[ISP Vendor Name]

CYBER SUPPLY CHAIN RISK MANAGEMENT PLAN

Version: V1.4
Version Date: [DD Month YYYY]

Prepared by: Employee Name, Title, Company Name
Employee Name, Title, Company Name
Employee Name, Title, Company Name

TEMPLATE OVERVIEW

***[INSTRUCTIONS:** The "Template Overview" section is intended to be instructional and can be deleted up on completion of the subgrantees completion of their Cyber Supply Chain Risk Management Plan.]*

Template Revision History

The following table shall be used to track authorship for any changes, modifications, or updates to this document.

Table 0-1: Document Revision History

Version	Date	Description of Change	Author
1.0	11/28/23	Template	Commonwealth of Virginia
1.4	10/21/2024	Revise for NIST 2.0	Commonwealth of Virginia

Template Introduction

The purpose of this template is for the Commonwealth of Virginia to provide this document as an accelerator for Internet Service Providers (ISPs) to help them define, document, and disseminate a Cyber Supply Chain Risk Management Plan ("C-SCRM Plan"). Use of this document or the associated checklist are not required. Organizations with existing Cyber Supply Chain Risk Management Plans can continue to use the existing documentation, provided it meets the requirements outlined in the ***National Institute of Standards and Technology (NIST) Interagency or Internal Reports (NISTIR) 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*** and ***National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.***

Document Components

The following outlines the key elements of this template and how to update the document appropriately.

Instructions

Instructions are included in this document to provide clarity, further guidance, and additional resources for the associated phase of the document. The instructions are not intended for direct use within the final program document and should be removed before the document is finalized.

For the purposes of this document, all instructions are written in italicized red text. The end of all instructions will include a reminder that this text should be removed from the document. Below is a visual example of the instructions found in this document.

***[INSTRUCTIONS:** This will provide additional clarity on how to compose that section of the document.*

Delete this instruction and all other instructions from your final version of the document.]

Example Text

Examples are included in this document as an initial starting point for the authors of the final program document. These excerpts may be included in the final program document, but should be reviewed, updated, and customized to the ISP Vendor's specific organization. While example text may be included in the final program document, the example tag at the beginning should be removed.

For purpose of this document, all examples are prefixed by the word "example" in bold, blue, all capital letters contained within square brackets, while the text itself should appear normal. This example tag should be removed throughout the document. Below is a visual example of the example tag found in this document.

[EXAMPLE] This text is an example of the content that may be contained after an example tag.

Update Tags

Update tags are included in this document to provide visual highlights for information that needs to be customized for the ISP Vendor's specific organization or where more information is needed.

For purpose of this document, all update tags are highlighted in yellow. These are the only highlights in the document. Sections that require generation of new content rather than minor revisions will be tagged with the word "update" in bold, black, all capital letters contained within square brackets. Below is a visual example of the update tag found in this document.

[UPDATE]

Implementation Summary Tables

At the beginning of each phase of the NIST C-SCRM program leveraged in this document, an Implementation Summary table has been included where the authors of this document can report on the overall implementation and operationalization of the associated phase of the program. This table includes four (4) key pieces of information:

- **Implementation Status** – describes the status of the operationalization of the controls.
- **Responsible Role** – the title of the organizational role responsible for ensuring the implementation and operationalization of the plan as well as maintaining and updating this section of the plan. Note: Titles are used in lieu of personnel names as the role should still be responsible with staff turnover.
- **Implementation Plan** – If the controls are not fully implemented and operationalized, a timeline and remediation steps should be clearly defined.
- **Planned Date for Full Implementation** – If the controls are not fully implemented and operationalized, the intended date for full implementation should be listed. If the controls are already implemented, this date should reflect the date the program was successfully established and operationalized as defined.

The following describes the listed implementation statuses:

- **Implemented** – The program has been fully operationalized as documented.
- **Partially Implemented** – Some parts of the program have been operationalized, but work is still in progress for full implementation.

- **Planned** – The plan for the control has been clearly defined and documented in the plan, but the organization has not begun to operationalize the defined program.
- **Alternative Implementation** – The control cannot be implemented as intended or designed, but compensating controls have been established to provide equivalent or better protection. Controls with alternative implementation should have a documented explanation in the Implementation Plan.
- **Not Applicable** – The control does not apply to the specific in scope environment. Controls that are not applicable should have a documented explanation in the Implementation Plan.

