përfshijnë personat që drejojnë në mënyrë efektive veprimtarinë e subjektit financiar, ose që janë drejtues të funksioneve kryesore;

28) “mikrondërmarrje” – në kuptim të kësaj rregulloreje, nënkupton një subjekt financiar, i cili ka të punësuar më pak se 10 persona dhe xhiroja vjetore dhe/ose totali i bilancit të tij vjetor nuk tejkalon vlerën ekuivalente në Lek të 2 milionë eurove;

29) “ndërmarrje e vogël” – në kuptim të kësaj rregulloreje, nënkupton një subjekt financiar që ka të punësuar 10 ose më shumë persona, por më pak se 50 persona, dhe xhiroja vjetore dhe/ose një totali i bilancit të tij vjetor tejkalon vlerën ekuivalente në Lek të 2 milionë eurove, por nuk tejkalon vlerën ekuivalente në Lek të 10 milionë eurove;

30) “ndërmarrje e mesme” – në kuptim të kësaj rregulloreje, nënkupton një subjekt financiar që nuk është një ndërmarrje e vogël dhe që ka të punësuar më pak se 250 persona dhe një xhiro vjetore që nuk tejkalon vlerën ekuivalente në Lek të 50 milionë eurove dhe/ose një total bilanci vjetor që nuk tejkalon vlerën ekuivalente në Lek të 43 milionë eurove;

31) “EBA” (*European Banking Authority*) – është Autoriteti Bankar Evropian;

32) “EIOPA” (*European Insurance and Occupational Pensions Authority*) – është Autoriteti Evropian Mbikëqyrës për Sigurimet dhe Pensionet Profesionale;

33) “ECB” (*European Central Bank*) – është Banka Qendrore Evropiane;

34) “ESMA” (*European Securities and Markets Authority*) – është Autoriteti Evropian Mbikëqyrës për Titujt dhe Tregjet e Kapitalit;

35) “ESA” – janë Autoritetet Mbikëqyrëse Evropiane si EBA-ja, ESMA dhe EIOPA;

36) “ENISA” – është Agjencia për Sigurinë Kibernetike e Bashkimit Evropian;

37) “Mbikëqyrës Kryesor” (*Lead Overseer*) – është Autoriteti Mbikëqyrës Evropian i caktuar në përputhje me nenin 31(1), shkronja “b”, të Rregullores (BE) 2022/2554 dhe sipas parashikimeve të nenit 60 të kësaj rregulloreje;

38) “Komiteti i Përbashkët (*Joint Committee*)” – nënkupton komitetin e referuar në nenin 54 të Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010.

Neni 5

Parimi i proporcionalitetit

1. Subjektet financiare zbatojnë kërkesat e kreut II të kësaj rregulloreje, në përputhje me parimin e proporcionalitetit, duke konsideruar madhësinë dhe profilin e rrezikut, si dhe natyrën, shkallën dhe kompleksitetin e shërbimeve, aktivitetit dhe operacioneve të tyre.

2. Përveç sa parashikohet në pikën 1 të këtij neni, zbatimi i kërkesave të krerëve III, IV dhe nënkreut I të kreut V të kësaj rregulloreje nga subjektet financiare, do të jetë në proporcion me madhësinë dhe profilin e rrezikut, si dhe me natyrën, shkallën dhe kompleksitetin e shërbimeve, aktivitetit dhe operacioneve të tyre, siç përcaktohet në kërkesat përkatëse të atyre krerëve.

3. Banka e Shqipërisë merr në konsideratë zbatimin e parimit të proporcionalitetit nga subjektet financiare, kur shqyrton konsistencën e kuadrit të administrimit të rrezikut të TIK-ut, në bazë të raporteve të paraqitura nga subjektet me kërkesë të Bankës së Shqipërisë, siç përcaktohet në nenin 7, pika 6, dhe nenin 17, pika 3, të kësaj rregulloreje.

KREU II

ADMINISTRIMI I RREZIKUT TË TIK-ut

NËNKREU I

QEVERISJA DHE ORGANIZIMI I SUBJEKTEVE FINANCIARE

Neni 6 Qeverisja dhe organizimi

1. Subjektet financiare krijojnë sistemin e brendshëm të qeverisjes dhe të kontrollit që siguron një administrim efektiv dhe të kujdesshëm të të gjitha rreziqeve të TIK-ut, në përputhje me nenin 7, pikat 4 dhe 5, të kësaj rregulloreje, me qëllim sigurimin e një niveli të lartë të qëndrueshmërisë operacionale digjitale. Ky sistem duhet t'u referohet dhe të përshtatet me standardet më të mira të fushës së teknologjisë së informacionit dhe sigurisë së informacionit.

2. Organi drejtues i subjektit përcakton, miraton, mbikëqyr dhe është përgjegjës për zbatimin e të gjitha marrëveshjeve që lidhen me sistemin e administrimit të rrezikut të TIK-ut, të parashikuar në nenin 7, pika 1, të kësaj rregulloreje.

3. Për qëllime të pikës 2 të këtij neni, organi drejtues:

a) ka përgjegjësinë përfundimtare për administrimin e rrezikut të TIK-ut të subjektit financiar;

b) harton politika që sigurojnë standarde të larta të disponueshmërisë, autenticitetit, integritetit dhe konfidencialitetit të të dhënave;

c) përcakton role dhe përgjegjësi të qarta për të gjitha funksionet që lidhen me TIK-un dhe krijojnë sisteme të përshtatshme qeverisëse për të siguruar një komunikim, bashkëpunim dhe koordinim efektiv dhe në kohë, midis këtyre funksioneve;

d) ka përgjegjësinë për përcaktimin dhe miratimin e strategjisë për qëndrueshmërinë operacionale digjitale, siç parashikohet në nenin 7, pika 9, të kësaj rregulloreje, përfshirë edhe përcaktimin e nivelit të duhur të tolerancës ndaj rrezikut të TIK-ut të subjektit financiar, siç parashikohet në nenin 7, pika 9, shkronja "b", të kësaj rregulloreje;

e) miraton, mbikëqyr (*oversee*) dhe rishikon periodikisht zbatimin e politikës së vazhdimësisë së biznesit të TIK-ut dhe planit të rimëkëmbjes nga fatkeqësitë e TIK-ut të subjektit financiar, të parashikuara përkatësisht në pikat 1 dhe 3 të nenit 12 të kësaj rregulloreje, që mund të përshtatet si një politikë e veçantë, pjesë integrale e politikës së përgjithshme të vazhdimësisë së biznesit të subjektit financiar dhe planeve të rimëkëmbjes të tij;

f) miraton dhe rishikon periodikisht planet e auditit të brendshëm të subjektit financiar për TIK, auditimet e TIK-ut dhe modifikimet materiale të tyre;

g) shpërndan dhe rishikon periodikisht buxhetin e duhur për të përmbushur nevojat e subjektit financiar për qëndrueshmërinë operacionale digjitale të tij, në lidhje me të gjitha llojet e burimeve, duke përfshirë programet e ndërgjegjësimit për sigurinë e TIK-ut, trajnimin mbi qëndrueshmërinë operacionale digjitale të parashikuar në nenin 15, pika 7, të kësaj rregulloreje, si dhe për aftësitë në fushën e TIK-ut për të gjithë stafin e subjektit financiar;

h) miraton dhe rishikon periodikisht politikën e subjektit financiar për marrëveshjet në lidhje me përdorimin e shërbimeve të TIK-ut të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut;

i) krijojnë kanale raportimi në nivel subjekti, për të qenë të informuar siç duhet, për:

i. marrëveshjet e lidhura me ofruesit e shërbimeve të palëve të treta të TIK-ut për përdorimin e shërbimeve të TIK-ut;

ii. çdo ndryshim material përkatës të planifikuar, në lidhje me ofruesit e shërbimeve të palëve të treta të TIK-ut;

iii. ndikimin e mundshëm të këtyre ndryshimeve në funksionet kritike ose të rëndësishme që janë subjekt i atyre marrëveshjeve, duke përfshirë një përmbledhje të analizës së rrezikut, për të vlerësuar ndikimin e këtyre ndryshimeve, për incidentet madhore të lidhura me TIK-un dhe ndikimin e tyre, si dhe për reagimin, rimëkëmbjen dhe masat korrigjuese të subjektit financiar.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, caktojnë një funksion ose person përgjegjës për monitorimin e marrëveshjeve të lidhura me ofruesit e shërbimeve të

palëve të treta të TIK-ut për përdorimin e shërbimeve të TIK-ut, ose caktojnë një anëtar të drejtimit të lartë, si përgjegjës për mbikëqyrjen e ekspozimit përkatës ndaj rrezikut dhe të dokumentacionit përkatës.

5. Anëtarët e organit drejtues të subjektit financiar duhet të trajnohen rregullisht për t'u përditësuar me njohuritë dhe aftësitë e përshtatshme, për të kuptuar dhe vlerësuar rrezikun e TIK-ut dhe ndikimin e tij në veprimtarinë e subjektit financiar, në përputhje edhe me nivelin e rrezikut të TIK-ut që duhet të administrohet.

NËNKREU II SISTEMI I ADMINISTRIMIT TË RREZIKUT TË TIK-ut

Neni 7

Sistemi i administrimit të rrezikut të TIK-ut

1. Subjektet financiare krijojnë një sistem të shëndoshë, gjithëpërfshirës dhe të mirë-dokumentuar të administrimit të rrezikut të TIK-ut, si pjesë të sistemit të përgjithshëm të administrimit të rrezikut të subjektit, i cili iu mundëson adresimin/administrimin e rrezikut të TIK-ut, në mënyrë të shpejtë, efikase dhe gjithëpërfshirëse, si dhe sigurimin e një niveli të lartë të qëndrueshmërisë operacionale digjitale.

2. Sistemi i administrimit të rrezikut të TIK-ut, i parashikuar në pikën 1 të këtij neni, përfshin strategjitë, politikat, procedurat, protokollet e TIK-ut dhe mekanizmat e nevojshme për të mbrojtur në mënyrë të duhur dhe efektive të gjitha asetet e informacionit dhe asetet e TIK-ut, duke përfshirë programet dhe pajisjet kompjuterike, serverët, si dhe për të mbrojtur të gjithë komponentët dhe infrastrukturat fizike përkatëse, të tilla si: ambientet, qendrat e të dhënave dhe zonat e caktuara të ndjeshme (sensitive), për të siguruar që të gjitha asetet e informacionit dhe asetet e TIK-ut janë të mbrojtura në mënyrë të përshtatshme nga rreziqet, duke përfshirë edhe nga dëmtimi dhe aksesit ose përdorimi i paautorizuar.

3. Subjektet financiare, në përputhje me sistemin e administrimit të rrezikut, minimizojnë efektet e rrezikut të TIK-ut, duke hartuar strategji, politika, procedura, protokolle të TIK-ut dhe mekanizma të përshtatshme. Subjektet i paraqesin Bankës së Shqipërisë, me kërkesën e kësaj të fundit, një informacion të plotë dhe të përditësuar mbi rreziqet e TIK-ut dhe mbi sistemin e administrimit të rrezikut të TIK-ut.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, i caktojnë funksionit të kontrollit, përgjegjësinë për administrimin dhe mbikëqyrjen e rrezikut të TIK-ut dhe sigurojnë një nivel të përshtatshëm pavarësie të këtij funksioni, për të shmangur konfliktin e interesit.

5. Subjektet financiare sigurojnë ndarjen e duhur dhe pavarësinë midis funksioneve të administrimit të rrezikut të TIK-ut, funksioneve të kontrollit dhe funksioneve të auditit të brendshëm, sipas modelit të tri linjave të mbrojtjes.

6. Sistemi i administrimit të rrezikut të TIK-ut dokumentohet dhe rishikohet të paktën një herë në vit, ose në mënyrë periodike për mikrondërmarrjet, dhe në çdo rast kur ndodhin incidente madhore të lidhura me TIK-un, si dhe në përputhje me rekomandimet mbikëqyrëse ose konkluzionet që rrjedhin nga testimi i qëndrueshmërisë operacionale digjitale ose nga proceset e kontrollit. Sistemi i administrimit të rrezikut të TIK-ut duhet të përmirësohet vazhdimisht në bazë të mësimave të nxjerra nga zbatimi dhe monitorimi. Subjektet i paraqesin Bankës së Shqipërisë, me kërkesën e kësaj të fundit, një raport mbi rishikimin e sistemit të administrimit të rrezikut të TIK-ut.

7. Sistemi i administrimit të rrezikut të TIK-ut të subjekteve financiare, me përjashtim të mikrondërmarrjeve, do të jetë subjekt i auditit të brendshëm në mënyrë të rregullt, në përputhje me planin e auditit të brendshëm të subjektit. Punonjësit e njësisë së auditit të brendshëm duhet të zotërojnë njohuri, aftësi dhe ekspertizë të mjaftueshme për rrezikun e TIK-ut, si dhe pavarësinë e duhur. Frekuenca dhe fokusi i auditimeve të TIK-ut duhet të jetë në përputhje me rrezikun e TIK-ut të subjektit financiar.

8. Bazuar në gjetjet e auditit të brendshëm, subjektet financiare krijojnë një proces formal për ndjekjen e gjetjeve, duke përfshirë rregullat për verifikimin në kohë dhe korrigjimin e gjetjeve kritike të auditit të brendshëm në lidhje me TIK-un.

9. Sistemi i administrimit të rrezikut të TIK-ut përfshin një strategji të qëndrueshmërisë operacionale digjitale, që përcakton se si zbatohet ky sistem i administrimit të rrezikut. Për këtë qëllim, strategjia e qëndrueshmërisë operacionale digjitale do të përfshijë metodat për të adresuar rrezikun e TIK-ut dhe për të realizuar objektivat specifike të TIK-ut, duke:

a) shpjeguar se si sistemi i administrimit të rrezikut të TIK-ut mbështet strategjinë dhe objektivat e veprimtarisë së subjektit financiar;

b) përcaktuar nivelin e tolerancës ndaj rrezikut për rrezikun e TIK-ut, në përputhje me oreksin për rrezik të subjektit, dhe duke analizuar tolerancën ndaj ndikimit të ndërprerjeve të TIK-ut;

c) vendosur objektiva të qartë të sigurisë së informacionit, përfshirë treguesit kyç të performancës dhe metrikat kyçe të rrezikut;

d) shpjeguar arkitekturën e referencës së TIK-ut dhe çdo ndryshim të nevojshëm për të arritur objektivat specifike të subjektit;

e) përshkruar mekanizmat e ndryshëm të krijuar nga subjekti, për të zbuluar incidentet e lidhura me TIK-un, për të parandaluar dhe për t'u mbrojtur nga efektet e tyre;

f) evidentuar situatën aktuale të qëndrueshmërisë operacionale digjitale, bazuar në numrin e incidenteve madhore të raportuara të lidhura me TIK-un dhe efektivitetin e masave parandaluese të ndërmarra;

g) zbatuar testimin e qëndrueshmërisë operacionale digjitale, në përputhje me kreun IV të kësaj rregulloreje;

h) planifikuar një strategji komunikimi në rast incidentesh të lidhura me TIK-un, publikimi i të cilave kryhet në përputhje me nenin 16 të kësaj rregulloreje.

10. Subjektet financiare, në kuadër të strategjisë së qëndrueshmërisë operacionale digjitale të parashikuar në pikën 9 të këtij neni, mund të përcaktojnë një strategji gjithëpërfshirëse të TIK-ut me shumë shitës (*multivendor strategy*), në nivel grupi ose subjekti, që paraqet varësitë kryesore nga ofruesit e shërbimeve të palëve të treta të TIK-ut dhe që shpjegon arsyetimin për prokurimin e disa ofruesve të shërbimeve të palëve të treta.

11. Subjektet financiare, në përputhje me kërkesat përkatëse ligjore e nënligjore për marrëveshjet me të tretët, mund të transferojnë detyrimin për verifikimin e përputhshmërisë me kërkesat e administrimit të rrezikut të TIK-ut, te subjekte të tjera brenda grupit ose palë të treta të jashtme. Në rastin e këtij transferimi, subjekti financiar mbetet plotësisht përgjegjës për verifikimin e përputhshmërisë me kërkesat e administrimit të rrezikut të TIK-ut.

Neni 8

Sistemet, protokollet dhe mekanizmat e TIK-ut

1. Subjektet financiare, për të adresuar dhe administruar rrezikun e TIK-ut, përdorin dhe mbajnë sisteme, protokolle dhe mekanizma të përditësuara të TIK-ut, të cilat:

a) janë të përshtatshme për madhësinë e operacioneve që mbështesin zhvillimin e veprimtarisë të tyre, në përputhje me parimin e proporcionalitetit të parashikuar në nenin 5 të kësaj rregulloreje;

- b) janë të besueshme;
- c) kanë kapacitet të mjaftueshëm për të përpunuar me saktësi të dhënat e nevojshme për kryerjen e aktiviteteve dhe ofrimin e shërbimeve në kohë, dhe për t'u marrë me urdhrat, mesazhet ose vëllimet e transaksioneve gjatë kohës së pikut, sipas nevojës, përfshirë edhe rastet e prezantimit të teknologjive të reja;
- d) janë teknologjikisht fleksibël, për t'u përballur në mënyrë të përshtatshme me nevojat shitesë të përpunimit të informacionit, siç kërkohet në kushte të stresuara të tregut ose në situata të tjera të pafavorshme.

Neni 9 **Identifikimi**

1. Si pjesë të sistemit të administrimit të rrezikut të TIK-ut të parashikuar në nenin 7, pika 1, të kësaj rregulloreje, subjektet financiare identifikojnë, klasifikojnë dhe dokumentojnë në mënyrë të përshtatshme, të gjitha funksionet e biznesit, rolet dhe përgjegjësitë e mbështetura nga TIK-u, asetet e informacionit dhe asetet e TIK-ut që mbështesin këto funksione, si dhe rolet dhe ndërvarësitë në lidhje me rrezikun e TIK-ut. Subjektet financiare rishikojnë sipas nevojës dhe të paktën çdo vit, përshtatshmërinë e këtij klasifikimi dhe të çdo dokumentacioni përkatës.

2. Subjektet financiare identifikojnë në mënyrë të vazhdueshme, të gjitha burimet e rrezikut të TIK-ut, në veçanti ekspozimin ndaj rrezikut drejt dhe nga subjektet e tjera financiare, dhe vlerësojnë kërcënimet kibernetike dhe vulnerabilitetet e TIK-ut që lidhen me funksionet e tyre të biznesit të mbështetura nga TIK-u, me asetet e informacionit dhe me asetet e TIK-ut. Subjektet financiare rishikojnë në baza të rregullta dhe të paktën çdo vit, skenarët e rrezikut që ndikojnë në to.

3. Subjektet financiare, me përjashtim të mikrondërmarrjeve, kryejnë një vlerësim të rrezikut, për çdo ndryshim të rëndësishëm në infrastrukturën e rrjetit dhe sistemeve të informacionit, në proceset ose procedurat që prekin funksionet e tyre të biznesit të mbështetura nga TIK-u, asetet e informacionit ose asetet e TIK-ut.

4. Subjektet financiare identifikojnë të gjitha asetet e informacionit dhe asetet e TIK-ut, duke përfshirë edhe faqet në distancë (*remote sites*), burimet e rrjetit dhe pajisjet kompjuterike (*hardware*), dhe caktojnë ato asete që konsiderohen si kritike. Subjektet financiare hartojnë konfigurimin e aseteve të informacionit dhe aseteve të TIK-ut, si dhe lidhjet dhe ndërvarësinë ndërmjet aseteve të ndryshme të informacionit dhe të TIK-ut.

5. Subjektet financiare identifikojnë dhe dokumentojnë të gjitha proceset që varen nga ofruesit e shërbimeve të palëve të treta të TIK-ut dhe identifikojnë ndërlidhjet me ofruesit e shërbimeve të palëve të treta të TIK-ut që mbështetin funksionet kritike ose të rëndësishme.

6. Për qëllime të pikave 1, 4 dhe 5 të këtij neni, subjektet financiare duhet të mbajnë inventarët përkatës dhe t'i përditësojnë rregullisht dhe sa herë që ndodhin ndryshime të rëndësishme, siç parashikohet në pikën 3 të këtij neni.

7. Subjektet financiare, me përjashtim të mikrondërmarrjeve, kryejnë rregullisht dhe të paktën një herë në vit, një vlerësim specifik të rrezikut të TIK-ut, për të gjitha sistemet e vjetra të TIK-ut, veçanërisht para dhe pas lidhjes së teknologjive, aplikacioneve ose sistemeve.

Neni 10 **Mbrojtja dhe parandalimi**

1. Për qëllime të mbrojtjes së përshtatshme të sistemeve të TIK-ut dhe të organizimit të masave të reagimit, subjektet financiare monitorojnë dhe kontrollojnë vazhdimisht sigurinë dhe funksionimin e sistemeve dhe mekanizmave të TIK-ut, si dhe minimizojnë ndikimin e

rrezikut të TIK-ut mbi sistemet e TIK-ut, nëpërmjet angazhimit të mekanizmave, politikave dhe procedurave të duhura të sigurisë të TIK-ut.

2. Subjektet financiare hartojnë, prokurojnë dhe zbatojnë politikat, procedurat, protokollet dhe mekanizmat e sigurisë së TIK-ut, që synojnë sigurimin e qëndrueshmërisë, vazhdimësisë dhe disponueshmërisë së sistemeve të TIK-ut, në veçanti për ata që mbështetin funksionet kritike ose të rëndësishme, si dhe ruajtjen e standardeve të larta të disponueshmërisë, autenticitetit, integritetit dhe konfidencialitetit të të dhënave, qoftë në qetësi, në përdorim apo në tranzit.

3. Për të arritur objektivat e parashikuar në pikën 2 të këtij neni, subjektet financiare përdorin teknologjinë (zgjidhjet) dhe proceset e TIK-ut, të cilat janë të përshtatshme për to, në përputhje me parimin e proporcionalitetit të parashikuar në nenin 5 të kësaj rregulloreje. Këto teknologji (zgjidhje) dhe procese të TIK-ut:

- a) garantojnë sigurinë e mjeteve të transferimit të informacionit/të dhënave;
- b) minimizojnë rrezikun e korrupsionit ose humbjes së të dhënave, aksesit të paautorizuar dhe të defekteve teknike që mund të pengojnë aktivitetin e biznesit;
- c) parandalojnë mungesën e disponueshmërisë, dëmtimin e autenticitetit dhe integritetit, shkeljet e konfidencialitetit dhe humbjen e të dhënave;
- d) sigurojnë që të dhënat mbrohen nga rreziqet që lidhen me administrimin e të dhënave/të informacionit, përfshirë administrimin e dobët, rreziqet që lidhen me përpunimin e të dhënave dhe gabimet njerëzore.

4. Si pjesë të sistemit të administrimit të rrezikut të TIK-ut të parashikuar në nenin 7, pika 1, të kësaj rregulloreje, subjektet financiare:

- a) zhvillojnë dhe dokumentojnë një politikë të sigurisë së informacionit që përcakton rregullat për të mbrojtur disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave, aseteve të informacionit dhe aseteve të TIK-ut, përfshirë edhe të klientëve të tyre, ku është e zbatueshme;
- b) duke ndjekur një qasje të bazuar në rrezik, krijojnë një rrjet të shëndoshë dhe strukturë të qëndrueshme të administrimit të infrastrukturës, duke përdorur teknikat, metodat dhe protokollet e duhura, që mund të përfshijnë zbatimin e mekanizmave të automatizuar, për të izoluar asetet e informacionit të prekur në rast të sulmeve kibernetike;
- c) zbatojnë politika që kufizojnë aksesin fizik ose logjik në asetet e informacionit dhe asetet e TIK-ut, në nivelin që kërkohet vetëm për funksionet dhe aktivitetet legjitime dhe të miratuara, si dhe krijojnë për këtë qëllim një sërë politikash, procedurash dhe kontrollesh që adresojnë të drejtat për akses dhe sigurojnë një administrim të shëndoshë të tyre;
- d) zbatojnë politika dhe protokolle për mekanizma autentifikimi të thelluar, bazuar në standardet përkatëse dhe sisteme të dedikuara kontrolli, si dhe masa mbrojtëse për të parandaluar aksesin në çelësat kriptografikë, ku të dhënat enkriptohen (kodohen) bazuar në rezultatet e klasifikimit të miratuar të të dhënave dhe proceseve të vlerësimit të rrezikut të TIK-ut;
- e) zbatojnë politika, procedura dhe kontrole të dokumentuara për administrimin e ndryshimeve të TIK-ut, duke përfshirë ndryshimet në programet dhe pajisjet kompjuterike (*software* dhe *hardware*), komponentët *firmware*, ndryshime të parametrave të sistemeve ose të sigurisë, që bazohen në një metodë/qasje të vlerësimit të rrezikut dhe janë pjesë integrale e procesit të përgjithshëm të administrimit të ndryshimeve të subjektit financiar, në mënyrë që të sigurohet që të gjitha ndryshimet në sistemet e TIK-ut, regjistrohen, testohen, vlerësohen, miratohen, zbatohen dhe verifikohen në mënyrë të kontrolluar;
- f) kanë politika të dokumentuara të përshtatshme dhe gjithëpërfshirëse për rishikimet dhe përditësimet.

5. Për qëllime të shkronjës “b” të pikës 4 të këtij neni, subjektet financiare projektojnë infrastrukturën e lidhjes së rrjetit në mënyrë të tillë që të lejojë ndarjen dhe segmentimin e saj

në mënyrë të menjëhershme, për të minimizuar dhe parandaluar përhapjen (*contagion*) e problemit, veçanërisht për proceset financiare të ndërlidhura.

6. Për qëllime të shkronjës “e” të pikës 4 të këtij neni, procesi i administrimit të ndryshimeve të TIK-un, miratohet nga organet drejtuese përkatëse dhe ka protokolle specifike në fuqi.

Neni 11

Zbulimi

1. Subjektet financiare duhet të kenë mekanizma për zbulimin e menjëhershëm të aktiviteteve anormale, në përputhje me nenin 18 të kësaj rregulloreje, duke përfshirë çështjet e performancës së rrjetit të TIK-un dhe incidentet e lidhura me TIK-un, si dhe për të identifikuar të gjitha pikat e vetme materiale të mundshme të dështimit.

2. Subjektet financiare testojnë rregullisht të gjithë mekanizmat e zbulimit të parashikuar në pikën 1 të këtij neni, në përputhje me nenin 42 të kësaj rregulloreje.

3. Mekanizmat e zbulimit të parashikuar në pikën 1 të këtij neni mundësojnë nivele të shumëfishta kontrolli, përcaktojnë kufij alarmi dhe kritere për të aktivizuar dhe iniciuar proceset e përgjigjes/reagimit ndaj incidenteve të lidhura me TIK-un, përfshirë edhe mekanizma automatikë alarmi për punonjësit përkatës përgjegjës për reagimin ndaj incidenteve të lidhur me TIK-un.

4. Subjektet financiare dedikojnë burime dhe aftësi të mjaftueshme për të monitoruar aktivitetin e përdoruesve, shfaqjen e anomalive të TIK-un dhe incidenteve të lidhura me TIK-un, në veçanti, sulmeve kibernetike.

Neni 12

Reagimi dhe rimëkëmbja

1. Subjektet financiare hartojnë një politikë gjithëpërfshirëse të vazhdimësisë së biznesit të TIK-un, si pjesë të sistemit të administrimit të rrezikut të TIK-un të parashikuar në pikën 1 të nenit 7 të kësaj rregulloreje dhe bazuar në kërkesat e identifikimit të përcaktuara në nenin 9 të kësaj rregulloreje, e cila mund të përshtatet si një politikë e veçantë, pjesë integrale e politikës së përgjithshme të vazhdimësisë së biznesit të subjektit financiar.

2. Subjektet financiare zbatojnë politikën e vazhdimësisë së biznesit të TIK-un të parashikuar në pikën 1 të këtij neni, nëpërmjet marrëveshjeve, planeve, procedurave dhe mekanizmave të dedikuara, të përshtatshëm dhe të dokumentuar që synojnë:

a) sigurimin e vazhdimësisë së funksioneve kritike ose të rëndësishme të subjektit financiar;

b) reagimin, në mënyrë të shpejtë, të përshtatshme dhe efektive, dhe zgjidhjen e të gjitha incidenteve të lidhura me TIK-un, në një mënyrë që kufizon dëmet dhe i jep përparësi rifillimit të aktiviteteve dhe masave të rimëkëmbjes;

c) aktivizimin pa vonesë të planeve të dedikuara që mundësojnë masat e kontrollit, proceset dhe teknologjitë e përshtatshme për çdo lloj incidenti të lidhur me TIK-un dhe parandalimin e dëmeve të mëtejshme, si dhe procedurat e përshtatura të reagimit dhe rimëkëmbjes, të krijuara në përputhje me nenin 14 të kësaj rregulloreje;

d) vlerësimin paraprak të ndikimit, dëmeve dhe humbjeve;

e) vendosjen e masave të komunikimit dhe menaxhimit të krizave, që sigurojnë që informacioni i përditësuar t'i transmetohet të gjithë stafit përkatës të brendshëm dhe palëve të jashtme të interesuara, në përputhje me nenin 16 të kësaj rregulloreje, dhe t'i raportohet Bankës së Shqipërisë, në përputhje me nenin 30 të kësaj rregulloreje.

3. Subjektet financiare zbatojnë plane të reagimit dhe të rimëkëmbjes të lidhura me TIK-un, si pjesë të sistemit të administrimit të rrezikut të TIK-un të parashikuar në pikën 1 të nenit 7 të

kësaj rregulloreje, të cilët, në rastin e subjekteve financiare që nuk janë mikrondërmarrje, do të jenë subjekt i rishikimeve të pavarura të auditit të brendshëm.

4. Subjektet financiare hartojnë, mirëmbajnë dhe testojnë periodikisht planet e duhura të vazhdimësisë së biznesit të TIK-ut, veçanërisht në lidhje me funksionet kritike ose të rëndësishme të deleguara të palëve të treta, ose të kontraktuara nëpërmjet marrëveshjeve me ofruesit e shërbimeve të palëve të treta të TIK-ut.

5. Subjektet financiare, si pjesë të politikës së përgjithshme të vazhdimësisë së biznesit, duhet të kryejnë një analizë të ndikimit në biznes (ANB) të ekspozimeve të tyre ndaj ndërprerjeve të rënda të aktivitetit/biznesit. Sipas analizës së ndikimit në biznes, subjektet financiare vlerësojnë ndikimin e mundshëm të ndërprerjeve të rënda të aktivitetit/biznesit, me anë të kriterëve sasiore dhe cilësore, duke përdorur të dhëna të brendshme dhe të jashtme dhe analiza të skenarëve, sipas rastit. Analiza e ndikimit në biznes duhet të konsiderojë kritikabilitetin e funksioneve të biznesit të identifikuar dhe të përcaktuar, proceset mbështetëse, varësitë ndaj palëve të treta dhe asetet e informacionit, si dhe ndërvarësinë e tyre. Subjektet financiare duhet të sigurojnë që asetet e TIK-ut dhe shërbimet e TIK-ut janë projektuar dhe përdorur në përputhje të plotë me analizën e ndikimit në biznes, veçanërisht në lidhje me sigurinë në mënyrë të mjaftueshme të tepërisë së të gjithë komponentëve kritikë.

6. Si pjesë të administrimit gjithëpërfshirës të rrezikut të TIK-ut, subjektet financiare duhet të:

a) testojnë planet e vazhdimësisë së biznesit të TIK-ut dhe planet e reagimit dhe të rimëkëmbjes së TIK-ut, në lidhje me sistemet e TIK-ut që mbështetin të gjitha funksionet, të paktën çdo vit, si dhe pas ndryshimeve thelbësore në sistemet e TIK-ut që mbështetin funksionet kritike ose të rëndësishme;

b) testojnë planet e komunikimit në situata krize, të hartuara në përputhje me nenin 16 të kësaj rregulloreje.

7. Për qëllime të shkronjës “a” të pikës 6 të këtij neni, subjektet financiare, me përjashtim të mikrondërmarrjeve, do të përfshijnë në planet e testimit skenarë të sulmeve kibernetike dhe kalimeve ndërmjet infrastrukturës parësore të TIK-ut dhe infrastrukturës dytësore (*redundant capacity*), *backups* dhe objekteve dytësore, të nevojshme për të përmbushur detyrimet e përcaktuara në nenin 14 të kësaj rregulloreje.

8. Subjektet financiare duhet të rishikojnë rregullisht politikën e tyre të vazhdimësisë së biznesit të TIK-ut dhe planin e reagimit dhe rimëkëmbjes nga fatkeqësitë e TIK-ut, duke marrë parasysh rezultatet e testeve të kryera në përputhje me pikën 6 të këtij neni dhe rekomandimet që rrjedhin nga kontrollet e auditimit ose rishikimet mbikëqyrëse.

9. Subjektet financiare, me përjashtim të mikrondërmarrjeve, krijojnë një funksion të menaxhimit të krizave, i cili, në rast të aktivizimit të planit të tyre të vazhdimësisë së biznesit të TIK-ut ose planit të reagimit dhe rimëkëmbjes nga fatkeqësitë e TIK-ut, përcakton procedura të qarta për administrimin e komunikimeve të brendshme dhe të jashtme në situata krize, në përputhje me nenin 16 të kësaj rregulloreje.

10. Subjektet financiare duhet të mbajnë regjistrime lehtësisht të aksesueshme të aktiviteteve para dhe gjatë ngjarjeve të ndërprerjes së aktivitetit, kur aktivizohet plani i vazhdimësisë së biznesit të TIK-ut ose plani i reagimit dhe rimëkëmbjes nga fatkeqësitë e TIK-ut.

11. Subjektet financiare, me përjashtim të mikrondërmarrjeve, raportojnë në Bankën e Shqipërisë, me kërkesë të kësaj të fundit, një vlerësim të të gjitha kostove dhe humbjeve të shkaktuara nga incidentet madhore të lidhura me TIK-un, sipas përcaktimeve të nenit 13 të kësaj rregulloreje.

Neni 13

Vlerësimi i kostove dhe humbjeve të shkaktuara nga incidentet madhore të lidhura me TIK-un

1. Për qëllime të pikës 11 të nenit 12 të kësaj rregulloreje, subjektet financiare duhet të vlerësojnë kostot dhe humbjet vjetore të agreguara, të shkaktuara nga incidentet madhore të lidhura me TIK-un, duke përfshirë të gjitha kostot dhe humbjet që lidhen me incidentet madhore të TIK-ut që kanë ndodhur brenda vitit referencë, për të cilin Banka e Shqipërisë ka kërkuar vlerësimin. Subjekti financiar mund të zgjedhë nëse viti referencë do të korrespondojë me vitin kalendarik ose me vitin kontabël të përfunduar të subjektit financiar, për të cilin ky i fundit ka finalizuar pasqyrat financiare. Pasi subjekti financiar të ketë vendosur nëse do të bazojë vlerësimin në vitin kalendarik apo në vitin kontabël, ky vendim duhet të zbatohet edhe për vlerësimet e ardhshme të kostove dhe humbjeve vjetore të agreguara. Subjekti financiar mund ta ndryshojë këtë vendim duke njoftuar Bankën e Shqipërisë, me kusht që Banka e Shqipërisë të mos ketë kundërshtime brenda dy muajve nga marrja e njoftimit. Subjektet financiare nuk duhet të përfshijnë kostot dhe humbjet që lidhen me incidente që kanë ndodhur përpara ose pas vitit referencë.

2. Subjektet financiare duhet të përfshijnë në vlerësim, të gjitha incidentet që lidhen me TIK-un, të cilat, pavarësisht shkakt, janë klasifikuar si madhore, në përputhje me nënkreun II të kreut III të kësaj rregulloreje dhe:

a) për të cilat subjekti financiar ka paraqitur një raport përfundimtar, në përputhje me nenin 30, pika 6, shkronja “c”, të kësaj rregulloreje gjatë vitit referencë përkatës; ose

b) çdo incident për të cilin subjekti financiar ka paraqitur në vitet referencë të mëparshme një raport përfundimtar, në përputhje me nenin 30, pika 6, shkronja “c”, të kësaj rregulloreje, që ka pasur një ndikim financiar të matshëm mbi subjektin financiar gjatë vitit referencë përkatës.

3. Subjektet financiare duhet të vlerësojnë kostot dhe humbjet vjetore të agreguara, duke ndjekur hapat e mëposhtëm në mënyrë të njëpasnjëshme:

a) të vlerësojnë kostot dhe humbjet e çdo incidenti madhor që lidhet me TIK-un, siç përcaktohet në pikën 2 të këtij neni, individualisht. Këto vlerësime duhet të japin kostot dhe humbjet bruto, duke marrë parasysh llojet e kostove dhe humbjeve të përcaktuara në nenin 26, pikat 1 dhe 2, të kësaj rregulloreje;

b) për secilin incident madhor të lidhur me TIK-un, subjektet financiare duhet, gjithashtu, të vlerësojnë vlerat e rikuperuara (*financial recoveries*), siç përcaktohet në Aneksin 2 të kësaj rregulloreje;

c) subjektet financiare aggregojnë kostot dhe humbjet bruto dhe vlerat e rikuperuara për të gjitha incidentet madhore që lidhen me TIK-un.

4. Si bazë për vlerësimet, subjektet financiare duhet t’u referohen kostove, humbjeve dhe vlerave të rikuperuara që pasqyrohen në pasqyrat e tyre financiare, si për shembull pasqyrën e të ardhurave dhe shpenzimeve, ose, kur është e zbatueshme, në raportimet mbikëqyrëse, për vitin referencë përkatës.

Në vlerësimin e tyre, subjektet financiare duhet të përfshijnë, gjithashtu, provigjionet kontabël që pasqyrohen në pasqyrat financiare të vitit referencë përkatës.

Në rastet kur të dhënat e sakta nuk janë të disponueshme, subjektet financiare duhet të bazojnë vlerësimin e tyre në të dhëna dhe informacione të tjera të disponueshme, sa më shumë që të jetë e mundur.

5. Subjektet financiare duhet të përfshijnë rregullimet mbi kostot dhe humbjet e një vlerësimi të paraqitur për një vit të mëparshëm, në vlerësimin e vitit referencë përkatës, në të cilin janë bërë këto rregullime.

6. Subjektet financiare duhet të përfshijnë në raportin e tyre të vlerësimit të kostove dhe humbjeve vjetore të përmbledhura edhe ndarjen e kostove dhe humbjeve bruto dhe të vlerave të rikuperuara për secilin incident madhor të lidhur me TIK-un, që është përfshirë në agregim.

7. Subjektet financiare duhet të përdorin formularin në Aneksin 5 të kësaj rregulloreje, për të paraqitur në Bankën e Shqipërisë vlerësimin e kostove dhe humbjeve të tyre vjetore të agreguara për vitin referencë.

Për çdo element të përfshirë në vlerësimin e vitit referencë, në përputhje me pikat 2 dhe 5 të këtij neni, subjektet financiare duhet të përdorin të njëjtat kode reference të incidenteve që kanë përdorur në raportin përfundimtar, në përputhje me nenin 30, pika 6, shkronja “c”, të kësaj rregulloreje.

Neni 14

Politikat dhe procedurat e *backup*-it dhe procedurat dhe metodat e rikuperimit dhe rimëkëmbjes

1. Me qëllim sigurimin e rikuperimit (rikthimit në gjendjen e mëparshme) të sistemeve të TIK-ut dhe të dhënave në një kohë sa më të shkurtër, si dhe kufizimin në maksimum të kohëzgjatjes së padisponueshmërisë, ndërprerjeve dhe humbjeve, si pjesë e sistemit të tyre të administrimit të rrezikut të TIK-ut, subjektet financiare hartojnë dhe dokumentojnë:

a) politika dhe procedura *backup*-i që specifikojnë shtrirjen e të dhënave që i nënshtrohen *backup*-it dhe frekuencën minimale të *backup*-it, bazuar në kritikalitetin e informacionit ose konfidencialitetin e të dhënave;

b) procedura dhe metoda të rikuperimit dhe rimëkëmbjes.

2. Subjektet financiare krijojnë sisteme të *backup*-it, të cilat aktivizohen në përputhje me politikat dhe procedurat e *backup*-it, si dhe me procedurat dhe metodat e rikuperimit dhe rimëkëmbjes. Aktivizimi i sistemeve të *backup*-it nuk duhet të rrezikojë sigurinë e rrjetit dhe sistemeve të informacionit, ose disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave. Subjektet financiare testojnë periodikisht procedurat e *backup*-it, si dhe procedurat dhe metodat e rikuperimit dhe rimëkëmbjes.

