
BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

# RREGULLORE PËR SISTEMET E INFORMACIONIT DHE MENAXHIMIN E RREZIKUT KIBERNETIK

**Përmbajtja**

Në bazë të nenit 35, paragrafit 1, nën-paragrafit 1.1 dhe nenit 65, paragrafit 1 dhe 2 të Ligjit nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës (Gazeta Zyrtare e Republikës së Kosovës, Nr. 77/16 Gusht 2010), të ndryshuar dhe plotësuar me Ligjin Nr.05/L-150 (GZ Nr.10/03 Prill 2017), nenin 85 dhe 114 të Ligjit Nr.04/L-093 për Bankat Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare (GZ/Nr. 11/11 Maj 2012), neni 8 i Ligjit nr.04/L-155, për sistemin e pagesave (GZ/Nr. 12, 03 Maj 2013), nenin 4, paragrafi 3 i Ligjit Nr.05/L-045 për Sigurimet (GZ Nr.38/4 Dhjetor 2015), neni 29 paragrafi 8 i Ligjit Nr. 04/L-018 për sigurimin e detyrueshëm nga autopërgjegjësia (GZ Nr.4/11 Korrik 2011), nenin 4 paragrafi 1, neni 20 paragrafi 1 , neni 13, paragrafin 13.1, nënparagrafi (d) të Ligjit Nr.04/L-101 për Fondet Pensionale të Kosovës (GZ/ Nr.10/8 Maj 2012) dhe nenin 34 të Ligjit Nr.08/L-295 për Kripto-Asetet (GZ Nr.21/22 Nëntor 2024) , Bordi i Bankës Qendrore të Republikës së Kosovës, në mbledhjen e mbajtur më 29 gusht 2025, miratoi këtë:

# RREGULLORE PËR SISTEMET E INFORMACIONIT DHE MENAXHIMIN E RREZIKUT KIBERNETIK

## KAPITULLI I
## DISPOZITA TË PËRGJITHSHME

### Neni 1
### Qëllimi dhe fushëveprimi

1. Kjo Rregullore përcakton standardet, kriteret dhe procedurat minimale të teknologjisë informative dhe rrezikut kibernetik për Institucionet Financiare (IF) të aplikuara, në varësi të kompleksitetit dhe nivelit të përdorimit të teknologjisë informative.
2. Kjo Rregullore zbatohet për të gjitha Institucionet Financiare-IF të licencuara apo mbikëqyrura nga Banka Qendrore e Republikës së Kosovë (BQK).
3. Kjo rregullore nuk zbatohet për Institucioneve Financiare Jo-Bankare që kryejnë vetëm aktivitete të Këmbimit Valutor, si dhe Ndërmjetësit e Sigurimeve.

### Neni 2
### Përkufizimet

1. Termat dhe përkufizimet e përdorura në këtë rregullore kanë kuptimet e mëposhtme:
   1.1. **Apetiti i rrezikut** - Niveli i përgjithshëm dhe llojet e rrezikut që një IF është i gatshëm të marrë përsipër, të vendosura paraprakisht dhe brenda kapacitetit të tij të rrezikut, për të arritur objektivat e tij strategjikë dhe planin e biznesit.
   1.2. **Artikulli i Konfigurimit (ang: Configuration Item - CI)** - Një komponent i menaxhuar i një sistemi TI (harduer, softuer ose dokumentacion) i ndjekur për menaxhimin e ndryshimeve dhe ofrimin e shërbimeve.
   1.3. **Asetet mbështetëse** - Njerëzit, teknologjia, informacioni dhe pajisjet e nevojshme për kryerjen e operacioneve kritike.

1.4. **Autentifikimi me Shumë Faktorë (ang: Multi Factor Autentification - MFA)** - Një mekanizëm sigurie që kërkon forma të shumëfishta verifikimi (p.sh., fjalëkalime, elemente biometrike, tokena sigurie, etj) përpara se të mundësohet qasja.

1.5. **Bord Këshillues për Ndryshime (ang: Change Advisory Board - CAB)** - është një strukturë brenda procesit të menaxhimit të ndryshimeve në IT (Change Management) që ka për detyrë të rishikojë, vlerësojë dhe miratojë ose refuzojë propozimet për ndryshime në mjedisin e IT-së.

1.6. **Bordi i Drejtorëve (BD)** - Organi qeverisës, përgjegjës për mbikëqyrjen e menaxhimit të rrezikut të TIK , qëndrueshmërisë operacionale, politikave të sigurisë kibernetike dhe pajtueshmërisë me kërkesat rregullatorë të një IF .

1.7. **Cloud Computing** - Përdorimi i burimeve kompjuterike të shkallëzueshme sipas kërkesës, të tilla si: hapësira për ruajtje të të dhënave, fuqia përpunuese dhe softueri - të ofruara nëpërmjet internetit.

1.8. **DevSecOps** - Integrimi i praktikave të sigurisë në zhvillimin e softuerëve dhe operacionet e TI, për të garantuar zhvillim të sigurt të sistemeve të TI-së.

1.9. **Enkriptimi i të dhënave** - Procesi i kodimit të të dhënave për të parandaluar qasjen e paautorizuar, duke siguruar konfidencialitetin dhe integritetin.

1.10. **Incident** - çdo ngjarje e paqellimshme, e paparashikuar ose eqëllimshme, që ndikon ose ka potencial të ndikojë negativisht në konfidencialitetin, integritetin, disponueshmërinë ose autenticitetin e të dhënave, sistemeve dhe shërbimeve të teknologjisë së informacionit dhe komunikimit (TIK), të cilat mbështesin funksionet kritike ose të rregulluara të IF, duke shkaktuar ndërprerje operacionale, humbje të dhënave, dëme financiare, rrezik për stabilitetin e tregut financiar ose cenim të besueshmërisë dhe reputacionit të institucionit. Është një ngjarje që ka, ose mund të ketë potencialisht, një ndikim negativ në konfidencialitetin, integritetin ose disponueshmërinë e informacionit ose sistemeve të informacionit të IF

1.11. **Institucione Financiare (IF)** – Në vazhdimësi të kësaj Rregulloreje, do t'u referohemi si Institucione Financiare, apo shkurt IF institucioneve te cilat përfshijnë Bankat, Institucionet Mikrofinanciare, Institucionet Financiare Jo-bankare, Kompanitë e Sigurimeve, Byronë Kosovare të Sigurimeve , Fondet e Kursimeve Pensionale, Operatorët e Kriptovalutave dhe subjektet e tjera që kryejnë aktivitete financiare, siç përcaktohet në çdo Ligj përkatës për qëllimet e kësaj rregulloreje.

1.12. **Inteligjenca e Kërcënimeve Kibernetike (ang: Cyber Threat Intelligence - CTI)** - Mbledhja, analiza dhe ndarja e informacionit mbi kërcënimet e sigurisë kibernetike, për të përmirësuar zbulimin dhe zbutjen e rrezikut.

1.13. **Klasifikimi i të dhënave** - Procesi i kategorizimit të të dhënave, bazuar në legjislacionin përkatës në fuqi, në varësi të nivelit të ndjeshmërisë së kërkesave për përputhshmëri dhe nevoja për siguri.

1.14. **Korniza e Menaxhimit të Rrezikut (ang: Risk Management Framework - RMF)** - Një qasje e strukturuar për përcaktimin e roleve, përgjegjësive, vlerësimeve të rrezikut, masave zbutëse dhe aktiviteteve monitoruese që lidhen me TIK dhe sigurinë kibernetike.

1.15. **Asnjëherë Vetëm** - Një parim sigurie që kërkon që veprimet kritike ose të ndjeshme të kryhen në prani të një numri me të madh të personave, të autorizuar për të parandaluar mashtrimet ose gabimet.

1.16. **Menaxhimi i Arnimeve (ang: Patch)** - Një politikë që rregullon vendosjen e arnimeve të softuerit për të adresuar dobësitë e sigurisë dhe për të ruajtur integritetin e sistemit.

1.17. **Menaxhimi i Asgjësimit të Sigurt** - Procedurat që sigurojnë asgjësimin e sigurt të aseteve dhe të dhënave të TI, duke ruajtur privatësinë e të dhënave dhe pajtueshmërinë mjedisore.

1.18. **Menaxhimi i Identitetit dhe Qasjes (ang: Identity Access Management - IAM)** - Një kornizë që siguron qasje të sigurt dhe të kontrolluar në sistemet e TI, duke zbatuar parime të tilla si: qasja me të drejta minimale, ndarja e detyrave dhe kontrollet e qasjes bazuar në role.

1.19. **Menaxhimi i Incidenteve** - Një qasje sistematike për zbulimin, reagimin ndaj, zbutjen dhe rimëkëmbjen nga incidentet e sigurisë kibernetike dhe TIK.

1.20. **Menaxhimi i kontraktimeve të jashtme dhe ofruesve të shërbimeve teknologjike ( ang: Outsourcing and Technology Service Provider Management - OTSPM)** - Korniza rregullatore që rregullon përdorimin e ofruesve të shërbimeve të jashtme për funksione kritike, duke siguruar llogaridhënie dhe pajtueshmëri.

1.21. **Menaxhimi i Ndryshimeve** - Një proces i strukturuar që siguron që ndryshimet në sistemet e TIK të vlerësohen, miratohen, zbatohen dhe dokumentohen me ndërprerje minimale.

1.22. **Menaxhimi i Rrezikut Teknologjik (ang: Technology Risk Management - TRM)** - Një qasje e strukturuar për identifikimin, vlerësimin, zbutjen dhe monitorimin e rreziqeve që lidhen me TIK dhe sigurinë kibernetike.

1.23. **Menaxhimi i Rrezikut të Modelit të Inteligjencës Artificiale (IA)** - Procesi i sigurimit që modelet e inteligjencës artificiale janë transparente, të shpjegueshme, të audituehsme dhe të lira nga paragjykimet.

1.24. **Menaxhimi i Rrezikut të TIK** - Procesi i menaxhimit të rreziqeve që lidhen me teknologjinë e informacionit dhe komunikimit, duke siguruar operacione të sigurta dhe elastike.

1.25. **Menaxhimi i Sigurisë së Sistemeve të Virtualizuara** - Masat e sigurisë për mjediset e virtualizuara, duke përfshirë: hipervizorët, makinat virtuale dhe infrastrukturën e bazuar në cloud.

1.26. **Menaxhimi i Sigurt i Qendrës së të Dhënave** - Masat që sigurojnë mbrojtjen fizike dhe kibernetike të një infrastrukture të qendrës së të dhënave të IF.

1.27. **Menaxhimi i Sigurt i Rrjetit** - Politikat dhe kontrollet që sigurojnë funksionimin dhe segmentimin e sigurt të një rrjeti të TI-së të IF.

1.28. **Menaxhimi i Vazhdimësisë së Biznesit (ang: Business Continuity Management - BCM) -** Një qasje strategjike për të siguruar që funksionet kritike të biznesit mund të

vazhdojnë gjatë dhe pas ndërprerjeve, si rezultat i sulmeve kibernetike, problemeve teknike ose fatkeqësive natyrore.

1.29. **Monitorimi dhe Raportimi i Rrezikut -** Vlerësimi dhe raportimi i vazhdueshëm i ekspozimit ndaj Rrezikut tek menaxhmenti i lartë dhe autoritetet rregullatore.

1.30. **Ndarja e Detyrave (ang: Segregation of Duties - SoD) -** Një mekanizëm kontrolli që siguron që përgjegjësitë kryesore të ndahen midis individëve të shumtë, për të zvogëluar rrezikun e mashtrimit, gabimeve ose veprimeve të paautorizuara.

1.31. **Ndërfaqet e Programimit të Aplikacioneve (ang: Application Programming Interfaces - API**) - Ndërfaqe që u mundësojnë sistemeve të komunikojnë në mënyrë të sigurt, me kontrolle që sigurojnë konfidencialitetin dhe integritetin e të dhënave.

1.32. **Nevoja për përdorim (ang: Need-to-Use Basis)** – Një politikë kufizimi ku qasja në sisteme, të dhëna ose burime jepet vetëm kur kërkohet shprehimisht për një detyrë ose funksion specifik.

1.33. **Ofruesi i Shërbimeve Teknologjike (ang: Technology Service Provider - TSP) -** Një entitet i jashtëm që ofron shërbime TI, infrastrukturë ose aplikacione për organizatat, shpesh sipas një marrëveshjeje kontraktuale.

1.34. **Ofruesit e Shërbimeve të Palëve të Treta -** Entitete të jashtme që ofrojnë shërbime të lidhura me TIK, duke përfshirë cloud computing, kontraktimin dhe zgjidhje të sigurisë kibernetike.

1.35. **Operacione Kritike -** Ndërprerja e së cilës do të ndikonte në funksionimin e vazhdueshëm të IF ose për rolin e saj në sistemin financiar. Nëse një operacion i caktuar është "kritik" varet nga natyra e IF dhe roli i tij në sistemin financiar.

1.36. **Pajtueshmëria Rregullatore e IA -** Kërkesa që IF të sigurojnë që aplikacionet e IA në funksionet kritike të përmbushin standardet ligjore dhe rregullatore.

1.37. **Parandalimi i Rrjedhjes së të Dhënave (ang: Data Leak Prevention - DLP) -** Masat dhe teknologjitë e sigurisë të dizajnuara për të zbuluar, monitoruar dhe parandaluar qasjen, transmetimin ose modifikimin e paautorizuar të të dhënave të ndjeshme.

1.38. **Phishing -** Praktika mashtruese e dërgimit të email-eve ose mesazheve të tjera që pretendojnë se vijnë nga një dikush tjetër, me qëllim nxitjen e individëve që të zbulojnë kredencialet e tyre, apo informacione personale, të tilla si fjalëkalime,numra kartash krediti, apo informata të tjera konfidenciale.

1.39. **Plani i Reagimit ndaj Incidenteve Kibernetike** - Një grup veprimesh të paracaktuara që një ndërmjetës financiar ndjek për të përmbajtur, zbutur dhe rikuperuar nga një incident kibernetik.

1.40. **Plani i Rimëkëmbjes nga Fatkeqësitë (ang: Disaster Recovery Plan - DRP) -** Një strategji e dokumentuar për rivendosjen e sistemeve dhe të dhënave të TIK pas një dështimi të madh ose incidenti kibernetik.

1.41. **Praktikat e Kodimit të Sigurt** - Metodologji programimi, të hartuara për të parandaluar dobësitë, siç janë: sulmet e injektimit, shkeljet e të dhënave dhe shfrytëzimet e sistemit.

1.42. **Privilegji më i Vogël** - Një parim sigurie ku përdoruesve, aplikacioneve ose sistemeve u jepet vetëm niveli minimal i qasjes së nevojshme për të kryer funksionet e tyre të punës.

1.43. **Qendra e Operacioneve të Sigurisë Kibernetike (Security Operations Center - SOC)** - Një njësi e centralizuar përgjegjëse për monitorimin, zbulimin, analizimin dhe reagimin ndaj kërcënimeve të sigurisë kibernetike.

1.44. **Qeverisja dhe Mbikëqyrja** - Korniza e brendshme brenda një institucioni financiar për të menaxhuar Teknologjinë e Informacionit dhe Komunikimit (TIK) dhe rreziqet kibernetike në mënyrë të kujdesshme dhe efektive.

1.45. **Qeverisja e Cloud Computing** - Mbikëqyrja e shërbimeve të bazuara në 'Cloud' për të siguruar sigurinë e të dhënave, pajtueshmërinë rregullatore dhe qëndrueshmërinë operacionale.

1.46. **Qeverisja e Inteligjencës Artificiale (IA)** - Politikat dhe kornizat që sigurojnë përdorim etik, të përgjegjshëm dhe në përputhje me rregullatorët të IA në shërbimet financiare.

1.47. **Qëndrueshmëria Operacionale** - Është aftësia e një IF për të kryer operacione kritike përgjatë pengesave operacionale. Kjo aftësi i mundëson një IF të identifikojë dhe të mbrohet nga kërcënimet dhe dështimet e mundshme, të përgjigjet dhe të përshtatet, si dhe të rikuperohet dhe të mësojë nga ngjarjet shkatërruese në mënyrë që të minimizojë ndikimin e tyre në kryerjen e operacioneve kritike përgjatë pengesave operacionale . Duke marrë parasysh qëndrueshmërinë e tij operacionale, një IF duhet të supozojë se do të ndodhin ndërprerje dhe të marrë parasysh apetitin e tij të përgjithshëm për rrezik dhe tolerancën ndaj ndërprerjeve.

1.48. **Ransomware** - një lloj softueri keqdashës që enkripton ose bllokon të dhënat dhe sistemet e një përdoruesi ose institucioni, duke kërkuar pagesë (shpërblim) për t'i rikthyer ato në gjendjen e tyre të zakonshme.

1.49. **Raportimi Rregullator i Incidenteve Kibernetike** - Kërkesa që IF të raportojnë incidentet e sigurisë kibernetike në Bankën Qendrore të Republikës së Kosovës (BQK) brenda afateve të përcaktuara kohore.

1.50. **Redundant** – pasja e sistemeve, komponentëve ose burimeve shtesë ose të dyfishta për të siguruar kopje rezervë në rast se kryesori dështon — duke siguruar funksionim të vazhdueshëm dhe disponueshmëri të lartë.

1.51. **Ruajtja dhe Rimëkëmbja** - Procesi i ruajtjes së sigurt të kopjeve të të dhënave dhe sigurimi i rikthimit të tyre në rast të dëmtimit ose humbjes.

1.52. **Siguria e Pajisjeve Fundore** - Masa për të mbrojtur pajisje të tilla si: kompjuterët e punës, laptopët dhe pajisjet mobile nga kërcënimet kibernetike.

1.53. **Sigurimi i Auditimit të Pavarur** - Procesi i shqyrtimit të pavarur të kontrolleve të sigurisë së TIK, qeverisjes dhe pajtueshmërisë rregullatore.

1.54. **Sillni Pajisjen Tuaj (ang: Bring Your Own Device - BYOD)** - Një politikë që u lejon punonjësve të përdorin pajisjet e tyre personale, si telefonat inteligjentë dhe laptopët, për qëllime pune, duke ofruar fleksibilitet dhe komoditet, por duke kërkuar menaxhim të kujdesshëm të rreziqeve të sigurisë.

1.55. **Skanimi i dobësive** - Vlerësime të rregullta të sistemeve të TIK për të identifikuar dhe zbutur dobësitë e sigurisë.

1.56. **Strategjia e TIK** - Një plan që përputh aftësitë e TIK me objektivat e përgjithshme të biznesit të IF, duke mbuluar avancimet e sistemeve, politikat e sigurisë kibernetike dhe varësitë nga palët e treta.

1.57. **Stres Testi në IA** - Procesi i vlerësimit të sistemeve të IA në kushte të ndryshme për të vlerësuar qëndrueshmërinë dhe besueshmërinë e tyre.

