sonatype

DORA Compliance Checklist:

How Sonatype helps you

DORA, an EU-wide requirement passed in 2024 and to be enforced starting in January 2025, requires financial entities to put measures in place to protect against cybersecurity threats and disruptions to ICT services. Two elements of DORA stand out: the **ICT Risk Management Framework** and **Regulation 56**, which emphasises the importance of open source analysis.

This guide can help you determine how prepared your organisation is to comply with DORA's key components.

DORA Compliance Checklist: Navigate New Cybersecurity Measures

ICT Risk Management

- ☐ Do we have processes to identify, monitor, and manage ICT risks?
- ☐ Are our ICT risk management policies and procedures up-to-date and aligned with regulatory requirements?
- ☐ Do we have a process for continuous monitoring of ICT systems and services?

Incident Reporting

- ☐ Do we have an incident reporting process in place for security-related incidents?
- ☐ Can we detect, manage, and report significant incidents within the required timeframe?
- ☐ Have we conducted training and awareness programs for incident reporting?

Information Security

- ☐ Are our information security measures adequate to protect against ICT risks?
- ☐ Do we regularly review and update our information security policies?
- ☐ Are employees trained on information security protocols and practices?

Business Continuity and Disaster Recovery

- ☐ Do we have a robust business continuity and disaster recovery plan for ICT disruptions?
- ☐ Are these plans tested regularly, and are staff trained on their roles in these plans?
- ☐ Are backup systems and data recovery processes in place and regularly tested?

Resilience Testing

- ☐ Have we implemented a testing program to assess our ICT systems' resilience?
- ☐ Do we conduct regular penetration testing, vulnerability assessments, and other resilience tests?
- ☐ Are test results reviewed, and are necessary improvements implemented promptly?

Business Continuity and Disaster Recovery

- ☐ Do we have a robust business continuity and disaster recovery plan for ICT disruptions?
- ☐ Are these plans tested regularly, and are staff trained on their roles in these plans?
- ☐ Are backup systems and data recovery processes in place and regularly tested?

SBOM Creation and Maintenance

- ☐ Do we generate SBOMs for all software, including third-party and open-source components?
- ☐ Are our SBOMs updated regularly to reflect any changes in the software components?
- ☐ Are we identifying and documenting all software components, including their versions, in our SBOMs?
- ☐ Do we have a process for verifying the authenticity and integrity of each component listed in the SBOM?

How Sonatype Can Help

Monitoring the health and policy compliance of open source components is essential to meeting these DORA requirements. Sonatype is the industry's only comprehensive, proactive solution for end-to-end software supply chain security, with more than 300 million open source components catalogued. Sonatype also provides constant updates for third-party policies, and an easy-to-use administrative UI simplifies policy management.

DORA is just one part of the global trend of cybersecurity requirements. To learn more about how we can help you ensure compliance, check out our **DORA User's Guide to Compliance**.

