Prevalent™

A Checklist for Compliance

NIST and Third-Party Risk Management

Table of Contents

NIST and Third-Party 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, nearly 50% of private sector organizations have also adopted their guidelines, making NIST publications the primary standards for evaluating IT controls.

Although several NIST special publications have specific controls that address third-party supplier IT security, the most applicable are:

- **SP 800-53 Rev. 5:** Security and Privacy Controls for Information Systems and Organizations
- **SP 800-161 Rev. 1:** Cybersecurity Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- **Cybersecurity Framework v1.1:** Framework for Improving Critical Infrastructure Cybersecurity

These guidelines complement one another, so your organization can standardize on one special publication can cross-map to the others – in effect meeting multiple requirements using a single framework.

This guide examines the applicable supply chain cybersecurity controls and guidance in NIST publications and identifies capabilities available in the Prevalent Third-Party Risk Management Platform that you can use to meet NIST requirements for stronger supply chain security.

Supply Chain Risk Management Controls in SP 800-53 Rev. 5

NIST supply chain security and data privacy controls have evolved with each SP 800-53 revision. For example, in SP 800-53 Rev. 4 Supply Chain Protection was covered under a broader "System & Service Acquisition" control group. This single control addressed the need to identify vulnerabilities throughout an information system's lifecycle, and to respond through strategy and controls. It encouraged organizations to procure third-party solutions to implement security safeguards. It also required organizations to review and assess suppliers and their products prior to engagement for broader supply chain visibility.

Acknowledging the increasing number of third-party supplier-related data breaches and other security events, SP 800-53 Rev. 5 expands and refines the supply chain security and privacy guidelines by establishing an entirely new control group, "SR-Supply Chain Risk Management." It also requires organizations to develop and plan for managing supply chain risks by:

- Using formal risk management plans and policies to drive the supply chain management process
- Emphasizing security and privacy through collaboration in identifying risks and threats, and through the application of security and privacy-based controls
- Requiring transparency of systems and products (e.g., lifecycle, traceability, and component authenticity)
- Increasing awareness of the need to pre-assess organizations, and to ensure visibility into issues and breaches

How SP 800-161 Rev. 1 Complements Supply Chain Risk Management

NIST SP 800-53 is considered the foundation upon which all other cybersecurity controls are built. With SP 800-161 Rev. 1, NIST outlines a complementary framework to frame, assess, respond to, and monitor cybersecurity supply chain risks.

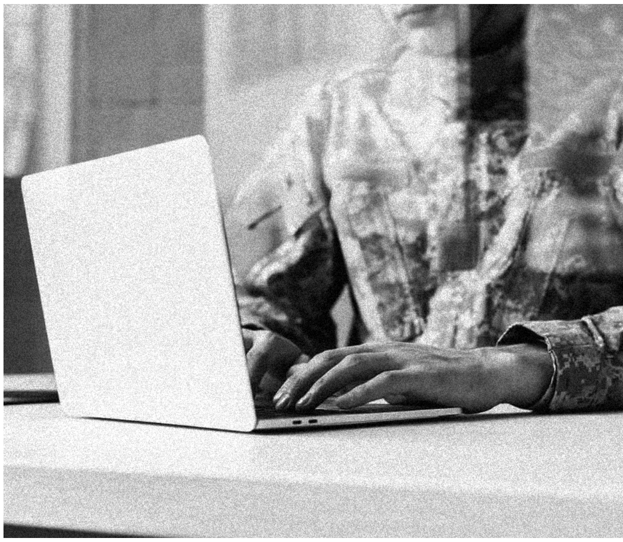
SP 800-161 further identifies the following dimensions that form the framework of cybersecurity supply chain management:

- Culture and Awareness
- Security
- Suitability
- Safety
- Reliability
- Usability
- Quality
- Efficiency
- Maintainability
- Integrity
- Scalability
- Resilience

Together, SP 800-53 and supplemental SP 800-161 control guidance present a comprehensive framework for assessing and mitigating supplier cybersecurity risks.

