sonatype

Sonatype Security Research

Risk Management Framework and the Sonatype Platform

DoD Implementation Guide - NIST SP 800-53 Rev 5 / CNSSI 1253

Understanding the Framework: NIST RMF vs. DoD RMF

This document maps the Sonatype platform to the Department of Defense (DoD) Risk Management Framework (RMF) requirements. The objective is to clarify how these two key frameworks interrelate:

- **NIST RMF:** The seven-step cybersecurity framework by NIST for all U.S. federal agencies.
- **NIST SP 800-53:** Catalog of security and privacy controls; RMF selects controls from this catalog.
- **DoD RMF:** The DoD's specific RMF implementation, defined in DoDI 8510.01.
- **CNSSI 1253:** Defines mandatory NIST 800-53 control baselines for DoD and National Security Systems (NSS).

In short, the DoD RMF guides programs toward achieving an Authority to Operate (ATO), using NIST 800-53 controls with CNSSI 1253 baselines. The Sonatype platform automates and provides evidence for these controls.

Executive Summary

The Sonatype platform provides automated controls that help DoD programs achieve ATO under DoDI

8510.01. It delivers automated evidence and enforcement for mandatory controls from NIST SP 800-53 Release 5.2.0, particularly within the Supply Chain Risk Management (SR), System and Services Acquisition (SA), System and Information Integrity (SI), and Configuration Management (CM) control families.

This document references NIST SP 800-53 Release 5.2.0, published August 27, 2025, which includes enhancements to software update and patch management controls in response to Executive Order 14306. These updates strengthen requirements for software resiliency by design, developer testing, update deployment management, and software integrity validation.

As DoD systems increasingly depend on open-source and third-party components, a lack of proper supply chain management introduces mission risk. Sonatype directly addresses these SR controls, ensuring compliance and operational assurance.

More than **2,000 organizations**, including **70% of the Fortune 100**, and a blend of **DoD/Department of War (DoW), Intelligence , and Civilian agencies**, rely on Sonatype for software supply chain security.

Note: NIST RMF emphasizes automation in control assessment for speed, effectiveness, and continuous monitoring — all native capabilities of Sonatype.

Sonatype's capabilities directly address the software update security requirements emphasized in NIST SP 800-53 Release 5.2.0, which implements Executive Order 14306 guidance on strengthening the Nation's cybersecurity through improved software update practices and supply chain resilience.

Detailed Mapping: Supply Chain Risk Management Controls

Control ID	Control Requirement	Sonatype Platform Capability Mapping
SR-1	Develop, document, and disseminate supply chain risk management policy and procedures.	Sonatype Lifecycle: Policy-as-Code engine codifies risk policies. Lifecycle Policy Management: Pre-built, tunable policy templates. Audit Trail Generation: Documents enforcement actions. Compliance Reporting: Produces compliance evidence.

SR-2	Develop and maintain a supply chain risk management plan.	Sonatype Lifecycle: Continuous monitoring for real-time assessment. Sonatype SBOM Manager: Creates component inventories. Risk Dashboard: Centralized risk visibility. Automated Risk Scoring and Trend Analysis.
SR-3	Establish supply chain controls and protective processes.	Sonatype Repository Firewall: Blocks malicious/vulnerable components. Lifecycle Policy Engine: Automated enforcement. Component Intelligence Database: 40+ risk data sources. License & Vulnerability Detection: Ensures compliance.
SR-4	Maintain valid provenance of system components.	Sonatype Nexus Repository: Immutable storage with integrity checks. Component Signatures & Provenance Tracking. Sonatype SBOM Manager: Documents origins. Quarantine & Mirroring: Ensures the use of trusted sources.
SR-5	Employ acquisition strategies, contract tools, and procurement methods to protect against supply chain risks.	System Lifecycle Procurement Guidance: Provides real-time component risk assessments to inform acquisition decisions. Vendor Risk Assessment: Evaluates publisher and maintainer security posture. Cost-Risk Analysis: Quantifies security risk cost for procurement justification. Contract Language Support: Provides measurable data to include supply chain security clauses in contracts. **Supporting Products:** Sonatype Lifecycle, Sonatype Nexus Repository.
SR-6	Assess and review supply chain-related risks associated with suppliers or contractors.	Publisher Intelligence: Provides comprehensive insight into component publishers and maintainers. Supplier Risk Scoring: Automates assessment of supplier security practices. Community Health Metrics: Evaluates open source project activity, responsiveness, and sustainability. Maintenance Activity Tracking: Monitors frequency and quality of supplier updates. Supplier Performance Dashboard: Centralizes supplier risk data for periodic review. **Supporting Products:** Sonatype Lifecycle, Sonatype Repository Firewall, Intelligence Data Service, Sonatype Nexus Repository.
SR-7	Employ OPSEC controls for supply chain information.	Air-Gapped Deployment (SAGE). Role-Based Access & Audit Logging. Encryption & Secure Communication.
SR-8	Establish supply chain notification agreements.	Security Advisory Integration & Real-Time Alerting. Incident Response Integration & Stakeholder Notifications. Supporting Products: Sonatype Lifecycle, Sonatype Repository Firewall.
SR-9	Implement tamper resistance and detection.	Sonatype Repository Firewall: Blocks tampered components. Integrity Verification & Malware Detection. Behavioral Analysis: Detects anomalous activity.
SR-10	Inspect systems/ components for tampering.	Continuous Monitoring & Lifecycle Scanning. Change Detection & Forensics.