1.58. **Sulm i Shpërndarë i Mohimit të Shërbimeve (ang: Distributed Denial of Service - DDoS)** - Një sulm i shpërndarë i mohimit të shërbimit (DDoS) është një sulm kibernetik që mbingarkon një sistem, rrjet ose faqe interneti të synuar me trafik të tepërt nga burime të shumëfishta, duke shkaktuar ngadalësime ose ndërprerje.

1.59. **Testimi i depërtueshmërisë (ang: Penetration Testing)** - Sulme kibernetike të simuluara të kryera për të vlerësuar mbrojtjen dhe qëndrueshmërinë e sigurisë kibernetike të një institucioni financiar.

1.60. **Trajtimi i Rrezikut** - Zbatimi i masave për të zbutur ose zvogëluar rreziqet në një nivel të pranueshëm.

1.61. **Transparenca e Vendimeve të IA** - Kërkesa që IF të zbulojë kur vendimet e nxitura nga inteligjenca artificiale ndikojnë te klientët dhe të ofrojë një mekanizëm për ankesa.

1.62. **Ushtrime për Reagim ndaj Incidenteve** - Aktivitete testimi dhe trajnimi për të vlerësuar efektivitetin e një plani reagimi ndaj incidenteve të IF.

1.63. **Virtualizim** - përdorimi i teknologjive ose teknikave softuerike për të krijuar një shtresë abstraksioni mbi burimet fizike të teknologjisë së informacionit (serverë, rrjete, ruajtje të të dhënave ose desktopë), me qëllim që të mundësohet ndarja, izolimi dhe ekzekutimi i mjediseve të pavarura logjike mbi të njëjtën infrastrukturë fizike.

1.64. **Vlerësimi i Kompetencës së Furnizuesit** - Vlerësimi i palëve të treta për të siguruar që ata plotësojnë ekspertizën e kërkuar për funksionet e kontraktuara të TIK.

1.65. **Vlerësimi i rrezikut** - Identifikimi dhe vlerësimi i kërcënimeve, dobësive dhe pasojave të mundshme për të përcaktuar gjasat dhe ndikimin e rrezikut.

1.66. **Vlerësimi i Rrezikut të Kërcënimit dhe Cenueshmërisë (ang: Threat and Vulnerability Risk Assessment - TVRA)** - Një proces që vlerëson kërcënimet dhe dobësitë e mundshme në mjediset e TI-së dhe atyre fizike të një organizate, për të përcaktuar rreziqet e sigurisë dhe strategjitë e zbutjes së rreziqeve të identifikuara.

1.67. **Zyrtari Kryesor i Sigurisë së Informacionit (ang: Chief Information Security Officer - CISO)** - Një ekzekutiv i lartë përgjegjës për krijimin dhe mirëmbajtjen e një vizioni, strategjie dhe programesh siguri të IF, për të mbrojtur asetet e informacionit dhe sistemet e TIK.

1.68. **Zyrtari Kryesor i Teknologjisë (ang: Chief Technology Officer - CTO)** - Një ekzekutiv përgjegjës për mbikëqyrjen e strategjisë teknologjike, infrastrukturës dhe qëndrueshmërisë digjitale të një IF.

## Neni 3
## Parimi i Proporcionalitetit

1. Të gjitha bankat duhet të veprojnë në pajtim me kërkesat sipas dispozitave të kësaj rregulloreje.
2. Përveç institucioneve të përmendura në paragrafin 1 të këtij neni, Institucionet e tjera që i nënshtrohen kësaj rregulloreje janë përgjegjëse për të siguruar pajtueshmërinë me kërkesat përkatëse bazuar në madhësinë e tyre, profilin e përgjithshëm të rrezikut, organizimin e brendshëm dhe natyrën, fushëveprimin, kompleksitetin dhe rrezikshmërinë e shërbimeve, aktiviteteve dhe operacioneve të tyre, pavarësisht nëse ofrohen aktualisht apo synohen.
3. Gjatë mbikëqyrjes së institucioneve financiare, BQK do të vlerësojë përputhshmërinë si me tekstin, ashtu edhe me frymën dhe qëllimin e kësaj rregulloreje, dhe vendimet e saj për çështje të tilla janë përfundimtare. Ky parim i proporcionalitetit siguron që detyrimet rregullatore të përshtaten në mënyrë të përshtatshme me karakteristikat dhe rreziqet specifike të secilit institucion, duke ruajtur njëkohësisht llogaridhënien për pajtueshmërinë.
4. IF që kanë kompleksitet dhe shkallë më të lartë të teknologjisë në përdorim mund të vendosin masa shtesë përkatëse, duke përfshirë përdorimin e teknologjive të avancuara për të zbutur rreziqe të tilla.

# KAPITULLI II
# QEVERISJA DHE MBIKËQYRJA

## Neni 4
## Qeverisja dhe organizimi

1. IF duhet të ketë një kornizë të qeverisjes dhe kontrollit të brendshëm që siguron një menaxhim efektiv dhe të kujdesshëm të Teknologjisë së Informacionit dhe Komunikimit (TIK) dhe rreziqeve kibernetike, me qëllim arritjen e një niveli të lartë të qëndrueshmërisë operative digjitale.
2. Bordi i Drejtorëve (BD) duhet të rishikojë dhe miratojë qasjen e qëndrueshmërisë operacionale të IF, duke marrë parasysh tolerancën e përgjithshme të IF për ndërprerjet në operacionet e saj kritike. Në formulimin e tolerancës së IF për ndërprerjet, BD duhet të marrë në konsideratë aftësitë operacionale të IF, duke pasur parasysh një gamë të gjerë skenarësh të rëndë, por të besueshëm, që do të ndikonin në operacionet e saj kritike. BD duhet të sigurojë që politikat e IF të adresojnë në mënyrë efektive rastet kur aftësitë e IF janë të pamjaftueshme për të përmbushur tolerancën e deklaruar për ndërprerjet.
3. BD është përgjegjës për miratimin e të gjitha politikave që lidhen me sistemet e informacionit (duke përfshirë, por pa u kufizuar në TIK, Sigurinë e Informacionit dhe/ose Kibernetike) dhe çdo vit duhet të vlerësojë përshtatshmërinë e politikave dhe t'i rishikojë ato.
4. BD dhe menaxhmenti i lartë i IF duhet të sigurojnë kontrolle të brendshme efektive dhe që praktikat e menaxhimit të rrezikut të zbatohen për të arritur sigurinë dhe besueshmërinë e mjedisit të saj operativ të TIK.

5. BD dhe menaxhmenti i lartë duhet të kenë anëtarë me përvojën e nevojshme për të kuptuar dhe menaxhuar rreziqet teknologjike, të cilat përfshijnë rreziqet e paraqitura nga kërcënimet kibernetike.
6. IF duhet të ketë funksione të përshtatshme në lidhje me menaxhimin e TIK, rrezikut të TIK, sigurisë së sistemit të TIK dhe vazhdimësisë së biznesit.
7. IF duhet të caktojë një person ose njësi përgjegjëse për sigurinë e informacionit, e cila duhet të menaxhojë sigurinë e sistemit të informacionit dhe të koordinojë politikat dhe proceset e sigurisë së informacionit që lidhen me funksionet dhe platformat teknologjike. Njësia apo personi përgjegjës për sigurinë e informacionit duhet t'i raportojë Kryeshefit Ekzekutiv dhe duhet të jetë i pavarur nga njësitë e tjera organizative. Nëpërmjet Kryeshefit Ekzekutiv, duhet të raportojë të paktën një herë në vit dhe sipas nevojës te BD, i cili duhet të jetë i informuar për operacionet dhe funksionet që lidhen me sigurinë e informacionit.
8. IF duhet të emërojë nga një zyrtar kryesor të Informacionit dhe të Teknologjisë, si dhe një Zyrtar kryesor të Sigurisë së Informacionit, që zotërojnë ekspertizën dhe përvojën e nevojshme. BQK duhet të informohet 30 ditë më parë për emërime të tilla, duke dhënë një justifikim për kandidatët e propozuar. BQK rezervon të drejtën për të kundërshtuar çdo emërim të tillë gjatë periudhës së njoftimit ose në një fazë të mëvonshme. IF që, sipas nenit 3 të kësaj rregulloreje, vendos të mos caktojë role të tilla duhet të sigurojë ekspertizë, përvojë dhe pavarësi të mjaftueshme për të ushtruar role të tilla në mënyrë efektive.
9. IF duhet të sigurojë numër të mjaftueshëm të stafit të IF me aftësi relevante për të mbështetur nevojat e tyre operacionale të TIK dhe proceset e tyre të menaxhimit të rrezikut të TIK, si dhe për të siguruar zbatimin e strategjisë së tyre të TIK, duke caktuar fondet e nevojshme dhe duke ofruar trajnime të përshtatshme mbi rreziqet e TIK për anëtarët e stafit, përfshirë mbajtësit e funksioneve kyçe, në bazë vjetore ose më shpesh nëse është e nevojshme.
10. BD dhe menaxhmenti i lartë duhet të sigurojnë që vendimet kryesore të TIK të merren në përputhje me tolerancën e rrezikut të IF.
11. BD dhe menaxhmenti i lartë duhet të kultivojnë një kulturë të fortë të ndërgjegjësimit dhe menaxhimit të rrezikut teknologjik, duke përfshirë higjienën kibernetike në të gjitha nivelet e stafit të IF.
12. BD ose një komitet i deleguar prej tij është përgjegjës për:
    12.1. sigurimin e një kornize të shëndoshë dhe të fuqishme të menaxhimit të rrezikut;
    12.2. zbatimin dhe mirëmbajtjen në mënyrë efektive të politikave, procedurave dhe standardeve, për të menaxhuar rreziqet e TIK dhe kibernetike;
    12.3. sigurimin e një funksioni të menaxhimit të rrezikut teknologjik (MRrT) (ang: Technology Risk Management) për të mbikëqyrur kornizën dhe strategjinë e menaxhimit të rrezikut teknologjik (KSMRrT) ( ang: Technology Risk Management Framework And Strategy), duke ofruar një perspektivë të pavarur mbi rreziqet teknologjike me të cilat përballet IF;
    12.4. dhënien për drejtuesit e lartë, të cilët janë përgjegjës për ekzekutimin e KSMRrT e IF, autoritet të mjaftueshëm, burime dhe qasje në BD;
    12.5. miratimin e deklaratës së tolerancës së rrezikut që artikulon natyrën dhe shkallën e rreziqeve teknologjike që IF është i gatshëm dhe i aftë të marrë përsipër;

12.6. rishikimin e rregullt të KSMRrT për rëndësi të vazhdueshme;

12.7. vlerësimin e kompetencave të menaxhimit për menaxhimin e rreziqeve teknologjike, dhe

12.8. sigurimin e krijimit të një funksioni të pavarur auditimi për të vlerësuar efektivitetin e mjedisit të kontrollit të brendshëm të IF, menaxhimit të rrezikut dhe qeverisjes.

13. Menaxhmenti i lartë është përgjegjës për:

13.1. krijimin e KSMRrT;

13.2. menaxhimi i rreziqeve teknologjike në përputhje me KSMRrT e përcaktuar;

13.3. përcaktimin e qartë për rolet dhe përgjegjësitë e stafit në menaxhimin e rreziqeve teknologjike, dhe

13.4. informimin e menjëhershëm të BD për zhvillimet dhe incidentet e rëndësishme dhe të pafavorshme të rreziqeve teknologjike që ka të ngjarë të kenë një ndikim të madh në IF.

## Neni 5
## Strategjia, politikat dhe procedurat

1. IF për menaxhimin të mirëfilltë të Teknologjisë së Informacionit dhe Komunikimit (TIK) duhet të:

1.1. Miratojë një strategji të TIK

1.2. Përcaktojë plane veprimi që mbështesin zbatimin e strategjisë së TIK, dhe

1.3. Krijojë procese për të monitoruar dhe matur efektivitetin e strategjisë.

2. Organi menaxhues ka përgjegjësi të përgjithshme për përcaktimin, miratimin dhe mbikëqyrjen e zbatimit të strategjisë së TIK të IF si pjesë e strategjisë së tyre të përgjithshme të biznesit, si dhe për krijimin e një kornize efektiv të menaxhimit të Rrezikut për rreziqet e TIK dhe sigurisë për të siguruar pajtueshmërinë me legjislacionin/rregulloret në fuqi.

3. IF duhet ta përshtas strategjinë e TIK me strategjinë e përgjithshme të biznesit, në mënyrë që të mbulojë:

3.1. Si duhet të evoluojë TIK për të mbështetur dhe zbatuar në mënyrë efektive strategjinë e biznesit, duke përfshirë evoluimin e strukturës organizative, ndryshimet në sistemin e TIK dhe varësitë kryesore me palët e treta;

3.2. Strategjinë e planifikuar dhe evoluimin e arkitekturës së TIK, duke përfshirë varësitë nga palët e treta; dhe

3.3. Objektiva të qarta të sigurisë së informacionit, duke u përqendruar në sistemet e TIK dhe shërbimet, stafin dhe proceset e TIK.

4. Në planin e veprimit të përmendur në paragrafin 1, nënparagrafi 1.2 të këtij neni, IF përcakton aktivitetet që duhen ndërmarrë për të arritur objektivat e strategjisë së TIK. IF shqyrton rregullisht planet e veprimit për të siguruar rëndësinë dhe përshtatshmërinë e tyre.

5. IF duhet të krijojë politika, standarde dhe procedura, dhe, kur është e përshtatshme, të përfshijë standardet e industrisë dhe praktikat më të mira për të menaxhuar rreziqet teknologjike dhe për të mbrojtur asetet e informacionit. Politikat, standardet dhe procedurat duhet gjithashtu të

rishikohen dhe përditësohen rregullisht (të paktën një herë në vit), duke marrë në konsideratë mjedisin në zhvillim të teknologjisë dhe kërcënimeve kibernetike.

6. Politikat mbi menaxhimin e TIK duhet të përcaktojnë të paktën elementët e mëposhtëm:

   6.1. Administrimi dhe funksionimi i sistemeve të TIK

   6.2. Struktura organizative për menaxhimin e TIK

   6.3. Infrastruktura harduerike dhe softuerike e fushës së TIK (diagramet e konfigurimit)

   6.4. Klasifikimi i dokumentacionit dhe mbrojtja e sistemeve dhe të dhënave

   6.5. Kopja rezervë e të dhënave të sistemeve të informacionit

   6.6. Plani i vazhdimësisë së biznesit

   6.7. Sistemet e menaxhimit të ndryshimeve

   6.8. Menaxhimi i incidenteve

   6.9. Menaxhimi i Rrezikut të sistemit të TI-së

   6.10. Përcaktimi i mekanizmave të sigurisë së sistemeve të TIK, dhe

   6.11. Menaxhimi i palëve të treta.

7. Procedurat duhet të përcaktojnë hapa dhe veprime specifike për zbatimin efektiv të politikave. Ato duhet të sigurojnë operacione të qëndrueshme, të sigurta dhe efikase në të gjitha sistemet e TIK. Çdo element procedural duhet të jetë në përputhje me fushat e politikave të përcaktuara, duke mbuluar operacionet e përditshme, përgjigjet ndaj emergjencave dhe metodat për të mbrojtur integritetin e të dhënave dhe sigurinë e sistemit.

8. IF duhet të shqyrtojë dhe vlerësojë plotësisht rreziqet që lidhen me devijimet politikat, standardet dhe procedurat e miratuara dhe të marrë miratimin e menaxhmentit të lartë për devijimet materiale. Devijimet e miratuara duhet të rishikohen periodikisht për të siguruar që rreziqet e mbetura të jenë në një nivel të pranueshëm.

9. Proceset e pajtueshmërisë (p.sh., modeli me tre linja) duhet të zbatohen për të verifikuar që politikat, standardet dhe procedurat janë respektuar. Këto përfshijnë procese përcjellëse për mospërputhshmëri.

## Neni 6
## Menaxhimi i informacionit dhe aseteve të TIK

1. Për të pasur një pamje të saktë dhe të plotë të mjedisit operativ të TIK të IF, IF-të duhet të krijojë praktika të menaxhimit të aseteve të informacionit dhe të mbajë një inventar të të gjitha aseteve, si fizike ashtu edhe logjike, që përfshijnë sa vijon:

   1.1. identifikimi i aseteve të informacionit që mbështesin biznesin e IF dhe ofrimin e shërbimeve, duke përfshirë llojin e aseteve, formatin, vendndodhjen, informata për kopjet rezervë (kur është e aplikueshme), informacionin mbi licencat dhe vlerën për biznesit.

   1.2. klasifikimi i aseteve të informacionit bazuar në rëndësinë e tyre kritike.

1.3. përcaktimi i pronësisë së aseteve të informacionit, si dhe rolet dhe përgjegjësitë e stafit që menaxhon këto asete. Pronari i aseteve është përgjegjës për:

1.3.1.sigurimin që informacioni dhe asetet që lidhen me përpunimin e informacionit klasifikohen sipas ndjeshmërisë

1.3.2.përcaktimi dhe rishikimi i rregullt i kufizimeve të qasjes dhe klasifikimit; dhe

1.3.3.vendosja e politikave, standardeve dhe procedurave për të menaxhuar asetet e informacionit bazuar në rëndësinë e tyre kritike.

## Neni 7
## Menaxhimi i ofruesve të shërbimeve të palëve të treta

1. Pa cenuar rregullativen për kontraktim të jashtëm, përpara se të hyjë në marrëveshje kontraktuale ose partneritete me palë të treta, IF duhet të vlerësojë ekspozimin e tij ndaj rreziqeve teknologjike që mund të ndikojnë në konfidencialitetin, integritetin dhe disponueshmërinë e sistemeve dhe të dhënave të TIK, dhe të menaxhojë ekspozime të tilla gjatë gjithë ciklit jetësor të palëve të treta. Përveç kësaj, duhet të ketë një strategji të përshtatshme daljeje për të adresuar largimet e planifikuara dhe të paplanifikuara nga teknologjitë në përdorim.
2. Për të siguruar vazhdimësinë e shërbimeve të TIK dhe sistemeve të TIK, dhe pa paragjykuar kërkesat e tjera të zbatueshme në përputhje me rregullativen për kontraktim të jashtëm, IF duhet të sigurojë që kontratat dhe marrëveshjet e nivelit të shërbimit (si për rrethana normale ashtu edhe në rast të ndërprerjes së shërbimit) me ofruesit (ofruesit e kontraktimit të shërbimeve të jashtme, entitetet në grup ose ofruesit e palëve të treta) përfshijnë sa vijon:
   2.1. objektiva dhe masa të përshtatshme dhe proporcionale në lidhje me sigurinë e informacionit, duke përfshirë kërkesa të tilla si kërkesat minimale të sigurisë kibernetike; specifikimet e ciklit jetësor të të dhënave të IF; çdo kërkesë në lidhje me enkriptimin e të dhënave, sigurinë e rrjetit dhe proceset e monitorimit të sigurisë, si dhe vendndodhjen e qendrave të të dhënave, dhe
   2.2. procedurat e trajtimit të incidenteve operative dhe të sigurisë, duke përfshirë përshkallëzimin dhe raportimin.
3. IF duhet të monitorojë dhe të kërkojë siguri mbi nivelin e përputhshmërisë së këtyre ofruesve me objektivat e sigurisë, masat dhe objektivat e performancës së IF.
4. Në mënyrë të vazhdueshme, IF duhet të mbajë një regjistër të të gjithë ofruesve të shërbimeve të palëve të treta (përfshirë shërbimet cloud) dhe të sigurojë që këta ofrues të ruajnë një standard të lartë kujdesi në mbrojtjen e konfidencialitetit dhe integritetit të të dhënave, si dhe në sigurimin e disponueshmërisë së sistemit.