Supply Chain Risk Management Requirements in the Cybersecurity Framework v1.1

The Cybersecurity Framework is another NIST publication that applies to third-party risk management and supply chain security. The Framework leverages existing security frameworks, such as CIS, COBIT, ISA, ISO/IEC and NIST, to avoid creating an undue burden on organizations to address requirements. Specific supply chain risk management subcategories identified in the CSF include:



- **ID.SC-1:** Identify, establish, assess, and manage cyber supply chain risk management processes, and ensure that organizational stakeholders agree.
- **ID.SC-2:** Identify, prioritize, and assess suppliers and third-party partners of information systems, components, and services using a cyber supply chain risk assessment process.
- **ID.SC-3:** Implement appropriate measures in supplier and third-party partner contracts to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- **ID.SC-4:** Routinely assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- **ID.SC-5:** Conduct response and recovery planning and testing with suppliers and third-party providers.

The next section of this checklist cross-maps applicable supplier risk management guidance between these three NIST publications.

Mapping Prevalent Capabilities to NIST Cybersecurity Supply Chain Risk Management Control Requirements

The summary table below maps capabilities available in the Prevalent Third-Party Risk Management Platform to select third-party vendor or supplier controls present in SP 800-53, with SP 800-161 and the Cybersecurity Framework v1.1 control overlays (**bolded**) applied to the table to illustrate cross-mapping.

NOTE: *This table should not be considered definitive guidance. For a complete list of controls, please review the complete SP 800-53, SP 800-161 and Cybersecurity Framework v1.1 requirements in detail and consult your auditor.*

Table 1. Prevalent Mappings to NIST Cybersecurity Supply Chain Risk Management-Related Controls

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

<table>
<tr><th>Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1</th><th>Prevalent Third-Party Risk Management Platform Capabilities</th></tr>
<tr><td colspan="2"><b>CA-2 (1)</b> Control Assessments | Specialized Assessments
<b>Supplemental C-SCRM Guidance:</b> Enterprises should use a variety of assessment techniques and methodologies, such as continuous monitoring, insider threat assessment, and malicious user assessment. These assessment mechanisms are context-specific and require the enterprise to understand its supply chain and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.
<b>CA-2 (3)</b> Control Assessments | Leveraging Results from External Organizations
<b>Supplemental C-SCRM Guidance:</b> For C-SCRM, enterprises should use external security assessments for suppliers, developers, system integrators, external system service providers, and other ICT/OTrelated service providers. External assessments include certifications, third-party assessments, and – in the federal context – prior assessments performed by other departments and agencies. Certifications from the International Enterprise for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology Forum (OTTF) may also be used by non-federal and federal enterprises alike, if such certifications meet agency needs.</td></tr>
</table>

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
Control Assessments | Specialized Assessments Continued ID.RA-1: Asset Vulnerabilities are identified and documented. DE.DP-4: Event detection information is communicated.	The Prevalent Third-Party Risk Management Platform includes more than 100 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that automatically maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls. Prevalent Vendor Threat Monitor (VTM) continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform by monitoring the Internet and dark web for cyber threats and vulnerabilities. It also correlates assessment findings with research on operational, financial, legal and brand risks in a unified risk register that enables centralized risk triage and response. With the Prevalent Platform, you can efficiently communicate with vendors and coordinate remediation efforts. Capture and audit conversations; record estimated completion dates; accept or reject submissions on an answer-by-answer basis; assign tasks based on risks, documents or entities; and match documentation and evidence to risks.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
CA-7 (3) Continuous Monitoring | Trend Analyses **Supplemental C-SCRM Guidance:** The information gathered during continuous monitoring/trend analyses serves as input into C-SCRM decisions, including criticality analysis, vulnerability and threat analysis, and risk assessments. It also provides information that can be used in incident response and potentially identify a supply chain cybersecurity compromise, including an insider threat.	
ID.RA-1: Asset Vulnerabilities are identified and documented. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors. DE.CM-1: The network is monitored to detect potential cybersecurity events. RS.AN-1: Notifications from detection systems are investigated. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked companies by monitoring 1,500+ criminal forums; thousands of onion pages, 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