SR-11	Implement anti-counterfeit policy and training.	Sonatype Repository Firewall & Authenticity Verification. Digital Signature Validation & Typosquatting Detection.
SR-12	Dispose of components securely.	Sonatype Lifecycle Management: Tracks component lifecycles. Deprecation Alerts, Secure Removal & Migration Planning.

System and Services Acquisition (SA) Controls

NIST SP 800-53 Release 5.2.0 introduces enhanced controls in the SA family specifically addressing software development security and update management in response to Executive Order 14306.

Control ID	Control Requirement	Sonatype Platform Capability Mapping
SA-15(13)	Developer testing and evaluation plans for updates.	Sonatype Lifecycle: Continuous Integration/Continuous Deployment (CI/CD) integration provides automated testing and evaluation of components during updates. Policy Engine: Enforces quality and security gates before updates proceed. Continuous Monitoring: Validates updates against organizational security policies throughout the development lifecycle. **Note:** This control was added in Release 5.2.0 to address Executive Order 14306 requirements.
SA-24	Software and system resiliency by design.	Sonatype Repository Firewall: Blocks known malicious updates and compromised components before they enter the software supply chain. Policy-Compliant Component Selection: Automatically filters update requests to prevent selection of versions that violate security policies. Release Integrity: Machine learning-based detection identifies suspicious or unusual software releases with pending or suspicious integrity ratings. **Note:** This control was added in Release 5.2.0 to address Executive Order 14306 requirements.

Configuration Management (CM) Controls

Control ID	Control Requirement	Sonatype Platform Capability Mapping
CM-8	Maintain an accurate inventory of components.	Sonatype Lifecycle + Sonatype SBOM Manager: Centralized inventory and SBOM generation, ingestion, and continuous monitoring. Dependency Mapping & Enterprise Dashboard.
CM-10	Ensure software usage complies with DoD licensing.	Sonatype Lifecycle + Advanced Legal Pack: License analysis and policy enforcement. Conflict Detection & Compliance Reporting.
CM-5	Restrict access to change libraries.	Sonatype Nexus Repository: Controlled repositories.Change Control Logs & Approval Workflows.

System and Information Integrity (SI) Controls

Control ID	Control Requirement	Sonatype Platform Capability Mapping
SI-2	Track and remediate flaws enterprise-wide.	Sonatype Lifecycle: Identifies vulnerabilities. Remediation Tracking & Risk-Based Prioritization.
SI-02(07)	Software update deployment and management.	Sonatype Lifecycle for SCM: Provides automated pull requests for security updates with policy-compliant version recommendations. Automated Commit Feedback: Delivers real-time policy evaluation information directly into source control commits. SBOM Manager: Tracks software composition changes across updates with continuous monitoring for newly discovered vulnerabilities. Compliance Stage Monitoring: Provides dedicated monitoring for ongoing compliance verification post-deployment. **Note:** This control enhancement was added in Release 5.2.0 to address Executive Order 14306 requirements for secure software update practices.
SI-7	Verify software integrity.	Sonatype Nexus Repository + Sonatype Repository Firewall: Cryptographic integrity monitoring. Baseline Comparison & Integrity Alerts.

Risk Assessment (RA) and Incident Response (IR)

Control ID	Control Requirement	Sonatype Platform Capability Mapping
RA-5	Conduct vulnerability scanning and facilitate interoperability.	Sonatype Lifecycle: Specialized open-source scanning.Tool Integration with DISA & HBSS.
IR-6	Report vulnerabilities and provide supply chain info.	Sonatype SBOM Manager + Sonatype Lifecycle: Zero-day impact analysis. Rapid Response & Automated Reporting.

Configuration Management (CM) Controls

Accelerates ATO Process

- Sonatype Lifecycle and Sonatype SBOM Manager capabilities directly support the RMF process by generating a machine-readable SBOM. This SBOM file serves as the primary 'artifact' or evidence that is uploaded to eMASS.
- Continuous compliance with real-time monitoring.
- Audit trail generation for assessment and review.

Supports Mission Assurance

- Proactive protection against supply chain compromise.
- Zero-day response and rapid impact analysis.
- Air-gapped deployment options (SAGE) for IL6/IL6+ environments.

Enables DevSecOps Integration

- Native CI/CD Pipeline Integration.
- Seamless developer workflow alignment.
- Automation-first approach for efficiency and security.

Ensures Compliance

- Addresses CNSSI 1253 baselines for National Security Systems.
- Supports DoDI 8510.01 RMF implementation.
- Provides FISMA compliance evidence.
- FIPS 140-3 mode available for deployments requiring cryptographic module validation

Reduces Mission Risk

- AI-powered real-time protection blocks 2,100+ malicious components monthly.
- Comprehensive Threat Intelligence from 40+ data sources.
- Full Enterprise Visibility across DoD applications.
- VEX (Vulnerability Exploitability eXchange) integration for comprehensive vulnerability assessment andannotation workflows.