## Neni 8
## Rishikimi i kompetencave dhe i të kaluarës

1. IF duhet të sigurojë që personeli, duke përfshirë kontraktorët dhe ofruesit e shërbimeve, të ketë nivelin e kërkuar të kompetencës dhe aftësive për të kryer funksionet e TIK në një mjedis të

TIK, për të menaxhuar rreziqet teknologjike. I gjithë stafi i TIK duhet të ketë përshkrime të detajuara të detyrave dhe përgjegjësive të punës për të siguruar që rolet, përgjegjësitë dhe aftësitë e nevojshme janë të përcaktuara në mënyrë adekuate.

2. Duhet të kryhen verifikime të të kaluarës së personelit me qasje në të dhënat e IF dhe sistemet e TIK për të zbutur rrezikun e brendshëm, duke përfshirë rrezikun e shkeljes së të dhënave, sabotimit dhe mashtrimit nga stafi, kontraktorët dhe ofruesit e shërbimeve.
3. IF duhet të dokumentojë proceset në përputhje me këtë nen për të përmbushur kërkesat sipas këtij neni.

## Neni 9
## Ndërgjegjësimi dhe trajnimi për sigurinë e informacionit

1. IF duhet të krijojn një program gjithëpërfshirës trajnimi për ndërgjegjësimin mbi sigurinë e TIK për të ruajtur një nivel të lartë ndërgjegjësimi midis të gjithë stafit të IF. Programi i trajnimit duhet, të paktën, të përfshijë informacion mbi mjedisin mbizotërues të kërcënimeve kibernetike dhe implikimet e tij, politikat dhe standardet e sigurisë së TIK të IF, si dhe përgjegjësinë e secilit individ për ruajtjen e aseteve të informacionit. I gjithë personeli duhet të jetë i vetëdijshëm për ligjet, rregulloret dhe udhëzimet në fuqi që kanë të bëjnë me përdorimin dhe qasjen në asetet e informacionit.
2. Programi i trajnimit duhet të zhvillohet të paktën një herë në vit për të gjithë stafin, kontraktorët dhe ofruesit e shërbimeve që kanë qasje në asetet kritike të informacionit të IF.
3. BD duhet t'i nënshtrohet trajnimit për të rritur ndërgjegjësimin mbi rreziqet që lidhen me përdorimin e teknologjisë dhe për të përforcuar të kuptuarit e tyre të praktikave të MRrT.
4. Programi i trajnimit duhet të rishikohet periodikisht për të siguruar që përmbajtja e tij të mbetet aktuale dhe relevante. Rishikimi duhet të marrë në konsideratë ndryshimet në politikat e sigurisë së TIK të IF, rreziqet mbizotëruese dhe ato në zhvillim, mjedisin e kërcënimeve kibernetike në zhvillim, mësimet e nxjerra nga iniciativat e mëparshme të trajnimit dhe çdo nevojë trajnimi të identifikuar përmes vëzhgimeve të sjelljes, p.sh. testet e paparalajmëruara të phishing mbi stafin.

## Neni 10
## Parashikimi buxhetor

1. IF duhet të ndajnë fonde të mjaftueshme buxhetore për të përmbushur nivelin e duhur të përgatitjes kibernetike.
2. Buxheti i sigurisë kibernetike duhet të jetë i pavarur nga buxheti i përgjithshëm i TIK të IF, për të siguruar që zhvillimet e sistemeve të lidhura me biznesin të mos konkurrojnë për burimet e ndara për mbrojtjen e sistemeve të TIK.
3. Gjatë ndarjes së buxhetit për çdo vit, gjithashtu duhet të merren në konsideratë nevojat për trajnim të stafit të sistemeve të informacionit/sigurisë kibernetike.

## KAPITULLI III
## TEKNOLOGJIA DHE MENAXHIMI I RREZIKUT KIBERNETIK

### Neni 11
### Korniza e menaxhimit të rrezikut

1. IF duhet të krijojë një kornizë për menaxhimin e Rrezikut për të trajtuar në mënyrë efektive rreziqet e TIK dhe ato kibernetike. Duhet të krijohen struktura dhe procese të përshtatshme qeverisëse, me role, përgjegjësi dhe linja raportimi të përcaktuara mirë në të gjitha funksionet e ndryshme organizative.
2. Të gjitha rreziqet e identifikuara teknologjike duhet t'u caktohen pronarëve të rreziqeve, përgjegjës për vendosjen dhe zbatimin e masave të duhura të trajtimit të rreziqeve.
3. Procesi i menaxhimit të rrezikut duhet të ekzekutohet në mënyrë të përsëritur dhe të rregullt, duke përfshirë komponentët e mëposhtëm:
   3.1. vlerësimin e rrezikut, i përbërë nga identifikimin dhe analizën e rrezikut, për të kuptuar rreziqet me të cilat përballet IF;
   3.2. trajtimin e rrezikut, duke u përqendruar në zbatimin e masave për zbutjen e rrezikut që mbrojnë konfidencialitetin, integritetin dhe disponueshmërinë e aseteve të informacionit; dhe
   3.3. monitorimin, shqyrtimin dhe raportimin e rrezikut, duke u mundësuar palëve të interesuara të identifikojnë dhe komunikojnë menjëherë ndryshimet në rreziqe.
4. Duke pasur parasysh që biznesi, mjediset e TI dhe mjedisi i kërcënimeve kibernetike evoluojnë me kalimin e kohës, IF duhet të rishikojë rregullisht përshtatshmërinë dhe efektivitetin e kuadrit të tij të menaxhimit të rrezikut dhe të zbatojë masa korrigjuese sipas nevojës.
5. IF duhet të dokumentojë metodologjinë e menaxhimit të rrezikut që është në përdorim dhe ta miratojë atë nga BD.
6. IF duhet të dokumentojë në mënyrë gjithëpërfshirëse të gjitha përsëritjet e procesit të menaxhimit të rrezikut dhe rezultatet e tyre, siç janë kriteret e vlerësimit, të dhënat e përdorura, regjistrat e rrezikut dhe planet e riparimit.
7. Si minimum, një raport përmbledhës mbi rezultatet e procesit të menaxhimit të rrezikut, një regjistër rreziku dhe një plan i detajuar korrigjimi duhet të përgatiten për miratim nga bordi çdo vit.
8. Menaxhimi i Rrezikut Teknologjik (MRRT) duhet të përfshijë të gjitha sistemet e integruara të informacionit të IF në të gjitha fazat e zhvillimit të tyre.
9. Menaxhimi i rrezikut të sistemit të informacionit duhet të përfshijë planin vjetor të ndërgjegjësimit të punonjësve të IF për përdorimin adekuat të shërbimeve të ofruara përmes sistemit të informacionit të IF.

**Neni 12**
**Vlerësimi i rrezikut**

1. Të paktën një herë në vit ose në çdo rast ndryshimesh të rëndësishme në kërkesat e sigurisë së TIK, IF duhet të kryejë analizën e rrezikut të sistemeve të TIK, për të siguruar që ky rrezik të mbahet brenda kufijve të tolerancës në lidhje me aktivitetin e IF. Rezultatet e analizës së rrezikut duhet të dokumentohen.
2. Gjatë procesit të identifikimit të rrezikut, IF duhet të:
   2.1. identifikojë kërcënimet ndaj aseteve të saj të informacionit;
   2.2. identifikojë dobësitë që mund të shfrytëzohen nga kërcënimet;
   2.3. identifikojë kontrollet ekzistuese; dhe
   2.4. identifikojë pasojat e mundshme në skenarë të ndryshëm, nëse kërcënimet shfrytëzojnë dobësitë e identifikuara. Gjatë identifikimit të pasojave të mundshme, IF duhet të marrë në konsideratë faktorët financiarë, operacionalë, ligjorë, të reputacionit dhe rregullatorë
3. Gjatë procesit të analizimit të rrezikut, IF duhet të vlerësojë
   3.1. gjasat e kërcënimeve që të shfrytëzojnë dobësitë e identifikuara;
   3.2. madhësinë e pasojave nëse kërcënimet shfrytëzojnë dobësitë e identifikuara, dhe
   3.3. caktojë një matës të nivelit të rrezikut për secilin rrezik, bazuar në këto vlerësime.

**Neni 13**
**Trajtimi i rrezikut**

1. IF duhet të zhvillojë dhe zbatojë masa për zbutjen e rrezikut që janë në përputhje me kritikalitetin e aseteve të informacionit dhe nivelin e tolerancës së pranuar të rrezikut.
2. IF duhet të vlerësojë nëse rreziqet janë zvogëluar në një nivel të pranueshëm, pas zbatimit të masave zbutëse. Kriteret dhe autoritetet miratuese për pranimin e rrezikut të mbetur duhet të përcaktohen qartë dhe duhet të jenë në përputhje me tolerancën e rrezikut të IF.
3. Kur është e mundur, IF duhet të marrë në konsideratë mbulimin e sigurimit për teknologji të ndryshme të sigurueshme për të zbutur ndikimet financiare, të tilla si kostot e rimëkëmbjes dhe dëmshpërblimit.

**Neni 14**
**Monitorimi, rishikimi dhe raportimi i rrezikut**

1. IF duhet të krijojë një proces për vlerësimin dhe monitorimin e ndryshimeve në rrezik.
2. Rreziqet e rëndësishme duhet të monitorohen nga afër dhe t'i raportohen BD dhe menaxhmentit të lartë. Frekuenca e monitorimit dhe raportimit duhet të jetë në përputhje me nivelin e rrezikut.
3. Për të lehtësuar raportimin e rrezikut tek menaxhmenti, duhet të zhvillohen matës të rrezikut teknologjik për të nxjerrë në pah asetet e informacionit që kanë ekspozimin më të lartë ndaj rrezikut. Këta matës duhet të marrin në konsideratë ngjarjet e rrezikut, gjetjet e auditimit, si dhe kërkesat përkatëse rregullative.

**Neni 15**
**Korniza e menaxhimit të projekteve**

1. Për projektet e mëdha, duhet të krijohet një komitet drejtues i projekteve për të siguruar mbikëqyrje dhe qeverisje efektive të tyre.
2. Duhet të krijohet një kornizë menaxhimi projektesh për të siguruar qëndrueshmëri në praktikat e menaxhimit të projekteve dhe ofrimin e rezultateve që përmbushin objektivat dhe kërkesat e projekteve. Korniza duhet të mbulojë politikat, standardet, procedurat, proceset dhe aktivitetet që nga fillimi deri në mbyllje të projekteve.
3. Dokumentacioni i detajuar i projekteve të TIK duhet të krijohet, mirëmbahet dhe miratohet nga biznesi përkatës dhe menaxhmenti i TIK. Dokumentacioni duhet të përcaktojë rastin e biznesit, fushëveprimin dhe buxhetin e projektit, si dhe fazat kryesore, aktivitetet dhe rezultatet për secilën fazë të projektit. Rolet dhe përgjegjësitë e stafit të përfshirë në projekt duhet të përcaktohen qartë.

**Neni 16**
**Përvetësimi i sistemeve të TI-së**

IF duhet të krijojë standarde dhe procedura për vlerësimin dhe përzgjedhjen e furnitorëve për të siguruar që furnitori i përzgjedhur është i kualifikuar dhe i aftë të përmbushë kërkesat e projektit. Niveli i vlerësimit duhet të jetë në përputhje me rëndësinë e pritjeve nga projekti për IF.

**Neni 17**
**Cikli jetësor i zhvillimit të sistemit dhe siguria që nga dizajni**

1. IF duhet të krijojë një kornizë për të menaxhuar ciklin jetësor të zhvillimit të sistemeve (SDLC – ang: System Development Life Cycle), për të përcaktuar qartë proceset, procedurat dhe kontrollet në secilën fazë të ciklit jetësor, siç janë fillimi/planifikimi, analiza e kërkesave, projektimi, zbatimi, testimi dhe pranimi. Duhet të mirëmbahen standardet dhe procedurat për fazat e ndryshme.
2. IF duhet të përfshijë specifikimet e sigurisë në projektimin e sistemeve, të kryejë vlerësim të vazhdueshëm të sigurisë dhe t'i përmbahet praktikave të sigurisë në të gjithë ciklin jetësor të zhvillimit të sistemeve. Kërkesat e sigurisë duhet të mbulojnë fushat kryesore të kontrollit, të tilla si kontrolli i qasjes, autentifikimi, autorizimi, integriteti dhe konfidencialiteti i të dhënave, regjistrimi i aktivitetit, gjurmimi i ngjarjeve të sigurisë dhe trajtimi i përjashtimeve. Cikli jetësor i zhvillimit të sistemeve duhet të përfshijë funksionin e sigurisë së TI në çdo fazë të ciklit jetësor.

**Neni 18**
**Analiza e kërkesave të sistemit**

1. IF duhet të identifikojë, përcaktojë dhe dokumentojë kërkesat funksionale për sistemet e TI-së. Përveç kërkesave funksionale, duhet të përcaktohen dhe dokumentohen kërkesat kryesore si performanca e sistemit dhe kontrollet e sigurisë.

2. Gjatë përcaktimit të kërkesave të sigurisë, IF duhet të vlerësojë kërcënimet dhe rreziqet e mundshme të lidhura me sistemet e TI-së duke përcaktuar nivelin e sigurisë së nevojshme për të përmbushur nevojat e tij të biznesit.

**Neni 19**
**Dizajnimi dhe implementimi i sistemeve**

1. Si pjesë e fazës së projektimit, IF duhet të rishikojë arkitekturën dhe projektimin e propozuar të sistemit të TI-së duke përfshirë kontrollet e TI-së dhe të sigurisë së informacionit që do të ndërtohen në sistem, për të siguruar përputhshmërinë me kërkesat e përcaktuara.
2. IF duhet të verifikojë që kërkesat nga dizajnimi i sistemeve përmbushen gjatë projektimit dhe implementimit të sistemeve. Çdo ndryshim ose devijim nga kërkesat e përcaktuara duhet të miratohet nga palët përkatëse të interesit.
3. Ekspertët përkatës të fushës duhet të angazhohen për të marrë pjesë në shqyrtimin e projektit.

**Neni 20**
**Testimi dhe pranimi i sistemit**

1. Duhet të përcaktohet një metodologji për testimin e sistemit. Fushëveprimi i testimit duhet të mbulojë logjikën e biznesit, funksionin e sistemit, kontrollet e sigurisë dhe performancën e sistemit në kushte të ndryshme ngarkese dhe stresi. Një plan testimi duhet të përcaktohet dhe miratohet para testimit.
2. Çështjet e identifikuara gjatë testimit, duke përfshirë defektet e sistemit ose gabimet e softuerit, duhet të dokumentohen dhe adresohen siç duhet. Çështjet kryesore që mund të kenë një ndikim negativ në operacionet e IF ose ofrimin e shërbimit për klientët duhet t'i raportohen komitetit drejtues të projekteve dhe të adresohen para vendosjes në mjedisin punues.
3. Të gjitha rezultatet e testimit duhet të dokumentohen dhe të miratohen nga palët përkatëse të interesit.
4. Si pjesë e planifikimit të projektit, duhet të përcaktohen matësit e cilësisë së performancës së pritur.
5. Një entitet i pavarur duhet të ofrojë siguri të cilësisë për projektet e mëdha dhe nuk duhet të ketë konflikt interesi midis entitetit dhe zhvilluesit.

**Neni 21**
**Kodimi i sigurt, rishikimi i kodit burimor dhe testimi i sigurisë së aplikacionit**

1. IF duhet të miratojë standarde mbi kodimin e sigurt, shqyrtimin e kodit burimor dhe testimin e sigurisë së aplikacioneve.
2. Këto standarde duhet të mbulojnë praktikat e programimit të sigurt, validimin e të dhënave hyrëse, kodimin e të dhënave dalëse, kontrollet e qasjes, autentifikimin, praktikat kriptografike dhe trajtimin e gabimeve dhe përjashtimeve.

3. Duhet të përcaktohen politika dhe procedura mbi përdorimin e kodit të softuerit të palëve të treta dhe me burim të hapur, për të siguruar shqyrtimin dhe testimin para integrimit në softuerin e IF.
4. Për të lehtësuar korrigjimin e dobësive në kohën e duhur, IF duhet të mbajë regjistër të përditësimeve dhe dobësive të raportuara të kodit të softuerit të palëve të treta dhe atij me kod burimor të hapur që është përfshirë në softuerin e tij.
5. IF duhet të sigurojë që zhvilluesit e softuerëve të tij janë të trajnuar ose kanë njohuritë dhe aftësitë e nevojshme për të zbatuar kodim të sigurt dhe standarde të sigurisë së aplikacioneve gjatë zhvillimit të aplikacioneve.
6. IF duhet të krijojë një strategji gjithëpërfshirëse për të realizuar validimin dhe testimin e sigurisë së aplikacionit.
7. Të gjitha problemet dhe defektet e softuerit të zbuluara nga shqyrtimi i kodit burimor dhe testimi i sigurisë së aplikacionit duhet të jene të regjistruara dhe gjurmueshme . Problemet kryesore dhe defektet e softuerit duhet të korrigjohen para vendosjes në prodhim.

## Neni 22
## Menaxhimi i DevSecOps

1. Nëse miratohet një qasje DevSecOps, IF duhet të sigurojë që aktivitetet dhe proceset përkatëse të jenë në përputhje me kornizën e ciklit jetësor të zhvillimit të sistemit dhe proceset e menaxhimit të shërbimeve të TI (p.sh., menaxhimi i konfigurimit, menaxhimi i ndryshimeve ose menaxhimi i publikimit të softuerit).
2. IF duhet të zbatojë masa të përshtatshme sigurie dhe të zbatojë ndarjen e detyrave për funksionet e zhvillimit, testimit dhe publikimit të softuerit në proceset e tij DevSecOps.