<table>
<tr><th>Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1</th><th>Prevalent Third-Party Risk Management Platform Capabilities</th></tr>
<tr><td colspan="2">**CP-2 (3)** Contingency Plan | Coordinate with External Service Providers
Supplemental C-SCRM Guidance: Enterprises should ensure that the supply chain network, information systems, and components provided by an external service provider have appropriate failover (to include personnel, equipment, and network resources) to reduce or prevent service interruption or ensure timely recovery. Enterprises should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms that address critical components and functionality support in case of denial-of-service attacks to ensure the continuity of operations. Enterprises should coordinate with external service providers to identify service providers' existing contingency plan practices and build on them as required by the enterprise's mission and business needs. Such coordination will aid in cost reduction and efficient implementation. Enterprises should require their prime contractors who provide a mission- and business-critical or -enabling service or product to implement this control and flow down this requirement to relevant sub-tier contractors.</td></tr>
<tr><td>ID.BE-1: The organization's role in the supply chain is identified and communicated.
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
DE.AE-4: Impact of events is determined.
RS.RP-1: Response plan is executed during or after an incident.
RS.CO-3: Information is shared consistent with response plans.
RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
RS.AN-2: The impact of the incident is understood.
RS.AN-4: Incidents are categorized consistent with response plans.
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.</td><td>The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact of supply chain breaches by centrally managing vendors, proactively conducting event assessments, scoring identified risks, and accessing remediation guidance.
The Prevalent Platform includes unified capabilities for assessing, analyzing and addressing weaknesses in supplier business resilience plans. This enables you to proactively work with your supplier community to prepare for pandemics, environmental disasters, and other potential crises.
In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals.
All risk intelligence is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.</td></tr>
</table>

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

<table>
<tr><th>Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1</th><th>Prevalent Third-Party Risk Management Platform Capabilities</th></tr>
<tr><td colspan="2"><b>IR-4 (3)</b> Incident Handling | Supply Chain Coordination

<b>Supplemental C-SCRM Guidance:</b> A number of enterprises may be involved in managing incidents and responses for supply chain security. After initially processing the incident and deciding on a course of action (in some cases, the action may be “no action”), the enterprise may need to coordinate with their suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, root cause, and corrective actions. Enterprises should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers with mature capabilities for supporting supply chain cybersecurity incident handling is important for reducing exposure to cybersecurity risks throughout the supply chain. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A review (and potential revision) of the agreement is recommended, based on the lessons learned from previous incidents. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.</td></tr>
<tr><td><b>ID.SC-5:</b> Response and recovery planning and testing are conducted with suppliers and third-party providers.

DE.AE-2: Detected events are analyzed to understand attack targets and methods.

DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

DE.AE-4: Impact of events is determined.

DE.AE-5: Incident alert thresholds are established.

RS.RP-1: Response plan is executed during or after an incident.

RS.CO-3: Information is shared consistent with response plans.</td><td>The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, proactively conducting event assessments, scoring identified risks, and accessing remediation guidance.

The Prevalent Platform includes unified capabilities for assessing, analyzing and addressing weaknesses in supplier business resilience plans. This enables you to proactively work with your supplier community to prepare for pandemics, environmental disasters, and other potential crises.

In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals.

All risk intelligence is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.</td></tr>
</table>

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
Incident Handling | Supply Chain Coordination Continued RS.CO-4: Coordination with stakeholders occurs consistent with response plans. RS.AN-1: Notifications from detection systems are investigated. RS.AN-2: The impact of the incident is understood. RS.AN-4: Incidents are categorized consistent with response plans. RS.MI-2: Incidents are mitigated. RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	*(See previous page.)*
IR-5 Incident Monitoring **Supplemental C-SCRM Guidance:** Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, response decisions, and activities.	Prevalent Contract Essentials is a SaaS solution that centralizes the distribution, discussion, retention, and review of vendor contracts. It also includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With Contract Essentials, your procurement and legal teams have a single solution to ensure that key contract clauses are in place, and that service levels and response times are managed.
IR-6 (1) Incident Reporting | Supply Chain Coordination **Supplemental C-SCRM Guidance:** Communications of security incident information from the enterprise to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and vice versa require protection. The enterprise should ensure that information is reviewed and approved for sending based on its agreements with suppliers and any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly defined in the agreement. The enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
Incident Reporting | Supply Chain Coordination Continued **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. RS.CO-2: Incidents are reported consistent with established criteria.	All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
IR-8 Incident Response Plan **Supplemental C-SCRM Guidance:** Enterprises should coordinate, develop, and implement an incident response plan that includes information-sharing responsibilities with critical suppliers and, in a federal context, interagency partners and the FASC. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance. The Incident Response Service provides the foundation to be well prepared for board and executive questions regarding the impact of supply chain incidents; and demonstrate proof of your third-party breach response plan with auditors and regulators.
PM-16 Threat Awareness Program **Supplemental C-SCRM Guidance:** When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the organization's information sharing policy.	
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources. ID.RA-3: Threats, both internal and external, are identified and documented. ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked companies by monitoring 1,500+ criminal forums; thousands of onion pages, 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
PM-31 Continuous Monitoring Strategy **Supplemental C-SCRM Guidance:** The continuous monitoring strategy and program should integrate C-SCRM controls at Levels 1, 2, and 3 in accordance with the Supply Chain Risk Management Strategy.	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked companies by monitoring 1,500+ criminal forums; thousands of onion pages, 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
RA-1 Policy and Procedures **Supplemental C-SCRM Guidance:** Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be defined.	The Prevalent Platform includes more than 100 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls. With the Prevalent Platform, you can automatically generate a risk register upon survey completion, ensuring that the entire risk profile (or a role-specific version) can be viewed in the centralized, real-time reporting dashboard – and reports can be downloaded and exported to determine compliance status. This filters out unnecessary noise and zeroes in on areas of possible concern, providing visibility and trending to measure program effectiveness. Then, you can take actionable steps to reduce vendor risk with built-in remediation recommendations and guidance.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

