QUICK READ

ox security

How ASPM Solutions Help Organizations Prepare for the EU's DORA

The European Union's Digital Operational Resilience Act (DORA), passed in late 2022, is set to take full effect by early 2025. DORA establishes new cybersecurity standards for financial institutions operating and doing business in the European Union (EU), given their heavy reliance on information and communications technology (ICT). Recognizing the systemic risks posed by ICT, DORA aims to safeguard financial firms, their customers, and the broader financial ecosystem from cyberattacks.

This legislation mandates robust cybersecurity practices across the board, from identifying and managing ICT assets to responding to cyber incidents. As financial services firms increasingly rely on software applications — both commercial-off-the-shelf and custom-built — for core operations, it's imperative to ensure the security of these applications. DORA's emphasis on identifying, managing, and mitigating ICT risks directly impacts the application security (AppSec) landscape, which necessitates robust development, testing, and deployment practices.

What does DORA include?

Like the U.S. National Cybersecurity Strategy, DORA prioritizes digital resilience over specific vulnerabilities. This shift requires CEOs and executive leadership to establish cybersecurity strategies at the highest organizational level. By doing so, DORA addresses a long-standing challenge in the cybersecurity community: recognizing the strategic, operational, and financial implications of poor cybersecurity practices for the entire organization and its stakeholders.

As outlined in the legislation, DORA aims to streamline and enhance ICT risk requirements within the existing operational risk framework. By consolidating disparate regulations, DORA reduces regulatory complexity, promotes supervisory convergence, and increases legal clarity. Additionally, it is expected to lower compliance costs, particularly for cross-border financial institutions, and mitigate competitive distortions. This risk-centric approach fosters a more comprehensive organizational approach to security rather than relying solely on the security team.

Elements of the Act

DORA specifies five areas on which financial institutions must focus to achieve digital resilience and meet the requirements:

Within those pillars, there are several sections that focus on how financial institutions can tactically and strategically achieve the above requirements, including:

- Governance protocols
- Risk management frameworks
- Identification, protection and prevention, detection, response and recovery
- Harmonization of tools and technologies

While not explicitly highlighted in DORA, AppSec suffers from the same lapses and oversights as general cybersecurity. This is why DORA was written and passed — to alleviate these gaps and help financial organizations improve best practices and protocols — and why AppSec must be a key consideration when architecting to meet DORA's mandates.

Application Security Posture Management's Role in DORA

Financial institutions have grown increasingly reliant on applications for normal day-to-day operations. As a result, threat actors have taken a keen interested in exploiting them, which elevates application security from a basic functionality to a strategic imperative.

Again, while DORA isn't an AppSec-focused regulation, its elements necessitate greater rigor in AppSec processes and approach. Articles in the Act that impact AppSec include:

ARTICLE 6	**ICT Risk Management:** Managing risks associated with software applications cannot be separated from overall security or business risk management, as they are a core operational element for most businesses today.
ARTICLE 8	**Identification:** Accurate identification and classification of applications — including the software bill of materials (SBOM), entire codebase, and application dependencies — are crucial for assessing and governing risk.
ARTICLE 10	**ICT Incident Reporting:** Application vulnerabilities and exploits are often the root cause of incidents, making AppSec essential for incident prevention and response.
ARTICLE 11	**Digital Resilience Testing:** Application security testing (AST) is a critical component of assessing an organization's digital resilience.

How does DORA impact AppSec?

DORA addresses cybersecurity holistically, and as such, application security must be part of organizations' plans. Applications are the lifeblood of modern financial institutions, and as such, secure applications are fundamental to maintaining operational resilience. Vulnerabilities in applications can lead to data breaches, financial losses, and reputational damage, and stronger AppSec and development practices can mitigate these risks and reduce the likelihood of organizational disruptions caused by application compromise.

Digital Resilience and AppSec: DORA stresses digital resilience. Securing applications and holistic ASPM are critical to this effort since they are a prime attack target. Financial institutions must implement processes and tooling that provide centralized, unified application security management, from code to cloud and from cloud to code.

