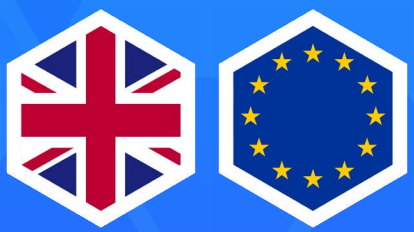
sonatype

What DORA Means for Financial Entities in the EU

User's Guide to Compliance



Digital Operational Resilience Act (DORA)

DORA is an EU regulation that sets out to enhance the cybersecurity of financial institutions, including banks, insurance firms, and investment companies. It does this by standardising operational resilience regulations across the financial industry, applying more than 22,000 financial entities and information and communications technology (ICT) service providers operating within the EU, as well as the ICT infrastructure supporting them from outside the EU. This is an EU-wide requirement passed in 2024 and must be enforced starting in January 2025.

This is an EU-wide requirement passed in 2024 and must be enforced starting in January 2025.

DORA focuses on five key areas:

ICT Risk Management

ICT Related Incident Management, Classification, and Reporting

Digital Operational Resilience Testing

ICT Third-Party Risk Management

Information Sharing Arrangements

Optimise and Protect Your Software Supply Chain

Although EU-based financial institutions are the primary focus, this regulation will undoubtedly have implications for organizations around the world. Sonatype protects and defends organisations from the inherent risks in the open source software ecosystem and has been at the forefront of protecting the software supply chain for more than two decades. In the table below, we outline how Sonatype can help address DORA's ICT risk management framework.

Article 6: Section 8 of DORA provides an ICT risk management framework that covers the following areas:

The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:

a. explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;

b. establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;

c. setting out clear information security objectives, including key performance indicators and key risk metrics;

d. explaining the ICT reference architecture and any changes needed to reach specific business objectives;

e. outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;

f. evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;

g. implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;

h. outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.

DORA classifies open source analysis, also known as Software Composition Analysis (SCA), as a basic security requirement in Regulation 56. Consequently, all financial entities governed by DORA must develop capabilities in this area.

Sonatype's platform is a leading provider of comprehensive solutions for open source analysis, scanning software, and vulnerability assessments.

Developing these foundational capabilities is essential before any advanced security activities are undertaken according to DORA.

DORA Regulation 56

DORA includes language outlining how to achieve a high level of digital operational resilience and **emphasises open source analysis as a fundamental security requirement:**

