BANCA NAȚIONALĂ A ROMÂNIEI

# *DORA – Regulamentul cu privire la reziliența operațională a sectorului financiar*

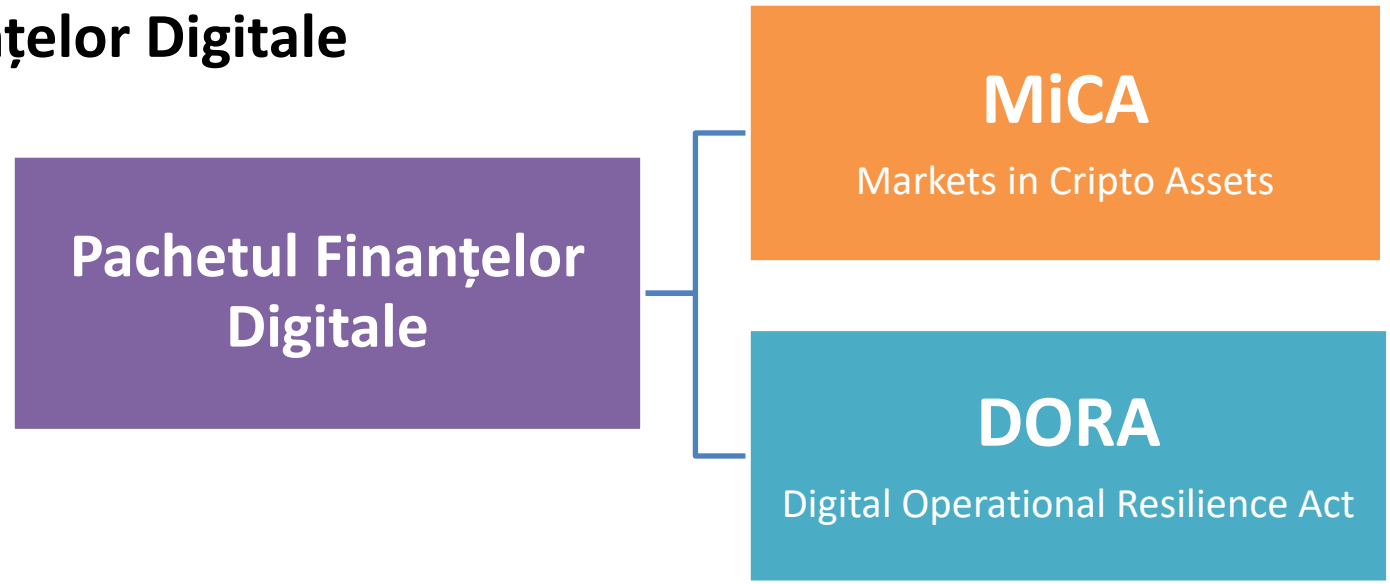
*Claudiu Negrea – Director adjunct,*

*Direcția monitorizare a infrastructurilor pieței financiare și a plăților*

*Mai 2024*

# Context

- Progresul tehnologic, tehnologii utilizate transversal în sectorul financiar și dependența sectorului de tehnologie;
- Septembrie 2020 – Comisia Europeană publică **Strategia Finanțelor Digitale**



# Etape

- ✓ **9 noiembrie 2022** – DORA a fost votată în Parlamentul European;
- ✓ **14 decembrie 2022** – a fost adoptată *Directiva (UE) 2022/2556 privind reziliența operațională digitală pentru sectorul financiar,* care stipulează modificări asupra altor reglementări sectoriale, pentru a le permite să fie în vigoare simultan;
- ✓ **16 ianuarie 2023** – DORA a intrat în vigoare, sub *Regulamentul (UE) 2022/2554;*
- ➢ **17 ianuarie 2025** – Regulamentul DORA va deveni aplicabil.

