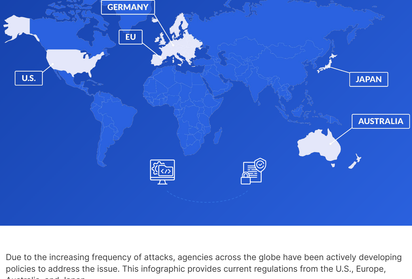
Scribe

Ensuring the Security of Software Supply Chains:
Meeting Compliance and Legal Obligations



Due to the increasing frequency of attacks, agencies across the globe have been actively developing policies to address the issue. This infographic provides current regulations from the U.S., Europe, Australia, and Japan.

Familiarity with these requirements is essential for software vendors and security engineering teams aiming to sell software in these markets.

U.S.

Executive Order 14028

"There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended."

Read the Order

National Cybersecurity Strategy Implementation Plan

A comprehensive framework designed to bolster the nation's cyber defenses and capabilities. It outlines specific objectives and initiatives to enhance cybersecurity across government agencies, critical infrastructure, and the private sector.

Read the Plan

NIST SP 800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Guidelines and best practices for managing cybersecurity risks throughout the supply chain at all levels of the organization. It incorporates cybersecurity supply chain risk management (C-SCRM) into risk management procedures.

Read it Now

FDA-2021-D-1158: Cybersecurity in Medical Devices

"Because vulnerability management is a critical part of a device's security risk management processes, an SBOM should be maintained as part of the device's configuration management, be regularly updated to reflect any changes to the software"

Read it Now

M-23-16: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

"This memorandum reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and extends the timelines for agencies to collect attestations from software producers"

Read it Now

PCI DSS v4 Requirement 6: Develop and Maintain Secure Systems and Software

This requirement emphasizes the importance of implementing secure coding practices, and regularly updating software. It aims to mitigate the risk of unauthorized access or exploitation of sensitive payment card data.

Read it Now

CISA's Secure Software Development Attestation Form

Once finalized, the form will require software vendors supplying the federal government to confirm specific practices ensuring the security of their software, third-party components, and development environment.

Read it Now

EU

The European Cyber Resilience Act (CRA)

The European Cyber Resilience Act is a legal framework that describes the cybersecurity requirements for hardware and software products with digital elements placed on the market of the European Union. Manufactures are now obliged to take security seriously throughout a product's life cycle.

Read it Now

Regulation 2022/2554: The Digital Operational Resilience Act (DORA)

Financial entities must possess the capacity and personnel to gather data on vulnerabilities, cyber threats, and ICT incidents, especially cyber-attacks, and analyze their potential impact on digital operational resilience.

Read it Now

Regulation 2022/0272: Horizontal Cybersecurity Requirements for Products with Digital Elements (proposed)

To aid vulnerability analysis, manufacturers should identify and document all components present in products with digital elements, which can be accomplished by creating a software bill of materials.

Read it Now

Germany

BSI technical guidelines on cyber resilience requirements for software supply chain

"The technical guidelines define formal and technical specifications for software parts (SBOM), thereby offering recommendations to software manufacturers for the design of SBOMs that serve to increase security in the software supply chain."

Read it Now

Australia

ASD Cyber Security Guidelines

These guidelines offer practical advice for organizations to safeguard their systems and data from cyber threats. They address governance, physical security, personnel security, and information and communication technology security.

Read it Now

Japan

Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management

It is expected that organizations will proceed with the implementation of an SBOM while confirming the main implementation items in each step and the points that shall be recognized when implementing the SBOM.

Read it Now