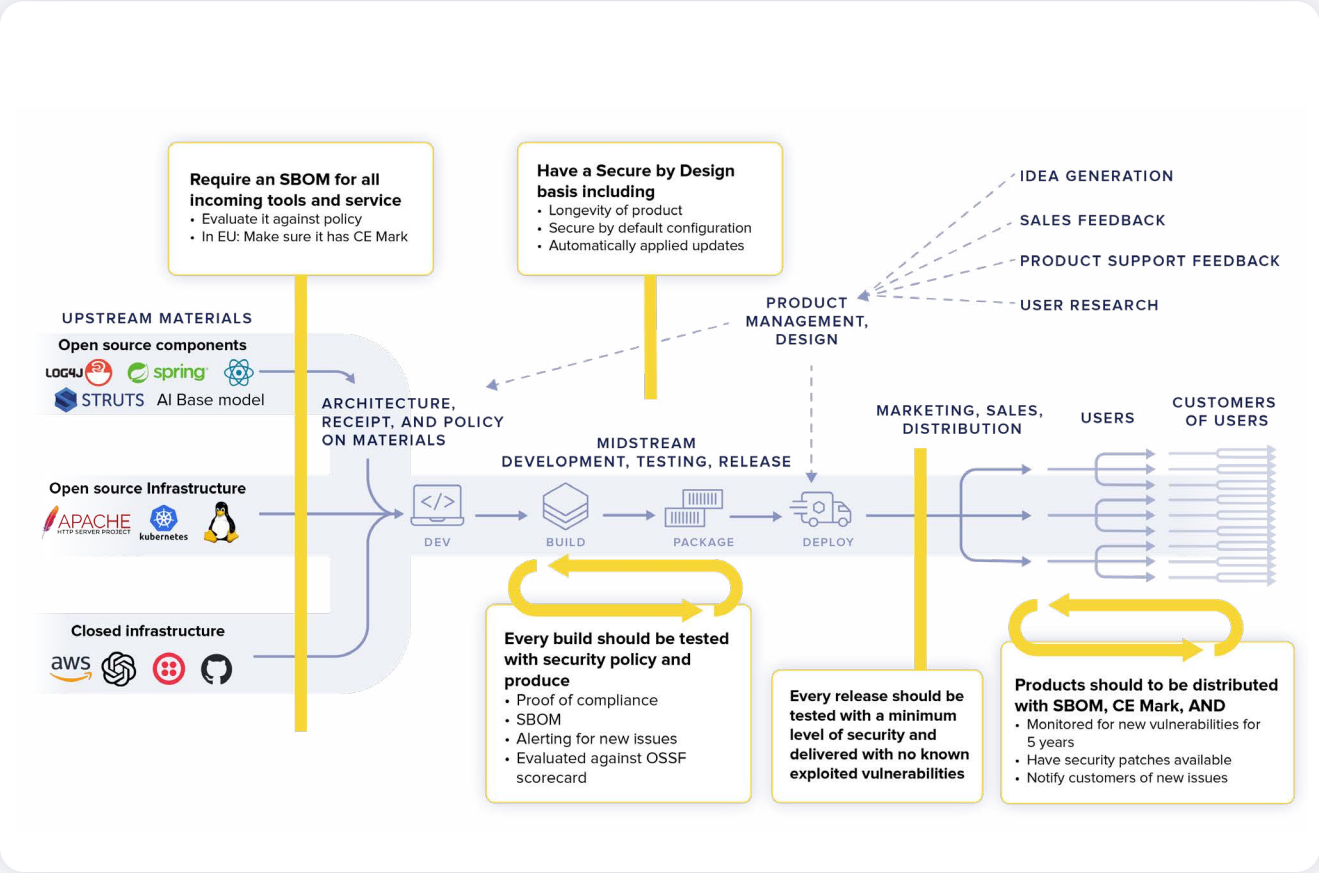
> *In order to achieve a high level of digital operational resilience, and in line with both the relevant international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing) and with the frameworks applied in the Union, such as the TIBER-EU, financial entities should regularly test their ICT systems and staff having ICT-related responsibilities with regard to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential ICT vulnerabilities.*
>
> *To reflect differences that exist across, and within, the various financial subsectors as regards financial entities' level of cybersecurity preparedness,* ***testing should include a wide variety of tools and actions****, ranging from the assessment of basic requirements (e.g. vulnerability assessments and scans,* ***open source*** **analyses***, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing or end-to-end testing) to more advanced testing by means of TLPT.*
>
> *Such advanced testing should be required only of financial entities that are mature enough from an ICT perspective to reasonably carry it out. The digital operational resilience testing required by this Regulation should thus be more demanding for those financial entities meeting the criteria set out in this Regulation (for example, large, systemic and ICT-mature credit institutions, stock exchanges, central securities depositories and central counterparties) than for other financial entities.*
>
> *At the same time, the digital operational resilience testing by means of TLPT should be more relevant for financial entities operating in core financial services subsectors and playing a systemic role (for example, payments, banking, and clearing and settlement), and less relevant for other subsectors (for example, asset managers and credit rating agencies).*

Sonatype is the best fit for organizations with a diverse software supply chain; that want assurance that security, license, and operational risk aren't being introduced; and that have the resources to integrate the suite of products."

– The Forrester Wave Software Composition Analysis

Sonatype protects and defends organisations and government agencies from the inherent risks in the open source software ecosystem, and we're a leader in analysis, scanning, and vulnerability assessment of OSS components. Our platform makes it possible to define policies for securing open source components and enforcing them throughout development. Continuous automated monitoring lets you stay current on any new policy violations discovered, even after the software is built. Sonatype also provides constant updates for third-party policies, and an easy-to-use administrative UI simplifies policy management.

Incorporating robust security measures into the development process is necessary to strengthen your approach to open source components. SDLC processes that take into account best practices will minimize risks.



To learn more about how we can help you ensure compliance with emerging and existing regulations, schedule a demo today.

sonatype

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Life Cycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com