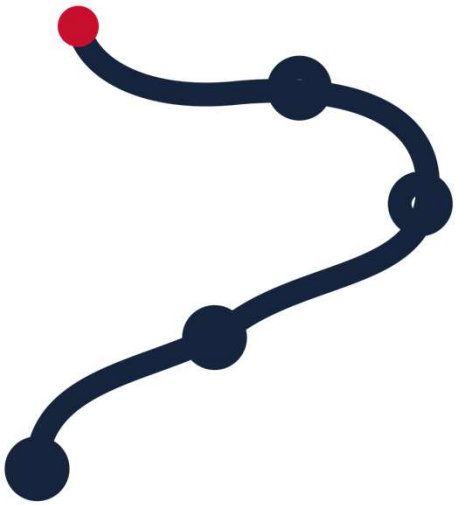
AUTORITETI I MBIKËQYRJES FINANCIARE

# Qëndrueshmëria Operacionale Dixhitale

Rregullorja DORA dhe Transpozimi i saj në Kuadrin Rregullator Shqiptar

**TIRANË**
**25.06.2026**

# Agjenda



1 **Konteksti evropian**
Integrimi në BE dhe Kapitulli 9 “Shërbimet financiare”

2 **Rregullorja DORA e BE-së**
Shtyllat e qëndrueshmërisë operacionale dixhitale

3 **Transpozimi në Shqipëri**
Rregullorja e AMF — struktura, parimet dhe afatet

4 **Fusha e zbatimit**
Subjektet e përfshira dhe parimi i proporcionalitetit

5 **Shtyllat e rregullores dhe Roli i drejtimit**
Përgjegjësitë e organit drejtues dhe detyrimet kryesore

6 **Mbikëqyrja dhe hapat e ardhshëm**
Si do ta verifikojë AMF zbatimin — dhe diskutimi

RREGULLORJA E BE-së

# Çfarë është DORA?

**Digital Operational Resilience Act · Rregullorja (BE) 2022/2554**

Rregullorja e Bashkimit Evropian për qëndrueshmërinë operacionale dixhitale të sektorit financiar: siguron që subjektet të parandalojnë, të përballojnë dhe të rikuperohen shpejt nga incidentet e teknologjisë së informacionit.

### NIVELI 1 · AKTI BAZË

Rregullorja DORA — kërkesat themelore për gjithë sektorin financiar.

### NIVELI 2 · INSTRUMENTET TEKNIKE

14 standarde teknike (RTS / ITS) — 4 prej tyre tashmë të transpozuara nga AMF.

## RRUGA KOHORE — NGA BE NË SHQIPËRI

# DORA — piketë mbyllëse e integrimit evropian

**Shqipëria po negocion anëtarësimin në BE**

Përafrimi i legjislacionit është motori kryesor i procesit.

**Kapitulli 9 — “Shërbimet financiare”**

**DORA është pjesë e acquis**

NEGOCIATAT E ANËTARËSIMIT → TRANSPOZIMI I ACQUIS → TREGU I PËRBASHKËT

*“Closing benchmark” kritik nën Kapitullin 9 — dëshmi konkrete e përafrimit me standardet më të larta të BE-së.*

KUADRI SHQIPTAR

# Transpozimi në Shqipëri — Rregullorja e AMF

**80**

nene — të bazuara plotësisht në DORA

**6**

krerë tematikë

**1 janar 2028**

hyrja në fuqi e detyrimeve

## KOMPETENCAT & SANKSIONET

Masat zbatuese dhe sanksionet plotësohen me ligj të përbashkët, i përgatitur së bashku me Bankën e Shqipërisë.

***Rregullorja vendos standardet — ligji garanton zbatueshmërinë!***

FUSHA E ZBATIMIT

# Kush përfshihet — dhe kush mbikëqyr

**DERI TANI**

**Kuadër rregullator i fragmentuar dhe i kufizuar** — pa një kuadër të integruar për qëndrueshmërinë operacionale digjitale.

## SUBJEKTET E LICENCUARA NGA AMF

- Shoqëritë e sigurimit dhe të risigurimit
- Sipërmarrjet e investimeve kolektive (SIK)
- Fondet e pensioneve private (FPP)
- Shoqëritë administruese
- Shoqëritë komisionere
- Ofruesit e shërbimeve të TIK

## TRE AUTORITETE ME ROLE PLOTËSUESE

### AMF

**SEKTORI FINANCIAR JOBANKAR**

Mbikëqyrje e drejtpërdrejtë; pranon raportet e incidenteve; mbikëqyr ofruesit kritikë të TIK.

