REPUBLIKA E SHQIPËRISË
AUTORITETI I MBIKËQYRJES FINANCIARE
BORDI

RREGULLORE
"PËR QËNDRUESHMËRINË OPERACIONALE DIGJITALE NË SUBJEKTET E LICENCUARA NGA AUTORITETI I MBIKËQYRJES FINANCIARE"

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

1. Objekti i kësaj rregulloreje është unifikimi i kërkesave që lidhen me sigurinë e rrjetit dhe sistemeve të informacionit që mbështesin veprimtarinë e subjekteve financiare të licencuara dhe të mbikëqyrura nga Autoriteti i Mbikëqyrjes Financiare, këtu e në vijim "Autoriteti".

2. Kjo rregullore përcakton sa më poshtë:
   a) Kërkesat e zbatueshme për subjektet financiare në lidhje me:
      i. menaxhimin e rrezikut të teknologjisë së informacionit dhe komunikimit (*TIK*);
      ii. raportimin pranë Autoritetit të incidenteve madhore të lidhura me TIK, si dhe njoftimin, mbi bazë vullnetare, të kërcënimeve të rëndësishme kibernetike;
      iii. testimin e qëndrueshmërisë operacionale digjitale;
      iv. shkëmbimin e informacionit dhe inteligjencës në lidhje me kërcënimet dhe cenueshmëritë kibernetike;
      v. masat për administrimin e rrezikut nga palët e treta që ofrojnë shërbime TIK.
   b) Kërkesat mbi marrëveshjet kontraktuale të lidhura ndërmjet ofruesve të shërbimeve TIK palë të treta dhe subjekteve financiare;
   c) Rregullat për ngritjen dhe funksionimin e kuadrit mbikëqyrës për ofruesit kritikë të shërbimeve TIK palë të treta, kur këta ofrojnë shërbime për subjektet financiare.
   d) Rregulla për bashkëpunimin ndërmjet autoriteteve përgjegjëse, si dhe rregulla për mbikëqyrjen dhe zbatimin nga autoritetet përgjegjëse në lidhje me të gjitha çështjet e mbuluara nga kjo rregullore.
   e) Për subjektet financiare të identifikuara si entitete të rëndësishme në përputhje me rregullat kombëtare që transpozojnë nenin 3, të Direktivës (BE) 2022/2555, kjo rregullore do të konsiderohet si një akt ligjor sektorial i Bashkimit për qëllimet e nenit 4, të asaj Direktivë.

Neni 2
Baza ligjore

Kjo rregullore hartohet në zbatim të nenit 14, pika 2, e ligjit nr. 9572, datë 03.07.2006 "Për Autoritetin e Mbikëqyrjes Financiare", i ndryshuar.

Neni 3
Fusha e zbatimit

1. Kjo rregullore zbatohet për subjektet e mëposhtme:

   a) shoqëritë komisionere, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   b) ofruesit e shërbimeve të kripto-aseteve të autorizuar, sipas legjislacion në fuqi që rregullon tregjun e kripto aseteve, si dhe emetuesit e tokenëve të referuar në asete, sipas legjislacionit të zbatueshëm për tegjet e kripto aseteve;

   c) depozitarët qendrorë të titujve, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   d) kundërpala qendrore (*CCP-të*) sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   e) vendet e tregtimit, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   f) regjistrat/sistemet për grumbullimin e të dhënave të tregtimit, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   g) administruesit e fondeve të investimeve alternative, sipas legjislacionit të zbatueshëm për fondet e investimeve alternative;

   h) shoqëritë e administrimit të sipërmarrjeve të investimeve kolektive, sipas legjislacionit të zbatueshëm për sipërmarrjet e investimeve kolektive;

   i) ofruesit e shërbimeve të raportimit të të dhënave, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   j) shoqëritë e sigurimit dhe risigurimit, sipas legjislacionit të zbatueshëm për sigurimin dhe risigurimin;

   k) ndërmjetësit e sigurimeve, ndërmjetësit e risigurimeve dhe ndërmjetësit ndihmës të sigurimeve sipas legjislacionit të zbatueshëm për sigurimin dhe risigurimin;

   l) shoqëritë administruese të fondeve të pensioneve private, sipas legjislacionit të zbatueshëm për fondet e pensionit privat;

   m) agjencitë e vlerësimit të kreditit, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   n) administratorët e treguesve referues kritikë (critical benchmarks) sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

   o) ofruesit e shërbimeve të financimit me shuma të vogla përmes një grupi personash (*crowdfunding*), sipas legjislacionit të zbatueshëm për financimin me shuma të vogla përmes një grupi personash;

p) regjistrat/sistemet për grumbullimin e të dhënave të produkteve të titullzuara, sipas legjislacionit të zbatueshëm për tregjet e kapitalit;

q) ofruesit e shërbimeve TIK, palë të treta.

2. Për qëllime të kësaj rregulloreje, subjektet e përmendura në pikën 1, shkronja "a" deri në "q", do të referohen si "subjekte financiare".

3. Kjo rregullore nuk zbatohet për:

a) administruesit e fondeve të investimeve alternative të përmendur në nenin 3, paragrafi 2, të Direktivës së Bashkimit Evropian 2011/61/BE;

b) shoqëritë e sigurimit dhe risigurimit të përmendura në nenin 4, të Direktivës 2009/138/KE;

c) institucionet e pensioneve profesionale të punësimit që operojnë skema pensioni të cilat, së bashku, nuk kanë më shumë se 15 anëtarë në total;

d) personat fizikë ose juridikë të përjashtuar në përputhje me parashikimet e nenit 2 dhe nenit 3, të Direktivës së Bashkimit Evropian 2014/65/BE;

e) shoqëritë e sigurimit, ndërmjetësit e risigurimeve dhe ndërmjetës sigurimi me veprimtari plotësuese që konsiderohen si mikro ndërmarrje ose ndërmarrje të vogla apo të mesme;

f) institucionet postare të transfertave (post office giro institutions) të parashikuara në nenin 2, paragrafi 5, pika 3, të Direktivës së Bashkimit Evropian 2013/36/BE.

4. Autoriteti mund të përjashtojë nga fusha e zbatimit të kësaj rregulloreje subjektet e përmendura në nenin 2, paragrafi 5, pikat 4 deri në 23, të Direktivës 2013/36/BE që ndodhen brenda territoreve të tyre përkatëse. Autoriteti 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 mjete të tjera lehtësisht të aksesueshme.

Neni 4
Përkufizime

Për qëllim të kësaj rregulloreje, termat e mëposhtëm kanë kuptimin si vijon:

1. **"Qëndrueshmëri operacionale digjitale"** – është aftësia e një subjekti financiar për të ndërtuar, garantuar dhe rishikuar integritetin dhe besueshmërinë e tij operacionale, duke siguruar, drejtpërdrejt ose tërthorazi, përmes përdorimit të shërbimeve të ofruara nga ofrues të shërbimeve TIK palë të treta, gamën e plotë të kapaciteteve të lidhura me TIK-un, të nevojshme për të adresuar sigurinë e rrjeteve dhe të sistemeve të informacionit që përdor një subjekt financiar dhe që mbështesin ofrimin e vazhdueshëm të shërbimeve financiare dhe cilësinë e tyre, përfshirë gjatë ndërprerjeve;

2. **"Rrjet dhe sistem informacioni"** – është një rrjet dhe sistem informacioni, siç përcaktohet në ligjin "Për sigurinë kibernetike";

3. **“Sistem TIK i trashëguar (legacy)”** – është një sistem TIK që ka arritur fundin e ciklit të tij jetësor (*end-of-life*), që nuk është më i përshtatshëm për përmirësime ose rregullime për arsye teknologjike ose tregtare, ose që nuk mbështetet më nga furnizuesi i tij apo nga një ofrues i shërbimeve TIK i palës së tretë, por që ende është në përdorim dhe mbështet funksionet e subjektit financiar;

4. **“Siguria e rrjeteve dhe sistemeve të informacionit”** – është siguria e rrjetit dhe sistemeve të informacionit, siç përcaktohet në ligjin “Për sigurinë kibernetike”;

5. **“Rrezik TIK”** – është çdo rrethanë që mund të identifikohet në mënyrë të arsyeshme në lidhje me përdorimin e rrjeteve dhe sistemeve të informacionit, e cila, nëse materializohet, mund të kompromet ojë sigurinë e rrjeteve dhe të sistemeve të informacionit, të çdo mjeti ose procesi që varet nga teknologjia, të operacioneve dhe proceseve, ose të ofrimit të shërbimeve duke prodhuar efekte të pafavorshme në mjedisin digjital ose fizik;

6. **“Aset informacioni”** – është informacioni, pavarësisht nga forma, formati apo mjeti në të cilin ruhet, i cili ka vlerë për subjektin financiar dhe duhet mbrojtur nga qasja, përdorimi ose dëmtimi i paautorizuar.

7. **“Aset TIK”** – çdo komponent softuerik ose harduerik, përfshirë infrastrukturën dhe burimet e rrjetit, që përdoret për funksionimin e sistemeve të informacionit të subjektit financiar.

8. **“Incident i lidhur me TIK”** – është çdo ngjarje e paparashikuar që vë në rrezik sigurinë e rrjeteve dhe sistemeve të informacionit dhe që ka ndikim negativ mbi disponueshmërinë, integritetin, origjinalitetin ose konfidencialitetin e të dhënave ose në shërbimet e ofruara nga subjekti financiar;

9. **“Incident madhor i lidhur me TIK”** – është një incident i lidhur me TIK-un që ka një ndikim të lartë të pafavorshëm në rrjetet dhe sistemet e informacionit që mbështesin funksione kritike ose të rëndësishme të subjektit financiar;

10. **“Kërcënim kibernetik”** – është çdo ngjarje, veprim ose rrethanë e mundshme, e cila ka potencialin të dëmtojë, të ndërpresë, të kompromet ojë ose të ndikojë në mënyrë të pafavorshme në funksionimin, konfidencialitetin, integritetin ose disponueshmërinë e rrjeteve dhe sistemeve të informacionit, si dhe të cenojë sigurinë e përdoruesve apo të personave të tjerë të lidhur me to, sipas legjislacionit në fuqi “Për sigurinë kibernetike”;

11. **“Kërcënim i rëndësishëm kibernetik”** – është një kërcënim kibernetik, karakteristikat teknike të të cilit tregojnë se ai mund të ketë potencialin për të shkaktuar një incident madhor të lidhur me TIK-un ose një incident madhor operativ ose të sigurisë;

12. **“Sulm kibernetik”** – është një incident ose çdo rrethanë, ngjarje ose veprim i mundshëm që mund të dëmtojë, ndërpresë ose në mënyra të tjera të ndikojë negativisht në sistemet e rrjeteve dhe informacionit, në përdoruesit e këtyre sistemeve dhe tek personat e tjerë;

13. **“Inteligjencë kërcënimi”** ***(threat intelligence)*** – është informacioni që është grupuar, transformuar, analizuar, interpretuar ose pasuruar për të ofruar kontekstin e nevojshëm për marrjen e vendimeve dhe për të mundësuar një kuptimin me qëllim zbutjen e ndikimit të një incidenti të lidhur me TIK-un ose të një kërcënimi kibernetik, duke përfshirë detajet teknike të një sulmi kibernetik, autorët e tij, mënyrën e veprimit (*modus operandi*) dhe motivin.

14. **“Cënueshmëri”** – është një dobësi ose mangësi mbrojtjeje ose mangësi të një aseti, sistemi, procesi ose kontrolli që mund të shfrytëzohet;

15. **“Plan masash korrigjuese”** është dokumenti i hartuar nga subjekti financiar pas identifikimit të dobësive, mangësive ose incidenteve TIK, i cili përcakton:

    a) masat teknike dhe organizative që do të ndërmerren;

    b) prioritetin e zbatimit në bazë të nivelit të rrezikut;

    c) afatet kohore për realizimin e tyre;

    d) përgjegjësitë përkatëse;

    e) mekanizmat e monitorimit dhe raportimit të progresit.

16. **“Strategji daljeje”** është plani i dokumentuar i subjektit financiar për ndërprerjen e rregullt, të sigurt dhe pa ndërprerje materiale të marrëdhënies kontraktuale me një ofrues shërbimi të TIK, përfshirë masat për transferimin e shërbimeve te një ofrues alternativ ose rikthimin e tyre brenda subjektit, si dhe procedurat për mbrojtjen e të dhënave, vazhdimësinë operacionale dhe minimizimin e rrezikut.

17. **“Testim i depërtimit i ndikuar nga kërcënimi (*TLPT*)”** – është një kuadër testimi që imiton taktikat, teknikat dhe procedurat e aktorëve kërcënues realë, të perceptuar si paraqitës të një kërcënimi të vërtetë kibernetik, i cili realizon një test të kontrolluar, të përshtatur dhe të bazuar në inteligjencë (*red team*) mbi sistemet kritike operative të subjektit financiar në mjedisin e tij të prodhimit;

18. “**Red team**” janë testues të brendshëm ose të jashtëm të kontraktuar ose të caktuar për kryerjen e testeve *TLTP*;

19. “**Testues i pavarur**” është personi fizik ose juridik, i brendshëm ose i jashtëm, që kryen testime të qëndrueshmërisë operacionale dixhitale, përfshirë testime të bazuara në kërcënime (*Threat-Led Penetration Testing – TLPT*), i cili:

    a) është funksionalisht i ndarë nga zhvillimi, operimi dhe administrimi i sistemeve që teston;

    b) nuk ndodhet në konflikt interesi;

    c) zotëron kualifikimet, ekspertizën teknike dhe përvojën e nevojshme;

    d) vepron në përputhje me standarde profesionale dhe kërkesa të sigurisë së informacionit.

20. **“Rrezik TIK i palës së tretë”** nënkupton një rrezik TIK që mund të lindë për një subjekt financiar në lidhje me përdorimin e shërbimeve TIK të ofruara nga ofruesit e shërbimeve TIK të palëve të treta ose nga nënkontraktorët e këtyre të fundit, përfshirë përmes një marrëveshje nënkontraktimi *(outsourcing);*

21. **“Ofrues i shërbimeve TIK i palëve të treta”** – person juridik i cili ofron shërbime TIK për subjektet financiare në bazë të një marrëveshjeje kontraktuale.

22. **“Ofrues i shërbimeve TIK brenda grupit”** – është një shoqëri që është pjesë e një grupi financiar dhe që ofron kryesisht shërbime TIK për subjektet financiare brenda të njëjtit grup ose për subjektet financiare që i përkasin të njëjtit skemë mbrojtjeje institucionale, përfshirë shoqëritë mëmë, shoqëritë bija, degët ose entitete të tjera që janë nën të njëjtën pronësi ose kontroll;

23. **“Zinxhir furnizimi TIK”** është një sekuencë marrëveshjesh kontraktuale të lidhura me shërbimin TIK, që i ofrohet subjektit financiar nga ofruesi i drejtpërdrejtë i shërbimeve TIK palë e tretë, duke filluar nga ofruesi i drejtpërdrejtë, i cili ka një ose disa ofrues të tjerë të shërbimeve TIK të nënkontraktuara;

24. **“Rradha (*rank*)”** është pozicioni i një ofruesi të shërbimeve të TIK palë e tretë në zinxhirin e furnizimit me shërbime të TIK;"

25. **“Shërbime TIK”** – janë shërbime digjitale dhe të dhënash të ofruara përmes sistemeve TIK për një ose më shumë përdorues të brendshëm ose të jashtëm në mënyrë të vazhdueshme, duke përfshirë “*hardware as a service*” dhe shërbimet harduerike që përfshijnë ofrimin e mbështetjes teknike përmes përditësimeve të softuerit ose firmware-it nga ofruesi i pajisjes harduerike, duke përjashtuar shërbimet tradicionale të telefonisë analoge;

26. **“Funksion kritik ose i rëndësishëm”** – është një funksion, ndërprerja e të cilit do të ndikonte ndjeshëm në performancën financiare të një subjekti financiar, ose në qëndrueshmërinë ose vazhdimësinë e shërbimeve dhe veprimtarive të tij, ose ndërprerja, dështimi apo kryerja me mangësi e atij funksioni do të ndikonte ndjeshëm në pajtueshmërinë e vazhdueshme të subjektit financiar me kushtet dhe detyrimet e autorizimit të tij, ose me detyrime të tjera sipas legjislacionit përkatës të shërbimeve financiare;

27. **“Ofrues kritik i shërbimeve TIK, palë e tretë”** – është ofruesi i shërbimeve TIK i përcaktuar si kritik nga AMF, në përputhje me nenin 57, të kësaj rregulloreje.

28. **“Ofrues i shërbimeve TIK i themeluar në një shtet të tretë”** – është një person juridik i regjistruar jashtë territorit të Republikës së Shqipërisë, që ofron shërbime TIK për një subjekt financiar vendas sipas një marrëveshje kontraktuale.

29. **“Shoqëri bijë”**– ka kuptimin e përcaktuar në ligjin “Për tregtarët dhe shoqëritë tregtare”;

30. **“Grup”** – është shoqëria mëmë dhe të gjitha filialet e saj, sipas kuptimit të ligjit “Për shoqëritë tregtare;

31. **“Shoqëri mëmë”** – sipas përcaktimeve në ligjin “Për tregtaret dhe shoqëritë tregtare”;

32. **“Nënkontraktor TIK i themeluar në një shtet të tretë”** – është personi juridik i regjistruar jashtë territorit shqiptar, i cili ka lidhur një marrëveshje kontraktuale ose me një ofrues të shërbimeve TIK të palës së tretë, ose me një ofrues të tillë të vendosur në një vend tjetër;

33. **“Rrezik i përqendrimit TIK”** – është një ekspozim ndaj një ose disa ofruesve kritikë të shërbimeve TIK të ndërlidhur, që krijon një shkallë varësie nga këta ofrues, në mënyrë të tillë që pamundësia, dështimi ose çdo lloj tjetër mos përmbushjeje nga ana e një ofruesi mund të rrezikojë potencialisht aftësinë e një subjekti financiar për të ofruar funksione kritike ose të rëndësishme ose mund t’i shkaktojë pasoja të tjera të pafavorshme, përfshirë humbje të mëdha, ose të rrezikojë stabilitetin financiar të Bashkimit në tërësi;

34. **“Organ drejtues”** nënkupton organin drejtues të subjektit financiar sipas përkufizimit të dhënë në legjislacionin në fuqi, ose personat që drejtojnë realisht subjektin ose ushtrojnë funksione kyçe në përputhje me legjislacionin përkatës.

35. **“Ofrues i shërbimeve të raportimit të të dhënave’** është ofruesi i shërbimeve të raportimit të të dhënave, sipas kuptimit dhe përcaktimeve të dhëna në nenin 2, paragrafi 1, pikat 34 deri në 36, të Rregullores (BE) Nr. 600/2014;"

36. **“Mikrondërmarrje”** – është subjekti financiar, përveç një vendi tregtimi, një ndërmjetësi shlyerjeje qendrore, një regjistri tregtimi ose një depozitari qendror të letrave me vlerë, që punëson më pak se 10 persona dhe ka një xhiro vjetore dhe/ose totali i bilancit vjetor nuk kalon vlerën ekuivalentë në lekë të 2 milionë euro;

37. “**Mbikëqyrësi Kryesor** (*Lead Overseer*) – është Autoritetin Mbikëqyrës Evropian të emëruar në përputhje me nenin 59, pika 1, shkronja “b”, të kësaj rregulloreje;

38. **‘Komiteti i Përbashkët’** nënkupton komitetin e referuar në nenin 54, të Rregulloreve (BE) Nr. 1093/2010, (BE) Nr. 1094/2010 dhe (BE) Nr. 1095/2010;

39. **“Ndërmarrje e vogël”** – është subjekti financiar që punëson të paktën 10 por jo më shumë se 50 persona, dhe që ka një xhiro vjetore dhe/ose total bilanci vjetor tejkalon vlerën ekuivalente në lekë të 2 milionë euro, por nuk tejkalon vlerën ekuivalente në lekë të 10 milionë euro;

40. **“Ndërmarrje e mesme”** – është subjekti financiar që nuk konsiderohet si ndërmarrje e vogël, që punëson më pak se 250 persona dhe ka një qarkullim vjetor që nuk kalon vlerën ekuivalente në lekë të 50 milionë euro dhe/ose një total bilanci vjetor që nuk kalon vlerën ekuivalente në lekë të 43 milionë euro;

41. **“Autoriteti përgjegjës”** në zbatim të kësaj rregulloreje, është Autoriteti i Mbikëqyrjes Financiare;

42. “**AKSK**” -është Autoriteti Kombëtar për Sigurinë Kibernetike;

Neni 5
Parimi i proporcionalitetit

1. Subjektet financiare zbatojnë rregullat e përcaktuara në Kreun II, të kësaj rregulloreje në përputhje me parimin e proporcionalitetit, duke marrë në konsideratë madhësinë e tyre, profilin e përgjithshëm të rrezikut, si dhe natyrën, përmasat dhe kompleksitetin e shërbimeve, veprimtarive dhe operacioneve që ato kryejnë.

2. Subjektet financiare zbatojnë dispozitat e Kreut III, IV, dhe Kreut V, Seksioni I, në mënyrë proporcionale me madhësinë, profilin e përgjithshëm të rrezikut, si dhe natyrën, përmasat dhe kompleksitetin e shërbimeve, veprimtarive dhe operacioneve të tyre, sipas përcaktimeve të parashikuara në këta kapituj.

3. Autoriteti i Mbikëqyrjes Financiare, bazuar në raportet e paraqitura nga subjektet financiare, me kërkesë të tij, sipas nenit 7, pika 5 dhe nenin 17, pika 2, të kësaj rregulloreje, merr në konsideratë zbatimin e parimit të proporcionalitetit nga subjektet financiare, gjatë vlerësimit të përputhshmërisë së kuadrit të menaxhimit të rrezikut TIK.

KREU II
MENAXHIMI I RREZIKUT TIK

Seksioni I
Qeverisja dhe organizimi i subjekteve financiare

Neni 6
Qeverisja dhe organizimi

1. Me qëllim sigurimin e një niveli të lartë qëndrueshmërie operacionale digjitale, subjektet financiare duhet të miratojnë rregulla të brendshme për qeverisjen dhe kontrollin, që garantojnë menaxhim efektiv dhe të kujdesshëm të rrezikut TIK, në përputhje me nenin 7, pika 4.

2. Organi drejtues i subjektit financiar përcakton, miraton, mbikëqyr dhe është përgjegjës për zbatimin e të gjitha masave që lidhen me menaxhimin e rrezikut TIK, të përmendur në nenin 7, pika 1. Për këtë qëllim, organi drejtues:

    a) është përgjegjës për menaxhimin e rrezikut TIK të subjektit financiar;
    b) miraton politika që synojnë garantimin e standardeve të larta të disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave;
    c) përcakton role dhe përgjegjësi të qarta për të gjitha funksionet që lidhen me TIK dhe vendos mekanizma të përshtatshëm të qeverisjes për të siguruar komunikim, bashkëpunim dhe koordinim efektiv dhe në kohë midis këtyre funksioneve;
    d) është përgjegjës për përcaktimin dhe miratimin e strategjisë së qëndrueshmërisë operacionale digjitale, siç parashikohet në nenin 7, pika 8, shkronja "b" duke përfshirë përcaktimin e nivelit të tolerancës ndaj rrezikut TIK të subjektit financiar;
    e) miraton, mbikëqyr dhe shqyrton periodikisht zbatimin e politikës së vazhdimësisë së biznesit për TIK dhe planeve të reagimit dhe rikuperimit nga incidentet TIK, të parashikuara përkatësisht në nenin 12, pika 1 dhe pika 3, të cilat mund të adoptohen si politika të dedikuara specifike, pjesë përbërëse e politikës së përgjithshme të vazhdimësisë së biznesit;
    f) miraton dhe shqyrton periodikisht planet e auditimit të brendshëm TIK, auditimet TIK dhe ndryshimet thelbësore në to;
    g) përcakton dhe rishikon periodikisht buxhetin e përshtatshëm për përmbushjen e nevojave të subjektit financiar në fushën e qëndrueshmërisë operacionale digjitale, për të gjitha llojet e burimeve, përfshirë programet e paralajmërimit mbi sigurinë TIK dhe trajnimet mbi qëndrueshmërinë operacionale digjitale, sipas parashikimit në nenin 15, pika 6, si dhe zhvillimin e aftësive TIK për të gjithë punonjësit;
    h) miraton dhe shqyrton periodikisht politikat e subjektit financiar për marrëveshjet që lidhen me përdorimin e shërbimeve TIK të ofruara nga palët e treta;
    i) vendos, në nivel grupi, kanale raportimi që informojnë në mënyrë të rregullt mbi:
        i. marrëveshjet e lidhura me ofruesit e shërbimeve TIK palë të treta për përdorimin e shërbimeve të tyre,

ii. çdo ndryshim thelbësor të planifikuar që lidhet me ofruesit e shërbimeve TIK palë të treta,
iii. ndikimin e mundshëm të këtyre ndryshimeve mbi funksionet kritike ose të rëndësishme që mbulohen nga këto marrëveshje, përfshirë një përmbledhje të analizës së rrezikut për vlerësimin e ndikimit të tyre, si dhe të paktën mbi incidentet madhore të lidhura me TIK dhe ndikimin e tyre, si dhe masat e marra për reagim, rikuperim dhe korrigjim.

3. Subjektet financiare, me përjashtim të mikrondërmarrjeve, caktojnë një funksion ose person përgjegjës, të dedikuar për monitorimin e marrëveshjeve të lidhura me përdorimin e shërbimeve TIK të ofruara nga palët e treta, ose caktojnë një anëtar të organeve të larta drejtuese si përgjegjës për mbikëqyrjen e ekspozimit ndaj rrezikut përkatës dhe dokumentacionin përkatës.

4. Anëtarët e organit drejtues të subjektit financiar, duhet të përditësojnë vazhdimisht njohuritë dhe aftësitë e tyre për të kuptuar dhe vlerësuar rrezikun TIK dhe ndikimin e tij mbi operacionet e subjektit financiar, përfshirë ndjekjen periodike të trajnimeve të posaçme, në përpjesëtim me nivelin e rrezikut TIK që menaxhohet.

Seksioni II
Kuadri i Menaxhimit të Rrezikut të TIK

Neni 7
Kuadri i menaxhimit të rrezikut të TIK

1. Subjektet financiare, duhet të kenë një kuadër të qëndrueshëm, gjithëpërfshirës dhe të mirë dokumentuar të menaxhimit të rrezikut TIK, si pjesë e sistemit të tyre të përgjithshëm të menaxhimit të rrezikut, i cili u mundëson atyre të adresojnë rreziqet TIK në mënyrë të shpejtë, efikase dhe të plotë, si dhe të sigurojnë një nivel të lartë të qëndrueshmërisë operacionale digjitale.

2. Kuadri i menaxhimit të rrezikut TIK, sipas pikës 1 të këtij neni, duhet të përfshijë të paktën strategjitë, politikat, procedurat, protokollet dhe mjetet TIK që janë të nevojshme për të mbrojtur në mënyrë të rregullt dhe të përshtatshme të gjitha asetet e informacionit dhe asetet TIK. Kuadri i menaxhimit të rrezikut TIK përfshin gjithashtu programe kompjuterike, pajisje harduerike, servera, si dhe infrastrukturat fizike përkatëse, si ambiente, qendrat e të dhënave dhe zona të ndjeshme të përcaktuara, për të garantuar mbrojtjen e tyre nga rreziqe të ndryshme, përfshirë dëmtimet dhe qasjet ose përdorimet e paautorizuara.

3. Në përputhje me kuadrin e menaxhimit të rrezikut TIK, subjektet financiare duhet të minimizojnë ndikimin e rrezikut TIK duke zbatuar strategji, politika, procedura, protokolle dhe mjete të përshtatshme TIK. Me kërkesë të Autoritetit subjektet financiare duhet të vënë në dispozicion, informacion të plotë dhe të përditësuar mbi rrezikun TIK dhe kuadrin e menaxhimit të këtij rreziku.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, i caktojnë funksionit të kontrollit, përgjegjësinë për menaxhimin dhe mbikëqyrjen e rrezikut të TIK dhe sigurojnë një nivel të përshtatshëm të pavarësisë të këtij funksioni për të shmangur konfliktin e interesit. Subjektet financiare duhet të garantojnë ndarjen dhe pavarësinë midis funksioneve të menaxhimit të rrezikut TIK, funksioneve të kontrollit dhe atyre të auditimit të brendshëm, në përputhje me modelin e "tre linjave të mbrojtjes".

5. Kuadri i menaxhimit të rrezikut TIK duhet të dokumentohet dhe të rishikohet të paktën një herë në vit, ose periodikisht në rastin e mikrondërmarrjeve, dhe në çdo rastkur ndodhin incidente madhore të lidhura me TIK-un, si dhe në përputhje me rekomandimet mbikëqyrëse ose pas rezultateve që dalin nga testimet ose auditimet përkatëse të qëndrueshmërisë digjitale operacionale. Ky kuadër duhet të përmirësohet vazhdimisht mbi bazën e zbatimit dhe monitorimit të tij. Autoritetit, me kërkesë të tij duhet t'i paraqitet një raport mbi rishikimin e kuadrit të menaxhimit të rrezikut TIK.

6. Kuadri i menaxhimit të rrezikut TIK i subjekteve financiare, me përjashtim të mikrondërmarrjeve, i nënshtrohet auditimit të brendshëm në mënyrë të rregullt, sipas planit të auditimit të subjektit financiar. Audituesit duhet të kenë njohuri, pavarësi, aftësi dhe ekspertizë të mjaftueshme në fushën e rrezikut TIK. Frekuenca dhe fokusi i auditimeve TIK duhet të jenë në përpjesëtim me nivelin e rrezikut TIK të subjektit financiar.