3. Gjatë rikuperimit të të dhënave të *backup*-it, duke përdorur sistemet e veta, subjektet financiare duhet të përdorin sisteme TIK që janë fizikisht dhe logjikisht të ndara nga sistemi kryesor i TIK-ut. Sistemet e TIK-ut duhet të jenë të mbrojtur në mënyrë të sigurt nga çdo akses i paautorizuar ose korruptim i TIK-ut dhe të lejojnë rikuperimin në kohë të shërbimeve, duke përdorur të dhënat dhe *backup*-et (kopjet rezervë) të sistemit sipas nevojës.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, duhet të mbajnë infrastruktura dytësore të TIK-ut, të pajisura me burime, kapacitete dhe funksionalitete që janë të mjaftueshme dhe të përshtatshme për të siguruar nevojat e biznesit. Mikrondërmarrjet vlerësojnë nevojat për të mbajtur infrastruktura dytësore të TIK-ut, bazuar në profilin e tyre të rrezikut.

5. Subjektet financiare, në përcaktimin e kohës së rimëkëmbjes dhe objektivave të pikës së rimëkëmbjes për çdo funksion, duhet të marrin parasysh nëse një funksion është apo jo kritik ose i rëndësishëm, si dhe ndikimin e përgjithshëm të mundshëm në eficiencën e tregut. Këta objektiva kohorë duhet të sigurojnë që, në skenarë ekstremë, të përmbushen nivelet e dakorduara të shërbimit.

6. Subjektet financiare, pasi rimëkëmben nga një incident i lidhur me TIK-un, duhet të kryejnë kontrollet e nevojshme, duke përfshirë rakordimet, në mënyrë që të sigurohet që integriteti i të dhënave është i nivelit më të lartë. Këto kontrolle do të kryhen, gjithashtu, gjatë rindërtimit të të dhënave nga palët e jashtme të interesuara, në mënyrë që të sigurohet që të gjitha të dhënat të jenë të përputhshme ndërmjet sistemeve të ndryshme.

Neni 15

Mësimet e nxjerra dhe zhvillimi

1. Subjektet financiare duhet të disponojnë aftësi të përshtatshme dhe personel të mjaftueshëm për të mbledhur informacion mbi vulnerabilitetet dhe kërcënimet kibernetike, incidentet e lidhura me TIK-un, veçanërisht sulmet kibernetike, dhe të analizojnë ndikimet e mundshme në qëndrueshmërinë e tyre operacionale digjitale.

2. Subjektet financiare duhet të kryejnë rishikime pas incidenteve të lidhura me TIK-un, pasi një incident i lidhur me TIK-un ndërpret aktivitetet e tyre kryesore, duke analizuar shkaqet e ndërprerjes dhe duke identifikuar përmirësimet e nevojshme në operacionet e TIK-ut ose brenda politikës së vazhdimësisë së biznesit të TIK-ut të parashikuar në nenin 12 të kësaj rregulloreje. Subjektet financiare, me përjashtim të mikrondërmarrjeve, i komunikojnë Bankës së Shqipërisë, me kërkesë të kësaj të fundit, ndryshimet e implementuara si rrjedhojë e rishikimeve pas ndodhjes së incidenteve të lidhura me TIK-un.

3. Rishikimet pas incidentit të lidhur me TIK-un, të parashikuara në pikën 2 të këtij neni, përcaktojnë nëse janë ndjekur procedurat e vendosura dhe veprimet e ndërmarra kanë qenë efektive, duke përfshirë në lidhje me:

a) shpejtësinë në përgjigjen ndaj alarmeve të sigurisë dhe përcaktimin e ndikimit të incidenteve të lidhura me TIK-un dhe ashpërsinë e tyre;

b) cilësinë dhe shpejtësinë në kryerjen e analizave forensike, kur është e përshtatshme;

c) efektivitetin e përshkallëzimit të incidentit brenda subjektit financiar;

d) efektivitetin e komunikimit të brendshëm dhe të jashtëm.

4. Subjektet konsiderojnë dhe përfshijnë në mënyrë të vazhdueshme në procesin e vlerësimit të rrezikut të TIK-ut, konkluzionet (mësimet) e nxjerra nga testimi i qëndrueshmërisë operacionale digjitale i kryer në përputhje me nenet 43 dhe 44 të kësaj rregulloreje dhe nga incidentet reale të ndodhura të lidhura me TIK-un, veçanërisht sulmet kibernetike, së bashku me sfidat me të cilat përballet aktivizimi i planeve të vazhdimësisë së biznesit ose rimëkëmbjes, së bashku me informacionin përkatës të shkëmbyer me palët dhe të vlerësuar gjatë rishikimeve mbikëqyrëse. Këto gjetje do të shërbejnë si bazë për rishikimet e përshtatshme të elementeve përkatëse të sistemit të administrimit të rrezikut të TIK-ut të parashikuar në nenin 7, pika 1, të kësaj rregulloreje.

5. Subjektet financiare monitorojnë efektivitetin e zbatimit të strategjisë së tyre të qëndrueshmërisë operacionale digjitale, të përcaktuar në nenin 7, pika 9, të kësaj rregulloreje. Subjektet hartëzojnë evolucionin në kohë të rreziqeve të TIK-ut, analizojnë frekuencën, llojet, madhësinë dhe evolucionin e incidenteve të lidhura me TIK-un, në veçanti sulmeve kibernetike dhe strukturave të tyre, me qëllim që të kuptojnë nivelin e ekspozimit ndaj rrezikut të TIK-ut, veçanërisht në lidhje me funksionet kritike ose të rëndësishme, dhe të përmirësojnë maturinë dhe gatishmërinë kibernetike të subjektit financiar.

6. Drejtuesit e TIK-ut raportojnë të paktën një herë në vit në organet drejtuese të subjektit financiar, mbi gjetjet e parashikuara në pikën 4 të këtij neni dhe paraqesin edhe rekomandimet e tyre.

7. Subjektet financiare zhvillojnë programe ndërgjegjësimi për sigurinë e TIK-ut dhe trajnime për qëndrueshmërinë operacionale digjitale, si module të detyrueshme në skemat e trajnimit të punonjësve. Këto programe dhe trajnime do të zbatohen për të gjithë punonjësit dhe për drejtuesit e subjektit dhe duhet të kenë një nivel kompleksiteti në proporcion me detyrat dhe funksionet e tyre. Kur është e përshtatshme, subjektet financiare përfshijnë në skemat përkatëse të trajnimit edhe ofruesit e shërbimeve të palëve të treta të TIK-ut, në përputhje me nenin 47, pika 2, shkronja “i”, të kësaj rregulloreje.

8. Subjektet financiare, me përjashtim të mikrondërmarrjeve, monitorojnë zhvillimet teknologjike përkatëse, në mënyrë të vazhdueshme, edhe me synimin për të kuptuar ndikimet e mundshme të këtyre teknologjive të reja mbi kërkesat e sigurisë së TIK-ut dhe qëndrueshmërinë operacionale digjitale. Subjektet duhet të përditësohen me proceset më të

fundit të administrimit të rrezikut të TIK-ut, për të luftuar në mënyrë efektive format aktuale ose të reja të sulmeve kibernetike.

Neni 16 **Komunikimi**

1. Si pjesë të sistemit të administrimit të rrezikut të TIK-ut të parashikuar në nenin 7, pika 1, të kësaj rregulloreje, subjektet financiare duhet të kenë plane komunikimi në situata krize, që u mundësojnë një njoftim të përgjegjshëm, për të paktën incidentet madhore ose vulnerabilitetet e lidhura me TIK-un, për klientët dhe kundërpartitë, si dhe për publikun, sipas rastit.

2. Si pjesë të sistemit të administrimit të rrezikut të TIK-ut, subjektet financiare zbatojnë politika komunikimi për punonjësit dhe për palët e jashtme të interesuara. Politikat e komunikimit për punonjësit duhet të konsiderojnë që të bëhet dallimi ndërmjet punonjësve të përfshirë në administrimin e rrezikut të TIK-ut, në veçanti punonjësve përgjegjës për reagimin dhe rimëkëmbjen, dhe pjesës tjetër të personelit që duhet të informohet.

3. Subjekti financiar cakton të paktën një person për zbatimin e strategjisë së komunikimit për incidentet e lidhura me TIK-un dhe për të përmbushur rolin e zëdhënësit të publikut dhe medias për këtë qëllim.

Neni 17 **Sistemi i thjeshtuar i administrimit të rrezikut të TIK-ut**

1. Nenet 6 deri në 16 të kësaj rregulloreje nuk zbatohen për institucionet e pagesave dhe institucionet e parasë elektronike që përjashtohen sipas parashikimeve të ligjit “Për shërbimet e pagesave”, të cilët krijojnë një sistem të thjeshtuar të administrimit të rrezikut të TIK-ut, siç parashikohet në pikën 2 të këtij neni.

2. Pa cenuar pikën 1 të këtij neni, subjektet e listuara në atë pikë:

a) krijojnë dhe mbajnë një sistem të shëndoshë dhe të dokumentuar të administrimit të rrezikut të TIK-ut, që detajon mekanizmat dhe masat që synojnë një administrim të shpejtë, efikas dhe gjithëpërfshirës të rrezikut të TIK-ut, duke përfshirë mbrojtjen e komponentëve dhe infrastrukturave fizike përkatëse;

b) monitorojnë vazhdimisht sigurinë dhe funksionimin e të gjitha sistemeve të TIK-ut;

c) minimizojnë ndikimin e rrezikut të TIK-ut nëpërmjet përdorimit të sistemeve, protokolleve dhe mekanizmave të shëndoshë, të qëndrueshëm dhe të përditësuar të TIK-ut, të cilat janë të përshtatshëm për të mbështetur performancën e aktiviteteve të tyre dhe ofrimin e shërbimeve dhe për të mbrojtur në mënyrë adekuate disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave në rrjet dhe sistemet e informacionit;

d) lejojnë që burimet e rrezikut dhe anomalitë e TIK-ut në rrjet dhe sistemet e informacionit të identifikohen dhe zbulohen menjëherë, dhe incidentet e lidhura me TIK-un të trajtohen me shpejtësi;

e) identifikojnë ndërvaresitë kryesore nga ofruesit e shërbimeve të palëve të treta të TIK-ut;

f) sigurojnë vazhdimësinë e funksioneve kritike ose të rëndësishme, nëpërmjet planeve të vazhdimësisë së biznesit dhe masave të reagimit dhe rimëkëmbjes, të cilat përfshijnë, të paktën, *backup*-in dhe masat e rikuperimit;

g) testojnë rregullisht planet dhe masat e parashikuara në shkronjën “f”, si dhe efektivitetin e kontroleve të zbatuara në përputhje me shkronjat “a” dhe “c” të kësaj pike;

h) zbatojnë, sipas rastit, konkluzionet përkatëse operationale që rezultojnë nga testet e parashikuara në shkronjën “g” dhe nga analiza pas incidentit në procesin e vlerësimit të rrezikut të TIK-ut, si dhe zhvillojnë, sipas nevojave dhe profilit të rrezikut të TIK-ut, programet e

ndërgjegjësimi për sigurinë e TIK-ut dhe trajnimin mbi qëndrueshmërinë operacionale digjitale për punonjësit dhe drejtuesit e subjektit.

3. Sistemi i administrimit të rrezikut të TIK-ut i parashikuar në pikën 2, shkronja “a”, të këtij neni, duhet të dokumentohet dhe rishikohet periodikisht nga subjektet dhe pas ndodhjes së incidenteve madhore të lidhura me TIK-un, në përputhje me udhëzimet mbikëqyrëse. Subjektet e përmirësojnë vazhdimisht sistemin e administrimit të rrezikut të TIK-ut, në bazë të mësimave të nxjerra nga zbatimi dhe monitorimi. Subjektet i komunikojnë Bankës së Shqipërisë, me kërkesë të kësaj të fundit, raportin mbi rishikimin e sistemit të administrimit të rrezikut të TIK-ut.

KREU III

ADMINISTRIMI, KLASIFIKIMI DHE RAPORTIMI I INCIDENTEVE TË LIDHUR ME TIK-un

NËNKREU I

ADMINISTRIMI DHE KLASIFIKIMI I INCIDENTEVE TË LIDHUR ME TIK-un

Neni 18

Procesi i administrimit të incidenteve të lidhura me TIK-un

1. Subjektet financiare përcaktojnë, krijojnë dhe zbatojnë një proces të administrimit të incidenteve të lidhura me TIK-un, për të zbuluar, administruar dhe njoftuar incidentet e lidhura me TIK-un.

2. Subjektet financiare regjistrojnë të gjitha incidentet e lidhura me TIK-un dhe kërcënimet kibernetike të rëndësishme. Subjektet financiare krijojnë procedura dhe procese të përshtatshme për të siguruar një monitorim, trajtim dhe ndjekje të vazhdueshme dhe të integruar të incidenteve të lidhura me TIK-un, për të siguruar që shkaqet kryesore të incidentit janë identifikuar, dokumentuar dhe adresuar, për të parandaluar përsëritjen e incidenteve të tilla.

3. Procesi i administrimit të incidenteve të lidhura me TIK-un, i parashikuar në pikën 1 të këtij neni:

- a) përcakton tregues të paralajmërimit të hershëm;
- b) krijon procedura për identifikimin, gjurmimin, regjistrimin, kategorizimin dhe klasifikimin e incidenteve të lidhura me TIK-un, sipas prioritetit të tyre dhe ashpërsisë, si dhe sipas kritikalitetit të shërbimeve të ndikuara nga incidenti, në përputhje me kriteret e parashikuara në nenin 19, pika 1, të kësaj rregulloreje;
- c) përcakton rolet dhe përgjegjësitë që duhet të aktivizohen për lloje dhe skenarë të ndryshëm incidentesh të lidhura me TIK-un;
- d) përcakton planet për komunikimin me punonjësit, me palët e jashtme të interesuara dhe me median, në përputhje me nenin 16 të kësaj rregulloreje, për njoftimin e klientëve, për procedurat e brendshme të përshkallëzimit, duke përfshirë ankesat e klientëve lidhur me TIK-un, si dhe për dhënien e informacionit subjekteve financiare që veprojnë si kundërparti të subjektit në fjalë, sipas rastit;
- e) siguron që të paktën incidentet madhore të lidhura me TIK-un të raportohen te drejtuesit përkatës dhe të informohet organi drejtues, të paktën për incidentet madhore të lidhura me TIK-un, duke shpjeguar ndikimin, reagimin dhe kontrollet shtesë që do të vendosen si rezultat i incidenteve të lidhura me TIK-un;
- f) krijon procedura të reagimit ndaj incidenteve të lidhura me TIK-un, për të zbutur ndikimet dhe për të siguruar që shërbimet të bëhen funksionale dhe të sigurta në kohën e duhur.

Neni 19

Klasifikimi i incidenteve të lidhura me TIK-un dhe i kërcënimeve kibernetike

1. Subjektet financiare klasifikojnë incidentet e lidhura me TIK-un dhe përcaktojnë ndikimin e tyre bazuar në kriteret e mëposhtme:

a) numrin dhe/ose rëndësinë e klientëve ose e kundërpartive financiare të prekur dhe, ku është e zbatueshme, vlerën ose numrin e transaksioneve të prekur nga incidenti i lidhur me TIK-un, si dhe nëse incidenti i lidhur me TIK-un ka pasur ndikim reputacional për subjektin;

b) kohëzgjatjen e incidentit të lidhur me TIK-un, duke përfshirë edhe kohën e ndërprerjes së shërbimeve;

c) shtrirjen gjeografike në lidhje me zonat e prekura nga incidenti i lidhur me TIK-un, veçanërisht nëse ai prek më shumë se dy shtete;

d) humbjet e të dhënave që shkakton incidenti i lidhur me TIK-un, në lidhje me disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave;

e) kritikalitetin e shërbimeve të prekura, duke përfshirë transaksionet dhe operacionet e subjektit financiar;

f) ndikimin ekonomik të incidentit të lidhur me TIK-un, në terma absolutë dhe relativë, në veçanti në kostot direkte e indirekte dhe humbjet.

2. Subjektet financiare klasifikojnë kërcënimet kibernetike si të rëndësishme, bazuar në kritikalitetin e shërbimeve në rrezik, duke përfshirë transaksionet dhe operacionet e subjektit financiar, numrin dhe/ose rëndësinë e klientëve ose të kundërpartive financiare të synuar, si dhe shtrirjen gjeografike të zonave në rrezik.

NËNKREU II

KRITERET E KLASIFIKIMIT TË INCIDENTEVE TË LIDHURA me TIK-un DHE TË KËRCËNIMEVE KIBERNETIKE

Neni 20

Klientët, kundërpartitë financiare dhe transaksionet

1. Për qëllime të pikës 1, shkronja “a”, të nenit 19 të kësaj rregulloreje, numri i klientëve të prekur nga incidenti, pasqyron numrin e të gjithë klientëve të prekur, persona fizikë apo juridikë, që nuk janë ose nuk kanë qenë në gjendje të përdorin shërbimin e ofruar nga subjekti financiar gjatë incidentit, ose që janë ndikuar negativisht nga incidenti. Ky numër duhet të përfshijë edhe palët e treta të mbuluara në mënyrë eksplicite nga marrëveshja kontraktuale ndërmjet subjektit financiar dhe klientit, si përfitues të shërbimit të prekur.

2. Për qëllime të pikës 1, shkronja “a”, të nenit 19 të kësaj rregulloreje, numri i kundërpartive financiare të prekura nga incidenti pasqyron numrin e të gjitha kundërpartive financiare të prekura nga incidenti, që kanë lidhur një marrëveshje kontraktuale me subjektin financiar.

3. Për të vlerësuar rëndësinë e klientëve dhe kundërpartive financiare të prekura nga incidenti, siç parashikohet në pikën 1, shkronja “a”, të nenit 19 të kësaj rregulloreje, subjekti financiar merr në konsideratë masën në të cilën ndikimi mbi një klient ose një kundërparti financiare do të ndikojë në zbatimin e objektivave të biznesit të subjektit financiar, si dhe në efektin e mundshëm të incidentit në efektivitetin e tregut.

4. Për shumën ose numrin e transaksioneve të prekura nga incidenti, siç parashikohet në pikën 1, shkronja “a”, të nenit 19 të kësaj rregulloreje, subjekti financiar merr në konsideratë të gjitha transaksionet e prekura që përfshijnë një shumë monetare, ku të paktën një pjesë e transaksionit kryhet në Shqipëri.

5. Në rastet kur nuk disponohen të dhëna reale mbi numrin e klientëve ose kundërpartive financiare të prekur ose mbi numrin ose shumën e transaksioneve të prekura, subjekti financiar

i vlerëson këta numra ose shuma bazuar në të dhënat e disponueshme nga periodha të krahasueshme reference.

Neni 21

Ndikimi reputacional

1. Për qëllime të përcaktimit të ndikimit reputacional të incidentit, siç parashikohet në pikën 1, shkronja “a”, të nenit 19 të kësaj rregulloreje, subjekti financiar merr në konsideratë se incidenti ka pasur një ndikim reputacional, kur plotësohet të paktën një nga kriteret e mëposhtme:

- a) ngjarja është pasqyruar në media;
- b) incidenti ka rezultuar në ankesa të përsëritura nga klientë të ndryshëm ose kundërpartitë financiare, për shërbimet që përballen me klientët ose marrëdhëniet kritike të biznesit;
- c) subjekti financiar nuk do të jetë në gjendje ose ka të ngjarë të mos jetë në gjendje të përmbushë kërkesat rregullatore si rezultat i incidentit;
- d) subjekti financiar do të humbasë ose ka të ngjarë të humbasë klientët ose kundërpartitë financiare, me një ndikim material në biznesin e tij, si rezultat i incidentit.

2. Gjatë vlerësimit të ndikimit reputacional të incidentit, subjektet financiare marrin në konsideratë nivelin e shikueshmërisë që incidenti ka fituar ose ka të ngjarë të fitojë, në lidhje me secilën nga kriteret e renditura në pikën 1 të këtij neni.

Neni 22

Kohëzgjatja dhe koha e ndërprerjes së shërbimeve

1. Për qëllime të pikës 1, shkronja “b”, të nenit 19 të kësaj rregulloreje, subjektet financiare llogaritin kohëzgjatjen e një incidenti, nga momenti kur ndodh incidenti deri në momentin kur ai zgjidhet.

2. Kur subjektet financiare nuk janë në gjendje të përcaktojnë momentin kur ka ndodhur incidenti, ato do të matin kohëzgjatjen e incidentit nga momenti i zbulimit të tij. Kur subjektet financiare marrin dijeni se incidenti ka ndodhur përpara zbulimit të tij, ata do të matin kohëzgjatjen nga momenti kur incidenti është regjistruar në regjistrat (*log-et*) e rrjetit ose të sistemit ose në burime të tjera të dhënash.

3. Kur subjektet financiare nuk e dinë ende se kur do të zgjidhet incidenti ose nuk janë në gjendje të verifikojnë të dhënat e regjistruara në regjistrat (*log-et*) ose në burimet e tjera të të dhënave, ato përdorin vlerësimet e tyre.

4. Për qëllime të pikës 1, shkronja “b”, të nenit 19 të kësaj rregulloreje, subjektet financiare llogaritin kohën e ndërprerjes së shërbimit të një incidenti, nga momenti kur shërbimi është plotësisht ose pjesërisht i padisponueshëm për klientët, kundërpartitë financiare ose përdoruesit e tjerë të brendshëm ose të jashtëm, deri në momentin kur aktivitetet ose operacionet e rregullta janë rikthyer në nivelin e shërbimit që ofrohej para incidentit. Kur ndërprerja e shërbimit shkakton një vonesë në ofrimin e shërbimit pas rikthimit/rikuperimit të aktiviteteve ose operacioneve të rregullta, koha e ndërprerjes do të llogaritet që nga fillimi i incidentit deri në momentin kur ky shërbim i vonuar ofrohet plotësisht.

5. Në rastet kur subjektet financiare nuk janë në gjendje të përcaktojnë momentin e fillimit të ndërprerjes së shërbimit, ato do të matin kohën e ndërprerjes së shërbimit që nga momenti i zbulimit të tij.

Neni 23

Shtrirja gjeografike

1. Për qëllime të përcaktimit të shtrirjes gjeografike në lidhje me zonat e prekura nga incidenti, siç parashikohet në pikën 1, shkronja “c”, të nenit 19 të kësaj rregulloreje, subjektet financiare vlerësojnë nëse incidenti ka apo ka pasur ndikim në shtete të tjera, dhe në veçanti vlerësojnë rëndësinë e ndikimit në lidhje me një nga sa vijon:

- a) klientët dhe kundërpasagjerët financiarë në shtete të tjera;
- b) degët ose subjektet e tjera financiare të grupit, që kryejnë veprimtari në shtete të tjera;
- c) infrastrukturën e tregut financiar ose ofruesit e palëve të treta, të cilët mund të prekin subjektet financiare në shtete të tjera, ku ofrojnë shërbime, për aq sa një informacion i tillë është i disponueshëm.

Neni 24

Humbja e të dhënave

1. Për qëllime të përcaktimit të humbjes së të dhënave që shkakton incidenti, siç parashikohet në pikën 1, shkronja “d”, të nenit 19 të kësaj rregulloreje, subjektet financiare marrin parasysh:

- a) në lidhje me disponueshmërinë e të dhënave, nëse incidenti i ka bërë të dhënat sipas kërkesës së subjektit financiar, klientëve ose kundërpasagjerëve të tij, të paaksesueshme ose të papërdorshme, në mënyrë të përkohshme ose të përhershme;
- b) në lidhje me autenticitetin e të dhënave, nëse incidenti ka cenuar besueshmërinë e burimit të të dhënave;
- c) në lidhje me integritetin e të dhënave, nëse incidenti ka rezultuar në modifikim të paautorizuar të të dhënave që e bën atë të pasaktë ose të paplotë;
- d) në lidhje me konfidencialitetin e të dhënave, nëse incidenti ka rezultuar në aksesimin ose zbulimin e të dhënave nga një palë ose sistem i paautorizuar.

Neni 25

Kritikaliteti i shërbimeve të prekura

1. Për qëllime të përcaktimit të kritikalitetit të shërbimeve të prekura, siç parashikohet në pikën 1, shkronja “e”, të nenit 19 të kësaj rregulloreje, subjektet financiare vlerësojnë nëse incidenti:

- a) prek ose ka prekur shërbimet e TIK-ut ose rrjetet dhe sistemet e informacionit që mbështesin funksione kritike ose të rëndësishme të subjektit financiar;
- b) prek ose ka prekur shërbimet financiare të ofruara nga subjekti financiar, për të cilat është licencuar/regjistruar nga Banka e Shqipërisë;
- c) ka krijuar një akses të suksesshëm, keqdashës dhe të paautorizuar në rrjetin dhe sistemet e informacionit të subjektit financiar.

Neni 26

Ndikimi ekonomik

1. Për qëllime të përcaktimit të ndikimit ekonomik të incidentit, siç parashikohet në pikën 1, shkronja “f”, të nenit 19 të kësaj rregulloreje, subjektet financiare, pa llogaritur vlerat e rikuperuara, marrin parasysh llojet e mëposhtme të kostove direkte dhe indirekte, si dhe humbjeve që janë shkaktuar si rezultat i incidentit:

- a) fondet ose aktivet financiare të përvetësuara (*expropriated*), për të cilat ato janë përgjegjëse, duke përfshirë aktivet e humbura për shkak të vjedhjes;

b) kostot për zëvendësimin ose zhvendosjen e pajisjeve (*hardware*), programeve kompjuterike (*software*) ose infrastrukturës;

c) kostot e personelit, përfshirë edhe kostot që lidhen me zëvendësimin ose zhvendosjen e personelit, rekrutimin e personelit shtesë, shpërblimet për punën jashtë orarit dhe rikuperimin e aftësive të humbura ose të dëmtuara;

d) tarifat për mosrespektimin e detyrimeve kontraktuale;

e) kostot për zgjidhjen e mosmarrëveshjeve dhe kompensimin e klientëve;

f) humbjet për shkak të të ardhurave të munguara;

g) kostot që lidhen me komunikimin e brendshëm dhe të jashtëm;

h) kostot e konsulencës, duke përfshirë kostot që lidhen me këshillimin ligjor, shërbimet mjekoligjore dhe shërbimet e rehabilitimit.

2. Kostot dhe humbjet e parashikuara në pikën 1 të këtij neni, nuk përfshijnë kostot që janë të nevojshme për funksionimin e përditshëm të biznesit, veçanërisht sa vijon:

a) kostot për mirëmbajtjen e përgjithshme të infrastrukturës, pajisjeve, pajisjeve *hardware*, programeve kompjuterike (*software*), si dhe kostot për mbajtjen të përditësuar të aftësive të personelit;

b) kostot e brendshme ose të jashtme për të përmirësuar biznesin pas incidentit, duke përfshirë përmirësimet dhe iniciativat e vlerësimit të rrezikut;

c) primet e sigurimit.

3. Subjektet financiare llogaritin vlerën e kostove dhe të humbjeve, bazuar në të dhënat e disponueshme në momentin e raportimit. Subjektet financiare përdorin vlerësimet e tyre, nëse nuk mund të përcaktojnë vlerat reale të kostove dhe humbjeve.

4. Subjektet financiare mbledhin të gjitha kostot dhe humbjet e parashikuara në pikën 1 të këtij neni, për të vlerësuar ndikimin ekonomik të incidentit.

Neni 27

Incidentet madhore

1. Për qëllime të pikës 1 të nenit 30 të kësaj rregulloreje, një incident do të konsiderohet si incident madhor, kur ai ka prekur shërbimet kritike që parashikohen në nenin 25 të kësaj rregulloreje, si dhe nëse plotësohet ndonjë nga kushtet e mëposhtme:

a) është arritur kufiri i materialitetit i përcaktuar në nenin 28, pika 6, shkronja “b”, të kësaj rregulloreje;

b) janë arritur dy ose më shumë nga kufijtë e tjerë të materialitetit të përcaktuar në pika 1 deri në 7 të nenit 28 të kësaj rregulloreje.

2. Incidentet e përsëritura që individualisht nuk konsiderohen si incident madhor në përputhje me pikën 1 të këtij neni, do të konsiderohen si një incident madhor nëse plotësojnë të gjitha kushtet e mëposhtme:

a) incidentet kanë ndodhur të paktën dy herë brenda 6 muajve;

b) incidentet kanë të njëjtin shkak bazë të dukshëm;

c) incidentet së bashku plotësojnë kriteret për t’u konsideruar si një incident madhor, siç përcaktohet në pikën 1 të këtij neni.

3. Subjektet financiare do të vlerësojnë ekzistencën e incidenteve të përsëritura, në baza mujore.

4. Subjektet financiare që kanë informacion për incidentet jo madhore të përsëritura të lidhura me TIK-un, që plotësojnë në mënyrë kumulative kushtet për t’u konsideruar incident madhor i lidhur me TIK-un, siç parashikohet në pikën 2 të këtij neni, e paraqesin këtë informacion në një formë të përmbledhur (agreguar).

5. Kërkesat e parashikuara në pikat 2 dhe 3 të këtij neni, nuk zbatohen për mikrondërmarrjet dhe për subjektet e parashikuara në nenin 17 të kësaj rregulloreje.

6. Nëse pas vlerësimeve të mëtejshme, subjekti financiar arrin në përfundimin se incidenti i lidhur me TIK-un, i cili është raportuar më parë si incident madhor, në asnjë moment nuk ka përmbushur kriteret dhe kufijtë e klasifikimit të përcaktuar në këtë nen, subjekti financiar njofton Bankën e Shqipërisë se e ka riklasifikuar incidentin e lidhur me TIK-un, nga incident madhor në jomadhör, duke i paraqitur informacionin për këtë klasifikim në formularin e parashikuar në Aneksin 2 të kësaj rregulloreje në lidhje me fushat “lloji i raportit” dhe “informacione të tjera”.

Neni 28

Kufijtë e materialitetit për përcaktimin e incidenteve madhore

1. Kufiri i materialitetit për kriterin “klientët, kundërpартitë financiare dhe transaksionet” arrihet, kur plotësohet një nga kushtet e mëposhtme:

a) numri i klientëve të prekur është më i lartë se 10% e të gjithë klientëve që përdorin shërbimin e prekur;

b) numri i klientëve të prekur që përdorin shërbimin e prekur nga incidenti, është më i lartë se 100,000;

c) numri i kundërpартive financiare të prekura nga incidenti është më i lartë se 30% e të gjitha kundërpартive financiare që kryejnë aktivitete të lidhura me ofrimin e shërbimit të prekur nga incidenti;

d) numri i transaksioneve të prekura është më i lartë se 10% e numrit mesatar ditor të transaksioneve të kryera nga subjekti financiar, në lidhje me shërbimin e prekur nga incidenti;

e) vlera e transaksioneve të prekura është më e lartë se 10% e vlerës mesatare ditore të transaksioneve të kryera nga subjekti financiar, në lidhje me shërbimin e prekur nga incidenti;

f) janë prekur klientët ose kundërpартitë financiare që janë identifikuar si të rëndësishëm në përputhje me nenin 20, pika 3, të kësaj rregulloreje.

2. Për qëllime të pikës 1 të këtij neni, nëse numri real i klientëve ose kundërpартive financiare të prekur nga incidenti, ose numri apo vlera reale e transaksioneve të prekura nga incidenti nuk mund të përcaktohet, subjekti financiar vlerëson numrin apo vlerat, bazuar në të dhënat e disponueshme nga periudhat e krahasueshme të referencës.

3. Kufiri i materialitetit për kriterin “ndikimi reputacional” arrihet kur plotësohet ndonjë nga kushtet e parashikuara në nenin 21, pika 1, shkronjat “a” deri në “d”, të kësaj rregulloreje.

4. Kufiri i materialitetit për kriterin “kohëzgjatja dhe koha e ndërprerjes së shërbimeve” arrihet kur plotësohet një nga kushtet e mëposhtme:

a) kohëzgjatja e incidentit është më e gjatë se 24 orë;

b) koha e ndërprerjes së shërbimit është më e gjatë se 2 orë për shërbimet e TIK-ut që mbështesin funksione kritike ose të rëndësishme.

5. Kufiri i materialitetit për kriterin “shtrirja gjeografike” arrihet kur incidenti ka ndikim në dy ose më shumë shtete, në përputhje me nenin 23 të kësaj rregulloreje.

6. Kufiri i materialitetit për kriterin “humbjet e të dhënave” arrihet kur plotësohet ndonjë nga kushtet e mëposhtme:

a) çdo ndikim i përmendur në nenin 24 të kësaj rregulloreje, mbi disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave ka ose do të ketë një ndikim negativ në zbatimin e objektivave të biznesit të subjektit financiar, ose në aftësinë e tij për të përmbushur kërkesat rregullatore;

b) çdo akses i suksesshëm, keqdashës dhe i paautorizuar, që nuk mbulohet nga parashikimet e shkronjës “a” të kësaj pike, ndodh në rrjet dhe sistemet e informacionit, ku një akses i tillë mund të rezultojë në humbje të të dhënave.

7. Kufiri i materialitetit për kriterin “ndikim ekonomik” arrihet kur kostot dhe humbjet e shkaktuara subjektit financiar nga incidenti, kanë tejkaluar ose ka të ngjarë të tejkalojnë vlerën ekuivalente në Lek të shumës 100,000 euro.

Neni 29

Kufijtë për përcaktimin e kërcënimeve kibernetike të rëndësishme

1. Për qëllime të pikës 2 të nenit 19 të kësaj rregulloreje, një kërcënim kibernetik do të konsiderohet i rëndësishëm kur plotësohen të gjitha kushtet e mëposhtme:

a) kërcënimi kibernetik, nëse materializohet, mund të ndikojë ose mund të ketë ndikuar në funksionet kritike ose të rëndësishme të subjektit financiar, ose mund të prekë subjekte të tjera financiare, ofrues të palëve të treta, klientë ose kundërparti financiare, bazuar në informacionin në dispozicion të subjektit financiar;

b) kërcënimi kibernetik ka një probabilitet të lartë për t’u materializuar te subjekti financiar ose te subjekte të tjera financiare, duke marrë në konsideratë të paktën elementet e mëposhtme:

i. rreziqet e aplikueshme që lidhen me kërcënimin kibernetik të parashikuar në shkronjën “a” të kësaj pike, duke përfshirë edhe vulnerabilitetet e mundshme të sistemeve të subjektit financiar që mund të shfrytëzohen;

ii. aftësitë dhe synimet e aktorëve të kërcënimit në masën e njohur nga subjekti financiar;

iii. vazhdimësinë e kërcënimit dhe çdo njohuri të grumbulluar në lidhje me incidentet që kanë ndikuar te njësia ekonomike ose ofruesi i saj palë e tretë, klientët ose homologët financiarë;

c) kërcënimi kibernetik, nëse materializohet, plotëson një nga elementet e mëposhtme:

i. kriterin në lidhje me kritikalitetin e shërbimeve të prekura të parashikuar në nenin 19, pika 1, shkronja “e”, dhe të detajuar në nenin 25 të kësaj rregulloreje;

ii. kufirin e materialitetit të përcaktuar në nenin 28, pika 1, të kësaj rregulloreje;

iii. kufirin e materialitetit të përcaktuar në nenin 28, pika 5, të kësaj rregulloreje.

2. Subjekti financiar, në varësi të llojit të kërcënimit kibernetik dhe informacionit të disponueshëm, nëse arrin në përfundimin se mund të arrihen/plotësohen kufijtë e materialitetit të përcaktuar në nenin 28, pikat 3, 4, 6 dhe 7 të kësaj rregulloreje, mund të konsiderojë, gjithashtu, edhe këta kufij, kur përcakton një kërcënim kibernetik si të rëndësishëm.

NËNKREU III

RAPORTIMI I INCIDENTEVE TË LIDHURA me TIK-un DHE NJOFTIMI VULLNETAR PËR KËRCËNIMET KIBERNETIKE

Neni 30

Raportimi i incidenteve madhore të lidhura me TIK-un dhe njoftimi vullnetar për kërcënimet kibernetike të rëndësishme

1. Subjektet financiare raportojnë në Bankën e Shqipërisë incidentet madhore të lidhura me TIK-un, sipas kërkesave të përcaktuara në pikën 6 të këtij neni. Pa cenuar raportimin në Bankën e Shqipërisë në përputhje me këtë pikë, subjektet financiare paraqesin njoftimin fillestar dhe çdo raport të përmendur në pikën 6 të këtij neni, sipas formularëve të raportimit të parashikuar në nenin 36 të kësaj rregulloreje, edhe tek autoriteti përgjegjës për sigurinë kibernetike dhe/ose tek ekipet e përgjigjes ndaj incidenteve të sigurisë kibernetike (CSIRT), të ngritura në përputhje me ligjin “Për sigurinë kibernetike”.

2. Për qëllime të pikës 1 të këtij neni, subjektet financiare, pasi mbledhin dhe analizojnë të gjithë informacionin përkatës, përgatitin njoftimin dhe raportet e parashikuara në pikën 6 të këtij neni, sipas formularëve të raportimit të parashikuar në nenin 36 të kësaj rregulloreje, dhe i paraqesin pranë Bankës së Shqipërisë. Në rastet kur një pamundësi teknike pengon paraqitjen e njoftimit fillestar sipas formularëve të raportimit, subjektet financiare duhet të njoftojnë Bankën e Shqipërisë me mjete alternative.

3. Njoftimi fillestar dhe raportet e parashikuara në pikën 6 të këtij neni, do të përfshijnë të gjithë informacionin e nevojshëm për Bankën e Shqipërisë, për të përcaktuar rëndësinë e incidentit madhor të lidhur me TIK-un, si dhe për të vlerësuar ndikimet e mundshme në shtete të tjera (ndërkufitare).

4. Subjektet financiare njoftojnë vullnetarisht Bankën e Shqipërisë për kërcënime kibernetike, të rëndësishme për sistemin financiar, përdoruesit e shërbimeve ose klientët. Banka e Shqipërisë mund ta përcjellë këtë informacion edhe tek autoritete të tjera përkatëse. Subjektet financiare që njoftojnë Bankën e Shqipërisë sipas kërkesave të kësaj pike, paraqesin këtë njoftim edhe tek ekipet e përgjigjes ndaj incidenteve të sigurisë kibernetike (CSIRT), të ngritura në përputhje me ligjin “Për sigurinë kibernetike”.

5. Kur ndodh një incident madhor i lidhur me TIK-un dhe ka ndikim në interesat financiarë të klientëve, subjektet financiare, menjëherë dhe pa vonesa të panevojshme sapo vihen në dijeni të incidentit, informojnë klientët e tyre për incidentin madhor të lidhur me TIK-un, si dhe për të gjitha masat që janë marrë për të zbutur efektet negative të një incidenti të tillë. Në rast të një kërcënimi kibernetik të rëndësishëm, subjektet financiare, aty ku është e zbatueshme, informojnë klientët e tyre që mund të preken, për çdo masë të përshtatshme mbrojtëse që subjektet mund të ndërmarrin.

6. Subjektet financiare i paraqesin Bankës së Shqipërisë, sipas afateve kohore të parashikuara në nenin 35 të kësaj rregulloreje:

a) një njoftim fillestar;

b) një raport të ndërmjetëm, pas njoftimit fillestar të parashikuar në shkronjën “a” të kësaj pike, sapo statusi i incidentit origjinal të ketë ndryshuar ndjeshëm ose trajtimi i incidentit madhor të lidhur me TIK-un ka ndryshuar në bazë të informacionit të ri të disponueshëm, i ndjekur, sipas rastit, nga njoftime të përditësuara sa herë që disponohet një përditësim përkatës i statusit, si dhe sipas kërkesave specifike të Bankës së Shqipërisë;

c) një raport përfundimtar, kur ka përfunduar analiza e shkakut bazë, pavarësisht nëse masat zbutëse janë zbatuar apo jo, dhe kur shifrat reale të ndikimit janë të disponueshme për të zëvendësuar vlerësimet e paraqitura nga subjekti.

7. Subjektet financiare do të përdorin kanale të sigurta komunikimi për të dorëzuar njoftimin fillestar dhe raportet e ndërmjetme dhe përfundimtare. Subjektet financiare që nuk janë në gjendje të përdorin kanalet e sigurta të komunikimit, duhet të informojnë Bankën e Shqipërisë për incidentin madhor të lidhur me TIK-un, nëpërmjet mjeteve të tjera të sigurta të komunikimit, të dakorduara me Bankën e Shqipërisë. Nëse kërkohet nga Banka e Shqipërisë, subjektet financiare duhet të riparaqesin njoftimin fillestar, raportin e ndërmjetëm ose raportin përfundimtar, nëpërmjet kanalit të sigurt të komunikimit, pasi të jenë në gjendje ta bëjnë këtë.

8. Subjektet financiare mund të lidhin marrëveshje me të tretët për transferimin e detyrimeve për raportim sipas kërkesave të këtij neni. Pavarësisht nga transferimi i detyrimeve për raportim, subjekti financiar mbetet plotësisht përgjegjës për përmbushjen e kërkesave për raportimin e incidenteve.

9. Subjektet financiare që kanë lidhur marrëveshje me të tretët për transferimin e detyrimeve për raportim të incidenteve madhore të lidhura me TIK-un, në përputhje me pikën 8 të këtij neni, njoftojnë Bankën e Shqipërisë për atë marrëveshje, sapo të jetë nënshkruar marrëveshja dhe në çdo rast, jo më vonë se para njoftimit ose raportimit të parë.