### Banka e Shqipërisë

**SEKTORI BANKAR & NDËRSEKTORIAL**

Koordinim për ofruesit e përbashkët të TIK dhe incidentet që prekin disa sektorë.

### AKSK

**SIGURIA KIBERNETIKE KOMBËTARE**

Bashkëpunim për infrastrukturat kritike, CSIRT dhe shkëmbimin e inteligjencës.

# 2,5 miliardë USD

humbje direkte të raportuara në sektorin financiar global —që nga viti 2020

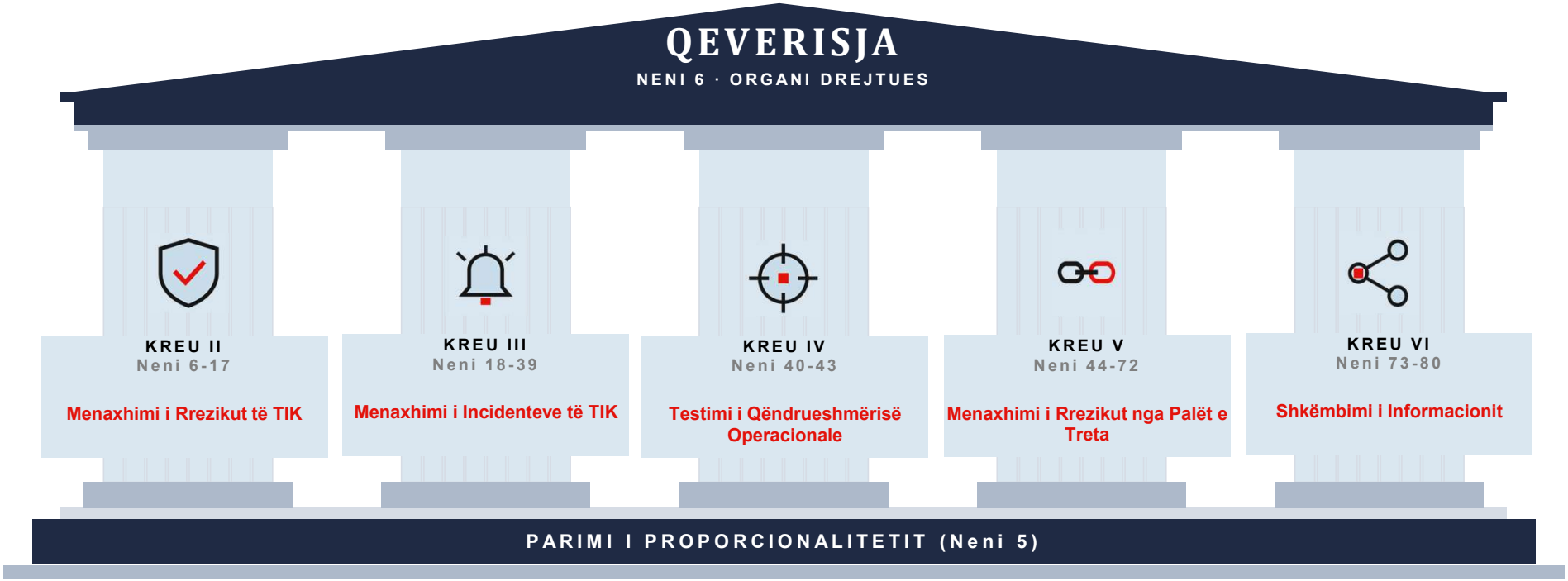
**1 në 5** sulme kibernetike në botë godet një institucion financiar.

## *Pyetja nuk është nëse, por kur?*

Burimi: FMN — Global Financial Stability Report, 2024

ARKITEKTURA E DORA-s

# Pesë shtyllat e DORA-s



MESAZHI KRYESOR PËR DREJTUESIT

# Përgjegjësia e organit drejtues

*“Rreziku i TIK nuk është çështje vetëm e IT-së — është përgjegjësi e drejtimit më të lartë.”*

### Përcakton dhe miraton

Strategjinë e qëndrueshmërisë dixhitale dhe kuadrin e rrezikut të TIK.

### Mbikëqyr zbatimin

Ndjek raportimet, incidentet madhore dhe planet e veprimit.

### Siguron burimet

Buxhet të dedikuar për sigurinë, testimin dhe kapacitetet njerëzore.