7. Bazuar në gjetjet e auditimeve të brendshme, subjektet financiare vendosin një proces formal ndjekjeje, duke përfshirë rregulla për verifikimin në kohë dhe korrigjimin e gjetjeve kritike të auditimit TIK.

8. Kuadri i menaxhimit të rrezikut TIK duhet të përfshijë një strategji për qëndrueshmërinë operacionale digjitale, e cila përcakton mënyrën e zbatimit të këtij kuadrit. Strategjia duhet të përfshijë metodat për adresimin e rrezikut TIK dhe për arritjen e objektivave specifike, duke:

    a) shpjeguar se si kuadri i menaxhimit të rrezikut TIK mbështet strategjinë dhe objektivat e veprimtarisë së subjektit financiar;

    b) përcaktuar nivelin e tolerancës ndaj rrezikut TIK, në përputhje me nivelin e gatishmërisë për të pranuar rrezikun e subjektit financiar, dhe analizuar tolerancën ndaj ndikimit nga ndërprerjet TIK;

    c) vendosur objektiva të qarta për sigurinë e informacionit, përfshirë treguesit kyç të performancës dhe treguesit kyç të rrezikut;

    d) shpjeguar arkitekturën e TIK dhe çdo ndryshim të nevojshëm për të arritur objektiva të caktuara të veprimtarisë;

    e) përcaktuar mekanizmat e ndryshëm të vendosur për të zbuluar incidentet e lidhura me TIK, për të parandaluar ndikimin e tyre dhe për të siguruar mbrojtje prej tyre;

    f) paraqitur situatën aktuale të qëndrueshmërisë operacionale digjitale mbi bazën e numrit të incidenteve madhore të raportuara që lidhen me TIK dhe efektivitetit të masave parandaluese;

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

    h) përcaktuar një strategji komunikimi në rast incidentesh të lidhura me TIK, publikimi i të cilave kërkohet në përputhje me nenin 16, të kësaj rregulloreje.

9. Subjektet financiare, në kuadër të strategjisë së qëndrueshmërisë operacionale digjitale të parashikuar në pikën 8, të këtij neni mund të përcaktojnë një strategji gjithëpërfshirëse TIK me shumë ofrues *"multi-vendor strategy",* në nivel grupi ose subjekti, duke treguar varësitë

kryesore nga ofruesit e shërbimeve TIK, palë të treta dhe duke shpjeguar arsyetimin e përzierjes së përdorimit të tyre.

10. Subjektet financiare, në përputhje me legjislacionin në fuqi, mund të delegojnë me kontraktim detyrën e verifikimit të përputhshmërisë me kërkesat e menaxhimit të rrezikut TIK tek një subjekt brenda grupit ose një subjekt i jashtëm. Në çdo rast subjekti financiar mbetet plotësisht përgjegjës për verifikimin e përputhjes me kërkesat e menaxhimit të rrezikut TIK.

Neni 8
Sistemet, protokollet dhe mjetet e TIK

1. Për të adresuar dhe menaxhuar rrezikun TIK, subjektet financiare duhet të përdorin dhe të mirëmbajnë sisteme, protokolle dhe mjete TIK të përditësuara, të cilat janë:

   a) të përshtatshme me madhësinë e operacioneve që mbështesin kryerjen e veprimtarive të tyre, në përputhje me parimin e proporcionalitetit, siç parashikohet në nenin 5, të kësaj rregullore;

   b) të besueshme;

   c) të pajisura me kapacitete të mjaftueshme për të përpunuar në mënyrë të saktë të dhënat e nevojshme për kryerjen e veprimtarive dhe ofrimin në kohë të shërbimeve, si dhe për të përballuar flukset maksimale, mesazheve ose transaksioneve, sipas nevojës, përfshirë edhe rastet kur futet një teknologji e re;

   d) teknologjikisht të qëndrueshme, me qëllim që të përballojnë në mënyrë të përshtatshme nevojat shtesë për përpunimin e informacionit që kërkohen në kushte të tensionuara tregu ose situata të tjera të pafavorshme.

Neni 9
Identifikimi

1. Subjektet financiare, në kuadër të menaxhimit të rrezikut TIK të përmendur në nenin 7, pika 1, të kësaj rregulloreje identifikojnë, klasifikojnë dhe dokumentojnë në mënyrë të përshtatshme të gjitha funksionet e veprimtarisë të mbështetura nga TIK, rolet dhe përgjegjësitë përkatëse, asetet e informacionit dhe asetet TIK që mbështesin këto funksione, si dhe rolin dhe varësitë e tyre në lidhje me rrezikun TIK. Subjektet financiare shqyrtojnë, sipas nevojës dhe jo më pak se një herë në vit, mjaftueshmërinë e këtij klasifikimi dhe çdo dokumentacioni përkatës.

2. Subjektet financiare, në mënyrë të vazhdueshme, identifikojnë të gjitha burimet e rrezikut TIK, në veçanti ekspozimin ndaj dhe nga subjektet e tjera financiare, si dhe vlerësojnë kërcënimet kibernetike dhe cenueshmëritë TIK që lidhen me funksionet e veprimtarisë të mbështetura nga TIK, asetet e informacionit dhe asetet TIK. Subjektet financiare shqyrtojnë herë pas here, jo më pak se një herë në vit, skenarët e rrezikut që prekin subjektet financiare.

3. Subjektet financiare, me përjashtim të mikrondërmarrjeve, kryejnë një vlerësim të rrezikut sa herë që ndodh një ndryshim madhor në infrastrukturën e rrjeteve dhe sistemeve të

informacionit, në proceset ose procedurat që ndikojnë funksionet e veprimtarisë të mbështetura nga TIK-u, asetet e informacionit ose asetet TIK.

4. Subjektet financiare, identifikojnë të gjitha asetet e informacionit dhe asetet TIK, përfshirë ato në vendndodhje të largëta, burimet e rrjetit dhe pajisjet kompjuterike *hardware*, dhe dokumentojnë ato që konsiderohen kritike. Ato duhet identifikojnë dhe dokumentojnë konfigurimin e aseteve të informacionit dhe aseteve TIK, si lidhjet dhe varësitë ndërmjet tyre.

5. Subjektet financiare, duhet identifikojnë dhe dokumentojnë të gjitha proceset që varen nga ofruesit e shërbimeve TIK palë të treta dhe evidentojnë ndërveprimet me ofruesit e shërbimeve TIK palë të treta , të cilët ofrojnë shërbime që mbështesin funksione kritike ose të rëndësishme.

6. Për qëllimet e pikave 1, 4 dhe 5, të këtij neni, subjektet financiare duhet të mbajnë regjistrat përkatës dhe t'i përditësojnë ato periodikisht dhe sa herë ndodh një ndryshim madhor, sipas përcaktimit në pikën 3, të këtij neni.

7. Subjektet financiare, me përjashtim të mikrondërmarrjeve, rregullisht dhe jo më pak se një herë në vit, kryejnë një vlerësim specifik të rrezikut TIK për të gjitha sistemet e trashëguara "*legacy*", dhe në çdo rast 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 dhe me synim organizimin e masave të reagimit, subjektet financiare monitorojnë dhe kontrollojnë vazhdimisht sigurinë, funksionimin e sistemeve dhe mjeteve të TIK, duke minimizuar ndikimin e rrezikut të TIK mbi to, përmes përdorimit të mjeteve, politikave dhe procedurave të përshtatshme të sigurisë TIK.

2. Subjektet financiare hartojnë, sigurojnë dhe zbatojnë politika, procedura, protokolle dhe mjete sigurie për TIK që synojnë të garantojnë qëndrueshmërinë, vazhdimësinë dhe disponueshmërinë e sistemeve të TIK, veçanërisht për ato që mbështesin funksione kritike ose të rëndësishme, si dhe ruajnë standarde të larta të disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave, kur këto ndodhen në gjendje pushimi (*stand by*), në përdorim (*in use*) ose në tranzit (*in transit).*

3. Për arritjen e objektivave të përmendura në pikën 2, të këtij neni subjektet financiare përdorin zgjidhje dhe procese TIK të përshtatshme, në përputhje me parimin e proporcionalitetit të parashikuar në nenin 5, të kësaj rregulloreje. Këto zgjidhje dhe procese duhet të:

   a) garantojnë sigurinë e mjeteve të transferimit të të dhënave;

   b) minimizojnë rrezikun e dëmtimit ose humbjes së të dhënave, aksesit të paautorizuar dhe defekteve teknike që mund të pengojnë veprimtarinë e subjektit;

   c) parandalojnë mungesën e disponueshmërisë, cenimin e origjinalitetit dhe integritetit, shkeljet e konfidencialitetit dhe humbjen e të dhënave;

d) sigurojnë mbrojtjen e të dhënave nga rreziqet që burojnë nga menaxhimi i tyre, përfshirë administrimin e dobët, rreziqet lidhur me përpunimin dhe gabimet njerëzore.

4. Si pjesë e kuadrit të menaxhimit të rrezikut TIK, të parashikuar në nenin 7, pika 1**,** subjektet financiare duhet të:

a) hartojnë dhe dokumentojnë një politikë sigurie të informacionit që përcakton rregulla për mbrojtjen e disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave, aseteve të informacionit dhe aseteve TIK, përfshirë edhe ato të klientëve, kur është e aplikueshme;

b) ndjekin një qasje të bazuar në rrezik, krijojnë një strukturë të menaxhimit të rrjetit dhe infrastrukturës, duke përdorur teknika, metoda dhe protokolle të përshtatshme, që mund të përfshijnë zbatimin e mekanizmave të automatizuar për izolimin e aseteve të informacioni të prekura, në rast sulmesh kibernetike;

c) zbatojnë politika që kufizojnë qasjen fizike ose logjike në asetet e informacionit dhe asetet TIK vetëm në atë që kërkohet për funksione dhe veprimtari legjitime dhe të miratuara, dhe për këtë qëllim vendosin politika, procedura dhe kontrolle që trajtojnë të drejtat e qasjes dhe sigurojnë mirë administrimin e tyre;

d) zbatojnë politika dhe protokolle për mekanizma të fortë autentifikimi, bazuar në standardet përkatëse dhe sisteme kontrolli të dedikuara, si dhe masa mbrojtëse për çelësat kriptografikë, ku të dhënat enkriptohen në bazë të rezultateve të proceseve të klasifikimit të të dhënave dhe të vlerësimit të rrezikut TIK;

e) zbatojnë politika, procedura dhe kontrolle të dokumentuara për menaxhimin e ndryshimeve TIK, përfshirë ndryshimet në *software*, *hardware*, komponentë *firmëare*, sisteme ose parametra sigurie, të bazuara në një qasje të vlerësimit të rrezikut dhe të integruara si pjesë e procesit të përgjithshëm të menaxhimit të ndryshimeve të subjektit financiar, me qëllim garantimin që të gjitha ndryshimet në sistemet TIK regjistrohen, testohen, vlerësohen, miratohen, zbatohen dhe verifikohen në mënyrë të kontrolluar;

f) kanë politika të dokumentuara të përshtatshme dhe gjithëpërfshirëse për rishikimet (*patch-et)* dhe përditësimet.

Për qëllimet të pikës 4, shkronja "b", të këtij neni, subjektet financiare projektojnë infrastrukturën e lidhjes së rrjetit në mënyrë që të mund të lejojë ndarjen dhe segmentimin e saj në mënyrë të menjëhershme, për të minimizuar dhe parandaluar përhapjen e rrezikut, veçanërisht për proceset financiare të ndërlidhura.

Për qëllimet të pikës 4, shkronja "e", të këtij neni, procesi i menaxhimit të ndryshimeve TIK miratohet nga organet drejtuese përkatëse dhe duhet të ketë protokolle specifike në fuqi.

Subjektet financiare zbatojnë mekanizma të automatizuar dhe të vazhdueshëm për zbulimin e anomalive dhe sinjalizimin e hershëm të incidenteve të mundshme të TIK, duke përfshirë analiza të sjelljeve të përdoruesve dhe monitorim të trafikut rrjetor. Këto mekanizma duhet të jenë në përputhje me rreziqet dhe funksionet kritike të subjektit dhe të integrohen si pjesë e kontrolleve të vazhdueshme të sigurisë.

Neni 11
Zbulimi

1. Subjektet financiare, duhet të kenë në funksion mekanizma për zbulimin e menjëhershëm të aktiviteteve anormale, në përputhje me nenin 18, përfshirë problemet e performancës së rrjeteve të TIK dhe incidentet e lidhura me TIK, si dhe për identifikimin e pikave të vetme kritike të dështimit "*single points of failure*".

   Subjektet financiare testojnë rregullisht të gjithë mekanizmat e zbulimit, në përputhje me nenin 41, të kësaj rregulloreje.

2. Mekanizmat e zbulimit të parashikuara në pikën 1, të këtij neni duhet të mundësojnë disa faza kontrolli, të përcaktojnë pragje dhe kritere sinjalizimi për aktivizimin dhe nisjen e proceseve të reagimit ndaj incidenteve të lidhura me TIK, përfshirë mekanizmat automatikë të njoftimit për personelin përkatës të ngarkuar me reagimin ndaj incidenteve të lidhura me TIK.

3 Subjektet financiare duhet të dedikojnë burime dhe kapacitete të mjaftueshme për monitorimin e aktivitetit të përdoruesve, shfaqjen e anomalive të TIK dhe incidenteve të lidhura me TIK, veçanërisht ndaj sulmeve kibernetike.

4 Përveç sa parashikohet në këtë nen, ofruesit e shërbimeve të raportimit të të dhënave duhet të kenë në funksion sisteme që verifikojnë në mënyrë efektive plotësinë e raporteve tregtare, të identifikojnë mungesat dhe gabimet e dukshme, si dhe të kërkojnë ri-transmetimin e këtyre raporteve.

Neni 12
Reagimi dhe rikuperimi

1. Subjektet financiare hartojnë një politikë gjithëpërfshirëse të vazhdimësisë së biznesit të TIK, si pjesë të kuadrit të menaxhimit të rrezikut të TIK të parashikuar në nenin 7, pika 1, të kësaj rregulloreje dhe bazuar në kërkesat e identifikimit të përcaktuara në nenin 9, të kësaj rregulloreje, e cila mund të miratohet si një politikë e veçantë, pjesë integrale e politikës së përgjithshme të vazhdimësisë së veprimtarisë së subjektit financiar.

2. Subjektet financiare, zbatojnë politikën për vazhdimësinë e biznesit për TIK përmes masave të dedikuara, të përshtatshme dhe të dokumentuara, planeve, procedurave dhe mekanizmave që synojnë:

   a) të sigurojnë vazhdimësinë e funksioneve kritike ose të rëndësishme të subjektit financiar;

   b) të reagojnë dhe të zgjidhin në mënyrë të shpejtë, të përshtatshme dhe efektive incidentet e lidhura me TIK, të minimizojnë dëmet dhe t'i japin përparësi rifillimit të aktiviteteve dhe veprimeve të rikuperimit;

   c) të aktivizojnë pa vonesë planet e dedikuara që mundësojnë masa izolimi, procese dhe teknologji të përshtatura për çdo lloj incidenti të lidhur me TIK dhe të parandalojnë dëme të mëtejshme, si dhe procedura të posaçme reagimi dhe rikuperimi të vendosura sipas nenit 14 të kësaj rregullore;

   d) të vlerësojnë paraprakisht ndikimet, dëmet dhe humbjet;

e) të përcaktojnë veprime komunikimi dhe menaxhimi të krizës, duke garantuar shpërndarjen e informacionit të përditësuar për të gjithë personelin e brendshëm dhe palët e jashtme të interesuara, në përputhje me nenin 16, si dhe raportimin tek Autoriteti, në përputhje me nenin 30.

3. Si pjesë e kuadrit të menaxhimit të rrezikut TIK të përmendur në nenin 7, pika 1, subjektet financiare, më përjashtim të mikrondërmarrjeve, zbatojnë planet për reagimin dhe rikuperimin nga incidentet të TIK, të cilat i nënshtrohen rishikimit të pavarur të auditit të brendshëm.

4. Subjektet financiare hartojnë, mirëmbajnë dhe testojnë periodikisht plane të përshtatshme të vazhdimësisë së biznesit për TIK, veçanërisht për funksionet kritike ose të rëndësishme të dhëna me kontratë ose të nënkontraktuara tek ofruesit e shërbimeve TIK, palë të treta.

5. Subjektet financiare, si pjesë e politikës së përgjithshme të vazhdimësisë së veprimtarisë, kryejnë një analizë të ndikimit në biznes *(ANB)* për ekspozimin e tyre ndaj ndërprerjeve të rënda të veprimtarisë. Në kuadër të analizës së ndikimit në biznes, subjektet financiare vlerësojnë ndikimin e mundshëm të ndërprerjeve të rënda të shërbimit, duke përdorur kritere sasiore dhe cilësore, si dhe të dhëna të brendshme e të jashtme dhe analiza të skenarëve, sipas rastit. Analiza e ndikimit në biznes duhet të marrë në konsideratë rëndësinë e funksioneve të biznesit të identifikuara dhe të përcaktuara, proceset mbështetëse, varësitë nga palët e treta dhe asetet e informacionit, si dhe ndërvarësitë e tyre. Subjektet financiare duhet të sigurojnë që asetet dhe shërbimet e TIK të projektohen dhe të përdoren në përputhje të plotë me analizën e ndikimit në biznes në veçanti për të garantuar praninë e kapaciteteve shtesë/rezervë për të gjithë komponentëve kritikë.

6. Si pjesë e menaxhimit gjithëpërfshirës të rrezikut TIK, subjektet financiare duhet të:

   a) testojnë planet e vazhdimësisë së biznesit të TIK, planet e reagimit dhe rikuperimit TIK, në lidhje me sistemet TIK që mbështesin të gjitha funksionet, të paktën një herë në vit, si dhe në rastet e ndryshimeve të rëndësishme në sistemet TIK që mbështesin funksione kritike ose të rëndësishme;

   b) testojnë planet e komunikimit në krizë, të parashikuara në nenin 16.

   Për qëllim të shkronjës "a", të pikës 6, subjektet financiare, me përjashtim të mikrondërmarrjeve përfshijnë në planet e testimit skenarë sulmesh kibernetike dhe kalimin ndërmjet infrastrukturës primare TIK dhe kapaciteteve rezervë, sistem rezervë *(backups)* dhe ambienteve shtesë/rezervë, të nevojshme për të përmbushur detyrimet e përcaktuara në nenin 14.

   Subjektet financiare rishikojnë rregullisht politikën e vazhdimësisë së biznesit për TIK dhe planet e reagimit dhe rikuperimit, duke marrë në konsideratë rezultatet e testeve të kryera sipas kësaj pike, si dhe rekomandimet që rrjedhin nga kontrollet e auditimit ose rishikimet mbikëqyrëse.

7. Subjektet financiare, me përjashtim të mikrondërmarrjeve duhet të kenë funksionin e menaxhimit të krizave, i cili, në rast të aktivizimit të planeve të vazhdimësisë së biznesit për TIK ose planeve të reagimit dhe rikuperimit, përcakton procedura të qarta për menaxhimin e komunikimeve të brendshme dhe të jashtme të krizës, në përputhje me nenin 16.

8. Subjektet financiare duhet të mbajnë të dhëna lehtësisht të aksesueshme për të gjitha aktivitetet para dhe gjatë ngjarjeve të ndërprerjeve, kur aktivizohen planet e vazhdimësisë së biznesit për TIK dhe planet e reagimit dhe rikuperimit.

9. Depozitarët qendrorë të titujve, vënë në dispozicion të Autoritetit kopje të rezultateve të testeve të vazhdimësisë së biznesit për TIK, ose të ushtrimeve të ngjashme.

10. Subjektet financiare, me përjashtim të mikrondërmarrjeve raportojnë pranë Autoritetit, me kërkesë të tij, vlerësimin e të gjitha kostove dhe humbjeve të akumuluara vjetore nga incidentet madhore të lidhura me TIK.

11. Autoriteti vlerëson kostot dhe humbjet të përvitshme të akumuluara, sipas parashikimeve të pikës 10, të këtij neni.

Neni 13
Vlerësimi i kostove dhe humbjeve të shkaktuara nga incidentet madhore të lidhura me TIK

1. Subjektet financiare duhet të vlerësojnë në përputhje me nenin 12, pika 11, të kësaj rregulloreje, kostot dhe humbjet vjetore të agreguara, të shkaktuara nga incidentet madhore të lidhura me TIK, duke përfshirë të gjitha kostot dhe humbjet që lidhen me incidentet madhore të TIK që kanë ndodhur brenda vitit referencë, për të cilin Autoriteti 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 vendos 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 Autoritetin, me kusht që Autoriteti 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, të cilat, pavarësisht shkakut, janë klasifikuar si madhore, në përputhje me seksionin 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 4, 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 4, 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, 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, pika 1 dhe 2, të kësaj rregulloreje;

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

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

4. Si bazë për vlerësimet, subjektet financiare duhet t'i 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 madhore të lidhur me TIK, që është përfshirë në agregim.

7. Subjektet financiare duhet të përdorin formularin në Aneksin 5, të kësaj rregulloreje, për të paraqitur në Autoritet 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 *backup-it* procedurat dhe metodat e rikthimit dhe rikuperimit

1. Për të siguruar rikthimin e sistemeve TIK dhe të dhënave me kohë sa më të shkurtër, me ndërprerje dhe humbje minimale, si pjesë e kuadrit të menaxhimit të rrezikut TIK, subjektet financiare hartojnë dhe dokumentojnë:

   a) politika dhe procedura *backup-i*, duke specifikuar llojin e të dhënave që i nënshtrohen *backup-it* dhe frekuencën minimale të tyre, bazuar në rëndësinë e informacionit ose nivelin e konfidencialitetit të të dhënave;

   b) procedura dhe metoda për rikthimin dhe rikuperimin.

2. Subjektet financiare, duhet të krijojnë sisteme *backup-i* që mund të aktivizohen në përputhje me politikat dhe procedurat përkatëse, si dhe me procedurat dhe metodat e rikthimit dhe rikuperimit. Aktivizimi i sistemeve të *backup-it* nuk duhet të cenojnë sigurinë e rrjeteve dhe sistemeve të informacionit, apo disponueshmërinë, origjinalitetin, integritetin dhe konfidencialitetin e të dhënave. Testimi i procedurave të sistemeve rezervë, si dhe i procedurave dhe metodave të rikthimit dhe rikuperimit, kryhet periodikisht.

3. Gjatë rikthimit të të dhënave nga *backup-i* përmes sistemeve të veta, subjektet financiare përdorin sisteme të TIK të ndara fizikisht dhe logjikisht nga sistemi burimor TIK. Këto sisteme duhet të jenë të mbrojtura në mënyrë të sigurt ndaj aksesit të paautorizuar ose korruptimit TIK dhe të mundësojnë rikthimin në kohë të shërbimeve përmes përdorimit të *backup-it* të të dhënave dhe sistemeve, sipas nevojës.

   Për Kundërpalën Qëndrore (central counterparties/CCP), planet e rikuperimit duhet të mundësojnë rikuperimin e të gjitha transaksioneve në momentin e ndërprerjes, në mënyrë që ato të vijojnë të operojnë me siguri dhe të përfundojnë shlyerjen në datën e planifikuar. Ofruesit e shërbimeve të raportimit të të dhënave, përveç kësaj, duhet të mirëmbajnë burime të përshtatshme dhe të kenë mundësi backup-i dhe riparimi, me qëllim që të ofrojnë dhe të ruajnë shërbimet e tyre në çdo kohë.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, mirëmbajnë kapacitete TIK shtesë/rezervë (*redundant*), të pajisura me burime, aftësi dhe funksione të përshtatshme për të garantuar nevojat e veprimtarisë. Mikrondërmarrjet vlerësojnë nevojën për të mirëmbajtur kapacitete shtesë/rezervë të TIK bazuar në profilin e tyre të rrezikut.
5. Depozitarët qendrorë të titujve duhet të mirëmbajnë të paktën një linjë dytësore përpunimi, e pajisur me burime, aftësi, funksione dhe staf të përshtatshëm për të garantuar nevojat e veprimtarisë. Qendra dytësore e përpunimit duhet të jetë:

   a) e pozicionuar në një distancë të tillë gjeografike nga qendra parësore e përpunimit, e cila garanton një profil të pavarur rreziku, si dhe parandalon cenimin e saj nga e njëjta ngjarje që prek qendrën parësore;

   b) e aftë të sigurojë vazhdimësinë e funksioneve kritike ose të rëndësishme në mënyrë identike me qendrën primare, ose të ofrojë nivelin e shërbimeve të nevojshme për të garantuar që subjekti financiar përmbush operacionet e tij kritike brenda objektivave të rikuperimit;

   c) e aksesueshme menjëherë nga stafi i subjektit financiar, për të garantuar vazhdimësinë e funksioneve kritike ose të rëndësishme në rast se qendra primare e përpunimit bëhet e papërdorshme.

6. Në përcaktimin e objektivave të kohës së rikuperimit (*RTO*) dhe të pikës së rikuperimit (*RPO*) për çdo funksion, subjektet financiare marrin në konsideratë nëse ai funksion është kritik ose i funksion rëndësishëm, si dhe me ndikim të mundshëm mbi efiçencën e tregut. Objektivat kohore duhet të sigurojnë që, edhe në skenarë ekstremë, të përmbushen nivelet e shërbimeve të dakordësuara.

7. Subjektet financiare, gjatë rikuperimit nga një incident i lidhur me TIK, kryejnë verifikimet e nevojshme, përfshirë kontrollet e shumëfishta dhe pajtimet

(*reconciliations)*, për të garantuar ruajtjen e nivelit më të lartë të integritetit të të dhënave. Këto kontrolle kryhen gjithashtu gjatë rindërtimit të të dhënave nga palët e jashtme të interesuara, për të garantuar që të gjitha të dhënat janë të qëndrueshme ndërmjet sistemeve.

Neni 15
Mësimet e nxjerra dhe zhvillimi

1. Subjektet financiare duhet të kenë kapacitete dhe personel të dedikuar për mbledhjen e informacionit mbi cenueshmëritë dhe kërcënimet kibernetike, incidentet e lidhura me TIK, veçanërisht sulmet kibernetike, si dhe për të analizuar ndikimet e mundëshme mbi qëndrueshmërinë operacionale digjitale.

2. Subjektet financiare duhet të kryejnë rishikime pas incidenteve të lidhura me TIK ose pas çdo incidenti madhor të lidhur me TIK që ka shkaktuar ndërprerje të funksioneve kryesore, duke analizuar shkaqet e ndërprerjes dhe duke identifikuar përmirësimet e nevojshme në operacionet e TIK ose në politikën e vazhdimësisë së biznesit për TIK, sipas nenit 12, të kësaj rregulloreje.

   Subjektet financiare, me përjashtim të mikrondërmarrjeve njoftojnë Autoritetin, me kërkesë të tij, për ndryshimet e implementuara si rrjedhojë e rishikimeve pas ndodhjes së incidenteve të lidhura me TIK, sipas parashikimeve të pikës 2, të këtij neni.

   Rishikimet e bëra pas ndodhjes së incidentit, të lidhura me TIK dhe të parashikuar në pikën 1, të këtij neni, përcaktojnë nëse procedurat e vendosura janë ndjekur dhe nëse masat e marra kanë qenë efektive, duke përfshirë sa më poshtë:

   a) shpejtësinë e reagimit ndaj sinjalizimeve të sigurisë dhe përcaktimin e ndikimit e rëndësisë së incidenteve të lidhura me TIK;

   b) cilësinë dhe shpejtësinë e kryerjes së analizës hetimore të TIK, kur kjo konsiderohet e përshtatshme;

   c) efektivitetin e procesit të përshkallëzimit të incidentit brenda subjektit financiar;

   d) efektivitetin e komunikimit të brendshëm dhe të jashtëm.

3. Subjektet financiare konsiderojnë dhe përfshijnë në mënyrë të vazhdueshme në procesin e vlerësimit të rrezikut të TIK, konkluzionet e nxjerra nga testimi i qëndrueshmërisë operacionale digjitale i kryer në përputhje me nenet 42 dhe 43, të kësaj rregulloreje dhe nga incidentet reale të ndodhura të lidhura me TIK, veçanërisht sulmet kibernetike, së bashku me sfidat me të cilat përballet aktivizimi i planeve të vazhdimësisë së biznesit ose rikuperimit, së bashku me informacionin përkatës të shkëmbyer me palët dhe të vlerësuar gjatë rishikimeve mbikëqyrëse. Gjetje do të shërbejnë si bazë për rishikimet e përshtatshme të elementëve përkatës të sistemit të administrimit të rrezikut të TIK të parashikuar në nenin 7, pika 1, të kësaj rregulloreje.

4. Subjektet financiare monitorojnë efektivitetin e zbatimit të strategjisë së qëndrueshmërisë operacionale digjitale të ngritur në përputhje dhe sipas parashikimeve të nenin 7, pika 8, të kësaj rregulloreje. Subjektet financiare duhet të identifikojnë dhe dokumentojnë evolucionin e incidenteve të lidhura më TIK me kalimin e kohës, të analizojnë shpeshtësinë, llojet, përmasat dhe zhvillimin e incidenteve të lidhura me TIK, veçanërisht sulmet kibernetike dhe modelet e tyre, me qëllim kuptimin e nivelit të ekspozimit ndaj

rrezikut TIK, në veçanti në lidhje me funksionet kritike ose të rëndësishme, si dhe forcimin e maturitetit kibernetik dhe gatishmërisë së subjektit financiar.

5. Stafi drejtues i TIK raporton të paktën një herë në vit para organeve drejtuese mbi gjetjet e përmendura në pikën 3, të këtij neni dhe paraqet rekomandimet përkatëse.