10. Subjektet financiare i paraqesin Bankës së Shqipërisë emrin, detajet e kontaktit dhe kodin e identifikimit të palës së tretë që do të dorëzojë në emër të tyre njoftimet ose raportet e incidenteve madhore të lidhur me TIK-un.

11. Subjektet financiare informojnë menjëherë Bankën e Shqipërisë nëse nuk vijnë të transferojnë detyrimin për raportim të incidenteve madhore të lidhura me TIK-un te palë të treta, siç parashikohet në pikën 8 të këtij neni.

12. Pas marrjes së njoftimit fillestar dhe të çdo raporti të përmendur në pikën 6 të këtij neni, Banka e Shqipërisë, brenda një kohe të arsyeshme, vë në dispozicion detaje të incidentit madhor të lidhur me TIK-un, edhe tek autoriteti përgjegjës për sigurinë kibernetike, pikat e vetme të kontaktit ose tek ekipet e përgjigjes ndaj incidenteve të sigurisë kibernetike (CSIRT), të ngritura në përputhje me ligjin “Për sigurinë kibernetike”, si dhe tek autoritete të tjera publike përkatëse.

13. Pas marrjes së njoftimit fillestar dhe të çdo raporti të përmendur në pikën 6 të këtij neni, Banka e Shqipërisë, brenda një kohe të arsyeshme dhe në përputhje me nenin 19(6) të Rregullores (BE) 2022/2554, vë në dispozicion detaje të incidentit madhor të lidhur me TIK-un, edhe tek EBA-ja dhe ECB-ja në rastin e subjekteve financiare të parashikuara në nenin 2, pika 1, shkronjat “a”, “b” dhe “d” të kësaj rregulloreje, si dhe te SRB-ja (*Single Resolution Board*) për subjektet e referuara në nenin 7(2) dhe 7(4)(b) e 7(5) të Rregullores (BE) 806/2014, nëse incidentet krijojnë rreziqe për garantimin e funksioneve kritike.

14. Pas marrjes së informacionit në përputhje me nenin 19(6) të Rregullores (BE) 2022/2554, EBA-ja dhe ECB-ja, në konsultim me ENISA-n dhe në bashkëpunim me Bankën e Shqipërisë, vlerësojnë nëse incidenti madhor i lidhur me TIK-un është i rëndësishëm për autoritetet përgjegjëse në shtetet e tjera anëtare. Pas këtij vlerësimi, EBA-ja njofton sa më shpejt që të jetë e mundur autoritetet përgjegjëse përkatëse në shtetet e tjera anëtare. ECB-ja njofton anëtarët e Sistemit Evropian të Bankave Qendrore mbi çështje të rëndësishme për sistemin e pagesave. Bazuar në njoftimin e marrë, autoritetet përgjegjëse të shteteve të tjera anëtare, kur është e përshtatshme, marrin të gjitha masat e nevojshme për të mbrojtur qëndrueshmërinë e menjëhershme të sistemit financiar.

15. Vlerësimi nëse incidenti madhor është i rëndësishëm për autoritetet përgjegjëse në shtetet e tjera anëtare, siç parashikohet në nenin 19(7) të Rregullores (BE) 2022/2554, bazohet në faktin nëse incidenti ka një shkak bazë që buron nga një shtet tjetër anëtar ose nëse incidenti ka ose ka pasur një ndikim të rëndësishëm në një shtet tjetër anëtar, në lidhje me cilindo nga elementet e mëposhtme:

- a) klientët ose kundërpasuritë financiare;
- b) një degë të subjektit financiar ose një subjekt tjetër financiar brenda grupit;
- c) një infrastrukturë të tregut financiar ose një ofrues të palës së tretë që mund të ndikojë në subjektet financiare të cilave iu ofron shërbime.

16. Detajet e incidenteve madhore që Banka e Shqipërisë i paraqet autoriteteve të tjera përgjegjëse në përputhje me pikën 12 të këtij neni, përmbajnë të njëjtin nivel informacioni, pa asnjë anonimizim, si njoftimet dhe raportet e incidenteve madhore të marra nga subjektet financiare në përputhje me pikën 6 të këtij neni.

17. Detajet e incidenteve madhore që Banka e Shqipërisë i paraqet autoriteteve të tjera përgjegjëse në përputhje me pikën 13 të këtij neni, si dhe njoftimet që do të bëhen nga EBA-ja dhe BQE tek autoritetet përkatëse përgjegjëse në shtetet e tjera anëtare në përputhje me nenin 19(7) të Rregullores (BE) 2022/2554, duhet të përmbajnë të njëjtin nivel informacioni, pa asnjë anonimizim, si njoftimet dhe raportet e incidenteve madhore të marra nga subjektet financiare në përputhje me nenin 19(4) të Rregullores (BE) 2022/2554.

18. Institucionet e kreditit të klasifikuara si “të rëndësishme” sipas nenit 6(4) të Rregullores (BE) nr. 1024/2013, raportojnë incidentet madhore të lidhur me TIK-un pranë Bankës së Shqipërisë, e cila ia transmeton menjëherë këtë raportim, Bankës Qendrore Evropiane (ECB).

19. Institucionet e kreditit të klasifikuara si “të rëndësishme” sipas nenit 6(4) të Rregullores (BE) nr. 1024/2013, mund të njoftojnë vullnetarisht Bankën e Shqipërisë për kërcënime kibernetike të rëndësishme, e cila ia transmeton menjëherë këtë njoftim Bankës Qendrore Evropiane (ECB).

Neni 31

Informacioni i përgjithshëm që përfshihet në njoftimin fillestar dhe raportet e ndërmjetme dhe përfundimtare mbi incidentet madhore të lidhura me TIK-un

1. Subjektet financiare përfshijnë në njoftimin fillestar, raportin e ndërmjetëm dhe raportin përfundimtar, siç parashikohet në nenin 30, pika 6, të kësaj rregulloreje, informacionin e përgjithshëm të mëposhtëm:

- a) llojin e raportit (njoftim fillestar, raport i ndërmjetëm ose raport përfundimtar);
- b) emrin e subjektit financiar, kodin NUIS/LEI të tij dhe llojin e subjektit financiar, siç përcaktohet në nenin 2, pika 1 të kësaj rregulloreje;
- c) emrin dhe kodin e identifikimit të subjektit që paraqet njoftimin fillestar, raportin e ndërmjetëm ose përfundimtar, për subjektin financiar;
- d) sipas rastit, emrat dhe kodet NUIS/LEI të të gjitha subjekteve financiare të përfshira në njoftimin fillestar ose raportin e ndërmjetëm ose përfundimtar të agreguar;
- e) detajet e kontaktit të personave përgjegjës për komunikimin me Bankën e Shqipërisë për incidentin madhor të lidhur me TIK-un;
- f) sipas rastit, identifikimin e shoqërisë mëmë të grupit të cilit i përket subjekti financiar;
- g) aty ku ka efekt monetar, paraqitet edhe monedha ku bazohen shumatat e raportuara.

Neni 32

Informacioni specifik për t'u përfshirë në njoftimin fillestar

1. Njoftimi fillestar i parashikuar në nenin 30, pika 6, shkronja “a”, të kësaj rregulloreje, përmban të paktën të gjithë informacionin specifik të mëposhtëm:

- a) kodin e referencës të incidentit, të caktuar nga subjekti financiar;
- b) datën e zbulimit, kohën e zbulimit dhe të klasifikimit të incidentit, në përputhje me nenin 27 të kësaj rregulloreje;
- c) një përshkrim të incidentit të lidhur me TIK-un;
- d) kriteret, të përcaktuara në nenet 20 deri në 27 të kësaj rregulloreje, në bazë të të cilave subjekti financiar e klasifikon incidentin e lidhur me TIK-un, si incident madhor;
- e) shtetet e tjera që ndikohen nga incidenti i lidhur me TIK-un;
- f) informacion se si u zbulua incidenti i lidhur me TIK-un;
- g) kur është e mundur, informacion në lidhje me origjinën e incidentit të lidhur me TIK-un;
- h) informacion nëse subjekti financiar ka aktivizuar një plan të vazhdimësisë së biznesit;
- i) kur është e aplikueshme, informacion në lidhje me riklasifikimin e incidentit të lidhur me TIK-un nga incident madhor në jomadhor;
- j) kur disponohet, çdo informacion tjetër përkatës.

Neni 33

Informacioni specifik për t'u përfshirë në raportet e ndërmjetme

1. Raportet e ndërmjetme siç parashikohen në nenin 30, pika 6, shkronja “b”, të kësaj rregulloreje, përmbajnë të paktën të gjithë informacionin specifik të mëposhtëm:

- a) aty ku është e aplikueshme, kodin e referencës së incidentit të caktuar nga Banka e Shqipërisë;

- b) datën dhe orën e ndodhjes së incidentit të lidhur me TIK-un;
- c) sipas rastit, datën dhe orën kur subjekti financiar ka rikuperuar aktivitetet e tij të rregullta;
- d) informacion se si janë përmbushur kriteret e përcaktuara në nenet 20 deri në 27 të kësaj rregulloreje, në bazë të të cilave subjekti financiar e ka klasifikuar incidentin e lidhur me TIK-un si incident madhor;
- e) llojin e incidentit të lidhur me TIK-un;
- f) aty ku është e aplikueshme, kërcënimet dhe teknikat e përdorura nga aktori i kërcënimit;
- g) zonat funksionale dhe proceset e biznesit të prekura;
- h) komponentët e infrastrukturës së prekur që mbështesin proceset e biznesit;
- i) ndikimi në interesat financiarë të klientëve;
- j) informacion në lidhje me raportimin për incidentin e lidhur me TIK-un tek autoritete të tjera;
- k) veprimet ose masat e përkohshme të ndërmarra ose të planifikuara për t'u ndërmarrë nga subjekti financiar, për t'u rikuperuar nga incidenti i lidhur me TIK-un;
- l) aty ku është e aplikueshme, informacion mbi treguesit e kompromentimit.

Neni 34

Informacioni specifik për t'u përfshirë në raportet përfundimtare

1. Raportet përfundimtare siç parashikohen në nenin 30, pika 6, shkronja "c", të kësaj rregulloreje, përmbajnë të paktën të gjithë informacionin specifik të mëposhtëm:
 - a) informacion rreth shkaqeve bazë të incidentit të lidhur me TIK-un;
 - b) datën dhe orën kur incidenti i lidhur me TIK-un u zgjidh dhe shkaku/shkaqet bazë u adresuan;
 - c) informacion mbi zgjidhjen e incidentit të lidhur me TIK-un;
 - d) aty ku është e aplikueshme, informacione të rëndësishme për autoritetin e ndërhyrjes së jashtëzakonshme;
 - e) informacion në lidhje me kostot dhe humbjet direkte dhe indirekte që rrjedhin nga incidenti i lidhur me TIK-un, si dhe informacion për vlerat e rikuperuara;
 - f) aty ku është e aplikueshme, informacion në lidhje me incidentet e përsëritura të lidhura me TIK-un.

Neni 35

Afatet kohore për njoftimin fillestar dhe paraqitjen e raporteve të ndërmjetme dhe përfundimtare

1. Subjektet financiare paraqesin pranë Bankës së Shqipërisë njoftimin fillestar dhe raportet e ndërmjetme dhe përfundimtare të parashikuara në nenin 30, pika 6, shkronjat "a", "b" dhe "c" të kësaj rregulloreje, brenda afateve kohore të mëposhtme:
 - a) për raportin fillestar: sa më shpejt që të jetë e mundur, por në çdo rast, brenda 4 orëve nga momenti i klasifikimit të incidentit të lidhur me TIK-un, si incident madhor i lidhur me TIK-un, dhe jo më vonë se 24 orë nga momenti kur subjekti financiar ka marrë dijeni për incidentin e lidhur me TIK-un;
 - b) për raportin e ndërmjetëm: jo më vonë se brenda 72 orëve nga paraqitja e njoftimit fillestar, edhe nëse statusi ose trajtimi i incidentit nuk ka ndryshuar, siç parashikohet në nenin 30, pika 6, shkronja "b", të kësaj rregulloreje. Subjektet financiare duhet të paraqesin një raport të ndërmjetëm të përditësuar pa vonesa të panevojshme dhe në çdo rast kur veprimtaria e tyre e rregullt (e zakonshme) është rikuperuar;

c) për raportin përfundimtar: jo më vonë se një muaj pas paraqitjes së raportit të ndërmjetëm, ose, sipas rastit, pas paraqitjes së raportit të ndërmjetëm të përditësuar më të fundit.

2. Kur subjekti financiar nuk e ka klasifikuar një incident të lidhur me TIK-un si incident madhor brenda 24 orëve nga momenti kur subjekti financiar ka marrë dijeni për incidentin e lidhur me TIK-un, por e klasifikon atë incident të lidhur me TIK-un si incident madhor në një fazë të mëvonshme, subjekti financiar duhet të paraqesë njoftimin fillestar brenda 4 orëve nga klasifikimi i incidentit të lidhur me TIK-un si incident madhor.

3. Subjektet financiare që nuk janë në gjendje të dorëzojnë njoftimin fillestar, raportin e ndërmjetëm ose raportin përfundimtar brenda afateve kohore të përcaktuara në pikën 1 të këtij neni, duhet të njoftojnë Bankën e Shqipërisë pa vonesa të panevojshme, por jo më vonë se afatet kohore përkatëse për paraqitjen e njoftimit ose raportit, si dhe të shpjegojnë arsyet e vonesës.

4. Kur afati kohor për dorëzimin e njoftimit fillestar, raportit të ndërmjetëm ose raportit përfundimtar bie në një ditë fundjave ose një feste zyrtare, subjekti financiar mund të paraqesë njoftimin fillestar, raportet e ndërmjetme ose përfundimtare deri në mesditën e ditës pasuese të punës.

5. Pika 4 e këtij neni nuk zbatohet për paraqitjen e një njoftimi fillestar ose një raporti të ndërmjetëm nga institucionet e kreditit dhe subjektet e tjera financiare të identifikuar si infrastruktura kritike dhe të rëndësishme, në përputhje me ligjin “Për sigurinë kibernetike”.

6. Banka e Shqipërisë mund të vendosë që pika 4 e këtij neni të mos zbatohet për paraqitjen e njoftimit fillestar ose të raportit të ndërmjetëm, edhe nga subjekte financiare të ndryshme nga ato të parashikuara në pikën 5 të këtij neni, të cilat janë të rëndësishme ose kanë karakter sistematik për sektorin financiar. Banka e Shqipërisë njofton vendimin e saj të subjektet financiare të identifikuar. Vendimi i Bankës së Shqipërisë do të zbatohet vetëm për incidentet e raportuara pas datës së njoftimit të vendimit të Bankës së Shqipërisë.

7. Subjektet financiare mund të kombinojnë paraqitjen e njoftimit fillestar, raportit të ndërmjetëm dhe raportit përfundimtar, duke i paraqitur pranë Bankës së Shqipërisë të dy ose të gjitha raportet në të njëjtën kohë, nëse aktivitetet e rregullta të subjektit janë rikuperuar ose analiza e shkakut bazë të incidentit është përfunduar dhe me kusht që të respektohen afatet kohore të përcaktuara në këtë nen.

Neni 36

Formularët e raportimit të incidenteve madhore të lidhura me TIK-un

1. Subjektet financiare do të përdorin formularët e raportimit të parashikuar në Aneksin 1 të kësaj rregulloreje, për të paraqitur pranë Bankës së Shqipërisë njoftimin fillestar, raportin e ndërmjetëm dhe raportin përfundimtar, siç përcaktohet në nenin 30, pika 6, të kësaj rregulloreje, si vijon:

a) subjektet financiare që paraqesin njoftimin fillestar duhet të plotësojnë fushat e formularit që i korrespondojnë informacionit që duhet të paraqitet në përputhje me nenin 32 të kësaj rregulloreje dhe, në rastet kur e disponojnë tashmë informacionin përkatës, mund të plotësojnë edhe ato fusha, plotësimi i të cilave nuk kërkohet për njoftimin fillestar, por kërkohet për një raport të ndërmjetëm ose përfundimtar;

b) subjektet financiare që paraqesin raportin e ndërmjetëm duhet të plotësojnë fushat e formularit që i korrespondojnë informacionit që duhet të paraqitet në përputhje me nenin 33 të kësaj rregulloreje dhe, në rastet kur e disponojnë tashmë informacionin përkatës, mund të plotësojnë edhe ato fusha, plotësimi i të cilave nuk kërkohet për raportin e ndërmjetëm, por kërkohet për raportin përfundimtar;

c) subjektet financiare që paraqesin raportin përfundimtar duhet të plotësojnë fushat e formularit që i korrespondojnë informacionit që duhet të paraqitet në përputhje me nenin 34 të kësaj rregulloreje.

2. Subjektet financiare sigurojnë që informacioni që përmban njoftimi fillestar, raporti i ndërmjetëm dhe përfundimtar, të jetë i plotë dhe i saktë.

3. Subjektet financiare paraqesin vlera/shuma të vlerësuara, bazuar në të dhëna dhe informacione të tjera të disponueshme, për aq sa është e mundur, nëse nuk disponohen të dhëna të sakta në momentin e raportimit për njoftimin fillestar ose raportin e ndërmjetëm.

4. Subjektet financiare, kur paraqesin një raport të ndërmjetëm ose përfundimtar, përdorin formularët e parashikuar në Aneksin 1 të kësaj rregulloreje, paraqesin të gjithë informacionin e kërkuar dhe përditësojnë, sipas rastit, informacionin që kanë paraqitur më parë në njoftimin fillestar ose në raportin e ndërmjetëm.

5. Subjektet financiare plotësojnë formularët e parashikuar në Aneksin 1, sipas udhëzimeve të përcaktuara në Aneksin 2 të kësaj rregulloreje.

Neni 37

Përmbajtja e njoftimit për kërcënimet kibernetike të rëndësishme

1. Përmbajtja e njoftimit për kërcënimet kibernetike të rëndësishme, të parashikuar në nenin 30, pika 4, të kësaj rregulloreje, përfshin:

a) informacione të përgjithshme për subjektin financiar që po njofton, siç përcaktohet në nenin 31 të kësaj rregulloreje;

b) datën dhe orën e zbulimit të kërcënimit kibernetik të rëndësishëm dhe çdo vulë tjetër kohore përkatëse në lidhje me kërcënimin kibernetik të rëndësishëm;

c) një përshkrim të kërcënimit kibernetik të rëndësishëm;

d) informacion në lidhje me ndikimin e mundshëm të kërcënimit kibernetik të rëndësishëm mbi subjektin financiar, klientët e tij ose kundërpartitë financiare;

e) kriteret e klasifikimit që do të kishin shkaktuar një raport incidenti madhor të përcaktuar në nenin 20 deri në 27 të kësaj rregulloreje, nëse kërcënimi kibernetik do të ishte materializuar;

f) informacion në lidhje me statusin e kërcënimit kibernetik të rëndësishëm dhe çdo ndryshim në aktivitetin e kërcënimit;

g) sipas rastit, një përshkrim të veprimeve të ndërmarra nga subjekti financiar për të parandaluar materializimin e kërcënimeve kibernetike të rëndësishme;

h) informacion në lidhje me çdo njoftim të kërcënimit kibernetik të rëndësishëm ndaj subjekteve financiare ose autoriteteve të tjera;

i) aty ku është e aplikueshme, informacion mbi treguesit e kompromentimit;

j) kur disponohet, çdo informacion tjetër përkatës.

2. Subjektet financiare që njoftojnë Bankën e Shqipërisë për kërcënimet kibernetike të rëndësishme sipas kërkesave të nenit 30, pika 4, të kësaj rregulloreje, plotësojnë formularët e parashikuar në Aneksin 3, sipas udhëzimeve të përcaktuara në Aneksin 4 të kësaj rregulloreje.

3. Subjektet financiare sigurojnë që informacioni që përmban njoftimi për kërcënimet kibernetike të rëndësishme të jetë i plotë dhe i saktë.

Neni 38

Raportimi i agreguar

1. Një ofrues shërbimi i palëve të treta, të cilit i janë transferuar detyrimet e raportimit, siç parashikohet në nenin 30, pika 8, të kësaj rregulloreje, mund të përdorë formularët e parashikuar në Aneksin 1 të kësaj rregulloreje për të raportuar informacion të agreguar në lidhje me një incident madhor të lidhur me TIK-un, që prek disa subjekte financiare, në një njoftim ose raport të vetëm, dhe ta paraqesë atë njoftim ose raport te Banka e Shqipërisë në emër të të gjitha subjekteve financiare të prekura, me kusht që të përmbushen të gjitha kushtet e mëposhtme:

a) incidenti madhor i lidhur me TIK-un që duhet raportuar buron nga ose shkaktohet nga një ofrues shërbimi i palëve të treta të TIK-ut;

b) ai ofrues shërbimi i palëve të treta të TIK-ut ofron shërbimin përkatës TIK për më shumë se një subjekt financiar, ose për një grup;

c) incidenti i lidhur me TIK-un klasifikohet si madhor nga secili subjekt financiar i përfshirë në njoftimin ose raportin e agreguar;

d) incidenti madhor i lidhur me TIK-un prek subjektet financiare brenda Shqipërisë dhe raporti i agreguar lidhet me subjektet financiare që mbikëqyren nga Banka e Shqipërisë;

e) Banka e Shqipërisë i ka lejuar në mënyrë të qartë këto lloj subjektsh financiarë të agregojnë raportimet e tyre.

2. Pika 1 e këtij neni nuk zbatohet për institucionet e kreditit të klasifikuara si “të rëndësishme”, sipas nenit 2, pika (16) e Rregullores (BE) nr. 468/2014 të Bankës Qendrore Evropiane (BQE), ku këto institucione do të përdorin formularët e parashikuar në Aneksin 1 të kësaj rregulloreje për të raportuar vetëm mbi baza individuale, informacionin në lidhje me një incident madhor të lidhur me TIK-un pranë Bankës së Shqipërisë.

3. Kur Banka e Shqipërisë kërkon informacion mbi ndikimin individual të incidentit madhor të lidhur me TIK-un mbi një subjekt të vetëm financiar, me kërkesë të saj, subjekti financiar duhet të paraqesë një njoftim ose një raport individual mbi incidentin madhor të lidhur me TIK-un.

Neni 39

Roli mbikëqyrës

1. Pa cenuar kontributin teknik, këshillat ose mjetet për korrigjimin dhe ndjekjen e mëtejshme që mund të sigurohen nga CSIRT-të, në përputhje me ligjin “Për sigurinë kibernetike”, Banka e Shqipërisë, me marrjen e njoftimit fillestar dhe të çdo raporti të parashikuar në nenin 30, pika 6, të kësaj rregulloreje, pranon marrjen e njoftimit apo të raportit dhe, ku është e mundur, i jep subjektit financiar komentet ose udhëzimet e nevojshme dhe proporcionale, në veçanti duke i vënë në dispozicion çdo informacion dhe inteligjencë anonime përkatëse për kërcënime të ngjashme, dhe mund të diskutojë zgjidhjet e aplikuara në nivel të subjektit financiar dhe mënyrat për të minimizuar dhe zbutur ndikimin negativ në të gjithë sektorin financiar. Në çdo rast, pavarësisht komenteve mbikëqyrëse të marra, subjektet financiare do të mbeten plotësisht përgjegjëse për trajtimin dhe për pasojat e incidenteve të lidhura me TIK-un, të raportuara në përputhje me nenin 30, pika 1, të kësaj rregulloreje.

Neni 40

Incidentet operacionale ose të sigurisë të lidhura me pagesat për bankat, institucionet e pagesave, ofruesit e shërbimit të informimit të llogarisë dhe institucionet e parasë elektronike

1. Kërkesat e përcaktuara në këtë kre do të zbatohen në të njëjtën mënyrë edhe për incidentet operacionale ose të sigurisë të lidhura me pagesat të parashikuara në nenin 89 të ligjit “Për shërbimet e pagesave”, përfshirë edhe incidentet madhore operacionale ose të sigurisë të lidhura me pagesat, për bankat, institucionet e pagesave, ofruesit e shërbimit të informimit të llogarisë dhe institucionet e parasë elektronike.

KREU IV

TESTIMI I QËNDRUESHMËRISË OPERACIONALE DIGJITALE

Neni 41

Kërkesa të përgjithshme për kryerjen e testimit të qëndrueshmërisë operacionale digjitale

1. Për qëllime të vlerësimit të shkallës së përgatitjes për trajtimin e incidenteve të lidhura me TIK-un, të identifikimit të dobësive, mangësive ose boshllëqeve në qëndrueshmërinë operacionale digjitale, si dhe të zbatimit të menjëhershëm të masave korrigjuese, subjektet financiare, me përjashtim të mikrondërmarrjeve, duke marrë parasysh kriteret e parashikuara në nenin 5, pika 2, të kësaj rregulloreje, krijojnë, mirëmbajnë dhe rishikojnë, një program të shëndoshë dhe gjithëpërfshirës të testimit të qëndrueshmërisë operacionale digjitale, si pjesë integrale të sistemit të administrimit të rrezikut të TIK-ut të parashikuar në nenin 7 të kësaj rregulloreje.

2. Programi i testimit të qëndrueshmërisë operacionale digjitale përfshin një sërë vlerësimesh, testesh, metodologjish, praktikash dhe mekanizmash që do të zbatohen në përputhje me kërkesat e neneve 42 dhe 43 të kësaj rregulloreje.

3. Subjektet financiare, me përjashtim të mikrondërmarrjeve, gjatë hartimit të programit të testimit të qëndrueshmërisë operacionale digjitale të parashikuar në pikën 1 të këtij neni, ndjekin një qasje të bazuar në rrezik, marrin parasysh kriteret e parashikuara në nenin 5, pika 2, të kësaj rregulloreje, si dhe duke konsideruar ambientin në zhvillim të rreziqeve të TIK-ut, çdo rrezik specifik ndaj të cilit është i ekspozuar ose mund të ekspozohet subjekti financiar, kritikalitetin e aseteve të informacionit dhe shërbimeve të ofruara, si dhe çdo faktor tjetër që subjekti financiar e gjykon të përshtatshëm.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, sigurojnë që testimet të kryhen nga palë të pavarura, qofshin ato të brendshme apo të jashtme. Kur testimet kryhen nga një testues i brendshëm, subjektet financiare i përkushtojnë burime të mjaftueshme dhe sigurojnë që konfliktet e interesit të shmangen gjatë fazave të projektimit dhe kryerjes së testimit.

5. Subjektet financiare, me përjashtim të mikrondërmarrjeve, hartojnë politika dhe procedura për të përcaktuar prioritetet, për të klasifikuar dhe korrigjuar të gjitha çështjet e identifikuara gjatë kryerjes së testeve, si dhe hartojnë metodologji të brendshme të vlerësimit, për të siguruar që të gjitha dobësitë, mangësitë ose boshllëqet e identifikuara janë adresuar plotësisht.

6. Subjektet financiare me përjashtim të mikrondërmarrjeve, të paktën çdo vit, kryejnë testimet përkatëse për të gjitha sistemet e TIK-ut dhe aplikacionet që mbështetin funksionet kritike ose të rëndësishme.

Neni 42

Testimi i mekanizmave dhe sistemeve të TIK-ut

1. Programi i testimit të qëndrueshmërisë operacionale digjitale i parashikuar në nenin 41 të kësaj rregulloreje, në përputhje me kriteret e parashikuara në nenin 5, pika 2, duhet të parashikojë kryerjen e testeve të përshtatshme, që përfshijnë vlerësimet dhe skanimet e cenueshmërisë, analizat e bazuara në burime të hapura (*open source analyses*), vlerësimet e sigurisë së rrjetit, analizat e mangësive (*gap analyses*), rishikimet e sigurisë fizike, pyetësorët dhe zgjidhjet e *software* të skanimit, rishikimet e kodit burimor (*source code*) aty ku është e mundur, testet e bazuara në skenarë, testimin e përputhshmërisë, testimin e performancës, testimin nga fundi në fund (*end-to-end testing*) ose testimin e depërtueshmërisë (*penetration testing*).

2. Mikrondërmarrjet kryejnë testet e parashikuara në pikën 1 të këtij neni, duke kombinuar një qasje të bazuar në rrezik me një planifikim strategjik të testimit të TIK-ut, duke marrë në konsideratë nevojën për të mbajtur një qasje të balancuar ndërmjet shkallës së burimeve dhe kohës që nevojitet për testimin e TIK-ut të parashikuar në këtë nen, nga njëra anë, dhe urgjencës,

llojit të rrezikut, kritikalitetit të aseteve të informacionit dhe shërbimeve të ofruara, si dhe faktorëve të tjerë të rrezikut, përfshirë edhe aftësinë e subjektit financiar për të ndërmarrë rreziqe të llogaritura, nga ana tjetër.

Neni 43

Testimi i avancuar i mekanizmave, sistemeve dhe proceseve të TIK-ut, bazuar në testimin e depërtueshmërisë të udhëhequr nga kërcënimi

1. Subjektet financiare, me përjashtim të mikrondërmarrjeve, dhe subjektet e parashikuara në pikën 1 të nenit 17 të kësaj rregulloreje, të identifikuar në përputhje me pikën 11 të këtij neni, duhet të kryejnë të paktën çdo 3 vjet testim të avancuar, nëpërmjet testimit të depërtueshmërisë të udhëhequr nga kërcënimi. Banka e Shqipërisë, bazuar në profilin e rrezikut të subjektit financiar dhe duke marrë në konsideratë rrethanat operationale, kur e gjykon të nevojshme, mund t'i kërkojë subjektit financiar të reduktojë ose të rritë shpeshtësinë e kryerjes së këtij testimi.

2. Testimi i depërtueshmërisë i udhëhequr nga kërcënimi duhet të mbulojë disa funksione ose të gjitha funksionet kritike ose të rëndësishme të subjektit financiar dhe duhet të kryhet në sistemet *live* të prodhimit që mbështesin funksione të tilla.

3. Subjektet financiare duhet të identifikojnë të gjitha sistemet, proceset dhe teknologjitë përkatëse bazë të TIK-ut që mbështesin funksionet kritike ose të rëndësishme dhe shërbimet e TIK-ut, duke përfshirë edhe ata që mbështesin funksionet kritike ose të rëndësishme, të cilat i janë transferuar ose kontraktuar ofruesve të shërbimeve të palëve të treta të TIK-ut.

4. Subjektet financiare vlerësojnë se cilat funksione kritike ose të rëndësishme duhet të mbulohen nga testimi i depërtueshmërisë i udhëhequr nga kërcënimi. Rezultati i këtij vlerësimi do të përcaktojë objektin/fushën e saktë të testimit të depërtueshmërisë të udhëhequr nga kërcënimi dhe duhet të miratohet nga Banka e Shqipërisë.

5. Në rastet kur ofruesit e shërbimeve të palëve të treta të TIK-ut përfshihen në fushën e testimit të depërtueshmërisë të udhëhequr nga kërcënimi, subjekti financiar duhet të marrë masat dhe garancitë e të nevojshme për të siguruar pjesëmarrjen e këtyre ofruesve të shërbimeve të palëve të treta të TIK-ut në testimin e depërtueshmërisë të udhëhequr nga kërcënimi dhe do të mbajë në çdo kohë përgjegjësinë e plotë për të siguruar përputhshmërinë me kërkesat e kësaj rregulloreje.

6. Pa rënë ndesh me parashikimet e pikës 2 dhe 3 të këtij neni, kur pjesëmarrja e një ofruesi të shërbimeve të palëve të treta të TIK-ut në testimin e depërtueshmërisë të udhëhequr nga kërcënimi, të parashikuar në pikën 5 të këtij neni, pritet në mënyrë të arsyeshme të ketë një ndikim negativ në cilësinë ose sigurinë e shërbimeve të ofruara nga ofruesi i shërbimeve të palëve të treta të TIK-ut për klientët që janë subjekte jashtë objektit të kësaj rregulloreje, ose në konfidencialitetin e të dhënave që lidhen me shërbime të tilla, subjekti financiar dhe ofruesi i shërbimeve të palëve të treta të TIK-ut mund të bien dakord me shkrim që ofruesi i shërbimeve të palëve të treta të TIK-ut të hyjë drejtpërdrejt në marrëdhënie kontraktuale me një testues të jashtëm, me qëllim kryerjen, nën drejtimin e një subjekti financiar të caktuar, të një testimi të përbashkët të depërtueshmërisë të udhëhequr nga kërcënimi, që përfshin disa subjekte financiare (*pooled testing*), të cilave ofruesi i shërbimeve të palëve të treta të TIK-ut iu ofron shërbime të TIK-ut.

7. Testimi i përbashkët i parashikuar në pikën 6 të këtij neni duhet të mbulojë gamën përkatëse të shërbimeve të TIK-ut që mbështesin funksione kritike ose të rëndësishme të kontraktuara nga subjektet financiare, me ofruesit përkatës të shërbimeve të palëve të treta të TIK-ut. Testimi i përbashkët duhet të konsiderohet si testim i depërtueshmërisë i udhëhequr nga kërcënimi, i kryer nga subjektet financiare që marrin pjesë në testimin e përbashkët. Numri

i subjekteve financiare që marrin pjesë në testimin e përbashkët duhet të kalibrohet në mënyrën e duhur, duke marrë parasysh kompleksitetin dhe llojet e shërbimeve të përfshira.

8. Subjektet financiare, në bashkëpunim me ofruesit e shërbimeve të palëve të treta të TIK-ut dhe palët e tjera të përfshira, duke përfshirë edhe testuesit, por duke përjashtuar Bankën e Shqipërisë, duhet të zbatojnë kontrolle efektive të administrimit të rrezikut, për të zbutur rreziqet e çdo ndikimi të mundshëm në të dhënat, dëmtimin e aseteve dhe ndërprerjen e funksioneve, shërbimeve ose operacioneve kritike ose të rëndësishme, në vetë subjektin financiar, kundërpартitë e tjera të tij ose në sektorin financiar në tërësi.

9. Në përfundim të testimit, pasi të jetë rënë dakord për raportet dhe planet e korrigjimit (*remediation plan*), subjekti financiar dhe, kur është e aplikueshme, testuesit e jashtëm i vënë në dispozicion Bankës së Shqipërisë një përmbledhje të gjetjeve përkatëse, planet e korrigjimit dhe dokumentacionin që konfirmon se testimi i depërtueshmërisë i udhëhequr nga kërcënimi është kryer në përputhje me kërkesat rregullative. Banka e Shqipërisë i jep subjekteve financiare një konfirmim që testi është kryer në përputhje me kërkesat e paraqitura në dokumentacion, me qëllim që të lejohet njohja reciproke e testeve të depërtueshmërisë të udhëhequra nga kërcënimet midis autoriteteve të ndryshme përgjegjëse.

Pa cenuar një konfirmim të tillë, subjektet financiare mbeten në çdo kohë plotësisht përgjegjëse për ndikimin e testeve të përmendura në pikën 6 dhe 7 të këtij neni.

10. Subjektet financiare kontraktjnë testuesit në përputhje me nenin 44 të kësaj rregulloreje, për qëllime të kryerjes së testimit të depërtueshmërisë të udhëhequr nga kërcënimi. Nëse subjektet financiare përdorin testues të brendshëm për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi, ata duhet të kontraktjnë testues të jashtëm për çdo tri teste të kryera.

11. Bankat me rëndësi sistemike, sipas përcaktimeve të Bankës së Shqipërisë, përdorin vetëm testues të jashtëm, në përputhje me nenin 44, pika 1, shkronjat “a” deri në “e” të kësaj rregulloreje.

12. Banka e Shqipërisë identifikon subjektet financiare që duhet të kryejnë testimin e depërtueshmërisë të udhëhequr nga kërcënimi, duke marrë parasysh kriteret e parashikuara në nenin 5, pika 2, të kësaj rregulloreje, bazuar në vlerësimin e elementeve të mëposhtme:

a) faktorët e lidhur me ndikimin, veçanërisht masën në të cilën shërbimet e ofruara dhe aktivitetet e ndërmarra nga subjekti financiar ndikojnë në sektorin financiar;

b) çështjet e mundshme të lidhura me stabilitetin financiar, duke përfshirë karakterin sistematik të subjektit financiar;

c) profilin specifik të rrezikut të TIK-ut, nivelin e pjekurisë së TIK-ut të subjektit financiar ose veçoritë teknologjike të tij.

Neni 44

Kërkesat për testuesit për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi

1. Subjektet financiare, për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi, do të përdorin vetëm testues që:

a) kanë përshtatshmëri dhe reputacion të lartë;

b) zotërojnë aftësi teknike dhe organizative dhe demonstrojnë ekspertizë specifike në inteligjencën e kërcënimit, testimin e depërtueshmërisë dhe testimin e ekipit të kuq (*red team testing*);

c) janë të certifikuar nga një organ akreditimi në një shtet anëtar të Bashkimit Evropian ose që respektojnë kodet formale të sjelljes ose etike;

d) ofrojnë një siguri të pavarur ose një raport auditimi, në lidhje me administrimin e shëndoshë të rreziqeve që lidhen me kryerjen e testimit të depërtueshmërisë të udhëhequr nga

kërcënimi, duke përfshirë mbrojtjen e duhur të informacionit konfidencial të subjektit financiar dhe korrigjimin për rreziqet e veprimtarisë të subjektit financiar;

e) mbulohen në mënyrën e duhur dhe plotësisht nga sigurimet përkatëse të dëmshpërblimit profesional, duke përfshirë rreziqet e sjelljes së keqe dhe neglizhencës.

2. Në rastet kur subjektet financiare përdorin testues të brendshëm, ata duhet të sigurohen që, përveç plotësimit të kërkesave në pikën 1 të këtij neni, plotësohen edhe kushtet e mëposhtme:

a) përdorimi i këtyre testuesve është miratuar nga Banka e Shqipërisë;

b) Banka e Shqipërisë ka verifikuar që subjekti financiar ka burime të mjaftueshme të dedikuara dhe ka siguruar që konfliktet e interesit janë shmangur gjatë gjithë fazave të projektimit dhe ekzekutimit të testit; dhe

c) ofruesi i kërcënimeve të inteligjencës është i jashtëm për subjektin financiar.

3. Subjektet financiare duhet të sigurojnë që marrëveshjet e lidhura me testues të jashtëm të kërkojnë një administrim të shëndoshë të rezultateve të testimit të depërtueshmërisë të udhëhequr nga kërcënimi dhe që çdo përpunim i të dhënave prej tyre, duke përfshirë çdo gjenerim, ruajtje, agregim, hartim, raportim, komunikim ose shkatërrim, të mos krijojë rreziqe për subjektet financiare.

KREU V

ADMINISTRIMI I RREZIKUT TË TIK-ut NGA PALËT E TRETA

NËNKREU I

PARIMET KRYESORE PËR NJË ADMINISTRIM TË SHËNDETSHËM TË RREZIKUT TË TIK-ut NGA PALËT E TRETA

Neni 45

Parimet e përgjithshme

1. Subjektet financiare administrojnë rrezikun e TIK-ut nga palët e treta, si një komponent integral të rrezikut të TIK-ut brenda sistemit të tyre të administrimit të rrezikut të TIK-ut, siç përcaktohet në nenin 7, pika 1, të kësaj rregulloreje dhe në përputhje me parimet e mëposhtme:

a) subjektet financiare që kanë marrëveshje kontraktuale për përdorimin e shërbimeve të TIK-ut, për të kryer operacionet e tyre të biznesit do të mbeten në çdo kohë plotësisht përgjegjës për respektimin dhe përmbushjen e të gjitha detyrimeve sipas legjislacionit në fuqi dhe kësaj rregulloreje;

b) administrimi i rrezikut të TIK-ut nga palët e treta nga ana e subjekteve financiare do të bazohet në parimin e proporcionalitetit, duke marrë parasysh:

i. natyrën, shkallën, kompleksitetin dhe rëndësinë e varësisë të lidhur me TIK-un,

ii. rreziqet që lindin nga marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut të lidhura me ofruesit e shërbimeve të palëve të treta të TIK-ut, duke marrë parasysh kritikalitetin ose rëndësinë e shërbimit, procesit ose funksionit përkatës dhe ndikimin e mundshëm në vazhdimësinë dhe disponueshmërinë e shërbimeve dhe veprimtarive financiare, në nivel individual dhe në nivel grupi.

2. Si pjesë të sistemit të tyre të administrimit të rrezikut të TIK-ut, subjektet financiare me përjashtim të mikrondërmarrjeve, si dhe subjektet e parashikuara në pikën 1 të nenit 17 të kësaj rregulloreje, miratojnë dhe rishikojnë rregullisht një strategji për rrezikun e TIK-ut nga palët e treta, duke marrë parasysh strategjinë me shumë shitës (*multivendor strategy*), të parashikuar

në pikën 10 të nenit 7 të kësaj rregulloreje. Kjo strategji do të përfshijë një politikë për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut dhe do të zbatohet individualisht dhe, sipas rastit, në baza të nënkonsoliduara dhe të konsoliduara. Organi drejtues i subjektit shqyrton rregullisht rreziqet e identifikuara në lidhje me marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, bazuar në shkallën dhe kompleksitetin e shërbimeve të subjektit.

