sonatype

FREQUENTLY ASKED QUESTIONS

SBOM S.O.S.
6 Things to Do Right Now

Sonatype invented software supply chain management, and our data powers the world's leading SCA tool. Trusted by 266 government agencies, 478 financial services firms, and 60 Fortune 100 companies, we're applying our open-source expertise to Software Bill of Materials (SBOM) compliance and monitoring. If you're just starting this journey, these steps can help you stay compliant, reduce vulnerabilities, and gain immediate insight across your software portfolio.

Grasp the regulatory landscape

Familiarize yourself with **applicable industry standards** and government-mandated requirements for SBOMs. For example, in the US, when the White House issued Executive Order 14028 on Improving the Nation's Cybersecurity, multiple agencies were tasked with defining best practices for ensuring the security of software supply chains. As a result, the Department of Commerce, in coordination with the National Telecommunications and Information Administration (NTIA), defined the "**minimum elements**" necessary for an effective SBOM. The National Cybersecurity Strategy also promotes the adoption of SBOMs as vital to a secure software development lifecycle. Similar legislation is being adopted around the world. In Europe, the **Network and Information Systems Directive (NIS2), the Cyber Resiliency Act (CRA)**, and the **Digital Operational Resilience Act (DORA)** all recognize the importance of having a full understanding of the software components being used in an application.

Understand the scale of your SBOM management needs

The number of SBOMs an enterprise can expect to manage is substantial, driven by the volume of both internal and external applications, their release/update frequencies, and regulatory retention requirements. Managing SBOMs encompasses first-party software released internally, third-party and commercial off-the-shelf (COTS) software that provides SBOMs, and archived binaries or legacy systems that might be uncovered during an SBOM implementation. This can add up fast. For example, we know the average enterprise manages more than 6,000 applications. Updated or released 12 times a year, this would generate 72,000 SBOMs annually. It's likely that you also have specific retention periods to comply with. For example, in the US, for certain federal agencies, this period is 7 years, bringing the number of SBOMs required to more than 500,000. This means you need to plan to store and manage these documents at scale, and to plan for the amount of total SBOMs to grow over time.

Prioritize automation

SBOMs are not meant to be created, stored, and forgotten. But without automation, it's impossible to do anything with the sheer number of SBOMs created. Automation makes it possible to update your SBOMs regularly or after significant updates or changes, including adding new components, updating existing ones, and removing depreciating elements. Instead, consider an SBOM as a snapshot in time, continuously monitored to catch new vulnerabilities and intentionally malicious information. This approach is especially crucial for addressing zero-day scenarios and maintaining a secure and efficient software supply chain. Automating SBOM generation not only simplifies the development processes but also provides a holistic view of software supply chain health.

Integrate SBOMs into your software development lifecycle

Make SBOMs part of your standard SDLC process. Development teams need to see security as part of the solution instead of a gating factor, and getting their visibility into vulnerabilities earlier in the process will help. Building SBOM creation into the CI/CD pipeline and automatically generating a list of all open source or third-party dependencies makes the SBOM an artifact of each release, providing an immutable, historical record of all components and risks present at the time of release. Make this so much a part of your SDLC process that software only gets deployed if it has an SBOM.

Use SBOMs to your advantage

SBOMs aren't just another bureaucratic requirement; by providing a detailed breakdown of the packages and libraries included in an application, they provide an opportunity to build better software and identify vendors with better software. SBOMs make it easier to track issues and cross-reference those against a vulnerability database (for example, **NIST's National Vulnerability Database)** and take action to update or replace components that are flagged for policy violations or security risks. Vulnerabilities can be present in every level of your software stack, so regularly verifying the accuracy and completeness of the SBOM by comparing it against the actual software components deployed will help investigate and resolve discrepancies, resulting in better, more secure applications.

Protect your SBOMs, but get comfortable with the idea of sharing

Being subjected to SBOM regulations is unavoidable, which means sharing SBOMs with customers, partners, or regulatory bodies. This can be intimidating, but the right tools can make the process not just manageable but also give you the peace of mind that your software is in the best shape possible. For projects that use proprietary source code, consider limiting SBOM access to customers or qualified leads. But for open source projects, dependency information is already publicly available. Store SBOMs in a secure yet centralized and accessible location for compliance and vulnerability management and make a plan to limit access to authorized personnel or use access controls to ensure that only those who need access can view or modify it. You can also require digital signatures that provide a unique identifier to authenticate that the SBOM originates with you. Any changes to the SBOM will generate a new signature. Providing training for developers and stakeholders on the importance of security is another way to increase the sensitive mindset when it comes to SBOM management.

Speak to an SBOM expert today

Sonatype SBOM Manager can help users assess the contents of an SBOM against regulatory or industry compliance standards. This tool provides specific details about the location of the affected file, where the file is referred to in other areas of the software, and recommendations on the next actions.

The sense of urgency around SBOMs

Legislative compliance is just part of the reason why SBOMs are important. Software liability is another growing trend, and SBOMs are the only way to provide a detailed inventory of every component within an application. An SBOM is an organization's best defense against potential legal culpability by showing that proper security measures were in place and that third-party components were managed effectively.

The increased emphasis on the value of SBOMs and the importance of good SBOM management are foundational to protecting the software supply chain, but navigating the best way forward can be daunting.

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

sonatype