6. Subjektet financiare zhvillojnë programe paralajmërimi për sigurinë e TIK dhe trajnime mbi qëndrueshmërinë operacionale digjitale, si module të detyrueshme në skemat e trajnimit të stafit. Këto programe dhe trajnime duhet të aplikohen për të gjithë punonjësit dhe për stafin drejtues, dhe të kenë një nivel përshtatje në propocion me detyrat dhe me funksionet e tyre. Kur është e përshtatshme, subjektet financiare përfshijnë edhe ofruesit e shërbimeve TIK, palë të treta në skemat përkatëse të trajnimit, në përputhje me nenin 46, pika 2, shkronja "i".

7. Subjektet financiare, me përjashtim të mikrondërmarrjeve, monitorojnë në mënyrë të vazhdueshme zhvillimet teknologjike përkatëse, me qëllim për të kuptuar ndikimin e mundshëm që mund të ketë përdorimi i teknologjive të reja mbi kërkesat e sigurisë së TIK dhe qëndrueshmërinë operacionale digjitale. Subjektet Financiare duhet të jenë gjatë gjithë kohës të përditësuara me proceset më të fundit të menaxhimit të rrezikut të TIK, në mënyrë që të luftojnë në mënyrë efektive format aktuale dhe të reja të sulmeve kibernetike.

Neni 16
Komunikimi

1. Subjektet financiare, si pjesë e kuadrit të menaxhimit të rrezikut TIK, të parashikuar në nenin 7, pika 1**,** të kësaj rregulloreje, duhet të kenë plane komunikimi për situata krize që mundësojnë një zbulim të përgjegjshëm, të paktën, të incidenteve madhore ose cenueshmërive që lidhen me TIK-un ndaj klientëve, partnerëve të biznesit si dhe ndaj publikut, sipas rastit.

2. Si pjesë e kuadrit të menaxhimit të rrezikut TIK, subjektet financiare zbatojnë politika komunikimi për stafin e brendshëm dhe për palët e jashtme të interesuara. Politikat e komunikimit për stafin duhet të marrin në konsideratë nevojën për diferencimin ndërmjet stafit të përfshirë drejtpërdrejt në menaxhimin e rrezikut TIK, veçanërisht atij përgjegjës për reagimin dhe rikuperimin, dhe stafit që vetëm informohet.

3. Subjektet financiare caktojnë të paktën një person përgjegjës për zbatimin e strategjisë së komunikimit në rast të incidenteve të lidhura me TIK, si dhe për përmbushjen e funksioneve të komunikimit me publikun dhe median për këtë qëllim.

Neni 17
Kuadri i thjeshtuar i menaxhimit të rrezikut të TIK

1. Nenet 6 deri në 16, të kësaj rregulloreje, nuk zbatohen për subjektet financiare të përmendura në nenin 3, pika 3.

   Përjashtimisht nga pika 1, e këtij neni subjektet e financiare të përmendura më sipër duhet të:

a) krijojnë dhe mirëmbajnë një kuadër të qëndrueshëm dhe të dokumentuar të menaxhimit të rrezikut të TIK, i cili përshkruan mekanizmat dhe masat për menaxhimin e shpejtë, efikas dhe gjithëpërfshirës të rrezikut të TIK, përfshirë mbrojtjen e komponentëve dhe infrastrukturave fizike përkatëse;

b) monitorojnë në mënyrë të vazhdueshme sigurinë dhe funksionimin e të gjitha sistemeve të TIK;

c) minimizojnë ndikimin e rrezikut të TIK përmes përdorimit të sistemeve, protokolleve dhe mjeteve të TIK, të cilat janë të përshtatshme për të mbështetur kryerjen e veprimtarive dhe ofrimin e shërbimeve, si dhe garantojnë mbrojtjen e disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave në rrjete dhe sisteme informacioni;

d) mundësojnë identifikimin dhe zbulimin e menjëhershëm të burimeve të rrezikut të TIK dhe anomalive në rrjet dhe në sistemet e informacionit, si dhe menaxhimin në kohë të incidenteve të lidhura me TIK;

e) identifikojnë varësitë kryesore nga ofruesit e shërbimeve TIK palë të treta;

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

g) testojnë rregullisht planet dhe masat e përmendura në shkronjën "f", si dhe efektivitetin e kontrolleve të zbatuara sipas shkronjave "a" dhe "c" të kësaj pike;

h) zbatojnë, sipas rastit, konkluzionet operacionale që rezultojnë nga testimet e përmendura në shkronjën "g" dhe nga analizat pas incidenteve, duke i integruar ato në procesin e vlerësimit të rrezikut TIK, dhe zhvillojnë, sipas nevojave dhe profilit të rrezikut TIK, programe paralajmërimi për sigurinë e TIK dhe trajnime mbi qëndrueshmërinë operacionale digjitale për stafin dhe drejtuesit.

2. Kuadri i menaxhimit të rrezikut TIK i parashikuar në pikën 1, shkronja "a", të këtij neni, duhet të dokumentohet dhe të rishikohet periodikisht, si dhe pas ndodhjes së incidenteve madhore të lidhura me TIK-un, në përputhje me udhëzimet mbikëqyrëse. Ky kuadër duhet të përmirësohet vazhdimisht mbi bazën e mësimeve të nxjerra nga zbatimi dhe monitorimi Subjektet i komunikojnë Autoritetit, me kërkesë të tij, raportin mbi rishikimin e sistemit të administrimit të rrezikut të TIK.

3. Autoriteti, harton udhëzime për standardet teknike, me qëllim që të:

a) specifikojë më tej elementet që duhet të përfshihen në kuadrin e menaxhimit të rrezikut TIK, të përmendur në pikën 1, shkronja "a";

b) specifikojë më tej elementet në lidhje me sistemet, protokollet dhe mjetet për të minimizuar ndikimin e rrezikut TIK, të përmendura në pikën 1, shkronja "c", me synimin për të garantuar sigurinë e rrjeteve, për të mundësuar masa të përshtatshme mbrojtëse kundër ndërhyrjeve dhe keqpërdorimit të të dhënave dhe për të ruajtur disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave;

c) specifikojë më tej komponentët e planeve të vazhdimësisë së biznesit TIK, të përmendur në pikën 1, shkronja "f";

d) specifikojë më tej rregullat mbi testimin e planeve të vazhdimësisë së biznesit dhe të siguron efektivitetin e kontrolleve të përmendura në pikën 1, shkronja "g", dhe të sigurojnë që një testim i tillë të marrë në konsideratë skenarë sipas të cilëve cilësia e ofrimit të një funksioni kritik ose të rëndësishëm përkeqësohet në nivele të papranueshme ose dështon;

e) specifikojë më tej përmbajtjen dhe formatin e raportit mbi rishikimin e kuadrit të menaxhimit të rrezikut TIK, të përmendur në pikën 2.

4. Autoriteti në hartimin e udhëzimeve të përcaktuara në pikën 3, të këtij neni, mban në konsideratë madhësinë dhe profilin e përgjithshëm të rrezikut të subjektit financiar, si dhe natyrën, shkallën dhe kompleksitetin e shërbimeve, veprimtarive dhe operacioneve të tij.

KREU III
MENAXHIMI, KLASIFIKIMI DHE RAPORTIMI I INCIDENTEVE TË LIDHURA ME TIK

Seksioni I
Menaxhimi dhe klasifikimi i incidenteve të lidhur me TIK

Neni 18
Procesi i menaxhimit të incidenteve të lidhura me TIK

1. Subjektet financiare përcaktojnë, krijojnë dhe zbatojnë një proces të menaxhimit të incidenteve të lidhura me TIK me qëllim zbulimin, menaxhimin dhe njoftimin e tyre.

2. Subjektet financiare regjistrojnë të gjitha incidentet e lidhura me TIK dhe kërcënimet kibernetike të rëndësishme. Subjektet financiare krijojnë procedura të përshtatshme për të siguruar monitorimin, trajtimin dhe ndjekjen e unifikuar dhe të integruar të incidenteve të lidhura me TIK-un, duke garantuar identifikimin, dokumentimin dhe adresimin e shkaqeve rrënjësore, me qëllim parandalimin e përsëritjes së tyre.

3. Procesi i menaxhimit të incidenteve të lidhura me TIK i parashikuar në pikën 1, të këtij neni duhet të:

a) përcaktojë tregues të paralajmërimit të hershëm;

b) krijojë procedura për identifikimin, gjurmimin, regjistrimin, kategorizimin dhe klasifikimin e incidenteve të lidhura me TIK, sipas përparësisë dhe rëndësisë së tyre, si dhe sipas nivelit të rëndësisë kritike të shërbimeve të prekura, në përputhje me kriteret e përcaktuara në nenin 19, pika 1;

c) caktojë rolet dhe përgjegjësitë që duhen aktivizuar për lloje dhe skenarë të ndryshëm të incidenteve të lidhura me TIK;

d) përcaktojë planet për komunikimin me stafin, palët e jashtme të interesuara dhe median, në përputhje me nenin 16, të kësaj rregulloreje, si dhe njoftimin e klientëve, për procedurat e brendshme të përshkallëzimit, përfshirë ankesat e klientëve të lidhura

me TIK, si dhe për dhënien e informacionit për subjektet financiare që veprojnë si partner biznesi sipas rastit;

e) sigurojë që, të paktën incidentet madhore të lidhura me TIK, të raportohen tek drejtuesi i lartë i drejtpërdrejtë, si dhe të informohen organet drejtuese, duke shpjeguar ndikimin, reagimin dhe kontrollet shtesë që duhet të vendosen si rezultat i tyre;

f) vendosë procedura të reagimit ndaj incidenteve të lidhura me TIK për të zbutur ndikimet dhe për të siguruar që shërbimet të bëhen funksionale dhe të sigurta brenda një kohe të arsyeshme.

Neni 19
Klasifikimi i incidenteve të lidhura me TIK dhe kërcënimet kibernetike

1. Subjektet financiare, duhet të klasifikojnë incidentet e lidhura me TIK dhe të përcaktojnë ndikimin e tyre mbi bazën e kritereve të mëposhtme:

   a) numri dhe/ose rëndësia e klientëve ose partnereve të biznesit të prekur dhe sipas rastit, shuma ose numri i transaksioneve të ndikuara nga incidenti i lidhur me TIK, si dhe nëse incidenti ka shkaktuar ndikim në reputacion;

   b) kohëzgjatja e incidentit të lidhur me TIK, përfshirë periudhën e ndërprjerjes së shërbimit;

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

   d) humbjet e të dhënave që shkakton incidenti i lidhur me TIK, në raport me disponueshmërinë, origjinalitetin, integritetin ose konfidencialitetin e të dhënave;

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

   f) ndikimi ekonomik, veçanërisht kostot dhe humbjet direkte dhe indirekte të shkaktuara nga incidenti i lidhur me TIK, si në terma absolutë ashtu edhe relativë.

2. Subjektet financiare, duhet të klasifikojnë kërcënimet kibernetike si të rëndësishme, bazuar në rëndësinë e shërbimeve të rrezikuara, përfshirë transaksionet dhe operacionet e subjektit financiar, numrin dhe/ose rëndësinë e klientëve ose partnerëve të biznesit të synuar dhe përhapjen gjeografike të zonave të rrezikuara.

Seksioni II
Kriteret e Klasifikimit të Incidenteve të Lidhur me TIK dhe të Kërcënimeve Kibernetike

Neni 20
Klientët, pala tjetër financiare dhe transaksionet

1. Për qëllime të nenit 19, të pika 1, shkronja "a", 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 mbuluar në mënyrë eksplicite nga marrëveshja kontraktuale ndërmjet subjektit financiar dhe klientit si përfitues të shërbimit të prekur.

2. Për qëllime të nenit 19, pika 1, shkronja "a", të kësaj rregulloreje, numri i palëve të tjetër financiare të prekura nga incidenti, pasqyron numrin e të gjithë pala tjetër financiare të prekur nga incidenti, që kanë lidhur një marrëveshje kontraktuale me subjektin financiar.

3. Për të vlerësuar rëndësinë e klientëve dhe palën tjetër financiare të prekur nga incidenti, siç parashikohet në nenin 19, pika 1, shkronja "a", të kësaj rregulloreje, subjekti financiar merr në konsideratë masën në të cilën ndikimi mbi një klient ose një pale tjetër 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 nenin 19, pika 1, shkronja "a", 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 pala tjetër financiare të prekura ose mbi numrin ose shumën e transaksioneve të prekura, subjekti financiar i vlerëson këto numra ose shuma, bazuar në të dhënat e disponueshme nga periudha të krahasueshme reference.

Neni 21
Ndikimi reputacional

1. Për qëllime të përcaktimit të ndikimit reputacional të incidentit, siç parashikohet në nenin 19, pika 1, shkronja "a", 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 pala tjetër 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 pala tjetër 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 shkallën e ekspozimit publik që incidenti ka marrë ose ka gjasa të marrë, në lidhje me secilin nga kriteret e renditur në pikën 1, të këtij neni.

Neni 22
Kohëzgjatja dhe koha e ndërprerjes së shërbimeve

1. Për qëllime të nenit 19**,** pika 1, shkronja "b", 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, ata masin kohëzgjatjen e incidentit nga momenti i zbulimit të tij. Kur subjektet financiare marrin dijeni se incidenti ka ndodhur përpara zbulimit të tij, duhet të masin 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 parashikojnë dot 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, ata përdorin vlerësimet e tyre.
4. Për qëllime të nenit 19, pika 1, shkronja "b", 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 pala tjetër 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, ata masin 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 nenin 19, pika 1, shkronja "c", 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 pala tjetër financiare në shtete të tjera;
   b) degët ose subjektet e tjera financiare të grupit, që kryejnë veprimtari në shtete të tjera;
   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, për aq sa një informacion i tillë është i disponueshëm.

Neni 24
Humbja e të dhënave

1. Për qëllime të përcaktimit të humbjeve të të dhënave që shkakton incidenti, siç parashikohet në nenin 19, pika 1, shkronja "d", 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 palëve të tjera, të pa aksesueshme ose të papërdorshme, në mënyrë të përkohshme ose të përhershme;
b) në lidhje me origjinalitetin 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
Rëndësia e shërbimeve të prekura

1. Për qëllime të përcaktimit të rëndësisë së shërbimeve të prekura, siç parashikohet në nenin 19, pika 1, shkronja "e", të kësaj rregulloreje, subjektet financiare vlerësojnë nëse incidenti:
   a) prek ose ka prekur shërbimet e TIK 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 nga Autoriteti;
   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. Me qëllim përcaktimin e ndikimit ekonomik të incidentit, siç parashikohet në nenin 19, pika 1, shkronja "f", të kësaj rregulloreje, subjektet financiare, pa llogaritur vlerat e rikuperuara, marrin parasysh llojet e mëposhtme të kostove direkte dhe indirekte dhe humbjeve, që janë shkaktuar si rezultat i incidentit:
   a) fondet ose aktivet financiare të përvetësuara (*expropriated*), për të cilat ata janë përgjegjës, 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 mjeko ligjore 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 përditësuara 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 nenit 30, pika 1, 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 kur numri i klientëve të prekur që përdorin shërbimin e prekur nga incidenti, është më i lartë se 100,000;
b) janë arritur dy ose më shumë nga kufijtë e tjerë të materialitetit të përcaktuar në nenin 28, pika 1, deri në 7, 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, që plotësojnë në mënyrë kumulative kushtet për t'u konsideruar incident madhor i lidhur me TIK, siç parashikohet në pikën 2, të këtij neni, e paraqesin këtë informacion në një formë të përmbledhur "*agreguar*".

5. Përjashtohen nga zbatimi i kërkesave të parashikuara në pikat 2 dhe 3, të këtij neni, mikrondërmarrjet dhe për subjektet e parashikuara në nenin 17, pika 1, të kësaj rregulloreje.

6. Nëse pas vlerësimeve të mëtejshme, subjekti financiar arrin në përfundimin se incidenti i lidhur me TIK, i cili është raportuar më parë si incident madhor, në asnjë moment nuk ka

përmbushur kriteret dhe kufijtë e klasifikimit të përcaktuara në këtë nen, subjekti financiar njofton Autoritetin se e ka riklasifikuar incidentin e lidhur me TIK, nga incident madhor në jomadhor, duke i paraqitur informacionin për këtë klasifikim sipas formularit të 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, pala tjetër 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 palëve të tjera financiare të prekura nga incidenti është më i lartë se 30% e të gjitha palëve të tjera 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 palët e tjera financiare që janë identifikuar si të rëndësishëm në përputhje me nenin 20, pika 3, të kësaj rregulloreje.

2. Nëse numri real i klientëve ose palëve të tjera 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 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, origjinalitetin, 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 lekë të shumës 100,000 euro.

Neni 29
Kufijtë për përcaktimin e kërcënimeve kibernetike të rëndësishme

1. Kërcënimi kibernetik do të konsiderohet si "kërcënim kibernetik 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 palën tjetër financiare, bazuar në informacionin në dispozicion të subjektit financiar;
b) kërcënimi kibernetik ka një probabilitet të lartë për t'u materializuar tek subjekti financiar ose tek subjekte të tjera financiare, duke marrë në konsideratë të paktën elementët e mëposhtëm:
    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 tek njësia ekonomike ose ofruesi i saj palë e tretë, klientët ose homologët financiarë;
c) kërcënimi kibernetik, nëse materializohet, plotëson një nga elementët e mëposhtëm:
    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.

Seksion III
Raportimi i incidenteve të lidhur me TIK dhe njoftimi vullnetar për kërcënimet kibernetike

Neni 30
Raportimi i incidenteve madhore të lidhura me TIK dhe njoftimi vullnetar i kërcënimeve të rëndësishme kibernetike

1. Subjektet financiare raportojnë pranë Autoritetit, çdo incident madhor të lidhur me TIK, në përputhje me kërkesat e përcaktuara në këtë rregullore. Subjektet financiare, për këtë qëllim hartojnë dhe paraqesin njoftimet dhe raportet, pas mbledhjes dhe analizimit të informacionit përkatës, duke përdorur formatet standarde sipas Aneksit 3.

   Pas mbledhjes dhe analizimit të të gjitha informacioneve përkatëse subjektet financiare përgatisin, njoftimin fillestar dhe raportet e përmendura në këtë pikë, duke përdorur formatet e përcaktuara nga Autoriteti.

   Njoftimi fillestar dhe raportet përfshijnë të gjitha informacionet e nevojshme për t'i mundësuar Autoritetit të përcaktojë rëndësinë e incidentit madhor që lidhet me TIK dhe të vlerësojë ndikimet e mundshme. Në rast të një pamundësie teknike e cila pengon paraqitjen e njoftimit fillestar duke përdorur formatin përkatës, subjektet financiare njoftojnë Autoritetin përmes mënyrave alternative.

2. Subjektet financiare, në mënyrë vullnetare njoftojnë Autoritetin për kërcënimet kibernetike të rëndësishme, kur ato konsiderojnë se këto kanë rëndësi për sistemin financiar, përdoruesit e shërbimeve ose klientët. Autoriteti, sipas rastit mund t'i përcjell këto njoftime pranë autoriteteve të tjera kompetente.

3. Kur ndodh një incident madhor që lidhet me TIK dhe ka ndikim mbi interesat financiare të klientëve, subjektet financiare, duhet pa vonesë të panevojshme dhe sapo të bëhen të vetëdijshme për të, të informojnë klientët e tyre për incidentin madhor që lidhet me TIK dhe për masat e marra për të zbutur efektet negative të atij incidenti.

   Në rastin e një kërcënimi të rëndësishëm kibernetik, subjektet financiare, kur është e aplikueshme, informojnë klientët e tyre potencialisht të prekur për çdo masë mbrojtëse të përshtatshme që ata mund të marrin në konsideratë.

4. Subjektet financiare i paraqesin Autoritetit, brenda afateve kohore të përcaktuar në përputhje me nenin 35, të kësaj rregulloreje:
   a) njoftimin fillestar;
   b) raportin e ndërmjetëm pas njoftimit fillestar të përmendur në shkronjën "a", sapo statusi i incidentit fillestar të ketë ndryshuar ndjeshëm ose trajtimi i incidentit madhor që lidhet me TIK të ketë ndryshuar bazuar në informacione të reja të disponueshme, i pasuar, sipas rastit, nga njoftime të përditësuara çdo herë që është në dispozicion një përditësim i rëndësishëm i statusit, si dhe pas një kërkese specifike nga autoriteti kompetent;
   c) raportin përfundimtar, kur analiza e shkaqeve rrënjësore është përfunduar, pavarësisht nëse masat zbutëse janë implementuar ose jo, dhe kur shifrat reale të

ndikimit janë të disponueshme për të zëvendësuar vlerësimet e paraqitura nga subjekti.

5. 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.
6. Subjektet financiare që kanë lidhur ose ndërprerë kontratën me të tretët për transferimin e detyrimeve për raportim të incidenteve madhore të lidhura me TIK, në përputhje me pikën 5 të këtij neni, njoftojnë Autoritetin, sapo të jetë nënshkruar ose ndërprerë kontrata dhe në çdo rast, jo më vonë se para njoftimit ose raportimit të parë. Subjektet financiare i paraqesin Autoritetit 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.
7. Pas marrjes së njoftimit fillestar dhe të çdo raporti të përmendur në pikën 4, Autoriteti, brenda një afati të arsyeshëm, vë në dispozicion detajet e incidentit madhor të raportuar që lidhet me TIK-un, tek:

    a) ESMA ose EIOPA, sipas rastit dhe fushës së kompetencës;

    b) AKSK ose pikave te vetme te kontaktit në përputhje me legjislacionin në fuqi për sigurinë kibernetike dhe marrëveshjet ndërinstitucionale, si dhe direktivës 2022/2585.

Pas marrjes së informacionit në përputhje me këtë nen, ESMA ose EIOPA në konsultim me ENISA-n dhe në bashkëpunim me Autoritetin, vlerësojnë nëse incidenti madhor që lidhet me TIK-un është i rëndësishëm për autoritetet kompetente në shtetet e tjera anëtare. Pas kësaj vlerësimi, ESMA ose EIOPA njoftojnë, sa më shpejt që të jetë e mundur, autoritetet kompetente përkatëse në shtetet e tjera anëtare. Bazuar në njoftim e marrë, autoritetet kompetente të vendeve të tjera anëtare kur është e përshtatshme, marrin të gjitha masat e nevojshme për të mbrojtur qëndrueshmërinë e menjëhershme të sistemit financiar.

Neni 31
Informacioni i përgjithshëm që përfshihet në njoftimin fillestar dhe raportet e ndërmjetme dhe përfundimtare mbi incidentet madhore të lidhura me TIK

1. Subjektet financiare përfshijnë në njoftimin fillestar, raportin e ndërmjetëm dhe raportin përfundimtar, siç parashikohet në nenin 30 pika 4, 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 të tij dhe llojin e subjektit financiar, siç përcaktohet në nenin 3, 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 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 Autoritetin për incidentin madhor të lidhur me TIK;

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 shumat e raportuara.

Neni 32
Informacioni specifik për t'u përfshirë në njoftimin fillestar

1. Njoftimi fillestar i parashikuar në nenin 30, pika 4, 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;
c) një përshkrim të incidentit të lidhur me TIK;

d) kriteret, të përcaktuara në nenet 27 dhe 28, të kësaj rregulloreje, në bazë të të cilave subjekti financiar e klasifikon incidentin e lidhur me TIK, si incident madhor;

e) shtetet e tjera që ndikohen nga incidenti i lidhur me TIK;

f) informacion se si u zbulua incidenti i lidhur me TIK;

g) kur është e mundur, informacion në lidhje me origjinën e incidentit të lidhur me TIK;

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 nga incident madhor në jomadhor;

j) kur disponohet, çdo informacion tjetër përkatës.

Neni 33
Informacioni specifik për t'u përfshirë në raportet e ndërmjetme

Raportet e ndërmjetme siç parashikohen në nenin 30, pika 4, 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 Autoriteti;
b) datën dhe orën e ndodhjes së incidentit të lidhur me TIK;
c) sipas rastit, datën dhe orën kur subjekti financiar ka rikuperuar aktivitetet e tij të rregullt;
d) informacion se si janë përmbushur kriteret e përcaktuara në nenin 19, të kësaj rregulloreje në bazë të të cilave subjekti financiar e ka klasifikuar incidentin e lidhur me TIK;
e) llojin e incidentit të lidhur me TIK;

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

Neni 34
Informacioni specifik për t'u përfshirë në raportet përfundimtare

Raportet përfundimtare siç parashikohen në nenin 30, pika 4, 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;
b) datën dhe orën kur incidenti i lidhur me TIK u zgjidh dhe shkaku/shkaqet bazë u adresuan;
c) informacion mbi zgjidhjen e incidentit të lidhur me TIK;
d) aty ku është e aplikueshme, informacione të rëndësishme për Autoritetin;
e) informacion në lidhje me kostot dhe humbjet direkte dhe indirekte që rrjedhin nga incidenti i lidhur me TIK, si dhe informacion për vlerat e rikuperuara;
f) aty ku është e aplikueshme, informacion në lidhje me incidentet e përsëritura të lidhura me TIK.

Neni 35

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

1. Subjektet financiare paraqesin pranë Autoritetit, njoftimin fillestar, raportet e ndërmjetme dhe përfundimtare të parashikuara në nenin 30, pika 4, shkronja "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, si incident madhor i lidhur me TIK, dhe jo më vonë se 24 orë nga momenti kur subjekti financiar ka marrë dijeni për incidentin e lidhur me TIK;

   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 në nenin 30, pika 4, 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 si incident madhor brenda 24 orëve nga momenti kur subjekti financiar ka marrë dijeni për incidentin e lidhur me TIK, por e klasifikon atë incident të lidhur me TIK 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 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 Autoritetin 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 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 subjektet financiare të identifikuara si infrastruktura kritike dhe të rëndësishme, në përputhje me ligjin "Për sigurinë kibernetike".

6. Autoriteti 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 sistemik për sektorin financiar. Autoriteti njofton vendimin e tij te subjektet financiare të identifikuara. Vendimi i Autoritetit do të zbatohet vetëm për incidentet e raportuara pas datës së njoftimit të vendimit të Autoritetit.

7. Subjektet financiare mund të kombinojnë paraqitjen e njoftimit fillestar, raportit të ndërmjetëm dhe raportit përfundimtar, duke i paraqitur pranë Autoritetit, të dy ose të gjithë 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

1. Subjektet financiare do të përdorin formularët e raportimit të parashikuar në Aneksin 1, të kësaj rregulloreje, për të paraqitur pranë Autoritetit, njoftimin fillestar, raportin e ndërmjetëm dhe raportin përfundimtar siç përcaktohet në nenin 30, pika 4, 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 vullnetar për kërcënimet kibernetike të rëndësishme

1. Përmbajtja e njoftimit **vullnetar** në lidhje për kërcënimet kibernetike të rëndësishme, të parashikuar në nenin 30, pika 2, 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 pala tjetër financiare;
e) kriteret e klasifikimit që do të kishin shkaktuar një raport incidenti madhor të përcaktuar në nenet 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 Autoritetin për kërcënimet kibernetike të rëndësishme sipas kërkesave të nenit 30, pika 2, 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 palë e tretë, të cilit i janë transferuar detyrimet e raportimit, siç parashikohet në nenin 30, pika 5, 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, që prek disa subjekte financiare, në një njoftim ose raport të vetëm, dhe ta paraqesë atë njoftim ose raport tek Autoriteti 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 që duhet raportuar buron nga ose shkaktohet nga një ofrues shërbimi të TIK palë e tretë;
b) ai ofrues shërbimi të TIK palë e tretë ofron shërbimin përkatës TIK për më shumë se një subjekt financiar, ose për një grup;
c) incidenti i lidhur me TIK klasifikohet si madhor nga secili subjekt financiar i përfshirë në njoftimin ose raportin e agreguar;
d) incidenti madhor i lidhur me TIK prek subjektet financiare brenda Shqipërisë dhe raporti i agreguar lidhet me subjektet financiare që mbikëqyren nga Autoriteti;
e) Autoriteti i ka lejuar në mënyrë të qartë këto lloj subjektesh financiare të agregojnë raportimet e tyre.
2. Kur Autoriteti kërkon informacion mbi ndikimin individual të incidentit madhor të lidhur me TIK 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.

Neni 39
Roli mbikëqyrës

Pa rënë ndesh me 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", Autoriteti, pas marrjes së njoftimit fillestar, dhe të çdo raporti të përmendur në

nenin 30, pika 4, konfirmon marrjen e njoftimit dhe kur është e zbatueshme, jep në mënyrë të përshtatshme dhe të menjëhershme reagime përkatëse dhe proporcionale ose udhëzime të nivelit të lartë për subjektin financiar, veçanërisht duke vënë në dispozicion çdo informacion dhe inteligjencë përkatëse të anonimizuar mbi kërcënime të ngjashme, si dhe mund të diskutojë masat korrigjuese të zbatuara në nivelin e 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, të raportuara në përputhje me nenin 30, pika 1, të kësaj rregulloreje.

Kreu IV
TESTIMI I QËNDRUESHMËRISË OPERACIONALE DIGJITALE

Neni 40
Kërkesat e përgjithshme për kryerjen e testimit të qëndrueshmërisë operacionale digjitale

1. Për qëllime të vlerësimit të gatishmërisë për trajtimin e incidenteve të lidhura me TIK, identifikimin e dobësive, mangësive dhe boshllëqeve në qëndrueshmërinë operacionale digjitale, si dhe zbatimin në kohë të masave korrigjuese, subjektet financiare, me përjashtim të mikrondërrmarrjeve , duke marrë në konsideratë kriteret e përcaktuara në nenin 5, pika 2, hartojnë, mirëmbajnë dhe rishikojnë një program gjithëpërfshirës për testimin e qëndrueshmërisë operacionale digjitale, si pjesë integrale e kuadrit të menaxhimit të rrezikut TIK, në përputhje nenin 7, të kësaj rregulloreje.