For purpose of this document, all implementation summary tables can be found at the beginning of each section as applicable. Below is a visual example of the update tag found in this document.

Table 0-2: EXAMPLE Implementation Summary

EXAMPLE Implementation Summary			
Implementation Status (check all that apply):		**Responsible Role:**	
☐ Implemented ☐ Partially Implemented ☐ Planned	☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)]	
Implementation Plan			**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]			DD Month YYYY

Key Terminology Definitions

At the end of this document, there is a table for all key terminology and definitions. Organizations may leverage the NIST, IR 7298, Revision 1, Glossary of Key Information Security Terms or the NIST Computer Security Resource Center (CSRC) Glossary found at https://csrc.nist.gov/glossary.

Document Updates

The Commonwealth of Virginia shall ensure that the latest version of the template is available at: [insert link].

Attached Checklist

When compiling the C-SCRM Plan, the "BEAD Cyber Supply Chain Risk Management Plan Checklist" can be used as guidance for developing a Cyber Supply Chain Risk Management strategy that meets NOFO requirements and incorporates leading practices. This checklist can be used to confirm that all applicable sections have been included in the C-SCRM Plan. The checklist contains:

- Topics included in Cyber Supply Chain Risk Management Plans; these topics correspond to sections in this Plan template.
- Steps to incorporate into the C-SCRM Plan, which specify content that should be detailed in the C-SCRM Plan.
- NOFO requirement verbiage, NOFO source references, and additional reference materials, as applicable, which provide additional context on the requirements.

DOCUMENT MAINTENANCE

[ISP Vendor] shall ensure that this document reviewed and updated at least annually and following any system update that affects the accuracy of the information contained within. If the plan is substantially updated, [ISP Vendor] must resubmit the information to the Commonwealth of Virginia within 30 days of revision.

Document Revision History

The following table shall be used to track authorship for any changes, modifications, or updates to this document.

Table 0-1: Document Revision History

Version	Date	Description of Change	Author
0.0	11/15/23	Template	Commonwealth of Virginia
1.0	##/##/##	Initial Draft	[Named Authors]

Document Approval History

This document shall be reviewed and updated at least annually or upon significant organizational change. [ISP Vendor] designates the [ISP Vendor] [Document Approvers] as the organizationally defined official(s) to manage the development, documentation, and dissemination of this plan. Their review and approval are required for all changes to this document and shall be tracked in the following table.

Table 0-2: Document Approval History

Version	Date	Documented Approver(s)
1.0	##/##/##	[Responsible Role], [Name of Personnel] [Responsible Role], [Name of Personnel]

Document Dissemination

This Cyber Supply Chain Risk Management Plan shall be stored and disseminated to [ISP Vendor] personnel through [insert technology name] under [Folder Name, if applicable].

Questions, comments, or concerns regarding this document should be directed to [Document Approvers (include contact information)].

Table of Contents

List of Tables

1 DOCUMENT OVERVIEW

1.1 Background

***[INSTRUCTIONS:** This section should include a summary of why Cyber Supply Chain Risk Management is important to the organization. In outlining the need for a robust Cyber Supply Chain Risk Management strategy, this section may include:*

- *the role that suppliers play in the global supply chain*
- *the role that suppliers play in supporting key business processes at the organization*
- *the organization's role in the supply chain*
- *the benefits of fostering strong supplier relationships*
- *the threats and risks that can arise from supplier relationships and the importance of mitigating supplier risk*
- *industry, third-party and/or compliance requirements relevant to Cyber Supply Chain Risk Management*
- *the impact of an adverse cybersecurity event at a supplier on business processes, sensitive data, critical systems and/or personnel*
- *how Cyber Supply Chain Risk Management supports the organization's business objectives*

This section should state that because of these factors, the organization has established a Cyber Supply Chain Risk Management Plan, which is outlined in the remainder of this document.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] This Cyber Supply Chain Risk Management (C-SCRM) Plan provides definitive information on the prescribed measures used to establish and enforce the C-SCRM Plan for [ISP Vendor].

The interdependence of organizations and their suppliers is a hallmark of modern business, and, while this connectedness has many benefits, it also has many risks. For example, threat actors who compromise vendors or exploit third party vulnerabilities can use this as an entry point into other organizations. Likewise, organizations who entrust any of their data to third parties could be exposed by a data breach at that third party. Additionally, an organization's business may be negatively impacted when its suppliers experience a business interruption, cyber incident, or disaster. It may also be increasingly difficult for organizations to maintain visibility and control over their own supply ecosystems. As such, use of a supplier increases the need for oversight of the process.