## Neni 23
## Ndërfaqet e Programimit të Aplikacioneve (API)

1. IF duhet të krijojë masa mbrojtëse të mjaftueshme për të menaxhuar zhvillimin dhe ofrimin e Ndërfaqeve të Programimit të Aplikacioneve (API – ang: Application Programming Interfaces) për ofrimin e sigurt të shërbimeve. Të gjitha kërkesat për kodim të sigurt, shqyrtim të kodit burimor dhe testim të sigurisë së aplikacionit janë po aq të zbatueshme për zhvillimin e API.
2. Përpara se të lejojë palët e treta të lidhen me sistemet e saj të TI nëpërmjet API, IF duhet të kryejë një vlerësim të rrezikut dhe të sigurojë që kontrollet e sigurisë për secilën API janë në përputhje me ndjeshmërinë dhe rëndësinë kritike të biznesit të të dhënave që shkëmbehen, si dhe me kërkesat e konfidencialitetit dhe integritetit të këtyre të dhënave.
3. IF duhet të vendosin standarde sigurie për hartimin dhe zhvillimin e API të sigurta. Standardet duhet të përfshijnë masa për të mbrojtur çelësat API ose token-at e qasjes, të cilët përdoren për të autorizuar qasjen në API për të shkëmbyer të dhëna konfidenciale. Duhet të përcaktohet dhe zbatohet një afat kohor i arsyeshëm për skadimin e token-ave të qasjes për të zvogëluar rrezikun e qasjes së paautorizuar.

4. Duhen miratuar standarde të forta të enkriptimit dhe kontrolle të menaxhimit të çelësave për të siguruar transmetimin e të dhënave të ndjeshme përmes API.
5. Një testim rigoroz sigurie i API duhet të kryhet midis IF dhe palëve ndërlidhëse përpara se ta vendosim në prodhim.
6. Sesionet që përfshijnë palët ndërlidhëse duhet të regjistrohen nga IF. Regjistrat duhet të përfshijnë detaje të tilla si identiteti i palës që bën lidhjen API, data dhe ora, si dhe transaksionet e ekzekutuara dhe të dhënat e qasura. Këto regjistra duhet të jenë të disponueshme për qëllime auditimi sipas nevojës.

## KAPITULLI IV
## MENAXHIMI I SHËRBIMEVE TË TI

### Neni 24
### Dokumentimi

1. IF duhet të mbajë dokumentacion të plotë dhe të përditësuar të infrastrukturës, aplikacioneve dhe sistemeve, sigurisë, faktorëve operacionalë dhe faktorëve të tjerë të rëndësishëm që lidhen me aktivitetin e TI.
2. Sistemet dhe shërbimet duhet të dokumentohen në një mënyrë që i mundëson stafit zëvendësues të drejtojë operacionet e TI me ndërprerje minimale, gjë që mund të arrihet përmes zhvillimit të manualeve gjithëpërfshirëse të operacioneve.
3. Të gjitha përditësimet duhet të regjistrohen dhe dokumentacioni duhet të rishikohet menjëherë për të reflektuar çdo ndryshim në infrastrukturë, aplikacione ose kërkesa rregullative.
4. IF duhet të zbatojë kontrolle qasjeje të bazuara në role për të kufizuar qasjen në dokumentacion të ndjeshëm dhe për të siguruar që vetëm personeli i autorizuar mund t'i shikojë ose modifikojë dokumentet.
5. I gjithë dokumentacioni kritik duhet të rishikohet të paktën një herë në vit ose sa herë që ka ndryshime të rëndësishme dhe të miratohet nga menaxhmenti i lartë.

### Neni 25
### Kontrollet fizike

1. IF duhet të marrë masat e nevojshme mbrojtëse për të parandaluar çdo qasje fizike të paautorizuar, ndërhyrje ose dëmtim të informacionit, pajisjeve të përpunimit të informacionit dhe operacioneve të IF, bazuar në standardet dhe praktikat më të mira ndërkombëtare. Auditime të rregullta duhet të kryhen për të siguruar integritetin dhe sigurinë e aseteve fizike.
2. IF duhet të krijojë procedura qasjeje dhe pune për zonat e sigurta për të gjithë punonjësit dhe palët e jashtme. Zonat e sigurta duhet të mbrohen përmes kontrolleve të qasjes për të siguruar që vetëm punonjësit e autorizuar të kenë qasje.

3. IF duhet të mbajë dokumentacion gjithëpërfshirës të politikave, procedurave dhe kontrolleve të sigurisë fizike dhe të mbajë të dhëna të hollësishme të të gjitha vlerësimeve të sigurisë, incidenteve dhe aktiviteteve të mirëmbajtjes.
4. IF duhet të zbatojë autentifikimin shumë-faktorësh (MFA) për qasjen në zonat e sigurta dhe të mbajë regjistra të detajuar të të gjitha qasjeve në zonat e sigurta dhe t'i rishikojë ato rregullisht.
5. Të gjitha qasjet e palëve të treta dhe vizitorëve duhet të regjistrohen dhe ata duhet të shoqërohen në çdo kohë përderisa ndodhen brenda zonave të sigurta.
6. Të gjitha zonat e sigurta duhet të jenë të pajisura me kamera mbikëqyrjeje dhe ato duhet të ofrojnë mbulim të plotë të zonës, duke siguruar që të mos mbeten hapësira të pambuluara.
7. Sistemi i mbikëqyrjes duhet të jetë në përputhje me rregulloret dhe standardet përkatëse të privatësisë, duke përfshirë protokollet e mbrojtjes së të dhënave, për të mbrojtur pamjet e regjistruara.
8. IF duhet të zbatojë të gjitha kontrollet e nevojshme në qendrën e të dhënave për të menaxhuar në mënyrë efektive faktorët mjedisorë, duke përfshirë, por pa u kufizuar në ekstremet e temperaturave, sistemet e zbulimit dhe shuarjes së zjarrit.
9. IF duhet të sigurojë sisteme që sigurojnë vazhdimësi të furnizimit me energji, siç janë UPS (Uninterruptible Power Supply), gjeneratorët rezervë ose të ngjashme, për të siguruar që të mos ketë ndërprerje të operacioneve gjatë ndërprerjeve të energjisë.

## Neni 26
## Softueri si Shërbim

1. Softueri si shërbim (SaaS – ang: Software as a Service) duhet të menaxhohet nëpërmjet masave të përshtatshme. IF duhet të zbatojë enkriptimin për të dhënat në qetësi dhe në tranzit, për të mbrojtur informacionin e ndjeshëm dhe praktika të fuqishme të menaxhimit të çelësave për të siguruar çelësat e enkriptimit. IF duhet të zbatojë procese formale të konfigurimit dhe dokumentimit.
2. IF duhet të përdorë zgjidhje ose procese të menaxhimit të identitetit dhe qasjes për të zbatuar kontrolle të rrepta të qasjes, mbrojtje të pikave fundore dhe monitorim të sigurisë, për t'u mbrojtur nga shkeljet e të dhënave dhe infeksionet nga programet keqdashëse/viruset.
3. IF duhet të kryejë vlerësime të rregullta të rrezikut specifik për menaxhimin e softuerëve dhe aplikacionet SaaS, për të identifikuar dobësitë dhe kërcënimet.
4. IF duhet të mbajë dokumentacion gjithëpërfshirës të të gjitha proceseve të menaxhimit të softuerit, duke përfshirë zhvillimin, testimin, vendosjen dhe masat e sigurisë.

## Neni 27
## Menaxhimi i konfigurimit

1. IF duhet të zhvillojë një proces efektiv të menaxhimit të konfigurimit për të siguruar menaxhim efektiv dhe në përputhje me rregullat e aseteve dhe shërbimeve të TI, duke përfshirë, por pa u kufizuar në harduerin, softuerin dhe dokumentacionin;

2. IF duhet të përcaktojë kritere për identifikimin dhe klasifikimin e Artikujve të Konfigurimit (AK – ang: Configuration Items-CI), si dhe të mirëmbajë një formë të regjistrit të AK (Artikujve të Konfigurimit);
3. Procesi i menaxhimit të konfigurimit duhet të integrohet me proceset e menaxhimit të ndryshimeve, për të siguruar që të gjitha ndryshimet në AK regjistrohen, vlerësohen dhe menaxhohen në mënyrë të përshtatshme;
4. IF duhet të zbatojë mekanizma për të ndjekur dhe raportuar statusin e të dhënave të konfigurimit.
5. Praktikat e menaxhimit të konfigurimit do t'i nënshtrohen rishikimeve dhe vlerësimeve të rregullta për të identifikuar mundësitë për përmirësim;
6. IF duhet të përdorë konfigurime dhe imazhe të standardizuara të softuerit sa herë që është e mundur.

**Neni 28**
**Menaxhimi i rifreskimit të teknologjisë**

1. IF duhet të krijojë dhe mirëmbajë një Strategji të Përditësimit të Teknologjisë që përshkruan qasjen për planifikimin dhe ekzekutimin e rifresikimeve teknologjike.
2. IF duhet të krijojë procedura për vlerësimin e domosdoshmërisë së rifresikimeve teknologjike. Kjo përfshin vlerësimin e performancës dhe besueshmërisë së teknologjisë ekzistuese.
3. I gjithë softueri (duke përfshirë sistemet operative) dhe hardueri (duke përfshirë pajisjet e rrjetit) duhet të jenë brenda periudhës së ciklit jetësor të mbuluar nga mbështetja aktive e ofruesit (duke përfshirë mbështetjen e zgjatur), nëse është e aplikueshme.
4. Kontratat e mirëmbajtjes ose të licencimit duhet të jenë në fuqi për qasje në përditësime, përmirësime të vogla dhe funksione të tjera kritike të mirëmbajtjes.
5. Vlerësimet e rrezikut për harduerin dhe softuerin që i afrohen datave të Përfundimit të Mbështetjes (EOS – ang: End-Of-Support) duhet të kryhen për të vlerësuar rreziqet e përdorimit të tyre të vazhdueshëm, dhe duhet të zbatohen masa efektive për zbutjen e rrezikut.
6. Procesi i Menaxhimit të Rifresikimit të Teknologjisë duhet t'i nënshtrohet rishikimeve dhe vlerësimeve të rregullta për të identifikuar fushat për përmirësim dhe për të optimizuar praktikat e rifreskimit.

**Neni 29**
**Menaxhimi i Arnimeve**

1. IF duhet të zhvillojë dhe zbatojë një Politikë gjithëpërfshirëse të Menaxhimit të Arnimeve (ang: Patch). Kjo politikë duhet të përcaktojë parimet dhe procedurat që rregullojnë identifikimin, vlerësimin, vendosjen dhe verifikimin e arnimeve.
2. IF duhet të përcaktojnë procedurat për identifikimin e arnimeve përkatëse. Kjo përfshin blerjen e arnimeve nga shitësit dhe prodhuesit që adresojnë dobësitë e sigurisë ose ofrojnë përditësime.

3. Një proces formal vlerësimi duhet të zbatohet për të vlerësuar ndikimin, rrezikun dhe përfitimet e arnimeve, si dhe planin e rikthimit, para vendosjes. Ky vlerësim duhet të përfshijë testimin e arnimeve në një mjedis të kontrolluar për të siguruar përputhshmërinë.

4. Të gjitha ndryshimet që lidhen me vendosjen e arnimeve duhet të dokumentohen, duke përfshirë detajet e arnimit, veprimet e vendosjes dhe çdo problem të hasur.

5. IF duhet të zbatojë procedura për të verifikuar që arnimet janë aplikuar në mënyrë korrekte dhe adresojnë në mënyrë efektive dobësitë ose problemet e identifikuara.

6. Aktivitetet e Menaxhimit të arnimeve duhet të integrohen me proceset e Menaxhimit të Ndryshimeve për të siguruar që vendosjet e arnimeve të planifikohen, miratohen dhe dokumentohen në përputhje me protokollet e menaxhimit të ndryshimeve.

**Neni 30**
**Menaxhimi i ndryshimeve**

1. IF duhet të krijojë Politika dhe Procedura të duhura për Menaxhimin e Ndryshimeve për të kontrolluar ndryshimet në mjedisin e TI me qëllim minimizimin e ndërprerjeve.

2. IF duhet të krijojnë një mekanizëm të formalizuar të menaxhimit të ndryshimeve, të cilin do ta mbikëqyrë një Bord Këshillimor për Ndryshime (ang: Change Advisory Board CAB), i përbërë nga palët kryesore të interesit, përfshirë menaxhimin e biznesit dhe TI, për të miratuar, shqyrtuar dhe përcaktuar përparësitë e ndryshimeve. Të gjitha ndryshimet duhet të testohen dhe miratohen siç duhet, dhe rezultatet e testimit duhet të pranohen dhe miratohen përpara se ndryshimet të vendosen në mjedisin e prodhimit.

3. Të gjitha ndryshimet e synuara duhet të dokumentohen mirë dhe të vlerësohen për rrezikun dhe kërkesat për ndryshim duhet të regjistrohen, kategorizohen dhe prioritizohen siç duhet. Analiza e rrezikut duhet të mbulojë faktorë të tillë, si: siguria dhe implikimet e ndryshimeve në lidhje me asetet e tjera të informacionit.

4. Përpara zbatimit të ndryshimeve, duhet të bëhet një kopje rezervë e aseteve të informacionit dhe të krijohet një plan rikthimi për t'u rikthyer në gjendjen e mëparshme, nëse paraqitet ndonjë problem gjatë ose pas zbatimit të ndryshimit. Ky plan duhet të testohet si pjesë e ciklit jetësor të projektit dhe zbatimit.

5. IF duhet të përcaktojë qartë procedurat për vlerësimin, miratimin dhe zbatimin e ndryshimeve emergjente. Duhet të identifikohen miratuesit e ndryshimeve emergjente dhe ndryshimet emergjente duhet të monitorohen dhe regjistrohen.

6. IF duhet të kryejë një shqyrtim pas zbatimit për të siguruar që ndryshimet të arrijnë rezultatet e dëshiruara.

**Neni 31**
**Menaxhimi i incidenteve**

1. IF duhet të zbatojë një Politikë gjithëpërfshirëse të Menaxhimit të Incidenteve dhe proceset e procedurat përkatëse për trajtimin, kategorizimin dhe prioritizimin e incidenteve të TI, duke përfshirë incidentet e sigurisë kibernetike.

2. IF duhet të zhvillojë dhe përditësojë rregullisht një plan reagimi ndaj incidenteve, të krijojë një ekip reagimi ndaj incidenteve dhe t'i pajisë ata me mjetet dhe burimet e nevojshme për trajtimin dhe menaxhimin e incidenteve;
3. IF përcakton rolet dhe përgjegjësitë e stafit dhe palëve të jashtme të përfshira në regjistrimin, analizën, përshkallëzimin, vendimmarrjen, zgjidhjen dhe monitorimin e incidenteve.
4. IF duhet të mbajë një regjistër për incidentet me qëllim ndjekjen dhe menaxhimin e incidenteve gjatë gjithë ciklit të tyre jetësor, nga zbulimi dhe regjistrimi deri te zgjidhja dhe mbyllja. Incidentet duhet të kategorizohen bazuar në llojin, kritikalitetin dhe ndikimin e tyre.
5. Për të përmirësuar strategjitë e reagimit dhe për të siguruar pajtueshmërinë me nivelet e shërbimit të dakorduara duhet të kryhen rishikime dhe vlerësime të rregullta të të dhënave të incidenteve për të identifikuar trendët mbi strategjitë e reagimit.
6. IF duhet të zbatojë mekanizma të raportimit të incidenteve nga ana e përdoruesve;
7. IF duhet të sigurojë disponueshmërinë e mjeteve ose mekanizmave të zbulimit, analizës dhe reagimit ndaj incidenteve.
8. IF duhet të sigurojë rikthimin e sistemeve dhe shërbimeve të prekura në funksionimin normal dhe të sigurojë që ato janë të sigurta përpara se t'i kthejë ato në shërbim;
9. IF duhet të sigurojë komunikim efektiv brenda institucionit gjatë dhe pas një incidenti, duke përfshirë edhe komunikimin me palët e jashtme. IF duhet të sigurojë që të zhvillohet një plan komunikimi dhe të rishikohet rregullisht.
10. IF duhet të njoftojë dhe raportojë incidentin në BQK, jo më vonë se 4 orë pas zbulimit të tij. Raporti ose njoftimi fillestar duhet të ofrojë informacion mbi kërcënimin e rëndësishëm, si dhe sistemet e prekura. Një raport i ndërmjetëm duhet të dorëzohet brenda 72 orëve dhe raporti përfundimtar brenda 30 ditëve. Modelet për dorëzimin e raportit janë dhënë në Shtojcat e këtij dokumenti.

**Neni 32**
**Rishikimi pas incidentit dhe mësimet e nxjerra**

1. IF duhet të mbajë të dhëna të hollësishme të procesit të trajtimit të incidentit, duke përfshirë veprimet e ndërmarra dhe vendimet e marra.
2. IF përgatit dhe dorëzon raporte tek palët përkatëse të interesit, duke përfshirë organet drejtuese dhe rregullatore.
3. IF duhet të rishikojë politikat dhe procedurat e reagimit ndaj incidenteve bazuar në reagimet dhe mësimet e nxjerra nga incidentet.

**Neni 33**
**Menaxhimi i identitetit dhe qasjes**

1. IF duhet të krijojë një politikë të duhur për identifikimin dhe menaxhimin e qasjes. Politika duhet të specifikojë politikën e fjalëkalimit, vërtetimin shumë-faktorësh dhe kriteret për qasje të privilegjuar, duke përfshirë palët e treta. IF duhet të zbatojë kontrolle të forta të fjalëkalimit

për qasjen e përdoruesve në sistemet e TI dhe vërtetimin dy-faktorësh ose shumë-faktorësh për llogaritë e administrimit të sistemit dhe qasjen në distancë.

2. IF duhet të zbatojë parime të tilla si "kurrë vetëm", "ndarje e detyrave" dhe " të drejtat minimale" kur u jep stafit qasje në asetet e informacionit.
3. Të drejtat e qasjes dhe privilegjet e sistemit duhet të jepen sipas roleve dhe përgjegjësive të stafit dhe palëve të treta.
4. IF duhet të zbatojë një proces menaxhimi të qasjes së përdoruesve, për të siguruar, ndryshuar dhe revokuar të drejtat e qasjes në asetet e informacionit. Të drejtat e qasjes duhet të autorizohen dhe miratohen nga palët përkatëse, siç janë pronarët e aseteve të informacionit.
5. IF duhet të sigurojë që përdoruesve do t'u jepen të drejta qasjeje vetëm në bazë të nevojës për t'i përdorur. Të drejtat e qasjes që nuk janë më të nevojshme, si për shembull për shkak të një ndryshimi në përgjegjësitë e punës ose statusin e punësimit të një përdoruesi, duhet të revokohen ose të çaktivizohen menjëherë. Ofruesit e shërbimeve me qasje në asetet e informacionit të IF duhet t'i nënshtrohen të njëjtave kufizime monitorimi dhe qasjeje si personeli i IF.
6. Qasja në llogari të privilegjuara, siç është qasja e zhvilluesit në një ambient të punës për të zgjidhur një problem, duhet të jepet vetëm në bazë të nevojës për përdorim dhe për periudhën minimale të nevojshme; aktivitetet e këtyre llogarive duhet të regjistrohen dhe të rishikohen si pjesë e monitorimit të vazhdueshëm të IF.
7. IF duhet të kryejë rishikime periodike të të drejtave të qasjes së përdoruesve të paktën çdo 6 muaj, për të siguruar që ato të mbeten të përshtatshme në mënyrë që të identifikojë dhe korrigjojë çdo qasje të paautorizuar.
8. IF duhet të mbajë regjistra gjithëpërfshirës të ngjarjeve të qasjes për të mbështetur monitorimin, auditimin dhe pajtueshmërinë.