2. Programi i testimit të qëndrueshmërisë operacionale digjitale, përfshin vlerësime, testime, metodologji, praktika dhe mjete që zbatohen në përputhje me nenet 41 dhe 42 të kësaj Rregulloreje.

3. Subjektet financiare, gjatë zbatimit të programit të parashikuar në pikën 1, të këtij neni, me përjashtim të mikrondërmarrjeve, ndjekin një qasje të bazuar në rrezik, duke marrë në konsideratë kriteret e përcaktuara në nenin 5, pika 2, si dhe duke vlerësuar dinamikën e zhvillimit të rrezikut të TIK, çdo rrezik specifik ndaj të cilit është ose mund të ekspozohet subjekti financiar, rëndësinë kritike të aseteve të informacionit dhe të shërbimeve të ofruara, si dhe çdo faktor tjetër që konsiderohet i përshtatshëm nga subjekti financiar.

4. Subjektet financiare, me përjashtim të mikrondërmarrjeve, sigurojnë që testet të kryhen nga palë të pavarura, qofshin këto pjesë të strukturave të të brendshme apo të jashtme. Kur testet kryhen nga testues pjesë e strukturave të brendshme, subjektet financiare vënë në dispozicion burime të mjaftueshme dhe garantojnë shmangien e konflikteve të interesit gjatë fazës së hartimit dhe ekzekutimit të testit.

5. Subjektet financiare, me përjashtim të mikrondërmarrjeve ,vendosin procedura dhe politika për të dhënë prioritetet, për të klasifikuar dhe adresuar të gjitha çështjet e evidentuara gjatë testimeve, si dhe vendosin metodologji të brendshme certifikimi për të siguruar që të gjitha dobësitë, mangësitë apo boshllëqet e identifikuara trajtohen plotësisht.

6. Subjektet financiare, me përjashtim të mikrondërmarrjeve, sigurojnë që të paktën një herë në vit, të kryhen teste mbi të gjitha sistemet dhe aplikacionet e TIK që mbështesin funksione kritike ose të rëndësishme.

Neni 41
Testimi i mjeteve dhe sistemeve TIK

1. Programi i testimit të qëndrueshmërisë operacionale digjitale i përmendur në nenin 40, duhet të parashikojë, në përputhje me kriteret e përcaktuara në nenin 5, pika 2, kryerjen e testeve të përshtatshme, të tilla si:

    a. analiza dhe skanime të cënueshmërisë të sigurisë

    b. analiza të burimeve të hapura (*open source analyses*),

    c. vlerësime të sigurisë së rrjetit,

    d. analiza të boshllëqeve (*gap analyses),*

    e. rishikime fizike të sigurisë,

    f. pyetësorë dhe zgjidhje softuerike për monitorimin dhe skanimin e infrastrukturës digjitale,

    g. rishikime të kodit burimor (*source code*), kur është e realizueshme,

    h. teste të bazuara në skenarë,

    i. teste të përputhshmërisë,

    j. teste performance,

    k. teste fund–më–fund (*end-to-end testing*),

    l. si dhe teste depërtimi *(penetration testing).*

2. Depozitarët qendrorë të titujve dhe kundërpala qëndrore kryejnë vlerësime të cenueshmërisë përpara çdo vendosjeje ose rivendosjeje të aplikacioneve dhe komponentëve të infrastrukturës ekzistuese ose të rinj, si dhe të shërbimeve TIK që mbështesin funksione kritike ose të rëndësishme të subjektit financiar.

3. Mikrondërmarrjet, duhet të kryejnë testet e përmendura në pikës 1, duke kombinuar një qasje të bazuar në rrezik me një planifikim strategjik të testimit të TIK, duke marrë në konsideratë siç duhet nevojën për të ruajtur një qasje të ekuilibruar midis shkallës së burimeve dhe kohës që do t'i ndahet testimit të TIK-ut të parashikuar në këtë nen, nga njëra anë, dhe urgjencës, llojit të rrezikut, rëndësisë kritike të aseteve të informacionit dhe shërbimeve të ofruara, si dhe çdo faktori tjetër përkatës, duke përfshirë aftësinë e subjektit financiar për të marrë rreziqe të llogaritura, nga ana tjetër.

Neni 42
Testimi i avancuar i mjeteve, sistemeve dhe proceseve TIK mbi bazuar në testimin e depërtueshmërisë të udhëhequr nga kërcënimi (*TLPT)*

1. Subjektet financiare, me përjashtim të atyre të përmendura në nenin 17 pika 1, paragrafi i parë, të identifikuara sipas pikës 8, paragrafi i tretë, të këtij neni, me përjashtim të mikrondërmarrjeve, kryejnë, të paktën çdo tre vjet, testime të avancuara përmes TLPT (*Threat-Led Penetration Testing).* Autoriteti, sipas rastit mund të kërkojë reduktimin ose shtimin e kësaj frekuence bazuar në profilin e rrezikut të subjektit financiar dhe rrethanave operacionale, të tij.

2. Çdo test depërtimi i ndikuar nga kërcënimet *(TLPT)* duhet të mbulojë disa ose të gjitha funksionet kritike ose të rëndësishme të subjektit financiar dhe të kryhet në sistemet e prodhimit live (*live production systems*) që mbështesin këto funksione.

   Subjektet financiare duhet të identifikojnë të gjitha sistemet, proceset dhe teknologjitë bazë të TIK që mbështesin funksione ose shërbime kritike ose të rëndësishme, përfshirë ato të dhëna me kontratë ose të nënkontraktuara tek ofrues të shërbimeve të TIK palë të treta.

   Subjektet financiare vlerësojnë funksionet kritike ose të rëndësishme që duhet të mbulohen nga testimi i depërtueshmërisë i udhëhequr nga kërcënimi . Rezultati i këtij vlerësimi duhet të përcaktojë objektin/fushën e saktë të testimit të depërtueshmërisë të udhëhequr nga kërcënimidhe certifikohet nga Autoriteti.

3. Kur ofruesit e shërbimeve të TIK, palë të treta përfshihen në fushën e testimit të depërtueshmërisë të udhëhequr nga kërcënimi *(TLPT)*, subjekti financiar merr masat dhe garancitë e nevojshme për të siguruar pjesëmarrjen e ofruesve të shërbimeve TIK, palë të treta në *TPLT* dhe në çdo rast është plotësisht përgjegjës për respektimin e kësaj rregulloreje.

4. Pa rënë ndesh me përcaktimet në pikën 2, kur pjesëmarrja e një ofruesi shërbimesh TIK palë e tretë, në testimin e depërtueshmërisë të udhëhequr nga kërcënimi *TLPT,* pritet të ketë ndikim negativ mbi cilësinë ose sigurinë e shërbimeve që ai ofron për klientë që nuk janë subjekte të kësaj rregulloreje, ose mbi konfidencialitetin e të dhënave përkatëse, subjekti financiar dhe ofruesi i shërbimeve të TIK mund të bien dakord me shkrim që ofruesi të lidhë drejtpërdrejt marrëveshje kontraktuale me një testues të jashtëm, për qëllime të kryerjes të një testimi të përbashkët të të depërtueshmërisë të udhëhequr nga kërcënimi *TLPT* që përfshin disa subjekte financiare (*pooled testing*) të cilat marrin shërbime nga ky ofrues, nën drejtimin e një subjekti financiar të caktuar.

   Testimi i përbashkët duhet të mbulojë gamën përkatëse të shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme, të kontraktuara nga subjektet financiare tek ofruesi përkatës i shërbimeve të TIK, palë e tretë. Testimi i përbashkët duhet të konsiderohet si *TLPT* i kryer nga subjektet financiare që marrin pjesë në testimin e përbashkët.

   Numri i subjekteve financiare pjesëmarrëse në testimin e përbashkët duhet të përcaktohet duke marrë parasysh kompleksitetin dhe llojin e shërbimeve të përfshira.

5. Subjektet financiare, në bashkëpunim me ofruesit e shërbimeve të TIK, palë të treta dhe palë të tjera të përfshira, duke përfshirë edhe testuesit, por duke përjashtuar Autoritetin, duhet të zbatojnë kontrolle efektive të menaxhimit të rrezikut për të zbutur rreziqet e

çdo ndikimi potencial mbi të dhënat, dëmtimin e aseteve dhe ndërprerjen e funksioneve, shërbimeve ose operacioneve kritike ose të rëndësishme në vetë subjektin financiar, tek palët e tjera ose në sektorin financiar.

6. Në përfundim të testimit, pasi të jenë dakordësuar raportet dhe planet e masave korrigjuese, subjekti financiar, kur është e aplikueshme dhe testuesit e jashtëm, i paraqesin Autoritetit një përmbledhje të gjetjeve përkatëse, planet e masave korrigjuese dhe dokumentacionin që dëshmon se testimi i depërtueshmërisë i udhëhequr nga kërcënimi *TLPT* është kryer në përputhje me kërkesat e kësaj rregullore.

7. Autoriteti i lëshon subjekteve financiare një vërtetim që konfirmon se testimi është kryer në përputhje me kërkesat, e paraqitura në dokumentacion, me qëllim mundësimin e njohjes reciproke të testimeve të depertueshmërisë të udhëhequr nga kërcënimi *TLPT* midis autoriteteve të ndryshme përgjegjëse.
Në çdo rast subjektet financiare mbeten plotësisht përgjegjëse për ndikimin e testeve të parashikuara në pikën 4, të këtij neni.

8. Subjektet financiare duhet të kontraktojnë testues të jashëm për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi *TLPT* në përputhje me nenin 43 të kësaj rregulloreje.

   Kur subjektet financiare përdorin testues të brendshëm për kryerjen e testeve të depërtueshmërisë të udhëhequr nga kërcënimi *TLPT*, pas çdo tre testesh të kryera, subjektet financiare kanë detyrimin të kontraktojnë testues të jashtëm.

   Autoriteti, identifikon subjektet financiare që janë të detyruara të kryejnë testimin e depërtueshmërisë të udhëhequr nga kërcënimi *TLPT*, duke marrë parasysh kriteret e përcaktuara në nenin 5, pika 2, të kësaj rregullore si dhe vlerësimin e faktorëve si më poshtë:

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

   b) pasojat e mundshme për stabilitetin financiar, përfshirë karakterin sistemik të subjektit financiar, në nivel kombëtar ose në nivel Bashkimi Evropian për aq sa është e aplikueshme;

   c) profilin specifik të rrezikut të TIK, nivelin e maturitetit të TIK të subjektit financiar ose veçoritë teknologjike të tij.

9. Member States may designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level and shall entrust it with all competences and tasks to that effect.

10. In the absence of a designation in accordance with paragraph 9 of this Article, and without prejudice to the power to identify the financial entities that are required to perform TLPT, a competent authority may delegate the exercise of some or all of the tasks referred to in this Article and Article 27 to another national authority in the financial sector.

11. Autoriteti, harton udhëzime për standardet teknike, sipas kornizës TIBER-EU me qëllim që të përcaktojë:

- kriteret e aplikimit të TLPT;
- kërkesat dhe standardet për përdorimin e testuesve të brendshëm;
- fushën, metodologjinë, rezultatet dhe fazat e riparimit të testimeve;
- llojin e bashkëpunimit mbikëqyrës dhe njohjes së ndërsjellë për subjektet financiare që operojnë në më shumë se një Shtet Anëtar.

Neni 43
Kërkesat për testuesit për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi TLPT

1. Subjektet financiare përdorin për kryerjen e testimit të depërtueshmërisë të udhëhequr nga kërcënimi *TLPT* vetëm testues që plotësojnë kërkesat e mëposhtme:

   a) kanë përshtatshmërinë dhe reputacionin të lartë;

   b) zotërojnë kapacitete teknike dhe organizative dhe dëshmojnë ekspertizë specifike në inteligjencën e kërcënimeve *(threat intelligence),* testimin e depërtimit dhe testimin e tipit *red team*;

   c) janë të certifikuar nga një organ akreditimi i një prej vendeve anëtare të Bashkimit Evropian ose ndjekin kode formale sjelljeje dhe etike;

   d) të garantojë vlerësim të pavarur ose raport auditimi, që vërteton menaxhimin e rreziqeve në mënyrë të shëndoshë dhe efektive gjatë zhvillimit të testimit (*TLPT*), duke garantuar mbrojtjen e informacionit konfidencial të subjektit financiar dhe parashikimin e mekanizmave të përshtatshëm të korrigjimit të rreziqeve të cilat mund të prekin veprimtarinë e subjektit financiar;

   e) të mbulohen në mënyrën e duhur dhe plotësisht me policën e sigurimit të përgjegjësisë profesionale, përfshirë rreziqet që vijnë si pasojë e sjelljessë gabuar ose nga neglizhenca.

2. Kur përdoren testues të brendshëm, subjektet financiare sigurojnë që, përveç kërkesave të përcaktuara në pikën 1, të këtij neni, të plotësohen edhe kushtet e mëposhtme:

   a) përdorimi i tyre është miratuar nga Autoriteti ose nga një autoritet tjetër publik

   b) Autoriteti ose Autoriteti tjetër publik, ka verifikuar se subjekti financiar ka burime të dedikuara të mjaftueshme dhe ka garantuar shmangien e konflikteve të interesit gjatë fazave të projektimit dhe ekzekutimit të testit;

   c) ofruesi i inteligjencës së kërcënimeve *(threat intelligence provider)* nuk është pjesë e subjektit financiar.

3. Kontratat e lidhura me testuesit e jashtëm duhet të parashikojë detyrimin për menaxhim të qëndrueshëm të rezultateve të testimit të depërtueshmërisë të udhëhequr nga kërcënimi *TLPT* dhe përpunimit të të dhënave që rrjedh prej saj, përfshirë gjenerimin,

ruajtjen, agregimin, hartimin, raportimin, komunikimin ose asgjësimin, nuk krijon rreziqe për subjektin financiar.

KREU V
MENAXHIMI I RREZIKUT TË PALËVE TË TRETA NË FUSHËN E TIK

Seksioni I
Parimet Kryesore për Menaxhimin të Rrezikut të Palëve të Treta në TIK

Neni 44
Parimet e përgjithshme

1. Subjektet financiare menaxhojnë rrezikun që buron nga palët e treta në fushën e teknologjisë së informacionit dhe komunikimit *(TIK)* si pjesë integrale e kuadrit të menaxhimit të rrezikut të TIK, sipas parashikimeve të nenit 7, pika 1, të kësaj rregulloreje dhe në përputhje me parimet e mëposhtme:

   a) subjektet financiare që lidhin marrëveshje kontraktuale për përdorimin e shërbimeve të TIK, në funksion të operacioneve të tyre të biznesit, mbeten në çdo rast plotësisht përgjegjëse për përmbushjen e detyrimeve që burojnë nga kjo rregullore dhe nga legjislacioni në fuqi;
   b) menaxhimi i rrezikut të palëve të treta në fushën e TIK nga subjektet financiare zbatohet duke respektuar parimin e proporcionalitetit, dhe duke marrë në konsideratë:

      i. natyrën, shkallën, kompleksitetin dhe rëndësinë e varësive nga shërbimet e TIK;

      ii. rreziqet që burojnë nga marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK të ofruara nga palët e treta, duke marrë parasysh rëndësinë e shërbimit, procesit apo funksionit përkatës, si dhe ndikimin e mundshëm në vazhdimësinë dhe disponueshmërinë e shërbimeve dhe aktiviteteve financiare, si në nivel individual ashtu edhe në nivel grupi.

2. Si pjesë e kuadrit të menaxhimit të rrezikut të TIK, subjektet financiare, përveç atyre të përmendura në nenin 17, pika 1, duhet të miratojnë dhe rishikojnë periodikisht strategjinë për menaxhimin e rrezikut nga palët e treta në fushën e TIK, duke marrë në konsideratë strategjinë e përdoruesve të shumtë të palëve të treta sipas nenit 7, pika 9, kur është e zbatueshme. Strategjia për menaxhimin e rrezikut nga palët e treta përfshin një politikë për përdorimin e shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të TIK palë të treta, dhe zbatohet si në nivel individual si dhe kur është e aplikueshme në nivel grupi. Organi drejtues, mbi bazën e një vlerësimi të profilit të përgjithshëm të rrezikut të subjektit financiar dhe të shkallës e kompleksitetit të shërbimeve të biznesit, rishikon rregullisht rreziqet e identifikuara që lidhen me marrëveshjet kontraktuale mbi shërbimet e TIK që mbështesin funksione kritike ose të rëndësishme.

3. Subjektet financiare, si pjesë e kuadrit të menaxhimit të rrezikut TIK, mbajnë dhe përditësojnë, në nivel subjekti, si dhe në nivel grupi, një regjistër informacioni lidhur

me të gjitha marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK të ofruara nga palët e treta.

Marrëveshjet kontraktuale të përmendura në paragrafin e mësipërm dokumentohen duke ndarë ato që mbulojnë funksione kritike ose të rëndësishme nga ato që nuk mbulojnë funksione të tilla.

Subjektet financiare raportojnë të paktën një herë në vit pranë Autoritetit mbi numrin e marrëveshjeve të reja për përdorimin e shërbimeve të TIK, kategoritë e ofruesve të shërbimeve TIK, llojin e marrëveshjeve kontraktuale si dhe shërbimet dhe funksionet që mbulohen.

Subjektet financiare vënë në dispozicion të Autoritetit, sipas kërkesës së tij, regjistrin e plotë të informacionit ose pjesë specifike të tij, së bashku me çdo informacion tjetër të konsideruar të nevojshëm për mbikëqyrjen efektive të subjektit financiar. Subjektet financiare informojnë në kohë Autoritetin për çdo marrëveshje të planifikuar mbi përdorimin e shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme, si dhe kur një funksion merr cilësinë e funksionit kritik ose të rëndësishëm.

4. Përpara lidhjes së një marrëveshjeje kontraktuale mbi përdorimin e shërbimeve TIK, subjektet financiare duhet të:

   a) vlerësojnë nëse marrëveshja mbulon përdorimin e shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme;

   b) verifikojnë nëse janë përmbushur kushtet mbikëqyrëse për lidhjen e kontratës;

   c) identifikojnë dhe vlerësojnë të gjitha rreziqet e lidhura me marrëveshjen, përfshirë mundësinë që një marrëveshje e tillë kontraktuale mund të kontribuojë në rritjen e rrezikut të përqendrimit të TIK, siç përmendet në nenin 45, të kësaj rregulloreje;

   d) kryejnë vlerësime (*due diligence)* mbi ofruesit potencialë të shërbimeve TIK, palë të treta dhe të sigurohen, gjatë gjithë procesit të përzgjedhjes dhe vlerësimit, se ofruesi i shërbimeve TIK, palë e tretë është i përshtatshëm;

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

5. Subjektet financiare lidhin marrëveshje kontraktuale vetëm me ofrues të shërbimeve TIK, palë e tretë që përmbushin standardet e duhura të sigurisë së informacionit. Në rastet kur këto marrëveshje lidhen me funksione kritike ose të rëndësishme, subjektet financiare, përpara lidhjes së tyre, duhet të marrin në konsideratë përdorimin nga ofruesit e shërbimeve të TIK palë e tretë të standardeve më të përditësuara dhe më cilësore të sigurisë së informacionit.

6. Për ushtrimin e të drejtave të aksesit, inspektimit dhe auditimit ndaj ofruesve të shërbimeve të TIK të palëve të treta, subjektet financiare, në bazë të një qasjeje të orientuar nga rreziku, përcaktojnë paraprakisht shpeshtësinë dhe fushëveprimin e auditimeve e të inspektimeve. Kjo bëhet duke respektuar standardet e pranuara të auditimit dhe në përputhje me udhëzimet mbikëqyrëse për përdorimin dhe zbatimin e këtyre standardeve.

7. Kur marrëveshjet kontraktuale me ofruesit e shërbimeve të TIK, palë e tretë përfshijnë kompleksitet të lartë teknik, subjekti financiar duhet të sigurohet që audituesit, qofshin të brendshëm apo të jashtëm, apo grup audituesish, kanë aftësitë dhe njohuritë e duhura për të kryer në mënyrë efektive auditimet dhe vlerësimet përkatëse. Subjektet financiare duhet të zgjidhin marrëveshjen kontraktuale mbi përdorimin e shërbimeve të TIK nëse ndodh një nga rrethanat e mëposhtme:

   a) konstatohen shkelje të rënda të ligjeve, rregulloreve ose kushteve kontraktuale nga ofruesi i shërbimeve të TIK, palë e tretë;

   b) gjatë monitorimit të rrezikut të palëve të treta në fushën e TIK, identifikohen rrethana që vlerësohen se ndikojnë në performancën e funksioneve të ofruara përmes marrëveshjes kontraktuale, përfshirë ndryshime materiale që prekin marrëveshjen ose situatën e ofruesit të shërbimeve të TIK;

   c) konstatohen dobësi të ofruesit të shërbimeve të TIK, të lidhura me menaxhimin e përgjithshëm të rrezikut të TIK dhe, në veçanti, me mënyrën e garantimit të disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave, personale apo të dhëna të tjera sensitive, ose jopersonale;

   d) si rezultat i kushteve të marrëveshjes kontraktuale ose rrethanave të lidhura me të, Autoriteti nuk mund të ushtrojë më mbikëqyrje efektive mbi subjektin financiar.

8. Për shërbimet e TIK që mbështesin funksione kritike ose të rëndësishme, subjektet financiare duhet të hartojnë strategji daljeje (*exit strategies*). Këto strategji dalje marrin në konsideratë rreziqet që mund të shfaqen në nivelin e ofruesve të shërbimeve të TIK, veçanërisht dështimin e mundshëm të tyre, përkeqësimin e cilësisë së shërbimeve të ofruara, çdo ndërprerje të veprimtarisë për shkak të ofrimit të papërshtatshëm ose mos ofrimit të shërbimeve TIK, ose çdo rreziku material që lidhet me vendosjen e duhur dhe të vazhdueshme të shërbimit përkatës, ose ndërprerjen e marrëveshjeve kontraktuale sipas pikës 7, të këtij neni.

   Subjektet financiare duhet të sigurohen që janë në gjendje të zgjidhin marrëveshjen kontraktuale pa shkaktuar:

   a) ndërprerje të veprimtarisë të subjektit;

   b) kufizim të përputhshmërisë me kërkesat rregullatore;

   c) dëmtim të vazhdimësisë dhe cilësisë së shërbimeve të ofruara për klientët.

Planet e daljes *(exit plans)*duhet të jenë gjithëpërfshirëse, të dokumentuara, të testohen dhe të rishikohen periodikisht, si dhe të jenë në përputhje me kriteret e përcaktuara në nenin 5, pika 2 të kësaj rregulloreje.

Subjektet financiare duhet të identifikojnë zgjidhje alternative dhe të zhvillojnë plane tranzicioni që u mundësojnë zhvendosjen e shërbimeve të TIK dhe të dhënat përkatëse nga ofruesi i shërbimeve të TIK, palë e tretë dhe t'i transferojnë ato në mënyrë të sigurt dhe të plotë te ofrues alternativë ose t'i rikthejnë ato brenda vetë subjektit.

9. Subjektet financiare duhet të kenë masa të përshtatshme emergjente për të ruajtur vazhdimësinë e biznesit në rast të rrethanave të përmendura në këtë pikë.

10. Autoriteti, harton udhëzim për të përcaktuar modelin standard të regjistrit të informacionit të përmendur në paragrafin 3, të këtij neni.

Neni 45
Vlerësimi paraprak i rrezikut të përqendrimit në fushën TIK në nivel subjekti

1. Gjatë identifikimit dhe vlerësimit të rreziqeve të përmendura në nenin 44, pika 4, shkronja "c", subjektet financiare duhet të marrin në konsideratë nëse lidhja e një marrëveshjeje kontraktuale lidhur me shërbimet e TIK që mbështesin funksione kritike ose të rëndësishme do të çonte në ndonjë nga rastet e mëposhtme:

   a) lidhjen e një kontrate me një ofrues të shërbimeve të TIK, palë e tretë që nuk është lehtësisht i zëvendësueshëm; ose

   b) ekzistencën e disa marrëveshjeve kontraktuale për ofrimin e shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme me të njëjtin ofrues të shërbimeve të TIK të palës së tretë ose me ofrues të shërbimeve të TIK të lidhur ngushtë me të.

Subjektet financiare duhet të vlerësojnë përfitimet dhe kostot e zgjidhjeve alternative, përfshirë përdorimin e ofruesve të ndryshëm të shërbimeve të TIK, duke marrë në konsideratë masën dhe mënyrën në të cilën këto zgjidhje përputhen me nevojat e veprimtarisë si dhe me objektivat e përcaktuara në strategjinë e tyre të qëndrueshmërisë digjitale.

2. Kur marrëveshjet kontraktuale mbi përdorimin e shërbimeve të teknologjisë së informacionit dhe komunikimit (TIK), të cilat mbështesin funksione kritike ose të rëndësishme, parashikojnë mundësinë që ofruesi i shërbimeve të TIK i palës së tretë të nënkontraktojë më tej këto shërbime tek ofrues të tjerë, subjektet financiare janë të detyruara të vlerësojnë me kujdes përfitimet dhe rreziqet që mund të lindin nga ky nënkontraktim, veçanërisht në rastet kur nënkontraktori është i vendosur jashtë territorit të Republikës së Shqipërisë.

Kur marrëveshjet kontraktuale lidhen me shërbime e TIK, që mbështesin funksione kritike ose të rëndësishme, subjektet financiare duhet të marrin parasysh parashikimet ligjore mbi falimentimin që do të zbatoheshin në rast të falimentimit të ofruesit të shërbimeve TIK, si dhe çdo kufizim që mund të lindë lidhur me rikuperimin urgjent të të dhënave të subjektit financiar.

Kur marrëveshjet kontraktuale mbi përdorimin e shërbimeve TIK që mbështesin funksione kritike ose të rëndësishme lidhen me një ofrues të shërbimeve TIK të vendosur jashtë territorit të Republikës së Shqipërisë, subjektet financiare duhet, përveç kërkesave të parashikuar këtë nen , duhet gjithashtu të marrin në konsideratë përputhshmërinë me parashikimet ligjore në ligjin "Për mbrojtjen e të dhënave personale".

Kur marrëveshjet kontraktuale mbi përdorimin e shërbimeve TIK që mbështesin funksione kritike ose të rëndësishme parashikojnë nënkontraktim, 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 aftësinë e Autoritetit për të ushtruar mbikëqyrje efektive ndaj subjektit financiar në këtë drejtim.

Neni 46
Dispozitat kryesore 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 TIK të palës së tretë. Kontrata e plotë duhet të përfshijë marrëveshjet mbi nivelet e shërbimit (*service level agreements*) dhe të dokumentohet në një akt të shkruar, i cili u vihet në dispozicion palëve në letër ose në një format elektronik të shkarkueshëm, të qëndrueshëm dhe të aksesueshëm.

2. Marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK duhet të përmbajnë, të paktën, elementet e mëposhtme:

   a) një përshkrim të qartë dhe të plotë të të gjitha funksioneve dhe shërbimeve të TIK që do të ofrohen nga ofruesi i shërbimeve të TIK të palës së tretë, duke përcaktuar nëse lejohet apo jo nënkontraktimi i një shërbimi të TIK, që mbështet një funksion kritik ose të rëndësishëm, ose pjesë materiale të tij, dhe nëse lejohet, kushtet që do të zbatohen për një nënkontraktim të tillë;

   b) vendndodhjet, përkatësisht rajonet ose shtetet, ku do të ofrohen funksionet dhe shërbimet e TIK të kontraktuara ose të nënkontraktuara dhe ku do të përpunohen të dhënat, përfshirë vendndodhjen e ruajtjes, si dhe detyrimin e ofruesit të shërbimeve të TIK për të njoftuar paraprakisht subjektin financiar në rast ndryshimi të këtyre vendndodhjeve;

   c) dispozita mbi garantimin e disponueshmërisë, origjinalitetit, integritetit dhe konfidencialitetit të të dhënave, përfshirë të dhënat personale;

   d) dispozita mbi sigurimin e aksesit, rikuperimit dhe kthimit të të dhënave personale dhe jo personale të përpunuara nga subjekti financiar, në një format lehtësisht të aksesueshëm, në rast falimentimi, zgjidhjeje ose ndërprerjeje të operacioneve të biznesit të ofruesit të shërbimeve TIK, ose në rast të ndërprerjes së marrëveshjeve kontraktuale;

   e) përshkrime të niveleve të shërbimit (*service levels*), përfshirë përditësimet dhe rishikimet e tyre;

   f) detyrimin e ofruesit të shërbimeve të TIK për t'i ofruar asistencë subjektit financiar, pa kosto shtesë ose me një kosto të përcaktuar paraprakisht, në rast ndodhjeje të një incidenti të TIK që lidhet me shërbimin e ofruar;

   g) detyrimin e ofruesit të shërbimeve të TIK për të bashkëpunuar plotësisht me Autoritetin, përfshirë personat e caktuar prej tij;

   h) të drejtat për ndërprerjen e marrëveshjeve kontraktuale dhe afatet minimale të njoftimit për ndërprerjen, në përputhje me pritshmëritë e Autoritetit;

   i) kushtet për pjesëmarrjen e ofruesve të shërbimeve të TIK në programet e paralajmërimit për sigurinë e TIK dhe në trajnimet për qëndrueshmëri operacionale digjitale të subjekteve financiare, sipas nenit 15, pika 6.

