Prevalent™

A Guide to Simplify Supply Chain Reporting

The Top 15 NIST Supply Chain Risk Management Controls

Table of Contents

NIST and Supply Chain Risk Management **3**

The Top 15 Critical NIST SP 800-53 Controls for SCRM **3**

How Prevalent Helps **7**

About Prevalent **8**

NIST and Supply Chain Risk Management

The National Institute of Standards and Technology (NIST) is a federal agency within the United States Department of Commerce. NIST's responsibilities include establishing computer and information technology-related standards and guidelines for federal agencies. Because NIST publishes and maintains key resources for managing cybersecurity risks applicable to any company, many private sector organizations consider compliance with these standards and guidelines to be a top priority.

Several NIST special publications have specific controls that require organizations to establish and implement the processes to identify, assess and manage supply chain risk, among them SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. However, with more than 1,000 different controls available, identifying a starting point, or narrowing down which controls are considered critical, can be challenging.

Prevalent has identified the top 15 critical controls from SP 800-53 that all organizations can use as the starting point to build a strong supply chain cybersecurity framework.

The Top 15 Critical NIST SP 800-53 Controls for Supply Chain Risk Management

See the table below for a summary of each key control and important considerations.

	NIST Controls	Key Considerations
1	**RA-3: Risk Assessment** Conduct risk assessments, document the results and review and update the assessments at defined frequencies.	Build assessments using a clear framework for identifying, managing, monitoring, and responding to risks. Ensure that assessments consider internal and external threats, and are responsive to changes in the organization, its systems and external environmental conditions.
2	**RA-5: Vulnerability Monitoring & Scanning** Monitor and scan for vulnerabilities on systems and hosted applications. Consider tools and techniques to automate the process. Review scan reports and remediate actions.	Identify critical systems and networks and the level of scanning required for each. Use tools to improve the consistency and accuracy of reporting. Align the frequency of scanning with the criticality of systems and data being managed.
3	**SA-4: Acquisition Process** The NIST framework sets out requirements and criteria for identifying security and privacy controls within acquisition contracts for new systems. This includes functional and assurance requirements, documentation and criteria within development processes.	Ensure the implementation of minimum levels of security and privacy controls. Base controls on the organizations' risk assessments and risk appetite. Identify mechanisms needed to achieve minimum security standards to ensure the application of technical, administrative and physical controls.

	NIST Controls	Key Considerations
4	**SI-4: System Monitoring** Monitor systems to detect attacks and indicators of potential attacks, including unauthorized connections. Deploy monitoring capabilities and devices.	Consider internal and external monitoring when establishing a structured approach to monitoring the organizations' networks and systems. Also consider using intrusion detection tools and automated scanning for real-time analysis and to aid in rapid response to suspected attacks.
5	**AU-2: Event Logging** Identify types of events that systems are capable of logging, and establish a process for recording sufficient information to aid security alert notifications and response.	Include reporting on password changes, failed logons or failed access to systems. Consider administrator access, security or privacy changes and external credentials as well. Use a security information and event management (SIEM) application to help with analysis and reporting on security alerts.
6	**CM-8: System Component Inventory** Develop and document an inventory of system components that accurately reflects systems and contains sufficient information for effective accountability of all systems.	Use asset inventories to capture all organizational information system assets including the system name, software owners, software version numbers, hardware inventory specifications and software license information. Centralize the inventories and review them regularly to ensure accountability of critical assets.
7	**CM-3: Change Control** Determine and document configuration-controlled changes to systems. Retain records of changes, as well as monitored and reviewed change activities.	Clearly document system changes and follow a process for identifying, reviewing, reporting, and implementing changes. Indicate in change records what is to be changed, why and, when. Identify the impact of changes to wider systems and testing rollback procedures.
8	**SC-7: Boundary Protection** Monitor and control communications at external managed interfaces to the system and at key internal managed interfaces within the system.	Include the use of critical network components (e.g., gateways, routers and firewalls) for monitoring and controlling communications at external interfaces to systems. Limit external connections to systems, and set clear rules within security systems (e.g., deny-all, allow by exception rules, etc.).

