DORA – un rol esențial în asigurarea maturității entităților financiare în cadrul ecosistemului digital

Lect.univ.dr.ing.ec. Călin Rangu

Digital Operational Resilience Act Trained Professional (DORATPro)™

Certificate Number: 364890

De ce DORA determină necesitatea creșterii maturității digitale?

- DORA trece reziliența digitală **din ‘best practice’ în ‘licență de operare’**
- Este necesară **o maturitate demonstrabilă**
- **Factori principali**: presiunea **reglementării/supravegherii** și impactul **dependenței de furnizori**
- **DORA ca limbaj comun între risc, business, IT și achiziții**
- **Trebuie gestionată complexitatea ecosistemului: bancă ↔ fintech ↔ procesatori plăți ↔ cloud ↔ telecom ↔ furnizori.**

5 piloni de reziliență

1. **Managementul riscului ICT** – guvernanță, clasificare funcții critice/însemnate, BIA, toleranțe la întrerupere.
2. **Gestionare și raportare incidente ICT** – clasificare, SLA de raportare, lecții învățate.
3. **Testarea rezilienței** – exerciții periodice, purple teaming, TLPT pentru entitățile țintite.
4. **Risc terți ICT** – registru, clauze contractuale, sub-furnizori, exit & portabilitate, risc de concentrare.
5. **Schimb de informații** – cadre de partajare, protecția confidențialității.

- **Accent pe „artefacte doveditoare” (procese, controale, registre, rapoarte, minute, evidențe de test/exerciții).**

Ce e diferit față de „compliance as usual”

- **Trecerea de la check-list la rezultate măsurabile** (MTTD/MTTR, toleranțe, rate de succes ale recuperării).
- **Risc de concentrare la nivel de ecosistem** (nu doar la nivel de furnizor).
- **Timpi stricți pentru notificarea incidentelor majore (**necesită playbook operațional, nu doar politici).

- **Se trece de la contractul standard la contractul DORA-ready specific furnizorului si funcției CIF externalizate.**

Model de maturitate (5 niveluri) și de ce DORA accelerează creșterea

1 – Inițial: ad-hoc, politicile nu sunt implementate, evidențe lipsă

2 – Gestionat: procese de bază, BIA inițiale, roluri definite

3 – Standardizat: metodologii și acoperire 100% pe funcții critice/importante, toleranțe aprobate

4 – Măsurat: KPI/SLO (MTTD/MTTR), dashboard, corecții pe date

5 – Optimizat: simulări, concentrare, portabilitate și îmbunătățire continuă

1) Managementul riscului ICT

Lvl 1 – Inițial: politici fragmentare, fără BIA complet; toleranțe la întrerupere nedefinite; responsabilități neclare.

- *Evidențe lipsă/insuficiente:* nu există inventar servicii critice, nu există aprobare toleranțe.

Lvl 2 – Gestionat: BIA inițiale pe servicii principale; proprietari de servicii numiți; matrice riscuri ICT de bază.

- *Evidențe:* BIA v0, risk register, minute comitete.

Lvl 3 – Standardizat: BIA 100% pe servicii critice; toleranțe aprobate; metodologie standard pentru evaluarea riscurilor ICT.

- ***Evidențe:*** **politică aprobată, metodologie, trasabilitate risc→control.**

Lvl 4 – Măsurat: risc agregat pe servicii & procese; apetit la risc tradus în SLO/KPI (ex. MTTD/MTTR); trenduri & praguri de alertă.

- *Evidențe:* dashboard recurent, semnalizări depășire, acțiuni corective.

Lvl 5 – Optimizat: ajustare continuă a toleranțelor pe baza datelor; simulări „what-if” și analiză de concentrare.

- ***Evidențe:*** **rapoarte scenarii, decizii de investiții bazate pe risc.**

2) Incidente ICT și raportare

Lvl 1: răspuns ad-hoc; clasificare neuniformă; post-mortem ocazional.

Lvl 2: procedură de bază; timpi orientativi; șablon raport post-incident.

Lvl 3: clasificare standard; SLA de notificare; lecții învățate obligatorii.

Lvl 4: MTTD/MTTR măsurate și țintite; runbook-uri; simulări periodice (table-top).

Lvl 5: orchetrare și automatizare; integrare cu comunicarea clienților; raportare BNR/ASF pregătită si transmisă la o atingere.

3) Testarea rezilienței

Lvl 1: teste ocazionale, neplanificate.

Lvl 2: plan anual minim (backup/restore, DR parțial).

Lvl 3: program de testare pe toate funcțiile critice; criterii clare de trecere; acoperire 100% anual.

Lvl 4: testare bazată pe risc și scenarii; purple teaming; evidențe centralizate.