<table>
<tr><th>Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1</th><th>Prevalent Third-Party Risk Management Platform Capabilities</th></tr>
<tr><td colspan="2"><b>RA-3</b> Risk Assessment
<b>Supplemental C-SCRM Guidance:</b> Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments, which are performed as ongoing activities throughout the SDLC, and processes should be appropriately aligned with or integrated into ERM processes and governance.</td></tr>
<tr><td>ID.RA-1: Asset Vulnerabilities are identified and documented.
ID.RA-3: Threats, both internal and external, are identified and documented.
ID.RA-4: Potential business impacts and likelihoods are identified.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
<b>ID.SC-2:</b> Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
CSF DE.AE-4: Impact of events is determined.
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.</td><td>The Prevalent Platform includes more than 100 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls. Prevalent offers security, privacy, and risk management professionals an automated platform to manage the vendor risk assessment process and determine vendor compliance with IT security, regulatory, and data privacy requirements.
In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform also provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals.
All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.</td></tr>
</table>

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
RA-7 Risk Response **Supplemental C-SCRM Guidance:** Enterprises should integrate capabilities to respond to cybersecurity risks throughout the supply chain into the enterprise's overall response posture, ensuring that these responses are aligned to and fall within the boundaries of the enterprise's tolerance for risk. Risk response should include consideration of risk response identification, evaluation of alternatives, and risk response decision activities.	The Prevalent Platform features built-in guidance to remediate control failures or other identified risks to levels acceptable to your organization. Prevalent also enables risk assessors to communicate with third parties about remediations, document conversations and updates, and store supporting control documentation in a centralized repository.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
RA-9 Criticality Analysis **Supplemental C-SCRM Guidance:** Enterprises should complete a criticality analysis as a prerequisite input to assessments of cybersecurity supply chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a highquality criticality analysis, enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should also refer to Appendix F to supplement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Prevalent offers an inherent risk assessment questionnaire with clear scoring based on eight criteria to capture, track and quantify risks for all third parties. The assessment criteria include: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation Using the inherent risk assessment, you can automatically tier suppliers, set appropriate levels of further diligence, and determine the scope of subsequent, periodic assessments. Rule-based tiering logic enables suppliers to be categorized based on a range of data interaction, financial, regulatory and reputational considerations.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SA-4 (3) Acquisition Process | Continuous Monitoring Plan for Controls **Supplemental C-SCRM Guidance:** This control enhancement is relevant to C-SCRM and plans for continuous monitoring of control effectiveness and should therefore be extended to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	
PR.IP-2: A System Development Life Cycle to manage systems is implemented. DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform also provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SI-4 (1) System Monitoring | Integrated Situational Awareness **Supplemental C-SCRM Guidance:** System monitoring information may be correlated with that of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, if appropriate. The results of correlating monitoring information may point to supply chain cybersecurity vulnerabilities that require mitigation or compromises.	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors. DE.AE-4: Impact of events is determined. DE.CM-1: The network is monitored to detect potential cybersecurity events. DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events. DE.DP-4: Event detection information is communicated. RS.CO-3: Information is shared consistent with response plans. RS.AN-1: Notifications from detection systems are investigated.	Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform by monitoring the Internet and dark web for cyber threats and vulnerabilities — and correlating assessment findings with research on operational, financial, legal and brand risks in a unified risk register that enables centralized risk triage and response. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