## Neni 34
## Menaxhimi i rrjetit

1. IF duhet të krijojë dhe dokumentojë politika gjithëpërfshirëse të sigurisë së rrjetit.
2. IF duhet të instalojë pajisje sigurie të rrjetit, të tilla si firewalls, për të siguruar rrjetin midis IF dhe internetit, si dhe lidhjet me palët e treta.
3. IF duhet të zbatojë kontrolle të rrepta të qasjes në pajisjet dhe infrastrukturën e rrjetit, duke siguruar që vetëm personeli i autorizuar mund të bëjë ndryshime ose të ketë qasje në të dhëna të ndjeshme. Rregullat e kontrollit të qasjes në rrjet, në pajisjet e rrjetit duhet të dokumentohen dhe të rishikohen rregullisht.
4. Asetet e informacionit të IF duhet të grupohen në segmente të rrjetit bazuar në kritikalitetin e sistemeve, rolin funksional të sistemit ose ndjeshmërinë e të dhënave.
5. Të zbatojë kontrolle të qasjes në rrjet për të zbuluar dhe parandaluar lidhjen e pajisjeve të paautorizuara në rrjetin e saj dhe të sigurojë që të dhënat e ndjeshme të transmetuara përmes rrjetit të jenë të enkriptuara për ta mbrojtur atë nga përgjimi dhe qasja e paautorizuar.

6. IF duhet të marrë në konsideratë izolimin e aktiviteteve të shfletimit të internetit nga pajisjet e tij fundore përmes përdorimit të kontrolleve fizike ose logjike për të minimizuar ekspozimin ndaj sulmeve kibernetike.

7. IF duhet të zbatojë një zgjidhje efektive të mbrojtjes nga Sulm i Shpërndarë i Mohimit të Shërbimeve (DDoS – ang: Distributed Denial of Service) për të zbuluar dhe për t'iu përgjigjur llojeve të ndryshme të sulmeve të tilla.

8. IF duhet të kryejë vlerësime të rregullta të rrezikut të arkitekturës së rrjetit, duke përfshirë projektimin e sigurisë së rrjetit, si dhe ndërlidhjet e sistemit dhe rrjetit në mënyrë periodike për të identifikuar dobësitë e mundshme të sigurisë kibernetike.

9. IF duhet të krijojë dhe mirëmbajë plane rikuperimi për konfigurimet, pajisjet dhe të dhënat e rrjetit, për të siguruar vazhdimësinë dhe pajtueshmërinë e biznesit.

10. IF duhet të marrë masa mbrojtëse dhe të krijojë mekanizma për të mbrojtur rrjetin e brendshëm nga kërcënimet që vijnë nga burime të jashtme, të tilla si sulmet kibernetike dhe përpjekjet e tjera për të shkelur infrastrukturën e brendshme. Këto masa mbrojtëse duhet të përfshijnë:

    10.1. dokumentacionin e detajuar të pajisjeve fundore të rrjetit; dhe

    10.2. politikat dhe procedurat për qasjet dhe monitorimin e trafikut.

## Neni 35
## Menaxhimi i sigurisë së virtualizimit

1. IF duhet të dokumentojë dhe zbatojë politikat e sigurisë të përshtatura posaçërisht për teknologjitë e virtualizimit. Politika të tilla duhet të mbulojnë sigurinë, krijimin, shpërndarjen, ruajtjen, kopjimin rezervë, përdorimin, tërheqjen dhe shkatërrimin e imazheve virtuale.

2. IF duhet të sigurojë që standardet e sigurisë të vendosen për të gjithë komponentët e një zgjidhjeje virtualizimi. Të sigurojë që vetëm personeli i autorizuar të ketë qasje në shtresa virtualizimi (hipervisors) dhe sisteme operative hostuese, në përputhje me parimin e të drejtave minimale të nevojshme.

3. IF duhet të përdorë teknikat e segmentimit dhe izolimit të rrjetit për të ndarë mjediset virtuale.

4. IF duhet të mbajë një inventar të saktë dhe të përditësuar të burimeve dhe konfigurimeve virtuale.

5. IF sigurohet që të dhënat e ruajtura brenda makinave virtuale të jenë të enkriptuara dhe që janë zhvilluar procedurat e duhura të kopjimit të të dhënave dhe rikuperimit, për t'i mbrojtur nga humbja e të dhënave dhe shkeljet.

6. IF-të duhet të kryej auditime të rregullta të praktikave të sigurisë së virtualizimit për të siguruar respektimin e politikave të brendshme dhe kërkesave rregullative.

## Neni 36
## Siguria dhe privatësia e të dhënave

1. IF duhet të zhvillojë politika gjithëpërfshirëse për parandalimin e humbjes së të dhënave dhe të miratojë masa për të zbuluar dhe parandaluar qasjen, modifikimin, kopjimin ose transmetimin

e paautorizuar të të dhënave të tij të ndjeshme. Duhet të merren në konsideratë të dhënat në tranzit, të dhënat në qetësi dhe të dhënat në përdorim.

2. IF duhet të zbatojë masa të përshtatshme për të parandaluar dhe zbuluar vjedhjen e të dhënave, si dhe modifikimet e paautorizuara në sisteme dhe pajisje fundore. Duhet të zbatohen mekanizma monitorimi për të zbuluar incidente të mundshme të humbjes së të dhënave ose shkelje të politikave.
3. IF duhet të krijojë një politikë klasifikimi të të dhënave për të kategorizuar të dhënat bazuar në kërkesat e ndjeshmërisë dhe përputhshmërisë dhe të zbatojë kontrolle të rrepta të qasjes, për të siguruar që vetëm personeli i autorizuar mund të ketë qasje  në të dhënat e ndjeshme.
4. IF duhet të sigurohet që të dhënat e ndjeshme të jenë të enkriptuara si gjatë transportit ashtu edhe në gjendje qetësie, dhe të jenë të mbrojtura nga kontrolle të forta qasjeje.
5. IF duhet të zhvillojë një strategji për rikthimin e të dhënave kyçe ne rastet kur të dhënat në përdorim dhe kopjet rezerve online janë të kompremtuara..
6. IF duhet të sigurojë që sistemet e menaxhuara nga ofruesit e shërbimeve të jenë në përputhje me politikat e tyre të sigurisë së të dhënave të IF dhe detyrimet rregullatore.
7. Për të parandaluar rrjedhjen e të dhënave, duhet të zbatohen kontrolle të përshtatshme në mjediset jo-aktive të punës.
8. IF duhet të kufizojë përdorimin e të dhënave të ndjeshme të ambienteve aktive të punës, në mjedise jo-aktive të punës. Kur të dhënat e ambienteve aktive të punës duhet të përdoren në mjedise testimi, anonimizimi ose maskimi i të dhënave të paktën duhet të zbatohen.
9. IF duhet të përcaktojë dhe zbatojë politikat e ruajtjes së të dhënave që përputhen me kërkesat rregullatore dhe të dhënat duhet të fshihen përgjithmonë nga mediat e ruajtjes, sistemet dhe pajisjet fundore, para asgjësimit ose rishpërndarjes.

## Neni 37
## Menaxhimi i sigurisë së pajisjeve personale në mjedisin e punës

1. IF duhet të krijojë një politikë të qartë dhe gjithëpërfshirëse për pajisjet personale në mjedisin e punës (BYOD – ang: Bring Your Own Device) që përshkruan përdorimin e pranueshëm, kërkesat e sigurisë dhe përgjegjësitë e përdoruesit.
2. IF duhet të kryejë një vlerësim gjithëpërfshirës të rrezikut dhe duhet të merren masa të përshtatshme sigurie gjatë perdorimit të pajisjeve personale në mjedisin e punës (BYOD).
3. IF duhet të zbatojë kontrolle dhe masa për parandalimin e humbjes së të dhënave në kompjuterët personalë ose pajisjet mobile që përdoren për t'u qasur në asetet e informacionit të IF.
4. IF duhet të përdorë enkriptim për të dhënat e ndjeshme të ruajtura në pajisjet personale dhe për të dhënat e transmetuara midis këtyre pajisjeve dhe burimeve të institucionit.
5. IF duhet të sigurojë mundësinë për të fshirë të dhënat nga distanca nga pajisjet personale, në rast humbjeje, vjedhjeje ose pushimi nga puna të punonjësve.

6. IF duhet të zbatojë masa sigurie për pajisjet që hyjnë në rrjetin e saj, të tilla si firewall-e, VPN dhe sistemet e zbulimit të ndërhyrjeve për të monitoruar dhe mbrojtur nga kërcënimet.

7. IF sigurohet që të dhënat e institucionit mbahen të ndara nga të dhënat personale në pajisje, përmes përdorimit të kontejnerizimit ose zgjidhjeve të menaxhimit të pajisjeve mobile.

**Neni 38**
**Menaxhimi i asgjësimit të sigurt**

1. IF duhet të sigurojë që ekzistojnë procedura të përshtatshme për asgjësimin e aseteve të TI, si nga aspekti i privatësisë së të dhënave, ashtu edhe nga aspekti mjedisor.

2. IF duhet të kryejë vlerësime të rregullta të rrezikut për të identifikuar kërcënimet e mundshme që lidhen me asgjësimin e të dhënave dhe për të krijuar strategji lehtësuese.

3. IF duhet të përcaktojë metoda të pranueshme asgjësimi për lloje të ndryshme të të dhënave (p.sh., shkatërrim fizik, fshirje të të dhënave) në mjedise fizike dhe virtuale për të siguruar që të dhënat nuk mund të rindërtohen dhe duhet të mbajë dokumentacion të plotë të proceseve dhe rezultateve të asgjësimit.

4. IF duhet të rishikojë dhe përditësojë rregullisht praktikat e menaxhimit të asgjësimit të sigurt, bazuar në kërcënimet e reja, ndryshimet rregullatore dhe praktikat më të mira.

## KAPITULLI V
## OPERACIONET E SIGURISË KIBERNETIKE

**Neni 39**
**Inteligjenca e kërcënimeve kibernetike dhe ndarja e informacionit**

1. IF duhet të krijojë një proces për të mbledhur, përpunuar dhe analizuar informacionin që lidhet me sigurinë kibernetike për rëndësinë dhe ndikimin e tij të mundshëm në mjedisin e tij të biznesit dhe të TI. Informacioni që lidhet me sigurinë kibernetike duhet të përfshijë ngjarjet kibernetike, inteligjencën e kërcënimeve kibernetike dhe informacionin mbi dobësitë e sistemit. Kjo duhet të përfshijë rrjete vullnetare dhe bashkëpunuese të industrisë ose rrjete kombëtare të ndarjes së informacionit, nëse ekzistojnë rrjete të tilla.

2. IF duhet të marrë në konsideratë zbatimin e shërbimeve të monitorimit të inteligjencës kibernetike dhe të marrë pjesë aktive në marrëveshjet për ndarjen e informacionit mbi kërcënimet kibernetike me palë të besuara.

**Neni 40**
**Monitorimi dhe zbulimi i ngjarjeve kibernetike**

1. Për të lehtësuar monitorimin dhe analizën e vazhdueshme të ngjarjeve kibernetike, si dhe zbulimin dhe reagimin e shpejtë ndaj incidenteve kibernetike, IF duhet të kryejë funksione monitorimi, zbulimi, reagimi dhe rikuperimi. Në këtë drejtim, IF duhet të marrë në konsideratë krijimin e një Qendre të Operacioneve të Sigurisë (SOC – ang: Security Operations Center) ose

të marrë shërbime të menaxhuara sigurie sipas nenit 3 të kësaj rregulloreje. Duhet të përcaktohen proceset, rolet dhe përgjegjësitë për operacionet e sigurisë.

2. IF duhet të marrë në konsideratë dhënien e autoritetit të deleguar paraprakisht për veprime të caktuara emergjente për të përmbajtur incidentet dhe për të kufizuar përhapjen. Këtu mund të përfshihet, duke mos u kufizuar, pajisjet e emergjencës ose ndërprerjen e shërbimit kur nuk ka kohë për të mbledhur ekipin/planin e reagimit ndaj incidenteve.
3. Duhet të krijohet një proces për mbledhjen, përpunimin, shqyrtimin dhe ruajtjen e regjistrave të sistemit, për të lehtësuar operacionet e monitorimit të sigurisë së IF. Duhet të përcaktohet baza e kërkesave minimale të regjistrimit (p.sh., regjistrimi i ngjarjeve të suksesshme dhe të pasuksesshme të hyrjes, ndryshimet e privilegjeve, etj.). Këto regjistra duhet të mbrohen nga qasja e paautorizuar.
4. Për të lehtësuar identifikimin e anomalive, IF duhet të krijojë një profil bazë të aktiviteteve rutinë të secilit sistem TI dhe të analizojë aktivitetet e sistemit kundrejt profileve bazë. Profilet duhet të rishikohen dhe përditësohen rregullisht.
5. Për të identifikuar modelet e dyshimta ose anomali të aktivitetit të sistemit në regjistrat e sistemit duhet të kryhet korrelacioni i ngjarjeve të shumëfishta të regjistruara.
6. Duhet të krijohet një proces për të përshkallëzuar menjëherë aktivitetet e dyshimta ose anomali të sistemit ose sjelljen e përdoruesit tek palët përkatëse të interesit.

## Neni 41
## Reagimi, menaxhimi dhe raportimi i incidenteve kibernetike

1. IF duhet të krijojë një plan reagimi dhe menaxhimi ndaj incidenteve kibernetike për të izoluar dhe neutralizuar me shpejtësi një kërcënim kibernetik dhe për të rifilluar në mënyrë të sigurt shërbimet e prekura. Plani duhet të përshkruajë procedurat e komunikimit, koordinimit dhe reagimit për të adresuar skenarë të mundshëm të kërcënimeve kibernetike dhe duhet të integrohet me planet më të gjera të reagimit ndaj krizave dhe menaxhimit në të gjithë IF.
2. Si pjesë e planit, IF duhet të krijojë një proces për të hetuar dhe identifikuar mangësitë e sigurisë ose të kontrollit që çuan në shkelje. Hetimi duhet gjithashtu të vlerësojë shkallën e plotë të ndikimit tek IF dhe çdo palë e tretë e lidhur.
3. Informacioni nga inteligjenca kibernetike dhe mësimet e nxjerra nga incidentet kibernetike duhet të përdoren për të përmirësuar kontrollet ekzistuese ose për të përmirësuar planin e menaxhimit të incidenteve kibernetike.

## Neni 42
## Raportimi i incidenteve

Incidentet kibernetike dhe dështimet teknologjike duhet të raportohen tek Autoritetet Rregullatore përkatëse, sipas Neni 31 - Menaxhimi i incidenteve të kësaj rregulloreje.

## KAPITULLI VI
## REAGIMI DHE RIMËKËMBJA

### Neni 43
### Disponueshmëria e sistemit

Sistemet e TIK duhet të projektohen dhe zbatohen për të arritur nivelin e disponueshmërisë së sistemit që është në përputhje me nevojat e biznesit të tij. Nivelet e pranueshme të shërbimve ose të disponueshmërisë së sistemit duhet të përcaktohen për çdo funksion biznesi dhe të regjistrohen në marrëveshjet e nivelit të shërbimit të brendshme ose të jashtme.

### Neni 44
### Menaxhimi i vazhdimësisë së biznesit dhe rimëkëmbja nga fatkeqësitë

1. IF duhet të krijojnë një proces të shëndoshë menaxhimi të vazhdimësisë së biznesit për të maksimizuar aftësinë e tyre për të ofruar shërbime në mënyrë të vazhdueshme, për të arritur objektivat e tyre të disponueshmërisë të përcaktuara në marrëveshjet e tyre të nivelit të shërbimit dhe për të minimizuar humbjet në rast të ndërprerjeve të rënda të biznesit.
2. Si pjesë e menaxhimit të shëndoshë të vazhdimësisë së biznesit, IF duhet të kryejnë analizën e ndikimit në biznes (BIA – ang: Business Impact Analysis) duke analizuar ekspozimin e tyre ndaj dhe ndikimin nga ndërprerjet e biznesit. Duhet të merret në konsideratë një gamë skenarësh, duke përfshirë ato më të rënda, por të besueshme.
3. Analiza e ndikimit në biznes duhet të marrë në konsideratë gjithashtu rëndësinë e funksioneve të biznesit të identifikuara dhe të klasifikuara, proceseve mbështetëse, palëve të treta dhe aseteve të informacionit, si dhe ndërvarësitë e tyre.
4. IF duhet të përcaktojë objektivat e kohës së rikuperimit të sistemit dhe objektivat e pikës së rikuperimit që janë në përputhje me rezultatet e analizës se ndikimit në biznes .
5. IF duhet të sigurohen që karakteristikat e disponueshmërisë së sistemeve të TIK të jenë në përputhje me rezultatet e tyre të analizës së ndikimit në biznes. Për shembull, redundanca mund të zbatohet për disa komponentë kritikë për të parandaluar ndërprerjet e shkaktuara nga ngjarjet që ndikojnë në këta komponentë.
6. Bazuar në analizën e ndikimit në biznes të IF-së, IF duhet të hartojnë plane për të siguruar vazhdimësinë e biznesit dhe rimëkëmbjen nga fatkeqësitë. Këto plane, të cilat duhet të dokumentohen dhe miratohen nga organet menaxhuese të tyre, duhet të marrin në konsideratë në mënyrë specifike rreziqet që mund të ndikojnë në sistemet dhe shërbimet e TIK. IF duhet të koordinohen me palët përkatëse të interesit të brendshme dhe të jashtme, sipas rastit, gjatë hartimit të këtyre planeve.
7. Stafi duhet të trajnohet për të përdorur planet, dhe planet duhet të rishikohen, përditësohen dhe testohen të paktën një herë në vit ose pas ndryshimeve të rëndësishme në sistemet e TIK ose proceset e biznesit.