[ISP Vendor] relies on third parties to provide products and services that support critical business functions. Furthermore, [ISP Vendor] also plays an important role in the supply chain for its customers. Hence, managing risk in the supply chain (both upstream and downstream) helps ensure [ISP Vendor] can deliver on its brand promise.

As part of a holistic cybersecurity risk management strategy, [ISP Vendor] must account for the role that third parties play in supporting the business and the potential risks they introduce and manage these relationships through a Cyber Supply Chain Risk Management strategy.

The key to the effective use of a supplier is for [ISP Vendor] to appropriately assess, measure, monitor, and mitigate risks associated with the relationship. This includes reputational, operational, financial, compliance, and cyber risks. [ISP Vendor] is committed to responsibly managing activities conducted by

its suppliers, identifying, and controlling the risks arising from such relationships, and ensuring compliance to applicable regulations has been achieved.

An effective C-SCRM strategy is a team effort involving the participation and support of every [ISP Vendor] user who is involved in any stage of the supplier relationship. Therefore, it is the responsibility of these users to know these policies and to conduct their activities accordingly.

[UPDATE]

1.2 Purpose

[INSTRUCTIONS: *This section should outline the purpose of the Cyber Supply Chain Risk Management Plan, which may reference a desire to identify, track, mitigate and manage supplier risks. The goal of this section is to establish the risk-based foundation upon which the organization manages its supplier relationships.*

This section should also outline how the organization is implementing and supporting this Cyber Supply Chain Risk Management Plan—i.e., by implementing controls aligned to an industry framework (such as the National Institute of Standards and Technology [NIST] Interagency or Internal Reports [NISTIR] 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry and National Institute of Standards and Technology [NIST] Special Publication [SP] 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations); documenting supporting policies, procedures, and standards; socializing C-SCRM best practices and educating personnel at all levels; etc.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] The purpose of this Cyber Supply Chain Risk Management Plan is to support the overall cybersecurity posture, outline the Cyber Supply Chain Risk Management requirements and prescribe a comprehensive framework as follows:

- Create C-SCRM program based on the ***National Institute of Standards and Technology (NIST) Interagency or Internal Reports (NISTIR) 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations***.
- Integrate cybersecurity objectives into the entirety of the supplier relationship.
- Outline a strategy for identifying, assessing, and mitigating cyber supply chain risks.
- Manage supplier relationships on an ongoing basis, beginning with sound due diligence prior to entering into the relationship and continuing with robust monitoring of the relationship.
- Protect the confidentiality, integrity, and availability of any [ISP Vendor] data and systems that may be impacted by suppliers.
- Cultivate strong relationships with suppliers who support key business processes at [ISP Vendor].
- Structuring the supply chain in a way that helps ensure business resiliency.

This plan, including the related policies, standards, procedures, and guidelines, are necessary to support the management of supplier risks in daily operations. The development of policies provides due care to ensure that [ISP Vendor] users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help [ISP Vendor] comply with current and future legal obligations to ensure long-term due diligence.

[UPDATE]

1.3 Scope

***[INSTRUCTIONS:** This section should define the scope of Cyber Supply Chain Risk Management practices across the organization. When drafting this section, consider what would fall under the purview of centralized Cyber Supply Chain Risk Management. Alternatively, scope can be defined more broadly as **all** personnel, data, systems, activities, assets, resources, and locations that (1) are within the organization's environment; and/or (2) are used for business purposes; and/or (3) are owned or managed by the organization.*

Consider how exceptions or out-of-scope items are handled. Are there any notable out-of-scope exceptions worth calling out in this section—such as sister organizations, subsidiaries, locations, etc.—that are not subject to Cyber Supply Chain Risk Management practices? Alternatively, this section can (1) direct readers to an exceptions policy that outline a process for reviewing and approving items that are not within scope of Cyber Supply Chain Risk Management, and/or (2) allow supporting security policies to carve out exceptions or specify further requirements, as appropriate, and/or (3) allow certain groups/departments to create more restrictive policies/procedures/standards that apply to a subset of the organization, as long as they comply with the general requirements of this Cyber Supply Chain Risk Management Plan.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] This plan applies to any business arrangement between [ISP Vendor] and third parties that provide services or products to [ISP Vendor] in the capacity of a supplier or vendor partner. Employees and contractors of [ISP Vendor] are required to adhere to this policy.