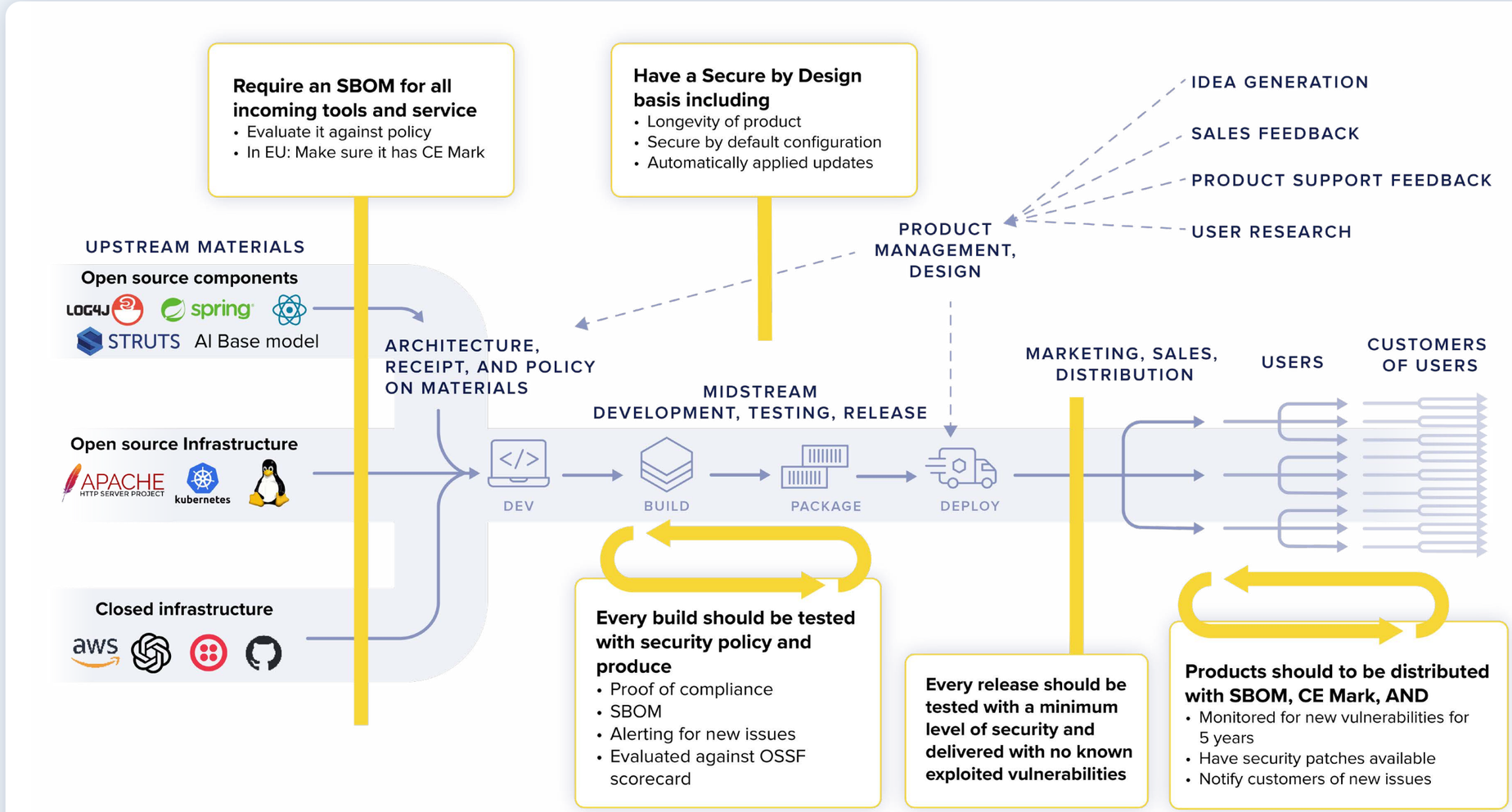
sonatype

How Sonatype's Platform helps you comply

Simplify SBOM Compliance and Security Monitoring with Sonatype SBOM Manager

More than 70 percent of Fortune 100 companies manage their software supply chains with Sonatype, and our SBOM Manager has been developed to take the uncertainty out of SBOM collection and monitoring compliance.

Request a demo today



Discover our full range of products that support your compliance journey

Maven Central Repository
World's largest Java repository, administered by Sonatype

Sonatype Lifecycle
Achieve faster release velocity with reliable SDLC security automation

Sonatype SBOM Manager
Simplify Software Bill of Materials compliance and monitoring

Sonatype Nexus Repository
Smart repository to manage and build artifacts, trusted by more than 150K organizations

Sonatype Developer
Prioritized recommendations and reliable automations for developer velocity

Advanced Legal Pack
Automate and streamline OSS component licensing and legal compliance

Sonatype Repository Firewall
Automatically spot and stop risk before entering your repository

Sonatype Container
Protection for container, network, process and file system