# DORA – bazată pe cerințe din reglementări existente

| Building block | Main elements of the buiding block | EU financial services Level 1 and Level 2 legislation | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Payments (PSD2) | Banks (CRD/CRR) | Investment firms (MIFID) | Trading Venues (MIFID) | CCPs (EMIR) | CSDs (CSDR) | Trade Repositories (EMIR) | Insurance (SolvencyII) | Asset Management (UCITS/AIFMD) | CRAs | Data Reporting Service Providers (DRSPs) | Audit | IORPs |
| ICT risk management | Arrangmenents (policies, procedures and systems) on risks to which the entity is exposed to | | art. 74(1) | art. 16(4), (5) | art. 47 (1) | art. 26(1) | L2 - art. 68(1) | Art 79 | | L2 - art. 40(1) - both art. 15(2) - A | Annex I - Section A, (4) | | | art. 28(3) |
| | Operational risk framework / policy | art. 95(1) | | | | Art. 28 (risk committee) | L2 - art. 70(1) | | | L2 - art. 13(1) - A | | | | |
| | Risk management policy | | | L2 - art. 23(1) | | L2 art.4 | | | art. 41(3) | L2 - art. 38(1) - U | | | | art. 25(1) |
| | Information security framework/strategy | art. 95(1) | | L2 - art. 18 (AT) | | L2 - art. 9(3) | L2 - art. 70(9), art. 75(6) | | | | | | | |
| | Appropriate IT tools, reliable, resilient and secure systems (to ensure security / integrity / confidentiality) | art. 95(1), art. 97(3) L2 - chapter II,IV,V | | art. 16(5) L2 - art. 21(2) | art. 48(1) L2 - art. 23(1),(2) | art. 26(6) and L2 art.9 | art. 45(1) L2 - art. 75 | L2 - art. 79(1) | L2 - art. 259(1) | L2 - art. 57(2) - A | | art. 64(4), 65(5), 66(3) + L2 - art. 9(1) | | |
| | Business continuity policy | | art. 85(2) | art. 17 (1) and L2 - art. 14(1) - (AT) L2 - art. 21(3) | art. 48(1) | art. 34(1) L2 - art. 17 | L2 - art. 76(1) | art. 79(2) | L2 - art. 259(3) | L2 - art. 57(3) - A | L2 - art. 11(2) | | art. 24a 1(h) | art. 21(5) |
| | Contingency plans | | art. 85(2) | | art. 47(1) | part of BCP as referred to in art. 34 | | | art. 41(4) | | | | | art. 21(5) |
| | Crisis management and communications | | | | | L2 - art. 22 | L2 - art. 78(4) | | | | | | | |
| | Disaster recovery plan | | | | | art. 34(1) L2 - art. 19 | L2 - art. 76(1), art. 78 | art. 79(2) | | | | | | |
| | 2h RTO | | | | L2 - art. 15(2) | L2 - art. 17(6) | L2 - art. 78(2) | | | | | | | |
| Incident reporting | Reporting of operational incidents to CAs | art. 96(1) | | | L2 - art. 23(3) L2 - art. 81(1) | | art. 45(6) L2 - art. 43(h) | | | | | | | |
| | Procedures to record, monitor and resolve operational incidents | | | | | | L2 - art. 71(4) | | | | | | art. 24a 1(i) | |
| | Breaches in physical and electronic security measures | art. 96(1) | | L2 - art. 18(3) (AT) | | | | | | | | L2 - art. 9(4) | | |
| Testing | Testing of IT tools, systems and procedures | L2 - art. 3(1) | | | | partly relevant by general provisions art. 49 | art. 45(5) L2 - art. 75(6) | | | | | | | |
| | Penetration testing | | | L2 - art. 18(4) (AT) | | | | | | | | | | |
| Third party risk | Outsourcing - the entity remains fully responsible | art. 19(6) art. 20(2) | | L2 - art. 4(1) (AT) L2 - art. 31(1) | L2 - art. 6(1) | art. 35(1) | art. 30(1) | | art. 49(1) | | | L2 - art. 6(4) | | art. 31(2) |
| | Outsourcing is governed by a written agreement | | | L2 - art. 31(3) | L2 - art. 6(4) | | art. 30(2) | L2 - art.16 | | | L2 - art. 25 | | | art. 31(5) |
| | Outsourcing - report to CAs on the outsourcing | art. 19(6) | | | L2 - art. 6(5), (7) | art. 35 approval by CA required | | | art. 49(3) | art. 20(1) - A | | | | art. 31(6) |
| | Identify critical service providers (CSPs) and manage dependencies | | | | | L2 - art. 18(3) | L2 - art. 68(1), (2) | | | | | | | |
| | Inform CAs on dependencies with CSPs | | | | | | L2 - art. 68(5) | | | | | L2 - art. 6(6) | | |
| | Robust arrangements for the selection and substitution of IT third party service providers | | | | | | L2 - art. 79(9) | | | | | | | |
| | Due diligence when outsourcing to third party service providers | | | L2 - art. 31(2) | | | | | | | | | | |
| | Outsourcing to third party service providers located in a third country | | | L2 - art. 32 | | | | | | | | | | |

# Scop

- Instituțiile financiare în scopul DORA, sub atribuțiile BNR:
  - instituțiile de credit (IC),
  - instituțiile de plată (IP),
  - furnizorii de servicii de informare cu privire la conturi (FSIC),
  - instituțiile de monedă electronică (IEME),
  - depozitarii centrali de titluri de valoare,
  - contrapărțile centrale,
  - sisteme de plăți (vor fi incluse la nivel național);
- Cerințele din Reg. DORA se aplică după **principiul proporționalității,** microîntreprinderile sunt exceptate de la unele cerințe.