## Neni 45
## Testimi i planit të rimëkëmbjes nga fatkeqësitë

1. Palët përkatëse të interesit, përfshirë ata në funksionet e biznesit dhe të TIK, duhet të marrin pjesë në testet e vazhdimësisë së biznesit dhe të rimëkëmbjes nga fatkeqësitë për t'u njohur me proceset e rimëkëmbjes dhe për të përcaktuar nëse sistemet po funksionojnë siç pritet.
2. Një test i vazhdimësisë së biznesit/rimëkëmbjes nga fatkeqësitë duhet të bazohet në një plan testimi që përfshin objektivat dhe fushëveprimin, skenarët e testimit, me detaje të aktiviteteve që do të kryhen gjatë dhe pas testimit, si dhe kriteret për matjen e suksesit të testit.
3. Testimi duhet të përfshijë skenarë të ndryshëm të mundshëm ndërprerjesh, duke përfshirë paaftësinë e plotë dhe të pjesshme të qendrës primare të të dhënave dhe dështimet kryesore të sistemit. Ai gjithashtu duhet të adresojë varësitë e rikuperimit midis aseteve të ndryshme të informacionit, duke përfshirë ato të menaxhuara nga palë të treta.
4. Kur asetet e informacionit menaxhohen nga ofruesit e shërbimeve, IF duhet të vlerësojë aftësitë e tyre të rimëkëmbjes nga fatkeqësitë dhe të sigurojë që marrëveshjet e rimëkëmbjes nga fatkeqësitë për këto asete informacioni të jenë vendosur, testuar dhe verifikuar për të përmbushur nevojat e biznesit të IF. IF duhet të angazhojë ofruesin e tij të shërbimit për të testuar hapat e rimëkëmbjes që kërkojnë veprime të koordinuara.

## Neni 46
## Kopjet rezervë dhe rimëkëmbja

1. IF duhet të përcaktojë politika dhe procedura për kopje rezervë të rregullta që mundësojnë rimëkëmbjen në rast të ndërprerjes së sistemit, dëmtimit të të dhënave ose fshirjes. Arkivimi i të dhënave për ruajtje afatgjatë duhet të përfshihet në politika dhe procedura.
2. Për të siguruar që disponueshmëria e të dhënave është në përputhje me kërkesat e biznesit të IF, IF duhet të krijojë një politikë për të menaxhuar ciklin jetësor të të dhënave rezervë. Kjo duhet të përfshijë frekuencën e kopjes rezervë të të dhënave, periudhën e ruajtjes së të dhënave, numrin e kopjeve rezervë online dhe offline, menaxhimin e mekanizmave të ruajtjes së të dhënave dhe shkatërrimin e sigurt të mediave të kopjeve rezervë në fund të ciklit të tyre jetësor.
3. Për të adresuar rreziqet e ransomware-it, IF duhet të marrë në konsideratë krijimin e kopjeve rezervë me hapësirë të ndarë nga pjesa tjetër e rrjetit (air-gapped) ose të pandryshueshme (immutable backups).
4. IF duhet të testojë periodikisht rikthimin e sistemit të tij dhe kopjet rezervë të të dhënave për të vërtetuar efektivitetin e procedurave të rikthimit. Për sistemet kritike, testet e rikthimit duhet të kryhen të paktën çdo gjashtë muaj, ndërsa për sistemet jo-kritike, testet duhet të kryhen të paktën një herë në vit.
5. Për të mbrojtur kopjet rezervë nga qasja dhe modifikimi i paautorizuar, IF duhet të sigurojë që çdo e dhënë konfidenciale e ruajtur në mediumet e kopjes rezervë është e sigurt (p.sh., e enkriptuar).
6. Kopjet rezervë të të dhënave të klientëve dhe të dhënave të tjera kritike për funksionimin e IF duhet të jenë redundant (p.sh., të paktën në dy kopje ekuivalente) dhe të ruhen në vende të veçanta dhe të sigurta që nuk ka gjasa të ndikohen nga e njëjta fatkeqësi.

## Neni 47
## Qendra e të dhënave

1. IF duhet të kryejë një Vlerësim të Rrezikut të Kërcënimeve dhe Cenueshmërisë (ang: Threat And Vulnerability Risk Assessment -TVRA) për qendrat e tij të të dhënave (ang: Data Centre-DC) për të identifikuar cenueshmëritë, dobësitë dhe masat mbrojtëse të mundshme që duhet të vendosen për të mbrojtur qendrat e të dhënave (QDh) nga kërcënimet fizike dhe mjedisore. Përveç kësaj, vlerësimi duhet të marrë në konsideratë klimën politike dhe ekonomike të vendit në të cilin ndodhen QDh. Vlerësim i Rrezikut të Kërcënimeve dhe Cenueshmërisë duhet të rishikohet sa herë që ka një ndryshim të rëndësishëm në mediumin e kërcënimeve ose kur ka një ndryshim material në mjedisin e qendrës së të dhënave.
2. IF duhet të sigurojë redundancë të mjaftueshme për energjinë, lidhjen e rrjetit, ftohjen dhe sisteme të tjera elektrike dhe mekanike brenda QDH për të eliminuar rrezikun e pikave të vetme të dështimit. Duhet t'i kushtohet vëmendje sa vijon:
   2.1. diversifikimi i komunikimeve të të dhënave, shtigjeve të rrjetit dhe furnizuesve;
   2.2. vendosja e pajisjeve të energjisë, si UPS dhe gjeneratorët rezervë, dhe
   2.3. zbatimi i pajisjeve të ftohjes redundante në mënyrë të përshtatshme (p.sh., kullat e ftohjes, furnizimi me ujë të ftohtë dhe njësitë e ajrit të kondicionuar të dhomave të kompjuterëve) për të kontrolluar nivelet e temperaturës dhe lagështisë në QDh dhe për të parandaluar luhatjet potencialisht të dëmshme për sistemet.
3. Si pjesë e kontrolleve mjedisore të qendrës së të dhënave, IF duhet të zbatojë pajisje ose sisteme për zbulimin dhe shuarjen e zjarrit, si detektorë tymi ose nxehtësie, sisteme shuarjeje me gaz inert dhe sisteme spërkatëse me ujë të lagësht ose të thatë.
4. Qendra dytësore e të dhënave ose e rimëkëmbjes nga fatkeqësitë e IF duhet të jetë e ndarë gjeografikisht nga qendra e saj parësore ose e punës. Kjo do të sigurojë që ndërprerjet në infrastrukturën bazike (p.sh., telekomunikacioni dhe energjia) dhe/ose rreziqet mjedisore në një vendndodhje të caktuar të mos ndikojnë në të dyja vendet njëkohësisht.
5. Kontrollet e sigurisë fizike dhe mjedisore të QDh duhet të monitorohen 24/7.
6. Planet e reagimit dhe procedurat për incidentet fizike dhe mjedisore në QDH duhet të përcaktohet dhe testohen për një nivel të caktuar eskalimi.
7. QDh duhet të ketë kontrolle të përshtatshme fizike të qasjes. Praktikat më të mira përfshijnë:
   7.1. dhënia e qasjes stafit në bazë të nevojës, duke e revokuar menjëherë qasjen kur nuk është më e nevojshme;
   7.2. zbatimin e protokolleve të duhura të njoftimit dhe miratimit për vizitorët në qendrën e të dhënave. Të gjithë vizitorët duhet të shoqërohen nga stafi i autorizuar në çdo kohë ndërsa ndodhen në qendrën e të dhënave;
   7.3. sigurimi dhe monitorimi i pikave të qasjes fizike në qendrën e të dhënave në çdo kohë;
   7.4. kufizimin dhe monitorimin e qasjes në raftet e pajisjeve;
   7.5. sigurimi që stafi me qasje fizike në raftet e pajisjeve të mos ketë gjithashtu qasje në sistemet e informacionit;

7.6. kufizimin e qasjes në çelësa dhe pajisje të tjera fizike vetëm për stafin e autorizuar, duke i zëvendësuar ose ndryshuar menjëherë ato nëse janë vendosur gabimisht, humbasin ose vidhen, dhe

7.7. duke ndarë zonat e përbashkëta nga zonat e ndjeshme të sigurisë.

## KAPITULLI VII
## SKANIMI, TESTIMI, USHTRIMET DHE NDËRPRERJA

### Neni 48
### Skanimi i dobësive

IF duhet të krijojë një proces për skanimin e rregullt të dobësive për të identifikuar dobësitë e sigurisë dhe për të adresuar menjëherë rreziqet që lidhen me to. Frekuenca e skanimit duhet të jetë në përputhje me rëndësinë kritike të sistemeve të TI dhe rrezikun e sigurisë ndaj të cilit ato ekspozohen.

### Neni 49
### Testimi i depërtueshmërisë

1. IF duhet të kryejë testime të depërtueshmërisë (penetration testing) për të marrë një kuptim të thellë të mbrojtjeve të tij të sigurisë kibernetike.
2. Shërbimet digjitale të jashtme të IF duhet t'i nënshtrohen testeve të depërtimit në intervale të rregullta. Për IF e kategorizuara sipas Nenit 3 paragrafi 1, testet e depërtimit duhet të kryhen të paktën një herë në vit dhe pas çdo ndryshimi të madh në sistemet themelore. Për të gjitha IF e tjera, testimi i depërtimit duhet të kryhet të paktën çdo dy vjet dhe pas çdo modifikimi të madh të sistemit.
3. Testimi duhet të kryhet nga persona me njohuri dhe ekspertizë të mjaftueshme, si dhe kompetentë për të kryer aktivitete të tilla.

### Neni 50
### Ushtrimet për reagim ndaj incidenteve

1. IF duhet të kryejë ushtrime të rregullta kibernetike për të validuar procedurat e reagimit ndaj incidenteve kibernetike dhe rimëkëmbjes, duke përfshirë planet e komunikimit. Këto ushtrime mund të përfshijnë ushtrime në tavolinë (ang: a tabletop exercise) dhe simulime sulmesh. Përveç kësaj, ato mund të kombinohen me testimin e depërtimit dhe testimin të PVB/PRF(planifikimi i vazhdimësisë së biznesit/planifikimi i rimëkëmbjes nga fatkeqësitë).

   1.1. Për qëllime të këtij neni, një sulm i madh kibernetik mund të jetë një skenar ndërprerjeje në një test planifikimi të rimëkëmbjes nga fatkeqësitë.

2. Në varësi të objektivave të ushtrimit, IF duhet të përfshijë palët përkatëse të interesit, duke përfshirë menaxhmentin e lartë, njësitë e biznesit, specialistët e komunikimit të korporatave,

ekipet e menaxhimit të krizave, ofruesit e shërbimeve dhe stafin teknik përgjegjës për zbulimin, reagimin dhe rimëkëmbjen e kërcënimeve kibernetike.

### Neni 51
### Menaxhimi i masave korrigjuese

1. IF duhet të krijojnë një proces gjithëpërfshirës të masave korrigjuese për të ndjekur dhe zgjidhur problemet e identifikuara përmes skanimit të cenueshmërisë, testimit të depërtimit dhe ushtrimeve kibernetike. Procesi duhet të përfshijë minimalisht sa vijon:

   1.1. vlerësimi i kritikalitetit dhe klasifikimi i një problemi (duke përfshirë sinjalizimin dhe verifikimin e pozitivëve të rremë);

   1.2. afat kohor për të zgjidhur probleme me rëndësi të ndryshme, dhe

   1.3. vlerësimin e rrezikut dhe strategjitë e zbutjes për të menaxhuar devijimet nga korniza.

## KAPITULLI VIII
## GARANCIA E PAVARUR

### Neni 52
### Auditimi

1. Kërkesat e përcaktuara në Rregulloren për Kontrollet e Brendshme dhe Auditimin e Brendshëm të IF-ve zbatohen për auditimin e sistemit të informacionit.
2. Funksioni i auditimit të brendshëm duhet të kryejë auditime të brendshme të TI, kontrolleve të sigurisë kibernetike, qeverisjes, përputhshmërisë dhe proceseve të kontraktimit të jashtëm nga auditorë me njohuri, aftësi dhe kompetenca të mjaftueshme në TI dhe rreziqet e sigurisë, për të ofruar siguri të pavarur të efektivitetit të tyre për BD dhe menaxhmentin e lartë. Auditorët duhet të jenë të pavarur brenda ose nga IF dhe shpeshtësia dhe fokusi i auditimeve të tilla duhet të jetë në përputhje me rreziqet përkatëse të TI dhe sigurisë.
3. BD i IF duhet të miratojë planin vjetor të auditimit, duke përfshirë çdo auditim të TI dhe çdo modifikim material të tij. Plani i auditimit dhe ekzekutimi i tij, duke përfshirë shpeshtësinë e auditimit, duhet të pasqyrojnë dhe të jenë në përpjesëtim me rreziqet e natyrshme të TI dhe të sigurisë në IF dhe duhet të përditësohen rregullisht. Qëllimi dhe shpeshtësia e auditimeve duhet të jenë në përputhje me kritikalitetin dhe profilin e rrezikut të aseteve, funksioneve dhe proceseve të informacionit.
4. Duhet të vendoset një proces formal ndjekjeje, duke përfshirë dispozita për verifikimin dhe korrigjimin në kohë të gjetjeve kritike të auditimit të TI.
5. Vëzhgimet me rrezik të lartë dhe veprimet korrigjuese të ndërmarra duhet t'i raportohen BD, pa vonesa të panevojshme.
6. Së paku, IF duhet të punësojë staf të auditimit të brendshëm me kompetencë dhe aftësi për të zhvilluar një plan vjetor të auditimit të rrezikut teknologjik dhe për të kuptuar gjetjet, rreziqet dhe rekomandimet e ofruesve të specializuar të jashtëm.

7. Aktiviteti i fushës së TI duhet t'i nënshtrohet të paktën një rishikimi periodik vjetor që përqendrohet në metodologjinë e bazuar në rrezik.
8. IF duhet të sigurojë që auditorët e tij të rrezikut teknologjik të kenë nivelin e kërkuar të kompetencës dhe aftësive për të vlerësuar në mënyrë efektive përshtatshmërinë e politikave, procedurave, proceseve dhe kontrolleve të zbatuara të TI.

## KAPITULLI IX
## MENAXHIMI I OFRUESVE TË SHËRBIMEVE TEKNOLOGJIKE TË KONTRAKTUARA NGA JASHTË

### Neni 53
### Proporcionaliteti

Gjatë zbatimit të kërkesave të përcaktuara në këtë rregullore, IF duhet të marrin në konsideratë kompleksitetin e funksioneve të kontraktuara, rreziqet që rrjedhin nga marrëveshja e kontraktimit, rëndësinë kritike të funksionit të kontraktuar dhe ndikimin e mundshëm të kontraktimit në vazhdimësinë e aktiviteteve të tyre.

### Neni 54
### Qeverisja

1. Delegimi i funksioneve ose përdorimi i ofruesve të shërbimeve teknologjike (OShT) nuk e liron bordin nga përgjegjësitë e tij. IF mbeten përgjegjës dhe plotësisht të përgjegjshëm për përmbushjen e të gjitha detyrimeve të tyre rregullatore, duke përfshirë aftësinë për të mbikëqyrur kontraktimin e funksioneve kritike ose të rëndësishme.
2. IF duhet të sigurojë që ofruesit e shërbimeve teknologjike (OShT), përfshirë edhe për kontraktimet e jashtme, të mos rezultojë në rritje të rrezikut teknologjik dhe kibernetik.
3. IF për qeverisje të mirëfilltë të delegimit të funksioneve ose përdorimit të ofruesve të shërbimeve teknologjike duhet të:
   3.1. caktojë qartë përgjegjësitë për dokumentimin, menaxhimin dhe kontrollin e marrëveshjeve të kontraktim të jashtëm;
   3.2. ndajë burime të mjaftueshme për të siguruar pajtueshmërinë me të gjitha kërkesat ligjore dhe rregullatore, duke përfshirë udhëzimet dhe dokumentimin e monitorimin e të gjitha marrëveshjeve të jashtme;
   3.3. krijojë një funksion të kontraktimit të jashtëm ose të caktojë një anëtar të lartë të stafit që i përgjigjet bordit (p.sh., një mbajtës i funksionit kyç) dhe që është përgjegjës për menaxhimin dhe mbikëqyrjen e rreziqeve të marrëveshjeve të kontraktim të jashtëm si pjesë e kuadrit të kontrollit të brendshëm të institucionit dhe mbikëqyrjen e dokumentimit të marrëveshjeve të kontraktim të jashtëm.
4. Kur bën kontraktim të jashtëm, IF duhet të sigurojë të paktën sa vijon:

4.1. miratimin dhe zbatimin e vendimeve që lidhen me aktivitetet e saj të biznesit dhe funksionet kritike ose të rëndësishme;

4.2. mirëmbajtjen e zhvillimit të rregullt të biznesit të saj dhe ofrimin e shërbimeve financiare;

4.3. identifikim, vlerësim, menaxhim dhe zbutjen adekuate të rreziqeve që rrjedhin nga kontraktim të jashtëm;

4.4. kur është e aplikueshme, rregullime të përshtatshme për konfidencialitetin në lidhje me të dhënat dhe informacionet e tjera;

4.5. mirëmbajtja e një rrjedhe të përshtatshme të informacionit përkatës me ofruesit e shërbimeve;

5. Në rast të ndërprerjes së pa planifikuar të shërbimeve të kontraktuara, të funksioneve kritike ose të rëndësishme, institucioni ndërmerr të paktën njërin nga prej veprimeve të mëposhtme, brenda një afati kohor të përshtatshëm:

5.1. transferimi i funksionit te ofruesit alternativë të shërbimeve;

5.2. ri-integrimi i funksionit në institucion; ose

5.3. ndërprerjen e aktiviteteve të biznesit që varen nga funksioni; dhe

5.4. Kur të dhënat personale përpunohen nga ofruesit e shërbimeve të vendosura në vendet e treta, të dhënat përpunohen në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale.

**Neni 55**
**Vlerësimi i rrezikut**

1. IF duhet të përcaktojë nëse delegimi nga një institucion për kryerjen e proceseve, shërbimeve ose aktiviteteve te një ofrues shërbimesh bie nën përkufizimin e kontraktimit të jashtëm (outsourcing).

2. Për qëllimet e kësaj Rregulloreje, përcaktimet si në vijim nuk do të konsiderohet si kontraktim të jashtëm:

2.1. shërbime të shërbimeve globale të komunikimit financiar (p.sh., SWIFT) nëse burimet kryesore të sistemit të informacionit të nevojshme për ofrimin e një shërbimi të tillë janë brenda institucionit;

2.2. funksioni që kërkohet ligjërisht të kryhet nga një ofrues shërbimesh (p.sh., auditimi statutor);

2.3. shërbime informacioni për tregun (p.sh., ofrimi i të dhënave nga Bloomberg, Moody's, Standard & Poor's, IFtch);

2.4. infrastrukturat globale të rrjetit (p.sh., Visa, MasterCard) dhe shërbimet e telekomunikacionit;

2.5. marrëveshjet e kliringut dhe shlyerjes midis shtëpive të kliringut, kundër palëve qendrore dhe institucioneve të shlyerjes dhe anëtarëve të tyre;

2.6. infrastrukturat globale të mesazheve financiare që i nënshtrohen mbikëqyrjes nga autoritetet përkatëse;

2.7. shërbime bankare korrespondente;

2.8. blerja e shërbimeve që përndryshe nuk do të kryheshin nga institucioni (p.sh. këshilla nga një arkitekt, dhënia e mendimit ligjor dhe përfaqësimi para gjykatës dhe organeve administrative, pastrimi, kopshtaria dhe mirëmbajtja e ambienteve të institucionit, shërbimet mjekësore, servisimi i makinave të kompanisë, furnizimi me ushqim, shërbimet e makinave shitëse, shërbimet administrative, shërbimet e udhëtimit, shërbimet e zyrave postare, recepsionistët, sekretarët dhe operatorët e centralit), mallrat (p.sh. kartat plastike, lexuesit e kartave, furnizimet e zyrës, kompjuterët personalë, mobiljet) ose shërbimet (p.sh. energjia elektrike, gazi, uji, linja telefonike);

2.9. softuer i cili, duke qenë i gatshëm, është komercialisht i disponueshëm në treg dhe nuk kërkon përshtatje të konsiderueshme; dhe

2.10. shërbime të tjera të ngjashme me ato të përcaktuara në nën-paragrafët 2.1 deri në 2.9 të këtij paragrafi, me kusht që BQK të japë mendimin paraprak që dispozitat e kësaj Rregulloreje nuk zbatohen për përdorimin e këtyre shërbimeve.

