sonatype

CRA Compliance Checklist:

How Sonatype helps you

The **Cyber Resilience Act (CRA)**, covers all products with digital elements that can be connected to a device or a network.

The CRA includes eight annexes that provide detailed requirements and standards, including Essential Cybersecurity Requirements (Annex I) and Reporting Obligations of Manufacturers (Article 11). Only products that comply with these requirements will be allowed on the market. Technical documentation proving compliance is necessary, and imported products require a CE mark.

This checklist covers key elements of Annex I and Article 11, and how Sonatype can help support compliance throughout the SDLC.

Here are some questions to consider when determining your preparedness to comply with CRA requirements.

Risk Assessment

- ☐ Are we conducting cybersecurity risk analysis throughout the complete development lifecycle?
- ☐ Are all software components regularly scanned for vulnerabilities?
- ☐ Do we have an inventory of all hardware and software assets?
- ☐ Is there a process for prioritising and addressing identified vulnerabilities based on severity and impact?
- ☐ Are patches and updates applied in a timely manner?

Access Control and Third-Parties

- ☐ Are controls in place to ensure that only authorised personnel can access sensitive systems and data?
- ☐ Are these access controls regularly reviewed and updated?
- ☐ Are our suppliers and third-party partners also complying with our cybersecurity requirements?
- ☐ Do we have agreements in place that mandate cybersecurity standards for third parties?

Incident Response

- ☐ Are there predefined procedures for responding to and recovering from cyber incidents?
- ☐ Is our incident response plan tested regularly and updated as needed?
- ☐ Have we established communication plans for internal and external stakeholders in the event of a security incident?
- ☐ Do you have SBOMs collected for rapid triaging of issues?

Reporting Obligations

- ☐ Is there an established incident response plan for potential security breaches?
- ☐ Are all software security incidents documented and reported as required by regulatory standards?
- ☐ Do we automate the production of SBOMs and other evidence to speed up report generation?

Data Protection

- ☐ Are we taking steps to protect the confidentiality of all sensitive and personal data?
- ☐ Do we have measures in place to detect and respond to data breaches?
- ☐ Are adequate security controls in place to protect software and data integrity?
- ☐ Is encryption used for sensitive data at rest and in transit?
- ☐ Are regular security audits conducted to ensure compliance with internal and external standards?

Standards and Policies

- ☐ Do we have a comprehensive cybersecurity policy in place?
- ☐ Are all employees aware of and trained on these policies?
- ☐ Do we have a designated person or team responsible for these policies?

How Sonatype Can Help Optimise and Protect Your Software Supply Chain

Vulnerability scanning is central to the CRA, and only products that comply with the security and vulnerability management requirements above will be allowed on the market. Products will be presumed to be compliant, but sanctions will apply if they are discovered not to be. The Sonatype platform can help developers gather and report on compliance information, identify vulnerabilities, and meet the reporting requirements. To learn more about how we can help you ensure compliance, download our **CRA User's Guide to Compliance**.

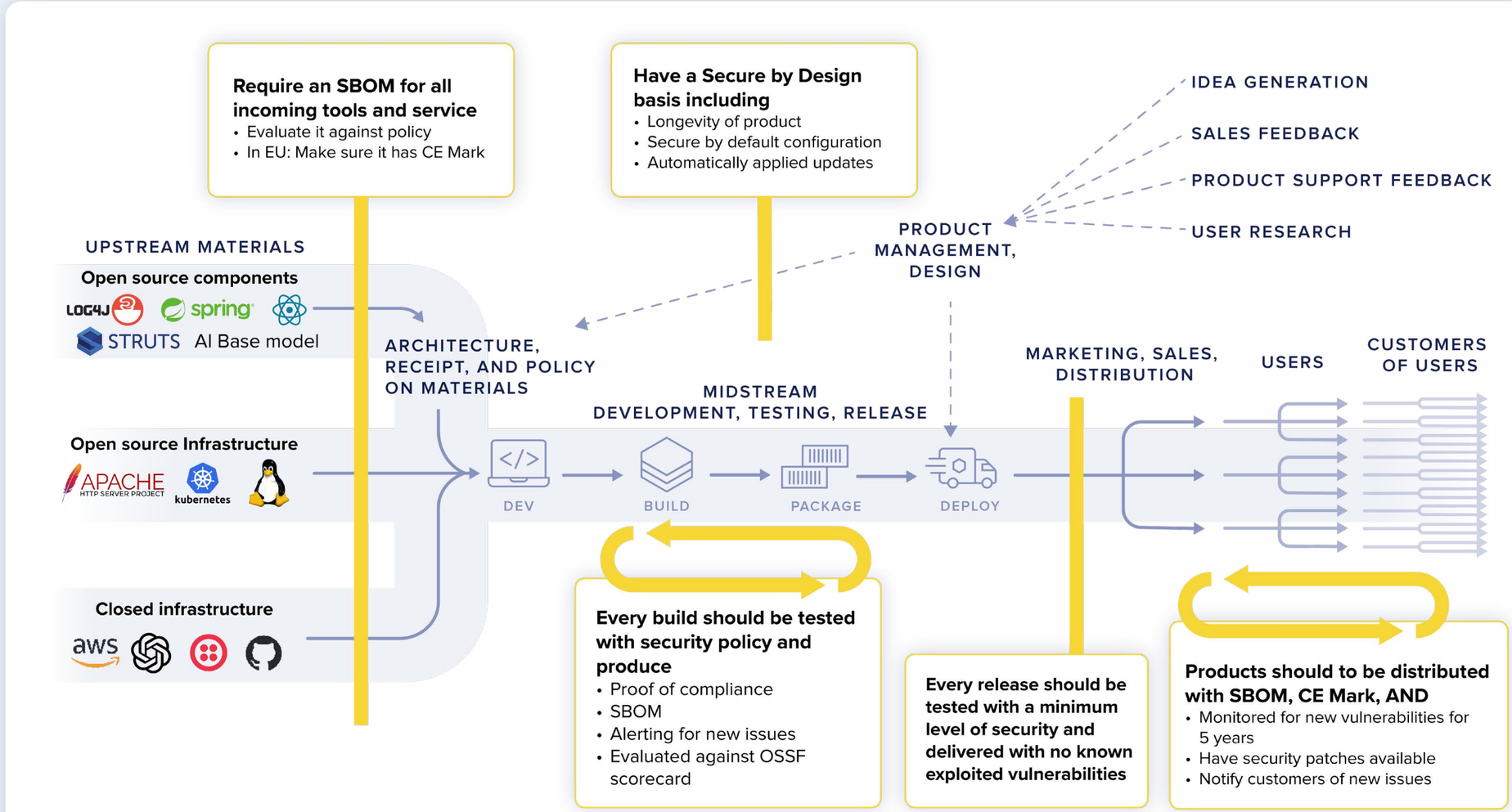
sonatype

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