# Ce aduce nou DORA

- Armonizarea cerințelor transversal-sectoriale – cerințele sunt aplicabile la peste 20 de tipuri de entități financiare;
- Crearea unui cadru comun de supraveghere a rezilienței operaționale la nivel european;
- Supravegherea centralizată la nivel european a **furnizorilor terți esențiali de servicii TIC;**
- Impunerea testelelor de tip **TLPT** ca fiind obligatorii la nivelul entități financiare mari;
- Statut de *lex specialis* față de directiva NIS 2.

# Cei patru piloni DORA

Gestionarea **riscurilor TIC**

Gestionarea, clasificarea și raportarea **incidentelor legate de TIC**

**Testarea** rezilienței operaționale digitale

Gestionarea riscurilor TIC generate de **părți terțe**

# I. Gestionarea riscurilor TIC

- În prezent, cerințele aplicate prestatorilor de servicii de plată (IC, IP, FSIC, IEME) sunt definite în cadrul actual de reglementare al ***Regulamentului 2/2020*** (cadrul ***Legii 209/2019 privind serviciile de plată***) – bazat pe *EBA Guidelines on ICT and security risk management* și sunt monitorizate de BNR;
- Cerințele din DORA se ghidează după principii similare, dar au o complexitate mai ridicată și pun accentul pe **asigurarea rezilienței operaționale.**


RTS-uri publicate:

- RTS cu privire la cadrul de gestionare a riscurilor;
- RTS cu privire la cadrul de gestionare a riscurilor **simplificat.**

# I. Gestionarea riscurilor TIC

*Diferențe față de cerințele actuale*

- Responsabilități specifice definite explicit pentru **organul de conducere;**
- **Strategia privind reziliența operațională digitală** (față de Regulamentul 2/2020 unde se stabilește necesitatea de a avea o strategie TIC);
- Necesitatea de a avea sisteme, protocoale și instrumente TIC **reziliente** pentru gestionarea riscurilor TIC, accentul fiind pus pe capacitatea acestora de a permite entităților să își desfășoare activitatea și să furnizeze serviciile în timp util în situații de stres sau de criză;
- Accent pe **dependențele de furnizorii terți** în cadrul identificării și clasificării funcțiilor, rolurilor și responsabilităților;
- Infrastructura de conectare a rețelei într-un mod care permite întreruperea sau segmentarea instantanee a acesteia, pentru a reduce la minimum și a **preveni contagiunea**, în special în cazul proceselor financiare interconectate;