### Trajnohet vazhdimisht

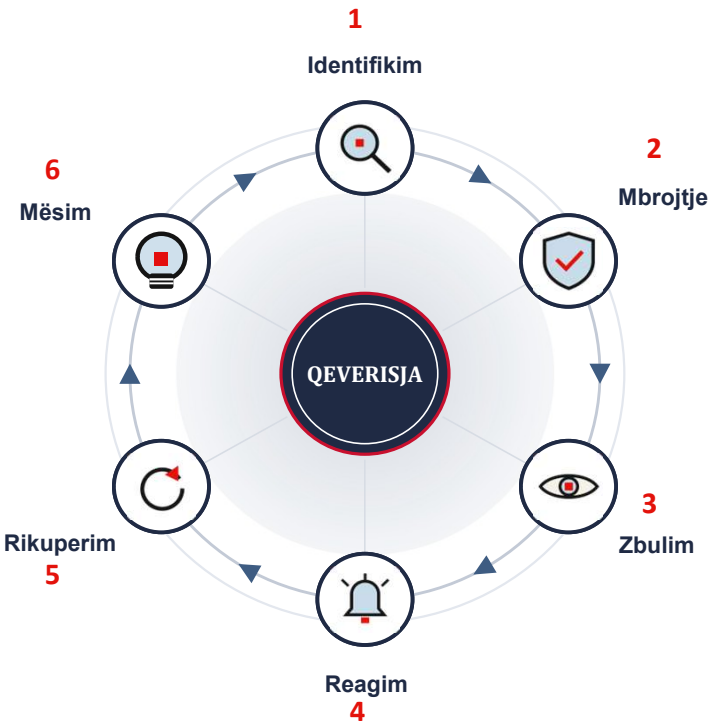
Njohuri të përditësuara për rrezikun e TIK dhe ndikimin e tij.

**NENI 6**

Rregullorja ia ngarkon shprehimisht organit drejtues **përgjegjësinë përfundimtare** për qëndrueshmërinë operacionale dixhitale.

# Menaxhimi i rrezikut të TIK

*Themeli i gjithë rregullores: kuadër i dokumentuar, proporcional — me përgjegjësi të qartë në nivel bordi*




## ÇFARË DUHET TË EKZISTOJË NË ÇDO SUBJEKT

- **Strategji e qëndrueshmërisë dixhitale** — e miratuar nga organi drejtues
- **Politika bazë të dokumentuara** — siguria e informacionit, asetet, aksesi, backup-i
- **Sisteme dhe mekanizma zbulimi** — Monitorim I vazhdueshem per te identifikuar anomalite dhe aktivitetet e dyshimta
- **Plane vazhdimësie dhe rikuperimi** — të testuara rregullisht — jo vetëm në letër
- **Funksion kontrolli i pavarur** — i ndarë nga IT operacionale; raporton te drejtimi

SHTYLLA 02 · KREU III

# Menaxhimi dhe raportimi i incidenteve

*Një gjuhë e përbashkët për incidentet — nga zbulimi te raportimi pranë AMF*

## 01 · MENAXHIMI

- Proces i dokumentuar: zbulim, regjistrim, trajtim
- Role dhe përgjegjësi të qarta komunikimi
- Pikë e vetme kontakti për incidentet e TIK

## 02 · KLASIFIKIMI

- Kritere të qarta materialiteti per klasifikimin
- klientët, transaksionet, shërbimet
- Kohëzgjatja, shtrirja dhe humbja e të dhënave

## 03 · RAPORTIMI

- Tri faza: fillestar → i ndërmjetëm → përfundimtar
- Incidentet madhore raportohen pranë AMF
- Formularë standardë dhe afate të përcaktuara

**Qëllimi nuk është ndëshkimi** — raportimi i shpejtë mbron klientët, subjektin dhe tregun.

SHTYLLA 03 · KREU IV

# Testimi i qëndrueshmërisë operacionale

*Siguria provohet — nuk supozohet: program vjetor, i bazuar në rrezik dhe proporcional*

## Teste bazë

për të gjitha subjektet

ÇDO VIT

- Pjesë e kuadrit të menaxhimit të rrezikut të TIK
- Testim i performancës dhe i skenarëve të ndërprerjes
- Trajtim sistematik i dobësive të gjetura
- Vlerësime të cenueshmërisë dhe teste sigurie

## TLPT — testim i avancuar

Threat-Led Penetration Testing

SUBJEKTE SISTEMIKE

- Simulon sulme të vërteta kibernetike — provë e qëndrueshmërisë reale
- Mbulon funksionet kritike, përfshirë palët e treta
- Testues të pavarur, të certifikuar dhe kompetentë
- 1 here ne 3 vjet