3. Marrëveshjet kontraktuale mbi përdorimin e shërbimeve të TIK që mbështesin funksione kritike ose të rëndësishme duhet të përfshijnë, përveç elementeve të përcaktuara në paragrafin 2, edhe këto elemente shtesë:

a) përshkrime të plota të niveleve të shërbimit, përfshirë përditësimet dhe rishikimet e tyre, me objektiva të saktë sasiorë dhe cilësorë të performancës brenda niveleve të dakorduara të shërbimit, që i mundësojnë subjektit financiar monitorim efektiv dhe ndërmarrjen e veprimeve korrigjuese pa vonesë të panevojshme, në rast mosrealizimi të këtyre niveleve;

b) afate njoftimi dhe detyrime raportimi të ofruesit të shërbimeve të TIK ndaj subjektit financiar, përfshirë njoftimin mbi çdo zhvillim që mund të ketë ndikim material në aftësinë e ofruesit për të ofruar në mënyrë efektive shërbimet të TIK që mbështesin funksione kritike ose të rëndësishme, në përputhje me nivelet e shërbimit të dakorduara;

c) kërkesat për ofruesin e shërbimeve të TIK që të zbatojë dhe të testojë plane të vazhdimësisë së biznesit dhe të ketë në vend masa, mjete dhe politika sigurie të TIK që garantojnë një nivel të përshtatshëm sigurie për ofrimin e shërbimeve nga subjekti financiar, në përputhje me kuadrin e tij rregullator;

d) detyrimin e ofruesit të shërbimeve të TIK për të marrë pjesë dhe bashkëpunuar plotësisht në testet e depërtimit të ndikuara nga kërcënimet *(TLPT)* të subjektit financiar, sipas neneve 42 dhe 43;

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

(i) të drejta të pakufizuara të aksesit, inspektimit dhe auditimit nga subjekti financiar ose një palë e tretë e caktuar prej tij, si dhe nga Autoriteti, përfshirë të drejtën për të marrë kopje të dokumentacionit përkatës në vend, nëse ky është kritik për operacionet e ofruesit të shërbimeve të TIK, dhe ushtrimi efektiv i të cilave nuk pengohet nga marrëveshje të tjera kontraktuale ose politika të zbatimit;

(ii) të drejtën për të rënë dakord mbi nivele alternative sigurie, nëse preken të drejtat e klientëve të tjerë;

(iii) detyrimin e ofruesit të shërbimeve të TIK për të bashkëpunuar plotësisht gjatë inspektimeve dhe auditimeve në vend të kryera nga Autoriteti, subjekti financiar ose një palë e tretë e caktuar;

(iv) detyrimin për të ofruar detaje mbi qëllimin, procedurat dhe shpeshtësinë e inspektimeve dhe auditimeve.

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

(i) gjatë së cilës ofruesi i shërbimeve të TIK do të vazhdojë të ofrojë funksionet ose shërbimet e TIK përkatëse, me qëllim reduktimin e rrezikut të ndërprerjes së aktivitetit të subjektit financiar ose për të mundësuar zgjidhjen dhe ristrukturimin efektiv të tij;

(ii) duke i mundësuar subjektit financiar migrimin tek një ofrues tjetër i shërbimeve të TIK ose kalimin në zgjidhje të brendshme (*in house*), 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 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 të një palë e tretë e pavarur, e caktuar nga ofruesi i shërbimeve të palëve të treta të TIK, dhe që subjekti financiar është në gjendje të kërkojë informacion dhe garantimin e performancës së ofruesit të shërbimeve të palëve të treta të TIK, në çdo kohë nga pala e tretë.

5. Gjatë negocimit të marrëveshjeve kontraktuale, subjektet financiare dhe ofruesit e shërbimeve të TIK duhet të marrin në konsideratë përdorimin e klauzolave standarde kontraktuale të zhvilluara nga autoritetet publike për shërbime specifike.

6. Autoriteti do të hartojë udhëzime teknike për të saktësuar elementët e parashikuar në pikën 2, shkronja "a" të këtij neni. Gjatë përgatitjes së udhëzimeve, duhet të merren parasysh madhësia dhe profili i përgjithshëm i rrezikut i subjektit financiar, si dhe natyra, shkalla dhe kompleksiteti i shërbimeve, aktiviteteve dhe operacioneve të tij.

Seksioni II

Politika për përdorimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të TIK palë e tretë

Neni 47
Profili i përgjithshëm i rrezikut dhe kompleksiteti

1. Subjektet financiare, si pjesë e kuadrit të tyre të menaxhimit të rrezikut të TIK, duhet të miratojnë dhe rishikojnë rregullisht një politikë për përdorimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofrues shërbimesh të TIK, palë të treta.

2. Politika për përdorimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofrues të shërbimeve të TIK palë të treta (në këtë Seksion 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 elementët që lidhen me:

a) llojin e shërbimeve të TIK të përfshira në marrëveshjen kontraktuale për përdorimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të TIK palë të treta (në këtë Seksion do të quhet "Marrëveshja kontraktuale"), ndërmjet subjektit financiar dhe ofruesit të shërbimeve të TIK palë e tretë;
b) vendndodhjen e ofruesit të shërbimeve të TIK palë e tretë ose të shoqërisë mëmë të tij;
c) nëse shërbimet e TIK që mbështesin funksionet kritike ose të rëndësishme ofrohen nga një ofrues shërbimesh të TIK të vendosur brenda Republikës së Shqipërisë ose në një vend tjetër, duke marrë gjithashtu në konsideratë edhe vendin nga ku ofrohen shërbimet e TIK, si dhe vendin ku përpunohen dhe ruhen të dhënat;
d) natyrën e të dhënave që shkëmbehen me ofruesin e shërbimeve të TIK palë e tretë;
e) nëse ofruesi i shërbimeve të TIK palë e tretë është pjesë e të njëjtit grup me subjektin financiar të cilit i ofrohen shërbimet;

f) përdorimin e ofruesve të shërbimeve të TIK palë të treta që janë të licencuar, të regjistruar ose subjekt i mbikëqyrjes së Autoritetit ose një autoriteti tjetër mbikëqyrës brenda Shqipërisë, si dhe përdorimin e ofruesve të shërbimeve të TIK palë të treta që nuk janë të tillë;
g) përdorimin e ofruesve të shërbimeve të TIK palë të treta 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 TIK palë të treta që nuk janë të tillë;
h) nëse ofrimi i shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme është përqendruar tek një ofrues i vetëm i shërbimeve të TIK palë e tretë ose tek një numër i vogël ofruesish të shërbimeve të TIK palë e tretë;
i) transferueshmërinë e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme tek një ofrues tjetër shërbimesh të TIK palë e tretë, përfshirë edhe si pasojë e veçorive teknologjike;
j) ndikimin e mundshëm të ndërprerjeve në ofrimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme, mbi vazhdimësinë e veprimtarisë së subjektit financiar dhe mbi disponueshmërinë e shërbimeve të tij.

Neni 48
Zbatimi në nivel grupi

Në rastet kur kjo rregullore zbatohet në baza të konsoliduara ose nën-konsoliduara, shoqëria mëmë e cila është përgjegjëse për përgatitjen e pasqyrave financiare të konsoliduara ose nën konsoliduara të grupit, duhet të sigurojë zbatim të njëtrajtshëm të politikës 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 49
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 që mbështesin funksionet kritike ose të rëndësishme. "Politika" duhet gjithashtu të përcaktojë kohën kur ky vlerësim duhet të kryhet dhe të rishikohet.

3. "Politika" duhet të përcaktojë qartë përgjegjësitë e brendshme për miratimin, menaxhimin, kontrollin dhe dokumentimin e marrëveshjeve përkatëse kontraktuale dhe të sigurojë 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 që ofrohen në bazë të tyre.

4. Pa cënuar përgjegjësinë përfundimtare të subjektit financiar për mbikëqyrjen efektive të marrëveshjeve kontraktuale përkatëse, "politika" duhet të përmbajë kërkesa për vlerësimin nëse ofruesi i shërbimeve të TIK palë e tretë disponon burime të mjaftueshme për të garantuar

që subjekti financiar i përmbush të gjitha kërkesat ligjore dhe rregullative që lidhen me shërbimet e TIK që mbështesin funksionet kritike ose të rëndësishme të ofruara.

5. "Politika" duhet të identifikojë qartë rolin/funksionin ose personin nga drejtimi i lartë i subjektit financiar, i cili është përgjegjës për monitorimin e marrëveshjeve kontraktuale. "Politika" përcakton mënyrën se si ky rol/funksion ose personi 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 shpeshtësinë e raportimeve të tilla.

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

a) kuadrin e menaxhimit të rrezikut të TIK, 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, 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 që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofrues të shërbimeve të TIK palë të treta, 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 TIK palë të treta të bashkëpunojnë me Autoritetin;
d) duhet të parashikojnë kërkesa që subjekti financiar, audituesit e jashtëm të tij dhe Autoriteti të kenë akses efektiv në të dhënat dhe ambientet që lidhen me përdorimin e shërbimeve të TIK që mbështesin funksionet kritike ose të rëndësishme.

Neni 50
Fazat kryesore të ciklit për hartimin dhe zbatimin e marrëveshjeve kontraktuale

"Politika" përcakton kërkesat, përfshirë rregullat, përgjegjësitë dhe proceset, për secilën fazë kryesore të ciklit 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 që mbështesin funksionet kritike ose të rëndësishme, të ofruara nga ofruesit e shërbimeve të TIK palë të treta;
b) planifikimin e "marrëveshjeve kontraktuale", duke përfshirë vlerësimin e rrezikut, verifikimin e kujdesshëm (*due diligence*), sipas përcaktimeve në nenet 51 dhe 52, të kësaj rregulloreje, si dhe procesin e miratimit të marrëveshjeve të reja ose të

ndryshimeve të rëndësishme në marrëveshjet ekzistuese, sipas përcaktimeve të nenit 54, 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 53, 54 dhe 55, të kësaj rregulloreje, duke përfshirë edhe në nivel të konsoliduar dhe nën konsoliduar, 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 44, pika 3, të kësaj rregulloreje;
f) strategjitë e daljes (*exit strategies*) dhe proceset e ndërprerjes së marrëveshjeve kontraktuale, sipas përcaktimeve në nenin 56, të kësaj rregulloreje.

Neni 51
Vlerësimi paraprak i rrezikut

1. "Politika" parashikon kërkesa që subjekti financiar të përcaktojë nevojat e biznesit, përpara se të lidhi 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 nën konsoliduar, 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 që mbështesin funksionet kritike ose të rëndësishme nga ofruesit e shërbimeve të palëve të treta të TIK, 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;
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 TIK palë të treta;
i) rrezikun e përqendrimit të shërbimeve të TIK në nivel subjekti.

Neni 52
Verifikimi i kujdesshëm (*due diligence)*

1. "Politika" parashikon një proces të përshtatshëm dhe proporcional për përzgjedhjen dhe vlerësimin e ofruesve potencialë të shërbimeve të TIK palë të treta, duke marrë parasysh nëse ofruesi i shërbimit të TIK 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 TIK palë e tretë:

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 menaxhimit të rrezikut dhe kontrolle të brendshme, si dhe kur është e zbatueshme, autorizimet ose regjistrimet përkatëse për ofrimin e shërbimeve të TIK 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 dhe për t'i zbatuar ato, kur është e përshtatshme, për të siguruar një sistem efektiv dhe të shëndetshëm të qëndrueshmërisë operacionale digjitale;
c) përdor ose synon të përdorë nën kontraktorë të TIK, për të kryer shërbimet e TIK 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 TIK palë e tretë, për të ofruar shërbimet ose në aftësinë e subjektit financiar për të marrë këto shërbime të TIK;
e) pranon marrëveshjet kontraktuale që sigurojnë mundësinë efektive për kryerjen e auditimeve tek ofruesi i shërbimeve të TIK palë e tretë, përfshirë auditimet në vend, nga vetë subjekti financiar, palë të treta të caktuara prej tij, ose Autoriteti;
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 kuadrit të menaxhimit të rrezikut të ofruesve të shërbimeve të TIK palë e tretë, për shërbimet e TIK 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 TIK palë e tretë.

3. "Politika" duhet të përcaktojë procesin e verifikimit të kujdesshëm (*due diligence*) për përzgjedhjen dhe vlerësimin e ofruesve potencialë të shërbimeve të TIK palë e tretë dhe të tregojë se cilët nga elementet e mëposhtëm do të përdoren për nivelin e nevojshëm të sigurisë mbi performancën e ofruesit të shërbimeve të TIK palë e tretë:

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 TIK palë e tretë;
c) përdorimi i raporteve të auditimit të kryera nga funksioni i auditit të brendshëm të ofruesit të shërbimeve të TIK palë e tretë;
d) përdorimi i certifikimeve të përshtatshme nga palët e 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 TIK palë e tretë.

4. Subjektet financiare duhet të sigurojnë një nivel të përshtatshëm garancie mbi performancën e ofruesit të shërbimeve të TIK palë e tretë, 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 53
Konflikti i interesit

1. "Politika" duhet të specifikojë masa të përshtatshme për identifikimin, parandalimin dhe menaxhimin e konflikteve aktuale ose të mundshme të interesit, që mund të lindin nga përdorimi të shërbimeve të TIK të ofruar nga palë të treta. 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 që mbështesin funksionet kritike ose të rëndësishme, ofrohen nga ofrues shërbimesh të TIK brenda grupit, politika duhet të specifikojë që vendimmarrja mbi kushtet përkatëse të shërbimeve të TIK, përfshirë kushtet financiare, të bëhet në mënyrë objektive.

Neni 54
Dispozitat kontraktuale

1. "Politika" duhet të specifikojë që çdo marrëveshje kontraktuale të jetë në formë të shkruar dhe të përfshijë të gjitha elementet e parashikuara në nenin 46, 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 duhet 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 shërbimet e TIK. 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, 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 të të njëjtit ofrues shërbimesh të TIK palë e tretë, 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 TIK palë e tretë.

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 në rast se subjekti financiar:

a) vlerëson si të përshtatshëm planin e auditimit të ofruesit të shërbimeve të TIK palë e tretë, për marrëveshjet kontraktuale përkatëse;
b) siguron që shtrirja e certifikimeve ose raporteve të auditimit mbulon sistemet dhe kontrollet kryesore të identifikuara 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 vjetëruara;
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) vlerëson se certifikimet janë lëshuar dhe auditimet janë kryer në përputhje me standarde profesionale të pranuara gjerësisht dhe që përfshijnë testimin e efektivitetit operacional të kontrolleve kryesore në fuqi;
g) ka të drejtën kontraktuale për të kërkuar, me një frekuencë të arsyeshme dhe të justifikuar nga pikëpamja e menaxhimit të rrezikut, ndryshime në shtrirjen e certifikimeve ose të raporteve të auditimit, edhe në sisteme dhe kontrolle 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 55
Monitorimi i marrëveshjeve kontraktuale

1. "Politika" duhet të parashikojë kërkesa që marrëveshjet kontraktuale të përcaktojë masa dhe tregues kryesorë për monitorimin e vazhdueshëm të performancës së ofruesve të shërbimeve të TIK palë e tretë, 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 TIK palë e tretë, 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, duke përfshirë kur është e përshtatshme, aplikimin e penaliteteve kontraktuale.

2. "Politika" përcakton mënyrën se si subjekti financiar vlerëson nëse ofruesit e shërbimeve të TIK palë e tretë, të përdorur për shërbimet e TIK 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 TIK palë të treta 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 dhe raporte mbi masat dhe testimet e vazhdimësisë së biznesit;
b) performanca e ofruesve të shërbimeve të TIK palë të treta, vlerësohet nëpërmjet treguesve kryesorë të performancës *(key performance indicators KPI),* treguesve kryesorë të kontrollit *(key control indicators KCI),* auditimeve, vetë certifikimeve dhe rishikimeve të pavarura, në përputhje me kuadrin e menaxhimit të rrezikut të TIK të subjektit financiar;
c) subjekti financiar merr informacione të tjera përkatëse nga ofruesit e shërbimeve të TIK palë e tretë;
d) subjekti financiar të njoftohet, kur është e përshtatshme, për incidentet e lidhura me TIK dhe incidentet operacionale 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 52, 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 TIK palë të treta, përfshirë incidentet e lidhura me TIK dhe incidentet operacionale ose të sigurisë që lidhen me pagesat, në ofrimin e shërbimeve të TIK 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 56
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.

Seksioni III

Kuadri i Mbikëqyrjes për ofruesit e shërbimeve të TIK palë të treta të konsideruar kritikë

Neni 57
Përcaktimi i ofruesve kritikë të shërbimeve TIK, palë të treta

1. Autoriteti, përcakton ofruesit e shërbimeve TIK palë të treta, të cilët konsiderohen kritikë për subjektet financiare, pas një vlerësimi që merr në konsideratë kriteret e përcaktuara në pikën 2, të këtij neni.

2. Përcaktimi i përmendur në pikën 1, bazohet në të gjitha kriteret e mëposhtme, në lidhje me shërbimet TIK të ofruara nga ofruesi i shërbimeve TIK të palës së tretë:

   a) ndikimi sistemik mbi stabilitetin, vazhdimësinë ose cilësinë e ofrimit të shërbimeve financiare në rast se ofruesi përkatës i shërbimeve TIK do të përballej me një dështim operacional në shkallë të gjerë, duke marrë parasysh numrin e subjekteve financiare dhe vlerën totale të aseteve të subjekteve financiare, të cilave ai u ofron shërbime;

   b) karakteri ose rëndësia sistemike e subjekteve financiare që mbështeten tek ofruesi përkatës i shërbimeve TIK, e vlerësuar në përputhje me parametrat e mëposhtëm:
      i. numri i institucioneve me rëndësi sistemike globale *(G-SII)* ose institucioneve të tjera me rëndësi sistemike *(O-SII*) që mbështeten tek ofruesi përkatës i shërbimeve TIK;

      ii. shkalla e ndërvarësisë midis *G-SII-ve* ose *O-SII-ve* të përmendura në nën-pikën "i" dhe subjekteve të tjera financiare, përfshirë rastet kur G-SII-të ose O-SII-të ofrojnë shërbime infrastrukturore financiare për subjekte të tjera financiare;

c) varësia e subjekteve financiare nga shërbimet e ofruara nga ofruesi përkatës i shërbimeve TIK në lidhje me funksione kritike ose të rëndësishme të subjekteve financiare, që në fund përfshijnë të njëjtin ofrues shërbimesh TIK, pavarësisht nëse subjektet financiare mbështeten mbi këto shërbime në mënyrë direkte apo indirekte, përmes marrëveshjeve të nënkontraktimit;

d) shkalla e zëvendësueshmërisë së ofruesit të shërbimeve TIK, duke marrë në konsideratë parametrat e mëposhtëm:

   i. mungesa e alternativave reale, qoftë edhe të pjesshme, për shkak të numrit të kufizuar të ofruesve të shërbimeve TIK palë të treta që operojnë në një treg specifik, ose për shkak të pjesës së tregut që zotëron ofruesi përkatës, ose kompleksitetit apo sofistikimit teknik, përfshirë teknologji me të drejtë pronësie ekskluzive, si dhe karakteristikat e veçanta të organizimit apo aktivitetit të tij;

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

3. Kur ofruesi i shërbimeve TIK i palës së tretë bën pjesë në një grup, kriteret e përmendura në pikën 2, të këtij neni merren në konsideratë në lidhje me shërbimet TIK të ofruara nga grupi në tërësi.

4. Ofruesit kritikë të shërbimeve TIK palë të treta që janë pjesë e një grupi caktojnë një person juridik si pikë koordinimi, për të siguruar përfaqësim dhe komunikim të duhur me Autoritetin.

5. Përcaktimi i përmendur në pikën 1, shkronja "a", nuk zbatohet për:

   i. subjektet financiare që ofrojnë shërbime të TIK për subjekte të tjera financiare;
   ii. ofruesit e shërbimeve të TIK brenda grupit.

6. Autortieti do të hartojë udhëzime me qëllim përcaktimin e kritereve për caktimin e ofruesve të shërbimeve TIK palë e tretë si kritikë për subjektet financiare

Neni 58
Kompetencat e Autoritetit për mbikëqyrjen ndaj ofruesve kritikë të shërbimeve të TIK, palë të treta

Në përmbushje të detyrimeve të parashikuara nga ky seksion Autoriteti ka kompetencat si vijon:

a) të kërkojë informacion periodik teknik dhe operacional nga ofruesit kritikë të TIK, 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 jap rekomandime ose urdhra mbikëqyrës me afate detyruese për zbatim, kur konstatohen mangësi ose rreziqe serioze.
d) të vendos një mekanizëm formal ndjekjeje të përmbushjes së këtyre rekomandimeve nga ana e ofruesit të shërbimeve TIK palë e tretë, duke përfshirë plane masash dhe verifikim progresi.
e) të kërkojë kufizimin ose ndërprerjen e përdorimit të një ofruesi kritik palë e tretë në rast të vazhdimit të shkeljeve, pengimit të mbikëqyrjes ose rrezikimit të qëndrueshmërisë operacionale të sektorit financiar.
f) të kërkojë që ofruesi kritikë palë e tretë, me seli jashtë territorit të Republikës së Shqipërisë, të caktojë një përfaqësues ligjor në Shqipëri ose të pranojnë shprehimisht juridiksionin e Autoritetit, si kusht për të ofruar shërbime kritike ndaj subjekteve të mbikëqyrura.

Seksioni IV

Kuadri i Mbikëqyrjes për ofruesit e shërbimeve të TIK palë të treta të konsideruar kritikë në Union

Neni 59
Përcaktimi i ofruesve kritikë të shërbimeve TIK të palëve të treta

1. Autoritetet Evropiane Mbikëqyrëse (*ESA-t*), përmes Komitetit të Përbashkët (*Joint Committee*) bazuar në rekomandimin e Forumit të Mbikëqyrjes i ngritur sipas nenit 60, pika 1, kryejnë detyrat e mëposhtme:

a) përcaktojnë ofruesit e shërbimeve të TIK palë e tretë, që konsiderohen kritikë për subjektet financiare, pas një vlerësimi bazuar në kriteret e përcaktuara në pikën 2, të këtij neni;
b) caktojnë Autoritetin Mbikëqyrës Kryesor (*Lead Overseer*) për secilin ofrues kritik të shërbimeve të TIK, që është ESA 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 TIK, vërtetuar nga bilancet individuale të subjekteve financiare.

2. Përcaktimi i përmendur në pikën 1, shkronja "a", bazohet në të gjitha kriteret e mëposhtme që lidhen me shërbimet e TIK të ofruara nga ofruesi përkatës i shërbimeve të TIK palë e tretë:
   a) ndikimi sistemik mbi stabilitetin, vazhdimësinë ose cilësinë e ofrimit të shërbimeve financiare, në rast se ofruesi i shërbimeve të TIK 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 tij;
   b) karakteri ose rëndësia sistemike e subjekteve financiare që mbështeten tek ofruesi përkatës i shërbimeve të TIK, i vlerësuar në përputhje me parametrat e mëposhtëm:
      i. numri i institucioneve globalisht sistemike (G-SII) ose institucioneve të tjera sistemike (O-SII) që mbështeten tek ofruesi përkatës i shërbimeve TIK;
      ii. ndërvarësia midis G-SII-ve ose O-SII-ve të përmendura në pikën "i" dhe subjekteve të tjera financiare, përfshirë rastet kur këto institucione ofrojnë shërbime infrastrukturore financiare për subjekte të tjera financiare;
   c) Varësia e subjekteve financiare nga shërbimet e ofruara nga ofruesi përkatës i shërbimeve të TIK, në lidhje me funksione kritike ose të rëndësishme, përfshirë rastet kur këto funksione mbështeten tek i njëjti ofrues i shërbimeve TIK, pavarësisht nëse kjo varësi është e drejtpërdrejtë apo e tërthortë, përmes marrëveshjeve të nënkontraktimit.
   d) shkalla e zëvendësueshmërisë së ofruesit të shërbimeve të TIK, 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 teknologjinë e mbrojtur me të drejta pronësie ekskluzive, si dhe veçorive specifike të organizimit apo aktivitetit të ofruesit të shërbimeve TIK;
      ii. vështirësitë në migrimin pjesor ose të plotë të të dhënave dhe ngarkesave përkatëse nga ofruesi ekzistues TIK tek një tjetër, për shkak të kostove financiare të konsiderueshme, kohës ose burimeve të nevojshme, apo për shkak të rrezikut të shtuar TIK ose rreziqeve të tjera operacionale që mund të lindin gjatë këtij procesi.

3. Kur ofruesi i shërbimeve TIK i përket një grupi, kriteret e përmendura në pikën 2, merren në konsideratë në lidhje me shërbimet TIK të ofruara nga grupi në tërësi.
4. Ofruesit kritikë të shërbimeve TIK që janë pjesë e një grupi, caktojnë një person juridik, si pikë koordinimi, për të siguruar përfaqësimin dhe komunikimin e duhur me Autoritetin Mbikëqyrës Kryesor (*Lead Overseer*).

5. Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*) njofton ofruesin e shërbimeve TIK, për rezultatin e vlerësimit që çon në përcaktimin e tij si kritik, sipas pikës 1, shkronja "a".
   Brenda 6 javëve nga data e njoftimit, ofruesi i shërbimeve TIK mund të paraqesë pranë Autoritetit Mbikëqyrës Kryesor (*Lead Overseer*) një deklaratë të arsyetuar, e cila mund të shoqërohet me çdo informacion përkatës për qëllime të vlerësimit. Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*) 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 TIK si kritik, ESA-t, përmes 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 TIK 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", nuk aplikohet për rastet e mëposhtme:
   i. subjektet financiare që ofrojnë shërbime TIK për subjekte të tjera financiare;
   ii. ofruesit e shërbimeve TIK 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;
   iii. ofruesit brenda grupit të shërbimeve TIK;
   iv. ofruesit e shërbimeve TIK palë e tretë që ofrojnë shërbime TIK vetëm në një shtet anëtar për subjekte financiare që janë aktive vetëm në atë shtet.
7. ESA-t, përmes Komitetit të Përbashkët, krijojnë, publikojnë dhe përditësojnë çdo vit listën e ofruesve kritikë të shërbimeve TIK palë e tretë, në nivel Bashkimi (*Unioni*).
8. Për qëllimet e pikës 1, shkronja "a", autoritetet kompetente publikojnë çdo vit dhe në mënyrë të përmbledhur raportet e përmendura në nenin 44, pika 3, nënparagrafi i tretë, tek "Forumi i Mbikëqyrjes" i krijuar sipas nenit 60, të kësaj rregulloreje. Forumi i Mbikëqyrjes, vlerëson varësitë e subjekteve financiare nga ofruesit e shërbimeve TIK, bazuar në informacionin e marrë nga autoritetet kompetente.
9. Ofruesit e shërbimeve TIK palë e tretë që nuk janë përfshirë në listën e përmendur në pikën 7, mund të kërkojnë të përcaktohen si kritikë, në përputhje me pikën 1, shkronja "a".
   Për këtë qëllim, ofruesi i shërbimeve TIK, paraqet një kërkesë të arsyetuar pranë EBA, ESMA ose EIOPA, të cilat, përmes Komitetit të Përbashkët, vendosin nëse do ta përcaktojnë ofruesin përkatës të shërbimeve TIK si kritik, në përputhje me pikën 1, shkronja "a".
   Vendimi i përmendur në nënparagrafin e dytë miratohet dhe i njoftohet ofruesit të shërbimeve të TIK, brenda 6 muajve nga marrja e kërkesës.
10. Subjektet financiare, mund të përdorin shërbimet e një ofruesi të shërbimeve TIK palë e tretë të vendosur në një shtet të tretë dhe që është përcaktuar si kritik sipas pikës 1, shkronja "a", vetëm nëse ky ofrues ka krijuar një degë ose filial në Bashkimin Evropian brenda 12 muajve pas përcaktimit.
11. Ofruesi kritik i shërbimeve TIK i përmendur në pikën 10, njofton Autoritetin Mbikëqyrës Kryesor (*Lead Overseer*)për çdo ndryshim në strukturën e menaxhimit të degës ose filialit të krijuar në Bashkim (*Union*).

Neni 60
Struktura e Kuadrit të Mbikëqyrjes

1. Komiteti i Përbashkët (*Joint Committee*), në përputhje me nenin 57, paragrafi 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 Autoritetit Mbikëqyrës Kryesor (*Lead Overseer*) të përmendur në nenin 59, pika 1, shkronja "b", të kësaj rregulloreje, në fushën e rrezikut të shërbimeve të TIK palë e tretë dhenë të gjitha sektorët financiarë. Forumi i Mbikëqyrjes përgatit pozicionet dhe aktet e përbashkëta të këtij Komiteti në këtë fushë.

   Komiteti i përbashkët diskuton rregullisht zhvillimet mbi rrezikun dhe cenueshmëritë e TIK dhe nxit një qasje të qëndrueshme në monitorimin e rrezikut të palëve të treta të TIK në nivel Bashkimi (*Union*).

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 TIK palë e tretë, dhe promovon masa koordinimi për forcimin e qëndrueshmërisë operacionale digjitale të subjekteve financiare, përhapjen e praktikave më të mira në adresimin e rrezikut të përqendrimit të TIK 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 TIK palë e tretë, të cilat miratohen nga Komiteti i Përbashkët, si qëndrim i përbashkët të ESA-ve, në përputhje me nenin 56, paragrafi 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 kompetent përkatës, siç përcaktohet në nenin 46, të rregullores (BE) nr.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 kompetent i përcaktuar në nenin 46 të rregullores (BE) nr.2022/2554, për secilin Shtet Anëtar, me statusin e vëzhguesit;
   e) kur është e aplikueshme, një përfaqësues me status vëzhguesi, i autoriteteve kompetente 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 TIK palë e tretë.

   Forumi i Mbikëqyrjes, kur e konsideron të përshtatshme, kërkon këshillim nga ekspertë të pavarur, të emëruar në përputhje me pikën 6.