3. Si pjesë të sistemit të tyre të administrimit të rrezikut të TIK-ut, subjektet financiare mbajnë dhe përditësojnë rregullisht, në nivel subjekti dhe në nivele të nënkonsoliduara dhe të konsoliduara, një regjistër që përmban informacion në lidhje me të gjitha marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut.

4. Marrëveshjet kontraktuale të përmendura në pikën 3 të këtij neni duhet të dokumentohen në mënyrën e duhur, duke bërë dallimin midis marrëveshjeve që mbulojnë shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme dhe atyre që nuk mbulojnë këto shërbime.

5. Subjektet financiare raportojnë të paktën çdo vit në Bankën e Shqipërisë, informacion mbi numrin e marrëveshjeve të reja për përdorimin e shërbimeve të TIK-ut, kategoritë e ofruesve të shërbimeve të palëve të treta të TIK-ut, llojet e marrëveshjeve kontraktuale, si dhe shërbimet dhe funksionet e TIK-ut që ofrohen.

6. Subjektet financiare vënë në dispozicion të Bankës së Shqipërisë, sipas kërkesës së saj, regjistrin e plotë të informacionit ose sipas kërkesës, seksione të specifikuara të tij, së bashku me çdo informacion që konsiderohet i nevojshëm për të mundësuar mbikëqyrjen efektive të subjektit financiar.

7. Subjektet financiare informojnë Bankën e Shqipërisë në kohën e duhur për çdo marrëveshje kontraktuale të planifikuar për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, si dhe në rastet kur një funksion është bërë kritik ose i rëndësishëm.

8. Para se të lidhin një marrëveshje kontraktuale për përdorimin e shërbimeve të TIK-ut, subjektet financiare duhet të:

a) vlerësojnë nëse marrëveshja kontraktuale mbulon përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme;

b) vlerësojnë nëse janë përmbushur kërkesat mbikëqyrëse për kontraktimin;

c) identifikojnë dhe vlerësojnë të gjitha rreziqet përkatëse në lidhje me marrëveshjen kontraktuale, duke përfshirë edhe mundësinë që marrëveshje të tilla kontraktuale mund të kontribuojnë në përforcimin e rrezikut të përqendrimit të TIK-ut, siç parashikohet në nenin 46 të kësaj rregulloreje;

d) kryejnë verifikimin e kujdesshëm (*due diligence*) për ofruesit e mundshëm të shërbimeve të palëve të treta të TIK-ut dhe të sigurojnë përgjatë procesit të përzgjedhjes dhe vlerësimit që ofruesi i shërbimit të palës së tretë të TIK-ut është i përshtatshëm;

e) identifikojnë dhe vlerësojnë konfliktet e interesit që mund të shkaktojnë marrëveshja kontraktuale.

9. Subjektet financiare mund të hyjnë në marrëveshje kontraktuale vetëm me ofrues të shërbimeve të palëve të treta të TIK-ut që janë në përputhje me standardet e duhura të sigurisë së informacionit. Kur këto marrëveshje kontraktuale janë të lidhura me funksione kritike ose të rëndësishme, subjektet financiare, përpara se të lidhin marrëveshjet, duhet të marrin në konsideratë përdorimin nga ofruesit e shërbimeve të palëve të treta të TIK-ut, të standardeve më të përditësuara dhe me cilësinë më të lartë të sigurisë së informacionit.

10. Në ushtrimin e të drejtave të aksesit, inspektimit dhe auditimit mbi ofruesin e shërbimeve të palëve të treta të TIK-ut, subjektet financiare, duke ndjekur një qasje të bazuar në rrezik, përcaktojnë frekuencën e auditimeve dhe inspektimeve dhe fushat që do të auditohen nëpërmjet

respektimit të standardeve të auditimit përgjithësisht të pranuar, në përputhje edhe me çdo udhëzim mbikëqyrës për përdorimin dhe përfshirjen e këtyre standardeve të auditimit.

11. Në rastet kur marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut sjellin një nivel të lartë kompleksiteti teknologjik, subjekti financiar duhet të verifikojë që auditorët e brendshëm apo të jashtëm, ose një grup auditorësh, zotërojnë aftësitë dhe njohuritë e duhura për të kryer në mënyrë efektive auditimet dhe vlerësimet përkatëse.

12. Subjektet financiare duhet të sigurojnë që marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut të ndërpriten, nëse vërehen/ndodhin situatat e mëposhtme:

a) shkelje të rënda nga ofruesi i shërbimeve të palëve të treta të TIK-ut, të ligjeve, rregulloreve ose kushteve kontraktuale;

b) situatat e identifikuara gjatë monitorimit të rrezikut të TIK-ut nga palët e treta, që konsiderohen të afta të ndryshojnë performancën e funksioneve të ofruara nëpërmjet marrëveshjes kontraktuale, duke përfshirë ndryshimet materiale që ndikojnë në marrëveshjen ose situatën e ofruesit të shërbimeve të palëve të treta të TIK-ut;

c) dobësi të evidentuara të ofruesit të shërbimeve të palëve të treta të TIK-ut që lidhen me administrimin e tij të përgjithshëm të rrezikut të TIK-ut dhe veçanërisht me mënyrën se si ai siguron disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave, qofshin këto të dhëna personale ose të dhëna të tjera të ndjeshme ose të dhëna jopersonale;

d) situata kur Banka e Shqipërisë nuk mund të mbikëqyrë më efektivisht subjektin financiar si rezultat i marrëveshjes kontraktuale përkatëse.

13. Subjektet financiare duhet të hartojnë strategji daljeje (*exit strategies*) për shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme. Këto strategji duhet të marrin parasysh rreziqet që mund të shfaqen në nivel të ofruesit të shërbimeve të palëve të treta të TIK-ut, veçanërisht një dështim i mundshëm i këtij të fundit, një përkeqësim i cilësisë së shërbimeve të TIK-ut të ofruara, çdo ndërprerje e veprimtarisë për shkak të ofrimit të papërshtatshëm ose të dështuar të shërbimeve të TIK-ut, ose çdo rrezik material që lind në lidhje me vendosjen e duhur dhe të vazhdueshme të shërbimit përkatës të TIK-ut, ose ndërprerjen e marrëveshjeve kontraktuale me ofruesit e shërbimeve të palëve të treta të TIK-ut në ndonjë nga situatat e parashikuara në pikën 12 të këtij neni.

14. Subjektet financiare duhet të sigurojnë që janë në gjendje të ndërpresin marrëveshjet kontraktuale pa:

a) ndërprerje të veprimtarisë së tyre;

b) kufizuar/ndikuar përputhshmërinë me kërkesat rregullative;

c) dëmtuar vazhdimësinë dhe cilësinë e ofrimit të shërbimeve për klientët.

15. Planet e daljes (*exit plans*) duhet të jenë gjithëpërfshirëse, të dokumentuara dhe, në përputhje me kriteret e parashikuara në nenin 5, pika 2, të kësaj rregulloreje, duhet të testohen mjaftueshëm dhe të rishikohen në mënyrë periodike.

16. Subjektet financiare duhet të identifikojnë zgjidhje alternative dhe të zhvillojnë plane tranzicioni që u mundësojnë atyre zhvendosjen e funksioneve të kontraktuara dhe të dhënave përkatëse nga ofruesi i shërbimeve të palëve të treta të TIK-ut dhe transferimin e tyre në mënyrë të sigurt dhe integrale tek ofruesit alternativë ose riinkorporimin e tyre brenda vetë subjektit.

17. Subjektet financiare marrin masat e duhura të emergjencës për të ruajtur vazhdimësinë e biznesit në të gjitha situatat e parashikuara në pikën 13 të këtij neni.

Neni 46

Vlerësimi paraprak i rrezikut të përqendrimit të TIK-ut në nivel subjekti

1. Subjektet financiare, kur kryejnë identifikimin dhe vlerësimin e rrezikut të përqendrimit të TIK-ut të përmendur në shkronjën “c” të pikës 8 të nenit 45 të kësaj rregulloreje, duhet të marrin parasysh edhe nëse lidhja e një marrëveshjeje kontraktuale për shërbimet e TIK-ut që

mbështesin funksionet kritike ose të rëndësishme, do të çonte në ndonjë nga situatat e mëposhtme:

a) kontraktimin me një ofrues shërbimi të palëve të treta të TIK-ut, i cili nuk është lehtësisht i zëvendësueshëm; ose

b) krijimin e marrëveshjeve të shumta kontraktuale për ofrimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, me të njëjtin ofrues shërbimi të palëve të treta të TIK-ut ose me ofrues të shërbimeve të palëve të treta të TIK-ut të lidhur ngushtë me njëri-tjetrin.

2. Subjektet financiare vlerësojnë përfitimet dhe kostot e zgjidhjeve alternative, të tilla si përdorimi i ofruesve të ndryshëm të shërbimeve të palëve të treta të TIK-ut, duke marrë parasysh nëse dhe si zgjidhjet e parashikuara përputhen me nevojat dhe objektivat e biznesit të përcaktuar në strategjinë e tyre të qëndrueshmërisë digjitale.

3. Në rastet kur marrëveshja kontraktuale për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, përfshin mundësinë që një ofrues i shërbimeve të palëve të treta të TIK-ut të nënkontraktojë më tej shërbime të TIK-ut që mbështesin funksionet kritike ose të rëndësishme me ofrues të tjerë të shërbimeve të palëve të treta të TIK-ut, subjektet financiare do të vlerësojnë përfitimet dhe rreziqet që mund të lindin nga ky nënkontraktim, veçanërisht në rastin kur nënkontraktori i TIK është i themeluar në një shtet tjetër.

4. Në rastet kur marrëveshjet kontraktuale lidhen me shërbimet e TIK-ut që mbështesin funksione kritike ose të rëndësishme, subjektet financiare duhet të marrin në konsideratë edhe parashikimet ligjore mbi falimentimin, që do të zbatoheshin në rast të falimentimit të ofruesit të shërbimeve të palëve të treta të TIK-ut, si dhe çdo kufizim që mund të lindë në lidhje me rikuperimin urgjent të të dhënave të subjektit financiar.

5. Në rastet kur marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK-ut që mbështesin funksione kritike ose të rëndësishme, lidhen me një ofrues të shërbimeve të palëve të treta të TIK-ut të themeluar në një shtet tjetër, subjektet financiare, përveç kërkesave të parashikuara në pikën 4 të këtij neni, duhet të marrin në konsideratë edhe përputhshmërinë me kërkesat për mbrojtjen e të dhënave të parashikuara në legjislacionin shqiptar dhe zbatimin efektiv të ligjit në atë shtet.

6. Në rastet kur marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK-ut që mbështesin funksione kritike ose të rëndësishme parashikojnë nënkontraktimin, subjektet financiare duhet të vlerësojnë nëse dhe si zinxhirët potencialisht të gjatë ose kompleksë të nënkontraktimit mund të ndikojnë në aftësinë e tyre për të monitoruar plotësisht funksionet e kontraktuara dhe në aftësinë e Bankës së Shqipërisë për të mbikëqyrur në mënyrë efektive subjektin financiar në këtë drejtim.

Neni 47

Kërkesat kryesore për marrëveshjet kontraktuale

1. Marrëveshja kontraktuale përcakton në mënyrë të qartë dhe me shkrim, të drejtat dhe detyrimet e subjektit financiar dhe të ofruesit të shërbimeve të palëve të treta të TIK-ut. Kontrata e plotë duhet të përfshijë edhe marrëveshjet mbi nivelin e shërbimeve dhe duhet të dokumentohet në një dokument të shkruar, i cili i vihet në dispozicion palëve në letër ose në një format tjetër i cili është i shkarkueshëm, i qëndrueshëm dhe i aksesueshëm.

2. Marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut përfshijnë të paktën elementet e mëposhtme:

a) një përshkrim të qartë dhe të plotë të të gjitha funksioneve dhe shërbimeve të TIK-ut që do të ofrohen nga ofruesi i shërbimeve të palëve të treta të TIK-ut, duke përcaktuar nëse lejohet nënkontraktimi i një shërbimi të TIK-ut që mbështet një funksion kritik ose të rëndësishëm, ose

pjesë të rëndësishme të këtij shërbimi dhe, nëse lejohet, kushtet që do të zbatohen për një nënkontraktim të tillë;

b) vendndodhjet (rajonet apo shtetet) ku do të ofrohen funksionet dhe shërbimet e TIK-ut të kontraktuara ose të nënkontraktuara dhe ku do të përpunohen të dhënat, duke përfshirë vendndodhjen e ruajtjes së tyre dhe kërkesën që ofruesi i shërbimeve të palëve të treta të TIK-ut të njoftojë subjektin financiar, nëse parashikon ndryshimin e këtyre vendndodhjeve;

c) parashikimet për aksesin, disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin në lidhje me mbrojtjen e të dhënave, përfshirë edhe të dhënat personale;

d) parashikimet për sigurimin e aksesit, rikuperimit dhe kthimit, në një format lehtësisht të aksesueshëm të të dhënave personale dhe jopersonale të përpunuara nga subjekti financiar, në rast falimentimi, ndërhyrjeje të jashtëzakonshme ose ndërprerjeje të operacioneve të biznesit të ofruesit të shërbimeve të palëve të treta të TIK-ut, ose në rast të përfundimit të marrëveshjes kontraktuale;

e) përshkrime të plota të nivelit të shërbimit, duke përfshirë përditësimet dhe rishikimet e tyre;

f) detyrimin e ofruesit të shërbimeve të palëve të treta të TIK-ut, për t'i ofruar ndihmë subjektit financiar, pa kosto shtesë ose me një kosto që është e përcaktuar paraprakisht, në rast se ndodh një incident TIK i lidhur me shërbimin e TIK-ut që i ofrohet subjektit financiar;

g) detyrimin e ofruesit të shërbimeve të palëve të treta të TIK-ut, për të bashkëpunuar plotësisht me Bankën e Shqipërisë në rolin e autoritetit mbikëqyrës dhe të autoritetit të ndërhyrjes së jashtëzakonshme të subjektit financiar, duke përfshirë edhe me personat e caktuar prej saj;

h) të drejtën e përfundimit të marrëveshjes kontraktuale dhe periudhën minimale të njoftimit për përfundimin e kësaj marrëveshje, në përputhje me pritshmëritë e Bankës së Shqipërisë në rolin e autoritetit mbikëqyrës dhe të autoritetit të ndërhyrjes së jashtëzakonshme;

i) kushtet për pjesëmarrjen e ofruesve të shërbimeve të palëve të treta të TIK-ut në programet e ndërgjegjësimi për sigurinë e TIK-ut dhe trajnimet për qëndrueshmërinë operacionale digjitale të subjekteve financiare, në përputhje me nenin 15, pika 7, të kësaj rregulloreje.

3. Marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut që mbështesin funksione kritike ose të rëndësishme, përveç sa parashikohet në pikën 2 të këtij neni, përfshijnë të paktën edhe elementet e mëposhtme:

a) përshkrime të plota të nivelit të shërbimit, duke përfshirë përditësimet dhe rishikimet e tyre me objektiva të saktë sasiore dhe cilësore të performancës brenda niveleve të dakorduara të shërbimit, për të lejuar monitorimin efektiv të shërbimeve të TIK-ut nga subjekti financiar, si dhe për të mundësuar ndërmarrjen e masave të duhura korrigjuese, pa vonesa të panevojshme, kur nivelet e shërbimit të rëna dakord nuk përmbushen;

b) periudhat e njoftimit dhe detyrimet e raportimit të ofruesit të shërbimeve të palëve të treta të TIK-ut ndaj subjektit financiar, duke përfshirë njoftimin për çdo zhvillim që mund të ketë një ndikim material në aftësinë e ofruesit të shërbimeve të palëve të treta të TIK-ut, për të ofruar në mënyrë efektive shërbimet e TIK-ut që mbështesin funksione kritike ose të rëndësishme, në përputhje me nivelet e dakorduara të shërbimit;

c) kërkesat për ofruesin e shërbimeve të palëve të treta të TIK-ut, për të zbatuar dhe testuar planet e emergjencës së biznesit dhe për të disponuar masa, mekanizma dhe politika të sigurisë të TIK-ut, që garantojnë një nivel të mjaftueshëm sigurie për ofrimin e shërbimeve nga subjekti financiar, në përputhje me kuadrin e tij rregullator;

d) detyrimin e ofruesit të shërbimeve të palëve të treta të TIK-ut, për të marrë pjesë dhe për të bashkëpunuar plotësisht në testimin e depërtueshmërisë të udhëhequr nga kërcënimi të subjektit financiar, siç parashikohet në nenet 43 dhe 44 të kësaj rregulloreje;

e) të drejtën për të monitoruar në mënyrë të vazhdueshme performancën e ofruesit të shërbimeve të palëve të treta të TIK-ut, që përfshin:

i. të drejtat e pakufizuara të aksesit, inspektimin dhe auditimin nga subjekti financiar ose nga një palë e tretë e caktuar, si dhe nga Banka e Shqipërisë, si dhe të drejtën për të marrë në vend (*on-site*) kopje të dokumentacionit përkatës, nëse janë kritike për veprimtarinë e ofruesit të shërbimeve të palëve të treta të TIK-ut, ushtrimi efektiv i së cilës nuk pengohet ose kufizohet nga marrëveshje të tjera kontraktuale ose politika të zbatimit;

ii. të drejtën për të rënë dakord për nivelet alternative të sigurimit nëse preken të drejtat e klientëve të tjerë;

iii. detyrimin e ofruesit të shërbimeve të palëve të treta të TIK-ut, për të bashkëpunuar plotësisht gjatë inspektimeve në vend dhe auditimeve të kryera nga Banka e Shqipërisë, Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*), subjekti financiar ose një palë e tretë e përcaktuar, dhe

iv. detyrimin për të paraqitur detaje mbi qëllimin, procedurat që do të ndiqen dhe shpeshtësinë e këtyre inspektimeve dhe auditimeve;

f) strategjitë e daljes (*exit strategies*), në veçanti përcaktimin e një periudhe tranzicioni të përshtatshme të detyrueshme:

i. gjatë së cilës ofruesi i shërbimeve të palëve të treta të TIK-ut do të vazhdojë të ofrojë funksionet ose shërbimet përkatëse të TIK-ut, me synimin për të zvogëluar rrezikun e ndërprerjes së veprimtarisë (*risk of disruption*) të subjektit financiar, ose për të siguruar ndërhyrjen e jashtëzakonshme dhe ristrukturimin e saj efektiv;

ii. që i lejon subjektit të zhvendoset në një ofrues tjetër të shërbimeve të palëve të treta të TIK-ut, ose në zgjidhje të brendshme, në përputhje me kompleksitetin e shërbimit të ofruar.

4. Pa rënë ndesh me parashikimet e shkronjës “e” të pikës 3 të këtij neni, ofruesi i shërbimeve të palëve të treta të TIK-ut dhe subjekti financiar që është një mikrondërmarrje, mund të bien dakord që të drejtat e aksesit, inspektimit dhe auditimit nga subjekti financiar të mund të delegohen te një palë e tretë e pavarur, e caktuar nga ofruesi i shërbimeve të palëve të treta të TIK-ut, dhe që subjekti financiar është në gjendje të kërkojë informacion dhe garantimin e performancës së ofruesit të shërbimeve të palëve të treta të TIK-ut, në çdo kohë nga pala e tretë.

5. Subjektet financiare dhe ofruesit e shërbimeve të palëve të treta të TIK-ut, kur negociojnë marrëveshjet kontraktuale, marrin në konsideratë përdorimin e klauzolave standarde kontraktuale të zhvilluara nga autoritetet publike për shërbime specifike.

NËNKREU II

POLITIKA PËR PËRDORIMIN E SHËRBIMEVE TË TIK-ut QË MBËSHTESIN FUNKSIONET KRITIKE OSE TË RËNDËSISHME, TË OFRUARA NGA OFRUESIT E SHËRBIMEVE TË PALËVE TË TRETA TË TIK-ut

Neni 48

Profili i përgjithshëm i rrezikut dhe kompleksiteti

1. Si pjesë të sistemit të tyre të administrimit të rrezikut të TIK-ut, subjektet financiare miratojnë dhe rishikojnë rregullisht një politikë për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut, siç parashikohet në nenin 45, pika 2, të kësaj rregulloreje.

2. Politika për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut (e cila për thjeshtësi në këtë nënkre do të quhet “politika”), duhet të marrë në konsideratë madhësinë dhe profilin e përgjithshëm të rrezikut të subjektit financiar, si dhe natyrën, shkallën dhe elementet e kompleksitetit të shtuar ose të reduktuar të shërbimeve, aktiviteteve dhe operacioneve të tij, përfshirë elementet që lidhen me:

a) llojin e shërbimeve të TIK-ut të përfshira në marrëveshjen kontraktuale për përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut (e cila për thjeshtësi në këtë nënkre do të quhet “marrëveshja kontraktuale”), ndërmjet subjektit financiar dhe ofruesit të shërbimeve të palëve të treta të TIK-ut;

b) vendndodhjen e ofruesit të shërbimeve të palëve të treta të TIK-ut ose të shoqërisë mëmë të tij;

c) nëse shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme ofrohen nga një ofrues i shërbimeve të palëve të treta të TIK-ut i vendosur brenda Shqipërisë ose në një vend tjetër, duke marrë, gjithashtu, në konsideratë edhe vendin nga ku ofrohen shërbimet e TIK-ut, si dhe vendin ku përpunohen dhe ruhen të dhënat;

d) natyrën e të dhënave që shkëmbehen me ofruesin e shërbimeve të palëve të treta të TIK-ut;

e) nëse ofruesi i shërbimeve të palëve të treta të TIK-ut është pjesë e të njëjtit grup me subjektin financiar të cilit i ofrohen shërbimet;

f) përdorimin e ofruesve të shërbimeve të palëve të treta të TIK-ut që janë të licencuar, të regjistruar ose subjekt i mbikëqyrjes së Bankës së Shqipërisë ose një autoriteti tjetër mbikëqyrës brenda Shqipërisë, si dhe përdorimin e ofruesve të shërbimeve të palëve të treta të TIK-ut që nuk janë të tillë;

g) përdorimin e ofruesve të shërbimeve të palëve të treta të TIK-ut që janë të licencuar, të regjistruar ose subjekt i mbikëqyrjes së një autoriteti mbikëqyrës në një vend të tjetër, si dhe përdorimin e ofruesve të shërbimeve të palëve të treta të TIK-ut që nuk janë të tillë;

h) nëse ofrimi i shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme është përqendruar te një ofrues i vetëm i shërbimeve të palëve të treta të TIK-ut ose te një numër i vogël ofruesish të shërbimeve të palëve të treta të TIK-ut;

i) transferueshmërinë e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme te një ofrues tjetër shërbimesh i palëve të treta të TIK-ut, përfshirë edhe si pasojë e veçorive teknologjike;

j) ndikimin e mundshëm të ndërprerjeve në ofrimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, mbi vazhdimësinë e aktiviteteve të subjektit financiar dhe mbi disponueshmërinë e shërbimeve të tij.

Neni 49

Zbatimi në nivel grupi

Në rastet kur kjo rregullore zbatohet në baza të konsoliduara ose nënkonsoliduara, shoqëria mëmë që është përgjegjëse për përgatitjen e pasqyrave financiare të konsoliduara ose nënkonsoliduara të grupit, duhet të sigurojë që politika të zbatohet në mënyrë të njëtrajtshme në të gjitha subjektet financiare që janë pjesë e grupit dhe të jetë e përshtatshme për zbatimin efektiv të kësaj rregulloreje në të gjitha nivelet përkatëse të grupit.

Neni 50

Mekanizmat e qeverisjes

1. Organet drejtuese rishikojnë politikën të paktën një herë në vit dhe e përditësojnë atë, kur është e nevojshme. Ndryshimet e bëra në politikë zbatohen në kohën e duhur dhe sa më shpejt të jetë e mundur brenda kuadrit të marrëveshjeve kontraktuale përkatëse. Subjekti financiar dokumenton afatin kohor të planifikuar për zbatimin e këtyre ndryshimeve.

2. Politika përcakton ose i referohet një metodologjie për përcaktimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme. Politika duhet, gjithashtu, të përcaktojë kohën kur ky vlerësim duhet të kryhet dhe të rishikohet.

3. Politika përcakton qartë përgjegjësitë e brendshme për miratimin, administrimin, kontrollin dhe dokumentimin e marrëveshjeve përkatëse kontraktuale dhe siguron që brenda subjektit financiar të disponohen aftësitë, përvoja dhe njohuritë e duhura për të mbikëqyrur (*oversee*) në mënyrë efektive këto marrëveshje kontraktuale, përfshirë shërbimet e TIK-ut që ofrohen në bazë të tyre.

4. Pa cenuar përgjegjësinë përfundimtare të subjektit financiar për mbikëqyrjen efektive të marrëveshjeve kontraktuale përkatëse, politika duhet të përmbajë kërkesa për vlerësimin nëse ofruesi i shërbimeve të palëve të treta të TIK-ut disponon burime të mjaftueshme për të garantuar që subjekti financiar i përmbush të gjitha kërkesat ligjore dhe rregullative që lidhen me shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme të ofruara.

5. Politika identifikon qartë rolin/funksionin ose personin nga drejtimi i lartë i subjektit financiar, që është përgjegjës për monitorimin e marrëveshjeve kontraktuale përkatëse. Politika përcakton mënyrën se si ky rol/funksion ose person nga drejtimi i lartë, bashkëpunon me funksionet e kontrollit, përveç rasteve kur është pjesë e tyre, dhe përcakton linjat e raportimit ndaj organit drejtues, përfshirë natyrën e informacionit që do të raportohet dhe dokumentet që do të paraqiten, si dhe shpeshësinë e raportimeve të tilla.

6. Politika duhet të sigurojë që marrëveshjet kontraktuale të jenë në përputhje me:

a) sistemin e administrimit të rrezikut të TIK-ut, të parashikuar në nenin 7 të kësaj rregulloreje;

b) politikën e sigurisë së informacionit, të parashikuar në nenin 10, pika 4, të kësaj rregulloreje;

c) politikën e vazhdimësisë së biznesit të TIK-ut, të parashikuar në nenin 12 të kësaj rregulloreje;

d) kërkesat për raportimin e incidenteve, të përcaktuara në nenin 30 të kësaj rregulloreje.

7. Politika përmban kërkesa që shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofrues të shërbimeve të palëve të treta të TIK-ut, t'i nënshtrohen rishikimit të pavarur dhe të përfshihen në planin e auditit.

8. Politika duhet të përcaktojë në mënyrë të qartë që marrëveshjet kontraktuale:

a) nuk e përjashtojnë subjektin financiar dhe organet e tij drejtuese, nga detyrimet rregullatore dhe përgjegjësitë ndaj klientëve të tij;

b) nuk duhet të pengojnë mbikëqyrjen efektive të subjektit financiar dhe nuk duhet të bien ndesh me kufizimet mbikëqyrëse mbi shërbimet dhe veprimtaritë e subjektit;

c) duhet të parashikojnë kërkesa që ofruesit e shërbimeve të palëve të treta të TIK-ut të bashkëpunojnë me Bankën e Shqipërisë;

d) duhet të parashikojnë kërkesa që subjekti financiar, audituesit e jashtëm të tij dhe Banka e Shqipërisë të kenë akses efektiv në të dhënat dhe ambientet që lidhen me përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme.

Neni 51

Fazat kryesore të ciklit jetësor për hartimin dhe zbatimin e marrëveshjeve kontraktuale

Politika përcakton kërkesat, përfshirë rregullat, përgjegjësitë dhe proceset, për secilën fazë kryesore të ciklit jetësor të marrëveshjeve kontraktuale, duke përfshirë të paktën sa vijon:

a) përgjegjësitë e organit drejtues, përfshirë pjesëmarrjen e tij, sipas rastit, në procesin e vendimmarrjes mbi përdorimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të palëve të treta të TIK-ut;

b) planifikimin e marrëveshjeve kontraktuale, duke përfshirë vlerësimin e rrezikut, verifikimin e kujdesshëm (*due diligence*), sipas përcaktimeve në nenet 52 dhe 53 të kësaj rregulloreje, si dhe procesin e miratimit të marrëveshjeve të reja ose të ndryshimeve të rëndësishme në marrëveshjet ekzistuese, sipas përcaktimeve të nenit 55, pika 4, të kësaj rregulloreje;

c) përfshirjen e njësive të biznesit, funksioneve të kontrollit të brendshëm dhe njësive të tjera përkatëse në lidhje me marrëveshjet kontraktuale;

d) zbatimin, monitorimin dhe administrimin e marrëveshjeve kontraktuale, sipas përcaktimeve në nenet 54, 55 dhe 56 të kësaj rregulloreje, duke përfshirë edhe në nivel të konsoliduar dhe nënkonsoliduar, kur është e zbatueshme;

e) dokumentimin dhe ruajtjen e të dhënave, duke marrë parasysh kërkesat që lidhen me regjistrin e informacionit, të përcaktuara në nenin 45 të kësaj rregulloreje;

f) strategjitë e daljes (*exit strategies*) dhe proceset e ndërprerjes së marrëveshjeve kontraktuale, sipas përcaktimeve në nenin 57 të kësaj rregulloreje.

Neni 52

Vlerësimi paraprak i rrezikut

1. Politika parashikon kërkesa që subjekti financiar të përcaktojë nevojat e biznesit, përpara se të lidhet një marrëveshje kontraktuale.

2. Politika parashikon kërkesa që vlerësimi i rrezikut të kryhet në baza individuale të subjektit financiar dhe, kur është e zbatueshme, në nivel të konsoliduar dhe nënkonsoliduar, përpara se të lidhet një marrëveshje kontraktuale.

3. Vlerësimi i rrezikut duhet të marrë në konsideratë të gjitha kërkesat përkatëse të përcaktuara në këtë rregullore dhe në legjislacionin përkatës të fushës për subjektin financiar. Ky vlerësim duhet të marrë në konsideratë, në mënyrë të veçantë, ndikimin e ofrimit të shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme nga ofruesit e shërbimeve të palëve të treta të TIK-ut, mbi subjektin financiar, si dhe të gjitha rreziqet që burojnë nga këto shërbime, duke përfshirë:

- a) rrezikun operacional;
- b) rrezikun ligjor;
- c) rrezikun e TIK-ut;
- d) rrezikun reputacional;
- e) rrezikun e lidhur me mbrojtjen e të dhënave konfidenciale ose personale;
- f) rrezikun e lidhur me disponueshmërinë e të dhënave;
- g) rrezikun e lidhur me vendndodhjen ku përpunohen dhe ruhen të dhënat;
- h) rrezikun e lidhur me vendndodhjen e ofruesit të shërbimeve të palëve të treta të TIK-ut;
- i) rrezikun e përqendrimit të shërbimeve të TIK-ut në nivel subjekti.

Neni 53

Verifikimi i kujdesshëm (*due diligence*)

1. Politika parashikon një proces të përshtatshëm dhe proporcional për përzgjedhjen dhe vlerësimin e ofruesve potencialë të shërbimeve të palëve të treta të TIK-ut, duke marrë parasysh nëse ofruesi i shërbimit të TIK-ut është ose jo një ofrues brenda grupit. Politika duhet të parashikojë kërkesa që subjekti financiar, përpara lidhjes së marrëveshjes kontraktuale, të vlerësojë nëse ofruesi i shërbimit të palëve të treta të TIK-ut:

a) ka reputacion të mirë, aftësi, ekspertizë dhe burime të mjaftueshme financiare, njerëzore dhe teknike, standarde të sigurisë së informacionit, strukturë organizative të përshtatshme,

sistem të administrimit të rrezikut dhe kontrole të brendshme, si dhe, kur është e zbatueshme, autorizimet ose regjistrimet përkatëse për ofrimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme në mënyrë të besueshme dhe profesionale;

b) ka aftësinë për të monitoruar zhvillimet përkatëse teknologjike, për të identifikuar praktikat kryesore të sigurisë së TIK-ut dhe për t'i zbatuar ato, kur është e përshtatshme, për të siguruar një sistem efektiv dhe të shëndetshëm të qëndrueshmërisë operationale digjitale;

c) përdor ose synon të përdorë nënkontraktorë të TIK-ut, për të kryer shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme, ose pjesë të rëndësishme të tyre;

d) është i vendosur ose përpunon apo ruan të dhënat në një shtet tjetër dhe, nëse po, nëse kjo praktikë ndikon në nivelin e rrezikut operacional ose reputacional, apo rrezikun e ndikimit nga masa kufizuese, përfshirë embargot dhe sanksionet, që mund të ndikojnë në aftësinë e ofruesit të shërbimeve të palëve të treta të TIK-ut, për të ofruar shërbimet ose në aftësinë e subjektit financiar për të marrë këto shërbime të TIK-ut;

e) pranon marrëveshjet kontraktuale që sigurojnë mundësinë efektive për kryerjen e auditimeve tek ofruesi i shërbimeve të palëve të treta të TIK-ut, përfshirë auditimet në vend, nga vetë subjekti financiar, palë të treta të caktuara prej tij, ose Banka e Shqipërisë;

f) vepron në mënyrë etike dhe me përgjegjësi sociale, respekton të drejtat e njeriut dhe të fëmijëve, përfshirë ndalimin e punës së fëmijëve, respekton parimet e zbatueshme për mbrojtjen e mjedisit dhe garanton kushte të përshtatshme pune.

2. Politika përcakton nivelin e kërkuar të garancisë lidhur me efektivitetin e sistemit të administrimit të rrezikut të ofruesve të shërbimeve të palëve të treta të TIK-ut, për shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme. Politika duhet të përmbajë kërkesa që procesi i verifikimit të kujdesshëm (*due diligence*) të përfshijë një vlerësim të ekzistencës së masave për zbutjen e rrezikut dhe të masave për vazhdimësinë e biznesit, si dhe të mënyrës se si sigurohet funksionimi i tyre brenda ofruesit të shërbimeve të palëve të treta të TIK-ut.

3. Politika duhet të përcaktojë procesin e verifikimit të kujdesshëm (*due diligence*) për përzgjedhjen dhe vlerësimin e ofruesve potencialë të shërbimeve të palëve të treta të TIK-ut dhe të tregojë se cilat nga elementet e mëposhtme do të përdoren për nivelin e nevojshëm të sigurisë mbi performancën e ofruesit të shërbimeve të palëve të treta të TIK-ut:

a) auditime ose vlerësime të pavarura të kryera nga vetë subjekti financiar ose në emër të tij;

b) përdorimi i raporteve të pavarura të auditimit të përgatitura me kërkesë të ofruesit të shërbimeve të palëve të treta të TIK-ut;

c) përdorimi i raporteve të auditimit të kryera nga funksioni i auditit të brendshëm të ofruesit të shërbimeve të palëve të treta të TIK-ut;

d) përdorimi i certifikimeve të përshtatshme nga palë të treta;

e) përdorimi i çdo informacioni tjetër përkatës, të disponueshëm nga subjekti financiar, ose i çdo informacioni tjetër të ofruar nga ofruesi i shërbimeve të palëve të treta të TIK-ut.

4. Subjektet financiare duhet të sigurojnë një nivel të përshtatshëm garancie mbi performancën e ofruesit të shërbimeve të palëve të treta të TIK-ut, duke marrë parasysh elementet e përcaktuara në shkronjat nga “a” deri në “e” të pikës 3 të këtij neni. Kur është e përshtatshme, mund të përdoret më shumë se një nga elementet e parashikuara në këto shkronja.

Neni 54

Konflikti i interesit

1. Politika duhet të specifikojë masat e përshtatshme për identifikimin, parandalimin dhe administrimin e konflikteve aktuale ose të mundshme të interesit, që mund të lindin nga përdorimi i ofruesve të shërbimeve të palëve të treta të TIK-ut. Këto masa duhet të ndërmerren përpara lidhjes së marrëveshjeve kontraktuale përkatëse dhe të sigurojnë një monitorim të vazhdueshëm të këtyre konflikteve të interesit.

2. Kur shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme, ofrohen nga ofrues shërbimesh të TIK-ut brenda grupit, politika duhet të specifikojë që vendimmarrja mbi kushtet përkatëse të shërbimeve të TIK-ut, përfshirë kushtet financiare, të bëhet në mënyrë objektive.

Neni 55

Klauzolat kontraktuale

1. Politika duhet të specifikojë që çdo marrëveshje kontraktuale përkatëse të jetë në formë të shkruar dhe të përfshijë të gjitha elementet e parashikuara në nenin 47, pikat 2 dhe 3 të kësaj rregulloreje. Politika duhet, gjithashtu, të përfshijë elemente që lidhen me kërkesat e përcaktuara në nenin 1, pika 1, shkronja “a”, të kësaj rregulloreje, si dhe me çdo dispozitë tjetër përkatëse ligjore, sipas rastit.

2. Politika duhet të specifikojë që marrëveshjet kontraktuale përkatëse të përfshijnë të drejtën e subjektit financiar për të pasur akses në informacion, për të kryer inspektime dhe auditime, si dhe për të zhvilluar testime për TIK-un. Për këtë qëllim, politika duhet të parashikojë kërkesa që subjekti financiar të përdorë metodat e mëposhtme, pa cenuar përgjegjësinë përfundimtare të tij:

a) auditin e brendshëm të vetë subjektit financiar ose auditimin nga një palë e tretë e caktuar prej tij;

b) kur është e përshtatshme, auditime të përbashkëta dhe testime të përbashkëta të TIK-ut, përfshirë testimin e depërtueshmërisë të udhëhequr nga kërcënimi (*TLPT*), të organizuara në mënyrë të përbashkët me subjekte të tjera financiare ose me shoqëri të kontraktuara që përdorin shërbimet e TIK-ut të të njëjtit ofrues shërbimesh të palëve të treta të TIK-ut, dhe që kryhen nga ato subjekte financiare ose shoqëri të kontraktuara ose nga një palë e tretë e caktuar prej tyre;

c) kur është e përshtatshme, certifikime nga palë të treta;

d) kur është e përshtatshme, raporte auditimi të brendshme ose të palëve të treta, të vëna në dispozicion nga ofruesi i shërbimeve të palëve të treta të TIK-ut.

3. Subjekti financiar nuk duhet të mbështetet gjatë gjithë kohës vetëm mbi certifikimet e parashikuara në pikën 2, shkronja “c”, të këtij neni, apo mbi raportet e auditimit të parashikuara në shkronjën “d” të pikës 2 të këtij neni. Politika duhet të lejojë përdorimin e metodave të parashikuara në pikën 2, shkronjat “c” dhe “d” të këtij neni, vetëm nëse subjekti financiar:

a) është i kënaqur me planin e auditimit të ofruesit të shërbimeve të palëve të treta të TIK-ut, për marrëveshjet kontraktuale përkatëse;

b) siguron që shtrirja e certifikimeve ose raporteve të auditimit mbulon sistemet dhe kontrollet kryesore të identifikuar prej tij dhe siguron përputhshmërinë me kërkesat rregullatore përkatëse;

c) vlerëson në mënyrë tërësore përmbajtjen e certifikimeve ose raporteve të auditimit dhe verifikon që ato të mos jenë të vjetruara;

d) siguron që sistemet dhe kontrollet kryesore të jenë të përfshira në versionet e ardhshme të certifikimit ose të raportit të auditimit;

e) është i kënaqur me kompetencën profesionale të palës certifikuese ose audituesit;

f) është i kënaqur që certifikimet janë lëshuar dhe auditimet janë kryer në përputhje me standarde profesionale të pranuar gjerësisht dhe që përfshijnë testimin e efektivitetit operacional të kontroleve kryesore në fuqi;

g) ka të drejtën kontraktuale për të kërkuar, me një frekuencë të arsyeshme dhe të justifikuar nga pikëpamja e administrimit të rrezikut, ndryshime në shtrirjen e certifikimeve ose të raporteve të auditimit, edhe në sisteme dhe kontrole të tjera përkatëse;

h) ka të drejtën kontraktuale për të kryer auditime individuale dhe të përbashkëta sipas diskrecionit të tij, në lidhje me marrëveshjet kontraktuale dhe për ta ushtruar këtë të drejtë në përputhje me frekuencën e rënë dakord.

4. Politika duhet të sigurojë që çdo ndryshim thelbësor i marrëveshjes kontraktuale të formalizohet në një dokument të shkruar, të datuar dhe të nënshkruar nga të gjitha palët, si dhe duhet të përcaktojë procesin e rinovimit të marrëveshjeve kontraktuale.