Some requirements apply specifically to persons with a specific job function (e.g., a system administrator); otherwise, all personnel supporting [ISP Vendor] business functions relative to supplier relationships shall comply with the policies. Other departments shall use these requirements or may create a more restrictive policy, but none that are less restrictive, less comprehensive, or less compliant than these requirements.

This plan does not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect.

A range of security training measures must be undertaken to achieve widespread compliance with various information security obligations. The details of specific requirements may vary from this policy based on various security and compliance obligations that pertain specifically to [ISP Vendor]. All corporate standards are considered baseline requirements and may be superseded by any system-specific standards as needed so long as the corporate requirements are met.

[UPDATE]

1.4 Roles & Responsibilities

***[INSTRUCTIONS**: This section should define roles (either titles, individuals, teams, or groups) related to responsibilities outlined in this document, such as:*

- *Ownership of the Cyber Supply Chain Risk Management program*
- *Review of supplier contracts*

- *Assessment of the Cyber Supply Chain Risk Management program*
- *Reporting/tracking of the Cyber Supply Chain Risk Management program*
- *Performing supplier risk assessments and tracking supplier risk*
- *Training and educating users on the Cyber Supply Chain Risk Management program.*
- *Executive oversight of the Cyber Supply Chain Risk Management program*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE]

ISP Vendor Position	Responsibilities
Named Owner, Chief Information Security Officer, OR Position Title	Ownership of the Cyber Supply Chain Risk Management program (defining, documenting, managing, updating, and disseminating a Cyber Supply Chain Risk Management program)
Legal OR Position Title	Review of supplier contracts to ensure supplier responsibilities are properly articulated
Audit Committee OR Position Title	Assessment of the Cyber Supply Chain Risk Management program
Security Director OR Position Title	Reporting/tracking of the Cyber Supply Chain Risk Management program; ensure monitoring procedures are robust and will provide guidance to those involved in the operational management of supplier risk
Security Manager OR Position Title	Performing supplier risk assessments, tracking supplier risk
Security Manager OR Position Title	Training and educating users on the Cybersecurity Risk Management program
Executive Team OR Position Title	Executive oversight of the Cyber Supply Chain Risk Management program

[UPDATE]

1.5 Management Commitment & Program Status

[INSTRUCTIONS: *This section should outline leadership's commitment to Cyber Supply Chain Risk Management to establish accountability at the executive level.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] The [ISP Vendor] **Executive Team** recognizes the importance of Cyber Supply Chain Risk Management and has authorized [Document Approvers] to define, document, and disseminate a Cyber Supply Chain Risk Management program that accomplishes this mission.

[UPDATE]

[EXAMPLE] [ISP Vendor] is committed to the importance of operationalizing the defined Cyber Supply Chain Risk Management Plan. As such, [ISP Vendor] [has/has not] fully implemented the Cyber Supply Chain Risk Management Plan as defined in this document. **[If ISP Vendor has not fully implemented the plan, add]** The following areas are pending operationalization and are schedule for full implementation by the timelines listed:

- **[UPDATE]**

1.6 Coordination Among Organizational Entities

***[INSTRUCTIONS**: This section should demonstrate that this Cyber Supply Chain Risk Management Plan is supported and deployed consistently at all levels of the organization. As the organization works to achieve the Cyber Supply Chain Risk Management Plan's objectives, effective coordination fosters consistency and helps avoid duplication of efforts. This can be exhibited by the formation of committees with representation from various departments/teams; coordination of risk management efforts between key stakeholders; and/or alignment between various policies, procedures, and standards.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] [ISP Vendor] recognizes the importance of organizational coordination. This document contains references and coordination with the following policies, standards, procedures, departments, committees, and teams.