# II. Incidentele legate de TIC

**Gestionarea și clasificarea incidentelor TIC**

**Raportarea incidentelor majore TIC**

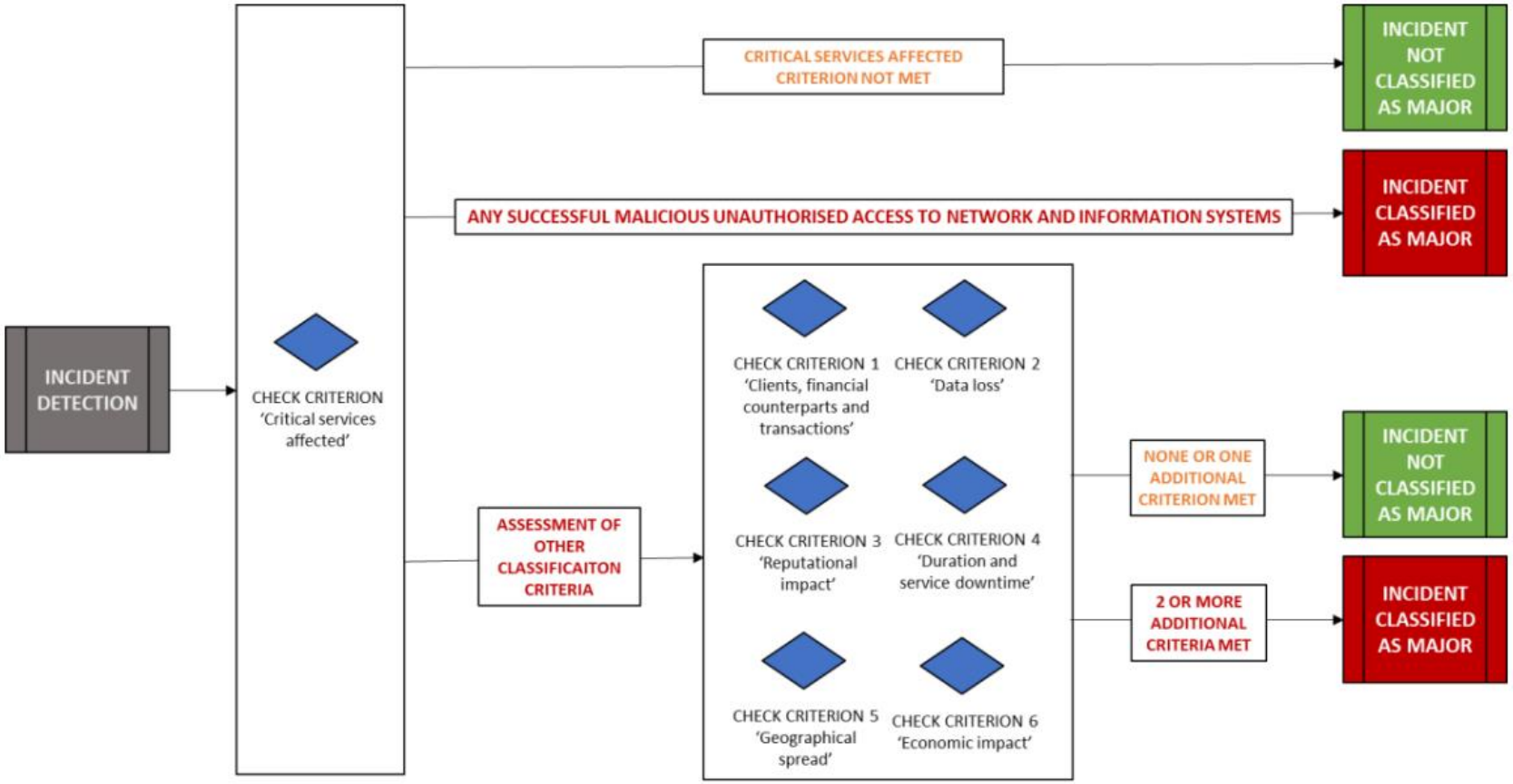
- **Cadrul actual** de gestionare și raportare a incidentelor TIC și de securitate majore legate de plăți – definit în prezent de *Regulamentul 2/2020*, **va fi adaptat și inclus în raportarea DORA;**
- **BNR** este **punctul central** de raportare a incidentelor majore;

Reglementări și standarde:

- RTS cu privire la **criteriile de clasificare** a incidentelor TIC *15 ianuarie 2024;*
- RTS pentru **specificarea raportării** incidentelor majore TIC *17 iulie 2024;*
- ITS pentru stabilirea **detaliilor de raportare** a incidentelor majore TIC *17 iulie 2024;*
- Ghiduri pentru estimarea **costurilor/pierderilor agregate** cauzate de incidente majore TIC *17 iulie 2024;*
- Raport de fezabilitate pentru stabilirea unui singur HUB european pentru evenimente majore TIC *17 ian. 2025.*
- Recomandări ESRB *17 iulie 2024*, *iulie 2025.*

# II. Incidentele legate de TIC

## *Clasificarea incidentelor majore*




*Sursa: Final report on draft RTS specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under DORA.*

# II. Incidentele legate de TIC

## *Raportarea incidentelor majore către BNR*

- Raportarea incidentelor majore în DORA este definită în mod similar raportării actuale a incidentelor majore cu privire la plăți;
- **Trei notificări**: raportul inițial, raportul intermediar și raportul final - termenele de raportare și conținutul rapoartelor urmează să fie stabilite în cadrul unor **RTS** dedicate;
- Obligația raportării poate fi externalizată, în conformitate cu legislația sectorială a Uniunii și cu cea națională, către un furnizor terț de servicii, dar **entitatea financiară rămâne pe deplin responsabilă** de îndeplinirea cerințelor legate de raportare a incidentului.

# III. Testarea rezilienței operaționale digitale

## Testare de bază

- examinări ale vulnerabilităților
- teste, analize, verificări de securitate;
- teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste end-to-end sau teste de penetrare.