5. Çdo shtet anëtar cakton autoritetin kompetent përkatës, i cilit emëron përfaqësuesin e vet në nivel drejtues, i përmendur në pikën 4, shkronja "b" dhe e njofton Autoritetin Mbikëqyrës Kryesor përkatës 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 kompetente të caktuara nga shtetet anëtare.
6. Ekspertët e pavarur të përmendur në pikën 4, paragrafin e dytë, 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 operacionale digjitale dhe sigurisë TIK. Ata veprojnë në mënyrë të pavarur dhe objektive, në interes të vetëm të Bashkimit Evropian si një e 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 Seksion nuk cënojnë 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, përmes Komitetit të Përbashkët dhe mbi bazën e punës përgatitore të kryer nga Forumi i Mbikëqyrjes, paraqesin çdo vit një raport mbi zbatimin e këtij Seksioni në Parlamentin Evropian, Këshillin dhe Komisionin.

Neni 61
Detyrat e Autoritetit Mbikëqyrës Kryesor (*Lead Overseer*)

1. Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*), i emëruar në përputhje me nenin 59, pika 1, shkronja "b", ushtron mbikëqyrjen ndaj ofruesve kritikë të shërbimeve të TIK, palë e tretë, për të gjitha çështjet që lidhen me mbikëqyrjen dhe vepron si pikë kryesore kontakti për këta ofrues.
2. Për qëllimet të pikës 1, Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*) vlerëson nëse ofruesi kritik i shërbimeve të TIK, ka vendosur rregulla, procedura, mekanizma dhe ka marrë masa të plota, të qëndrueshme dhe efektive për të menaxhuar rrezikun e TIK që mund t'u shkaktojë subjekteve financiare. Ky vlerësim përqendrohet kryesisht në shërbimet e TIK të ofruara nga ofrues kritik, që mbështesin funksione kritike ose të rëndësishme të subjekteve financiare.
   Kur është e nevojshme për të adresuar të gjithë rreziqet përkatëse, vlerësimi zgjerohet edhe mbi shërbimet e TIK që mbështesin funksione të tjera, përveç atyre kritike ose të rëndësishme.
3. Vlerësimi i përmendur në pikën 2, duhet të përfshijë:
   a) kërkesat e TIK për të garantuar, sigurinë, disponueshmërinë, vazhdimësinë, ruajtjen e aftësisë për të përballuar rritjen e ngarkesës së përdoruesve apo volumit të të dhënave dhe cilësinë e shërbimeve që ofruesi kritik i shërbimeve të TIK 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) sigurinë fizike që kontribuon në sigurimin e sigurisë së TIK, përfshirë sigurinë e ndërtesave, objekteve dhe bazës së të dhënave;
   c) proceset e menaxhimit të rrezikut, përfshirë politikat e menaxhimit të rrezikut të TIK, politikën e vazhdimësisë së biznesit të TIK dhe planet e reagimit dhe rikuperimit të TIK;

d) kuadrin e qeverisjes, përfshirë një strukturë organizative me linja të qarta, transparente dhe të qëndrueshme përgjegjësie dhe llogaridhënieje, që mundësojnë menaxhim efektiv të rrezikut të TIK;
e) identifikimin, monitorimin dhe raportimin e menjëhershëm të incidenteve të rëndësishme të TIK 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, që sigurojnë ushtrim efektiv të të drejtave të përfundimit të marrëdhënieve kontraktuale nga subjektet financiare;
g) testimin e sistemeve, infrastrukturës dhe kontrolleve të TIK;
h) auditimet e TIK;
i) përdorimin e standardeve kombëtare dhe ndërkombëtare përkatëse që zbatohen për ofrimin e shërbimeve të TIK ndaj subjekteve financiare.

4. Bazuar në vlerësimin e përmendur në pikën 2, dhe në bashkëpunim me Rrjetin e Përbashkët të Mbikëqyrjes (*Joint Oversight Network – JON*) të përmendur në nenin 62, pika 1, Autoriteti Mbikëqyrës Kryesor miraton një plan mbikëqyrjeje individual të qartë**,** të detajuar dhe të arsyetuar, që përshkruan objektivat vjetore të mbikëqyrjes dhe veprimet kryesore të planifikuara për secilin ofrues kritik të shërbimeve të TIK.
Ky plan i komunikohet çdo vit ofruesit përkatës të shërbimeve të TIK.

Para miratimit të planit të mbikëqyrjes, Autoriteti Mbikëqyrës Kryesor i dërgon ofruesit kritik një draft të planit të mbikëqyrjes.

Pas marrjes së këtij drafti, ofruesi kritik i shërbimeve të TIK mund të paraqesë brenda 15 ditëve kalendarike një deklaratë të arsyetuar, duke paraqitur ndikimin e mundshëm ndaj klientëve që janë subjekte jashtë fushës së kësaj Rregulloreje 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 njoftuar ofruesve kritikë të shërbimeve të TIK, autoritetet kompetente mund të marrin masa ndaj këtyre ofruesve vetëm me marrëveshje dhe koordinim me Autoritetin Mbikëqyrës Kryesor.

Neni 62
Koordinimi operacional ndërmjet Autoriteteve Mbikëqyrëse Kryesore (*Lead Overseers*)

1. Për të siguruar një qasje të qëndrueshme ndaj mbikëqyrjes dhe me qëllim mundësimin e strategjive të përgjithshme mbikëqyrjeje të koordinuara dhe qasje operacionale, metodologji pune të bashkërenduar, tre Mbikëqyrësit Kryesorë të emëruar në përputhje me nenin 59, pika 1, shkronja "b", do të krijojnë një Rrjet të Përbashkët të Mbikëqyrjes (*Joint Oversight Network – JON*). Ky rrjet ka për për qëllim koordinimin ndërmjet fazave përgatitore dhe kryerjen e aktiviteteve të mbikëqyrjes mbi ofruesit kritikë të shërbimeve të TIK-ut si palë të treta, si dhe gjatë çdo veprimi që mund të jetë i nevojshëm në zbatim të nenit 70.
2. Për qëllim të pikës 1, Mbikëqyrësit Kryesorë, hartojnë një protokoll të përbashkët mbikëqyrjeje e cila specifikon në mënyrë të detajuar procedurat që duhen ndjekur për

koordinimin e përditshëm dhe të sigurojë shkëmbime dhe reagime të shpejta. Ky protokoll do të rishikohet periodikisht për të pasqyruar nevojat operacionale, në veçanti zhvillimet në praktikat e mbikëqyrjes.

3. Mbikëqyrësit Kryesorë, mbi baza ad hoc mund t'i bëjnë thirrje Bankës Qendrore Evropiane BQE-së dhe Agjencisë së Bashkimit Evropian për Sigurinë Kibernetike 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*).

Neni 63
Kompetencat e Autoritetit Mbikëqyrës Kryesor (Lead Overseer)

1. Mbikëqyrësi Kryesor (*Lead Overseer*) me qëllim kryerjen e detyrave të përcaktuara në këtë Seksion, në lidhje me ofruesit kritikë të shërbimeve të TIK palë e tretë ka kompetencat e mëposhtme:
   a) kërkon të gjithë informacionin dhe dokumentacionin sipas parashikimit në nenin 65
   b) kryen hetime të përgjithshme dhe inspektime në përputhje me nenet 66 dhe 67;
   c) kërkon pas përfundimit të inspektimit mbikëqyrës, raporte që specifikojnë veprimet që janë ndërmarrë ose mjetet juridike që janë zbatuar nga ofruesit kritikë të shërbimeve të TIK si palë e tretë, në lidhje me rekomandimet e referuara në shkronjën "d" të këtij paragrafi;
   d) jep rekomandime mbi fushat e parashikuara në nenin 61, pika 3, veçanërisht në lidhje me:
   i. përdorimin e kërkesave ose proceseve specifike të sigurisë dhe cilësisë së TIK, veçanërisht në lidhje me e implementimin e korrigjimeve (*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 të ofruara ndaj subjekteve financiare;
   ii. përdorimin e kushteve dhe termave, përfshirë zbatimin teknik të tyre, sipas të cilave ofruesit kritikë të shërbimeve TIK palë e tretë i ofrojnë shërbime TIK 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 sistemik në të gjithë sektorin financiar të Bashkimit në rast rrezikut të përqendrimit në fushën e TIK;
   iii. çdo nënkontraktim të planifikuar, ku Mbikëqyrësi Kryesor gjykon se nënkontraktimi i mëtejshëm, përfshirë marrëveshjet e nënkontraktimit që ofruesit kritikë të shërbimeve të TIK palë e tretë planifikojnë të lidhin me ofrues të shërbimeve të TIK palë e tretë ose me nënkontraktorë të TIK 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 65 dhe 66;
   iv. marrëveshja e nënkontaktimit duhet të parashikoje njëkohësisht të gjitha kushtet e mëposhtme:
      - nënkontraktori i parashikuar të jetë një ofrues i shërbimeve TIK palë e tretë ose një nënkontraktor i TIK 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 ose për subjektet financiare, përfshirë aftësinë e tyre për të përmbushur kërkesat mbikëqyrëse.

Për qëllimin e nënpikës "iv" të kësaj pike, ofruesit e shërbimeve të TIK palë e tretë, duke përdorur modelin e parashikuar në nenin 69, pika 1, shkronja "b", do t'i transmetojnë informacionin lidhur me nënkontraktimin Mbikëqyrësit Kryesor.

2. Gjatë ushtrimit të kompetencave të parashikuara në këtë nen, Mbikëqyrësi Kryesor duhet të:

   a) sigurojë koordinim të rregullt brenda Rrjetit të Përbashkët të Mbikëqyrjes (*JON*), dhe në veçanti të kërkojë qasje të qëndrueshme, lidhur me mbikëqyrjen e ofruesve kritikë të shërbimeve të TIK si palë të treta;
   b) marrë në konsideratë kuadrin e vendosur nga Direktiva (BE) 2022/2555 dhe, kur është e nevojshme, konsultohet me autoritetet kompetente përkatëse të caktuara ose të krijuara në përputhje me atë Direktivë, më qëllim shmangien dublikimin e masave teknike dhe organizative që mund të zbatohen ndaj ofruesit kritikë të shërbimeve të TIK si palë të treta në zbatim të asaj Direktive;
   c) synojë minimizimin, për aq sa është e mundur, të rrezikut të ndërprerjes së shërbimeve të ofruara nga ofruesit kritikë të shërbimeve të TIK palë e tretë për klientët që janë subjekte të ndryshme nga ata që përfshihen në fushën e zbatimit të kësaj Rregulloreje.

3. Mbikëqyrësi Kryesor konsultohet me Forumin e Mbikëqyrjes *(Oversight Forum)* përpara se të ushtrojë kompetencat e parashikuara në pikën 1, të këtij neni. Përpara se të japë rekomandime në përputhje me pikën 1, shkronja "d", Autoriteti Mbikëqyrës Kryesor u jep mundësi ofruesve të shërbimeve TIK të paraqesin, brenda 30 ditëve kalendarike, informacion që dëshmon ndikimin e pritshëm mbi klientët që janë subjekte jashtë fushës së zbatimit të Rregullores dhe, kur është e përshtatshme, të formulojnë zgjidhje për zbutjen e rreziqeve.
4. Autoriteti Mbikëqyrës Kryesor informon Rrjetin e Përbashkët të Mbikëqyrjes (*JON*) mbi rezultatet e ushtrimit të kompetencave të parashikuara në pikën 1, shkronjat "a" dhe "b". Mbikëqyrësi Kryesor, pa vonesë të pajustifikuar, përcjell raportet e përmenduara në pikën 1, shkronja "c", tek *JON* dhe tek autoritetet kompetente të subjekteve financiare që përdorin shërbimet e TIK të ofruesit kritik të shërbimeve, palë e tretë.
5. Ofruesit kritikë të shërbimeve të TIK palë e tretë do të bashkëpunojnë me mirëbesim me Mbikëqyrësin Kryesor (*Lead Overseer*) dhe do ta asistojë atë 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", dhe pas përfundimit të afatit prej të paktën 30 ditësh kalendarike nga data kur ofruesi kritik i shërbimeve të TIK palë e tretë ka marrë njoftimin për masat përkatëse, Mbikëqyrësi Kryesor vendos një gjobë periodike për të detyruar ofruesin kritik të shërbimeve të TIK palë e tretë të përmbushë këto masa.

7. Ofruesit kritik të shërbimeve të TIK palë e tretë, penalizohet me gjobë periodike sipas parashikimit në pikën 6, gjobë e cila vendoset mbi baza ditore derisa të arrihet përputhshmëria por jo më të gjatë se gjashtë muaj nga njoftimi i vendimit për vendosjen e gjobës periodike.
8. Shuma e gjobës periodike, e llogaritur nga data e përcaktuar në vendimin për vendosjen e saj, do të jetë deri në 1% të të ardhurave të përditshme mesatare në nivel botëror të ofruesit kritik të shërbimeve të TIK palë e tretë gjatë vitit të mëparshëm financiar. Gjatë përcaktimit të shumës së gjobës, Autoriteti Mbikëqyrës 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 të shërbimeve TIK me Autoritetin Mbikëqyrës Kryesor.

   Për qëllimet e nënparagrafit të parë, për të siguruar qasje të qëndrueshme, Autoriteti Mbikëqyrës Kryesor konsultohet me Rrjetin e Përbashkët të Mbikëqyrjes (*JON*).
9. Gjobat periodike kanë natyrë administrative dhe janë të ekzekutueshme. Ekzekutimi do të rregullohet sipas procedurës civile në fuqi në Shtetin Anëtar në territorin e të cilit do të kryhen inspektimet dhe qasja. Gjykatat kompetente për shqyrtimin e ankimit lidhur me sjelljen e parregullt të ekzekutimit do të jetë gjykata e Shtetit Anëtar përkatës. Shumat e mbledhura nga gjobat do t'i alokohen buxhetit të përgjithshëm të Bashkimit Evropian.
10. Mbikëqyrësi Kryesor (*Lead Overseer*) 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 propocional palëve të përfshira.
11. Para vendosjes së një gjobe periodike sipas pikës 6, Autoriteti Mbikëqyrës Kryesor u jep përfaqësuesve të ofruesit kritik të shërbimeve TIK 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.

    Të drejtat e mbrojtjes së palëve që i nënshtrohen procedurës respektohen plotësisht gjatë procesit.

    Ofruesi kritik i shërbimeve të TIK 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 Autoritetit Mbikëqyrës Kryesor.

Neni 64
Ushtrimi i kompetencave të Mbikëqyrësit Kryesor (*Lead Overseer*) jashtë *Unionit*

1. Kur objektivat e mbikëqyrjes nuk mund të arrihen me anë të ndërveprimit me filialin e krijuar për qëllimin e nenit 59, pika 12, ose përmes ushtrimit të aktiviteteve të mbikëqyrjes në ambiente të vendosura brenda Bashkimit, Autoriteti Mbikëqyrës Kryesor (*Lead Overseer*) mund të ushtrojë kompetencat e përcaktuara në dispozitat e mëposhtme, në çdo ambient të vendosur në një shtet të tretë, që është në pronësi ose përdoret për ofrimin e shërbimeve ndaj subjekteve financiare të Bashkimit, nga një ofrues kritik i shërbimeve TIK palëve e tretë, 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 63, pika 1,shkronja "a"; dhe

b) në nenin 63, pika 1, shkronja “b”, në përputhje me nenin 66, pika 2, shkronjat “a”, “b” dhe “d”, dhe në nenin 67, pika 1 dhe 2, shkronja “a”.

Kompetencat e parashikuara në nënparagrafin e parë, mund të ushtrohen duke iu nënshtruar të gjitha kushteve të mëposhtme:

i. kryerja e inspektimit në një vend të tretë konsiderohet e nevojshme nga Mbikëqyrësi Kryesor për t'i lejuar atij të kryejë plotësisht dhe efektivisht detyrat e tij sipas kësaj Rregulloreje;

ii. inspektimi në një vend të tretë lidhet drejtpërdrejt me ofrimin e shërbimeve të TIK për subjektet financiare në Bashkim (*Union*);

iii. ofruesi kritik i shërbimeve të TIK palë e tretë jep pëlqimin për kryerjen e një inspektimi në një vend të tretë; dhe

iv. autoriteti kompetent i vendit të tretë është njoftuar zyrtarisht nga Mbikëqyrësi Kryesor dhe nuk ka ngritur asnjë kundërshtim ndaj tij.

2. Pa cënuar kompetencat e institucioneve përkatëse të Bashkimit (*Unionit*) dhe të Shteteve Anëtare, për qëllimet e pikës 1, EBA, ESMA ose EIOPA lidhin marrëveshje bashkëpunimi administrative me autoritetin përkatës të vendit të tretë për të mundësuar inspektime në vendin e tretë nga Mbikëqyrësi Kryesor dhe ekipi caktuar prej tij për misionin e tij në vendin e tretë. Marrëveshja e bashkëpunimit nuk krijon detyrime ligjore lidhur me Unionin dhe Shtetet e tij Anëtare dhe as nuk pengon Shtetet Anëtare dhe autoritetet e tyre kompetente të lidhin marrëveshje dypalëshe ose shumëpalëshe me ato vende të treta dhe autoritetet e tyre përkatëse.

Marrëveshja e bashkëpunimit specifikon të paktën elementet e mëposhtme:

a) procedurat për koordinimin e aktiviteteve të mbikëqyrëse të kryera sipas kësaj Rregulloreje dhe çdo monitorim analog të rrezikut të TIK palë e tretë në sektorin financiar të ushtruar nga autoriteti kompetent i vendit të tretë, përfshirë detajet për transmetimin e marrëveshjes së këtij të fundit 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, në territorin nën juridiksionin e tij;

b) mekanizmin për transmetimin e çdo informacioni ndërmjet EBA-s, ESMA-s ose EIOPA-s dhe autoritetit kompetent të vendit të tretë, veçanërisht lidhur me informacionin që mund të kërkohet nga Mbikëqyrësi Kryesor në zbatim të nenit 65.

c) mekanizmat për njoftim të menjëhershëm nga autoriteti kompetent i vendit të tretë në fjalë tek EBA, ESMA ose EIOPA të rasteve kur një ofrues i shërbimeve të TIK palë e tretë i themeluar në një vend të tretë dhe i përcaktuar si kritik në përputhje me nenin 59, pika 1, shkronja “a”, konsiderohet se ka shkelur detyrimet ligjore sipas ligjeve të zbatueshme të atij shteti gjatë ofrimit të shërbimeve për institucionet financiare atje, si dhe për masat korrigjuese si dhe sanksionet e zbatuara;

d) transmetimin periodik të përditësimeve mbi zhvillimet rregullatore ose mbikëqyrëse lidhur me monitorimin e rrezikut të TIK pale e tretë, për institucionet financiare në shtetin e tretë përkatës;

e) detajet lidhur me autorizimin e pjesëmarrjes, sipas rastit, të një përfaqësuesi të autoritetit kompetent të një vendi të tretë, në inspektimet e kryera nga Mbikëqyrësi Kryesor dhe ekipi i autorizuar."

3. Kur Mbikëqyrësi Kryesor nuk është në gjendje të kryejë aktivitete mbikëqyrjeje jashtë Bashkimit *(Unionit)*, të parashikuara në pikat 1 dhe 2, Mbikëqyrësi Kryesor:
   a) ushtron kompetencat e tij sipas nenit 63, 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 këtij neni.

Në hartimin e rekomandimeve të Mbikëqyrësit Kryesor, të nxjerra në bazë të nenit 63, pika 1, shkronja "d", do të merren në konsideratë pasojat e mundshme të përcaktuara në shkronjën "b" të këtij paragrafi.

Neni 65
Kërkesa për informacion

1. Mbikëqyrësi Kryesor *(Lead Overseer)* me kërkesë ose me vendim, mund të kërkojë nga ofruesit kritikë të shërbimeve të TIK palë e treta të vënë në dispozicion të gjitha informacionet e nevojshme për ushtrimin e detyrave, në bazë të kësaj Rregulloreje, përfshirë dokumentet tregtare ose operacionale, kontratat, politikat, dokumentacionin teknik, raportet e auditimit të sigurisë së TIK, raportet e incidenteve të lidhura me TIK, si dhe çdo informacion që lidhet me palët ndaj të cilave ofruesi kritik i shërbimeve TIK palë e tretë ka nënkontraktuar funksione ose aktivitete operacionale.

2. Kur Mbikëqyrës Kryesor *(Lead Overseer)* bën kërkesë për informacion sipas pikës 1, ai duhet të:
   a) referohet në këtë nen si bazë ligjore të kërkesës;
   b) deklarojë qëllimin e kërkesës;
   c) specifikojë se çfarë informacioni kërkohet;
   d) vendosë një afat kohor brenda të cilit duhet të ofrohet informacioni;
   e) informojë përfaqësuesin e ofruesit kritik të shërbimeve të TIK palë e tretë nga i cili kërkohet informacioni se nuk është i detyruar të ofrojë informacionin, por në rast se përgjigjet ndaj kërkesës, informacioni i ofruar duhet të jetë i saktë dhe orientues.
3. Kur Mbikëqyrësi Kryesor *(Lead Overseer),* kërkon me vendim dhënien e informacionit sipas pikës 1, ai do të:
   a) referohet në këtë nen si bazë ligjore e kërkesës;
   b) deklarojë qëllimin e kërkesës;
   c) specifikojë se cili informacion kërkohet;
   d) vendosë një afat kohor brenda të cilit duhet të ofrohet informacioni;
   e) tregojë gjobat periodike të parashikuara në nenin 63, pika 6, në rast se informacioni i kërkuar është i paplotë ose kur ky informacion nuk ofrohet brenda afatit kohor të referuar në shkronjën "d" të këtij paragrafi;

f) tregojë të drejtën për të ankimuar vendimin përpara Bordit të Apelimit 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 TIK palë e tretë do të japin informacionin e kërkuar. Avokatët e autorizuar mund të cilët veprojnë në emër të klientëve të tyre për dorëzimin e informacionit. Ofruesi kritik i shërbimeve të TIK palë e tretë është plotësisht përgjegjës nëse informacioni i dhënë është i paplotë, i pasaktë ose çorientues.
5. Mbikëqyrësi Kryesor *(Lead Overseer)*duhet, pa vonesë të transmetojë një kopje të vendimit për dhënien e informacionit autoriteteve kompetente të subjekteve financiare që përdorin shërbimet e ofruesve përkatës kritikë të shërbimeve të TIK palë e tretë dhe Rrjeti i Përbashkët i Mbikëqyrjes *(JON).*

Neni 66
Hetimet e përgjithshme

1. Për të ushtruar detyrat sipas kësaj Rregulloreje, Mbikëqyrës Kryesor *(Lead Overseer*), i asistuar nga ekipi i përbashkët i inspektimit sipas nenit 68, pika 1, kur është e nevojshme mund të zhvillojë hetime ndaj ofruesve kritikë të shërbimeve TIK palë e tretë.

2. Mbikëqyrësi Kryesor*(Lead Overseer*) ka kompetencën për të:
   a) inspektuar regjistra (*records*), të dhëna, procedura dhe çdo material tjetër të rëndësishmëm për ushtrimin e detyrave të tij, pavarësisht nga formës ose mjetin në të cilin ruhen ato;
   b) marrë ose siguruar kopje të çertifikuara ose ekstrakte nga këto regjistra, të dhëna, procedura të dokumentuara dhe çdo material tjetër;
   c) thirrur përfaqësues të ofruesit kritik të shërbimeve të TIK palë e tretë, për të dhënë shpjegime me gojë ose me shkrim mbi fakte ose dokumente që lidhen me objektin dhe qëllimin e hetimit si dhe të regjistrojë përgjigjet;
   d) intervistuar çdo person fizik ose juridik që pranon të intervistohet me qëllim mbledhjen e informacionit lidhur me objektin hetimit;
   e) kërkuar regjistrime të komunikimeve telefonike dhe qarkullimit të të dhënave.

3. Zyrtarët dhe personat e autorizuar nga Mbikëqyrësi Kryesor (*Lead Overseer*) me qëllim kryerjen e hetimit të parashikuar në pikën 1, 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 63, pika 6, në rast se dorëzimi i regjistrimeve të kërkuara, të dhënat, procedurae e dokumentuara ose çdo materiali tjetër, ose përgjigjet ndaj pyetjeve të bëra përfaqësuesve të ofruesit të shërbimeve të TIK si palë e tretë nuk ofrohen ose janë të paplota.
4. Përfaqësuesit e ofruesve kritikë të shërbimeve të TIK palë e tretë janë të detyruar t'i nënshtrohen hetimeve në bazë të një vendimi të Mbikëqyrësit Kryesor (*Lead Overseer*). Vendimi duhet të specifikojë objektin dhe qëllimin e hetimit, gjobat periodike të parashikuara në nenin 63, pika 6, mjetet juridike të disponueshme sipas Rregulloreve (BE)

Nr. 1093/2010, (BE) Nr. 1094/2010 dhe (BE) Nr. 1095/2010, dhe të drejtën pwr tw ankimuar vendimin pranë Gjykatës së Drejtësisë (*Court of Justice*).

5. Përpara fillimit të hetimit, brenda një afati të arsyeshëm Mbikëqyrësi Kryesor (*Lead Overseer*) duhet të informojë autoritetet kompetente të subjekteve financiare që përdorin shërbimet e TIK të ofruesit kritik të shërbimeve të TIK palë e tretë, për hetimin e parashikuar dhe për identitetin e personave të autorizuar. Mbikëqyrësi Kryesor (*Lead Overseer*) do t'i komunikojë Rrjeti i Përbashkët i Mbikëqyrjes (*JON*) të gjithë informacionin e transmetuar në përputhjë me nënparagrafit e parë.

Neni 67
Inspektimet

1. Me qëllim përmbushjen e detyrave sipas kësaj Rregulloreje, Mbikëqyrësi Kryesor (*Lead Overseer*), i asistuar nga ekipet e përbashkëta të inspektimit të referuara në nenin 68, pika 1, kryen të gjitha inspektimet e nevojshme në vend (*on-site inspections*) në çdo mjedis biznesi, tokë ose pronë të ofruesve të shërbimeve të TIK, si palë të treta, siç janë zyrat qendrore, qendrat e operimit, mjediset dytësore, si dhe të kryejë inspektime në distancë (*off-site inspections*). Për qëllimet e ushtrimit të kompetencave të referuara në nënparagrafin e parë, Mbikëqyrësi Kryesor do të konsultohet me *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) Të vendosin "bllokim" mbi çdo ambient biznesi, libër apo regjistër të tillë, për periudhën dhe në masën e nevojshme për kryerjen e inspektimit. 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 63, pika 6, në rast se përfaqësuesit e ofruesve kritikë të shërbimeve të TIK-ut, si palë të treta në fjalë, nuk i nënshtrohen inspektimit.
3. Përpara fillimit të inspektimit, Mbikëqyrësi Kryesor informon autoritetet kompetente të subjekteve financiare që përdorin atë ofrues shërbimesh TIK si palë e tretë.
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 TIK-ut, si palë të treta, një njoftim paraprak, përveç rasteve kur një njoftim i tillë nuk është i mundur për shkak të një situate emergjente ose krize, apo kur dhënia e tij do të ndikonte në efektivitetin e inspektimit ose auditimit
6. Ofruesi kritik i shërbimeve të TIK-ut si palë e tretë do t'u nënshtrohet inspektimeve në vend me vendim të Mbikëqyrësit Kryesor. Vendimi do të specifikojë objektin dhe qëllimin e inspektimit, do të caktojë datën në të cilën do të fillojë inspektimi dhe do të tregojë gjobat periodike të parashikuara në nenin 63 pika 6, mjetet juridike të disponueshme sipas Rregulloreve (BE) Nr. 1093/2010, (BE) Nr. 1094/2010 dhe (BE) Nr. 1095/2010, si dhe të drejtën për të pasur vendimin të rishikuar nga Gjykata e Drejtësisë.

7. Kur zyrtarët dhe personat e tjerë të autorizuar nga Mbikëqyrësi Kryesor konstatojnë se një ofrues kritik i shërbimeve të TIK-ut si palë e tretë kundërshton një inspektim të urdhëruar në zbatim të këtij neni, Mbikëqyrësi Kryesor do të informojë ofruesin kritik të shërbimeve të TIK-ut si palë e tretë për pasojat e kundërshtimit, përfshirë mundësinë që autoritetet kompetente të subjekteve financiare përkatëse t'u kërkojnë subjekteve financiare të zgjidhin marrëveshjet kontraktuale të lidhura me atë ofrues kritik të shërbimeve të TIK-ut si palë e tretë.

Neni 68
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 TIK palë e tretë.
2. Ekipi i përbashkët i inspektimit (*joint examination team*), i përmendur në pikën 1, përbëhet nga anëtarë të stafit të:
   a) Autoriteteve Evropiane Mbikëqyrëse (ESAs);
   b) autoritetet kompetente përkatëse kombëtare që mbikëqyrin subjektet financiare të cilave ofruesi kritik i shërbimeve të TIK u ofron këto shërbime;
   c) autoriteti kombëtar kompetent sipas nenit 60, pika 4, shkronja "e", mbi baza vullnetare;
   d) një autoriteti kombëtar kompetent nga Shteti Anëtar, ku është themeluar ofruesi kritik i shërbimeve të TIK si palë e tretë, mbi baza vullnetare.

   Anëtarët e ekipit të përbashkët të inspektimit (*joint examination team*) duhet të kenë ekspertizë në çështjet e TIK dhe në rrezikun operacional. Ekipi i përbashkët i inspektimit (*joint examination team*), do të punojë nën koordinimin e një anëtari të stafit të caktuar të Mbikëqyrësit Kryesor (*the 'Lead Overseer coordinator')*.