Application Vulnerability Management: To ensure digital resilience, DORA necessitates a broader view of vulnerabilities, which means companies must understand their entire application security posture, including software composition analysis, code integrity, artifact integrity, secrets security, API security, and more.

Enhanced Testing Requirements: The regulation mandates regular testing to identify vulnerabilities and ensure resilience. Application-specific testing should be ongoing and continuous to verify that even small changes in applications don't introduce new vulnerabilities.

Software Supply Chain Security: Financial institutions must assess and manage the security risks posed by third-party components (libraries, open-source code), dependencies, and APIs. ASPM tools and processes should incorporate all the elements to identify, investigate, and remediate all app-related issues in one solution, helping reduce risk and align with DORA requirements.

Automated Response: To remain in line with DORA's requirements, security programs must be designed to facilitate effective incident response and recovery. AppSec and DevOps programs are no exception to this rule. ASPM fills this need by automating issue identification and remediation and by eliminating formerly cumbersome, manual AppSec practices.

Systemic attack surface reduction

This is what Active ASPM is all about, and why ASPM, application security testing, and software supply chain security tools, are a must for all organizations. These tools effectively reduce the amount and severity of application-related risk by systematically identifying all software and their security posture, allowing for deep analysis of application-related risk, and providing a way for organizations to prioritize and remediate vulnerabilities. ASPM achieves these goals through correlation and automation, which reduces the time, effort, and accuracy necessary to understand application or software security posture.

A robust ASPM solution like OX Security allows financial organizations to comply with DORA through its AppSec Data Fabric, which allows businesses to:

See everything

Continuously identify all applications, at any stage of development, and from any network environment

Consolidate AppSec data, from OX's native scanning solution and third-party solutions

Unearth vulnerabilities and issues that could pose a risk

Focus on what matters

Enrich data with threat intelligence and business relevancy to ensure all findings include context

Prioritize triage and improve mean-time-to-response by targeting the most business-critical vulnerabilities

Dive into the application attack path and dependencies to understand the potential impacts of an application compromise

Mitigate risk at scale

Use OSC&R, a MITRA ATT&K-like framework for software development, to understand software supply chain risks

Automate workflows and remediation tasks to block risky actions or vulnerable software

Comply with DORA and a host of other regulations via continuous monitoring, reporting, and remediation throughout the entire application lifecycle

The OX Security platform

It's important to note that not all ASPM or application security management solutions are created equal. OX Security is the only Active Application Security Posture Management (ASPM) platform designed to streamline and enhance the entire AppSec process. Through a combination of native scanning capabilities and robust integrations, OX is a unified platform that consolidates all the necessary AppSec tooling functionality into a single interface for efficient AppSec. OX provides real-time insights into the security posture of applications throughout the entire Software Development Lifecycle (SDLC); accurately assesses and prioritizes threats based on factors like exploitability, reachability, and impact; and offers automated actions to address vulnerabilities and reduce response times.

In short, ands in line with DORA's expectation, the OX Security Platform:

- Eliminates manual AppSec to foster simpler risk reduction
- Proactively identifies, protects, detects, and helps companies respond to application threats
- Enhances digital resiliency through accelerated secure software delivery

To learn more about how OX is going beyond traditional ASPM technologies and addressing the problems that are most critical for AppSec and DevOps teams:

WWW.OX.SECURITY/BOOK-A-DEMO/

About OX Security

At OX Security, we're simplifying application security (AppSec) with the first-ever Active ASPM platform offering seamless visibility and traceability from code to cloud and cloud to code. Leveraging our proprietary AppSec Data Fabric, OX delivers comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. Recently recognized as a Gartner Cool Vendor and a SINET 16 Innovator, OX is trusted by dozens of global enterprises and tech-forward companies. Founded by industry leaders Neatsun Ziv, former VP of CheckPoint's Cyber Security business unit, and Lior Arzi from Check Point's Security Division, OX's Active ASPM platform is more than a platform; it empowers organizations to take the first step toward eliminating manual AppSec practices while enabling scalable and secure development.

oxsecurity