	NIST Controls	Key Considerations
9	**IA-2: Identification and Authorization** Uniquely identify and authenticate users, including employees and contractors.	Identification and authentication methods can differ depending on the types of roles and systems or data being accessed. Employ a unique user ID for each employee or contractor as well as appropriate authentication, including passwords, multi-factor authentication techniques or biometrics.
10	**AC-3: Access Enforcement** Enforce approved authorization for logical access to information and system resources based on access control policies.	Grant access to information and system resources based on a defined access control policy that sets out the requirements for granting and revoking access, and necessary access restrictions. Use role-based access controls (RBAC) to simplify privilege administration.
11	**IR-4: Incident Handling and Response** Implement an incident handling capability, aligned to an incident response plan which includes preparation, detection and analysis, containment, eradication, and recovery.	A well-defined method for managing incidents includes establishing correct reporting and communication of incidents and should be managed by a defined group or set of roles. Include internal and external communication requirements, and methods of capturing incidents (e.g., events, actions taken, and lessons learned) in incident response processes.
12	**CP-2: Contingency Planning** Develop a contingency plan that is managed, coordinated, reviewed, updated and communicated.	Test contingency plans regularly to ensure that planned recovery objectives are achievable, and to identify gaps or additional controls or processes for full recovery and reconstitution.
13	**CP-4: Contingency Testing** Test the effectiveness of the contingency plan for systems using defined tests.	Include the use of critical network components (e.g., gateways, routers and firewalls) for monitoring and controlling communications at external interfaces to systems. Limit external connections to systems, and set clear rules within security systems (e.g., deny-all, allow by exception rules, etc.).

	NIST Controls	Key Considerations
14	**AT-2: Training and Awareness** Provide security and privacy training to system users.	Training and awareness form a critical component in ensuring all staff are aware of and follow security and privacy policies and practices. Conduct regular training on employee-specific controls. Consider different methods of training and awareness (e.g., internal marketing campaigns, practical exercises, etc.) to enhance employee knowledge.
15	**SR-2: Risk Management Plan** Develop, review, update and protect a supply chain risk management plan.	Create risk management plans to identify threats and vulnerabilities and calculate risks based on defined methodologies. Tailor plans to fit organizational risk policy and strategy, and update them to ensure risks and controls remain relevant to the organization.

How Prevalent Helps

The Prevalent Third-Party Risk Management (TPRM) Platform automates the critical tasks required to onboard, assess, manage, continuously monitor, and remediate third-party security, privacy, compliance, business resilience, incident response, and procurement-related risks across the vendor lifecycle.

The Prevalent solution delivers:

- Automated vendor onboarding and offboarding to help you keep up with business demands
- Profiling, tiering and inherent risk scoring for quick visibility into the risks new supply chain partners introduce to your organization and to right-size further due diligence
- Standard NIST and custom risk assessments with built-in workflow, tasks, and evidence management to ensure your team is collecting and analyzing the right information
- Continuous cybersecurity, business, reputational and financial risk monitoring to correlate risks against assessment results
- Machine learning analytics to normalize and correlate findings from multiple sources
- Compliance and risk reporting by framework or regulation to reduce the time required to meet auditor requests
- Remediation management with built-in guidance to accelerate risk reduction efforts
- A library of completed standardized risk assessments augmented by real-time risk metrics

The Prevalent TPRM Platform offers a complete framework for implementing policy management, auditing and reporting related to the third-party risk and supply chain compliance requirements of NIST SP 800-53 with a dedicated questionnaire and risk register, backed by third-party risk management expertise.

Contact Prevalent today for a free maturity assessment or request a demo to determine how your current TPRM policies stack up to these critical NIST controls.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the entire vendor lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.