Neni 56

Monitorimi i marrëveshjeve kontraktuale

1. Politika duhet të parashikojë kërkesa që marrëveshjet kontraktuale të përcaktojnë masat dhe treguesit kryesorë për monitorimin e vazhdueshëm të performancës së ofruesve të shërbimeve të palëve të treta të TIK-ut, duke përfshirë masat për monitorimin e përputhshmërisë me kërkesat që lidhen me konfidencialitetin, disponueshmërinë, integritetin dhe autenticitetin e të dhënave dhe informacionit, si dhe përputhshmërisë së ofruesve të shërbimeve të palëve të treta të TIK-ut, me politikat dhe procedurat përkatëse të subjektit financiar. Politika duhet, gjithashtu, të specifikojë masat që do të zbatohen, në rastet kur nuk arrihen nivelet e dakorduara të shërbimit, përfshirë, kur është e përshtatshme, aplikimin e penaliteteve kontraktuale.

2. Politika përcakton mënyrën se si subjekti financiar vlerëson nëse ofruesit e shërbimeve të palëve të treta të TIK-ut, të përdorur për shërbimet e TIK-ut që mbështesin funksionet kritike ose të rëndësishme, përmbushin standarde të përshtatshme të performancës dhe cilësisë, në përputhje me marrëveshjen kontraktuale dhe politikat e vetë subjektit financiar. Politika, në veçanti, duhet të sigurojë që:

a) ofruesit e shërbimeve të palëve të treta të TIK-ut t'i paraqesin subjektit financiar raporte të rregullta mbi veprimtarinë dhe shërbimet e tyre, duke përfshirë raporte periodike, raporte incidentesh, raporte mbi ofrimin e shërbimeve, raporte mbi sigurinë e TIK-ut dhe raporte mbi masat dhe testimet e vazhdimësisë së biznesit;

b) performanca e ofruesve të shërbimeve të palëve të treta të TIK-ut, vlerësohet nëpërmjet treguesve kryesorë të performancës (KPI), treguesve kryesorë të kontrollit (KCI), auditimeve, vetëcertifikimeve dhe rishikimeve të pavarura, në përputhje me sistemin e administrimit të rrezikut të TIK-ut të subjektit financiar;

c) subjekti financiar merr informacione të tjera përkatëse nga ofruesit e shërbimeve të palëve të treta të TIK-ut;

d) subjekti financiar të njoftohet, kur është e përshtatshme, për incidentet e lidhura me TIK-un dhe incidentet operationale ose të sigurisë që lidhen me pagesat;

e) të kryhen rishikime dhe auditime të pavarura për verifikimin e përputhshmërisë me kërkesat ligjore dhe rregullative dhe me politikat përkatëse të subjektit financiar.

3. Politika duhet të përcaktojë që vlerësimi i parashikuar në pikën 2 të këtij neni të dokumentohet dhe rezultatet e tij të përdoren për përditësimin e vlerësimit të rrezikut të subjektit financiar të parashikuar në nenin 53 të kësaj rregulloreje.

4. Politika duhet të përcaktojë masat e përshtatshme që subjekti financiar duhet të ndërmarrë, nëse identifikohen mangësi nga ana e ofruesve të shërbimeve të palëve të treta të TIK-ut, përfshirë incidentet e lidhura me TIK-un dhe incidentet operationale ose të sigurisë që lidhen me pagesat, në ofrimin e shërbimeve të TIK-ut që mbështesin funksionet kritike ose të rëndësishme, ose në përputhshmërinë me marrëveshjet kontraktuale apo kërkesat ligjore. Politika duhet, gjithashtu, të specifikojë mënyrën e monitorimit të zbatimit të këtyre masave, për të siguruar që ato të zbatohen në mënyrë efektive brenda një afati të përcaktuar, duke marrë në konsideratë edhe rëndësinë e mangësive të konstatuara.

Neni 57

Dalja nga marrëveshjet kontraktuale dhe ndërprerja e marrëveshjeve kontraktuale

1. Politika duhet të përmbajë kërkesa për hartimin e një plani daljeje (*exit plan*) të dokumentuar për çdo marrëveshje kontraktuale, si dhe për rishikimin dhe testimin periodik të këtij plani. Gjatë hartimit të planit të daljes duhet të merren parasysh këto elemente:

- a) ndërprerjet e papritura dhe të vazhdueshme të shërbimit;
- b) ofrimi i papërshtatshëm ose i dështuar i shërbimit;
- c) ndërprerja e papritur e marrëveshjes kontraktuale.

2. Plani i daljes (*exit plan*) duhet të jetë realist, i zbatueshëm, i bazuar në skenarë të besueshëm dhe në supozime të arsyeshme, dhe duhet të përfshijë një afat të planifikuar zbatimi që të jetë në përputhje me kushtet e daljes dhe të ndërprerjes të përcaktuara në marrëveshjet kontraktuale.

KREU VI

BASHKËPUNIMI NDËRKOMBËTAR DHE SHKËMBIMI I INFORMACIONIT

Neni 58

Bashkëpunimi ndërkombëtar

1. Banka e Shqipërisë mund të lidhë marrëveshje administrative me Autoritetin Bankar Evropian, me kërkesë të këtij të fundit, për qëllime të bashkëpunimit ndërkombëtar mbi rrezikun e palëve të treta të TIK-ut në sektorë të ndryshëm financiarë, në veçanti duke zhvilluar praktikatat më të mira për shqyrtimin e praktikave dhe kontrolleve të administrimit të rrezikut të TIK-ut, masave zbutëse dhe reagimit ndaj incidenteve.

Neni 59

Shkëmbimi i informacionit mbi të dhënat dhe inteligjencën për kërcënimet kibernetike

1. Subjektet financiare mund të shkëmbejnë ndërmjet tyre informacion dhe inteligjencë për kërcënimet kibernetike, duke përfshirë treguesit e kompromentimit, taktikat, teknikat dhe procedurat, sinjalizimet e sigurisë kibernetike dhe mjetet e konfigurimit, në masën që një shkëmbim i tillë i informacionit dhe inteligjencës:

a) synon rritjen e qëndrueshmërisë operacionale digjitale të subjekteve financiare, veçanërisht nëpërmjet rritjes së ndërgjegjësimit në lidhje me kërcënimet kibernetike, kufizimit ose pengimit të aftësisë së kërcënimeve kibernetike për t'u përhapur, mbështetjes së aftësive mbrojtëse të subjekteve financiare, teknikave të zbulimit të kërcënimeve, strategjive zbutëse ose fazave të reagimit dhe të rikuperimit;

b) kryhet brenda komuniteteve të besuara të subjekteve financiare;

c) zbatohet përmes marrëveshjeve për shkëmbimin e informacionit që mbrojnë natyrën potencialisht të ndjeshme të informacionit të shkëmbyer dhe që rregullohen nga rregullat e sjelljes, duke respektuar plotësisht konfidencialitetin e biznesit, mbrojtjen e të dhënave personale, në përputhje me legjislacionin për mbrojtjen e të dhënave personale, si dhe rregullat mbi politikën e konkurrencës.

2. Për qëllime të zbatimit të shkronjës “c” të pikës 1 të këtij neni, marrëveshjet për shkëmbimin e informacionit duhet të përcaktojnë kushtet për pjesëmarrje dhe, sipas rastit, duhet të përcaktojnë edhe detajet mbi përfshirjen e autoriteteve publike dhe kapacitetin në të cilin këto të fundit mund të lidhen me marrëveshjet për shkëmbimin e informacionit, mbi përfshirjen e ofruesve të shërbimeve të palëve të treta të TIK-ut, si dhe mbi elementet operacionale, duke përfshirë përdorimin e platformave të dedikuara të teknologjisë së informacionit.

3. Subjektet financiare njoftojnë Bankën e Shqipërisë për pjesëmarrjen e tyre në marrëveshjet për shkëmbimin e informacionit të parashikuara në pikën 1 të këtij neni, pas vërtetimit për anëtarësimin e tyre, ose, sipas rastit, për përfundimin e anëtarësimit të tyre, pasi ky të hyjë në fuqi.

KREU VII
KUADRI I MBIKËQYRJES PËR OFRUESIT KRITIKË TË SHËRBIMEVE TË
PALËVE TË TRETA TË TIK-ut

NËNKREU I
KUADRI I MBIKËQYRJES PËR OFRUESIT KRITIKË TË SHËRBIMEVE TË
PALËVE TË TRETA TË TIK-ut NË NIVEL BASHKIMI EVROPIAN

Neni 60

Përcaktimi i ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut

1. Autoritetet Evropiane Mbikëqyrëse (ESA-t), nëpërmjet Komitetit të Përbashkët (*Joint Committee*) dhe bazuar në rekomandimin e Forumit të Mbikëqyrjes të ngritur sipas nenit 32(1) të Rregullores (BE) 2022/2554:

a) përcaktojnë ofruesit e shërbimeve të palëve të treta të TIK-ut, që konsiderohen kritikë për subjektet financiare, pas një vlerësimi bazuar në kriteret e përcaktuara në nenin 31(2), të Rregullores (BE) 2022/2554 dhe sipas parashikimeve të pikës 2 të këtij neni;

b) caktojnë si Mbikëqyrës Kryesor (*Lead Overseer*) për secilin ofrues kritik të shërbimeve të TIK-ut, ESA që është përgjegjëse, në përputhje me Rregulloret (BE) nr. 1093/2010, (BE) nr. 1094/2010 ose (BE) nr. 1095/2010, për subjektet financiare që zotërojnë së bashku pjesën më të madhe të vlerës totale të aktiveve, nga totali i aktiveve të të gjitha subjekteve financiare që përdorin shërbimet e ofruesit përkatës të shërbimeve të palëve të treta të TIK-ut, vërtetuar nga bilancet individuale të atyre subjekteve financiare.

2. Përcaktimi i përmendur në pikën 1, shkronja “a”, të këtij neni, bazohet në të gjitha kriteret e mëposhtme që lidhen me shërbimet e TIK-ut të ofruara nga ofruesi përkatës i shërbimeve të palëve të treta të TIK-ut:

a) ndikimi sistematik mbi stabilitetin, vazhdimësinë ose cilësinë e ofrimit të shërbimeve financiare, në rast se ofruesi i shërbimeve të palëve të treta të TIK-ut do të përballej me një dështim operacional në shkallë të gjerë për ofrimin e shërbimeve të tij, duke marrë parasysh numrin e subjekteve financiare dhe vlerën totale të aktiveve të subjekteve financiare që përdorin shërbimet e këtij ofruesi;

b) karakteri ose rëndësia sistematike e subjekteve financiare që mbështeten tek ofruesi përkatës i shërbimeve të palëve të treta të TIK-ut, i vlerësuar në përputhje me parametrat e mëposhtëm:

i. numri i institucioneve me rëndësi sistematike globale (G-SII) ose institucioneve të tjera me rëndësi sistematike (O-SII) që mbështeten tek ofruesi përkatës i shërbimeve TIK,

ii. ndërvarësia midis G-SII-ve ose O-SII-ve të përmendura në nënpikën “i” dhe subjekteve të tjera financiare, përfshirë rastet kur këto institucione ofrojnë shërbime të infrastrukturës financiare për subjekte të tjera financiare;

c) varësia e subjekteve financiare nga shërbimet e ofruara nga ofruesi përkatës i shërbimeve të palëve të treta të TIK-ut, në lidhje me funksione kritike ose të rëndësishme, përfshirë rastet kur këto funksione mbështeten te i njëjti ofrues i shërbimeve TIK-ut, pavarësisht nëse kjo varësi është e drejtpërdrejtë apo e tërthortë, përmes marrëveshjeve të nënkontraktimit;

d) shkalla e zëvendësueshmërisë së ofruesit të shërbimeve të palëve të treta të TIK-ut, duke marrë në konsideratë kriteret e mëposhtme:

i. mungesën e alternativave reale, qoftë edhe të pjesshme, për shkak të numrit të kufizuar të ofruesve aktivë në një treg të caktuar, pjesës së tregut që zotëron ofruesi përkatës, ose kompleksitetit teknik apo nivelit të sofistikimit, përfshirë në lidhje me çdo teknologji pronësore, si dhe veçoritë specifike të organizimit apo aktivitetit të ofruesit të shërbimeve të palëve të treta të TIK-ut,

ii. vështirësitë në migrimin pjesor ose të plotë të të dhënave dhe ngarkesave përkatëse nga ofruesi ekzistues te një tjetër, për shkak të kostove financiare të konsiderueshme, kohës ose burimeve të tjera të nevojshme, apo për shkak të rrezikut të shtuar të TIK-ut ose rreziqeve të tjera operationale që mund të lindin gjatë këtij procesi të migrimit.

3. Në rastet kur ofruesi i shërbimeve të palëve të treta të TIK-ut i përket një grupi, kriteret e përmendura në pikën 2 të këtij neni merren në konsideratë në lidhje me shërbimet e TIK-ut të ofruara nga grupi në tërësi.

4. Ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut që janë pjesë e një grupi, caktojnë një person juridik si pikë koordinimi për të siguruar përfaqësimin dhe komunikimin e duhur me Mbikëqyrësin Kryesor.

5. Mbikëqyrësi Kryesor njofton ofruesin e shërbimeve të palëve të treta të TIK-ut, për rezultatin e vlerësimit që çon në përcaktimin e tij si kritik, sipas nenit 31(1), shkronja “a”, të Rregullores (BE) 2022/2554.

Brenda 6 javëve nga data e njoftimit, ofruesi i shërbimeve të palëve të treta të TIK-ut mund të paraqesë pranë Mbikëqyrësit Kryesor një deklaratë të arsyetuar, e cila mund të shoqërohet me çdo informacion përkatës për qëllime të vlerësimit. Mbikëqyrësi Kryesor shqyrton deklaratën e arsyetuar dhe mund të kërkojë informacione shtesë, të cilat duhet të dorëzohen brenda 30 ditëve kalendarike nga marrja e kërkesës.

Pas përcaktimit të një ofruesi të shërbimeve të palëve të treta të TIK-ut si kritik, ESA-t, nëpërmjet Komitetit të Përbashkët, njoftojnë zyrtarisht ofruesin për këtë përcaktim dhe për datën e fillimit nga e cila ai do t’i nënshtrohet aktivitetit të mbikëqyrjes.

Kjo datë nuk mund të jetë më vonë se një muaj nga njoftimi. Ofruesi i shërbimeve të palëve të treta të TIK-ut njofton të gjitha subjektet financiare që u ofron shërbime, për përcaktimin e tij si ofrues kritik.

6. Përcaktimi i përmendur në pikën 1, shkronja “a”, të këtij neni, nuk aplikohet për rastet e mëposhtme:

a) subjektet financiare që ofrojnë shërbime të TIK-ut për subjekte të tjera financiare;

b) ofruesit e shërbimeve të TIK-ut që i nënshtrohen kuadrit mbikëqyrës të krijuar për qëllimet e mbështetjes së detyrave të përmendura në nenin 127, paragrafi 2, të Traktatit për Funksionimin e Bashkimit Evropian;

c) ofruesit e shërbimeve të TIK-ut brenda grupit;

d) ofruesit e shërbimeve të palëve të treta të TIK-ut që ofrojnë shërbime të TIK-ut vetëm në një shtet anëtar për subjekte financiare që janë aktive vetëm në atë shtet.

7. ESA-t, nëpërmjet Komitetit të Përbashkët, krijojnë, publikojnë dhe përditësojnë çdo vit listën e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut, në nivel Bashkimi Evropian.

8. Për qëllimet e nenit 31(1), shkronja “a”, të Rregullores (BE) 2022/2554, Banka e Shqipërisë i përcjell çdo vit dhe në mënyrë të përmblodhur raportet e përmendura në nenin 45, pika 5, të kësaj rregulloreje, te Forumi i Mbikëqyrjes i krijuar sipas nenit 32 të Rregullores (BE) 2022/2554. Forumi i Mbikëqyrjes vlerëson varësitë e subjekteve financiare nga ofruesit e shërbimeve të TIK-ut, bazuar në informacionin e marrë nga Banka e Shqipërisë dhe autoritetet e tjera përgjegjëse.

9. Ofruesit e shërbimeve të palëve treta të TIK-ut që nuk janë përfshirë në listën e përmendur në pikën 7 të këtij neni, mund të kërkojnë të përcaktohen si kritikë, në përputhje me pikën 1, shkronja “a”, të këtij neni.

Për këtë qëllim, ofruesi i shërbimeve të palëve të treta të TIK-ut paraqet një kërkesë të arsyetuar pranë EBA-së, ESMA-s ose EIOPA-s, të cilat, nëpërmjet Komitetit të Përbashkët, vendosin nëse do ta përcaktojnë ofruesin përkatës të shërbimeve të palëve të treta të TIK-ut si kritik, në përputhje me nenin 31(1), shkronja “a”, të Rregullores (BE) 2022/2554.

Vendimi i përmendur në nënparagrafin e dytë të kësaj pike miratohet dhe i njoftohet ofruesit të shërbimeve të palëve të treta të TIK-ut, brenda 6 muajve nga marrja e kërkesës.

10. Subjektet financiare mund të përdorin shërbimet e një ofruesi të shërbimeve të palëve të treta të TIK-ut të vendosur në një vend të tretë dhe që është përcaktuar si kritik sipas nenit 31(1), shkronja “a”, të Rregullores (BE) 2022/2554, vetëm nëse ky ofrues ka krijuar një filial në Bashkimin Evropian brenda 12 muajve pas përcaktimit.

11. Ofruesi kritik i shërbimeve të palëve të treta të TIK-ut i përmendur në pikën 10 të këtij neni, njofton Mbikëqyrësin Kryesor për çdo ndryshim në strukturën e menaxhimit të filialit të krijuar në Bashkimin Evropian.

Neni 61

Struktura e Kuadrit të Mbikëqyrjes

1. Komiteti i Përbashkët (*Joint Committee*), në përputhje me nenin 57(1) të Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010, krijon Forumin e Mbikëqyrjes si një nënkomitet, me qëllim mbështetjen e punës së Komitetit të Përbashkët (*Joint Committee*) dhe të Mbikëqyrësit Kryesor (*Lead Overseer*) të referuar në nenin 31(1), shkronja “b”, të Rregullores (BE) 2022/2554, në fushën e rrezikut të TIK-ut nga palët e treta në të gjithë sektorët financiarë. Forumi i Mbikëqyrjes përgatit draft-qëndrimet dhe draft-aktet e përbashkëta të këtij Komiteti në këtë fushë.

Komiteti i përbashkët diskuton rregullisht zhvillimet mbi rrezikun dhe vulnerabilitetet e TIK-ut dhe nxit një qasje të qëndrueshme në monitorimin e rrezikut të TIK-ut nga palët e treta në nivel Bashkimi Evropian.

2. Forumi i Mbikëqyrjes kryen çdo vit një vlerësim kolektiv të rezultateve dhe gjetjeve të aktiviteteve të mbikëqyrjes të kryera për të gjithë ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, dhe promovon masa koordinimi për forcimin e qëndrueshmërisë operationale digjitale të subjekteve financiare, nxitjen e praktikave më të mira në adresimin e rrezikut të përqendrimit të TIK-ut dhe identifikimin dhe vlerësimin e masave për zbutjen e rreziqeve ndërsektoriale.

3. Forumi i Mbikëqyrjes paraqet kritere vlerësimi gjithëpërfshirëse për ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, të cilat miratohen nga Komiteti i Përbashkët, si qëndrim i përbashkët të ESA-ve, në përputhje me nenin 56(1) të Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010.

4. Forumi i Mbikëqyrjes përbëhet nga:

a) Kryetarët e ESA-ve;

b) një përfaqësues në nivel drejtues nga stafi aktual i autoritetit përgjegjës përkatës, siç përcaktohet në nenin 46 të Rregullores (BE) 2022/2554, për secilin shtet anëtar;

c) Drejtorët Ekzekutivë të secilës ESA dhe një përfaqësues nga Komisioni Evropian, nga Bordi Evropian i Rrezikut Sistemik (*ESRB*), nga Banka Qendrore Evropiane (*BQE*) dhe nga ENISA, me statusin e vëzhguesit;

d) kur është e nevojshme, një përfaqësues shtesë nga një autoritet përgjegjës i përcaktuar në nenin 46 të Rregullores (BE) 2022/2554, për secilin shtet anëtar, me statusin e vëzhguesit;

e) kur është e aplikueshme, një përfaqësues me status vëzhguesi, i autoriteteve përgjegjëse të caktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555, përgjegjëse për mbikëqyrjen e një subjekti thelbësor ose të rëndësishëm sipas asaj direktive, që është përcaktuar si ofrues kritik i shërbimeve të palëve të treta të TIK-ut.

Forumi i Mbikëqyrjes, kur e konsideron të përshtatshme, kërkon këshillim nga ekspertë të pavarur, të emëruar në përputhje me nenin 32(6) të Rregullores (BE) 2022/2554.

5. Çdo shtet anëtar cakton autoritetin përgjegjës përkatës, i cilit emëron përfaqësuesin e vet në nivel drejtues, i referuar në pikën 4, shkronja “b”, dhe njofton Mbikëqyrësin Kryesor për këtë emërim.

ESA-t publikojnë në faqet e tyre zyrtare të internetit listën e përfaqësuesve të nivelit të lartë drejtues nga stafi aktual i autoriteteve përgjegjëse të caktuara nga shtetet anëtare.

6. Ekspertët e pavarur të përmendur në pikën 4, paragrafi i dytë të këtij neni, emërohen nga Forumi i Mbikëqyrjes të përzgjedhur nga një grup ekspertësh nëpërmjet një procesi publik dhe transparent aplikimi.

Ekspertët e pavarur emërohen mbi bazën e ekspertizës së tyre në çështjet e stabilitetit financiar, qëndrueshmërisë operationale digjitale dhe sigurisë së TIK-ut. Ata veprojnë në mënyrë të pavarur dhe objektive, në interes të vetëm të Bashkimit Evropian si një i tërë, dhe nuk kërkojnë e as marrin udhëzime nga institucionet ose organet e BE-së, nga ndonjë qeveri e një shteti anëtar apo nga ndonjë organ tjetër publik ose privat.

7. Kërkesat e përcaktuara në këtë kre nuk cenojnë zbatimin e Direktivës (BE) 2022/2555 dhe të rregullave të tjera të Bashkimit Evropian mbi mbikëqyrjen e ofruesve të shërbimeve të “cloud computing”.

8. ESA-t, nëpërmjet Komitetit të Përbashkët dhe mbi bazën e punës përgatitore të kryer nga Forumi i Mbikëqyrjes, paraqesin çdo vit një raport mbi zbatimin e seksionit II të kreut V të Rregullores (BE) 2022/2554 në Parlamentin Evropian, Këshillin Evropian dhe Komisionin Evropian.

Neni 62

Detyrat e Mbikëqyrësit Kryesor (*Lead Overseer*)

1. Mbikëqyrësi Kryesor, i përcaktuar në përputhje me nenin 31(1), shkronja “b”, të Rregullores (BE) 2022/2554, ushtron mbikëqyrjen ndaj ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut, dhe për të gjitha çështjet që lidhen me mbikëqyrjen, vepron si pikë kryesore kontakti për këta ofrues.

2. Për qëllime të nenit 33(1) të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor vlerëson nëse ofruesi kritik i shërbimeve të palëve të treta të TIK-ut ka vendosur rregulla, procedura dhe mekanizma, si dhe ka marrë masa të plota, të qëndrueshme dhe efektive për të administruar rrezikun e TIK-ut që mund t’iu shkaktojë subjekteve financiare. Ky vlerësim përqendrohet kryesisht në shërbimet e TIK-ut të ofruara nga ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut që mbështesin funksione kritike ose të rëndësishme të subjekteve financiare.

Kur është e nevojshme për të adresuar të gjitha rreziqet përkatëse, vlerësimi zgjerohet edhe mbi shërbimet e TIK-ut që mbështesin funksione të tjera, përveç atyre kritike ose të rëndësishme.

3. Vlerësimi i përmendur në pikën 2 të këtij neni, përfshin:

a) kërkesat e TIK-ut për të garantuar sigurinë, disponueshmërinë, vazhdimësinë, shkallëzimin dhe cilësinë e shërbimeve që ofruesi kritik i shërbimeve të palëve të treta të TIK-ut u ofron subjekteve financiare, si dhe aftësinë për të ruajtur në çdo kohë standarde të larta të disponueshmërisë, autenticitetit, integritetit dhe konfidencialitetit të të dhënave;

b) masat e sigurisë fizike që kontribuojnë në mbrojtjen e sigurisë së TIK-ut, përfshirë sigurinë e ndërtesave, objekteve dhe bazës së të dhënave;

c) proceset e administrimit të rrezikut, përfshirë politikat e administrimit të rrezikut të TIK-ut, politikën e vazhdimësisë së biznesit të TIK-ut dhe planet e reagimit dhe rimëkëmbjes të TIK-ut;

d) mekanizmat e qeverisjes, përfshirë një strukturë organizative me linja të qarta, transparente dhe të qëndrueshme përgjegjësie dhe llogaridhënieje, që mundësojnë një administrim efektiv të rrezikut të TIK-ut;

e) identifikimin, monitorimin dhe raportimin e menjëhershëm të incidenteve të rëndësishme të lidhur me TIK-un ndaj subjekteve financiare, si dhe menaxhimin dhe zgjidhjen e këtyre incidenteve, në veçanti të sulmeve kibernetike;

f) mekanizmat për transferimin e të dhënave (*data portability*) dhe aplikacioneve për ndërveprueshmërinë e aplikacioneve që sigurojnë ushtrim efektiv të të drejtave të përfundimit të marrëdhënieve kontraktuale nga subjektet financiare;

g) testimin e sistemeve, infrastrukturës dhe kontrolleve të TIK-ut;

h) auditimet e TIK;

i) përdorimin e standardeve kombëtare dhe ndërkombëtare përkatëse që zbatohen për ofrimin e shërbimeve të TIK-ut ndaj subjekteve financiare.

4. Bazuar në vlerësimin e referuar në pikën 2 të nenit 33 të Rregullores (BE) 2022/2554, dhe në bashkëpunim me Rrjetin e Përbashkët të Mbikëqyrjes (*Joint Oversight Network – JON*) të referuar në nenin 34(1) të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor miraton një plan mbikëqyrjeje individual të qartë, të detajuar dhe të arsyetuar, që përshkruan objektivat vjetorë të mbikëqyrjes dhe veprimet kryesore të planifikuara për secilin ofrues kritik të shërbimeve të palëve të treta të TIK-ut.

Ky plan i komunikohet çdo vit ofruesit përkatës të shërbimeve të palëve të treta të TIK-ut.

Para miratimit të planit të mbikëqyrjes, Mbikëqyrësi Kryesor i dërgon ofruesit kritik të shërbimeve të palëve të treta të TIK-ut një draft të planit të mbikëqyrjes.

Pas marrjes së këtij drafti, ofruesi kritik i shërbimeve të palëve të treta të TIK-ut mund të paraqesë brenda 15 ditëve kalendarike një deklaratë të arsyetuar, duke paraqitur ndikimin e mundshëm mbi klientët që janë subjekte jashtë fushës së Rregullores (BE) 2022/2554 dhe, kur është e aplikueshme, duke propozuar zgjidhje për zbutjen e rreziqeve.

5. Pasi planet vjetore të mbikëqyrjes të përmendura në pikën 4 janë miratuar dhe iu janë njoftuar ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut, Banka e Shqipërisë mund të marrë masa ndaj këtyre ofruesve vetëm me marrëveshje me Mbikëqyrësin Kryesor.

Neni 63

Koordinimi operacional ndërmjet Mbikëqyrësve Kryesorë (*Lead Overseers*)

1. Për të siguruar një qasje të qëndrueshme ndaj aktiviteteve të mbikëqyrjes dhe me qëllim mundësimin e strategjive të përgjithshme të mbikëqyrjes, të koordinuara, si dhe qasjeve operationale dhe metodologjive të punës të bashkërenduara, tre Mbikëqyrësit Kryesorë të përcaktuar në përputhje me nenin 31(1), shkronja “b”, të rregullores (BE) 2022/2554, do të krijojnë një Rrjet të Përbashkët të Mbikëqyrjes (*JON*). Ky rrjet ka për qëllim koordinimin ndërmjet fazave përgatitore dhe kryerjen e aktiviteteve të mbikëqyrjes mbi ofruesit kritikë përkatës të shërbimeve të palëve të treta të TIK-ut, si dhe gjatë çdo veprimi që mund të jetë i nevojshëm në zbatim të nenit 42 të Rregullores (BE) 2022/2554 dhe sipas parashikimeve të nenit 71 të kësaj rregulloreje.

2. Për qëllime të pikës 1 të nenit 34 të Rregullores (BE) 2022/2554, Mbikëqyrësit Kryesorë hartojnë një protokoll të përbashkët mbikëqyrjeje që specifikon në mënyrë të detajuar procedurat që duhen ndjekur për koordinimin e përditshëm dhe për të siguruar shkëmbime dhe reagime të shpejta. Ky protokoll do të rishikohet periodikisht për të pasqyruar nevojat operationale, në veçanti zhvillimet në praktikën e mbikëqyrjes.

3. Mbikëqyrësit Kryesorë, mbi baza *ad hoc*, mund t’i bëjnë thirrje Bankës Qendrore Evropiane dhe ENISA-s për të ofruar këshilla teknike, për të ndarë përvojën praktike ose për t’u përfshirë në takime të caktuara të koordinimit të Rrjetit të Përbashkët të Mbikëqyrjes (*JON*).

Kompetencat e Mbikëqyrësit Kryesor (*Lead Overseer*)

1. Mbikëqyrësi Kryesor, me qëllim kryerjen e detyrave të përcaktuara në seksionin II të kreut V të Rregullores (BE) 2022/2554, në lidhje me ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, ka kompetencat e mëposhtme:

a) kërkon të gjithë informacionin dhe dokumentacionin sipas parashikimeve në nenin 37 të Rregullores (BE) 2022/2554;

b) kryen hetime të përgjithshme dhe inspektive në përputhje me nenet 38 dhe 39 të Rregullores (BE) 2022/2554;

c) kërkon, pas përfundimit të aktivitetit mbikëqyrës, raporte që specifikojnë veprimet që janë ndërmarrë ose masat korrigjuese që janë zbatuar nga ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, në lidhje me rekomandimet e referuara në shkronjën “d” të nenit 35(1) të Rregullores (BE) 2022/2554;

d) jep rekomandime mbi fushat e parashikuara në nenin 33(3) të Rregullores (BE) 2022/2554, veçanërisht në lidhje me:

i. përdorimin e kërkesave ose proceseve specifike të sigurisë dhe cilësisë së TIK-ut, veçanërisht në lidhje me implementimin e *patch*-eve, përditësimeve, enkriptimit dhe masave të tjera të sigurisë, të cilat Mbikëqyrësi Kryesor i vlerëson si të nevojshme për garantimin e sigurisë së shërbimeve të TIK-ut të ofruara ndaj subjekteve financiare;

ii. përdorimin e kushteve dhe termave, përfshirë zbatimin teknik të tyre, sipas të cilave ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut i ofrojnë shërbime të TIK-ut subjekteve financiare, të cilat Mbikëqyrësi Kryesor i vlerëson si të rëndësishme për parandalimin e krijimit të pikave të vetme të dështimit, për shmangien e përhapjes së tyre, ose për minimizimin e ndikimit të mundshëm sistematik në të gjithë sektorin financiar të Bashkimit Evropian, në rast të rrezikut të përqendrimit të TIK-ut;

iii. çdo nënkontraktim të planifikuar, ku Mbikëqyrësi Kryesor gjykon se nënkontraktimi i mëtejshëm, përfshirë marrëveshjet e nënkontraktimit që ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut planifikojnë të lidhin me ofrues të shërbimeve të palëve të treta të TIK-ut ose me nënkontraktorë të TIK-ut të themeluar në një vend të tretë, mund të shkaktojë rreziqe për ofrimin e shërbimeve nga subjekti financiar, ose rreziqe për stabilitetin financiar, bazuar në shqyrtimin e informacionit të mbledhur në përputhje me nenet 37 dhe 38 të Rregullores (BE) 2022/2554;

iv. mos hyrjen në një marrëveshje të mëtejshme nënkontraktimi, kur plotësohen njëkohësisht të gjitha kushtet e mëposhtme:

- nënkontraktori i parashikuar është një ofrues i shërbimeve të palëve të treta të TIK-ut ose një nënkontraktor i TIK-ut i themeluar në një vend të tretë;

- nënkontraktimi lidhet me funksione kritike ose të rëndësishme të subjektit financiar, dhe

- Mbikëqyrësi Kryesor vlerëson se përdorimi i një nënkontraktimi të tillë paraqet një rrezik të qartë dhe serioz për stabilitetin financiar të Bashkimit Evropian ose për subjektet financiare, përfshirë aftësinë e tyre për të përmbushur kërkesat mbikëqyrëse.

Për qëllime të nënpikës “iv” të shkronjës “b” të nenit 35(1) të Rregullores (BE) 2022/2554, ofruesit e shërbimeve të palëve të treta të TIK-ut, i transmetojnë Mbikëqyrësit Kryesor informacionin lidhur me nënkontraktimin, duke përdorur formularët e parashikuar në nenin 41(1), shkronja “b” të Rregullores (BE) 2022/2554.

2. Gjatë ushtrimit të kompetencave të parashikuara në nenin 35 të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor:

a) siguron koordinim të rregullt brenda Rrjetit të Përbashkët të Mbikëqyrjes (*JON*), dhe në veçanti, kërkon qasje të qëndrueshme sipas rastit, lidhur me mbikëqyrjen e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut;

b) merr në konsideratë kuadrin e vendosur nga Direktiva (BE) 2022/2555 dhe, kur është e nevojshme, konsultohet me autoritetet përgjegjëse përkatëse të caktuara ose të krijuara në përputhje me atë Direktivë, më qëllim shmangien e dublikimit të masave teknike dhe organizative që mund të zbatohen ndaj ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut në zbatim të asaj Direktive;

c) synon minimizimin, për aq sa është e mundur, të rrezikut të ndërprerjes së shërbimeve të ofruara nga ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, për klientët që janë subjekte të ndryshme nga ata që përfshihen në fushën e zbatimit të Rregullores (BE) 2022/2554.

3. Mbikëqyrësi Kryesor konsultohet me Forumin e Mbikëqyrjes (*Oversight Forum*) përpara se të ushtrojë kompetencat e parashikuara në pikën 1 të nenit 35 të Rregullores (BE) 2022/2554. Përpara se të japë rekomandime në përputhje me pikën 1, shkronja “d”, të nenit 35 të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor u jep mundësi ofruesve të shërbimeve të palëve të treta të TIK-ut të paraqesin brenda 30 ditëve kalendarike, informacion që dëshmon ndikimin e pritshëm mbi klientët që janë subjekte jashtë fushës së zbatimit të Rregullores (BE) 2022/2554 dhe, kur është e përshtatshme, të formulojnë zgjidhje për zbutjen e rreziqeve.

4. Mbikëqyrësi Kryesor informon Rrjetin e Përbashkët të Mbikëqyrjes (*JON*) mbi rezultatet e ushtrimit të kompetencave të parashikuara në pikën 1, shkronjat “a” dhe “b” të nenit 35 të Rregullores (BE) 2022/2554. Mbikëqyrësi Kryesor, pa vonesë të pajustificuar, përcjell raportet e përmendura në pikën 1, shkronja “c”, të nenit 35 të Rregullores (BE) 2022/2554, te *JON* dhe tek autoritetet përgjegjëse të subjekteve financiare që përdorin shërbimet e TIK-ut të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut.

5. Ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut bashkëpunojnë me mirëbesim me Mbikëqyrësin Kryesor dhe e asistojnë në përmbushjen e detyrave.

6. Në rast të moszbatimit të plotë ose të pjesshëm të masave që kërkohet të merren në zbatim të ushtrimit të kompetencave sipas pikës 1, shkronjat “a”, “b” dhe “c” të nenit 35 të Rregullores (BE) 2022/2554 dhe pas përfundimit të afatit prej të paktën 30 ditësh kalendarike nga data kur ofruesi kritik i shërbimeve të palëve të treta të TIK-ut ka marrë njoftimin për masat përkatëse, Mbikëqyrësi Kryesor vendos një gjorbë periodike për të detyruar ofruesin kritik të shërbimeve të palëve të treta të TIK-ut të përmbushë këto masa.

7. Gjorbë periodike e parashikuar në pikën 6 vendoset mbi baza ditore, derisa të arrihet përputhshmëria, por jo më gjatë se gjashtë muaj nga njoftimi i vendimit tek ofruesi kritik i shërbimeve të palëve të treta të TIK-ut, për vendosjen e gjorbës periodike.

8. Shuma e gjorbës periodike, e llogaritur nga data e përcaktuar në vendimin për vendosjen e saj, arrin deri në 1% të të ardhurave të përditshme mesatare në nivel botëror të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut gjatë vitit të mëparshëm financiar. Gjatë përcaktimit të shumës së gjorbës, Mbikëqyrësi Kryesor merr parasysh kriteret e mëposhtme:

a) rëndësinë dhe kohëzgjatjen e mospërputhshmërisë;

b) nëse mospërputhshmëria është kryer me dashje ose nga pakujdesia;

c) nivelin e bashkëpunimit të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut me Mbikëqyrësin Kryesor.

Për qëllimet e nënparagrafit të parë, për të siguruar qasje të qëndrueshme, Mbikëqyrësi Kryesor konsultohet me Rrjetin e Përbashkët të Mbikëqyrjes (*JON*).

9. Sipas parashikimeve të pikës 9 të nenit 35 të Rregullores (BE) 2022/2554, gjorbë periodike kanë natyrë administrative dhe janë të ekzekutueshme. Ekzekutimi do të rregullohet sipas procedurave civile në territorin e Republikës së Shqipërisë, ku do të kryhen inspektimet dhe aksesit. Gjykata kompetente për shqyrtimin e ankimit lidhur me sjelljen e parregullt të ekzekutimit do të jetë gjykata e përcaktuar sipas legjislacionit në fuqi në territorin e Republikës

së Shqipërisë. Shumat e mbledhura nga gjobat do t'i alokohen buxhetit të përgjithshëm të Bashkimit Evropian.

10. Mbikëqyrësi Kryesor publikon çdo gjobë periodike që është vendosur, përveç rastit kur një publikim i tillë do të rrezikonte seriozisht tregjet financiare ose do t'u shkaktonte dëm jo proporcional palëve të përfshira.

11. Para vendosjes së një gjobe periodike sipas të nenit 35(6) të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor u jep përfaqësuesve të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut që i nënshtrohet procedurës, mundësinë për t'u dëgjuar lidhur me gjetjet dhe bazon vendimin e tij vetëm mbi gjetjet për të cilat ofruesi ka pasur mundësi të japë komente.

12. Të drejtat e mbrojtjes së palëve që i nënshtrohen procedurës, respektohen plotësisht gjatë procesit. Ofruesi kritik i shërbimeve të palëve të treta të TIK-ut ka të drejtë të ketë akses në dosje, duke respektuar interesin legjitim të palëve të tjera për mbrojtjen e sekreteve tregtare të tyre. E drejta e aksesit në dosje nuk shtrihet mbi informacionin konfidencial ose dokumentet e brendshme përgatitore të Mbikëqyrësit Kryesor.

Neni 65

Ushtrimi i kompetencave të Mbikëqyrësit Kryesor (*Lead Overseer*) jashtë Bashkimit Evropian

1. Kur objektivat e mbikëqyrjes nuk mund të arrihen me anë të ndërveprimit me filialin e krijuar për qëllime të nenit 31(12) të Rregullores (BE) 2022/2554, ose nëpërmjet ushtrimit të aktiviteteve të mbikëqyrjes në ambiente të vendosura brenda Bashkimit Evropian, Mbikëqyrësi Kryesor mund të ushtrojë kompetencat e përcaktuara në dispozitat e mëposhtme, në çdo ambient të vendosur në Republikën e Shqipërisë që është në pronësi ose përdoret për ofrimin e shërbimeve ndaj subjekteve financiare të Bashkimit Evropian, nga një ofrues kritik i shërbimeve të palëve të treta të TIK-ut, lidhur me veprimtarinë e tij tregtare, funksionet ose shërbimet, përfshirë çdo zyrë administrative, tregtare ose operacionale, ndërtesa, tokë, objekte apo prona të tjera:

a) në nenin 35(1), shkronja “a”, të Rregullores (BE) 2022/2554; dhe

b) në nenin 35(1), shkronja “b”, të Rregullores (BE) 2022/2554, në përputhje me nenin 38(2), shkronjat “a”, “b” dhe “d”, dhe në nenin 39(1) dhe (2), shkronja “a”, të Rregullores (BE) 2022/2554.

2. Kompetencat e parashikuara në nënparagrafin e parë të nenit 36(1) të Rregullores (BE) 2022/2554, mund të ushtrohen duke iu nënshtuar të gjitha kushteve të mëposhtme:

i. kryerja e inspektimit në Republikën e Shqipërisë konsiderohet e nevojshme nga Mbikëqyrësi Kryesor për t'i lejuar atij të kryejë plotësisht dhe me efektivitet detyrat e tij sipas Rregullores (BE) 2022/2554;

ii. inspektimi në Republikën e Shqipërisë lidhet drejtpërdrejt me ofrimin e shërbimeve të TIK-ut për subjektet financiare në Bashkimin Evropian;

iii. ofruesi kritik përkatës i shërbimeve të palëve të treta të TIK-ut jep pëlqimin për kryerjen e një inspektimi në ambientet e tij, të vendosura në Republikën e Shqipërisë; dhe

iv. Banka e Shqipërisë është njoftuar zyrtarisht nga Mbikëqyrësi Kryesor dhe nuk ka ngritur asnjë kundërshtim ndaj tij.