Reglementări și standarde:

- RTS cu privire la aspecte legate de TLPT

## Testarea avansată

- cadru axat pe **TLPT** – Threat-led Penetration Testing;
- bazat pe cadrul TIBER-EU, transpus in România prin *Regulamentul nr. 6/2022 privind cadrul de desfășurare a testelor de rezilienţă cibernetică* TIBER-RO;
- obligatorii pentru entitățile financiare identificate de BNR (**instituții de credit sistemice, IPF-uri etc.**).

# III. Testarea rezilienței operaționale digitale

## *Testarea de bază*

- abordare bazată pe riscuri;
- frecvență cel puțin anuală;
- echipe de testare interne sau externe;
- testarea tuturor **sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante;**
- Tipuri de teste:
  - **examinări ale vulnerabilităților;**
  - teste, analize, verificări de securitate;
  - teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste end-to-end, **teste de penetrare;**
  - evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end) sau teste de penetrare.

# III. Testarea rezilienței operaționale digitale

## *Testarea avansată - Threat-Led Penetration Testing*

Conform DORA:

- Art. 26 alin.(1), instituțiile financiare desemnate vor efectua, **cel puțin o dată la 3 ani**, teste de penetrare bazate pe amenințări (Threat-Led Penetration Testing - TLPT) în condiții asemănătoare testelor de tip TIBER.
- Art. 26 alin. (2) autoritățile europene de supraveghere au elaborat, în acord cu BCE, proiecte comune de standarde tehnice de reglementare în conformitate cu cadrul TIBER–EU pentru a aduce precizări suplimentare. Acestea urmează a fi publicate la data de 17 iulie 2024.
- cadrul TIBER-EU este transpus in România prin ***Regulamentul nr. 6/2022 privind cadrul de desfășurare a testelor de reziliență cibernetică*** TIBER-RO.

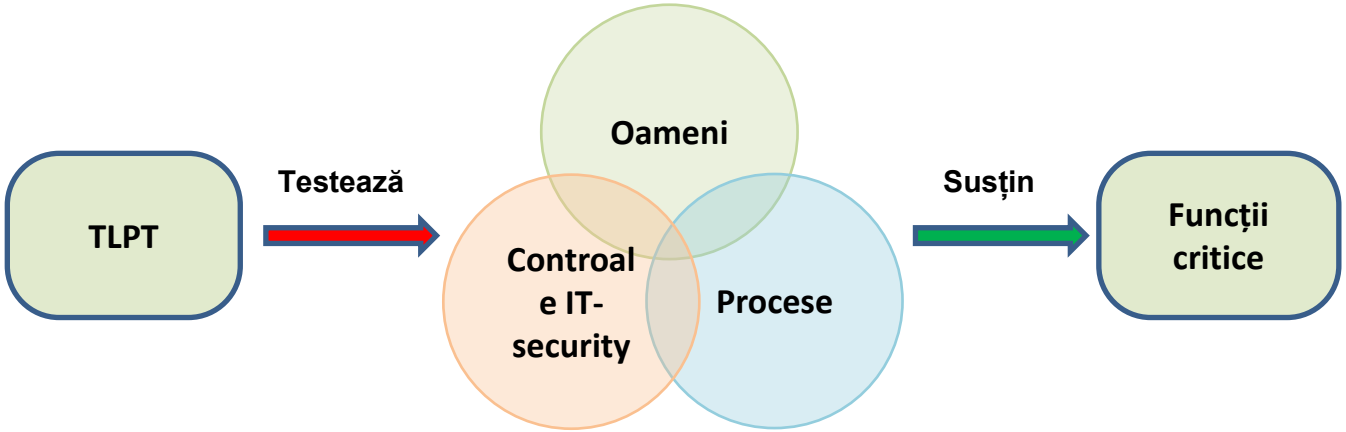
Reglementări și standarde:

- RTS cu privire la aspecte legate de TLPT

# Entități care vor efectua teste TLPT

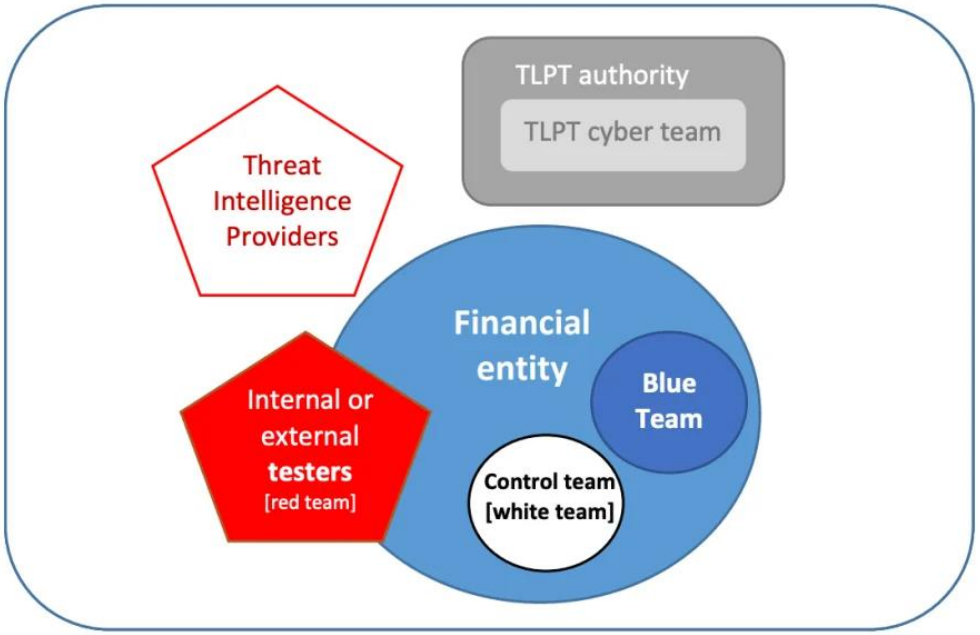
- Bănci G-SII (sistemice global) și O-SII ( alte instituții importante sistemic);
- Depozitari centrali;
- CCP-urile;
- Bursele;
- Asiguratori cu o cota de piață >10%;
- Sistemele de plăți (incluse la nivel național);
- Alte entități financiare cu potențial impact sistemic, sau de risc ICT, pe baza analizei autorității TLPT (BNR).

# Threat-led Penetration Testing (TLPT)




TLPT vizează funcțiile importante și critice ale entității testate!

# Participanți la TLPT




- Furnizorii de **Threat Intelligence** trebuie să fie externi;
- DORA permite utilizarea testerilor interni pentru **red team;**
- Entitățile financiare care au utilizat testerilor RT interni, trebuie să se asigure că **la fiecare trei teste** contractează **testeri RT externi;**

# TLPT– echipe implicate

| TLPT Cyber Team (TCT) | Echipa de control (White team) Entitatea testată (ET) | Furnizor TI (Threat Intelligence ) | Furnizor RT (Red Team ) | Echipa albastră (Blue Team) Entitatea testată |
|---|---|---|---|---|
|  |  |  |  |  |
| Coordonează, monitorizează și atestă desfășurarea testului. | Gestionează desfășurarea testului. | Furnizează servicii de informații de tip TI specifice ET. | Furnizează servicii de testare cibernetică. | Echipa de apărare din cadrul entității testate. |

**Echipa de reconstituire a testului (Purple Team)**

Formată din reprezentanți ai RT și BT.
Pot participa reprezentanți ai WT, TI și TCT.

