**UE a adoptat DORA, un fel de GDPR al siguranței cibernetice pentru organizațiile din sectorul financiar. Ce presupune noul cadru de reglementare pentru echipele de management?**

*Articol de opinie de Sergiu Zaharia, Director Cyber Strategy Advisory, Mihai Olteanu, Director Cyber Defense Advisory, și Adrian Ifrim, Director Cyber Risk Services, Deloitte România*

La finalul anului 2022, [actul de reglementare privind reziliența operațională digitală (DORA](https://www2.deloitte.com/ro/en/pages/risk/solutions/implementing-eus-digital-operational-resilience-act-dora.html?nc=42)) a fost publicat în monitorul oficial al Uniunii Europene, întrând în vigoare începând cu 16 ianuarie 2023. Complexitatea efectelor DORA asupra domeniului siguranței cibernetice pentru organizațiile din sectorul financiar este comparabilă cu ceea ce a însemnat GDPR pentru domeniul protecției datelor personale. DORA creează primul cadru legislativ care armonizează măsurile de securitate cibernetică și de risc pentru toate entitățile din sectorul financiar, nu doar pentru bănci, la nivel european.

**Cei patru piloni prezentați în DORA**

DORA are în vedere **patru piloni** pe care companiile din sectorul financiar trebuie să îi ia în considerare pentru a înțelege maniera în care practicile lor privind tehnologia informației și comunicațiilor, reziliența operațională și cibernetică, dar și managementul riscurilor rezultate în urma colaborării cu terți asigură continuitatea funcțiilor lor critice.

**Primul pilon** presupune crearea unui cadru de management al riscului în jurul unui set de principii și cerințe cheie în vederea **gestionării riscului privind tehnologia informației și comunicațiilor**.

**Al doilea pilon** vizează modalitatea de **raportare a incidentelor**, entitățile financiare fiind nevoite să notifice astfel de cazuri în 24 de ore de la producere. În decurs de o lună, organizația compromisă este nevoită să identifice cauza primară a atacului folosind [instrumente de detecție și răspuns](https://www2.deloitte.com/ro/en/pages/risk/solutions/security-information-event-management-siem-technology.html?nc=42) implementate cu ajutorul echipelor operaționale care trebuie să dea dovadă de o serie de abilități speciale în domeniu. Tehnologiile care pot sprijini procesele de detecție și răspuns sunt soluții cu care principalii jucătorii din sistemul bancar sunt cel mai probabil la zi, activând într-un sector deja puternic reglementat.

**Testarea rezilienței operaționale** reprezintă **al treilea pilon** pe care DORA îl reglementează, stabilind standarde la nivelul UE în vederea realizării acestor exerciții. Companiile care au depășit un anumit prag de maturitate – prag care va fi specificat într-un standard tehnic de reglementare ce nu a fost încă adoptat - trebuie să efectueze teste de securitate bazate pe informații despre amenințări cibernetice actuale (*Threat-Led Penetration Testing*) la fiecare trei ani, excepție făcând cazurile în care aceste dispoziții sunt modificate de autoritățile naționale. În țara noastră, Banca Națională a României a adoptat [cadrul TIBER-RO](https://www2.deloitte.com/ro/en/pages/risk/solutions/tiber-ro-framework.html?nc=42) în mai 2022, care se aplică instituțiilor financiare pe care le supraveghează. Acesta presupune testarea rezilienței cibernetice a companiilor din sectorul financiar la fiecare trei ani, iar cele care în prezent se pregătesc pentru implementarea regulamentului nr. 6/2022 privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO pot avea încredere că această activitate le va fi utilă în vederea respectării cerințelor avansate de testare specificate de DORA.

În final, **al patrulea pilon** precizează necesitatea adoptării unei strategii holistice în ceea ce privește gestionarea relației cu terții, care să permită o monitorizare completă din partea companiei.

**Implicații pentru echipele de conducere executivă**

Odată cu DORA, un cadru de reglementare mult mai strict decât alte inițiative similare din zona de securitate cibernetică și care va beneficia de o vizibilitate mai mare la nivel european, se observă o schimbare de paradigmă în ceea ce privește implementarea cerințelor, membrii echipelor de conducere executivă din sectorul financiar având un rol mult mai specific în acest sens. Astfel, aceștia vor fi nevoiți să aprobe un set de planuri cheie, cum ar fi strategia de reziliență operațională digitală a companiei și politica acesteia privind terții.

De asemenea, echipele de conducere trebuie să fie instruite și pregătite astfel încât să înțeleagă gradul de maturitate a organizației din perspectiva capacității de a face față potențialelor crize cibernetice și întreruperi majore care țin de tehnologia informației și comunicațiilor. Directorii executivi mai trebuie să știe și în ce măsură compania poate asigura continuitatea serviciilor critice în fața acestor provocări. În acest sens, companiile pot opta pentru organizarea periodică a [exercițiilor de simulare a unor potențiale atacuri cibernetice](https://www2.deloitte.com/ro/en/pages/technology/solutions/cyber-crisis-exercising.html?nc=42https://www2.deloitte.com/ro/en/pages/technology/solutions/cyber-crisis-exercising.html?nc=42), care ajută la exersarea capacității de răspuns la criză din perspectiva comunicării cu angajații, presa, autoritățile sau din cea juridică.

Un alt aspect de care managementul unei companii trebuie să țină cont este modalitatea în care DORA va afecta colaborarea cu terții. Astfel, este probabil ca directorii executivi să fie nevoiți să regândească deciziile strategice în privința partenerilor și să revizuiască rolul departamentelor de risc și achiziții.

Pe scurt, DORA va obliga managementul să devină un actor activ în procesul decizional care asigură reziliența cibernetică a organizației.

Deși direcțiile și conceptele pe care DORA le propune nu sunt noi, ele fiind deja introduse în unele directive și ghiduri de specialitate, implementarea cadrului va aduce în prim plan o serie de provocări pentru directorii executivi din sectorul financiar care, până în acest moment, se aflau preponderent pe lista de priorități a directorilor de securitate a informațiilor (*chief information security officer* - CISO) sau a directorilor de tehnologie (*chief technology officers* - CTO). Companiile trebuie să aplice prevederile DORA din 17 ianuarie 2025, așadar au la dispoziție o perioadă generoasă pentru a se pregăti, dar este important să aibă în vedere că aceste cerințe nu fac parte dintr-un exercițiu unic de conformare, ci dintr-un proces continuu, care le va ajuta să rămână în siguranță într-un peisaj al amenințărilor cibernetice aflat în plină evoluție.