**Qëllimi:** dobësitë identifikohen dhe adresohen sistematikisht — përpara se t'i gjejë sulmuesi.

SHTYLLA 04 · KREU V

# Rreziku nga palët e treta të TIK

**Parimi bazë: përgjegjësia nuk delegohet.** Subjekti mbetet plotësisht përgjegjës edhe kur shërbimi blihet nga jashtë.

## REGJISTRI I KONTRATAVE

- Të gjitha marrëveshjet me ofrues TIK — në një regjistër të vetëm
- Ndarje: funksione kritike / të tjera
- Raportohet pranë AMF — çdo vit dhe me kërkesë

## KERKESA KONTRAKTUALE

- Nivele shërbimi të matshme (SLA)
- Vendndodhja dhe mbrojtja e të dhënave
- Te drejta e auditimit

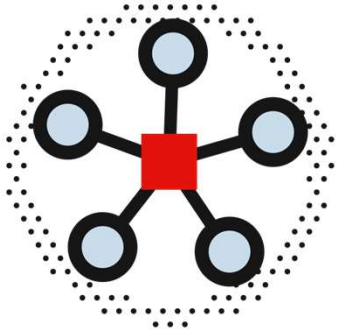
## MONITORIM I VAZHDUESHËM

- Vlerësim paraprak (due diligence) përpara lidhjes
- Vlerësim i rrezikut të përqendrimit
- Plane daljeje të hartuara — dhe të testuara

# Shkëmbimi i informacionit mbi kërcënimet

*Vullnetar — por i inkurajuar fuqishëm*

Rregullorja krijon bazën ligjore që subjektet financiare të shkëmbejnë mes tyre informacion mbi kërcënimet kibernetike, dobësitë dhe sulmet e vërejtura — në mjedis të besuar dhe pa cenuar konfidencialitetin.



## ÇFARË MUND TË SHKËMBEJNË SUBJEKTET

### Indikatorë kompromentimi

IOC nga sulme të zbuluara — adresa, skedarë, gjurmë

### Taktika dhe teknika

Mënyrat e veprimit të autorëve të kërcënimeve

### Inteligjencë kibernetike

Alarme, raporte dhe konteksti i kërcënimit

*Sulmuesi që prek një subjekt sot, mund të prekë gjithë sektorin nesër — **mbrojtja është kolektive.***

AFATET

# Koha për t'u përgatitur fillon tani

**16**

**MUAJ PËRGATITJE**

PERIUDHA PËRGATITORE

**Q2 2026**

Miratohet rregullorja e AMF

**1 janar 2028**

Rregullorja hyn plotësisht në fuqi

**Raportim 3-mujor i ecurisë pranë AMF**

*16 muaj duken shumë — por gap analysis, kontratat dhe testimi kërkojnë kohë. Subjektet që fillojnë sot, arrijnë rehat.*

KALENDARI

# Udhërrëfyesi deri më 1 janar 2028


## ÇFARË DUHET NGA TREGU— QË SOT

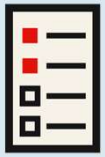
- Analizë e mangësive (gap analysis) ndaj kërkesave të reja
- Angazhim i bordit dhe mbështetje buxhetore
- Inventar i aseteve TIK dhe i kontratave me palë të treta
- Plan zbatimi 2-vjeçar — me afate dhe përgjegjësi të qarta

## ÇFARË DO TË BËJË AMF

- Udhëzues praktikë dhe formate standarde raportimi (RTS/ITS)
- Forcimi I Bashkëpunimit me AKSK dhe BSH
- Trajnime dhe takime sektoriale

MBIKËQYRJA

# Si do ta ndjekë AMF zbatimin



## Vetëvlerësim

Subjekti plotëson instrumentin standard të AMF-së.

ÇDO VIT

## Monitorim në distancë

Analizë e raporteve, regjistrave dhe incidenteve.

VAZHDIMISHT

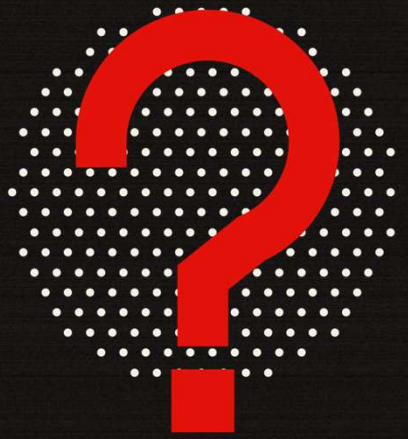
## Inspektim në vend

Verifikim teknik, intervista dhe test procedurash.

SIPAS RREZIKUT

MESAZHI PËRMBYLLËS

# Pyetja nuk është nëse
# Është kur
# Dhe përgatitja jonë fillon sot.



**PYETJE & DISKUTIM**

Konsultimi publik me tregun vijon gjatë vitit 2026.