3. IF duhet të vlerësojë rrezikun e mundshëm operacional të përdorimit të Ofruesi i Shërbimeve Teknologjike (OShT) dhe hyrjes në marrëveshje kontraktuale. IF duhet të marrë në konsideratë rezultatet e vlerësimit për të udhëhequr vendimet mbi dhënien e shërbimeve të jashtme dhe të ndërmarrë hapat e duhur për të shmangur rreziqet shtesë operacionale përpara se të hyjë në marrëveshje kontraktuale.

4. IF duhet ta konsiderojë gjithmonë një funksion si kritik ose të rëndësishëm në situatat e mëposhtme:

4.1. kur një defekt ose dështim në performancën e tij do të dëmtonte ndjeshëm performancën financiare dhe vazhdimësinë e aktivitetit të institucionit.

4.2. Kur detyrat operacionale të funksioneve të kontrollit të brendshëm kontraktohen, duhet të kryhet një vlerësim për të përcaktuar nëse një dështim për të ofruar funksionin e kontraktuar ose ofrimi i papërshtatshëm i tij do të ndikonte negativisht në efektivitetin e funksionit të kontrollit të brendshëm.

5. Me qëllim të menaxhimit të rrezikut të kontraktim të jashtëm është e nevojshme të përcaktohet kritikaliteti ose rëndësia e funksionit që do të nënkontraktohet.

6. IF duhet të përcaktojë kriteret dhe të përcaktojë metodologjinë për të vlerësuar kritikalitetin ose rëndësinë e një funksioni, duke përfshirë ndikimin e tij në pajtueshmërinë rregullatore dhe licencimin, ndikimin në performancën financiare, kontributin në qëndrueshmërinë operacionale dhe vazhdimësinë e shërbimeve, rëndësinë në ruajtjen e besimit të klientit dhe cilësisë së shërbimit, ndikimin e mundshëm në reputacionin ose pozicionin e institucionit në treg dhe shkallën e varësisë nga operacionet kryesore të biznesit.

7. Vlerësimi i rëndësisë ose i kritikalitetit është një proces i vazhdueshëm që duhet të kryhet në intervale të rregullta. Rishikimi i rregullt i vlerësimit të kritikalitetit ose të rëndësisë për t'u siguruar që ai të mbetet i rëndësishëm ndërsa kushtet e biznesit, rregulloret dhe operacionet ndryshojnë me kalimin e kohës.

8. Vlerësimi i funksioneve kritike ose të rëndësishme përfshin një qasje të strukturuar për të përcaktuar rëndësinë e secilit funksion për operacionet dhe detyrimet rregullatore të

institucionit. Ky vlerësim është thelbësor për të marrë vendime të informuara në lidhje me kontraktimin e jashtëm dhe për të siguruar që marrëveshjet e kontraktimit nuk kompromentojnë qëndrueshmërinë operacionale ose pajtueshmërinë rregullatore.

## Neni 56
## Marrëdhënia kontraktuale midis IF dhe një Ofruesi Shërbimesh

1. Kur hyn në një marrëveshje me një ofrues shërbimesh, IF duhet të sigurojë që fushëveprimi dhe përmbajtja e dispozitave kontraktuale të jenë të përshtatshme për rreziqet që lidhen me kontraktim të jashtëm dhe për fushëveprimin dhe kompleksitetin e funksioneve të jashtë-kontraktuara.
2. Institucionet duhet të lidhin një marrëveshje me shkrim me një ofrues shërbimesh, e cila duhet të përmbajë të paktën sa vijon:
   2.1. një përshkrim të detajuar të funksionit të kontraktuar që është objekt i marrëveshjes;
   2.2. data e fillimit dhe data e mbarimit të përmbushjes së detyrimeve kontraktuale;
   2.3. detyrimet financiare të palëve;
   2.4. dispozitat që rregullojnë mënyrën se si një institucion monitoron vazhdimisht kryerjen e funksionit, i cili është objekt i marrëveshjes, duke përfshirë llojet e raporteve që duhet të marrë institucioni nga ofruesi i shërbimit dhe shpeshtësinë e dorëzimit të tyre;
   2.5. detyrimin e ofruesit të shërbimit për të njoftuar institucionin në kohën e duhur për të gjitha faktet dhe ndryshimet në rrethana që kanë ose mund të kenë një ndikim të rëndësishëm në përmbushjen e detyrimeve kontraktuale;
   2.6. niveli i shërbimit të dakorduar dhe cilësia e funksioneve të kryera, duke përfshirë objektivat cilësorë dhe, kur është e aplikueshme, sasiorë të performancës për funksionin e kontraktuar, të cilat lejojnë ndërmarrjen e veprimeve korrigjuese në kohë nga institucioni;
   2.7. kur është e përshtatshme, detyrimin e sekretit të biznesit dhe detyrimin dhe mënyrën e mbrojtjes së të dhënave konfidenciale dhe personale, duke përfshirë dispozitat në lidhje me qasjen, disponueshmërinë, integritetin, privatësinë dhe sigurinë e të dhënave përkatëse;
   2.8. kur është e nevojshme, vendndodhjen/vendndodhjet ku do të ofrohet funksioni i kontraktuar dhe ku do të mbahen, përpunohen dhe ruhen të dhënat përkatëse, duke përfshirë një kërkesë për të njoftuar institucionin nëse ofruesi i shërbimit propozon të ndryshojë vendndodhjen/vendndodhjet;
   2.9. dispozita nëse lejohet nën-kontraktimi i funksionit;
   2.10. detyrimin e ofruesit të shërbimeve për të ofruar shërbimet në një mënyrë të tillë që të jetë plotësisht në përputhje me legjislacionin përkatës të Republikës së Kosovës;
   2.11. detyrimin e ofruesit të shërbimit për të siguruar të drejtat e qasjes dhe ekzaminimit në vend për BQK-në, në mënyrën e përcaktuar në nenin 5, paragrafi 2, të kësaj Rregulloreje;
   2.12. dispozita që sigurojnë që të dhënat që janë në pronësi të institucionit mund të qasen në rast të shpërbërjes ose ndërprerjes së operacioneve të biznesit të ofruesit të shërbimit (p.sh. falimentimi, zgjidhja e çështjeve, likuidimi ose procedura të ngjashme);

2.13. dispozita nëse ofruesi i shërbimit duhet të marrë një polisë sigurimi për dëmshpërblim profesional dhe, nëse është e aplikueshme, nivelin e mbulimit të sigurimit të kërkuar;

2.14. detyrimin e ofruesit të shërbimit për të bashkëpunuar me BQK-në si autoritete kompetente dhe autoritete të zgjidhjes së problemeve të institucionit;

2.15. kohëzgjatjen e marrëdhënies kontraktuale ose një tregues se marrëveshja është me kohëzgjatje të pacaktuar;

2.16. një përshkrim të kushteve për përfundimin dhe/ose anulimin e marrëveshjes me periudha njoftimi të përcaktuara për institucionin dhe për ofruesin e shërbimit;

2.17. të drejtat e institucionit për të ndërprerë ose anuluar një marrëveshje me ofruesin e shërbimit, nëse po, të urdhëruara nga BQK;

2.18. zgjedhja e ligjit të zbatueshëm; dhe

2.19. metoda e zgjidhjes së mosmarrëveshjeve.

3. Kur IF dhe ofruesi i shërbimit lidhin një marrëveshje për kontraktim të jashtëm për funksione kritike ose të rëndësishme, marrëveshja duhet, përveç përmbajtjes së specifikuar në paragrafin 2 të këtij neni, të përmbajë sa vijon:

3.1. detyrimin e ofruesit të shërbimit për të siguruar të drejtat e qasjes dhe të auditimit për institucionin në mënyrën e përcaktuar në nenin 57, paragrafi 2 i kësaj Rregulloreje;

3.2. dispozita mbi zbatimin dhe testimin e planeve të emergjencës së biznesit;

3.3. detyrimet e ofruesit të shërbimit në rastin e transferimit të funksionit të deleguar te një ofrues tjetër shërbimi ose përsëri te institucioni, duke përfshirë detyrimet në lidhje me trajtimin e të dhënave;

3.4. përcaktimin e një periudhe të përshtatshme tranzicioni, gjatë së cilës ofruesi i shërbimit, pas përfundimit ose anulimit të marrëveshjes së kontraktim të jashtëm, do të vazhdojë të ofrojë funksionin e kontraktuar për të zvogëluar rrezikun e ndërprerjeve; dhe

3.5. detyrimin e ofruesit të shërbimit për të mbështetur institucionin në transferimin ose ri-integrimin e rregullt të funksionit në rast të anulimit ose përfundimit të marrëveshjes së kontraktimit

4. Marrëveshja kontraktuale duhet të specifikojë nëse lejohet apo jo nën-kontraktimi i funksioneve kritike ose të rëndësishme, ose pjesëve materiale të tyre.

5. Nëse lejohet nën-kontraktimi i funksioneve kritike ose të rëndësishme, institucionet duhet të përcaktojnë nëse pjesa e funksionit që do të nën-kontraktohet është, si e tillë, kritike apo e rëndësishme (d.m.th., një pjesë materiale e funksionit kritik ose të rëndësishëm) dhe, nëse po, ta regjistrojnë atë në regjistër.

6. Kur një marrëveshje për kontraktim të jashtëm për funksione kritike ose të rëndësishme përfshin mundësinë e nën-kontraktimit, përveç përmbajtjes së specifikuar në paragrafët 2 dhe 3 të këtij neni, ajo marrëveshje duhet të përmbajë të paktën sa vijon:

6.1. detyrimin e ofruesit të shërbimit për të njoftuar institucionin për çdo nën-kontraktim të planifikuar, ose ndryshime materiale të tij, brenda periudhës që do t'i lejonte institucionit të kryente një vlerësim të rrezikut të ndryshimeve të propozuara dhe, kur është e nevojshme,

të kundërshtonte në kohën e duhur nën-kontraktimin e planifikuar, ose ndryshimet materiale të tij;

6.2. E drejta për të anuluar/përfunduar marrëveshjen kur nën-kontraktimi rrit rreziqet për institucionin ose kur ofruesi i shërbimit nën-kontrakton pa njoftuar institucionin dhe në raste të tjera të justifikuara;

6.3. kur nën-kontraktimi përfshin përpunimin e të dhënave personale, detyrimi i ofruesit të shërbimit për të marrë autorizim me shkrim nga institucioni;

6.4. detyrimin e ofruesit të shërbimit për të mbikëqyrur ato shërbime që i ka nën-kontraktuar;

6.5. kushtet që duhen përmbushur në rastin e nën-kontraktimit;

6.6. llojet e funksioneve që nuk mund të nën-kontraktohen;

6.7. detyrimin e ofruesit të shërbimit për të kërkuar miratim me shkrim nga institucioni për çdo nën-kontraktim të planifikuar, ose ndryshime materiale të tij, ose të drejtën për të kundërshtuar kontraktimin e planifikuar; dhe

6.8. detyrimin e ofruesit të shërbimit për të negociuar me nën-kontraktorin mbi të drejtat e qasjes dhe auditimit ose ekzaminimit në vend në mënyrën e përcaktuar në nenin 57, paragrafi 1 i kësaj Rregulloreje.

7. IF mund të lejojë nën-kontraktimin vetëm kur nën-kontraktori merr përsipër të veprojë në përputhje me ligjin në fuqi dhe kërkesat rregullatore, të përmbushë detyrimet përkatëse kontraktuale dhe t'i sigurojë institucionit dhe BQK të njëjtat të drejta qasjeje dhe auditimi ose ekzaminimi në vend si ato të dhëna nga ofruesi i shërbimit në përputhje me nenin 57 të kësaj Rregulloreje.

8. IF duhet të sigurojë që ofruesi i shërbimit mbikëqyr në mënyrë të përshtatshme nën-ofruesit e shërbimeve, në përputhje me politikën e përcaktuar nga institucioni. Nëse nën-kontraktimi i propozuar mund të ketë efekte negative materiale në marrëveshjen e nën-kontraktimit të një funksioni kritik ose të rëndësishëm ose do të çonte në një rritje materiale të rrezikut, duke përfshirë rastet kur kushtet në paragrafin 7 të këtij neni nuk do të plotësoheshin, institucioni duhet të ushtrojë të drejtën e tij për të kundërshtuar nën-kontraktimin, nëse është rënë dakord për një të drejtë të tillë, dhe/ose të ndërpresë kontratën.

## Neni 57
## Të drejtat e qasjes dhe auditimit ose ekzaminimit në vend

1. IF duhet të sigurojë, brenda marrëveshjes së kontraktimit të jashtëm me ofruesin e shërbimit, që ofruesi i shërbimit t'i sigurojë BQK ose çdo personi të emëruar nga BQK për këtë qëllim, sa vijon:

1.1. Qasje me kohë dhe të plotë në mjediset e biznesit, duke përfshirë pajisjet, sistemet, rrjetet, informacionin dhe të dhënat e përdorura për ofrimin e funksionit të kontraktuar, duke përfshirë informacionin financiar përkatës, personelin dhe auditorët e jashtëm të ofruesit të shërbimit.; dhe

1.2. Kryerja e ekzaminimeve në vend të një pjese të veprimtarisë së ofruesit të shërbimit që lidhet ose mund të lidhet me kontraktim të jashtëm, si dhe ekzaminimeve në vend të

kryerjes së funksioneve që janë objekt i marrëveshjes me ofruesin e shërbimit, për t'i mundësuar atij të monitorojë marrëveshjen e kontraktuar dhe për të siguruar pajtueshmërinë me të gjitha kërkesat rregullatore dhe kontraktuale të zbatueshme.

2. Lidhur me kontraktim të jashtëm të funksioneve kritike ose të rëndësishme, institucionet duhet të sigurojnë, brenda marrëveshjes së kontraktimit të funksioneve kritike ose të rëndësishme me ofruesin e shërbimit, që ofruesi i shërbimit t'i sigurojë institucionit, auditorëve të tij të jashtëm dhe personave të tjerë që ai emëron për këtë qëllim dhe BQK si autoritete të zgjidhjes/ përmbylljes së institucioneve të përcaktuara sipas legjislacionin qe rregullon këtë fushë, si vijon:

   2.1. qasje me kohë dhe të plotë në ambientet e biznesit, duke përfshirë pajisjet, sistemet, rrjetet, informacionin dhe të dhënat e përdorura për ofrimin e funksionit të kontraktimit , duke përfshirë informacionin financiar përkatës, personelin dhe auditorët e jashtëm të ofruesit të shërbimit; dhe

   2.2. Kryerja e auditimeve ose rishikimeve të një pjese të operacionit të ofruesit të shërbimit që lidhet ose mund të lidhet me kontraktim, si dhe rishikimet e performancës së funksioneve të kontraktuara që janë objekt i marrëveshjes me ofruesin e shërbimit, për t'i mundësuar atyre të monitorojnë marrëveshjen kontraktuale dhe për të siguruar pajtueshmërinë me të gjitha kërkesat rregullatore dhe kontraktuale të zbatueshme.

3. IF duhet të sigurojë, brenda marrëveshjes kontraktuale me ofruesin e shërbimit, që funksioni i tij i auditimit të brendshëm të jetë në gjendje të rishikojë funksionin e kontraktuar, duke përdorur një qasje të bazuar në rrezik.

4. Institucionet duhet të ushtrojnë të drejtat e tyre të qasjes dhe auditimit të përmendura në këtë nen dhe të përcaktojnë shpeshtësinë e auditimit dhe fushat që do të auditohen, duke përdorur një qasje të bazuar në rrezik.

5. Për qëllimin e kryerjes së auditimeve dhe shqyrtimeve të përmendura në paragrafin 2, nën-paragrafin 2.2, të këtij neni, një institucion mund të përdorë:

   5.1. auditime të përbashkëta të organizuara, së bashku me klientë të tjerë të të njëjtit ofrues shërbimesh dhe të kryera nga institucioni dhe këta klientë ose nga një palë e tretë e emëruar prej tyre; dhe

   5.2. certifikime nga palë të treta dhe raporte të auditimit nga palë të treta ose të brendshme, të vëna në dispozicion nga ofruesi i shërbimit.

6. Për dhënien me kontratë të funksioneve kritike ose të rëndësishme, një institucion vlerëson nëse certifikimet dhe raportet e palëve të treta, siç përmenden në paragrafin 5, nën-paragrafin 5.2, të këtij neni, janë të përshtatshme dhe të mjaftueshme për kryerjen e auditimeve dhe rishikimeve të duhura të marrëveshjeve të dhënies me kontratë dhe nuk mbështetet vetëm në këto raporte me kalimin e kohës.

7. Kur marrëveshja kontraktuale mbart një nivel të lartë kompleksiteti teknik, për shembull në rastin e kontraktimit të shërbimeve në ‘Cloud’, një institucion duhet të verifikojë:

   7.1. nëse personat e përmendur në paragrafin 5 të këtij neni që kryejnë auditimin dhe/ose vlerësimin kanë aftësi dhe njohuri të përshtatshme dhe relevante për të kryer auditime dhe/ose vlerësime relevante në mënyrë efektive; dhe

7.2. nëse stafi i institucionit që shqyrton certifikimet dhe/ose raportet nga personat e përmendur në paragrafin 5 të këtij neni ka aftësi dhe njohuri të përshtatshme dhe relevante për të kryer auditime dhe/ose shqyrtime relevante në mënyrë efektive.