3. Brenda 3 muajve nga përfundimi i një hetimi ose inspektimi, Mbikëqyrësi Kryesor (*Lead Overseer*), pas konsultimit me Forumin e Mbikëqyrjes (*Oversight Forum)*, miraton rekomandime që do t'i drejtohen ofruesit kritik të shërbimeve të TIK palë e tretë në zbatim të kompetencave të parashikuara në nenin 63.
4. Rekomandimet, referuar pikës 3, do t'i komunikohen menjëherë ofruesit kritik të shërbimeve të TIK palë e tretë dhe autoriteteve kompetente të subjekteve financiare të cilave ai u ofron shërbime TIK.

   Me qëllim e përmbushjes të veprimtarisë mbikëqyrëse, Mbikëqyrësi Kryesor (*Lead overseer*) mund të marrë në konsideratë çdo certifikim të palëve të treta dhe raporte të auditimit të brendshëm ose të jashtëm të palëve të treta të TIK, të vëna në dispozicion nga ky ofrues.

Neni 69
Harmonizimi i kushteve që mundësojnë kryerjen e aktiviteteve të mbikëqyrjes

1. Autoritetet Evropiane Mbikëqyrëse (*ESAs*), përmes Komitetit të Përbashkët (*Joint Committee*), hartojnë standarde teknike rregullatore, me qëllim përcaktimin e:

a) informacionit që duhet të ofrohet nga një ofrues i shërbimeve TIK palë e tretë, në kërkesën vullnetare për t'u përcaktuar si ofrues kritik, në përputhje me nenin 59, pika 11;
b) përmbajtjes, strukturës dhe formatit të informacionit që duhet paraqitur, publikuar ose raportuar nga ofruesit e shërbimeve të TIK palë e tretë, në përputhje me nenin 63, pika 1, duke përfshirë modelin standard për ofrimin e informacionit mbi marrëveshjet e nënkontraktimit;
c) kritereve për përcaktimin e përbërjes së ekipeve të përbashkëta të inspektimit (*joint examination teams*), me qëllim sigurimin e një pjesëmarrjeje të balancuar të anëtarëve të stafit nga ESAs dhe nga autoritetet kompetente përkatëse, përfshirë rregullat për emërimin, detyrat dhe mënyrën e funksionimit të tyre;
d) detajeve të vlerësimit nga autoritetet kompetente të masave të marra nga ofruesit kritikë të shërbimeve të TIK, bazuar në rekomandimet e Mbikëqyrësit Kryesor (*Lead Overseer*), në përputhje me nenin 70, pika 3.

Neni 70
Ndjekja (*Follow-up*) nga autoritetet kompetente

1. Brenda 60 ditëve kalendarike nga marrja e rekomandimeve të dhëna nga Mbikëqyrësi Kryesor (*Lead Overseer*) në përputhje me nenin 63, pika 1, shkronja "d", ofruesit kritikë të shërbimeve të TIK palë e tretë do të njoftojnë Mbikëqyrësin Kryesor (*Lead Overseer*) për qëndimin e tyre lidhur me ndjekjen dhe zbatimin e rekomandimeve ose do të ofrojnë një shpjegim të arsyetuar për mosndjekjen e rekomandimeve. Mbikëqyrësi Kryesor (*Lead Overseer*) duhet ta transmetojë këtë informacion menjëherë autoriteteve kompetente të subjekteve financiare në fjalë.
2. Mbikëqyrësi Kryesor (*Lead Overseer*) publikon rastet kur një ofrues kritik i shërbimeve të TIK palë e tretë nuk njofton Mbikëqyrësin Kryesor në përputhje me paragrafin 1, ose kur shpjegimi i ofruar nga ofruesi kritik i shërbimeve të TIK palë e tretë nuk konsiderohet i mjaftueshëm.. Informacioni i publikuar duhet të përmbajë identitetin e ofruesit kritik të shërbimeve TIK, si dhe llojin dhe natyrën e mospërputhjes. Publikimi duhet të kufizohet vetëm për që 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 (*Union*).

   Mbikëqyrësi Kryesor njofton ofruesin e shërbimeve të TIK palë e tretë për publikimin.

3. Autoritetet kompetente informojnë subjektet financiare përkatëse për rreziqet e identifikuara në rekomandimet drejtuar ofruesve kritikë të shërbimeve të TIK palë e tretë në përputhje me nenin 63, pika 1, shkronja "d". Gjatë menaxhimit të rrezikut të palës së tretë të TIK, subjektet financiare marrin parasysh rreziqet e referuara në nënparagrafine parë.

4. Kur autoriteti kompetent 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 menaxhimit të rrezikut të TIKt nga palë të treta, si dhe në mungesë

të dispozitave kontraktuale që adresojnë këto rreziqe, ai 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 63, pika 1, shkronja "c", dhe para marrjes së një vendimi siç parashikohet në pikën 6, të këtij neni, autoritetet kompetente, mbi baza vullnetare, mund të konsultohen me autoritetet kompetente të caktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555 përgjegjëse për mbikëqyrjen e një subjekti thelbësor ose të rëndësishëm që i nënshtrohet asaj Direktive, i cili është përcaktuar si një ofrues kritik i shërbimeve të TIK palë e tretë.
6. Autoritetet kompetente, si masë e fundit, pas njoftimit dhe konsultimit sipas pikave 4 dhe 5, të këtij neni, dhe në përputhje me nenin 78, të kësaj rregulloreje, mund të vendosin që subjektet financiare të pezullojnë përkohësisht, pjesërisht ose plotësisht, përdorimin apo vendosjen e një shërbimi të ofruar nga një ofrues kritik i shërbimeve të TIK palë e tretë, deri në adresimin e rreziqeve të identifikuara në rekomandimet përkatëse. Kur është e nevojshme, autoritetet kompetente mund të kërkojnë gjithashtu zgjidhjen, pjesërisht ose plotësisht, të marrëveshjeve kontraktuale përkatëse me këta ofrues.
7. Kur një ofrues kritik i shërbimeve të TIK-ut palë e tretë refuzon të zbatojë rekomandimet, 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 autoriteteve kompetente nuk rezultojnë efektive për zbutjen e rrezikut ndaj stabilitetit financiar, Mbikëqyrësi Kryesor, pas konsultimit me Forumin e Mbikëqyrjes, mund të japë opinione jo detyruese dhe jo publike për autoritetet kompetente, me qëllim promovimin e masave të qëndrueshme mbikëqyrëse.
8. Pas marrjes së raporteve sipas në nenin 63, pika 1, shkronja "c", autoritetet kompetente, kur marrin një vendim siç parashikohet në pikën 6, të këtij neni, marrin parasysh llojin dhe madhësinë e rrezikut i cili nuk është adresuar nga ofruesi kritik i shërbimeve të TIK palë e tretë, 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, menaxhimin e rrezikut dhe kontrollet e brendshme të ofruesit kritik të shërbimeve të TIK palë e tretë;
   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 ndërprerje në ofrimin e shërbimeve të tij;
   f) kur është e aplikueshme, opinionin vullnetar e autoriteteve kompetente të caktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555 përgjegjës për mbikëqyrjen e një subjekti thelbësor ose të rëndësishëm që i nënshtrohet kësaj Direktive, i cili është caktuar si ofrues kritik i shërbimeve të TIK palë e tretë, në përputhje me pikën 5, të këtij neni.

Autoritetet kompetente i japin subjekteve financiare kohën e nevojshme për të rishikuar marrëveshjet me ofruesit kritikë të shërbimeve TIK palë e tretë, me qëllim shmangien e rreziqeve për qëndrueshmërinë e operacioneve digjitale dhe duke mundësuar vendosjen e strategjive dalëse (*exit strategies*) dhe planeve të tranzicionit, sipas nenit 44.

9. Referuar parashikimit në pikën 6, të këtij neni, Vendimi sipas nenin 60, pika 4, shkronjat "a", "b" dhe "c", do t'u njoftohet anëtarëve të Forumit të Mbikëqyrjes (*Oversight Forum*) dhe *JON.* Ofruesit kritikë të shërbimeve të TIK palë e tretë të cilët preken nga Vendimi, do të bashkëpunojnë plotësisht me subjektet financiare të prekura, për pezullimin ose zgjidhjen e marrëveshjeve kontraktuale.
10. Autoritetet kompetente informojnë rregullisht Mbikëqyrësin Kryesor (*Lead Overseer*) mbi qasjet dhe masat e marra në detyrat e tyre mbikëqyrëse, lidhur me subjektet financiare si dhe mbi marrëveshjet kontraktuale të lidhura nga subjektet financiare ku ofruesit kritikë të shërbimeve të TIK palë e tretë nuk kanë mbështetur pjesërisht ose plotësisht rekomandimet e drejtuara atyre nga Mbikëqyrësi Kryesor (Lead Overseer).
11. Mbikëqyrësi Kryesor *(Lead Overseer)*, me kërkesë, udhëzon autoritetet kompetente mbi masat vijuese dhe mund të ofrojë sqarime të mëtejshme mbi rekomandimet e dhëna.

Neni 71
Tarifat e mbikëqyrjes

Mbikëqyrësi Kryesor, në përputhje me pikën 2, të këtij neni, tarifon ofruesit kritikë të shërbimeve të TIK palë e tretë, me tarifa. Këto tarifa mbulojnë shpenzimet e nevojshme të Mbikëqyrësit Kryesor (*Lead Overseer*) lidhur me kryerjen e detyrave mbikëqyrëse në zbatim të kësaj Rregulloreje, përfshirë rimbursimin e çdo kostoje që mund të shkaktohet si rezultat i punës së kryer nga ekipi i përbashkët i inspektimit (*joint examination team*) parashikuar në nenin 68, si dhe kostot e kështillimeve të ofruara nga ekspertët e pavarur siç parashikohet në nenin 60, pika 4, nënparagrafi i dytë, lidhur me çështjet që bien nën kompetencën e aktiviteteve të drejtpërdrejta të mbikëqyrjes.

Shuma e një tarife të ngarkuar ndaj një ofruesi kritik të shërbimeve të TIK palë e tretë do të mbulojë të gjitha kostot që rrjedhin nga ekzekutimi i detyrave të përcaktuara në këtë Seksion si dhe do të jetë proporcionale.

Neni 72
Bashkëpunimi ndërkombëtar

1. Pa cënuar nenin 64, EBA, ESMA dhe EIOPA, në përputhje me nenin 33, të Rregulloreve (BE) Nr. 1093/2010, (BE) Nr. 1095/2010 dhe (BE) Nr. 1094/2010, mund të lidhin marrëveshje administrative me autoritetet rregullatore dhe mbikëqyrëse të vendeve të treta për të nxitur bashkëpunimin ndërkombëtar mbi rrezikun e palëve të treta të TIK në sektorë të ndryshëm financiarë, veçanërisht duke zhvilluar praktikat më të mira, për rishikimin e praktikave dhe kontrolleve të menaxhimit të rrezikut të TIK, masave zbutëse dhe reagimeve ndaj incidenteve.

2. ESAs, përmes Komitetit të Përbashkët (*Joint Committee*), duhet të paraqesin çdo pesë vjet një raport të përbashkët konfidencial në Parlamentin Evropian, në Këshill dhe në Komision, duke përmbledhur gjetjet e diskutimeve përkatëse të mbajtura me autoritetet e vendeve të treta të referuar pikës 1, me fokus në zhvillimin e rrezikut të TIK nga palët e treta dhe ndikimi i tij në stabilitetin financiar, integritetin e tregut, mbrojtjen e investitorëve dhe funksionimin e tregut të brendshëm.

KREU VI
Marrëveshjet për ndarjen e informacionit

Neni 73
Marrëveshjet për shkëmbimin e informacionit mbi kërcënimet dhe inteligjencën kibernetike

1. Subjektet financiare mund të shkëmbejnë ndërmjet tyre informacion mbi kërcënimet kibernetike, përfshirë tregues të kompromitimit, taktika, teknika dhe procedura, alarme të sigurisë kibernetike dhe mjete konfigurimi, në masën një shkëmbim i tillë informacioni dhe inteligjence:

    a) synon të rrisë qëndrueshmërinë operacionale digjitale të subjekteve financiare, veçanërisht nëpërmjet përmirësimit të paralajmërimit ndaj kërcënimeve kibernetike, kufizimit ose parandalimit të përhapjes së tyre, forcimit të kapaciteteve mbrojtëse, teknikave të zbulimit të kërcënimeve, strategjive të zbutjes, si dhe fazave të reagimit dhe rikuperimit;
    b) zhvillohet brenda platformave të besuara të subjekteve financiare.
    c) zbatohet përmes marrëveshjeve për shkembimin e informacionit, të cilat mbrojnë natyrën potencialisht të ndjeshme të informacionit të ndarë dhe që qeverisen nga rregulla sjelljeje në përputhje të plotë me konfidencialitetin e biznesit, mbrojtjen e të dhënave personale dhe udhëzimeve mbi politikën e konkurrencës.

2. Për qëllimet e pikës 1, shkronja "c", marrëveshjet për shkëmbimin e informacionit përcaktojnë kushtet e pjesëmarrjes sipas rastit, përmbajnë detaje mbi përfshirjen e autoriteteve publike dhe rolin e tyre në këto marrëveshje, mbi përfshirjen e ofruesve të shërbimeve të TIK palë të treta, si dhe mbi elementet operacionale, përfshirë përdorimin e platformave të dedikuara IT.

3. Subjektet financiare, njoftojnë Autoritetin për pjesëmarrjen e tyre në marrëveshjet për shkëmbimin e informacionit të përmendura në pikën 1, menjëherë pas konfirmimit të anëtarësimit, ose sipas rastit, për ndërprerjen e anëtarësimit të tyre, në momentin kur kjo ndërprerje hyn në fuqi.

Neni 74
Bashkëpunimi me strukturat dhe institucionet e krijuara sipas Direktivës (BE) 2022/2555

1. Për të nxitur bashkëpunimin dhe për të mundësuar shkëmbimin mbikëqyrës ndërmjet autoriteve të caktuara në bazë të kësaj Rregulloreje dhe Grupit të Bashkëpunimit, Autoritetet Evropiane Mbikëqyrëse (ESA) dhe autoritetet kompetente mund të marrin pjesë në veprimtaritë e Grupit të Bashkëpunimit për çështje që lidhen me aktivitetet e tyre mbikëqyrëse në raport me subjektet financiare.

    ESA-të dhe autoritetet kompetente mund të kërkojnë të ftohen për të marrë pjesë në veprimtaritë e Grupit të Bashkëpunimit për çështje që lidhen me entitete të rëndësishme,

që i nënshtrohen Direktivës (BE) 2022/2555, të cilat janë përcaktuar gjithashtu si ofrues kritikë të shërbimeve TIK të palëve të treta, në përputhje me nenin 59 të kësaj Rregulloreje.

2. Kur është e përshtatshme, autoritetet kompetente mund të konsultohen dhe të shkëmbejnë informacion me pikat unike të kontaktit dhe me Ekipet e Reagimit ndaj Incidenteve të Sigurisë Kompjuterike (CSIRT-s) të caktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555.
3. Kur është e përshtatshme, autoritetet kompetente mund të kërkojnë këshillim dhe asistencë teknike përkatëse nga autoritetet kompetente të caktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555, dhe të krijojnë marrëveshje bashkëpunimi që mundësojnë vendosjen e mekanizmave efektivë dhe të shpejtë të koordinimit dhe reagimit.
4. Marrëveshjet e përmendura në pikën 3, të këtij neni mund të përcaktojnë, ndër të tjera, procedurat për koordinimin e aktiviteteve mbikëqyrëse dhe të mbikëqyrjes së përgjithshme në lidhje me entitetet thelbësore ose të rëndësishme që janë subjekt i Direktivës (BE) 2022/2555 dhe që janë caktuar si ofrues kritikë të shërbimeve TIK të palëve të treta në përputhje me nenin 59, të kësaj Rregulloreje, përfshirë zhvillimin, në përputhje me të drejtën kombëtare, të hetimeve dhe inspektimeve në terren, si dhe mekanizmat për shkëmbimin e informacionit ndërmjet autoritete kompetente sipas kësaj Rregulloreje dhe autoriteve kompetente të caktuara ose të krijuara në përputhje me atë Direktive, duke përfshirë aksesin në informacionin e kërkuar nga ato autoritete.

Neni 75
Bashkëpunimi ndërinstitucional

Autoriteti bashkëpunon ngushtë me AKSK dhe Bankën e Shqipërisë, me qëllim shkëmbimin e infromacionit që lidhet me ofruesit kritikë të shërbimeve TIK palë e tretë, informacion, i cili gjykohet se është i nevojshëm për zbatimin e kësaj Rregulloreje, veçanërisht në lidhje me rreziqet e identifikuara, qëndrime të mbajtura dhe masat e marra si pjesë e detyrave mbikëqyrjese.

Neni 76
Konfidencialiteti dhe mbrojtja e të dhënave

1. Çdo informacion konfidencial i marrë, i shkëmbyer ose i transmetuar në përputhje me këtë Rregullore i nënshtrohet kushteve të përcaktuara në pikën 2.
2. Detyrimi për ruajtjen e konfidencialitetit e kanë të gjithë personat që punojnë ose kanë punuar për Autoritetin ose subjekte të tjera publik ose privat, në zbatim të kësaj të cilët autoritetet u kanë deleguar kompetencat e tyre, përfshirë audituesit dhe ekspertët e kontraktuar prej tyre.
3. Autoriteti mund të përpunojë të dhënat personale vetëm kur është e nevojshme për qëllimin e përmbushjes së detyrimeve dhe funksionit të tij, në zbatim të kësaj rregulloreje, veçanërisht për qëllime që lidhen me hetimin, inspektimin, kërkesat për informacion, komunikimin, publikimin, vlerësimin, verifikimin, analizën dhe hartimin e planeve të mbikëqyrjes.
4. Informacioni që mbulohet nga sekreti profesional, përfshirë shkëmbimin e informacionit ndërmjet autoriteve kompetente sipas kësaj Rregulloreje dhe autoriteve kompetente të përcaktuara ose të krijuara në përputhje me Direktivën (BE) 2022/2555, nuk mund të

zbulohet për asnjë person ose autoritet tjetër, përveçse në bazë të dispozitave të përcaktuara në të drejtën e Bashkimit ose në të drejtën kombëtare.

5. Çdo informacion i shkëmbyer ndërmjet autoriteve kompetente në përputhje me këtë Rregullore, që ka të bëjë me kushtet tregtare ose operacionale, si dhe me çështje të tjera ekonomike ose personale, konsiderohet konfidencial dhe i nënshtrohet kërkesave të sekretit profesional, përveç rasteve kur autoriteti kompetent deklaron, në momentin e komunikimit, se një informacion i tillë mund të zbulohet, ose kur një zbulim i tillë është i nevojshëm për procedura gjyqësore.

Neni 77

Nxjerrja e akteve nënligjore për harmonizimin e mëtejshëm të mjeteve, metodave, proceseve dhe politikave të menaxhimit të rrezikut TIK

1. Autoriteti harton udhëzime për standardet rregullatore teknike, me qëllim që të:

a) specifikojnë elemente të tjera që duhet të përfshihen në politikat, procedurat, protokollet dhe mjetet e sigurisë të TIK, të përcaktuara në nenin 10, pika 2, me synimin për të garantuar sigurinë e rrjeteve, për të mundësuar masa të përshtatshme mbrojtëse kundër ndërhyrjeve dhe keqpërdorimit të të dhënave, për të ruajtur disponueshmërinë, autenticitetin, integritetin dhe konfidencialitetin e të dhënave, përfshirë teknikat kriptografike, si dhe për të garantuar një transmetim të saktë dhe të shpejtë të të dhënave pa ndërprerje të mëdha dhe vonesa të panevojshme;
b) zhvillojnë më tej komponentët e kontrolleve të të drejtave të menaxhimit të qasjes, të përmendur në nenin 10, pika 4, shkronja "c", dhe politikën përkatëse të burimeve njerëzore që përcakton të drejtat e aksesit, procedurat për dhënien dhe revokimin e të drejtave, monitorimin e sjelljeve anormale në lidhje me rrezikun e TIK përmes treguesve të përshtatshëm, përfshirë modelet e përdorimit të rrjetit, oraret, aktivitetin informatik dhe pajisjet e panjohura;
c) zhvillojnë më tej mekanizmat e përcaktuar në nenin 11, pika 1, që mundësojnë zbulimin e menjëhershëm të veprimtarive anormale dhe kriteret e përcaktuara në nenin 11, pika 2, që aktivizojnë proceset e zbulimit dhe reagimit ndaj incidenteve që lidhen me TIK;
d) specifikojnë më tej komponentët e politikës së vazhdimësisë së biznesit të TIK, të përcaktua në nenin 12, pika 1;
e) specifikojnë më tej testimin e planeve të vazhdimësisë së biznesit të TIK, të përcaktuar në nenin 12, pika 6, për të siguruar që një testim i tillë të marrë *duly* në konsideratë skenarë në të cilët cilësia e ofrimit të një funksioni kritik ose të rëndësishëm përkeqësohet në një nivel të papranueshëm ose dështon, dhe të marrë *duly* në konsideratë ndikimin e mundshëm të falimentimit ose dështimeve të tjera të ndonjë ofruesi përkatës të shërbimeve të TIK të palëve të treta dhe, kur është e aplikueshme, rreziqet politike në juridiksionet e ofruesve përkatës;
f) specifikojnë më tej komponentët e planeve të reagimit dhe rikuperimit të TIK, të përcaktuar në nenin 12, pika 3;
g) specifikojnë më tej përmbajtjen dhe formatin e raportit mbi rishikimin e kuadrit të menaxhimit të rrezikut të TIK, të përcaktuar në nenin 7, pika 5.

2. Autoriteti në hartimin e udhëzimeve të përcaktuara në pikën 1, të këtij neni, mban në konsideratë madhësinë dhe profilin e përgjithshëm të rrezikut të subjektit financiar, si dhe natyrën, shkallën dhe kompleksitetin e shërbimeve, veprimtarive dhe operacioneve të tij, duke marrë në konsideratë çdo veçori specifike që buron nga natyra e dallueshme e veprimtarive ndërmjet sektorëve të ndryshëm të shërbimeve financiare.

Neni 78
Dispozita të përgjithshme

1. Në rast të çdo mbivendosjeje ose mospërputhjeje midis kësaj rregulloreje dhe çdo rregulloreje tjetër që trajton aspekte të sigurisë së TIK, dispozitat e kësaj rregulloreje do të kenë përparësi dhe do të zëvendësojnë ato rregullore vetëm në masën që ekziston një mbivendosje ose mospërputhje.

2. Për zbatimin dhe sigurimin e respektimit të kësaj rregulloreje, Autoriteti i Mbikëqyrjes Financiare do të kryejë një vlerësim gjithëpërfshirës të qëndrueshmërisë operacionale digjitale për subjektet financiare të përcaktuara në nenin 3.

3. Ky vlerësim do të përfshijë një gamë mjetesh dhe metodologjish, duke përfshirë, por pa u kufizuar vetëm në udhëzues vetëvlerësimi, inspektime mbikëqyrëse në vend (*on site*), si dhe aktivitete monitorimi në distancë (*off site*).

4. Këto vlerësime do të përbëjnë një pjesë integrale të kuadrit ekzistues të vlerësimit të rrezikut operacional dhe do ta plotësojnë atë.

5. Objektivi i këtyre veprimtarive është garantimi i një niveli të lartë të qëndrueshmërisë operacionale digjitale dhe zbutja e rreziqeve që lidhen me cenueshmëritë e teknologjisë së informacionit dhe komunikimit (*TIK*) brenda institucioneve financiare.

6. Ky qasje synon të mbrojë integritetin operacional të institucioneve financiare shqiptare, duke kontribuar në forcimin e qëndrueshmërisë së infrastrukturës kritike.

Neni 79
Dispozitë kalimtare

1. Neni 3, pika 4, neni 30, pika 7, shkronja "a", si dhe paragrafi i fundit, neni 39, neni 74, si dhe parashikimet në Kreun V, Seksionin IV (nenet 59 deri 72) do të zbatohen nga data e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian.

Neni 80
Hyrja në fuqi

1. Kjo rregullore hyn në fuqi në datë 1 Janar 2028.
2. Subjektet e kësaj rregulloreje, marrin masa për plotësimin e kërkesave të rregullores dhe raportojnë në Autoritet çdo 3 muaj për masat e marra prej tyre, deri në datën 1 janar 2028.

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	Email i personit kryesor të kontaktit	
1.9	Numri i telefonit të personit kryesor të kontaktit	
1.10	Emri i personit dytësor të kontaktit	
1.11	E-mail i 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		
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	
2.3	Data dhe ora e klasifikimit si madhor të incidentit të lidhur me TIK	
2.4	Përshkrimi i incidentit madhor të lidhur me TIK	
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 e ka origjinën nga një ofrues shërbimi palë e tretë 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 Autoriteti	
3.2	Data dhe ora e ndodhjes së incidentit madhor të lidhur me TIK	
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 palëve të tjera financiare të prekura nga incidenti	
3.7	Përqindja e palëve të tjera financiare të prekura nga incidenti	
3.8	Ndikimi në klientët ose plaës tjetër 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 patur ende ndonjë ndikim	
3.13	Ndikimi reputacional	

3.14	Informacion kontekstual mbi ndikimin reputacional	
3.15	Kohëzgjatja e incidentit madhor të lidhur me TIK	
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 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 lidhur me TIK	
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 te 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	
4.11	Informacion i vlefshëm për Autoritetin	
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 qënë 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 detyrueshëm për njoftimin fillestar?	I detyrueshëm 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 në Autoritet.	Po	Po	Po	Opsione: — Njoftim fillestar; — Raport i ndërmjetëm; — Raport përfundimtar; — Incident madhor i riklasifikuar si jo-madhor
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 palë e tretë i cili raporton për një subjekt financiar, mund të përdorë një kod identifikimi të specifikuar sipas standardeve teknike të parashikuara në kuadrin nënligjor të Autoritetit, për regjistrin e informacionit në lidhje me marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK, të parashikuara në nenin 44 të kësaj rregulloreje.	Po	Po	Po	Alfanumerik

1.4. Lloji i subjektit financiar të prekur nga incidenti	Lloji i subjektit të parashikuar në nenin 3, pika 1 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 qe mund të zgjidhen të përmendur në pikën 1, të neni 3 "Fusha e zbatimit", të kësaj rregulloreje..
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 dhe që kërkohet të raportojë incidentin madhor në Autoritet, sipas nenit 30 të kësaj rregulloreje. 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, duke i ndare me pikëpresje; b) ofruesin e shërbimeve palëvee tretë 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 prekur nga incidenti (të ndara me pikëpresje).	Po, nëse subjekti financiar i prekur nga incidenti është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Po, nëse subjekti financiar i prekur nga incidenti është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Po, nëse subjekti financiar i prekur nga incidenti është i ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	Alfanumerik
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, i caktuar në përputhje me Organizatën Ndërkombëtare të Standardizimit. Në rastin e raportimeve të agreguara:	Po, nëse subjekti financiar i Prekur nga incidenti madhor	Po, nëse subjekti financiar i Prekur nga incidenti madhor është i	Po, nëse subjekti financiar i Prekur nga incidenti madhor është i	Kod unik alfanumerik prej 20 karakteresh i bazuar në standardet ISO 17442-1:2020.

	a) një listë me të gjithë kodet NUIS/LEI të subjekteve financiare të prekur nga incidentet madhore të lidhur me TIK, të ndara me pikëpresje b) ofruesi i shërbimeve palë e tretë 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 prekur nga incidenti (të ndara me pikëpresje). Renditja e kodeve dhe emrave të subjekteve financiare duhet të jetë e njëjtë.	është i 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	ndryshëm nga subjekti që raporton dhe në rast të një raportimi të agreguar	
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 Autoriteti 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. Numr i telefonit të personit kryesor të kontaktit	Numri i telefonit të personit kryesor të kontaktit që mund të përdoret nga Autoriteti 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 psh +3556XXXXXXXX (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	Po	Po	Po	Alfanumerik

	financiar.				
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 Autoriteti për të ndjekur komunikimin.	Po	Po	Po	Alfanumerik
1.12 Numri i telefonit të personit dytësor të kontaktit	Numri i telefonit të personit dytësor të kontaktit ose grupit përgjegjës, që mund të përdoret nga Autoriteti për të ndjekur komunikimin. Numri i telefonit që raportohet duhet të jetë i formatit si psh +3556XXXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).	Po	Po	Po	Alfanumerik
1.13 Emri i shoqërisë mëmë	Emri i shoqërisë mëmë fundore të grupit, të cilit i përket subjekti financiar i prekur nga incidenti, kur 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, kur 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. 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. Në rastet e incidenteve të përsëritura, data dhe ora kur uzbulua incidenti më i fundit i lidhur me TIK.	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 si madhor	Data dhe ora kur incidenti i lidhur me TIK u klasifikua si incident madhor, sipas kritereve 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. 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 palë e tretë ose tek 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 dhe për të përshkruar çdo informacion tjetër relevant në lidhje me incidentin e lidhur me TIK, 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 strukturave më të larta vendimmarrëse, që janë përfshirë në përgjigje të incidentit të lidhur me TIK.	Po	Po	Po	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)
2.5. Kriteri i klasifikimit që shkaktoi raportimin e incidentit	Kriteret e klasifikimit sipas kësaj rregulloreje, që kanë përcaktuar incidentin e lidhur me TIK 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	Po	Po	Po	Zgjedhje (e shumëfishtë): - klientët, palët e tjera financiare dhe transaksionet e prekura; - ndikimi reputacional;

	incidentin e lidhur me TIK si madhor, për të paktën një ose më shumë subjekte financiare.				- 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. Kur vlerësojnë ndikimin e incidentit madhor në shtete të tjera, subjektet financiare duhet të marrin në konsideratë nenin 22-29 të kësaj rregulloreje.	Po, nëse është arritur kufiri i shtrirjes gjeografi ke	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.	Po	Po	Po	Opsione: — siguria e teknologjisë së informacionit; — stafi; — kontrolli i brendshëm; — auditi i jashtëm; — klientët; — pala tjetër financiare; — ofruesit e shërbimeve të palë e tretë; — sulmuesit; — sistemet e monitorimit; — autoritetet/agjencitë/organet ligjzbatuese; — të tjera.
2.8. Informacion nëse incidenti madhor i lidhur me TIK e ka origjinën nga një Ofrues shërbimi	Tregues nëse incidenti madhor i lidhur me TIK e ka origjinën nga një ofrues shërbimi i palëve të treta ose nga një subjekt tjetër.	Po, nëse incidenti e ka origjinën nga një ofrues	Po, nëse incidenti e ka origjinën nga një ofrues shërbimi	Po, nëse incidenti e ka origjinën nga një ofrues shërbimi i	Alfanumerik

palëe tretë ose nga një subjekt tjetër financiar	Subjektet financiare duhet të tregojnë nëse incidentet madhore të lidhur me TIK e kanë origjinën nga një ofrues shërbimi palë e tretë 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 palëe tretë ose subjektit financiar dhe llojin e kodit të identifikimit (psh. LEI apo NUIS).	shërbimi palë e tretë ose nga njësubjekt tjetër financiar	palë e tretë ose nga një subjekt tjetër financiar	palëve të treta ose nga një subjekt tjetër financiar.	
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, si incident jo-madhor, 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.	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK është riklasifikuar si incident jo-madhor.	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK është riklasifikuar si incident jo-madhor.	Po, nëse ka informacione të tjera jo të përfshira në këtë formular ose incidenti madhor i lidhur me TIK është riklasifikuar si incident jo-madhor.	Alfanumerike
Përmbajtja e raportit të ndërmjetëm					
3.1. Kodi i Referencës së incidentit i caktuar Nga Autoriteti	Kodi i referencës së incidentit i caktuar nga Autoriteti, në kohën kur është marrë njoftimi fillestar, për të identifikuar në mënyrë të pa ngatërrueshme incidentin madhor të lidhur me TIK.	Jo	Po, nëse aplikohet	Po, nëse aplikohet.	Alfanumerik
3.2. Data dhe ora e ndodhjes së	Data dhe ora kur ka ndodhur incidenti madhor i	Jo	Po	Po	Standardi ISO 8601 (VVVV-MM-DD

incidentit madhor të lidhur me TIK	lidhur me TIK, 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.				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.	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, 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 gjithë 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, 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.	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