3. Pa cenuar kompetencat e institucioneve përkatëse të Bashkimit Evropian dhe të shteteve anëtare, për qëllimet e pikës 1 të Rregullores (BE) 2022/2554, EBA-ja lidh marrëveshje

administrative bashkëpunimi me Bankën e Shqipërisë për të mundësuar inspektime në Republikën e Shqipërisë nga Mbikëqyrësi Kryesor dhe ekipi i caktuar prej tij për misionin e tij në Republikën e Shqipërisë. Marrëveshja e bashkëpunimit nuk krijon detyrime ligjore lidhur me Bashkimin Evropian dhe shtetet e tij anëtare dhe as nuk pengon shtetet anëtare dhe autoritetet e tyre përgjegjëse të lidhin marrëveshje dypalëshe ose shumëpalëshe me Bankën e Shqipërisë.

Marrëveshja e bashkëpunimit specifikon të paktën elementet e mëposhtme:

a) procedurat për koordinimin e aktiviteteve të mbikëqyrjes të kryera sipas Rregullores (BE) 2022/2554 dhe çdo monitorim analog të rrezikut të TIK-ut nga palët e treta në sektorin financiar të kryer nga Banka e Shqipërisë, përfshirë detajet për transmetimin e dakordësisë së saj, për të lejuar kryerjen nga Mbikëqyrësi Kryesor dhe ekipi i caktuar prej tij, të hetimeve të përgjithshme dhe inspektimeve në vend, siç referohet në pikën 1, nënparagrafi i parë i shkronjës b të nenit 36 të Rregullores (BE) 2022/2554, në territorin e Republikës së Shqipërisë;

b) mekanizmin për transmetimin e çdo informacioni ndërmjet EBA-së dhe Bankës së Shqipërisë, veçanërisht lidhur me informacionin që mund të kërkohej nga Mbikëqyrësi Kryesor në zbatim të nenit 37 të Rregullores (BE) 2022/2554;

c) mekanizmat për njoftim të menjëhershëm nga Banka e Shqipërisë tek EBA-ja, të rasteve kur një ofrues i shërbimeve të palëve të treta të TIK-ut i themeluar në Republikën e Shqipërisë dhe i përcaktuar si kritik në përputhje me nenin 31(1), shkronja “a”, të Rregullores (BE) 2022/2554, konsiderohet se ka shkelur detyrimet ligjore sipas ligjeve të zbatueshme në Republikën e Shqipërisë gjatë ofrimit të shërbimeve për institucionet financiare atje, si dhe për masat korrigjuese dhe sanksionet e zbatuara;

d) transmetimin periodik të përditësimeve mbi zhvillimet rregullatore ose mbikëqyrëse lidhur me monitorimin e rrezikut të TIK-ut nga palët e treta, për institucionet financiare në Republikën e Shqipërisë;

e) detajet lidhur me autorizimin e pjesëmarrjes, sipas rastit, të një përfaqësuesi të Bankës së Shqipërisë në inspektimet e kryera nga Mbikëqyrësi Kryesor dhe ekipi i autorizuar.

4. Kur Mbikëqyrësi Kryesor nuk është në gjendje të kryejë aktivitete mbikëqyrëse jashtë Bashkimit Evropian, të parashikuara në pikat 1 dhe 2 të nenit 36 të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor:

a) ushtron kompetencat e tij sipas nenit 35 të Rregullores (BE) 2022/2554, duke u bazuar në të gjitha faktet dhe dokumentet që disponon;

b) dokumenton dhe shpjegon çdo pasojë që rrjedh nga pamundësia për të zhvilluar aktivitetet e mbikëqyrjes sipas nenit 36 të Rregullores (BE) 2022/2554.

5. Në hartimin e rekomandimeve të Mbikëqyrësit Kryesor, të nxjerra në bazë të nenit 35(1), shkronja “d”, të Rregullores (BE) 2022/2554, do të merren në konsideratë pasojat e mundshme të përmendura në shkronjën “b” të pikës 4 të këtij neni.

Neni 66

Kërkesa për informacion

1. Mbikëqyrësi Kryesor, me kërkesë ose me vendim, mund të kërkojë nga ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, t'i vënë në dispozicion të gjitha informacionet e nevojshme për ushtrimin e detyrave, në bazë të Rregullores (BE) 2022/2554, përfshirë dokumentet tregtare ose operationale, kontratat, politikat, dokumentacionin teknik, raportet e auditimit të sigurisë së TIK-ut, raportet e incidenteve të lidhura me TIK-un, si dhe çdo informacion që lidhet me palët ndaj të cilave ofruesi kritik i shërbimeve të palëve të treta të TIK-ut ka nënkontraktuar funksione operationale ose aktivitete.

2. Kur Mbikëqyrësi Kryesor bën kërkesë për informacion sipas pikës 1 të nenit 37 të Rregullores (BE) 2022/2554, ai:

- a) referon nenin 37 të Rregullores (BE) 2022/2554, si bazë ligjore të kërkesës;
- b) deklaron qëllimin e kërkesës;
- c) specifikon se çfarë informacioni kërkohet;
- d) vendos një afat kohor brenda të cilit duhet të ofrohet informacioni;
- e) informon përfaqësuesin e ofruesit kritik të shërbimeve të palëve të treta të TIK-ut nga i cili kërkohet informacioni, se nuk është i detyruar të ofrojë informacionin, por në rast se përgjigjet në mënyrë vullnetare ndaj kërkesës, informacioni i ofruar duhet të jetë i saktë dhe orientues.

3. Kur Mbikëqyrësi Kryesor kërkon me vendim dhënien e informacionit sipas pikës 1 të nenit 37 të Rregullores (BE) 2022/2554, ai:

- a) referon nenin 37 të Rregullores (BE) 2022/2554, si bazë ligjore të kërkesës;
- b) deklaron qëllimin e kërkesës;
- c) specifikon se cili informacion kërkohet;
- d) vendos një afat kohor brenda të cilit duhet të ofrohet informacioni;
- e) tregon gjobat periodike të parashikuara në nenin 35(6) të Rregullores (BE) 2022/2554, në rast se informacioni i kërkuar është i paplotë ose kur ky informacion nuk ofrohet brenda afatit kohor të referuar në shkronjën “d”;

- f) tregon të drejtën për të ankimuar vendimin përpara Bordit të Apelit të ESA (*ESA's Board of Appeal*) dhe për të kërkuar rishikimin e vendimit nga Gjykata e Drejtësisë e Bashkimit Evropian (*Court of Justice*), në përputhje me nenet 60 dhe 61 të Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010.

4. Përfaqësuesit e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut do të japin informacionin e kërkuar. Avokatët e autorizuar mund të veprojnë në emër të klientëve të tyre për dorëzimin e informacionit. Ofruesi kritik i shërbimeve të palëve të treta të TIK-ut është plotësisht përgjegjës nëse informacioni i dhënë është i paplotë, i pasaktë ose çorientues.

5. Mbikëqyrësi Kryesor, pa vonesë, i transmeton një kopje të vendimit për dhënien e informacionit, Bankës së Shqipërisë, si autoritet përgjegjës i subjekteve financiare që përdorin shërbimet e ofruesve kritikë përkatës të shërbimeve të palëve të treta të TIK-ut dhe Rrjetit të Përbashkët të Mbikëqyrjes (*JON*).

Neni 67

Hetimet e përgjithshme

1. Për të ushtruar detyrat sipas Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor, i asistuar nga ekipi i përbashkët i inspektimit sipas nenit 40(1) të Rregullores (BE) 2022/2554, kur është e nevojshme, mund të zhvillojë hetime ndaj ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut.

2. Mbikëqyrësi Kryesor, në përputhje me pikën 2 të nenit 38 të Rregullores (BE) 2022/2554, ka kompetencën për të:

- a) inspektuar regjistra (*records*), të dhëna, procedura dhe çdo material tjetër të rëndësishëm për ushtrimin e detyrave të tij, pavarësisht nga forma ose mjeti në të cilin ruhen ato;

- b) marrë ose siguruar kopje të certifikuara ose ekstrakte nga këta regjistra, të dhëna, procedura të dokumentuara dhe çdo material tjetër;

- c) thirrur përfaqësues të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut, për të dhënë shpjegime me gojë ose me shkrim mbi fakte ose dokumente që lidhen me objektin dhe qëllimin e hetimit, si dhe për të regjistruar përgjigjet;

- d) intervistuar çdo person fizik ose juridik që pranon të intervistohet, me qëllim mbledhjen e informacionit lidhur me objektin e hetimit;

- e) kërkuar regjistrime të komunikimeve telefonike dhe qarkullimit të të dhënave.

3. Zyrtarët dhe personat e autorizuar nga Mbikëqyrësi Kryesor, me qëllim kryerjen e hetimit të parashikuar në pikën 1 të nenit 38 të Rregullores (BE) 2022/2554, do të ushtrojnë kompetencat e tyre pas paraqitjes së një autorizimi me shkrim që specifikon objektin dhe qëllimin e hetimit. Autorizimi duhet, gjithashtu, të përmbajë gjobat periodike të parashikuara në nenin 35(6) të Rregullores (BE) 2022/2554, në rast se dorëzimi i regjistrimeve të kërkuara, të dhënat, procedurat e dokumentuara ose çdo material tjetër, ose përgjigjet ndaj pyetjeve të bëra përfaqësuesve të ofruesit të shërbimeve të palëve të treta të TIK-ut, nuk ofrohen ose janë të paplota.

4. Përfaqësuesit e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut janë të detyruar t'u nënshtrohen hetimeve në bazë të një vendimi të Mbikëqyrësit Kryesor. Vendimi specifikon objektin dhe qëllimin e hetimit, gjobat periodike të parashikuara në nenin 35(6) të Rregullores (BE) 2022/2554, mjetet juridike të disponueshme sipas Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010, dhe të drejtën për të ankimuar vendimin pranë Gjykatës së Drejtësisë të Bashkimit Evropian (*Court of Justice*).

5. Përpara fillimit të hetimit, brenda një afati të arsyeshëm, Mbikëqyrësi Kryesor informon Bankën e Shqipërisë, si autoritet përgjegjës i subjekteve financiare që përdorin shërbimet e TIK-ut të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut, për hetimin e parashikuar dhe për identitetin e personave të autorizuar. Mbikëqyrësi Kryesor i komunikon Rrjetit të Përbashkët të Mbikëqyrjes (*JON*) të gjithë informacionin e transmetuar në përputhje me këtë pikë.

Neni 68 Inspektimet

1. Me qëllim përmbushjen e detyrave sipas Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor, i asistuar nga ekipet e përbashkëta të inspektimit të referuara në nenin 40(1) të Rregullores (BE) 2022/2554, kryen të gjitha inspektimet e nevojshme në vend, në çdo mjedis biznesi, tokë ose pronë të ofruesve të shërbimeve të palëve të treta të TIK-ut, të tilla si zyrat qendrore, qendrat e operimit, mjediset dytësore, si dhe kryen inspektime në distancë (*off-site*). Për qëllimet e ushtrimit të kompetencave të referuara në këtë pikë, Mbikëqyrësi Kryesor konsultohet edhe me Rrjetin e Përbashkët të Mbikëqyrjes (*JON*).

2. Zyrtarët dhe personat e autorizuar nga Mbikëqyrësi Kryesor për të kryer një inspektim në vend kanë kompetencën për të:

a) hyrë në çdo mjedis biznesi, tokë ose pronë; dhe

b) bllokuar çdo ambient biznesi, libër apo regjistër të tillë, për periudhën e inspektimit dhe në masën e nevojshme për kryerjen e tij. Zyrtarët dhe personat e tjerë të autorizuar nga Mbikëqyrësi Kryesor ushtrojnë kompetencat e tyre pas paraqitjes së një autorizimi me shkrim, në të cilin përcaktohen objekti dhe qëllimi i inspektimit, si dhe gjobat periodike të parashikuara në nenin 35(6) të Rregullores (BE) 2022/2554, në rast se përfaqësuesit e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut në fjalë, nuk i nënshtrohen inspektimit.

3. Përpara fillimit të inspektimit, Mbikëqyrësi Kryesor informon Bankën e Shqipërisë, si autoritet përgjegjës i subjekteve financiare që përdorin atë ofrues shërbimesh të palëve të treta të TIK-ut.

4. Objekti i inspektimeve shtrihet mbi të gjitha sistemet, rrjetet, pajisjet, informacionin dhe të dhënat përkatëse të TIK-ut, që përdoren për ose që kontribuojnë në ofrimin e shërbimeve të TIK-ut për subjektet financiare.

5. Para zhvillimit të çdo inspektimi të planifikuar në vend, Mbikëqyrësi Kryesor u jep ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut një njoftim paraprak, përveç rasteve kur një njoftim i tillë nuk është i mundur për shkak të një situatë emergjente ose krize, apo kur dhënia e tij do të ndikonte në efektivitetin e inspektimit ose auditimit.

6. Ofruesi kritik i shërbimeve të palëve të treta të TIK-ut iu nënshtrohet inspektimeve në vend me vendim të Mbikëqyrësit Kryesor. Vendimi specifikon objektin dhe qëllimin e inspektimit, cakton datën në të cilën do të fillojë inspektimi dhe tregon gjobat periodike të parashikuara në nenin 35(6) të Rregullores (BE) 2022/2554, mjetet juridike të disponueshme sipas Rregulloreve (BE) nr. 1093/2010, (BE) nr. 1094/2010 dhe (BE) nr. 1095/2010, si dhe të drejtën për rishikim të vendimit nga Gjykata e Drejtësisë e Bashkimit Evropian.

7. Kur zyrtarët dhe personat e tjerë të autorizuar nga Mbikëqyrësi Kryesor konstatojnë se një ofrues kritik i shërbimeve të palëve të treta të TIK-ut kundërshton një inspektim të urdhëruar në zbatim të nenit 39 të Rregullores (BE) 2022/2554, Mbikëqyrësi Kryesor informon ofruesin kritik të shërbimeve të palëve të treta të TIK-ut për pasojat e kundërshtimit, përfshirë mundësinë që Banka e Shqipërisë, si autoritet përgjegjës i subjekteve financiare përkatëse, t'u kërkojë subjekteve financiare të zgjidhin marrëveshjet kontraktuale të lidhura me atë ofrues kritik të shërbimeve të palëve të treta të TIK-ut.

Neni 69

Mbikëqyrja e vazhdueshme

1. Gjatë kryerjes së aktiviteteve mbikëqyrëse, veçanërisht hetimeve të përgjithshme ose inspektimeve, Mbikëqyrësi Kryesor asistohet nga një ekip i përbashkët inspektimi (*joint examination team*), i cili krijohet për secilin ofrues kritik të shërbimeve të palëve të treta të TIK-ut.

2. Ekipi i përbashkët i inspektimit, i përmendur në pikën 1 të nenit 40 të Rregullores (BE) 2022/2554, përbëhet nga anëtarë të stafit të:

- a) Autoriteteve Mbikëqyrëse Evropiane (ESA);
- b) Bankës së Shqipërisë, si autoritet përgjegjës për mbikëqyrjen e subjekteve financiare, të cilave ofruesi kritik i shërbimeve të palëve të treta të TIK-ut u ofron shërbime të TIK-ut;
- c) autoritetit kombëtar përgjegjës sipas nenit 32(4), shkronja “e”, të Rregullores (BE) 2022/2554, mbi baza vullnetare;
- d) një autoriteti kombëtar përgjegjës nga shteti anëtar, ku është themeluar ofruesi kritik i shërbimeve të palëve të treta të TIK-ut, mbi baza vullnetare.

3. Anëtarët e ekipit të përbashkët të inspektimit kanë ekspertizë në çështjet e TIK-ut dhe në rrezikun operacional. Ekipi i përbashkët i inspektimit, do të punojnë nën koordinimin e një anëtari të caktuar të stafit të Mbikëqyrësit Kryesor (*the “Lead Overseer coordinator”*).

4. Brenda 3 muajve nga përfundimi i një hetimi ose inspektimi, Mbikëqyrësi Kryesor, pas konsultimit me Forumin e Mbikëqyrjes, miraton rekomandime që do t'i drejtohen ofruesit kritik të shërbimeve të palëve të treta të TIK-ut, në zbatim të kompetencave të parashikuara në nenin 35 të Rregullores (BE) 2022/2554.

5. Rekomandimet e parashikuara në pikën 4 i komunikohen menjëherë ofruesit kritik të shërbimeve të palëve të treta të TIK-ut dhe Bankës së Shqipërisë, si autoritet përgjegjës i subjekteve financiare të cilave ai u ofron shërbime të TIK-ut.

6. Me qëllim përmbushjen e aktiviteteve mbikëqyrëse, Mbikëqyrësi Kryesor mund të marrë në konsideratë çdo certifikim të palëve të treta ose raporte të auditimit të brendshëm ose të jashtëm të palëve të treta të TIK-ut, të vëna në dispozicion nga ky ofrues.

Neni 70

Ndjekja (*Follow-up*) nga Banka e Shqipërisë

1. Brenda 60 ditëve kalendarike nga marrja e rekomandimeve të dhëna nga Mbikëqyrësi Kryesor në përputhje me nenin 35(1), shkronja “d”, të Rregullores (BE) 2022/2554, ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut do të njoftojnë Mbikëqyrësin Kryesor për

qëndrimin e tyre lidhur me ndjekjen dhe zbatimin e rekomandimeve ose do të ofrojnë një shpjegim të arsyetuar për mosndjekjen e rekomandimeve. Mbikëqyrësi Kryesor ia transmeton këtë informacion menjëherë Bankës së Shqipërisë, si autoritet përgjegjës i subjekteve financiare në fjalë.

2. Mbikëqyrësi Kryesor publikon rastet kur një ofrues kritik i shërbimeve të palëve të treta të TIK-ut nuk njofton Mbikëqyrësin Kryesor në përputhje me pikën 1, ose kur shpjegimi i paraqitur nga ofruesi kritik i shërbimeve të palëve të treta të TIK-ut nuk konsiderohet i mjaftueshëm. Informacioni i publikuar duhet të përmbajë identitetin e ofruesit kritik të shërbimeve të palëve të treta të TIK-ut, si dhe llojin dhe natyrën e mospërputhjes. Informacioni i publikuar duhet të kufizohet vetëm për sa është e nevojshme dhe proporcionale, për të siguruar transparencë publike, përveç rasteve kur një publikim i tillë do të shkaktonte dëme jo proporcionale për palët e përfshira, ose do të rrezikonte seriozisht funksionimin e rregullt dhe integritetin e tregjeve financiare, stabilitetin e pjesshëm ose të plotë të sistemit financiar të Bashkimit Evropian.

Mbikëqyrësi Kryesor njofton ofruesin e shërbimeve të palëve të treta të TIK-ut për publikimin.

3. Banka e Shqipërisë informon subjektet financiare përkatëse për rreziqet e identifikuara në rekomandimet drejtuar ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut, në përputhje me nenin 35(1), shkronja “d”, të Rregullores (BE) 2022/2554. Gjatë administrimit të rrezikut të TIK-ut nga palë të treta, subjektet financiare marrin parasysh rreziqet e referuara në këtë pikë.

4. Kur Banka e Shqipërisë vlerëson se një subjekt financiar nuk ka marrë parasysh ose ka trajtuar në mënyrë të pamjaftueshme rreziqet specifike të identifikuara në rekomandime dhe gjetje, në kuadër të administrimit të rrezikut të TIK-ut nga palë të treta, si dhe në mungesë të dispozitave kontraktuale që adresojnë këto rreziqe, ajo njofton subjektin financiar për mundësinë e marrjes së një vendimi, në përputhje me pikën 6, brenda 60 ditëve kalendarike nga marrja e njoftimit.

5. Pas marrjes së raporteve të parashikuara në nenin 35(1), shkronja “c”, të Rregullores (BE) 2022/2554 dhe para marrjes së një vendimi siç parashikohet në pikën 6 të këtij neni, Banka e Shqipërisë, mbi baza vullnetare, mund të konsultohet me autoritetet e caktuara në përputhje me ligjin “Për sigurinë kibernetike”, si përgjegjëse për mbikëqyrjen e një subjekti thelbësor ose të rëndësishëm sipas përcaktimeve të atij ligji, që është përcaktuar si një ofrues kritik i shërbimeve të palëve të treta të TIK-ut.

6. Banka e Shqipërisë, si masë e fundit, pas njoftimit dhe konsultimit sipas pikave 4 dhe 5 të këtij neni, dhe në përputhje me nenin 50 të Rregullores (BE) 2022/2554, mund të vendosë që subjektet financiare të pezullojnë përkohësisht, pjesërisht ose plotësisht, përdorimin apo vendosjen e një shërbimi të ofruar nga një ofrues kritik i shërbimeve të palëve të treta të TIK-ut, deri në adresimin e rreziqeve të identifikuara në rekomandimet përkatëse. Kur është e nevojshme, Banka e Shqipërisë mund të kërkojë, gjithashtu, zgjidhjen, pjesërisht ose plotësisht, të marrëveshjeve kontraktuale përkatëse me këta ofrues.

7. Kur një ofrues kritik i shërbimeve të palëve të treta të TIK-ut, refuzon të zbatojë rekomandimet e Mbikëqyrësit Kryesor, duke ndjekur një qasje që mund të ketë ndikim negativ mbi një numër të madh subjektesh financiare ose mbi një pjesë të konsiderueshme të sektorit financiar, dhe paralajmërimet individuale të Bankës së Shqipërisë, si autoritet përgjegjës i subjekteve, nuk rezultojnë efektive për zbutjen e rrezikut të mundshëm ndaj stabilitetit financiar, Mbikëqyrësi Kryesor, pas konsultimit me Forumin e Mbikëqyrjes, mund të japë opinione jodetyruese dhe jopublike për Bankën e Shqipërisë, me qëllim promovimin e masave të qëndrueshme dhe konverguese mbikëqyrëse.

8. Pas marrjes së raporteve sipas nenit 35(1), shkronja “c”, të Rregullores (BE) 2022/2554, Banka e Shqipërisë, kur merr një vendim siç parashikohet në pikën 6 të këtij neni, merr në

konsideratë llojin dhe madhësinë e rrezikut që nuk është adresuar nga ofruesi kritik i shërbimeve të palëve të treta të TIK-ut, si dhe seriozitetin e mospërputhjes, duke pasur parasysh kriteret e mëposhtme:

- a) rëndësia dhe kohëzgjatja e mospërputhjes;
- b) nëse mospërputhja ka zbuluar dobësi serioze në procedurat, sistemet e menaxhimit, administrimin e rrezikut dhe kontrollet e brendshme të ofruesit kritik të shërbimeve të palëve të treta të TIK-ut;
- c) nëse mospërputhja ka kontribuar, ka shkaktuar ose ka krijuar lehtësi për kryerjen e një krimi financiar;
- d) nëse mospërputhja ka qenë e qëllimshme ose nga pakujdesia;
- e) nëse pezullimi ose zgjidhja e marrëveshjeve kontraktuale krijon rrezik për vazhdimësinë e veprimtarisë së biznesit të subjektit financiar, pavarësisht përpjekjeve të subjektit financiar për të shmangur ndërprerjet në ofrimin e shërbimeve të tij;
- f) kur është e zbatueshme, opinionin vullnetar të autoriteteve të caktuara në përputhje me ligjin “Për sigurinë kibernetike”, si përgjegjëse për mbikëqyrjen e një subjekti thelbësor ose të rëndësishëm sipas përcaktimeve të atij ligji, që është caktuar si ofrues kritik i shërbimeve të palëve të treta të TIK-ut, siç parashikohet në pikën 5 të këtij neni.

Banka e Shqipërisë i jep subjekteve financiare kohën e nevojshme për të rishikuar marrëveshjet me ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, me qëllim shmangien e efekteve në qëndrueshmërinë e tyre operacionale digjitale dhe duke mundësuar vendosjen e strategjive dalëse (*exit strategies*) dhe planeve të tranzicionit, sipas nenit 45 të kësaj rregulloreje.

9. Vendimi i parashikuar në pikën 6 të këtij neni, u njoftohet anëtarëve të Forumit të Mbikëqyrjes të referuar në nenin 32(4), shkronjat “a”, “b” dhe “c” të Rregullores (BE) 2022/2554, dhe Rrjetit të Përbashkët të Mbikëqyrjes (JON). Ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut që preken nga vendimi bashkëpunojnë plotësisht me subjektet financiare të prekura, për pezullimin ose zgjidhjen e marrëveshjeve kontraktuale.

10. Banka e Shqipërisë informon rregullisht Mbikëqyrësin Kryesor mbi qasjet dhe masat e marra në detyrat e saj mbikëqyrëse, lidhur me subjektet financiare si dhe mbi marrëveshjet kontraktuale të lidhura nga subjektet financiare ku ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, nuk kanë mbështetur pjesërisht ose plotësisht rekomandimet e drejtuara atyre nga Mbikëqyrësi Kryesor.

11. Mbikëqyrësi Kryesor, sipas kërkesës, mund të ofrojë sqarime të mëtejshme mbi rekomandimet e dhëna, për të udhëzuar Bankën e Shqipërisë mbi masat e mëtejshme për ndjekjen e tyre.

Neni 71

Tarifat e mbikëqyrjes

1. Mbikëqyrësi Kryesor, në përputhje me aktin e deleguar të parashikuar në pikën 2 të nenit 43 të Rregullores (BE) 2022/2554, tarifon ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut. Këto tarifa mbulojnë plotësisht shpenzimet e nevojshme të Mbikëqyrësit Kryesor lidhur me kryerjen e detyrave mbikëqyrëse në zbatim të Rregullores (BE) 2022/2554, përfshirë rimbursimin e çdo kostoje që mund të shkaktohet si rezultat i punës së kryer nga ekipi i përbashkët i inspektimit parashikuar në nenin 40 të Rregullores (BE) 2022/2554, si dhe kostot e këshillimeve të ofruara nga ekspertët e pavarur siç parashikohet në nenin 32(4), nënparagrafi

i dytë, të Rregullores (BE) 2022/2554, lidhur me çështjet që bien nën kompetencën e aktiviteteve të drejtpërdrejta të mbikëqyrjes.

2. Shuma e tarifës së ngarkuar ndaj një ofruesi kritik të shërbimeve të palëve të treta të TIK-ut do të mbulojë të gjitha kostot që rrjedhin nga ekzekutimi i detyrave të përcaktuara në seksionin II të kreut V të Rregullores (BE) 2022/2554, si dhe do të jetë proporcionale me xhiron e tij.

NËNKREU II KUADRI I MBIKËQYRJES PËR OFRUESIT KRITIKË TË SHËRBIMEVE TË PALËVE TË TRETA TË TIK-ut NGA BANKA E SHQIPËRISË

Neni 72

Përcaktimi i ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut nga Banka e Shqipërisë

1. Banka e Shqipërisë përcakton ofruesit e shërbimeve të palëve të treta të TIK-ut që konsiderohen kritikë për subjektet financiare, pas një vlerësimi që merr në konsideratë kriteret e përcaktuara në pikën 2 të këtij neni.

2. Përcaktimi i parashikuar në pikën 1 të këtij neni, bazohet në të gjitha kriteret e mëposhtme, në lidhje me shërbimet e TIK-ut të ofruara nga ofruesi i shërbimeve të palëve të treta të TIK-ut:

a) ndikimi sistemik mbi stabilitetin, vazhdimësinë ose cilësinë e ofrimit të shërbimeve financiare, në rast se ofruesi përkatës i shërbimeve të palëve të treta të TIK-ut do të përballej me një dështim operacional në shkallë të gjerë, duke marrë parasysh numrin e subjekteve financiare dhe vlerën totale të aktiveve të subjekteve financiare që përdorin shërbimet e këtij ofruesi;

b) karakteri ose rëndësia sistematike e subjekteve financiare që mbështeten tek ofruesi përkatës i shërbimeve të TIK-ut, e vlerësuar në përputhje me parametrat e mëposhtëm:

i. numri i institucioneve të kreditit me rëndësi sistematike që mbështeten tek ofruesi përkatës i shërbimeve të TIK-ut;

ii. shkalla e ndërvlerësimit midis institucioneve të përmendura në nënpikën “i” dhe subjekteve të tjera financiare;

c) varësia e subjekteve financiare nga shërbimet e ofruara nga ofruesi përkatës i shërbimeve të palëve të treta të TIK-ut, në lidhje me funksione kritike ose të rëndësishme, përfshirë rastet kur këto funksione mbështeten tek i njëjti ofrues i shërbimeve të TIK-ut, pavarësisht nëse kjo varësi është e drejtpërdrejtë apo e tërthortë, nëpërmjet marrëveshjeve të nënkontraktimit;

d) shkalla e zëvendësueshmërisë së ofruesit të shërbimeve të TIK-ut, duke marrë në konsideratë kriteret e mëposhtme:

i. mungesa e alternativave reale, qoftë edhe të pjesshme, për shkak të numrit të kufizuar të ofruesve aktivë në një treg të caktuar, pjesës së tregut që zotëron ofruesi përkatës, ose kompleksitetit teknik apo nivelit të sofistikimit, përfshirë në lidhje me çdo teknologji pronësore, si dhe veçoritë specifike të organizimit apo aktivitetit të ofruesit të shërbimeve të palëve të treta të TIK-ut;

ii. vështirësitë në migrimin pjesor ose të plotë të të dhënave dhe ngarkesave përkatëse nga ofruesi ekzistues te një tjetër, për shkak të kostove financiare të konsiderueshme, kohës ose burimeve të tjera të nevojshme, apo për shkak të rrezikut të shtuar të TIK-ut ose rreziqeve të tjera operationale që mund të lindin gjatë këtij procesi të migrimit.

3. Në rastet kur ofruesi i shërbimeve të palëve të treta të TIK-ut i përket një grupi, kriteret e përmendura në pikën 2 të këtij neni merren në konsideratë në lidhje me shërbimet e TIK-ut të ofruara nga grupi në tërësi.

4. Ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut që janë pjesë e një grupi, caktojnë një person juridik si pikë koordinimi për të siguruar përfaqësimin dhe komunikimin e duhur me Bankën e Shqipërisë.

5. Përcaktimi i përmendur në pikën 1 të këtij neni nuk zbatohet për:

- a) subjektet financiare që ofrojnë shërbime të TIK-ut për subjekte të tjera financiare;
- b) ofruesit e shërbimeve të TIK-ut brenda grupit.

Neni 73

Kompetencat e Bankës së Shqipërisë për mbikëqyrjen e ofruesve kritikë të shërbimeve të palëve të treta të TIK-ut të përcaktuar sipas nenit 72 të kësaj rregulloreje

Në përmbushje të detyrimeve të parashikuara në këtë nënkre, Banka e Shqipërisë ka të drejtë:

a) të kërkojë informacion periodik teknik dhe operacional nga ofruesit kritikë të shërbimeve të palëve të treta të TIK-ut, përfshirë strukturën organizative, planet e reagimit ndaj incidenteve, kontratat e nënkontraktimit dhe zinxhirët e varësisë;

b) të kryejë vlerësime dhe inspektime në vend (*on site*) ose në distance (*off site*), në hapësirat, sistemet dhe dokumentacionin e ofruesve kritikë;

c) të japë rekomandime ose urdhra mbikëqyrës me afate detyruese për zbatim, kur konstatohen mangësi ose rreziqe serioze;

d) të vendosë një mekanizëm formal ndjekjeje të përmbushjes së këtyre rekomandimeve nga ana e ofruesit kritik të shërbimeve të palëve të treta të TIK-ut, duke përfshirë plane masash dhe verifikim progresi;

e) të kërkojë kufizimin ose ndërprerjen e marrëveshjeve me një ofrues kritik të shërbimeve të palëve të treta të TIK-ut, në rast të vazhdimit të shkeljeve, pengimit të mbikëqyrjes ose rrezikimit të qëndrueshmërisë operationale digjitale të sektorit financiar;

f) të kërkojë që ofruesi kritik i shërbimeve të palëve të treta të TIK-ut, me seli jashtë territorit të Republikës së Shqipërisë, të caktojë një përfaqësues ligjor në Shqipëri ose të pranojë shprehimisht juridiksionin e Bankës së Shqipërisë, si kusht për të ofruar shërbime ndaj subjekteve financiare të mbikëqyrura prej saj.

KREU VIII

TË TJERA

Neni 74

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 75

Hyrja në fuqi dhe zbatimi i rregullores

1. Kjo rregullore hyn në fuqi në datë 1 janar 2028.

2. Dispozitat e nenit 2, pikat 3 dhe 4; nenit 30, pikat 13 deri në 15 dhe pikat 17 deri në 19; nenit 38, pika 2; neneve 60 deri në 64 dhe neneve 66 deri në 71 të kësaj rregulloreje, nuk zbatohen dhe nuk prodhojnë efekte juridike deri në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian. Duke filluar nga kjo datë, këto dispozita zbatohen nëpërmjet rregullores (BE) 2022/2554 të Parlamentit Evropian dhe e Këshillit “Për qëndrueshmërinë operationale digjitale të sektorit financiar”.

3. Subjektet e rregullores, deri në datën 1 janar 2028, marrin masa për plotësimin e kërkesave të rregullores dhe raportojnë në Bankën e Shqipërisë çdo 3 muaj për këto masa të marra prej tyre, duke filluar nga data 1 janar 2027.

4. Kjo rregullore do të qëndrojë në fuqi deri në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian.

Neni 76 Shfuqizime

Me hyrjen në fuqi të kësaj rregulloreje, shfuqizohet udhëzimi “Për raportimin e incidenteve madhore”, miratuar me vendimin nr. 10, datë 7.2.2024, të Këshillit Mbikëqyrës të Bankës së Shqipërisë.

Neni 77 Nxjerrja e standardeve rregullatore teknike për plotësimin e kuadrit të qëndrueshmërisë operacionale digjitale

Banka e Shqipërisë, me qëllim plotësimin e mëtejshëm të kuadrit për qëndrueshmërinë operacionale digjitale, nxjerr standarde rregullatore teknike në plotësim të kërkesave të kësaj rregulloreje.

Neni 78 Dispozitë e fundit

Anekset bashkëlidhur kësaj rregulloreje janë pjesë përbërëse e saj.

KRYETARI I KËSHILLIT MBIKËQYRËS
Gent Sejko

ANEKSI 1 FORMULARËT E RAPORTIMIT TË INCIDENTEVE MADHORE

Numri i fushës	Fusha e të dhënave	
Informacion i përgjithshëm mbi subjektin financiar		
1.1	Lloji i raportimit	
1.2	Emri i subjektit raportues	
1.3	Kodi i identifikimit të subjektit raportues	
1.4	Lloji i subjektit financiar të prekur nga incidenti	
1.5	Emri i subjektit financiar të prekur nga incidenti	
1.6	Kodi NUIS/LEI i subjektit financiar të prekur nga incidenti	
1.7	Emri i personit kryesor të kontaktit	
1.8	Posta elektronike e personit kryesor të kontaktit	
1.9	Numri i telefonit të personit kryesor të kontaktit	
1.10	Emri i personit dytësor të kontaktit	
1.11	Posta elektronike e personit dytësor të kontaktit	
1.12	Numri i telefonit të personit dytësor të kontaktit	
1.13	Emri i shoqërisë mëmë	
1.14	Kodi NUIS/LEI i shoqërisë mëmë	
1.15	Monedha raportuese	
Përmbajtja e njoftimit fillestar mbi incidentin madhor të lidhur me TIK-un		
2.1	Kodi i referencës së incidentit, i caktuar nga subjekti financiar	
2.2	Data dhe ora e zbulimit të incidentit madhor të lidhur me TIK-un	
2.3	Data dhe ora e klasifikimit të incidentit të lidhur me TIK-un si madhor	
2.4	Përshkrimi i incidentit madhor të lidhur me TIK-un	

2.5	Kriteri i klasifikimit që shkaktoi raportimin e incidentit	
2.6	Kufijtë e materialitetit për kriterin e klasifikimit “Shtrirja gjeografike”	
2.7	Zbulimi i incidentit madhor të lidhur me TIK	
2.8	Informacion nëse incidenti madhor i lidhur me TIK-un e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër financiar	
2.9	Aktivizimi i planit të vazhdimësisë së biznesit, nëse aktivizohet	
2.10	Informacione të tjera në lidhje me incidentin	
Përmbajtja e raportit të ndërmjetëm		
3.1	Kodi i referencës së incidentit i caktuar nga Banka e Shqipërisë	
3.2	Data dhe ora e ndodhjes së incidentit madhor të lidhur me TIK-un	
3.3	Data dhe ora kur shërbimet, aktivitetet ose operacionet u rikuperuan nga subjekti	
3.4	Numri i klientëve të prekur nga incidenti	
3.5	Përqindja e klientëve të prekur nga incidenti	
3.6	Numri i kundërpasive financiare të prekura nga incidenti	
3.7	Përqindja e kundërpasive financiare të prekura nga incidenti	
3.8	Ndikimi në klientët ose kundërpasitë financiare përkatëse	
3.9	Numri i transaksioneve të prekura nga incidenti	
3.10	Përqindja e transaksioneve të prekura nga incidenti	
3.11	Vlera e transaksioneve të prekura nga incidenti	
3.12	Informacion nëse vlerat janë reale, vlerësime, apo nëse nuk ka pasur ende ndonjë ndikim	
3.13	Ndikimi reputacional	
3.14	Informacion kontekstual mbi ndikimin reputacional	
3.15	Kohëzgjatja e incidentit madhor të lidhur me TIK-un	
3.16	Kohëzgjatja e ndërprerjes së shërbimeve	
3.17	Informacion nëse të dhënat për kohëzgjatjen e incidentit dhe kohëzgjatjen e ndërprerjes së shërbimeve janë reale apo vlerësime	
3.18	Llojet e ndikimit në shtete të tjera	
3.19	Përshkrim se si incidenti madhor i lidhur me TIK-un ka ndikim në shtete të tjera	
3.20	Kufiri i materialitetit për kriterin “Humbjet e të dhënave”	
3.21	Përshkrim i humbjes së të dhënave	
3.22	Kriteret e klasifikimit për “Shërbimet kritike të prekura”	
3.23	Llojet e incidenteve madhore të lidhura me TIK-un	
3.24	Lloje të tjera incidentesh	
3.25	Kërcënimet dhe teknikat e përdorura nga aktorët e kërcënimeve	
3.26	Lloje të tjera teknikash	
3.27	Informacion rreth zonave funksionale dhe proceseve të biznesit të prekura	
3.28	Komponentët e infrastrukturës së prekur që mbështesin proceset e biznesit	
3.29	Informacion mbi komponentët e infrastrukturës së prekur që mbështesin proceset e biznesit	
3.30	Ndikimi në interesat financiarë të klientëve	
3.31	Raportimi tek autoritete të tjera	
3.32	Specifikimi i autoriteteve “të tjera”	
3.33	Veprime/masa të përkohshme të ndërmarra apo të planifikuara për t’u ndërmarrë, për rikuperim nga incidenti	
3.34	Përshkrim i veprimeve/masave të përkohshme të ndërmarra apo të planifikuara për t’u ndërmarrë, për rikuperim nga incidenti	
3.35	Treguesit e kompromentimit	
Përmbajtja e raportit përfundimtar		
4.1	Klasifikimi në nivel të lartë i shkaqeve bazë të incidentit	
4.2	Klasifikim i detajuar i shkaqeve bazë të incidentit	
4.3	Klasifikim shtesë mbi shkaqet bazë të incidentit	
4.4	Lloje të tjera të shkaqeve bazë	
4.5	Informacione mbi shkaqet bazë të incidentit	
4.6	Përmbledhje e zgjidhjes së incidentit	
4.7	Data dhe ora kur shkaku bazë i incidentit u adresua	
4.8	Data dhe ora kur incidenti u zgjidh	
4.9	Informacion nëse data e zgjidhjes përfundimtare të incidentit ndryshon nga data fillestare e planifikuar për implementim	
4.10	Vlerësimi i rrezikut në funksionet me rëndësi kritike për qëllime të ndërhyrjes së jashtëzakonshme	
4.11	Informacion i vlefshëm për autoritetin e ndërhyrjes së jashtëzakonshme	
4.12	Kufijtë e materialitetit për klasifikimin e kriterit “Ndikimi ekonomik”	
4.13	Shuma e humbjeve dhe kostove bruto direkte dhe indirekte	

4.14	Shuma e rikuperuar	
4.15	Informacion nëse incidentet madhore kanë qenë të përsëritura	
4.16	Data dhe ora e ndodhjes së incidenteve të përsëritura	

