

Studiu Deloitte: organizațiile din domeniul serviciilor financiare încep să înregistreze progrese în implementarea noului regulament UE privind reziliența operațională digitală, DORA



Organizațiile active în industria serviciilor financiare încep să înregistreze progrese semnificative în implementarea modificărilor menite să asigure conformarea cu noul regulament UE Legea privind reziliența operațională digitală (*Digital Operational Resilience Act - DORA*), în contextul în care o treime dintre acestea (29%) au început să se pregătească încă din 2022 și, dintre acestea, 29% au finalizat deja, până în februarie 2023, 75% din pașii de implementare planificați, conform celei mai recente ediții a [studiului Deloitte despre DORA](#). Intrată în vigoare în 2023, DORA este cea mai importantă inițiativă de reglementare a UE privind reziliența operațională și securitatea cibernetică în sectorul serviciilor financiare și impune organizațiilor să implementeze modificări specifice în termen de 24 de luni de la adoptarea sa.

[Toți cei patru piloni ai DORA](#) – gestionarea riscurilor legate de tehnologia informației și comunicații (TIC), raportarea incidentelor, testarea operațională și de reziliența digitală, precum și managementul riscului generat de furnizorii TIC – generează la fel de multe provocări entităților din domeniul financiar, subliniază studiul, însă o treime dintre respondenți (33%) menționează că al patrulea este cel mai greu de respectat. Raportul evidențiază faptul că companiile sunt în urma în ceea ce privește evaluarea riscului generat de terți, în condițiile în care șapte din zece organizații participante la studiu (69%) îl efectuează doar o dată pe an, insuficient pentru a respecta cerințele DORA, în timp ce doar 13% îl efectuează în mod continuu, așa cum cere noul regulament. Respectarea acestor cerințe implică, de asemenea, revizuirea periodică a strategiei privind riscul generat de furnizorii de soluții TIC, luând în considerare strategia de a distribui serviciile pe furnizori multipli. O astfel de abordare va fi o provocare pentru jucătorii din industria serviciilor financiare, deoarece 29% dintre respondenți încă își definesc o strategie holistică privind colaborarea cu mai mulți furnizori de soluții de tehnologia informației și comunicații, iar 21% dintre ei vor trebui să și-o actualizeze până în 2025, pentru că au definit-o mai devreme de 2022.

Înțelegerea gradului de interconectare dintre furnizorii de soluții TIC și cei de soluții de tehnologie considerate critice este, de asemenea, una dintre provocările cu care organizațiile se pot confrunta pe parcursul implementării DORA. Patru din zece instituții financiare participante la studiu (43%) au menționat că nu au demarat încă acest proces care susține funcțiile critice și importante ale companiei. Studiul evidențiază faptul că funcțiile considerate critice și importante sunt autorizarea (14%) și autentificarea tranzacțiilor de plată (12%), urmate de operațiunile IT și tranzacțiile efectuate de clienți prin intermediul canalelor digitale (12% fiecare).

„Pentru a se conforma cerințelor DORA, organizațiile vor fi nevoite să facă o clasificare a funcțiilor critice sau importante, a caror întrerupere le-ar afecta rezultatele financiare și continuitatea serviciilor, dar și să și actualizeze constant lista acestor funcții și să le identifice de-a lungul întregului lanț al furnizorilor de servicii de tehnologia informației și comunicații, critice sau nu, astfel cum sunt definite în Standardele Tehnice de Reglementare, care vor intra în curând în vigoare. În plus, instituțiile financiare vor trebui să dezvolte metode de testare a scenariilor de reziliență și strategii multi-furnizor pentru toate sistemele care susțin funcții critice și importante”, a declarat **Sergiu Zaharia, Director Cyber Strategy Advisory, Deloitte România**.

DORA impune, de asemenea, instituțiilor financiare să efectueze anual [teste ale planului de răspuns la incidente](#). Patru din zece respondenți

(36%) au efectuat astfel de exerciții în ultimele 12 luni, testând funcțiile critice și pe cele importante, în timp ce 64% nu au efectuat astfel de teste în ultimele 12 luni.

Având în vedere cerințele DORA, organizațiile financiare vor trebui, de asemenea, să efectueze [teste de penetrare bazate pe amenințări \(TLPT\)](#) asupra tuturor sistemelor și aplicațiilor TIC critice și asupra funcțiilor importante, în mediul de producție. Jumătate dintre entitățile financiare chestionate au efectuat astfel de teste, iar restul au testat doar în mediu non-live. Instituțiile financiare preferă să efectueze teste de penetrare bazate pe amenințări utilizând un mix de echipe interne și de consultanți, 57% dintre respondenți având experți angajați de *Blue Team*, responsabili de asigurarea eficienței măsurilor de securitate din cadrul unei organizații, în timp ce rolurile de *Red Team*, care vizează încercarea de intruziune fizică sau digitală într-o organizație, și cele de *Purple Team*, o combinație între echipele *Blue* și *Red*, sunt acoperite de consultanți externi.

Ce mai recentă ediție a [studiului Deloitte privind DORA](#) sondează opiniile directorilor de securitate a informației (CISO), a directorilor IT (CIO), a managerilor de risc operațional, de risc IT și de risc (CRO) din instituții financiare din 20 de țări din Europa. Raportul își propune să înțeleagă cât de pregătite sunt instituțiile financiare pentru implementarea modificărilor impuse de DORA, precum și care sunt provocările asociate cu care se confruntă aceste instituții.

[Echipa de securitate cibernetică a Deloitte România](#) este specializată în oferirea de [servicii de strategie](#), incluzând [exerciții de simulare a crizelor cibernetice](#) și evaluări holistice ale nivelului de maturitate cibernetică de tip *deep dive*, [servicii de apărare](#), inclusiv [managementul identității și accesului](#), operațiuni de securitate, procese și [tehnologii de pregătire și de răspuns la incidente](#), precum și [servicii de atac](#), vizând în special efectuarea de teste de penetrare, precum [exercițiile de tip red-teaming \(TIBER-EU\)](#).

Echipa locală contribuie activ la cele mai importante exerciții cibernetice organizate în România. În ultimii ani, Deloitte România a fost una dintre puținele organizații private selectate pentru a participa, alături de Ministerul Apărării Naționale, la exercițiile anuale organizate de NATO. În 2022, echipa Deloitte a participat la unul dintre cele mai mari exerciții de securitate cibernetică organizate în România de Centrul Național CYBERINT din cadrul Serviciului Român de Informații. În plus, experții locali în securitate cibernetică, care dețin zeci de certificări de specialitate, oferă cursuri și certificări recunoscute internațional prin intermediul Deloitte Academy, divizia de formare profesională a Deloitte România. Deloitte este și centru oficial autorizat de training în România pentru Consiliul Internațional de Consultanți în E-Commerce, cunoscut și ca EC-Council.

La nivel global, pentru al unsprezecelea an consecutiv, Gartner a clasat Deloitte pe poziția de [lider în servicii de consultanță în securitate](#) după cota de piață.