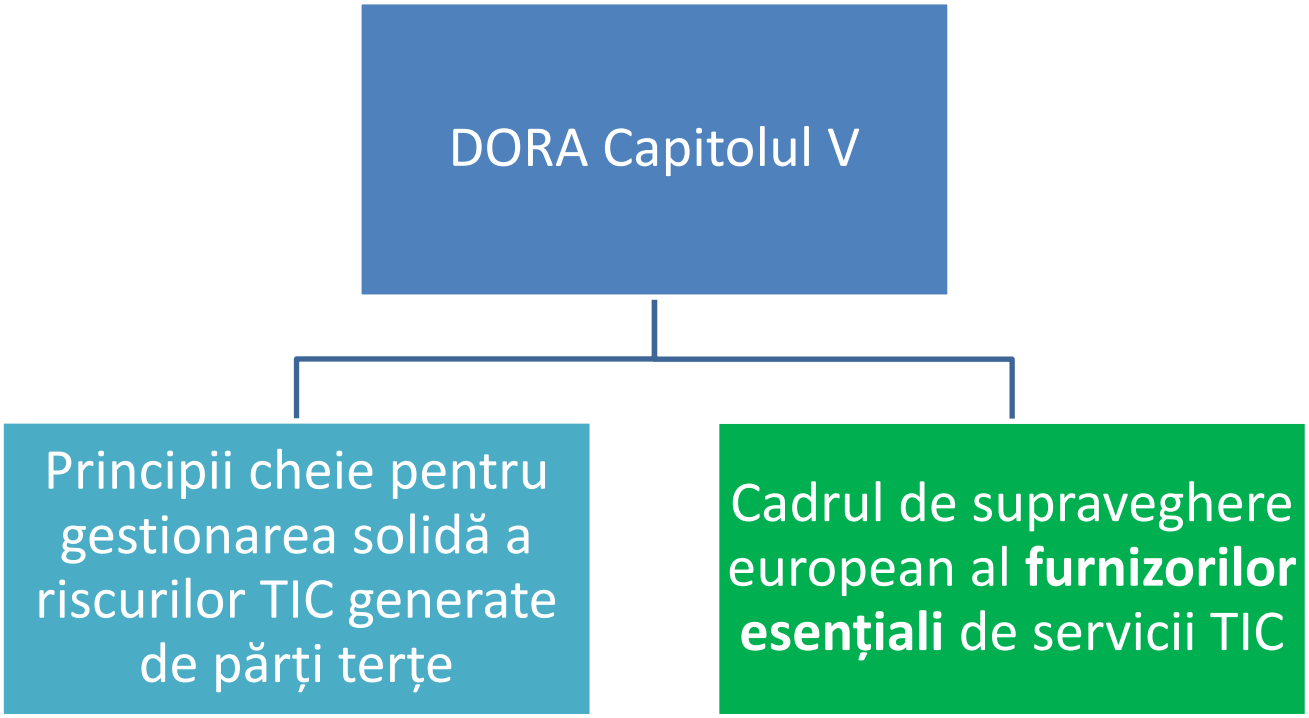
# Faze TLPT


Notification to perform a TLPT
•To the financial entity selected by TLPT authority
Preparation phase [6m]
•Within 3m Initiation documents, control team
•Within 6m scope specification documents
Testing phase
•Targeted threat intelligence report
•Red team test plan
•Active red team testing [≥ 12 weeks]
Closure phase [4m]
•Red team test report
•Blue team test report
•Test summary
•Exchange of feedback
•Remediation plans
End of TLPT
•TLPT authority delivers attestation to financial entity

# Implementare DORA TLPT la nivel național

- Este în curs de elaborare un **proiect de lege** pentru implementarea DORA;
- Prin acest proiect de lege, BNR va fi desemnată ca autoritate competentă pentru coordonarea și certificarea exercițiilor TLPT în RO;
- Proiectul de lege va include și criteriile naționale de desemnare a entităților în scopul TLPT;
- *Reg. BNR nr. 6/2022* va continua să fie aplicabil integral pentru sisteme de plăți și va fi adaptat, după finalizarea RTS TLPT DORA, pentru a nu dubla prevederile RTS în cazul altor entități financiare;
- Va avea loc periodic un proces de desemnare, sub art. 26 DORA, a entităților care vor trebui să efectueze teste TLPT;
- Testele TIBER, efectuate conform Reg. BNR nr. 6/2022, **rămân valabile și vor fi echivalate testelor TLPT,** după intrarea în vigoare a DORA;
- Furnizorii de servicii de testare, **începând cu 2025**, vor avea de acoperit toate statele membre și toate entitățile financiare în scopul DORA TLPT.

# IV. Gestionarea riscurilor TIC generate de părți terțe



# IV. Gestionarea riscurilor TIC generate de părți terțe

*Principii cheie pentru gestionarea solidă a riscurilor TIC generate de părți terțe – Cadru actual*

**În prezent**, în cazul externalizărilor notificate de prestatorii de servicii de plată, la nivelul BNR:

- sunt evaluate cerințele prudențiale definite în *EBA Guidelines on outsourcing arrangements;*
- sunt evaluate cerințele specifice privind măsurile de securitate referitoare la riscurile operaţionale şi de securitate aferente serviciilor de plată definite în *Regulamenul nr. 2/2020;*

# IV. Gestionarea riscurilor TIC generate de părți terțe

*Principii cheie pentru gestionarea solidă a riscurilor TIC generate de părți terțe – Cerințe DORA*