Lvl 5: optimizare continuă; chaos/chaos-engineering controlat pe componente critice; pregătire și execuție TLPT.

4) Risc terți ICT și concentrare

Lvl 1: registru incomplet; clauze contractuale generice; vizibilitate redusă la sub-furnizori.

Lvl 2: registru de bază; clauze parțiale (notificare incident, suport audit).

Lvl 3: registru complet + lanț subcontractori; clauze DORA-ready; planuri de exit documentate.

Lvl 4: monitorizare performanță/incident; scor de concentrare pe servicii critice; teste de exit periodice.

Lvl 5: strategii de portabilitate/multi-sursă; acorduri pre-negociate pentru migrare accelerată; early-warning pe furnizori.

5) Schimb de informații

Lvl 1: reactiv; fără canale formale.

Lvl 2: participare inițială la grupuri; proces de triere a informațiilor.

Lvl 3: integrare în playbook incidente; partajare controlată (legal/compliance).

Lvl 4: feed-uri curate în SOC/IR; indicatori utilizați în prevenție.

Lvl 5: contribuții regulate; colaborări bilaterale cu furnizori/sector.

Ținte de KPI per nivel (exemple orientative)

- **MTTD servicii critice**: L2 ≤ 15 min · L3 ≤ 10 min · L4 ≤ 5 min · L5 ≤ 2 min.
- **MTTR plăți/carduri** (P95): L2 ≤ 360 min · L3 ≤ 240 min · L4 ≤ 180 min · L5 ≤ 90 min.
- **Acoperire BIA** pe critice: L2 ≥ 60% · L3 = 100% · L4 evidențe la zi · L5 ajustare dinamică.
- **Contracte cu clauze DORA-ready** (furnizori critici): L2 ≥ 40% · L3 ≥ 70% · L4 ≥ 90% · L5 = 100% + teste de exit.
- **Acoperire testare funcții critice/an**: L2 ≥ 50% · L3 = 100% · L4 = 100% bazat pe risc · L5 + exerciții de degradare controlată.

Scoring & Heatmap pentru Board

- **Scor 1–5 per pilon, media ponderată → scor total.**
- **Ponderi recomandate (ajustabile): Risc ICT 25%, Terți 25%, Incidente 20%, Testare 20%, Schimb info 10%.**
- **Regulă de trecere: niciun pilon < 3 pe servicii critice; obiectiv strategic: ≥4 pe plăți/carduri.**
- **Evidențe obligatorii: pentru fiecare scor, anexează link la document/raport/ extras de sistem (nu doar declarații).**
- **Livrabil: heatmap trimestrial (R/G/A) + radar 5 axe cu scorurile curente vs țintă.**

Praguri (pentru Board)

- MTTD: Verde ≤ 5 min · Galben ≤ 10 min · Roșu > 10 min.
- MTTR (Plăți/Carduri): Verde ≤ 60/180 · Galben ≤ 90/240 · Roșu > 90/240.
- BIA critice <12m: Verde = 100% · Galben 90–99% · Roșu < 90%.
- Contracte DORA-ready (critici): Verde ≥ 90% · Galben 70–89% · Roșu < 70%.
- Acoperire testare/an (critice): Verde = 100% · Galben 70–99% · Roșu < 70%.
- Teste de exit (12m): Verde ≥ 2/an (total portofoliu) · Galben = 1 · Roșu = 0.

De ce DORA determină creșterea maturității

- De la politică la dovadă: artefacte, trasabilitate, registre, rapoarte
- Ferestre stricte de raportare → playbook și antrenament real
- Ecosistem și lanț de furnizori: risc de concentrare și exit
- Testare bazată pe risc + (unde e cazul) TLPT
- Guvernanță la nivel de Board: SLO/KPI & finanțare ghidată de gap-uri

Mini-caz: carduri + SEPA Instant

- Incident: cădere procesator carduri + latențe SEPA Inst
- Clasificare: % tranzacții respinse, durată estimată, impact, media
- Notificare: inițială ≤4h/≤24h de la detecție, intermediar ≤72h, final ≤1 lună
- Fallback: autorizare offline cu plafoane, rerutare, DR
- Lecții: reguli antifraudă în mod offline, SLA/contracte, loguri/audit, plan de substituție

Plan 0–90 zile (bancă)

- Inventar & clasificare funcții critice + toleranțe propuse
- Playbook incident major (Plăți & Carduri) + dry-run
- Sprint contractual Top-10 furnizori critici (clauze DORA)
- Dashboard KPI + colectare automată de evidențe
- Exercițiu de exit table-top
- Analiză concentrare + opțiuni de substituție pe 2 dependențe

Q&A

Mulțumesc,

Calin Rangu

calin@rangu.ro

www.calinrangu.ro