<table>
<tr><th>Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1</th><th>Prevalent Third-Party Risk Management Platform Capabilities</th></tr>
<tr><td colspan="2">**SI-5** Security Alerts, Advisories and Directives
Supplemental C-SCRM Guidance: The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation’s Cybersecurity.</td></tr>
<tr><td>ID.RA-1: Asset Vulnerabilities are identified and documented.
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.
ID.RA-3: Threats, both internal and external, are identified and documented.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).</td><td>Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform by monitoring the Internet and dark web for cyber threats and vulnerabilities — and correlating assessment findings with research on operational, financial, legal and brand risks in a unified risk register that enables centralized risk triage and response.
All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.</td></tr>
</table>

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SR-1 Policy and Procedures **Supplemental C-SCRM Guidance:** C-SCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Prevalent Program Design Services define and document your third-party risk management program. You get a clear plan that accounts for your specific needs while incorporating best practices for end-to-end TPRM.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SR-2 Supply Chain Risk Management Plan **Supplemental C-SCRM Guidance:** C-SCRM plans describe implementations, requirements, constraints, and implications at the system level. C-SCRM plans are influenced by the enterprise's other risk assessment activities and may inherit and tailor common control baselines defined at Level 1 and Level 2. C-SCRM plans defined at Level 3 work in collaboration with the enterprise's C-SCRM Strategy and Policies (Level 1 and Level 2) and the C-SCRM Implementation Plan (Level 1 and Level 2) to provide a systematic and holistic approach for cybersecurity supply chain risk management across the enterprise. C-SCRM plans should be developed as a standalone document and only integrated into existing system security plans if enterprise constraints require it.	Prevalent Program Design Services help you to continually improve your Prevalent Platform deployment, ensuring that your TPRM program maintains the flexibility and agility it needs to meet evolving business and regulatory requirements.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SR-6 Supplier Assessments and Reviews **Supplemental C-SCRM Guidance:** In general, an enterprise should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier or their provided services or products. Enterprises should consider applying this information against a consistent set of core baseline factors and assessment criteria to facilitate equitable comparison (between suppliers and over time). Depending on the specific context and purpose for which the assessment is being conducting, the enterprise may select additional factors. The quality of information (e.g., its relevance, completeness, accuracy, etc.) relied upon for an assessment is also an important consideration. Reference sources for assessment information should also be documented. The C-SCRM PMO can help define requirements, methods, and tools for the enterprise's supplier assessments. Departments and agencies should refer to Appendix E for further guidance concerning baseline risk factors and the documentation of assessments and Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	The Prevalent Platform includes more than 100 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security and business resilience controls. Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform by monitoring the Internet and dark web for cyber threats and vulnerabilities — and correlating assessment findings with research on operational, financial, legal and brand risks in a unified risk register that enables centralized risk triage and response.

SP 800-53r5 Control Number and Name Applicable to SP 800-161r1 Cybersecurity Supply Chain Risk Management

Applicable Supply Chain-Specific Control Cross-Mapping to CSF v1.1	Prevalent Third-Party Risk Management Platform Capabilities
SR-8 Notification Agreements **Supplemental C-SCRM Guidance:** At minimum, enterprises should require their suppliers to establish notification agreements with entities within their supply chain that have a role or responsibility related to that critical service or product. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	With the Prevalent Platform, you can collaborate on documents, agreements and certifications, such as NDAs, SLAs, SOWs and contracts, with built-in version control, task assignment and auto-review cadences. Manage all documents throughout the vendor lifecycle in centralized vendor profiles.
SR-13 Supplier Inventory **Supplemental C-SCRM Guidance:** Enterprises rely on numerous suppliers to execute their missions and functions. Many suppliers provide products and services in support of multiple missions, functions, programs, projects, and systems. Some suppliers are more critical than others, based on the criticality of missions, functions, programs, projects, systems that their products and services support, and the enterprise's level of dependency on the supplier. Enterprises should use criticality analysis to help determine which products and services are critical to determine the criticality of suppliers to be documented in the supplier inventory. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.	Prevalent offers an inherent risk assessment questionnaire with clear scoring based on eight criteria to capture, track and quantify risks for all third parties. Assessment criteria include: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation Using the inherent risk assessment, you can automatically tier suppliers, set appropriate levels of further diligence, and determine the scope of subsequent, periodic assessments. Rule-based tiering logic enables suppliers to be categorized based on a range of data interaction, financial, regulatory and reputational considerations.