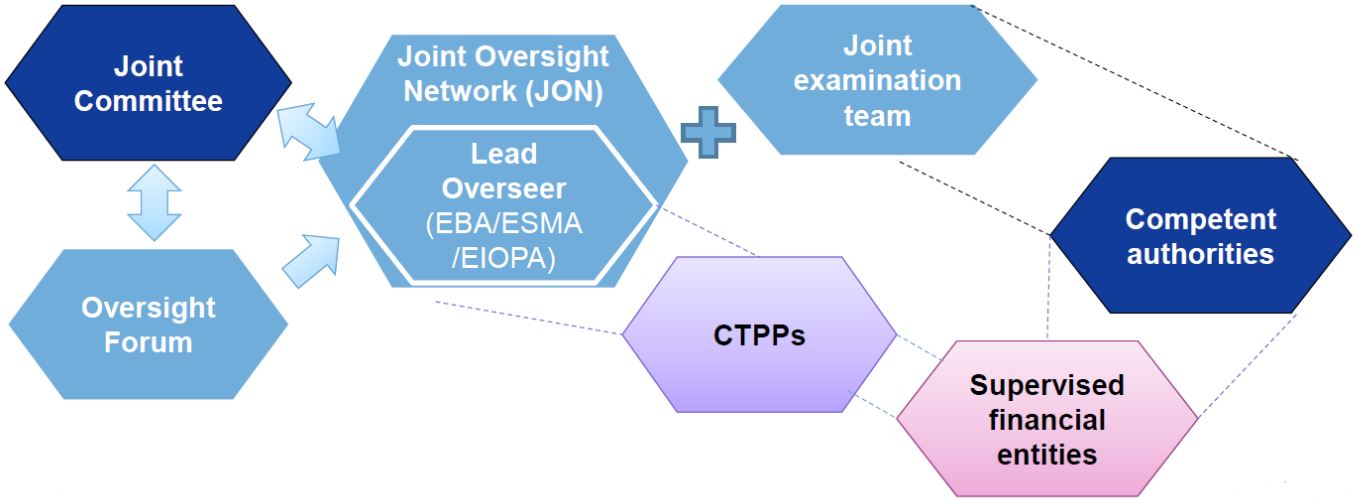
- Instituțiile financiare rămân complet responsabile pentru conformarea la obligațiile legale;
- Obligația de a avea o strategie și o politică cu privire la riscul TIC generat de părți terțe;
- Obligația de a avea un **Registru de informații** cu privire la furnizorii terți TIC;
- Riscurile generate de părți terțe trebuie incluse în evaluarea riscurilor, inclusiv **riscul de concentrare;**
- Evaluarea **lanțului de subcontractare**, acolo unde este cazul;
- Cerințe minime cu privire la **acordurile contractuale privind utilizarea serviciilor TIC**
- Dreptul autorității competente de a efectua **inspecții la sediile furnizorilor terți;**

Reglementări și standarde:

- RTS cu privire la politica serviciilor TIC *15 ianuarie 2024;*
- RTS cu privire la elemente legate de **subcontractarea** funcțiilor critice sau importante *17 iul. 2024;*

# IV. Gestionarea riscurilor TIC generate de părți terțe

*Cadrul de supraveghere european al **furnizorilor esențiali de servicii TIC***




Sursa: www.oenb.at

Reglementări și standarde:

- ITS pentru stabilirea șabloanelor pentru Registrul Informațiilor *15 ianuarie 2024;*
- Ghiduri cu privire la cooperarea între ESA-uri și autoritățile competente cu privire la structura cadrului de monitorizare *17 iulie 2024;*
- RTS pentru specificarea informațiilor cu privire la conduita de monitorizare *17 iulie 2024;*
- Call for advice cu privire la criteriile nivelului critic *15 iunie 2023;*
- Call for advice cu privire la taxele de supraveghere *15 iunie 2023;*

# Pregătiri și provocări viitoare

- Evaluarea nivelului de maturitate al entității față de cerințele DORA;
- Modificarea procedurilor interne prin adaptarea acestora la cerințele DORA și la noile standarde tehnice publicate;
- Asigurarea personalului și expertizei necesare, în contextul în care cadrul aduce unele cerințe noi și unele cu o complexitate mai ridicată;
- Necesitatea unor instrumente de evaluare și monitorizare a furnizorilor terți;

# Atribuțiile BNR în contextul DORA

În baza atribuțiilor statutare, BNR va fi responsabilă de:

- Evaluarea nivelului de maturitate a rezilienței operaționale, inclusiv a rezilienței cibernetice;
- Punctul central pentru raportarea incidentelor majore;
- Coordonarea testelor TLPT, bazate pe cadrul TIBER-RO;
- Monitorizarea furnizorilor terți TIC;
- Implicarea în activitatea de supraveghere a furnizorilor terți esențiali de servicii TIC, coordonată la nivel European.

# Mulțumesc!


Claudiu Negrea, email: claudiu.negrea@bnro.ro, tel. 031.132.3702

Director adjunct

Direcția monitorizare a infrastructurilor pieței financiare și a plăților