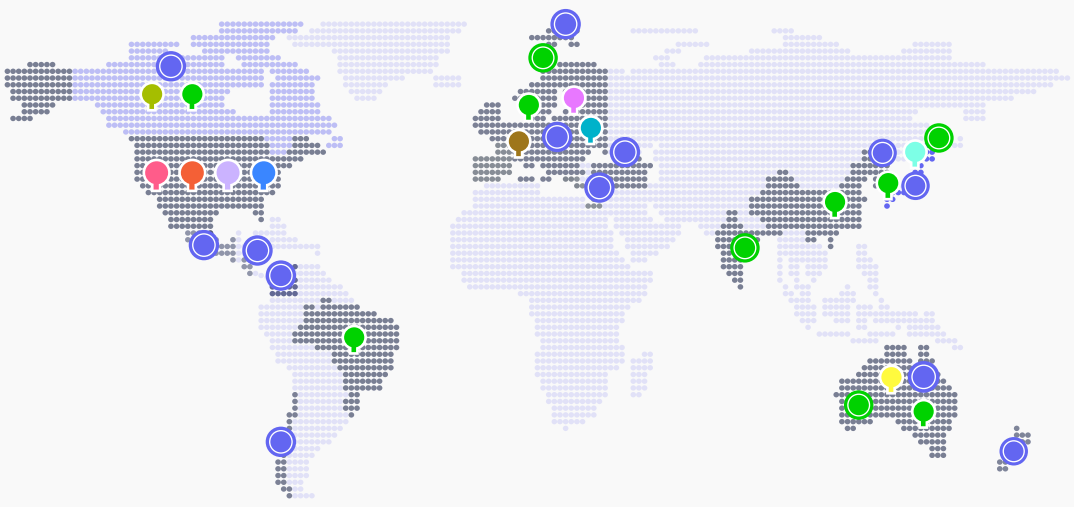
SCANOSS

Global Software Supply Chain Regulations:

What's Enforced, What's Coming

Where Software Supply Chain Regulations Apply



When These Rules Take Effect

2021

REGULATION: **EO 14028**
JURISDICTION: **United States**
AFFECTS: **Federal Software Suppliers**

2023

REGULATION: **Canada Cyber Centre Guidance**
JURISDICTION: **Canada**
AFFECTS: **Tech and Service Providers**

REGULATION: **ACSC Secure Software Guidelines**
JURISDICTION: **Australia**
AFFECTS: **All Developers**

REGULATION: **FDA Cybersecurity Guidance**
JURISDICTION: **United States**
AFFECTS: **Medical Device Manufacturers**

REGULATION: **METI SBOM Guidance**
JURISDICTION: **Japan**
AFFECTS: **Software Providers (Phased 2023–2024)**

REGULATION: **IMDRF SBOM Guidance**
JURISDICTION: **Global**
AFFECTS: **Regulated Medical Devices**

2024

REGULATION: **ICTS Supply Chain Regulations (expanding scope)**
JURISDICTION: **United States**
AFFECTS: **ICTS, Automotive, Consumer Devices**

REGULATION: **NIS2 Directive**
JURISDICTION: **European Union**
AFFECTS: **Critical Infrastructure, Digital Services**

2025

REGULATION: **DORA**
JURISDICTION: **European Union**
AFFECTS: **Financial Institutions**

REGULATION: **US Army SBOM Directive**
JURISDICTION: **United States**
AFFECTS: **Department of Defense Suppliers**

2027

REGULATION: **Cyber Resilience Act (CRA)**
JURISDICTION: **European Union**
AFFECTS: **All Digital Products**

Global Frameworks & Sector Alignments
(non-binding, cross-border initiatives)

These initiatives are not binding laws, but they shape international best practices and influence future regulation.

Framework
Reusable model for secure development or SBOMs.

United States, Canada, Japan	**NIST SSDF**	Widely adopted guidance for secure software development, referenced in EO 14028 and used across public and private sectors.
United States	**CNSS Policy 15**	Requires national security system operators to assess software component risk, maintain inventories, and align with secure development baselines.
Global	**ISO/IEC 5230**	International standard developed by the OpenChain project for managing open source licence compliance and component inventories.
Global	**NTIA/CISA SBOM Minimum Elements**	Defines the minimum structure and fields required in a valid SBOM. Implemented in SPDX and CycloneDX tooling.

Policy Initiatives
Government or global push shaping future rules.

Quad Countries

Quad Secure Software Principles
High-level government commitment to promote SBOM use and secure development practices among Quad member countries.

OECD member countries

OECD Transparency Recommendation
Draft for an ongoing effort to align software supply chain practices across OECD member states.

Sectoral Alignments

	IMDRF Medical Devices	SBOMs required in cybersecurity documentation for medical device approvals.
Global	**GSMA & 5G Supply Chain Security**	Telecom operators are aligning around SBOM use and software transparency standards for 5G and mobile infrastructure.

Guidance
Non-binding recommendations from public agencies.

Germany	**BSI Software Guidance**	Germany's BSI outlines SBOM use, secure-by-design practices, and component traceability aligned with EU regulation.
European Union	**ENISA Good Practices**	Recommends SBOM use, supplier audits, and vulnerability management for EU Member States. Supports NIS2 implementation.
United States	**CISA/NSA/ ODNI Series**	US inter-agency practices for developers, suppliers, and customers. Emphasises SBOM, secure tooling, and component trust.

Who Is Affected Inside Your Business?

Department	Impact
Legal	Disclosure, liability (NIS2, CRA)
Procurment	Supplier compliance, SBOM validation
Engineering	Inventory, SBOM formats
Security	OSS risk & compliance
Product	Documentation, provenance
Executives	Jurisdictional strategy, risk exposure

Are You Ready? Key Actions for 2025

- [x] SBOM generation embedded in CI/CD
- [x] Retention policies (FDA, DORA)
- [x] 3rd-party component visibility
- [x] Region-specific readiness plans
- [x] Unified compliance dashboards
- [x] Legal/security/procurement coordination

Software Regulation Is Now Global

SCANOSS helps organisations build continuous, verifiable software inventories using real-time open source risk intelligence.

SCANOSS