**Neni 58**
**Mbikëqyrja e funksioneve të jashtë-kontraktuara**

1. IF duhet të monitorojë, në mënyrë të vazhdueshme, performancën e ofruesve të shërbimeve në lidhje me të gjitha marrëveshjet e kontraktimit të jashtëm mbi një qasje të bazuar në rrezik dhe me fokusin kryesor në kontraktimine funksioneve kritike ose të rëndësishme, duke përfshirë sigurimin e disponueshmërisë, integritetit dhe sigurisë së të dhënave dhe informacionit. Kur rreziku, natyra ose shkalla e një funksioni të -kontraktuar ka ndryshuar materialisht, institucionet duhet të rivlerësojnë kritikalitetin ose rëndësinë e atij funksioni në përputhje me nenin 6 të kësaj Rregulloreje.
2. IF duhet të tregojë aftësitë, kujdesin e duhur kur monitoron dhe menaxhon marrëveshjet e kontraktuara.
3. IF duhet të përditësojë rregullisht vlerësimin e rrezikut dhe të raportojë periodikisht te organi drejtues mbi rreziqet e identifikuara në lidhje me kontraktimin e funksioneve kritike ose të rëndësishme.
4. IF duhet të sigurojnë, në mënyrë të vazhdueshme, që marrëveshjet e kontraktuara, me fokusin kryesor në kontraktimin e funksioneve kritike ose të rëndësishme, të përmbushin standardet e duhura të performancës dhe cilësisë në përputhje me politikat e tyre, duke:
   4.1. u siguruar që ata marrin raportet e duhura nga ofruesit e shërbimeve;
   4.2. vlerësuar performancën e ofruesve të shërbimeve, duke përdorur mjete të tilla si treguesit kryesorë të performancës, treguesit kryesorë të kontrollit, raportet e ofrimit të shërbimeve, vet-çertifikimin dhe rishikimet e pavarura; dhe
   4.3. rishikuar të gjitha informacionet e tjera relevante të marra nga ofruesi i shërbimit, duke përfshirë raportet mbi masat dhe testimet e vazhdimësisë së biznesit.
5. IF duhet të marrin masat e duhura nëse identifikojnë mangësi në ofrimin e funksionit të kontraktuar. Në veçanti, institucionet duhet të ndjekin çdo tregues që tregon se ofruesit e shërbimeve mund të mos e kryejnë funksionin kritik ose të rëndësishëm të kontraktuar në mënyrë efektive ose në përputhje me ligjet dhe kërkesat rregullatore në fuqi. Nëse identifikohen mangësi, institucionet financiare duhet të ndërmarrin veprime të duhura korrigjuese ose riparuese. Veprime të tilla mund të përfshijnë ndërprerjen e marrëveshjes së kontraktuar, me efekt të menjëhershëm, nëse është e nevojshme.

**Neni 59**
**Kompetenca e furnizuesit**

IF duhet të lidhë kontrata vetëm me furnizues që demonstrojnë kompetencë të lartë dhe personel të kualifikuar për funksionet e deleguara dhe Menaxhim të Rrezikut Teknologjik ( MRrT ) efektiv.

## Neni 60
## Cloud Computing

1. BQK duhet të njoftohet për planet për të lidhur kontrata me Ofruesit e Shërbimeve në ambientet Cloud(OShC) (ang: Cloud Service Provider -CSP) për ofrimin ose mbështetjen materiale të ofrimit të shërbimeve kritike, me një kohë të mjaftueshme paraprake (një muaj) para angazhimit, për t'i lejuar mbikëqyrësit të kryejë një vlerësim të rrezikut dhe të ngrejë shqetësime, nëse ka.
2. Përdorimi i shërbimeve të bazuara në Cloud për shërbime/funksione kritike duhet të miratohet nga bordi, dhe një regjistër i të gjitha shërbimeve Cloud të përdorura nga IF për funksione biznesi duhet të jetë i disponueshëm në çdo kohë.
3. Bordi dhe IF duhet të kuptojnë dhe të përmbushin përgjegjësitë e tyre në lidhje me sigurinë e burimeve të Cloud-it nën kontrollin e tyre ("siguria në Cloud"), ndërkohë që marrin siguri të pavarur se ekziston angazhim dhe kapacitet i mjaftueshëm i OShC në lidhje me sigurinë e infrastrukturës së burimeve të lartpërmendura të Cloud-it ("siguria e Cloud").
4. IF duhet të ruajë kontrollin mbi vendndodhjen e të dhënave financiare dhe personale të ruajtura dhe të përpunuara brenda OShC.
5. Ruajtja dhe përpunimi i të dhënave financiare dhe personale në Cloud duhet të kufizohet në juridiksione me ligje përkatëse ose traktate ndërkombëtare që sigurojnë të njëjtin nivel mbrojtjeje për të dhënat financiare dhe personale si legjislacioni vendas.
6. IF duhet t'i kërkojë OShC të marrë një deklaratë pa kundërshtime përpara se të nën-kontraktojë pjesë të shërbimit të dhënë me kontratë.
7. IF duhet t'i kërkojë OShC të sigurojë ndarje strikte logjike të të dhënave dhe burimeve të tij të virtualizuara nga shfrytëzuesit e tjerë të OShC.
8. Politikat e ndërprerjes duhet të parashikojnë një dalje dhe transferim të rregullt të të dhënave nëse IF ose ofruesi i shërbimeve në Cloud dëshiron ta ndërpresë kontratën.

# KAPITULLI X

# INTELIGJENCA ARTIFICIALE

## Neni 61
## Zhvillimi dhe vendosja e zgjidhjeve të mundësuara nga Inteligjenca Artificiale

1. IF duhet të krijojë një kornizë qeverisjeje për Inteligjencë Artificiale (IA) për të mbikëqyrur përdorimin e IA.
2. IF duhet ta përshtasin zhvillimin dhe vendosjen e IA me objektivat e tyre strategjike, udhëzimet etike dhe politikat e menaxhimit të rrezikut.
3. Bordet e drejtorëve duhet të sigurojnë që sistemet e IA të jenë në përputhje me kërkesat rregullatore dhe brenda apetitit të tyre për rrezik. IF duhet të sigurojnë ndërgjegjësim dhe llogaridhënie në nivel bordi për vendosjen e inteligjencës artificiale.

4. IF duhet të kryejë vlerësime gjithëpërfshirëse të rrezikut për sistemet e IA, duke përfshirë rreziqet operacionale, financiare, të reputacionit dhe ligjore.
5. IF duhet të sigurohen që sistemet e IA të jenë të lira nga paragjykimet, t'i përmbahen parimeve të trajtimit të drejtë dhe të mos çojnë në rezultate diskriminuese. Modelet e IA duhet të dokumentohen, duke u siguruar që ato të jenë të shpjegueshme dhe të auditueshme.
6. Sistemet e IA të përdorura në funksione kritike duhet t'i nënshtrohen testimit të stresit për të vlerësuar performancën e tyre në kushte të ndryshme.
7. IF duhet të sigurojë që të dhënat e përdorura në sistemet e IA janë të sakta, të plota dhe pa paragjykime.
8. IF duhet të validojë modelet e IA para vendosjes dhe rregullisht më pas.
9. IF duhet të sigurojë që sistemet e IA të jenë të interpretueshme për palët e interesuara të brendshme dhe, kur është e aplikueshme, për klientët.
10. IF duhet t'u bëjë të ditur klientëve kur IA përdoret në vendimet që i prekin ata (p.sh., miratimet e kredisë, profilizimi i rrezikut). Duhet të ofrohen kanale që klientët të apelojnë vendimet e mbështetura nga IA.
11. IF duhet të raportojë menjëherë incidentet që përfshijnë keq-funksionime të IA, shkelje ose rezultate negative.
12. IF duhet t'i përmbahet parimeve të drejtësisë, llogaridhënies, transparencës dhe dizajnit të përqendruar te njeriu.
13. Zbatimi i zgjidhjeve të mundësuara nga IA në funksionet kritike duhet të kërkojë miratim paraprak rregullator.

## KAPITULLI XI
## DISPOZITAT KALIMTARE PËRFUNDIMTARE

### Neni 62
### Zbatimi, masat përmirësuese dhe ndëshkimet administrative

Çdo shkelje e dispozitave të kësaj rregulloreje do të jetë subjekt i masave përmirësuese, ndëshkimeve administrative dhe ndëshkimeve monetare siç përcaktohet në Ligjin Nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës, të plotësuar dhe ndryshuar me Ligjin Nr. 05/L –150, Ligjin Nr. 04/L-093 për Bankat, Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare, Ligjin Nr. 04/L-155 për Sistemin e Pagesave, Ligjin Nr. 05/L -045 për Sigurimet, , Ligjin Nr. 04/L-101 për Fondet Pensionale të Kosovës, si dhe Ligjin Nr. 04/L-018 për Sigurimin e Detyrueshëm nga Autopërgjegjësia.

### Neni 63
### Zbatueshmëria

Kjo Rregullore do të mbizotërojë ndaj të gjitha dispozitave të akteve nënligjore normative të BQK-së që rregullojnë sistemet e informacionit dhe menaxhimin e rrezikut kibernetik, të institucioneve financiare të cilat nuk janë në përputhje me këtë rregullore.

**Neni 64**
**Shtojcat**

1. Pjesë përbërëse e kësaj rregulloreje janë shtojcat si vijon:
   1.1. Shtojca 1 – Model i Raportit të informimit të menjëhershëm
   1.2. Shtojca 2 - Model i Raportit të detajuar të incidentit.
2. Shtojca 1 - Model i Raportit të informimit të menjëhershëm dhe Shtojca 2 - Model i Raportit të detajuar të incidentit përmbajnë përcaktime dhe kërkesa minimale. Të njëjtat mund të plotësohen dhe zëvendësohen me udhëzim të veçantë të nxjerrë nga BQK-ja.

**Neni 65**
**Udhëzimet**

Për qëllime të zbatimit të kësaj Rregulloreje, BQK-ja të nxjerrë udhëzime të veçanta.

**Neni 66**
**Shfuqizimi**

1. Me hyrjen në fuqi të kësaj Rregulloreje, shfuqizohen dispozitat e mëposhtme:
   1.1. Rregullore mbi Teknologjinë e Informacionit për Bankat;
   1.2. Rregullore mbi Sistemet dhe Sigurinë e Informacionit për Fondet e Pensioneve;
   1.3. Neni 7 - Kërkesat për dhomën e serverëve, nga: Rregullorja për Kërkesat Minimale të Sigurisë
   1.4. Neni 3, paragrafi 2.d, nga: Rregullorja mbi Funksionet e Delegimit të Siguruesve.

**Neni 67**
**Hyrja në fuqi**

Kjo Rregullore hyn në fuqi 15 shtator 2025 . Institucionet financiare-IF janë të obliguara që të jenë në harmoni me kërkesat e kësaj rregulloreje, nga data 01 qershor 2026.

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

## SHTOJCA 1 - MODEL I RAPORTIT TË INFORMIMIT TË MENJËHERSHËM

| | RAPORTI I INFORMIMIT TË MENJËHERSHËM |
|---|---|
| **Shënime**: | |
| a | Incidenti duhet të raportohet brenda 4 orëve pas identifikimit të tij. Një raport i dytë në formatin e përcaktuar duhet të ofrohet pas hetimit paraprak, brenda 72 orëve nga ndodhja. Përditësimet duhet të ofrohen sa herë që ndodh ndonjë zhvillim deri në paraqitjen e raportit të mbyllies. |
| b | Raporti i incidentit duhet të dërgohet në Divizionin e Mbikëqyrjes së Sistemeve të Informacionit në adresën e dmsi@bqk-kos.org |
| c | Raporti duhet të paraprihet nga një bisedë e menjëhershme telefonike me zyrtarët e BQK (ndërsa raporti është duke u përgatitur). |
| d | Raporti duhet të nënshkruhet nga CISO. |
| **Informacion bazë** | |
| 1 | Emri dhe adresa e bankës raportuese |
| 2 | Emrat e dy kontakteve të nivelit të lartë. Përfshi numrat e telefonit dhe adresat emailt |
| **Përmbledhje e incidentit** | |
| 1 | Natyra e incidentit (p.sh., DDOS, ransomware, shkelje/vjedhje të dhënash, klonim ose defacement i uebit) |
| 2 | Përshkrim i shkurtër i incidentit |
| 3 | Koha e incidentit dhe koha e zbulimit |
| 4 | Sistemet e prekura (p.sh., CBS, Thesari, financimi tregtar, bankimi në internet, bankomatet, sistemet e pagesave si SWIFT, RTGS, ACH), duke treguar nëse sistemet e prekura janë kritike apo jokritike. |
| **Detajet e raportimit** | |
| 1 | Data dhe ora e raportimit te mbikëqyrësi / autoritetet e tjera |
| 2 | Emri i personit që raporton |
| 3 | Emri dhe të dhënat e kontaktit të CISO-s (të paktën dy numra telefoni dhe email-e) |
| **Njohuri e menjëhershme mbi shkakun e incidentit** | |
| 1 | Përshkrim i shkurtër i asaj që shkaktoi suksesin e sulmit |
| **Ndikimi i incidentit** | |
| 1 | Ndërprerje e pritur e sistemeve kritike që ndikojnë në transaksionet e klientëve dhe sistemet e pagesave |
| 2 | Shkalla dhe natyra në të cilën ka pasur një shkelje të të dhënave |
| 3 | Ndikimi financiar në aspektin e parave të vjedhura, transaksioneve të biznesit të |
| 4 | Disponueshmëria e stafit teknik për të trajtuar situatën dhe nëse i gjithë stafi i caktuar është i pranishëm. Nëse jo, renditni marrëveshjet alternative që janë bërë, duke përfshirë stafin e kontraktuar nga jashtë. |
| **Masat korrigjuese të marra** | |
| 1 | Masa të përkohshme për të zbutur/zgjidhur problemin dhe arsyet për marrjen e masave të tilla |
| 2 | Masat e marra për të mbrojtur të dhënat dhe detajet e tjera të nevojshme për një audit mjeko-ligjor |
| 3 | Hapat e ndërmarrë/që do të ndërmerren për të pastruar sistemin nga dëmtime të |
| 4 | Hapat e propozuar për të parandaluar përsëritjen e mëtejshme të këtij dëmi |
| **Menaxhimi i medias dhe palëve të interesuara** | |

| | |
|---|---|
| 1 | Çdo komunikim me median dhe palët e interesuara/autoritetet e ndryshme (p.sh., polisa kibernetike). Një kopje e komunikimeve të tilla duhet të bashkëngjitet. |
| 2 | Nëse dokumentet e komunikimit nuk janë mbledhur, jepni arsyet pse nuk janë mbledhur dhe veprimet e ardhshme në këtë drejtim. |
| **Nënshkrimi i CISO** | |
| **Emri dhe të dhënat e kontaktit - dy numra telefoni, adresa email** | |

## SHTOJCA 2 - MODEL I RAPORTIT TË DETAJUAR TË INCIDENTIT

| | |
|---|---|
| | **RAPORTI I DETAJUAR I INCIDENTIT** |
| **Emri dhe adresa e bankës** | |
| **Detajet e referencës** | |
| 1 | Numri i referencës dhe data e Raportit të Menjëhershëm të Informacionit (IIR) të |
| 2 | Natyra e incidentit të raportuar në IIR |
| 3 | Numri i përditësimit dhe data e këtij raporti |
| **Informacione kontakti**: | |
| 1 | Emri i personit që raporton dhe nënshkruan raportin |
| | Funksioni |
| | Numrat e telefonit të kontaktit (të paktën dy) |
| | Adresa e email-it të personit raportues |
| 2 | Emri i personit alternativ raportues |
| | Funksioni |
| | Numrat e telefonit të kontaktit (të paktën dy) |
| | Adresa e email-it të personit raportues |
| 3 | Emri i personit që ka paraqitur raportin bazë |
| | Funksioni |
| | Numrat e telefonit të kontaktit (të paktën dy) |
| | Adresa e email-it të personit raportues |
| | (**Korrespondenca duhet t'i dërgohet personit që paraqet raportin dhe të kopjohet te kontaktet e tjera. Priten përgjigje të shpejta ndaj korrespondencës**.) |
| **Detajet e incidentit** | |
| 1 | Ashpërsia e incidentit (ju lutemi tregoni detajet e shkallëve të ndryshme të përdorura) |
| 2 | Përshkrim i detajuar i sulmit |
| 3 | Aplikacionet/rrjeti i prekur që përballen me klientët |
| 4 | Si u zbulua sulmi për herë të parë? |
| 5 | Kush e zbuloi sulmin i pari? |
| 6 | Çfarë veprimi të menjëhershëm u ndërmor për të ndaluar përhapjen ose ndikimin e sulmit? |
| 7 | Në çfarë niveli u përshkallëzua veprimi? |
| 8 | Emri i prodhuesit të harduerit, zhvilluesit të softuerit, marka/modeli, etj., të aplikacioneve të prekura, duke përfshirë atë të sistemeve/rrjeteve në të cilat funksionojnë aplikacionet |
| 9 | A u informuan shitësit e mësipërm dhe cili ishte reagimi i tyre? |
| 10 | Detajet e portave TCP ose UDP të përfshira në incident |
| 11 | Adresa IP e sistemit të prekur dhe sulmuesit, nëse është e disponueshme |
| 12 | Statusi i veprimit të ndërmarrë për të pastruar sistemin dhe për të zgjidhur problemet |
| 13 | Kur mund të pritet rifillimi normal i biznesit? |
| 14 | Çfarë rregullimesh janë bërë për një audit pasues? |
| 15 | Çfarë rregullimesh janë bërë për një audit hetues? |
| 16 | A është ruajtur zinxhiri i kujdestarisë? Kjo përfshin mbajtjen e një regjistri të detajuar që tregon se kush i ka mbledhur, trajtuar, transferuar ose analizuar provat që nga fillimi i hetimit. |

| | |
|---|---|
| 17 | Çfarë provash janë sekuestruar dhe mbajtur në ruajtje të sigurt për analizë dhe si prova hetuesie? Provat mund të përfshijnë servera, disqe të forta, CD-ROM, email-e, imazhe, dokumente, regjistra etj. |
| 18 | Çfarë mjetesh hetuesie u përdorën për të mbledhur prova? |
| 19 | Cilët vektorë ishin të përfshirë në sulm? Jepni detaje mbi pajisjet, aplikacionet etj., dhe gjërat që shkuan keq. |
| | **Pajisjet**: servera, routerë, pajisje ruajtjeje, IPS, firewall-e, VPN, Wi-Fi, direktori aktive, IDS, ISAM, mail, DHCP, DNS, pika fundore, pajisje të lëvizshme, cloud, SaaS, aplikacione të shitësve të palëve të treta, etj.<br><br>**Natyra e sulmit**: kompromentim i fjalëkalimeve, ndërhyrje njerëzore, (phishing), inxhinieri sociale, spam, mail malware, certifikata të vjedhura, cenueshmëri e pazbuluar, mohim shërbimi, sulm zero-day, sulm ransomware, vjedhje të dhënash, etj. |
| 20 | Adresat IP dhe emrat e domeneve tek të cilët mund të gjurmohet sulmi |
| 21 | Trafik i pazakontë, aktivitet i pazakontë nga vende ku zakonisht nuk kryhet biznes, kërkesa të pazakonta nga përdorues me privilegje dhe administratorë, numër i lartë përpjekjesh për hyrje, kërkesa të shumëfishta për të njëjtin skedar, vëllim i madh kërkesash për të dhëna, ndryshime të pazakonta në sistem, domene të pazakonta, cilësime të paautorizuara, ndryshime në konfigurime, etj. |