ANEKSI 2

UDHËZIME MBI PLOTËSIMIN E FORMULARËVE TË RAPORTIMIT TË INCIDENTEVE MADHORE

Fusha e të dhënave	Përshkrimi	I detyrueshë m për njoftimin fillestar?	I detyrueshë m për raportimin e ndërmjetëm?	I detyrueshëm për raportimin përfundimtar ?	Lloji i fushës
Informacion i përgjithshëm mbi subjektin financiar					
1.1 Lloji i raportimit	Tregoni llojin e njoftimit ose raportit të incidentit që po dorëzohet te Banka e Shqipërisë.	Po	Po	Po	Opsione: - Njoftim fillestar; - Raport i ndërmjetëm; - Raport përfundimtar; - Incident madhor i riklasifikuar si jomadhor
1.2 Emri i subjektit raportues	Emri i plotë ligjor i subjektit raportues.	Po	Po	Po	Alfanumerik
1.3 Kodi i identifikimit të subjektit raportues	Kodi identifikimit të subjektit raportues Nëse njoftimin/raportimin e bën subjekti financiar, kodi i identifikimit duhet të jetë NUIS ose Identifikuesi Ligjor i Subjektit (LEI), i cili është një kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020. Një ofrues i shërbimeve të palëve të treta që raporton për një subjekt financiar, mund të përdorë një kod identifikimi të specifikuar sipas standardeve teknike të parashikuara në kuadrin nënligjor të Bankës së Shqipërisë, për regjistrin e informacionit në lidhje me marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut, të parashikuara në nenin 45 të kësaj rregulloreje.	Po	Po	Po	Alfanumerik
1.4 Lloji i subjektit financiar të prekur nga incidenti	Lloji i subjektit të parashikuar në pikën 1 të nenit 2 të kësaj rregulloreje, për të cilin paraqitet raportimi. Në rastet e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, duhet të përzgjidhen të gjitha llojet e subjekteve financiare të mbuluara nga raportimi i agreguar.	Po	Po	Po	Opsionet (mund të zgjidhen disa opsione): - institucionet e kreditit; - institucionet e pagesave; - institucionet e pagesave që përjashtohen sipas ligjit “Për shërbimet e pagesave”; - ofruesit e shërbimit të informimit të llogarisë; - institucionet e parasë elektronike; - institucionet e parasë elektronike që përjashtohen sipas ligjit “Për shërbimet e pagesave”; - emetuesit e tokenave të aseteve dhe emetuesit e tokenave të parasë elektronike.
1.5 Emri i subjektit financiar të prekur nga incidenti	Emri i plotë ligjor i subjektit financiar të prekur nga incidenti madhor i lidhur me TIK-un dhe që kërkohet të raportojë incidentin madhor te Banka e Shqipërisë, sipas nenit 30 të kësaj rregulloreje.	Po, nëse subjekti financiar i prekur nga incidenti është i	Po, nëse subjekti financiar i prekur nga incidenti është i	Po, nëse subjekti financiar i prekur nga incidenti është i	Alfanumerik

	Në rast të raportimit të agreguar: a) një listë të të gjithë emrave të subjekteve financiare të prekur nga incidentet madhore të lidhur me TIK-un, duke i ndarë me pikëpresje; b) ofruesin e shërbimeve të palëve të treta që njofton ose raporton për një incident madhor në mënyrë të agreguar, sipas nenit 38 të kësaj rregulloreje, duke listuar emrat e subjekteve financiare të prekura nga incidenti (të ndara me pikëpresje).	ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	nga subjekti që raporton dhe në rast të një raportimi të agreguar	
1.6 Kodi NUIS/LEI i subjektit financiar të prekur nga incidenti	Kodi NUIS ose Identifikuesi Ligjor i Subjektit (LEI) të prekur nga incidenti madhor i lidhur me TIK-un, i caktuar në përputhje me Organizatën Ndërkombëtare të Standardizimit. Në rastin e raportimeve të agreguara: a) një listë me të gjitha kodet NUIS/LEI të subjekteve financiare të prekura nga incidentet madhore të lidhur me TIK-un, të ndara me pikëpresje; b) ofruesi i shërbimeve të palëve të treta që njofton ose raporton për një incident madhor në mënyrë të agreguar, sipas nenit 38 të kësaj rregulloreje, duke listuar emrat e subjekteve financiare të prekura nga incidenti (të ndara me pikëpresje). Renditja e kodeve dhe emrave të subjekteve financiare duhet të jetë e njëjtë.	Po, nëse subjekti financiar i prekur nga incidenti madhor është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Po, nëse subjekti financiar i prekur nga incidenti madhor është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Po, nëse subjekti financiar i prekur nga incidenti madhor është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020.
1.7 Emri i personit kryesor të kontaktit	Emri dhe mbiemri i personit kryesor të kontaktit të subjektit financiar. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, emri i personit kryesor të kontaktit që paraqet raportimin e agreguar.	Po	Po	Po	Alfanumerik
1.8 Adresa e postës elektronike të personit kryesor të kontaktit	Adresa e postës elektronike të personit kryesor të kontaktit që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, adresa e postës elektronike të personit kryesor të kontaktit që paraqet raportimin e agreguar.	Po	Po	Po	Alfanumerik
1.9 Numri i telefonit të personit kryesor të kontaktit	Numri i telefonit të personit kryesor të kontaktit që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, numri i telefonit të personit kryesor të kontaktit që paraqet raportimin e agreguar. Numri i telefonit që raportohet duhet të jetë i formatit si p.sh. +3556XXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).	Po	Po	Po	Alfanumerik
1.10 Emri i personit dytësor të kontaktit	Emri dhe mbiemri i personit dytësor të kontaktit, ose emri i grupit përgjegjës të subjektit financiar, ose subjektit që paraqet raportin në emër të subjektit financiar.	Po	Po	Po	Alfanumerik
1.11 Adresa e postës elektronike të personit dytësor të kontaktit	Adresa e postës elektronike të personit dytësor të kontaktit ose një adresë funksionale e grupit përgjegjës, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin.	Po	Po	Po	Alfanumerik
1.12 Numri i	Numri i telefonit të personit dytësor të	Po	Po	Po	Alfanumerik

telefonit të personit dytësor të kontaktit	kontaktit ose grupit përgjegjës, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin. Numri i telefonit që raportohet duhet të jetë i formatit si p.sh. +3556XXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).				
1.13 Emri i shoqërisë mëmë	Emri i shoqërisë mëmë fundore të grupit, të cilit i përket subjekti financiar i prekur nga incidenti, nëse është e aplikueshme.	Po, nëse subjekti financiar i përket një grupi	Po, nëse subjekti financiar i përket një grupi	Po, nëse subjekti financiar i përket një grupi	Alfanumerik
1.14 Kodi NUIS/LEI i shoqërisë mëmë	Kodi NUIS ose LEI i shoqërisë mëmë fundore të grupit, të cilit i përket subjekti financiar i prekur nga incidenti, nëse është e aplikueshme. Kodi caktohet në përputhje me Organizatën Ndërkombëtare të Standardizimit.	Po, nëse subjekti financiar i përket një grupi	Po, nëse subjekti financiar i përket një grupi	Po, nëse subjekti financiar i përket një grupi	Kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020.
1.15 Monedha raportuese	Monedha e përdorur për raportimin e incidentit.	Po	Po	Po	Opsionet plotësohen duke përdorur kodet e monedhave ISO 4217.
Përmbajtja e njoftimit fillestar mbi incidentin madhor të lidhur me TIK					
2.1 Kodi i referencës së incidentit, i caktuar nga subjekti financiar	Kodi unik i referencës i caktuar nga subjekti financiar, për të identifikuar incidentet madhore të lidhur me TIK-un. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, kodi i referencës së incidentit, i caktuar ofruesi i shërbimeve të palëve të treta.	Po	Po	Po	Alfanumerik
2.2. Data dhe ora e zbulimit të incidentit madhor të lidhur me TIK	Data dhe ora kur subjekti financiar vihet në dijeni të incidentit të lidhur me TIK-un. Në rastet e incidenteve të përsëritura, data dhe ora kur u zbulua incidenti më i fundit i lidhur me TIK-un.	Po	Po	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat: sekondat)
2.3 Data dhe ora e klasifikimit të incidentit të lidhur me TIK-un si madhor	Data dhe ora kur incidenti i lidhur me TIK-un u klasifikua si incident madhor, sipas kriterëve të klasifikimit të parashikuara në këtë rregullore.	Po	Po	Po	Alfanumerik
2.4 Përshkrimi i incidentit madhor të lidhur me TIK	Përshkrimi i aspekteve më relevante të incidentit madhor të lidhur me TIK-un. Subjektet financiare duhet të ofrojnë një përmbledhje të nivelit të lartë të informacionit të mëposhtëm, si për shembull mbi shkaqet e mundshme, ndikimet e menjëhershme, sistemet e prekura dhe të tjera. Subjektet financiare duhet të përfshijnë, kur dihet ose pritet në mënyrë të arsyeshme që incidenti të ndikojë tek ofruesit e shërbimeve të palëve të treta ose te subjektet e tjera financiare, llojin e ofruesit ose subjektit financiar, emrin e tyre, kodet e tyre përkatëse të identifikimit dhe llojin e kodit të identifikimit (p.sh. LEI ose NUIS). Në raportet pasuese, përmbajtja e fushës mund të ndryshojë me kalimin e kohës për të pasqyruar të kuptuarin e vazhdueshëm të incidentit të lidhur me TIK-un dhe për të përshkruar çdo informacion tjetër relevant në lidhje me incidentin e lidhur me TIK-un, që nuk është përfshirë në fushat e të dhënave, duke përfshirë vlerësimin e brendshëm të ashpërsisë nga subjekti financiar (p.sh. shumë e ulët, e ulët, mesatare, e lartë, shumë e lartë) dhe një tregues të nivelit dhe emrit të	Po	Po	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat: sekondat)

	strukturave më të larta vendimmarrëse, që janë përfshirë në përgjigje të incidentit të lidhur me TIK-un.				
2.5 Kriteri i klasifikimit që shkaktoi raportimin e incidentit	Kriteret e klasifikimit sipas kësaj rregulloreje, që kanë përcaktuar incidentin e lidhur me TIK-un si madhor dhe kanë shkaktuar më pas njoftimin dhe raportimin. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, kriteret e klasifikimit që kanë përcaktuar incidentin e lidhur me TIK-un si madhor, për të paktën një ose më shumë subjekte financiare.	Po	Po	Po	Zgjedhje (e shumëfishtë): - klientët, kundërpартitë financiare dhe transaksionet e prekura; - ndikimi reputacional; - kohëzgjatja e incidentit dhe kohëzgjatja e ndërprerjes së shërbimeve; - shtrirja gjeografike; - humbja e të dhënave; - shërbimet kritike të prekura; - ndikimi ekonomik.
2.6 Kufijtë e materialitetit për kriterin e klasifikimit “Shtrirja gjeografike”	Shtetet e tjera të prekura nga incidenti madhor i lidhur me TIK-un. Kur vlerësojnë ndikimin e incidentit madhor në shtete të tjera, subjektet financiare duhet të marrin në konsideratë nenin 23 të kësaj rregulloreje.	Po, nëse është arritur kufiri i shtrirjes gjeografike	Po, nëse është arritur kufiri i shtrirjes gjeografike	Po, nëse është arritur kufiri i shtrirjes gjeografike	Zgjedhje e shumëfishtë duke përdorur ISO 3166 ALPHA -2 për shtetet e prekura.
2.7 Zbulimi i incidentit madhor të lidhur me TIK	Tregohet se si u zbulua incidenti madhor i lidhur me TIK-un.	Po	Po	Po	Opsione: - siguria e teknologjisë së informacionit; - stafi; - auditi i brendshëm; - auditi i jashtëm; - klientët; - kundërpартitë financiare; - ofruesit e shërbimeve të palëve të treta; - sulmuesit; - sistemet e monitorimit; - autoritetet/agjencitë/ organet ligjzbatuese; - të tjera.
2.8 Informacion nëse incidenti madhor i lidhur me TIK-un e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër financiar	Tregues nëse incidenti madhor i lidhur me TIK-un e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër. Subjektet financiare duhet të tregojnë nëse incidentet madhore të lidhur me TIK-un e kanë origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër (duke përfshirë subjektet që i përkasin të njëjtit grup të subjektit raportues), si dhe emrin, kodin e identifikimit të ofruesit të shërbimit të palëve të treta ose subjektit financiar dhe llojin e kodit të identifikimit (p.sh. LEI apo NUIS).	Po, nëse incidenti e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër financiar	Po, nëse incidenti e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër financiar	Po, nëse incidenti e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër financiar	Alfanumerik
2.9 Aktivizimi i planit të vazhdimësisë së biznesit, nëse aktivizohet	Tregues nëse ka pasur një aktivizim formal të planit të vazhdimësisë së biznesit nga subjekti financiar.	Po	Po	Po	Po/ Jo
2.10 Informacione të tjera në lidhje me incidentin	Informacione të tjera jo të përfshira në këtë formular. Subjektet financiare që kanë riklasifikuar një incident madhor të lidhur me TIK-un, si incident jomadhор, duhet të përshkruajnë arsyet përse ky incident nuk i përmbush dhe nuk pritet më t'i përmbushë kriteret për t'u klasifikuar si një incident madhor i lidhur me TIK-un.	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK-un është riklasifikuar si incident	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK-un është riklasifikuar si incident jomadhор.	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK-un është riklasifikuar si incident jomadhор.	Alfanumerike

		jomadhlor.			
Përmbajtja e raportit të ndërmjetëm					
3.1 Kodi i referencës së incidentit i caktuar nga Banka e Shqipërisë	Kodi i referencës së incidentit i caktuar nga Banka e Shqipërisë, në kohën kur është marrë njoftimi fillestar, për të identifikuar në mënyrë të pangatërrueshme incidentin madhor të lidhur me TIK-un.	Jo	Po, nëse aplikohet	Po, nëse aplikohet	Alfanumerik
3.2 Data dhe ora e ndodhjes së incidentit madhor të lidhur me TIK	Data dhe ora kur ka ndodhur incidenti madhor i lidhur me TIK-un, nëse është e ndryshme nga ora kur subjekti financiar është vënë në dijeni të incidentit. Në rastet e incidenteve të përsëritura, data dhe ora kur u zbulua incidenti më i fundit i lidhur me TIK-un.	Jo	Po	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
3.3 Data dhe ora kur shërbimet, aktivitetet ose operacionet u rikuperuan nga subjekti	Informacion mbi datën dhe orën e rikuperimit të shërbimeve, aktiviteteve apo operacioneve të prekura nga incidenti madhor i lidhur me TIK-un.	Jo	Po, nëse është plotësuar fusha 3.16 “Kohëzgjatja e ndërprerjes së shërbimeve”	Po, nëse është plotësuar fusha 3.16 “Kohëzgjatja e ndërprerjes së shërbimeve”	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
3.4 Numri i klientëve të prekur nga incidenti	Numri i klientëve të prekur nga incidenti madhor i lidhur me TIK-un që përdorin shërbimin e ofruar nga subjekti financiar Kur vlerësojnë numrin e klientëve të prekur, subjektet financiare duhet të kenë parasysh nenin 20, pika 1, dhe nenin 28, pika 1, shkronja “b”, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë numrin real të klientëve të prekur, duhet të përdorë vlerësimet bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, numri total i klientëve të prekur në të gjitha subjektet financiare.	Jo	Po	Po	Numër i plotë
3.5 Përqindja e klientëve të prekur nga incidenti	Përqindja e klientëve të prekur nga incidenti madhor i lidhur me TIK-un, në raport me numrin total të klientëve që përdorin shërbimin e prekur nga incidenti, të ofruar nga subjekti financiar. Në rastet kur incidenti ka prekur më shumë se një shërbim, shërbimet do të paraqiten në mënyrë të përmbledhur. Gjatë vlerësimit, subjektet financiare duhet të kenë parasysh nenin 20, pika 1, dhe nenin 28, pika 1, shkronja “a”, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë përqindjen reale të klientëve të prekur, duhet të përdorë vlerësimet bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, një subjekt financiar duhet të pjesëtojë numrin total të të gjithë klientëve të prekur nga incidenti, me numrin e përgjithshëm të klientëve të të gjitha subjekteve financiare.	Jo	Po	Po	Shprehur si përqindje – çdo vlerë deri në 5 karaktere numerike, deri në 1 shifër dhjetore, e shprehur si përqindje (p.sh. 2,4 në vend të 2,4 %). Nëse vlera ka më shumë se 1 shifër pas presjes dhjetore, subjektet raportuese do ta rrumbullakosin në vlerën gjysmë lart.
3.6 Numri i kundërpative financiare të prekura nga incidenti	Numri i kundërpative financiare të prekura nga incidenti madhor i lidhur me TIK-un, që kanë një kontratë me subjektin financiar. Kur vlerësojnë kundërpative	Jo	Po	Po	Numër i plotë

	financiare të prekura nga incidenti, subjektet financiare duhet të kenë parasysh nenin 20, pika 2, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë numrin real të kundërpartive financiare të prekura nga incidenti, duhet të përdorë vlerësimet, bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, numri total i kundërpartive financiare të prekura nga incidenti, në të gjitha subjektet financiare.				
3.7 Përqindja e kundërpartive financiare të prekura nga incidenti	Përqindja e kundërpartive financiare të prekura nga incidenti madhor i lidhur me TIK-un, në raport me numrin total të kundërpartive financiare që kanë një kontratë me subjektin financiar. Gjatë vlerësimit të përqindjes së kundërpartive financiare të prekura nga incidenti madhor i lidhur me TIK-un, subjektet financiare duhet të kenë parasysh nenin 20, pika 1, dhe nenin 28, pika 1, shkronja “c”, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë përqindjen reale të kundërpartive financiare të prekura nga incidenti, duhet të përdorë vlerësimet, bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, një subjekt financiar duhet të pjesëtojë numrin total të të gjitha kundërpartive financiare të prekura nga incidenti, me numrin e përgjithshëm të kundërpartive financiare të të gjitha subjekteve financiare.	Jo	Po	Po	Shprehur si përqindje – çdo vlerë deri në 5 karaktere numerike, deri në 1 shifër dhjetore, e shprehur si përqindje (p.sh. 2,4 në vend të 2,4 %). Nëse vlera ka më shumë se 1 shifër pas presjes dhjetore, subjektet raportuese do ta rrumbullakosin në vlerën gjysmë lart.
3.8 Ndikimi në klientët ose kundërpartitë financiare përkatëse	Çdo ndikim të klientët ose kundërpartitë financiare, siç referohet në nenin 20, pika 3, dhe nenin 28, pika 1, shkronja “f”, të kësaj rregulloreje.	Jo	Po, nëse është arritur kufiri i treguesit “Rëndësia e klientëve dhe kundërpartive financiare”	Po, nëse është arritur kufiri i treguesit “Rëndësia e klientëve dhe kundërpartive financiare”	Po/Jo
3.9 Numri i transaksioneve të prekura nga incidenti	Numri i transaksioneve të prekura nga incidenti madhor i lidhur me TIK-un. Kur vlerësohet ndikimi në transaksione, subjektet financiare duhet të marrin parasysh nenin 20, pika 4, të kësaj rregulloreje, duke përfshirë të gjitha transaksionet e prekura vendase ose ndërkuftare, që përfshijnë një shumë monetare, ku të paktën një pjesë e transaksionit kryhet në Shqipëri. Një subjekt financiar që nuk mund të përcaktojë numrin real të transaksioneve të prekura nga incidenti, duhet të përdorë vlerësimet, bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, një subjekt financiar duhet të paraqesë	Jo	Po, nëse transaksionet janë prekur nga incidenti	Po, nëse transaksionet janë prekur nga incidenti	Numër i plotë

	numrin total të të gjitha transaksioneve të prekura nga incidenti, në të gjitha subjektet financiare.				
3.10 Përqindja e transaksioneve të prekura nga incidenti	Përqindja e transaksioneve të prekura në raport me numrin mesatar ditor të transaksioneve vendase dhe ndërkufitare të kryera nga subjekti financiar në lidhje me shërbimin e prekur. Subjektet financiare duhet të marrin parasysh kërkesat e nenit 20, pika 4, dhe nenit 28, pika 1, shkronja “d”, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë përqindjen reale të transaksioneve të prekura nga incidenti, duhet të përdorë vlerësimet. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, një subjekt financiar duhet të pjesëtojë numrin total të të gjitha transaksioneve të prekura nga incidenti, me numrin total të transaksioneve të të gjitha subjekteve financiare të prekura.	Jo	Po, nëse transaksione t janë prekur nga incidenti	Po, nëse transaksionet janë prekur nga incidenti	Shprehur si përqindje – çdo vlerë deri në 5 karaktere numerike, deri në 1 shifër dhjetore, e shprehur si përqindje (p.sh. 2,4 në vend të 2,4 %). Nëse vlera ka më shumë se 1 shifër pas presjes dhjetore, subjektet raportuese do ta rrumbullakosin në vlerën gjysmë lart.
3.11 Vlera e transaksioneve të prekura nga incidenti	Vlera totale e transaksioneve të prekura nga incidenti madhor i lidhur me TIK-un vlerësohet në përputhje me nenin 20, pika 4, dhe nenin 28, pika 1, shkronja “e”, të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë vlerën reale të transaksioneve të prekura nga incidenti, duhet të përdorë vlerësimet, bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference. Një subjekt financiar raporton shumën monetare si vlerë pozitive. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, një subjekt financiar duhet të paraqesë vlerën totale të transaksioneve të prekura nga incidenti, në të gjitha subjektet financiare.	Jo	Po, nëse transaksione t janë prekur nga incidenti	Po, nëse transaksionet janë prekur nga incidenti	Monetare Subjektet financiare duhet të raportojnë shifrat në mijë njësi (p.sh. 2,5 në vend të 2 500).
3.12 Informacion nëse vlerat janë reale, vlerësime, apo nëse nuk ka pasur ende ndonjë ndikim	Informacion nëse vlerat e raportuara në fushat e të dhënave 3.4 deri në 3.11 janë reale ose vlerësime, ose nëse nuk ka pasur ende ndonjë ndikim.	Jo	Po	Po	Zgjedhje e shumëfishtë: - Shifra reale për klientët e prekur nga incidenti; - Shifra reale për kundërpartitë financiare të prekura nga incidenti; - Shifra reale për transaksionet e prekura nga incidenti; - Vlerësime për klientët e prekur nga incidenti; - Vlerësime për kundërpartitë financiare të prekura nga incidenti; - Vlerësime për transaksionet e prekura nga incidenti; - Pa ndikim te klientët; - Pa ndikim te kundërpartitë financiare; - Pa ndikim te transaksionet.
3.13 Ndikimi reputacional	Informacion në lidhje me ndikimin reputacional që rezulton nga incidenti madhor i lidhur me TIK-un, siç parashikohet në nenin 21 dhe nenin 29 të kësaj rregulloreje.	Jo	Po, nëse plotësohet kriteri “Ndikimi reputacional	Po, nëse plotësohet kriteri “Ndikimi reputacional”	Zgjedhje e shumëfishtë: - incidenti madhor i lidhur me TIK-un është pasqyruar në media; - incidenti madhor i lidhur

	Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, kategoritë e ndikimit reputacional që zbatohen për të paktën një subjekt financiar.		”		me TIK-un ka rezultuar në ankesa të përsëritura nga klientët të ndryshëm ose kundërpartitë financiare, për shërbimet që përballen me klientët ose marrëdhëniet kritike të biznesit; - subjekti financiar nuk do të jetë në gjendje ose ka të ngjarë të mos jetë në gjendje të përmbushë kërkesat rregullatore si rezultat i incidentit madhor të lidhur me TIK-un; - subjekti financiar do të humbasë ose ka të ngjarë të humbasë klientët ose kundërpartitë financiare, me një ndikim material në biznesin e tij, si rezultat i incidentit madhor të lidhur me TIK-un.
3.14 Informacion kontekstual mbi ndikimin reputacional	Informacion që përshkruan se si incidenti madhor i lidhur me TIK-un ka ndikuar ose mund të ndikojë në reputacionin e subjektit financiar, duke përfshirë shkeljet e ligjit, mospërmbushjen e kërkesave rregullative, numrin e ankesave të klientëve dhe të tjera. Informacioni duhet të përfshijë llojin e mediave (p.sh. media tradicionale dhe digjitale, bloget, platforma transmetimi) dhe mbulimin mediatik, duke përfshirë shtrirjen e mediave (lokale, kombëtare, ndërkombëtare). Mbulimi mediatik në këtë kontekst nuk nënkupton vetëm disa komente negative nga ndjekësit ose përdoruesit e rrjeteve sociale. Subjekti financiar, gjithashtu, do të tregojë nëse mbulimi mediatik nxori në pah rreziqe të rëndësishme për klientët e tij në lidhje me incidentin madhor të lidhur me TIK-un, duke përfshirë rrezikun e falimentimit të subjektit financiar ose rrezikun e humbjes së fondeve. Subjektet financiare, gjithashtu, tregojnë nëse kanë dhënë informacion për mediat që kanë shërbyer për të informuar në mënyrë të besueshme publikun për incidentit madhor të lidhur me TIK-un dhe pasojat e tij. Subjektet financiare, gjithashtu, mund të tregojnë nëse ka pasur informacion të rremë në media në lidhje me incidentin e lidhur me TIK-un, duke përfshirë informacione të bazuara në disinformimit të qëllimshëm të përhapur nga aktorët e kërcënimit, ose informacione në lidhje me ose ilustrimin e shpërfytyrimit të faqes së internetit të subjektit financiar.	Jo	Po, nëse plotësohet kriteri “Ndikimi reputacional”	Po, nëse plotësohet kriteri “Ndikimi reputacional”	Alfanumerik
3.15 Kohëzgjatja e incidentit madhor të lidhur me TIK	Subjektet financiare do të matin kohëzgjatjen e incidentit madhor të lidhur me TIK-un, nga momenti kur ndodhi incidenti, deri në momentin e zgjidhjes së tij. Subjektet financiare që nuk janë në gjendje të përcaktojnë momentin kur ka ndodhur incidenti madhor i lidhur me TIK-un, do të matin kohëzgjatjen e incidentit duke filluar nga momenti më	Jo	Po	Po	Ditë: Orë: Minuta

	i hershëm midis kohës së zbulimit të incidentit dhe kohës kur subjekti financiar e regjistroi incidentin në regjistrat e rrjetit ose sistemit ose burime të tjera të të dhënave. Subjektet financiare që nuk e dinë ende momentin kur do të zgjidhet incidenti madhor i lidhur me TIK-un, duhet të aplikojnë vlerësime. Vlera do të shprehet në ditë, orë dhe minuta. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, subjektet financiare matin kohëzgjatjen më të gjatë të incidentit madhor të lidhur me TIK-un, në rast të diferencave në kohëzgjatjen e incidentit midis subjekteve të ndryshme financiare.				
3.16 Kohëzgjatja e ndërprerjes së shërbimeve	Kohëzgjatja e ndërprerjes së shërbimeve e matur nga momenti kur shërbimi është plotësisht ose pjesërisht i padisponueshëm për klientët, kundërpартitë financiare ose përdoruesit e tjerë të brendshëm ose të jashtëm, deri në momentin kur aktivitetet ose operacionet e rregullta janë rikthyer në nivelin e shërbimit që ofrohej para ndodhjes së incidentit madhor të lidhur me TIK-un. Kur ndërprerja e shërbimeve shkakton një vonesë në ofrimin e shërbimit pas rikuperimit të aktiviteteve ose operacioneve të rregullta, subjektet financiare do të matin kohën e ndërprerjes së shërbimeve që nga fillimi i incidentit madhor të lidhur me TIK-un, deri në momentin kur fillon të ofrohet ai shërbim i vonuar. Subjektet financiare që nuk janë në gjendje të përcaktojnë momentin kur ka filluar ndërprerja e shërbimit, do të matin kohën e ndërprerjes së shërbimit që nga momenti më i hershëm midis zbulimit të incidentit dhe momentit kur incidenti është regjistruar. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, subjektet financiare matin kohëzgjatjen më të gjatë të incidentit madhor të lidhur me TIK-un, në rast të diferencave në kohëzgjatjen e incidentit midis subjekteve të ndryshme financiare.	Jo	Po, nëse incidenti ka shkaktuar një ndërprerje të shërbimeve	Po, nëse incidenti ka shkaktuar një ndërprerje të shërbimeve	Ditë: Orë: Minuta
3.17 Informacion nëse të dhënat për kohëzgjatjen e incidentit dhe kohëzgjatjen e ndërprerjes së shërbimeve janë reale apo vlerësime	Informacion nëse vlerat e raportuara në fushat e të dhënave 3.15 dhe 3.16 janë reale apo vlerësime.	Jo	Po, nëse plotësohet kriteri “Kohëzgjatja dhe kohëzgjatja e ndërprerjes së shërbimeve”	Po, nëse plotësohet kriteri “Kohëzgjatja dhe kohëzgjatja e ndërprerjes së shërbimeve”	Opsionet: - Shifra reale; - Vlerësime; - Shifra reale dhe vlerësime; - Nuk ka informacion në dispozicion.
3.18 Llojet e ndikimit në shtete të tjera	Lloji i ndikimit në shtetet e tjera. Tregues nëse incidenti madhor i lidhur me TIK-un ka pasur ndikim në shtete të tjera (përveç Shqipërisë), në përputhje me nenin 23 të kësaj rregulloreje, dhe në veçanti në lidhje me rëndësinë e ndikimit në lidhje me: a) klientët dhe kundërpартitë financiare të prekur në shtete të tjera; b) degët ose subjektet e tjera financiare të grupit, që kryejnë veprimtari në shtete të tjera; ose	Jo	Po, nëse përmbushet kufiri i kriterit “Shtrirja gjeografike”	Po, nëse përmbushet kufiri i kriterit “Shtrirja gjeografike”	Zgjedhja (e shumëfishtë): - klientët; - kundërpартitë financiare; - degë të subjektit financiar; - subjekte financiare brenda grupit, që kryejnë veprimtari në shtete të tjera; - infrastrukturë e tregut financiar; - ofrues shërbimi palë të

	c) infrastrukturat e tregut financiar ose ofruesit e palëve të treta, të cilët mund të prekin subjektet financiare në shtete të tjera, ku ofrojnë shërbime.				treta që janë të përbashkëta me subjekte të tjera financiare.
3.19 Përshkrim se si incidenti madhor i lidhur me TIK-un ka ndikim në shtete të tjera	Përshkrimi i ndikimit dhe ashpërsisë së incidentit madhor të lidhur me TIK-un, në secilin vend të prekur, duke përfshirë një vlerësim të ndikimit dhe ashpërsisë mbi: a) klientët; b) kundërpartitë financiare; c) degët e subjektit financiar; d) subjekte të tjera financiare brenda grupit që ushtrojnë veprimtari në shtetin tjetër; e) infrastrukturat e tregut financiar; f) ofrues të palëve të treta që mund të jenë të përbashkët për subjekte të tjera financiare.	Jo	Po, nëse përmbushet kufiri i kriterit “Shtirja gjeografike”	Po, nëse përmbushet kufiri i kriterit “Shtirja gjeografike”	Alfanumerik
3.20 Kufiri i materialitetit për kriterin “Humbjet e të dhënave”	Lloji i humbjeve të të dhënave që përfshin incidenti madhor i lidhur me TIK-un, përsa i përket disponueshmërisë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave. Subjektet financiare marrin parasysh gjatë vlerësimit edhe parashikimet e nenit 24 të kësaj rregulloreje. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, humbjet e të dhënave që prekin të paktën një subjekt financiar.	Jo	Po, nëse plotësohet kriteri “Humbjet e të dhënave”	Po, nëse plotësohet kriteri “Humbjet e të dhënave”	Zgjedhja (e shumëfishtë): - disponueshmëria; - autenticiteti; - integriteti; - konfidencialiteti.
3.21 Përshkrim i humbjes së të dhënave	Përshkrimi i ndikimit të incidentit madhor të lidhur me TIK-un, në disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave kritike në përputhje me nenin 24 të kësaj rregulloreje. Informacion mbi ndikimin në zbatimin e objektivave të biznesit të subjektit financiar ose në përmbushjen e kërkesave rregullatore. Si pjesë e informacionit të dhënë, subjektet financiare duhet të tregojnë nëse të dhënat e prekura janë të dhëna të klientit, të dhëna të subjekteve të tjera (p.sh. kundërpartive financiare) ose të dhëna të vetë subjektit financiar. Subjekti financiar, gjithashtu, mund të tregojë llojin e të dhënave të përfshira në incident – në veçanti, nëse të dhënat janë konfidenciale dhe çfarë lloj konfidencialiteti është përfshirë (p.sh. konfidencialiteti tregtar/biznesi, të dhënat personale, sekretet profesionale: sekretet bankar, sekreti i sigurimeve, sekreti i shërbimeve të pagesave etj.). Informacioni mund të përfshijë, gjithashtu, rreziqe të mundshme që lidhen me humbjet e të dhënave, të tilla si nëse të dhënat e prekura nga incidenti mund të përdoren për të identifikuar individët dhe që mund të përdoren nga aktori i kërcënimit për të marrë kredi pa pëlqimin e tyre, për të kryer sulme <i>phishing</i> , për të zbuluar informacion publikisht. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, paraqitet një përshkrim i përgjithshëm i ndikimit të incidentit në subjektet financiare të prekura. Kur ka dallime të ndikimit, përshkrimi i ndikimit tregon qartë ndikimin specifik në subjektet e ndryshme financiare.	Jo	Po, nëse plotësohet kriteri “Humbjet e të dhënave”	Po, nëse plotësohet kriteri “Humbjet e të dhënave”	Alfanumerik

3.22 Kriteret e klasifikimit për “Shërbimet kritike të prekura”	Informacion në lidhje me kriterin “Shërbime kritike të prekura nga incidenti”. Subjektet financiare do të marrin parasysh nenin 25 të kësaj rregulloreje në vlerësimin e tyre, duke përfshirë informacionin rreth: - shërbimeve ose veprimtarive të prekura që kërkojnë licencim, regjistrim ose që mbikëqyren nga Banka e Shqipërisë; ose - shërbimet e TIK-ut ose rrjetet dhe sistemet e informacionit që mbështesin funksionet kritike ose të rëndësishme të subjektit financiar; dhe - natyrën e aksesit me qëllime keqdashëse dhe të paautorizuar në rrjetin dhe sistemet e informacionit të subjektit financiar. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, ndikimi në shërbimet kritike që zbatohet për të paktën një subjekt financiar.	Jo	Po	Po	Alfanumerik
3.23 Llojet e incidenteve madhore të lidhur me TIK	Klasifikimi i incidentit sipas llojit.	Jo	Po	Po	Zgjedhja (e shumëfishtë): - i lidhur me sigurinë kibernetike; - dështim i proceseve; - dështim i sistemeve; - ngjarje e jashtme; - i lidhur me pagesat; - të tjera (specifiko).
3.24 Lloje të tjera incidentesh	Lloje të tjera të incidenteve të lidhur me TIK: subjektet financiare që kanë zgjedhur opsionin “Të tjera” në fushën 3.23, duhet të specifikojnë dhe tipin e incidentit të lidhur me TIK-un që ka ndodhur.	Jo	Po, nëse është zgjedhur opsioni “Të tjera” në fushën 3.23	Po, nëse është zgjedhur opsioni “Të tjera” në fushën 3.23	Alfanumerik
3.25 Kërcënimet dhe teknikat e përdorura nga aktorët e kërcënimeve	Tregoni kërcënimet dhe teknikat e përdorura nga aktori i kërcënimit, duke përfshirë: a) inxhinieri sociale, përfshirë edhe <i>phishing</i>; b) sulm i shpërndarë/sulm i mohimit të shërbimit (D/DoS); c) vjedhje e identitetit; d) enkriptim i të dhënave për ndikim, duke përfshirë <i>ransomware</i>; e) rrëmbim i burimeve; f) nxjerrje dhe manipulim i të dhënave, duke përjashtuar vjedhjen e identitetit; g) shkatërrim i të dhënave; h) deformim; i) sulm i zinxhirit të furnizimit; j) të tjera (specifikoni).	Jo	Po, nëse lloji i incidentit të lidhur me TIK-un është “i lidhur me sigurinë kibernetike” në fushën 3.23	Po, nëse lloji i incidentit të lidhur me TIK-un është “i lidhur me sigurinë kibernetike” në fushën 3.23	Zgjedhja (e shumëfishtë): - inxhinieri sociale, përfshirë edhe <i>phishing</i>; - sulm i shpërndarë/sulm i mohimit të shërbimit (D/DoS); - vjedhje e identitetit; - enkriptim i të dhënave për ndikim, duke përfshirë <i>ransomware</i>; - rrëmbim i burimeve; - nxjerrje dhe manipulim i të dhënave, duke përjashtuar vjedhjen e identitetit; - shkatërrim i të dhënave; - deformim; - sulm i zinxhirit të furnizimit; - të tjera (specifikoni).
3.26 Lloje të tjera teknikash	Lloje të tjera teknikash Subjektet financiare që kanë zgjedhur opsionin “të tjera” në fushën e të dhënave 3.25 duhet të specifikojnë llojin e teknikës.	Jo	Po, nëse është zgjedhur opsioni “të tjera” në fushën e të dhënave 3.25	Po, nëse është zgjedhur opsioni “të tjera” në fushën e të dhënave 3.25	Alfanumerik
3.27 Informacion rreth zonave funksionale dhe proceseve të biznesit të	Tregues të zonave funksionale dhe proceseve të biznesit që janë prekur nga incidenti, përfshirë produktet dhe shërbimet. Fushat funksionale përfshijnë, por nuk janë të kufizuara në: a) marketing dhe zhvillim biznesi;	Jo	Po	Po	Alfanumerik

prekura	b) shërbimi i klientit; c) menaxhimi produktit; d) përputhshmëria me kuadrin rregullativ; e) administrim i rrezikut; f) financë dhe kontabilitet; g) burimet njerëzore dhe shërbime të përgjithshme; h) teknologjia e informacionit. Proceset e biznesit përfshijnë, por nuk janë të kufizuara në: - informimi i llogarisë; - pranimi i transaksioneve të pagesave; - autentifikimi/autorizimi; - blerja dhe shitja e paketave të policave të sigurimit ndërmjet siguracioneve; - pagesat me karta; - administrimi i <i>cash</i>-it; - depozitimi ose tërheqja e parave; - klerimi; - konglomeratet e kredive të korporatave; - transfera të kredite; - ruajtja e sigurt e aseteve dhe kasat e sigurisë; - procesimi i të dhënave; - debitime direkte; - vendosja e instrumenteve financiare; - këmbimi valutor; - këshillimi për investimet; - administrimi i investimeve; - emetimi i instrumenteve të pagesave; - administrimi i kredidhënies; - dërgesat e parave; - urdhrat; - iniciimi i pagesave; - administrimi i portofolit; - marrja/transmetimi/ekzekutimi; - shlyerja; - monitorimi i transaksioneve. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, fushat funksionale dhe proceset e biznesit të prekura në të paktën një subjekt financiar.				
3.28 Komponentët e infrastrukturës së prekur që mbështesin proceset e biznesit	Informacioni nëse komponentët e infrastrukturës (serverët, sistemet operative, <i>software</i> , serverët e aplikacioneve, pjesët ndërmjetëse (<i>middleware</i>), komponentët e rrjetit, të tjerë) që mbështesin proceset e biznesit, janë prekur nga incidenti madhor i lidhur me TIK-un.	Jo	Po	Po	Opsione: - Po; - Jo; - Informacion jo i disponueshëm.
3.29 Informacion mbi komponentët e infrastrukturës së prekur që mbështesin proceset e biznesit	Përshkrim mbi ndikimin e incidentit madhor të lidhur me TIK-un mbi komponentët e infrastrukturës (përfshirë pjesët fizike (<i>hardware</i>) dhe pjesët logjike (<i>software</i>)) që mbështesin proceset e biznesit. Pjesët fizike përfshijnë serverë, kompjuterë, qendra të dhënash, çelësa (<i>switches</i>), rutera, shpërndarës (<i>hubs</i>). Pjesët logjike përfshijnë sisteme operative, aplikacione, baza të dhënash, mjete sigurie, komponentë rrjeti, të tjera). Përshkrimi duhet të përshkruajë ose emërtojë komponentët e infrastrukturës ose sistemet e prekur dhe, kur është e disponueshme:	Jo	Po, nëse incidenti ka prekur komponentët e infrastrukturës që mbështesin proceset e biznesit	Po, nëse incidenti ka prekur komponentët e infrastrukturës që mbështesin proceset e biznesit	Alfanumerik

	a) informacionin e versionit; b) infrastrukturën brendshme/pjesërisht kontraktuar/plotësisht e kontraktuar – emrin e ofruesit të palës së tretë; c) nëse infrastruktura përdoret ose ndahet në funksione të shumta biznesi; d) planet përkatëse të qëndrueshmërisë/vazhdimësisë/rimëkëmbjes/ zëvendësueshmërisë në fuqi.				
3.30 Ndikimi në interesat financiare të klientëve	Informacion nëse incidenti madhor i lidhur me TIK-un ka pasur ndikim në interesat financiare të klientëve.	Jo	Po	Po	Opsione: - Po; - Jo; - Informacion jo i disponueshëm.
3.31 Raportimi tek autoritete të tjera	Specifikimi i autoriteteve që janë informuar për incidentin madhor të lidhur me TIK-un.	Jo	Po	Po	Zgjedhja(e shumëfishtë): - Policia/organet ligjzbatuese; - CSIRT; - Autoriteti për mbrojtjen e të dhënave; - Agjencia Kombëtare e Sigurisë Kibernetike; - Asnjë; - Të tjera (specifiko).
3.32 Specifikimi i autoriteteve “të tjera”	Specifikimi i autoriteteve “Të tjera” të informuara për incidentin madhor të lidhur me TIK-un. Nëse zgjidhet fusha e të dhënave 3.31 “Të tjera”, përshkrimi duhet të përfshijë informacion të detajuar për autoritetin në të cilin subjekti financiar ka raportuar për incidentin madhor të lidhur me TIK-un.	Jo	Po, nëse autoritete “të tjera” janë informuar nga subjekti financiar për incidentin madhor të lidhur me TIK-un.	Po, nëse autoritete “të tjera” janë informuar nga subjekti financiar për incidentin madhor të lidhur me TIK-un.	Alfanumerik
3.33 Veprime/masa të përkohshme të ndërmarra apo të planifikuara për t’u ndërmarrë, për rikuperim nga incidenti	Tregues nëse subjekti financiar ka ndërmarrë (ose planifikon të ndërmarrë) ndonjë veprim të përkohshëm për t’u rikuperuar nga incidenti madhor i lidhur me TIK-un.	Jo	Po	Po	Po/Jo
3.34 Përshkrim i veprimeve/masave të përkohshme të ndërmarra apo të planifikuara për t’u ndërmarrë, për rikuperim nga incidenti	Informacioni duhet të përshkruajë masat e menjëhershme të ndërmarra, duke përfshirë izolimin e perimetrit të incidentit në nivel rrjeti, procedurat e vëna në zbatim (<i>workaround procedures activated</i>), bllokimi i portave USB, aktivizimi i planit të rimëkëmbjes nga fatkeqësitë apo edhe kontrole të tjera sigurie të ndërmarra. Subjektet financiare duhet të tregojnë datën dhe orën e zbatimit të veprimeve të përkohshme dhe datën e parashikuar për t’u rikthyer në normalitet (në sitin primar). Për veprimet e përkohshme që nuk janë zbatuar, por janë ende të planifikuara, të tregohet data kur parashikohet zbatimi i tyre. Nëse nuk janë ndërmarrë veprime/masa të përkohshme, tregoni arsyet përkatëse.	Jo	Po, nëse veprime/masat të përkohshme janë ndërmarrë apo janë planifikuar për t’u ndërmarrë (fusha e të dhënave 3.33).	Po, nëse veprime/masa të përkohshme janë ndërmarrë apo janë planifikuar për t’u ndërmarrë (fusha e të dhënave 3.33).	Alfanumerik
3.35 Treguesit e kompromentimit	Informacioni i lidhur me incidentin madhor të lidhur me TIK-un, që mund të ndihmojë në identifikimin e aktivitetit keqdashës brenda rrjetit ose sistemit të informacionit (treguesit e kompromentimit ose IoC, ku janë të zbatueshëm).	Jo	Po, nëse lloji i incidentit është “i lidhur me sigurinë kibernetike”	Po, nëse lloji i incidentit është “i lidhur me sigurinë kibernetike” në fushën 3.23	Alfanumerik