Summary Guidelines and Recommendations

To address the supply chain risk management control requirements established in SP 800-53, use the Cybersecurity Framework v1.1 supplemental guidance and consider implementing the following practices.

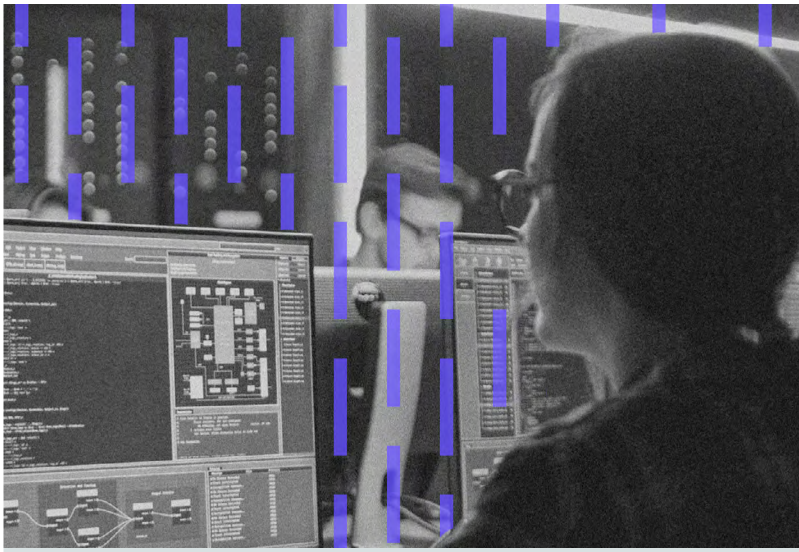
Table 2. Recommendations to Address CSF v1.1 Guidelines

NIST CSF v1.1 Summary Guidelines	Recommendations
Identify, establish, assess, and manage cyber supply chain risk management processes, and ensuring organizational stakeholders agree.	Define and document your third-party risk management program with expert professional services. Obtain a clear plan that accounts for your specific needs while incorporating best practices for end-to-end TPRM.
Identify, prioritize, and assess suppliers and third party partners of information systems, components, and services using a cyber supply chain risk assessment process.	Onboard, profile, tier and score inherent risks across all third parties as a critical first step in the onboarding and prioritization stages of the vendor lifecycle.
Implement appropriate measures in supplier and third-party partner contracts to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Use dedicated and custom contract assessment questionnaires to enable comprehensive reviews by identifying potential breaches of contract and other risks. Customizable surveys make it easy to gather and analyze necessary performance and contract data in a single risk register.
Routinely assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Use a comprehensive solution to address all information security topics as they pertain to supply chain partner security controls.
Conduct response and recovery planning and testing with suppliers and third-party providers.	Identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting proactive event assessments, scoring identified risks, and accessing remediation guidance.

The Prevalent Difference

NIST requires robust management and tracking of third-party supply chain security risks. SP 800-53, SP 800-161, and CSF v1.1 specify that a policy for managing risk should be in place; security controls should be selected; a policy should be codified in supplier agreements where appropriate; and suppliers should be managed and audited to the requirements and controls. In short, organizations need to establish and implement the processes to identify, assess and manage supply chain risk.

Prevalent can help by:



- Formalizing your third-party risk management program with industry best-practice guidance, adding consistency and repeatability to how you identify, manage, remediate and monitor supply chain risks across the vendor lifecycle
- Reducing the cost and complexity of third-party risk management with a managed services team that can handle vendor onboarding, assessment and management
- Comprehensively assessing vendors against NIST requirements and many other regulations, guidelines and frameworks – as well through an extensive survey template library
- Continuously monitoring your third parties for cybersecurity, business, reputational or financial risks that can impact their ability to deliver products and services
- Delivering the reporting required to demonstrate compliance inside and outside the organization
- Accelerating incident response by rapidly identifying and mitigating the impact of supply chain breaches through event collection, scoring identified risks, and accessing remediation guidance

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

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 and suppliers throughout the third-party 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.