sonatype

Global Regulations Cheat Sheet

How to navigate evolving cybersecurity and software supply chain requirements

Organizations today face a growing set of global regulations focused on software transparency, supply chain security, and operational resilience. While each framework varies, they share common themes: visibility into components, risk management, and rapid response to vulnerabilities.

This cheat sheet provides an overview of key regulations, a quick way to assess your readiness, and details on how Sonatype helps accelerate compliance.

1. SEBI Cybersecurity & Cyber Resilience Framework

CHECKLIST

- ☐ Do we maintain a complete and up-to-date SBOM for all applications?
- ☐ Are all third-party and open source components identified and tracked?
- ☐ Can we verify the integrity and authenticity of software components?
- ☐ Do we track licenses and supplier metadata for compliance purposes?
- ☐ Are vulnerabilities continuously monitored across all dependencies?

WHY IT MATTERS

SEBI requires regulated entities to strengthen cybersecurity posture with increased emphasis on software component visibility, SBOM adoption, and third-party risk management.

HOW SONATYPE HELPS

- Automatically generates and maintains **accurate SBOMs** across the SDLC
- Provides deep visibility into **open source and third-party components**
- Continuously monitors for **vulnerabilities, license risks, and integrity issues**
- Enables policy enforcement aligned with regulatory requirements

2. CERT-In Cybersecurity Directions (India)

CHECKLIST

- ☐ Do we detect and report incidents within mandated timeframes?
- ☐ Are logs collected, stored, and monitored across all systems?
- ☐ Do we have visibility into software vulnerabilities impacting operations?
- ☐ Are response processes documented and regularly tested?

FOCUS

Incident reporting, monitoring, and security controls

WHY IT MATTERS

CERT-In mandates strict requirements for **incident detection, reporting timelines, and system logging,** increasing accountability for cybersecurity operations.

HOW SONATYPE HELPS

- Identifies vulnerabilities early to **reduce incident likelihood**
- Provides continuous monitoring of component risk exposure
- Integrates into workflows to support **rapid remediation and reporting readiness**

3. DORA (EU Digital Operational Resilience Act)

CHECKLIST

- ☐ Do we continuously monitor ICT and software supply chain risks?
- ☐ Are third-party dependencies fully documented and assessed?
- ☐ Do we perform regular resilience and vulnerability testing?
- ☐ Can we respond quickly to software-related disruptions?

FOCUS

ICT risk management and operational resilience

WHY IT MATTERS

DORA standardizes how financial institutions manage **ICT risk, resilience testing, and third-party dependencies** across the EU.

HOW SONATYPE HELPS

- Enables full visibility into **software supply chains and dependencies**
- Continuously evaluates component health and policy compliance
- Supports proactive risk mitigation before issues impact operations

4. NIS2 Directive (EU)

CHECKLIST

- ☐ Do we assess cybersecurity risk across suppliers and software components?
- ☐ Are secure development practices enforced across teams?
- ☐ Do we monitor and remediate vulnerabilities continuously?
- ☐ Is executive oversight in place for cybersecurity risk?

FOCUS

Cyber risk management and supply chain security

WHY IT MATTERS

NIS2 expands cybersecurity obligations across industries, emphasizing **risk management, governance, and supply chain accountability.**

HOW SONATYPE HELPS

- Provides actionable insights into **component and supplier risk**
- Enforces security policies directly in developer workflows
- Reduces exposure through automated risk detection and remediation

5. U.S. Executive Order 14028

CHECKLIST

- [ ] Do we generate SBOMs for all delivered software?
- [ ] Are software components traceable and verifiable?
- [ ] Do we follow secure development and vulnerability management practices?
- [ ] Can we share SBOM data with stakeholders when required?

FOCUS

Software supply chain security and SBOM adoption

WHY IT MATTERS

This executive order drives adoption of **SBOMs, secure software development practices, and vendor transparency** across federal systems.

HOW SONATYPE HELPS

- Automates SBOM generation aligned with industry standards (CycloneDX, SPDX)
- Ensures complete visibility into all components, including transitive dependencies
- Supports compliance with federal supply chain security expectations

6. NIST SSDF (SP 800-218)

CHECKLIST

- [ ] Are security practices integrated into development workflows?
- [ ] Do we identify and remediate vulnerabilities early in the SDLC?
- [ ] Are software components continuously evaluated for risk?
- [ ] Do developers receive actionable security guidance?

FOCUS

Secure development lifecycle practices

WHY IT MATTERS

SSDF provides guidelines for embedding **security throughout the software development lifecycle**, from design to deployment.

HOW SONATYPE HELPS

- Integrates directly into developer tools for **real-time risk feedback**
- Automates vulnerability detection and prioritization
- Enables secure-by-design development practices

7. ISO/IEC 27001 (Software & Supply Chain Context)

CHECKLIST

- ☐ Are software components governed under security policies?
- ☐ Do we manage third-party and open source risk effectively?
- ☐ Are vulnerabilities tracked and remediated systematically?
- ☐ Is compliance continuously monitored and audited?

FOCUS

Information security management systems

WHY IT MATTERS

ISO 27001 requires organizations to implement structured **information security controls,** including those related to software and third-party risk.

HOW SONATYPE HELPS

- Centralizes policy management for **open source and third-party components**
- Provides audit-ready visibility into software risk posture
- Automates enforcement of security and compliance controls

8. PCI DSS (Software Security Aspects)

CHECKLIST

- ☐ Are vulnerabilities identified and remediated in a timely manner?
- ☐ Do we maintain secure configurations across applications?
- ☐ Are third-party components assessed for risk?
- ☐ Do we enforce secure development practices?

FOCUS

Protecting payment systems and sensitive data

WHY IT MATTERS

PCI DSS requires strong controls to protect **cardholder data,** including secure software and vulnerability management.

HOW SONATYPE HELPS

- Detects and prioritizes vulnerabilities impacting payment systems
- Prevents risky components from entering development pipelines
- Supports continuous compliance with security requirements

9. UK FCA / PRA Operational Resilience Requirements

CHECKLIST

- ☐ Do we understand critical software dependencies and their risks?
- ☐ Are resilience and recovery plans in place and tested?
- ☐ Can we quickly identify and remediate vulnerable components?
- ☐ Do we monitor third-party software risk continuously?

FOCUS

Business continuity and third-party risk

WHY IT MATTERS

UK regulators emphasize **operational resilience,** including the ability to withstand disruptions caused by technology and third-party dependencies.

HOW SONATYPE HELPS

- Maps and monitors **critical software dependencies**
- Enables rapid identification of vulnerable components
- Strengthens resilience through proactive risk management

SIMPLIFY COMPLIANCE ACROSS REGULATIONS

Sonatype provides a unified platform to help organizations address overlapping regulatory requirements by delivering:

- End-to-end software supply chain visibility
- Automated SBOM generation and management
- Continuous vulnerability and policy monitoring
- Developer-first security workflows

BOOK A PERSONALIZED DEMO