	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.				vlerën gjysmë lart.
3.6. Numri i palëve të tjera financiare të prekura nga incidenti	Numri i palëve të tjera financiare të prekura nga incidenti madhor i lidhur me TIK, që kanë një kontratë me subjektin financiar. Gjatë vlerësimit të numrit të palëve të tjera financiare të prekura, entitetet financiare duhet të kenë parasysh nenin 20, pika 2 të kësaj rregulloreje. Një subjekt financiar që nuk mund të përcaktojë numrin real të palëve të tjera 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 X38 të kësaj rregulloreje, numri total i palëve të tjera financiare të prekura nga incidenti, në të gjithë subjektet financiare.	Jo	Po	Po	Numër i plotë.
3.7. Përqindja e palëve të tjera financiare të prekura nga incidenti	Përqindja e palëve të tjera financiare të prekura nga incidenti madhor i lidhur me TIK, në raport me numrin total të palëve të tjera financiare që kanë një kontratë me subjektin financiar.	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

	Gjatë vlerësimit të përqindjes së palëve të tjera financiare të prekura nga incidenti madhor i lidhur me TIK, 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 palëve të tjera 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 x38 të kësaj rregulloreje, një subjekt financiar duhet të pjesëtojë numrin total të të gjitha palëve të tjera financiare të prekura nga incidenti, me numrin e përgjithshëm të palëve të tjera financiare të të gjitha subjekteve financiare.				%). 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 pala tjetër financiare përkatëse	Çdo ndikim tek klientët ose palëve të tjera 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 palëve të tjera financiare	Po, nëse është arritur kufiri i treguesit "Rëndësia e klientëve dhe palëve të tjera financiare	Po/Jo
3.9. Numri i Transaksioneve të prekura nga incidenti	Numri i transaksioneve të prekura nga incidenti madhor i lidhur me TIK. 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 ndërkufitare, që përfshijnë një shumë monetare, ku të paktën një pjesë	Jo	Po, nëse transaksionet janë prekur nga incidenti	Po, nëse transaksionet janë prekur nga incidenti	Numër i plotë.

	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 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 transaksionet 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 vlerësohet në përputhje me nenin 20, pika 4 dhe nenin 28, pika 1, shkronja "e" të kësaj rregulloreje.	Jo	Po, nëse transaksionet janë	Po, nëse transaksionet janë	Monetare Subjektet financiare duhet të

	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.		prekur nga incidenti	prekur nga incidenti	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 patur 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 palën tjetër financiare të prekura nga incidenti; — Shifra reale për transaksionet e prekura nga incidenti; — Vlerësime për klientët e prekur nga incidenti; — Vlerësime për palën tjetër financiare të prekura nga incidenti; — Vlerësime për transaksionet e prekura nga incidenti; — Pa ndikim te klientët; — Pa ndikim te pala tjetër financiare; — Pa ndikim te transaksionet.
3.13. Ndikimi reputacional	Informacion në lidhje me ndikimin reputacional që rezulton nga incidenti madhor i lidhur me TIK, siç parashikohet në nenin 21 dhe nenin 29 të kësaj rregulloreje. Në rastin e raportimit të agreguar sipas nenit 38 të	Jo	Po, nëse plotësohet kriteri "Ndikimi reputacional"	Po, nëse plotësohet kriteri "Ndikimi reputacional"	Zgjedhje e shumëfishtë: — incidenti madhor i lidhur me TIK është pasqyruar në media; — incidenti madhor i lidhur me TIK ka rezultuar në ankesa të

	kësaj rregulloreje, kategoritë e ndikimit reputacional që zbatohen për të paktën një subjekt financiar.				përsëritura nga klientë të ndryshëm ose pala tjetër financiare 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; — subjekti financiar do të humbasë ose ka të ngjarë të humbasë klientët ose pala tjetër financiare, me një ndikim material në biznesin e tij, si rezultat i incidentit madhor të lidhur me TIK.
3.14. Informacion kontekstual mbi ndikimin reputacional	Informacion që përshkruan se si incidenti madhor i lidhur me TIK 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, duke përfshirë rrezikun e falimentimit të subjektit financiar ose rrezikun e humbjes së fondeve	Jo	Po, nëse plotësohet kriteri “Ndikimi reputacional ”	Po, nëse plotësohet kriteri “Ndikimi reputacional ”	Alfanumerik

	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 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, 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.				
3.15. Kohëzgjatja e incidentit madhor të lidhur me TIK	Subjektet financiare do të matin kohëzgjatjen e incidentit madhor të lidhur me TIK, 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, do të matin kohëzgjatjen e incidentit duke filluar nga momenti më 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, 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, në rast të diferencave në kohëzgjatjen e incidentit midis subjekteve të ndryshme financiare.	Jo	Po	Po	Ditë:Orë:Minuta
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, palën tjetër 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.	Jo	Po, nëse incidenti ka shkaktuar një ndërprerje të shërbimeve	Po, nëse incidenti ka shkaktuar një ndërprerje të shërbimeve	Ditë:Orë:Minuta

	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, 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, në rast të diferencave në kohëzgjatjen e incidentit midis subjekteve të ndryshme financiare.				
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 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 pala tjetër financiare të prekur në shtete të tjera; b) degët ose subjektet e tjera financiare të grupit, që kryejnë veprimtari në shtete të tjera; ose c) infrastrukturat e tregut financiar ose ofruesit palë e tretë, të cilët mund të prekin subjektet	Jo	Po, nëse përmbushet kufiri i kriterit "Shtrirja gjeografike"	Po, nëse përmbushet kufiri i kriterit "Shtrirja gjeografike"	Zgjedhja (e shumëfishtë): — klientët; — pala tjetër financiare; — degë të subjektit financiar; — subjekte financiare brenda grupit, që kryejnë veprimtari në shtete të tjera; — infrastrukturë e tregut financiar; — ofrues shërbimi palë të treta që janë të përbashkëta me subjekte të tjera financiare.

	financiare në shtete të tjera, ku ofrojnë shërbime.				
3.19. Përshkrim se si incidenti madhor i lidhur me TIK ka ndikim në shtete të tjera	Përshkrimi i ndikimit dhe ashpërsisë së incidentit madhor të lidhur me TIK, në secilin vend të prekur, duke përfshirë një vlerësim të ndikimit dhe ashpërsisë mbi: a) klientët; b) pala tjetër 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 shwrbimipalë e tretë që mund të jenë të përbashkët për subjekte të tjera financiare.	Jo	Po, nëse përmbushet kufiri i kriterit "Shtrirja gjeografike"	Po, nëse përmbushet kufiri i kriterit "Shtrirja 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, 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, 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 veprimtarisw së 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	Jo	Po, nëse plotësohet kriteri "Humbjet e të dhënave"	Po, nëse plotësohet kriteri "Humbjet e të dhënave"	Alfanumerik

	të klientit, të dhëna të subjekteve të tjera (p.sh. pala tjetër 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, sekret profesional:, sekreti i sigurimeve, 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 kryer veprime pa pëlqimin e tyre, për të kryer sulme *phishing*, 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.				
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 Autoriteti; ose — shërbimet e TIK 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	Jo	Po	Po	Alfanumerik

	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.				
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 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 *phishing*; b) sulm i shpërndarë/sulm i mohimit të shërbimit (D/DoS); c) vjedhje e identitetit; d) enkriptim i të dhënave për ndikim, duke përfshirë *ransomware*; e) rrëmbim i burimeve; f) nxjerrje dhe manipulim i të dhënave, duke përjashtuar vjedhjen e identitetit; g) shkatërrim i të dhënave;	Jo	Po, nëse lloji i incidentit të lidhur me TIK është "i lidhur me sigurinë kibernetike" në fushën 3.23	Po, nëse lloji i incidentit të lidhur me TIK është "i lidhur me sigurinë kibernetike" në fushën 3.23	Zgjedhja (e shumëfishtë): — inxhinieri sociale, përfshirë edhe *phishing*; — sulm i shpërndarë/sulm i mohimit të shërbimit (D/DoS); — vjedhje e identitetit; — enkriptim i të dhënave për ndikim, duke përfshirë *ransomware*; — rrëmbim i burimeve; — nxjerrje dhe manipulim i të dhënave, duke përjashtuar vjedhjen e identitetit;

	h) deformim; i) sulm i zinxhirit të furnizimit; j) të tjera (specifikoni).				— 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 prekura	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; 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.	Jo	Po	Po	Alfanumerik

	Proceset e biznesit përfshijnë, por nuk janë të kufizuar në: — informacioni i llogarisë; — pranimi i transaksioneve të pagesave; — **shërbime aktuariale** — autentifikimi/autorizimi; — Autoriteti kompetent? — Regjistrim dhe verifikim i klientëve (client onboardong) — **administrim i përfitimeve**; — blerja dhe shitja e paketave të policave të sigurimit ndërmjet siguracioneve; — **menaxhim i kërkesave për dëmshpërblim në sigurime**; — **procesimi i kërkesave për dëmshpërblim në sigurime**; — klerimi; — sigurime ne grup (collective insurances); — ruajtja he administrimi i aseteve financiare (costudy and safekeeping); — procesimi i të dhënave; — debitime direkte; — vendosja e instrumenteve financiare; — këshillimi për investimet; — administrimi i investimeve; — emetimi i instrumenteve të pagesave; — urdhrat; — administrimi i portofolit; — marrja/transmetimi/ekzekutimi — risigurim — 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, *software*, serverët e aplikacioneve, pjesët ndërmjetëse (*middleware*), komponentët e rrjetit, të tjerë) që mbështesin	Jo	Po	Po	Opsione: — Po; — Jo;

	proceset e biznesit, janë prekur nga incidenti madhor i lidhur me TIK.				— 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 mbi komponentët e infrastrukturës (përfshirë pjesët fizike (*hardware*) dhe pjesët *software* që mbështesin proceset e biznesit. Pjesët fizike përfshijne serverë, kompjuterë, qendra të dhënash, *switches*, rutera, shpërndarës (*hubs*). Pjesët logjike përfshijnë sisteme operative, aplikacione, baza të të dhënave, mjete sigurie, komponentë rrjeti, të tjera). Përshkrimi duhet të përshkruajë ose emërtojë komponentët e infrastrukturës ose sistemet e prekur dhe, kur është e disponueshme: a) informacionin e versionit; b) infrastrukturën e brendshme/pjesërisht e kontraktuar/plotësisht e kontraktuar – emrin e ofruesit palë e tretë; c) nëse infrastruktura përdoret ose ndahet në funksione të shumta biznesi; d) planet përkatëse të qëndrueshmërisë/vazhdimësisë/rimëkëmbjes/ zëvendësueshmërisë në fuqi.	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
3.30. Ndikimi në interesat financiarë të klientëve	Informacion nëse incidenti madhor i lidhur me TIK ka patur ndikim në interesat financiarë të klientëve.	Jo	Po	Po	Opsione: — Po; — Jo; — Informacion jo i disponueshëm.

3.31. Raportimi te autoritete të tjera	Specifikimi i autoriteteve që janë informuar për incidentin madhor të lidhur me TIK.	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. Nëse zgjidhet fusha e të dhenave 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.	Jo	Po, nëse autoritete "të tjera" janë informuar nga subjekti financiar për incidentin madhor të lidhur me TIK.	Po, nëse autoritete "të tjera" janë informuar nga subjekti financiar për incidentin madhor të lidhur me TIK.	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.	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 ne zbatim (*workaround procedures activated*), bllokimi i portave USB, aktivizimi i planit të rikuperimit nga fatkeqësitë apo edhe kontrolle 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 *site* primar). Për veprimet e përkohshme që nuk janë zbatuar,	Jo	Po, nëse veprime/masa të përkohshme janë ndërmarrë apo janë planifikuar për t'u ndërmarrë (fusha e të	Po, nëse veprime/masa të përkohshme janë ndërmarrë apo janë planifikuar për t'u ndërmarrë (fusha e të	Alfanumerik

	por janë ende të planifikuara, të tregohet data kur parashikohet zbatimi i tyre. Nëse nuk janë ndërmarrë veprime/masa të përkohshme, tregoni arsyet përkatëse.		dhënave 3.33).	dhënave 3.33).	
3.35. Treguesit e kompromentimit	Informacion i lidhur me incidentin madhor të lidhur me TIK, që mund të ndihmojë në identifikimin e aktivitetit keqdashës brenda rrjetit ose sistemit të informacionit (treguesit e kompromentimit ose IoC, ku janë të zbatueshëm). 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 *URL*-ve; c) domenet; d) *hash*-et e skedarëve; e) të dhënat mbi programet keqdashëse (*malware*) (emri i *malware*, emrat e skedarëve dhe vendndodhjet e tyre, çelësat specifikë të regjistrit të lidhur me aktivitetin e *malware*); 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);	No	Po, nëse lloji i incidentit është "i lidhur me sigurinë kibernetike" në fushën 3.23	Po, nëse lloji i incidentit është "i lidhur me sigurinë kibernetike" në fushën 3.23	Alfanumerik

	h) të dhënat DNS-je dhe konfigurime të regjistrit; 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 i korrespondojnë sulmeve të njohura/komunikimeve të *botnet*, adresave IP të makinave të infektuara me programe keqdashëse (*bots*), 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 *phishing* ose faqe interneti të vëzhguara që mbajnë programe keqdashëse.				
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, 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, 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	Jo	Jo	Po	Zgjedhje (e shumëfishtë): — veprime të brendshme të qëllimshme; — dëmtime fizike të qëllimshme/manipulim/vjedhje; — veprime keqdashëse: veprime mashtruese;

	fushën 4.1, zgjidhni një ose disa nga opsionet e mëposhtme): a) veprime të brendshme të qëllimshme; b) dëmtime fizike të 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; d) pamjaftueshmëri ose dështim i veprimeve të TIK dhe i veprimeve të sigurisë së TIK; e) pamjaftueshmëri ose dështim i administrimit të projekteve të TIK; f) politika, procedura dhe dokumentacione të brendshme të papërshtatshme; g) blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK; 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 (*hardware*): incidente madhore të lidhur me TIK, të shkaktuara pajisjet (*hardware*), të cilat rezultojnë të papërshtatshme për sa i përket kapacitetit ose performancës për të përmbushur kërkesat ligjore e rregullative në fuqi;				— dështim i proceseve: monitorim i pamjaftueshëm ose dështim i monitorimit dhe kontrollit; — dështim i proceseve: pamjaftueshmëri/paqartësi rolesh dhe përgjegjësish; — dështim i proceseve: dështim i procesit të administrimit të rrezikut të TIK; — dështim i proceseve: pamjaftueshmëri ose dështim i veprimeve të TIK dhe i veprimeve të sigurisë së TIK; — dështim i proceseve: pamjaftueshmëri ose dështim i administrimit të projekteve të TIK; — dështim i proceseve: politika, procedura dhe dokumentacione të brendshme të papërshtatshme; — dështim i proceseve: blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK; — dështim i procesit: të tjera (specifikoni); — dështim i sistemit: kapaciteti dhe performanca fizike e pajisjeve (*hardware*); — dështim i sistemit: mirëmbajtja fizike e pajisjeve (*hardware*); — dështim i sistemit: vjetërimi i pajisjeve; — dështim i sistemit: përputhshmëria/konfigurimi i programeve (*software*); — dështim i sistemit: performanca e programeve (*software*); — dështim i sistemit: konfigurim i

	b) mirëmbajtja fizike e pajisjeve (*hardware*): incidente madhore të lidhur me TIK që rezultojnë nga mirëmbajtja jo e përshtatshme apo e pamjaftueshme e pjesëve përbërëse fizike të pajisjeve (*hardware*), përveç vjetërimit të pajisjeve; c) vjetërimi i pajisjeve: ky lloj shkaku bazë përfshin incidente madhore të lidhur me TIK që e kanë zanafillën nga komponentë të pajisjeve të vjetëruar; d) përputhshmëria/konfigurimi i programeve (*software*): incidentet madhore të lidhur me TIK të shkaktuara nga programet (*software*) që janë jo të përputhshëm me konfigurimet e sistemeve apo programeve të tjera, duke përfshirë incidentet madhore të lidhur me TIK që rezultojnë nga konfliktet e programeve (*software*), cilësime të pasakta, parametra të konfiguruara jo saktë që ndikojnë në funksionimin korrekt të sistemit; e) performanca e programeve (*software*): incidentet madhore të lidhur me TIK që rezultojnë si pasojë e performancës së dobët apo të pamjaftueshme të fragmenteve logjike (komponentëve *software*), për arsye të tjera nga ato të specifikuara në opsionin "përputhshmëria/konfigurimi i programeve (*software*)", duke përfshirë incidentet madhore të lidhur me TIK 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 (*software*) ose sistemit; f) konfigurimi i rrjetit: incidente madhore të lidhur me TIK që vijnë si pasojë e cilësimeve ose infrastrukturës të pasakta ose të konfiguruara gabimisht së rrjetit, duke				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).

	përfshirë incidente të madhore të lidhura me TIK të shkaktuara nga gabimet e konfigurimit të rrjetit, problemet e rrugëzimit (*routing*), konfigurimet e gabuara të *firewall*-it ose probleme të tjera të lidhura me rrjetin që ndikojnë në lidhjet ose komunikimin; g) dëmtime fizike: incidente madhore të lidhur me TIK të shkaktuara nga dëmtimet fizike të infrastrukturave të TIK, 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 që vijnë si pasojë e mungesës së ekspertizës ose aftësisë në trajtimin e sistemeve ose proceseve të TIK, 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 të shkaktuara nga mungesa e burimeve të nevojshme, përfshirë edhe pajisjet (*hardware*), programet (*software*), infrastrukturat, 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, 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, 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 palë e tretë; c) monitorim dhe verifikim i korrigjimit të vulnerabiliteteve; d) menaxhim i identitetit dhe aksesit; e) enkriptimi dhe kriptografia; f) regjistrim i ngjarjeve/logimi.	Jo	Jo	Po	Opsione (të shumëfishta): — monitorim i zbatimit të politikës; — monitorim i ofruesve të shërbimeve palë te tretë; — 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 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; — menaxhimi i vulnerabiliteteve dhe i *patch*-eve; — menaxhimii i ndryshimeve; — menaxhimi i kapaciteteve dhe

	2(c) Dështim i procesit të administrimit të rrezikut të TIK**:** 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) menaxhim i dobët i rreziqeve të mbetura të TIK. 2(d) Pamjaftueshmëri ose dështim i veprimeve të TIK dhe i veprimeve të sigurisë së TIK**:** a) menaxhimi i vulnerabiliteteve dhe i *patch*-eve; b) menaxhimi i ndryshimeve; c) menxhimi i kapaciteteve dhe performancës; d) administrimi i aseteve të TIK dhe klasifikimi i informacionit; e) *backup* dhe rikuperimi; f) trajtimi i gabimeve. 2(g) Blerje, zhvillim, mirëmbajtje sistemesh të papërshtatshme të TIK**:** a) blerja, zhvillimi dhe mirëmbajtja e sistemeve TIK të papërshtatshme; b) testimi i pamjaftueshëm i programeve (*software*) ose dështimi i testimit të programeve (*software*).				performancës; — menaxhimi i aseteve të TIK dhe klasifikimi i informacionit; — *backup* dhe rikuperimi; — trajtimi i gabimeve; — blerja, zhvillimi dhe mirëmbajtja e sistemeve TIK të papërshtatshme; — testimi i pamjaftueshëm i programeve (*software*) ose dështimi i testimit të programeve (*software*).
4.4 Lloje të tjera të shkaqeve bazë		Jo	Jo	Po, nëse është zgjedhur	Alfanumerik

	Subjektet financiare që kanë zgjedhur opsionin shkaqe bazë "të tjera" në fushën 4.2, duhet të specifikojnë këto shkaqe bazë.			opsioni shkaqe bazë "të tjera" në fushën 4.2.	
4.5 Informacione mbi shkaqet bazë të incidentit	Përshkrim i rrjedhës së ngjarjeve që çuan në incidentin madhor të lidhur me TIK dhe përshkrim i mënyrës se si incidenti madhor i lidhur me TIK 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. 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, 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 dhe për të parandaluar përsëritjen e incidentit. Konkluzione/mësime të nxjerra nga incidenti madhor i lidhur me TIK. 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 madhor të lidhur me TIK (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;	Jo	Jo	Po	Alfanumerik

	c) tregoni nëse procedurat janë përshtatur pas incidentit madhor të lidhur me TIK; 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 identifikuara në lidhje me qëndrueshmërinë e sistemeve të teknologjisë së informacionit të prekura nga incidenti /ose në lidhje me procedurat apo kontrollet ekzistuese, nëse është e zbatueshme. Subjektet financiare tregojnë qartë sesi veprimet korrigjuese të parashikuara, do të adresojnë shkaqet bazë të identifikuara dhe kur pritet të zgjidhet përfundimisht incidenti madhor i lidhur me TIK. **2. Konkluzione/mësime të 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 është e ndryshme nga data e planifikuar fillimisht për implementimin, kur është e zbatueshme.	Jo	Jo	Po	Alfanumerik
4.10	Vlerësim nëse incidenti madhor i lidhur me TIK paraqet rrezik për funksionet me rëndësi kritike	Jo	Jo	Po, nëse incidenti paraqet rrezik për	Alfanumerik

rikuperimit Vlerësimi i rrezikut për funksionet kritike për qëllime të zgjidhjes së problemeve	". .			funksionet me rëndësi kritike,	
4.11 Informacion i rëndësishëm për zgjidhjen e problemeve	Subjektet financiare, japin informacion mbi faktin nëse po, në ç'mënyrë incidenti madhor i lidhur me TIK ka ndikuar në aftësinë për zgjidhje të subjektit ose të grupit. Këto subjekte tregojnë gjithashtu nëse incidenti madhor i lidhur me TIK ndikon në aftësinë paguese (solvency) ose likuiditetin e subjektit financiar, si dhe, kur është e mundur, japin një vlerësim sasior të ndikimit. Këto subjekte ofrojnë gjithashtu informacion mbi: • ndikimin në vazhdimësinë operacionale; • ndikimin në aftësinë për zgjidhje të subjektit; • çdo ndikim shtesë në kostot dhe humbjet që rrjedhin nga incidenti madhor i lidhur me TIK, përfshirë ndikimin në pozicionin e kapitalit të subjektit financiar; dhe • nëse marrëveshjet kontraktuale për përdorimin e shërbimeve TIK mbeten të qëndrueshme dhe plotësisht të zbatueshme, në rast të zgjidhjes së subjektit.	Jo	Jo	Po, nëse incidenti ka ndikuar në aftësinë për zgjidhje tw subjektit	Alfanumerik

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, 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 pësuara nga subjekti financiar si pasojë e incidentit madhor të lidhur me TIK, duke përfshirë: a) shuma e fondeve ose aktiveve financiare të përvetësuara (*expropriated*), për të cilat subjekti financiar është përgjegjës; b) shuma e kostove për zëvendësimin ose zhvendosjen e pajisjeve (*hardware*), programeve kompjuterike (*software*), 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 mjeko-ligjore dhe shërbimet e rehabilitimit; i) shuma e kostove dhe humbjeve të tjera, duke përfshirë:	Jo	Jo	Po	Monetare

	i. shpenzime të drejtpërdrejta në pasqyrën e të ardhurave dhe shpenzimeve, duke përfshirë zhvlerësimet dhe kostot e shitjes, për shkak të incidentit madhor të lidhur me TIK; ii. provigjionet të pasqyruara në pasqyrën e të ardhurave dhe shpenzimeve kundrejt humbjeve të mundshme që lidhen me incidentin madhor të lidhur me TIK; iii. humbje të mbetura pezull (*pending losses*), në formën e humbjeve që rrjedhin nga incidenti madhor i lidhur me TIK, 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, 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 (*timing losses*), 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 fianciare 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 lidhur me TIK janë përsëritur dhe së bashku konsiderohen si një incident madhor në kuptimin e nenit 27, pika 2 të kësaj rregulloreje. Subjektet financiare duhet të tregojne nëse incidentet jo madhore të lidhur me TIK janë të përsëritur dhe së bashku konsiderohen si një incident madhor i lidhur me TIK. Subjektet financiare duhet të tregojnë sa herë kanë ndodhur këto incidente jo madhore të lidhur me TIK.	Jo	Jo	Po, nëse incidenti madhor përbëhet nga disa incidente jo madhore të përsëritur.	Alfanumerik
4.16 Data dhe ora e ndodhjes së incidenteve të përsëritura	Nëse subjektet financiare raportojne incidente të përsëritur të lidhur me TIK, paraqesin datën dhe orën kur ka ndodhur incidenti i parë i lidhur me TIK.	Jo	Jo	Po, për incidente të përsëritur	Standardi ISO 8601 (VVVV-MM-DD Ora: minutat:sekondat)

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 paraqet që 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 palë e tretë paraqet njoftimin për një subjekt financiar, mund të përdorë një kod identifikimi të specifikuar sipas standardeve teknike të parashikuara në kuadrin nënligjor të Autoritetit, për regjistrin e informacionit në lidhje me marrëveshjet kontraktuale për përdorimin e shërbimeve të TIK, të parashikuara në nenin 44 të kësaj rregulloreje.	Po	Alfanumerik
3.Lloji i subjektit financiar që paraqet njoftimin	Lloji i subjektit të parashikuar në pikën 1 të nenit3 të kësaj rregulloreje, që paraqet njoftimin.		Opsionet e parashikuara ne nenin 3 pika 1 “Fusha e zbatimit’

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 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 Autoriteti për të ndjekur komunikimin.	Po	Alfanumerik
8. Numri i telefonit të personit kryesor kontaktit	Numri i telefonit të personit kryesor të kontaktit që mund të përdoret nga Autoriteti për të ndjekur komunikimin. Numri i telefonit që raportohet duhet të jetë i formatit si psh +3556XXXXXXXX (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 Autoriteti 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 Autoriteti 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 Autoriteti për të ndjekur komunikimin, nëse është i disponueshëm. Numri i telefonit që raportohet duhet të jetë i formatit si psh +3556XXXXXXXX (përfshirë edhe prefiksin e shtetit përkatës).	Po, nëse numri i telefonit i personit dytësor të kontaktit, që mund të përdoret nga Autoriteti 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 të rëndësishëm kibernetik	Përshkrimi i aspekteve më të rëndësishme të 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 kërcenimit të rëndësishëm kibernetik; dhe d) informacion mbi burimin e informacionit për kërcënimin kibernetik.	Po	Alfanumerik
14.Informac Ion mbi ndikimin potencial	Informacion mbi ndikimin e mundshëm/potencial të kërcënimit kibernetik mbi subjektin financiar, klientët e tij ose palë 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, pala tjetër 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. Veprime te 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.Treguesi t e kompromenti it	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 vendndodhjet e tyre, çelësat specifikë të regjistrit të lidhur me	Po, nëse informacioni mbi treguesit e kompromentimit të lidhur me kërcënimin kibernetik, është i disponueshëm.	Alfanumerik

	aktivitetin e *malware*); 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 regjistrit; 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 i korrespondojnë sulmeve të njohura/komunikimeve të *botnet*, adresave IP të makinave të infektuara me programe keqdashëse (*bots*), 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 *phishing* ose faqe interneti të vëzhguara që mbajnë programe keqdashëse.		
20. Informac ion 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	**.....**	**.....**		