	Kjo fushë aplikohet vetëm për ato subjekte financiare që janë brenda fushës së zbatimit të Ligjit “Për sigurinë kibernetike” dhe për ato subjekte financiare të identifikuara si infrastruktura kritike dhe të rëndësishme sipas atij ligji. IoC i ofruar nga subjekti financiar duhet të përfshijë kategoritë e mëposhtme të të dhënave: a) adresat IP; b) adresat e <i>URL</i>-ve; c) domenet; d) <i>hash</i>-et e skedarëve; e) të dhënat mbi programet keqdashëse (<i>malware</i>) (emri i <i>malware</i>, emrat e skedarëve dhe vendndodhjet e tyre, çelësat specifikë të regjistrimit të lidhur me aktivitetin e <i>malware</i>); f) të dhënat e aktivitetit të rrjetit (portat, protokollat, adresat, referuesit, agentët e përdoruesve, titujt, regjistra specifikë ose modele dalluese në trafikun e rrjetit); g) të dhënat e mesazheve të postës elektronike (dërguesi, marrësi, subjekti, titulli, përmbajtja); h) të dhënat DNS-je dhe konfigurime të regjistrimit; i) aktivitetet e llogarisë së përdoruesit (hyrjet, aktiviteti i llogarisë së përdoruesit të privilegjuar, përshkallëzimi i privilegjeve); j) trafiku i bazës së të dhënave (lexim/shkrim) kërkesat për të njëjtin skedar. Në praktikë, ky informacion mund të përfshijë të dhëna të lidhura me treguesit që përshkruajnë sjelljet në trafikun e rrjetit që u korrespondojnë sulmeve të njohura/komunikimeve të <i>botnet</i>, adresave IP të makinave të infektuara me programe keqdashëse (<i>bots</i>), të dhëna në lidhje me serverat “komanda dhe kontroll”, të përdorur nga programe keqdashëse (zakonisht domain ose adresat IP) dhe URL-të në lidhje me faqet <i>phishing</i> ose faqe interneti të vëzhguara që mbajnë programe keqdashëse.		në fushën 3.23		
Përmbajtja e raportit përfundimtar					
4.1 Klasifikimi në nivel të lartë i shkaqeve bazë të incidentit	Klasifikimi në nivel të lartë i shkaqeve bazë të incidentit madhor të lidhur me TIK-un, sipas llojit të incidentit, duke përfshirë kategoritë e niveleve të larta të mëposhtme: a) Veprime keqdashëse; b) Dështim i proceseve; c) Dështim i sistemeve; d) Gabim njerëzor; e) Ngjarje e jashtme.	Jo	Jo	Po	Zgjedhje (e shumëfishtë): - Veprime keqdashëse; - Dështim i proceseve; - Dështim i sistemeve; - Gabim njerëzor; - Ngjarje e jashtme.
4.2 Klasifikim i detajuar i shkaqeve bazë të incidentit	Klasifikim i detajuar i shkaqeve bazë të incidentit madhor të lidhur me TIK-un, sipas llojit të incidentit, duke përfshirë kategoritë e mëposhtme të detajuara, të lidhura me kategoritë e niveleve të larta të raportuara në fushën 4.1: 1. Veprime keqdashëse (nëse është përzgjedhur në fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) veprime të brendshme të qëllimshme; b) dëmtime fizike të	Jo	Jo	Po	Zgjedhje (e shumëfishtë): - veprime të brendshme të qëllimshme; - dëmtime fizike të qëllimshme/manipulim/vje dhe; - veprime keqdashëse: veprime mashtruese; - dështim i proceseve: monitorim i pamjaftueshëm ose dështim i monitorimit dhe kontrollit;

	qëllimshme/manipulim/vjedhje; c) veprime mashtruese. 2. Dështim i proceseve (nëse është përzgjedhur në fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) monitorim i pamjaftueshëm ose dështim i monitorimit dhe kontrollit; b) pamjaftueshmëri/paqartësi rolesh dhe përgjegjësish; c) dështim i procesit të administrimit të rrezikut të TIK-ut; d) pamjaftueshmëri ose dështim i veprimeve të TIK-ut dhe i veprimeve të sigurisë së TIK; e) pamjaftueshmëri ose dështim i administrimit të projekteve të TIK-ut; f) politika, procedura dhe dokumentacione të brendshme të papërshtatshme; g) blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK-ut; h) të tjera (specifikoni). 3. Dështim ose keqfunksionim i sistemit (nëse është përzgjedhur në fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) kapaciteti dhe performanca fizike e pajisjeve (<i>hardware</i>): incidente madhore të lidhur me TIK-un, të shkaktuara pajisjet (<i>hardware</i>), të cilat rezultojnë të papërshtatshme për sa i përket kapacitetit ose performancës për të përmbushur kërkesat ligjore e rregullative në fuqi; b) mirëmbajtja fizike e pajisjeve (<i>hardware</i>): incidente madhore të lidhur me TIK-un që rezultojnë nga mirëmbajtja jo e përshtatshme apo e pamjaftueshme e pjesëve përbërëse fizike të pajisjeve (<i>hardware</i>), përveç vjetërimit të pajisjeve; c) vjetërimi i pajisjeve: ky lloj shkakua bazë përfshin incidente madhore të lidhur me TIK-un që e kanë zanafillën nga komponentë të vjetruar të pajisjeve; d) përputhshmëria/konfigurimi i programeve (<i>software</i>): incidentet madhore të lidhur me TIK-un të shkaktuara nga programet (<i>software</i>) që janë jo të përputhshëm me konfigurimet e sistemeve apo programeve të tjera, duke përfshirë incidentet madhore të lidhur me TIK-un që rezultojnë nga konfliktet e programeve (<i>software</i>), cilësime të pasakta, parametra të konfiguruar jo saktë që ndikojnë në funksionimin korrekt të sistemit; e) performanca e programeve (<i>software</i>): incidentet madhore të lidhur me TIK-un që rezultojnë si pasojë e performancës së dobët apo të pamjaftueshme të fragmenteve logjike (komponentëve <i>software</i>), për arsye të tjera nga ato të specifikuar në opsionin “përputhshmëria/konfigurimi i programeve (<i>software</i>)”, duke përfshirë incidentet madhore të lidhur me TIK-un të shkaktuara nga koha e ulët e përgjigjes, konsumi i tepërt i burimeve ose ekzekutimi jo efikas i kërkesave, që ndikon në performancën e programit (<i>software</i>) ose sistemit; f) konfigurimi i rrjetit: incidente madhore të lidhur me TIK-un që vijnë				- dështim i proceseve: pamjaftueshmëri/paqartësi rolesh dhe përgjegjësish; - dështim i proceseve: dështim i procesit të administrimit të rrezikut të TIK-ut; - dështim i proceseve: pamjaftueshmëri ose dështim i veprimeve të TIK-ut dhe i veprimeve të sigurisë së TIK; - dështim i proceseve: pamjaftueshmëri ose dështim i administrimit të projekteve të TIK-ut; - dështim i proceseve: politika, procedura dhe dokumentacione të brendshme të papërshtatshme; - dështim i proceseve: blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK-ut; - dështim i procesit: të tjera (specifikoni); - dështim i sistemit: kapaciteti dhe performanca fizike e pajisjeve (<i>hardware</i>); - dështim i sistemit: mirëmbajtja fizike e pajisjeve (<i>hardware</i>); - dështim i sistemit: vjetërimi i pajisjeve; - dështim i sistemit: përputhshmëria/konfigurimi i programeve (<i>software</i>); - dështim i sistemit: performanca e programeve (<i>software</i>); - dështim i sistemit: konfigurim i rrjetit; - dështim i sistemit: dëmtim fizik; - dështim i sistemit: të tjera (specifikoni); - gabim njerëzor: harresa; - gabim njerëzor: gabime; - gabim njerëzor: aftësi dhe njohuri; - gabim njerëzor: burime njerëzore të pamjaftueshme; - gabim njerëzor: keqkomunikim; - gabim njerëzor: të tjera (specifikoni); - ngjarje të jashtme: fatkeqësi natyrore/forca madhore; - ngjarje të jashtme: dështim i palëve të treta; - ngjarje të jashtme: të tjera (specifikoni).
--	--	--	--	--	--

	si pasojë e cilësimeve ose infrastrukturës të pasakta ose të konfiguruar gabimisht së rrjetit, duke përfshirë incidente madhore të lidhura me TIK-un të shkaktuara nga gabimet e konfigurimit të rrjetit, problemet e rrugëzimit (<i>routing</i>), konfigurimet e gabuara të <i>firewall</i>-it ose probleme të tjera të lidhura me rrjetin që ndikojnë në lidhjet ose komunikimin; g) dëmtime fizike: incidente madhore të lidhur me TIK-un të shkaktuara nga dëmtimet fizike të infrastrukturave të TIK-ut, që çojnë në dështime të sistemeve; h) të tjera (specifikoni). 4. Gabime njerëzore (nëse është përzgjedhur në fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) harresa (të paqëllimshme); b) gabime; c) aftësi dhe njohuri: incidente madhore të lidhur me TIK-un që vijnë si pasojë e mungesës së ekspertizës ose aftësisë në trajtimin e sistemeve ose proceseve të TIK-ut, të cilat mund të shkaktohen nga trajnimi i pamjaftueshëm, njohuritë e pamjaftueshme ose boshllëqet në aftësitë e nevojshme për të kryer detyra specifike ose për të adresuar sfidat teknike; d) burime njerëzore të pamjaftueshme: incidente madhore të lidhur me TIK-un të shkaktuara nga mungesa e burimeve të nevojshme, përfshirë edhe pajisjet (<i>hardware</i>), programet (<i>software</i>), infrastrukturën, ose personelin, dhe përfshirë situatat kur burimet e pamjaftueshme çojnë në dështime të sistemeve ose pamundësi për të plotësuar kërkesat e biznesit; e) keqkomunikim; f) të tjera (specifikoni). 5. Ngjarje të jashtme (nëse është përzgjedhur në fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) fatkeqësi natyrore /forca madhore; b) dështime të palëve të treta; c) të tjera (specifikoni). Subjektet financiare duhet të mbajnë parasysh që, për incidentet madhore të përsëritura të lidhur me TIK-un, të merret parasysh shkaku rrënjësor i dukshëm specifik i incidentit dhe jo kategoritë e përgjithshme të përfshira në këtë fushë.				
4.3 Klasifikim shtesë mbi shkaqet bazë të incidentit	Klasifikim shtesë i shkaqeve bazë të incidentit madhor të lidhur me TIK-un, sipas llojit të incidentit, duke përfshirë kategoritë shtesë të klasifikimit të lidhura me kategoritë e detajuara të raportuara në fushën 4.2. Fusha është e detyrueshme për raportin përfundimtar, nëse kategoritë specifike që kërkojnë detajim të hollësishëm janë raportuar në fushën 4.2. 2(a) Monitorim i pamjaftueshëm ose dështim i monitorimit dhe kontrollit: a) monitorim i zbatimit të politikës; b) monitorim i ofruesve të shërbimeve të palëve të treta; c) monitorim dhe verifikim i korrigjimit të vulnerabiliteteve; d) menaxhim i identitetit dhe aksesit;	Jo	Jo	Po	Opsione (të shumëfishta): - monitorim i zbatimit të politikës; - monitorim i ofruesve të shërbimeve të palëve të treta; - monitorim dhe verifikim i korrigjimit të vulnerabiliteteve; - menaxhim i identitetit dhe aksesit; - enkriptimi dhe kriptografia; - regjistrim i ngjarjeve/logimi; - dështim në përcaktimin e niveleve të sakta të

	e) enkriptimi dhe kriptografia; f) regjistrim i ngjarjeve/logimi. 2(c) Dështim i procesit të administrimit të rrezikut të TIK-ut: a) dështim në përcaktimin e niveleve të sakta të tolerancës ndaj rrezikut; b) vlerësime të pamjaftueshme të vulnerabiliteteve dhe kërcënimeve; c) masa të papërshtatshme të trajtimit të rreziqeve; d) administrim i dobët i rreziqeve të mbetura të TIK-ut. 2(d) Pamjaftueshmëri ose dështim i veprimeve të TIK-ut dhe i veprimeve të sigurisë së TIK: a) administrimi i vulnerabiliteteve dhe i <i>patch</i>-eve; b) administrimi i ndryshimeve; c) administrimi i kapaciteteve dhe performancës; d) administrimi i aseteve të TIK-ut dhe klasifikimi i informacionit; e) <i>backup</i> dhe rikuperimi; f) trajtimi i gabimeve. 2(g) Blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK-ut: a) blerja, zhvillimi dhe mirëmbajtja e sistemeve TIK të papërshtatshme; b) testimi i pamjaftueshëm i programeve (<i>software</i>) ose dështimi i testimit të programeve (<i>software</i>).				tolerancës ndaj rrezikut; - vlerësime të pamjaftueshme të vulnerabiliteteve dhe kërcënimeve; - masa të papërshtatshme të trajtimit të rreziqeve; - administrim i dobët i rreziqeve të mbetura të TIK-ut; - administrimi i vulnerabiliteteve dhe i <i>patch</i>-eve; - administrimi i ndryshimeve; - administrimi i kapaciteteve dhe performancës; - administrimi i aseteve të TIK-ut dhe klasifikimi i informacionit; - <i>backup</i> dhe rikuperimi; - trajtimi i gabimeve; - blerja, zhvillimi dhe mirëmbajtja e sistemeve TIK të papërshtatshme; - testimi i pamjaftueshëm i programeve (<i>software</i>) ose dështimi i testimit të programeve (<i>software</i>).
4.4 Lloje të tjera të shkaqeve bazë	Subjektet financiare që kanë zgjedhur opsionin shkaqe bazë "të tjera" në fushën 4.2, duhet të specifikojnë këto shkaqe bazë.	Jo	Jo	Po, nëse është zgjedhur opsioni shkaqe bazë "të tjera" në fushën 4.2.	Alfanumerik
4.5 Informacione mbi shkaqet bazë të incidentit	Përshkrim i rrjedhës së ngjarjeve që çuan në incidentin madhor të lidhur me TIK-un dhe përshkrim i mënyrës se si incidenti madhor i lidhur me TIK-un ka një shkak bazë të dukshëm të ngjashëm, nëse ai incident klasifikohet si incident i përsëritur, duke përfshirë një përshkrim të përmbledhur të të gjitha arsyeve themelore dhe faktorëve kryesorë që kontribuan në ndodhjen e këtij incidenti madhor të lidhur me TIK-un. Në rastet kur ka pasur veprime keqdashëse, përshkruani mënyrën e kryerjes së veprimit keqdashës, duke përfshirë taktikat, teknikat dhe procedurat e përdorura, si dhe vektorin e hyrjes së incidentit madhor të lidhur me TIK-un, përfshirë një përshkrim të hetimeve dhe analizave që çuan në identifikimin e shkaqeve bazë, nëse është e zbatueshme.	Jo	Jo	Po	Alfanumerik
4.6 Përmbledhje e zgjidhjes së incidentit	Informacione shtesë mbi veprimet/masat e marra/të planifikuara, për të zgjidhur përfundimisht incidentin madhor të lidhur me TIK-un dhe për të parandaluar përsëritjen e incidentit. Konkluzione/mësime të nxjerra nga incidenti madhor i lidhur me TIK-un. Përshkrimi duhet të përmbajë pikat e mëposhtme: 1. Përshkrim i veprimeve/masave për zgjidhjen e incidentit a) veprimet/masat e marra për zgjidhjen përfundimtare të incidentit	Jo	Jo	Po	Alfanumerik

	madhor të lidhur me TIK-un (duke përjashtuar çdo veprim të përkohshëm); b) për çdo veprim/masë të ndërmarrë, tregoni përfshirjen e mundshme të ndonjë ofruesi palë e tretë, si dhe të ndonjë subjekti financiar; c) tregoni nëse procedurat janë përshtatur pas incidentit madhor të lidhur me TIK-un; d) tregoni ndonjë kontroll shtesë të ndërmarrë ose të planifikuar për t'u kryer, me afatet përkatëse për implementimin e tyre. Çështje të mundshme të identifikuar në lidhje me qëndrueshmërinë e sistemeve të teknologjisë së informacionit të prekura nga incidenti /ose në lidhje me procedurat apo kontrollat ekzistuese, nëse është e zbatueshme. Subjektet financiare tregojnë qartë sesi veprimet korrigjuese të parashikuara do të adresojnë shkaqet bazë të identifikuar dhe kur pritet të zgjidhet përfundimisht incidenti madhor i lidhur me TIK-un. 2.Konkluzione/mësimet nxjerra Subjektet financiare duhet të përshkruajnë gjetjet nga rishikimet pas incidentit.				
4.7 Data dhe ora kur shkaku bazë i incidentit u adresua	Data dhe ora kur u adresua shkaku bazë i incidentit.	Jo	Jo	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
4.8 Data dhe ora kur incidenti u zgjidh	Data dhe ora e zgjidhjes së incidentit.	Jo	Jo	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
4.9 Informacion nëse data e zgjidhjes përfundimtare të incidentit ndryshon nga data fillestare e planifikuar për implementim	Përshkrim i arsyes përse data e zgjidhjes përfundimtare të incidentit madhor të lidhur me TIK-un është e ndryshme nga data e planifikuar fillimisht për implementimin, kur është e zbatueshme.	Jo	Jo	Po	Alfanumerik
4.10 Vlerësimi i rrezikut në funksionet me rëndësi kritike për qëllime të ndërhyrjes së jashtëzakonshme	Vlerësim nëse incidenti madhor i lidhur me TIK-un paraqet rrezik për funksionet me rëndësi kritike, në kuptim të ligjit "Për rimëkëmbjen dhe ndërhyrjen e jashtëzakonshme në banka, në Republikën e Shqipërisë". Subjektet e ligjit "Për rimëkëmbjen dhe ndërhyrjen e jashtëzakonshme në banka, në Republikën e Shqipërisë", duhet të tregojnë nëse incidenti paraqet rrezik për funksionet me rëndësi kritike në kuptim të atij ligji.	Jo	Jo	Po, nëse incidenti paraqet rrezik për funksionet me rëndësi kritike, në kuptim të ligjit "Për rimëkëmbjen dhe ndërhyrjen e jashtëzakonshme në banka, në Republikën e Shqipërisë".	Alfanumerik
4.11 Informacion i vlefshëm për autoritetin e ndërhyrjes së jashtëzakonshme	Përshkrim nëse po dhe në ç'mënyrë incidenti madhor i lidhur me TIK-un ka ndikuar në ndërhyrjen e jashtëzakonshme të subjektit apo grupit. Subjektet e ligjit "Për rimëkëmbjen dhe ndërhyrjen e jashtëzakonshme në banka, në Republikën e Shqipërisë", duhet të japin informacion nëse po dhe në ç'mënyrë incidenti madhor i lidhur me TIK-un ka ndikuar në ndërhyrjen e jashtëzakonshme të subjektit apo grupit	Jo	Jo	Po, nëse incidenti ka ndikuar në ndërhyrjen e jashtëzakonshme të subjektit apo grupit	Alfanumerik

	grupit. Këto subjekte duhet të tregojnë, gjithashtu, nëse incidenti madhor i lidhur me TIK-un ndikon në qëndrueshmërinë financiare ose likuiditetin e subjektit financiar dhe vlerësimin e mundshëm sasior të ndikimit. Këto subjekte duhet të japin, gjithashtu, informacion mbi ndikimin në vazhdimësinë operacionale, ndikimin në mundësinë e ndërhyrjes së jashtëzakonshme të subjektit, çdo ndikim shtesë në kostot dhe humbjet nga incidenti madhor i lidhur me TIK-un, duke përfshirë pozicionin e kapitalit të subjektit financiar, dhe nëse marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK-ut janë ende të qëndrueshme dhe plotësisht të zbatueshme në rast të ndërhyrjes së jashtëzakonshme të subjektit.				
4.12 Kufijtë e materialitetit për klasifikimin e kriterit “Ndikimi ekonomik”	Informacion i detajuar mbi kufijtë që janë arritur nga incidenti madhor i lidhur me TIK-un, në lidhje me kriterin “Ndikimi ekonomik”, i parashikuar në nenin 26 të kësaj rregulloreje.	Jo	Jo	Po	Alfanumerik
4.13 Shuma e humbjeve dhe kostove bruto direkte dhe indirekte	Shuma totale e kostove dhe humbjeve bruto direkte dhe indirekte të pësura nga subjekti financiar si pasojë e incidentit madhor të lidhur me TIK-un, duke përfshirë: a) shuma e fondeve ose aktiveve financiare të përvetësuarra (<i>expropriated</i>), për të cilat subjekti financiar është përgjegjës; b) shuma e kostove për zëvendësimin ose zhvendosjen e pajisjeve (<i>hardware</i>), programeve kompjuterike (<i>software</i>) ose infrastrukturës; c) shuma e kostove të personelit, përfshirë edhe kostot që lidhen me zëvendësimin ose zhvendosjen e personelit, rekrutimin e personelit shtesë, shpërblimet për punën jashtë orarit dhe rikuperimin e aftësive të humbura ose të dëmtuara të stafit; d) shuma e tarifave të detyrueshme për shkak të mosrespektimit të detyrimeve kontraktuale; e) shuma e kostove për zgjidhjen e mosmarrëveshjeve dhe kompensimin e klientëve; f) shuma e humbjeve për shkak të të ardhurave të munguara; g) shuma e kostove që lidhen me komunikimin e brendshëm dhe të jashtëm; h) shuma e kostove të konsulencës, duke përfshirë kostot që lidhen me këshillimin ligjor, shërbimet mjekoligjore dhe shërbimet e rehabilitimit; i) shuma e kostove dhe humbjeve të tjera, duke përfshirë: i. shpenzime të drejtpërdrejta në pasqyrën e të ardhurave dhe shpenzimeve, duke përfshirë zhvlerësimet dhe kostot e shitjes, si dhe fshirjet e kredive për shkak të incidentit madhor të lidhur me TIK-un; ii. provigjionet kontabël të pasqyruara	Jo	Jo	Po	Monetare

	në pasqyrën e të ardhurave dhe shpenzimeve kundrejt humbjeve të mundshme që lidhen me incidentin madhor të lidhur me TIK-un; iii. humbje të mbetura pezull (<i>pending losses</i>), në formën e humbjeve që rrjedhin nga incidenti madhor i lidhur me TIK-un, të cilat janë të regjistruara përkohësisht në llogari tranzitore/pezull dhe që nuk janë reflektuar ende në pasqyrën e të ardhurave dhe shpenzimeve, por që planifikohen të përfshihen brenda një periudhe kohore që përputhet me madhësinë dhe kohëzgjatjen e zërit të mbetur pezull; iv. të ardhura materiale të pambledhura, të lidhura me detyrime kontraktuale ndaj palëve të treta, duke përfshirë vendimin për të kompensuar një klient pas incidentit madhor të lidhur me TIK-un, jo përmes rimbursimit ose pagesës direkte, por përmes një rregullimi të të ardhurave, që përjashton ose ul tarifat kontraktuale për një periudhë të caktuar kohore në të ardhmen; v. humbje në kohë (<i>timing losses</i>), kur ato shtrihen në më shumë se një vit kontabël dhe sjellin rrezik ligjor. Subjektet financiare duhet të marrin parasysh në vlerësimin e tyre, kërkesat e nenit 26, pikat 1 dhe 2 të kësaj rregulloreje. Subjektet financiare nuk duhet të përfshijnë në këtë shifër asnjë vlerë të rikuperuar. Subjektet financiare duhet të raportojnë shumën monetare si një vlerë pozitive. Në rastin e raportimit të agreguar sipas nenit 38 të kësaj rregulloreje, subjektet financiare duhet të marrin parasysh shumën totale të kostove dhe humbjeve për të gjitha subjektet financiare. Subjektet financiare duhet të raportojnë shifrat në mijë njësi.				
4.14 Shuma e rikuperuar	Vlera totale e rikuperuar. Vlera e rikuperimeve duhet të lidhet me humbjen origjinale të shkaktuar nga incidenti i ndodhur, pavarësisht kohës së marrjes së vlerës së rikuperuar, në formë fondesh ose përfitimesh financiare. Subjektet financiare duhet të raportojnë shumën monetare si një vlerë pozitive. Në rastin e raportimit të agreguar, sipas nenit 38 të kësaj rregulloreje, subjektet financiare duhet të marrin parasysh vlerën totale të rikuperuar, për të gjitha subjektet financiare.	Jo	Jo	Po	Monetare Subjektet financiare duhet të raportojnë shifrat në mijë njësi.
4.15 Informacion nëse incidentet madhore kanë qenë të përsëritura	Informacion nëse disa incidente jo madhore të lidhura me TIK-un janë përsëritur dhe së bashku konsiderohen si një incident madhor në kuptimin e nenit 27, pika 2, të kësaj rregulloreje. Subjektet financiare duhet të tregojnë nëse incidentet jo madhore të lidhura me TIK-un janë të përsëritur dhe së bashku konsiderohen si një incident madhor i lidhur me TIK-un. Subjektet financiare duhet të tregojnë sa herë kanë ndodhur këto incidente jo madhore të lidhura me TIK-un.	Jo	Jo	Po, nëse incidenti madhor përbëhet nga disa incidente jo madhore të përsëritura.	Alfanumerik
4.16 Data dhe ora e ndodhjes së incidenteve	Nëse subjektet financiare raportojnë incidente të përsëritura të lidhura me TIK-un, paraqesin datën dhe orën kur	Jo	Jo	Po, për incidente të përsëritur	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)

të përsëritura	ka ndodhur incidenti i parë i lidhur me TIK-un.				
----------------	---	--	--	--	--

ANEKSI 3

FORMULARËT PËR NJOFTIMIN E KËRCËNIMEVE KIBERNETIKE TË RËNDËSISHME

Numri i fushës	Fusha e të dhënave	
1	Emri i subjektit financiar që paraqet njoftimin	
2	Kodi i identifikimit të subjektit që paraqet njoftimin	
3	Lloji i subjektit financiar që paraqet njoftimin	
4	Emri i subjektit financiar	
5	Kodi NUIS/LEI i subjektit financiar	
6	Emri i personit kryesor të kontaktit	
7	Adresa e postës elektronike të personit kryesor të kontaktit	
8	Numri i telefonit të personit kryesor të kontaktit	
9	Emri i personit dytësor të kontaktit	
10	Adresa e postës elektronike të personit dytësor të kontaktit	
11	Numri i telefonit të personit dytësor të kontaktit	
12	Data dhe ora e zbulimit të kërcënimit kibernetik	
13	Përshkrimi i kërcënimit të rëndësishëm kibernetik	
14	Informacion mbi ndikimin potencial	
15	Kriteret e klasifikimit të incidentit potencial	
16	Statusi i kërcënimit kibernetik	
17	Veprimet e ndërmarra për të parandaluar materializimin e kërcënimit	
18	Njoftimi i palëve të tjera të përfshira	
19	Treguesit e kompromentimit	
20	Informacion tjetër i lidhur me ngjarjen	

ANEKSI 4

UDHËZIME MBI PLOTËSIMIN E FORMULARËVE TË NJOFTIMIT PËR KËRCËNIMET KIBERNETIKE TË RËNDËSISHME

Fusha e të dhënave	Përshkrimi	Fushë e detyrueshme	Lloji i fushës
1. Emri i subjektit financiar që paraqet njoftimin	Emri i plotë ligjor i subjektit që paraqet njoftimin	Po	Alfanumerik
2. Kodi i identifikimit të subjektit që paraqet njoftimin	Kodi i identifikimit të subjektit që paraqet njoftimin Nëse njoftimin e bën subjekti financiar, kodi i identifikimit duhet të jetë NUIS ose Identifikuesi Ligjor i Subjektit (LEI), i cili është një kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020. Nëse një ofrues i shërbimeve të palëve të treta paraqet njoftimin për një subjekt financiar, mund të përdorë një kod identifikimi të specifikuar sipas standardeve teknike të parashikuara në kuadrin nënligjor të Bankës së Shqipërisë, për regjistrin e informacionit në lidhje me marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK-ut, të parashikuara në nenin 45 të kësaj rregulloreje.	Po	Alfanumerik
3. Lloji i subjektit financiar që paraqet njoftimin	Lloji i subjektit të parashikuar në pikën 1 të nenit 2 të kësaj rregulloreje, që paraqet njoftimin.		Opsionet (mund të zgjidhen disa opsione): - institucionet e kreditit;

			- institucionet e pagesave; - institucionet e pagesave që përjashtohen sipas ligjit “Për shërbimet e pagesave”; - ofruesit e shërbimit të informimit të llogarisë; - institucionet e parasë elektronike; - institucionet e parasë elektronike që përjashtohen sipas ligjit “Për shërbimet e pagesave”; - emetuesit e tokenave të aseteve dhe emetuesit e tokenave të parasë elektronike.
4. Emri i subjektit financiar	Emri i plotë ligjor i subjektit financiar që njofton për kërcënimin e rëndësishëm kibernetik.	Po, nëse subjekti financiar është i ndryshëm nga subjekti që paraqet njoftimin.	Alfanumerik
5. Kodi NUIS/LEI i subjektit financiar	Kodi NUIS/LEI i subjektit financiar që njofton për kërcënimin e rëndësishëm kibernetik, i caktuar në përputhje me Organizatën Ndërkombëtare të Standardizimit.	Po, nëse subjekti financiar që njofton për kërcënimin e rëndësishëm kibernetik, është i ndryshëm nga subjekti që paraqet raportin.	Kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020.
6. Emri i personit kryesor të kontaktit	Emri dhe mbiemri i personit kryesor të kontaktit të subjektit financiar.	Po	Alfanumerik
7. Adresa e postës elektronike të personit kryesor të kontaktit	Adresa e postës elektronike të personit kryesor të kontaktit që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin.	Po	Alfanumerik
8. Numri i telefonit të personit kryesor të kontaktit	Numri i telefonit të personit kryesor të kontaktit që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin. Numri i telefonit që raportohet duhet të jetë i formatit si p.sh. +3556XXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).	Po	Alfanumerik
9. Emri i personit dytësor të kontaktit	Emri dhe mbiemri i personit dytësor të kontaktit të subjektit financiar ose të subjektit që paraqet njoftimin në emër të subjektit financiar, kur është e zbatueshme.	Po, nëse emri dhe mbiemri i personit dytësor të kontaktit të subjektit financiar ose të subjektit që paraqet njoftimin në emër të subjektit financiar është i disponueshëm.	Alfanumerik
10. Adresa e postës elektronike të personit dytësor të kontaktit	Adresa e postës elektronike të personit dytësor të kontaktit ose një adresë funksionale e grupit përgjegjës, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin, nëse është e disponueshme.	Po, nëse adresa e postës elektronike të personit dytësor të kontaktit ose një adresë funksionale e grupit përgjegjës, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin, është e disponueshme.	Alfanumerik
11. Numri i telefonit të personit dytësor të kontaktit	Numri i telefonit i personit dytësor të kontaktit, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin, nëse është i disponueshëm. Numri i telefonit që raportohet duhet të jetë i formatit si p.sh. +3556XXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).	Po, nëse numri i telefonit i personit dytësor të kontaktit, që mund të përdoret nga Banka e Shqipërisë për të ndjekur komunikimin, është i disponueshëm.	Alfanumerik
12. Data dhe ora e zbulimit të kërcënimit kibernetik	Data dhe ora kur subjekti financiar është vënë në dijeni për kërcënimin e rëndësishëm kibernetik.	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
13. Përshkrimi i kërcënimit	Përshkrimi i aspekteve më të rëndësishme të	Po	Alfanumerik

të rëndësishëm kibernetik	kërcënimit të rëndësishëm kibernetik. Subjektet financiare duhet të paraqesin: a) një përmbledhje të përgjithshme të aspekteve më të rëndësishme të kërcënimit të rëndësishëm kibernetik; b) rreziqet përkatëse që burojnë nga ky kërcënim, duke përfshirë vulnerabilitetet e mundshme të sistemeve të subjektit financiar, që mund të shfrytëzohen; c) informacion mbi probabilitetin e materializimit të kërcënimit të rëndësishëm kibernetik; dhe d) informacion mbi burimin e informacionit për kërcënimin kibernetik.		
14. Informacion mbi ndikimin potencial	Informacion mbi ndikimin e mundshëm/potencial të kërcënimit kibernetik mbi subjektin financiar, klientët e tij ose kundërpartit të tjera financiare, nëse kërcënimi kibernetik është materializuar.	Po	Alfanumerik
15. Kriteret e klasifikimit të incidentit potencial	Kriteret e klasifikimit që mund të kishin shkaktuar një raportim për incident madhor, nëse kërcënimi kibernetik do të ishte materializuar.	Po	Zgjedhje (e shumëfishtë): - klientët, kundërpartitë financiare dhe transaksionet e prekura; - ndikimi reputacional; - kohëzgjatja e incidentit dhe kohëzgjatja e ndërprerjes së shërbimeve; - shtrirja gjeografike; - humbja e të dhënave; - shërbimet kritike të prekura; - ndikimi ekonomik.
16. Statusi i kërcënimit kibernetik	Informacion mbi statusin e kërcënimit kibernetik për subjektin financiar dhe nëse ka pasur ndonjë ndryshim në aktivitetin e kërcënimit. Në rastet kur kërcënimi kibernetik ka ndaluar komunikimin me sistemet e informacionit të subjektit financiar, statusi mund të shënohet si "joaktiv". Nëse subjekti financiar ka informacion që kërcënimi vazhdon të jetë aktiv kundrejt palëve të tjera apo ndaj sistemit financiar në tërësi, statusi duhet të shënohet si "aktiv".	Po	Zgjedhje: - aktiv; - joaktiv.
17. Veprimet e ndërmarra për të parandaluar materializimin e kërcënimit	Informacion i përgjithshëm mbi veprimet e ndërmarra nga subjekti financiar për të parandaluar materializimin e kërcënimeve kibernetike të rëndësishme, nëse është e aplikueshme.	Po	Alfanumerik
18. Njoftimi i palëve të tjera të përfshira	Informacion mbi njoftimin e kërcënimit kibernetik të subjekte të tjera financiare ose autoriteteve të tjera.	Po, nëse subjekte financiare të tjera ose autoritete të tjera janë informuar mbi kërcënimin kibernetik.	Alfanumerik
19. Treguesit e kompromentimit	Informacion i lidhur me kërcënimin kibernetik që mund të ndihmojë në identifikimin e aktivitetit keqdashës brenda rrjetit ose sistemit të informacionit (treguesit e kompromentimit ose IoC, ku janë të zbatueshëm). Treguesit e kompromentimit (IoC) të paraqitur nga subjekti financiar mund të përfshijnë, por nuk kufizohen në kategoritë e mëposhtme të të dhënave: a) adresat IP; b) adresat e URL-ve; c) domenet; d) hash-et e skedarëve; e) të dhënat mbi programet keqdashëse (malware) (emri i malware, emrat e skedarëve dhe	Po, nëse informacioni mbi treguesit e kompromentimit të lidhur me kërcënimin kibernetik është i disponueshëm.	Alfanumerik

	vendndodhjet e tyre, çelësat specifikë të regjistrimit të lidhur me aktivitetin e <i>malware</i>); f) të dhënat e aktivitetit të rrjetit (portat, protokollet, adresat, referuesit, agjentët e përdoruesve, titujt, regjistra specifikë ose modele dalluese në trafikun e rrjetit); g) të dhënat e mesazheve të postës elektronike (dërguesi, marrësi, subjekti, titulli, përmbajtja); h) të dhënat DNS-je dhe konfigurime të regjistrimit; i) aktivitetet e llogarisë së përdoruesit (hyrjet, aktiviteti i llogarisë së përdoruesit të privilegjuar, përshkallëzimi i privilegjeve); j) trafiku i bazës së të dhënave (lexim/shkrim) kërkesat për të njëjtin skedar. Ky lloj informacioni mund të përfshijë të dhëna të lidhura me treguesit që përshkruajnë sjelljet në trafikun e rrjetit që u korrespondojnë sulmeve të njohura/komunikimeve të <i>botnet</i>, adresave IP të makinave të infektuara me programe keqdashëse (<i>bots</i>), të dhëna në lidhje me serverat “komanda dhe kontroll”, të përdorur nga programe keqdashëse (zakonisht domain ose adresat IP) dhe URL-të në lidhje me faqet <i>phishing</i> ose faqe interneti të vëzhguara që mbajnë programe keqdashëse.		
20. Informacion tjetër i lidhur me ngjarjen	Informacion tjetër në lidhje me kërcënimin e rëndësishëm kibernetik.	Po, nëse aplikohet dhe nëse ka informacion tjetër të disponueshëm që nuk është përfshirë në formular.	Alfanumerik

ANEKSI 5
FORMULARI I RAPORTIMIT TË KOSTOVE DHE HUMBJEVE BRUTO DHE VLERAVE TË
RIKUPERUARA GJATË VITIT REFERENCË

Emri i subjektit financiar				
NUIS/LEI				
Data e fillimit dhe fundit të vitit referencë të subjektit financiar				
Monedha				
Numri i incidentit	Data e paraqitjes së raportit përfundimtar të incidentit	Numri i referencës të incidentit	Kostot dhe humbjet bruto nga incidenti gjatë vitit referencë (në mijë njësi)	Vlerat e rikuperuara nga incidenti gjatë vitit referencë (në mijë njësi)
1				
2				
....				
Totali për vitin referencë				