- [ISP Vendor] Cybersecurity Governance Committee
- List of Named [ISP Vendor] Departments/Teams
- [ISP Vendor] Supporting Policies
- [ISP Vendor] Supporting Standards
- [ISP Vendor] Supporting Procedures

[UPDATE]

1.7 Compliance

***[INSTRUCTIONS**: This section should affirm the expectation of compliance with this C-SCRM Plan, along with any disciplinary action that may be pursued due to noncompliance. It is recommended to have HR/legal teams review this section to ensure it aligns with relevant HR policies.*

This section can also contain a reference to (or a summary of) the exceptions process. This process would provide a structure for handling any system, activity, process, entity, or control that does not comply with the requirements of this C-SCRM Plan. The exceptions process should include steps for documenting, submitting, reviewing, and approving exceptions, along with plans for mitigating risks associated with the exception.

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] Any [ISP Vendor] user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, federal and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

1.7.1 Exceptions

While every exception to a standard potentially weakens protection mechanisms for [ISP Vendor] information systems and underlying data, occasionally exceptions will exist. Information security considerations such as regulatory, compliance, confidentiality, integrity, and availability requirements are most easily met when all users employ centrally supported or recommended standards. [ISP Vendor] understands that centrally supported or recommended technologies are not always feasible for a specific system or team. Deviation from centrally supported or recommended technologies is discouraged. However, it may be considered provided that the alternative presents a reasonable, justifiable business, or research case for an information security policy exception; resources are sufficient to properly implement and maintain the alternative technology; the process outlined in this document and other related documents is followed and other policies and standards are upheld.

An exception may be granted by the [Authorized Persons], or their designee, for non-compliance with a policy or standard resulting from:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Implementation of a solution with equivalent or superior protection to the requirements in the policy or standard.
- Impending retirement of a system.
- Inability to implement the policy or standard due to some limitation (i.e., technical constraint, business limitation or statutory requirement).
- Compliance would cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance (i.e., the cost to comply offsets the risk of non-compliance)

Exceptions are reviewed for validity on a case-by-case basis and their approval is not automatic. Exceptions that are granted will be for a specific time-period, not to exceed one year. Upon expiration of the exception, an extension of the exception may be requested, if it is still required.

2 CYBER SUPPLY CHAIN RISK MANAGEMENT OVERVIEW

***[INSTRUCTIONS**: This section should summarize the organization's understanding of Cyber Supply Chain Risk Management, along with a high-level overview of the primary components of the organization's Cyber Supply Chain Risk Management strategy (further details of each component of the strategy can be described in Section 3: Cyber Supply Chain Risk Management Plan). If applicable, this section should also reference the framework by which the organization structures and aligns its Cyber Supply Chain Risk Management strategy and why this framework was chosen.*

Delete this instruction and all other instructions from your final version of the document.]

[EXAMPLE] Cyber Supply Chain Risk Management is the systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats, whether presented by the supplier, the product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). A Cyber Supply Chain Risk Management strategy addresses the implementation of processes, tools or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities with an organization's digital supply chain in order to infiltrate the IT environment, exfiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

[ISP Vendor] leverages key components of the ***National Institute of Standards and Technology (NIST) Interagency or Internal Reports (NISTIR) 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*** and ***National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*** to define, document and disseminate a Cyber Supply Chain Risk Management program that meets compliance requirements and leading practices.

***[INSTRUCTIONS**: More information on these documents and additional guidance can be found here:*

- *NIST Interagency or Internal Reports (NISTIR) 8276: Key Practices in Cyber Supply Chain Risk Management: Observations from Industry: https://csrc.nist.gov/pubs/ir/8276/final ; https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf*
- *NIST Special Publication (SP) 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations: https://csrc.nist.gov/pubs/sp/800/161/r1/final ; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf*

Delete this instruction and all other instructions from your final version of the document.]

As defined by NIST, there are eight key practices in Cyber Supply Chain Risk Management, which include:

- Integrate C-SCRM Across the Organization
- Establish a Formal C-SCRM Program
- Know and Manage Critical Suppliers
- Understand the Organization's Supply Chain
- Closely Collaborate with Key Suppliers

- Include Key Suppliers in Resilience and Improvement Activities
- Assess and Monitor Throughout the Supplier Relationship
- Plan for the Full Life Cycle

3 CYBER SUPPLY CHAIN RISK MANAGEMENT PLAN

The information included in this section outlines the [ISP Vendor]'s plans to establish a Cyber Supply Chain Risk Management program for each of the selected NISTIR steps.

***[INSTRUCTIONS**: This section details how the organization has implemented each component of the Cyber Supply Chain Risk Management strategy throughout its environment. This section provides further detail of how the organization is achieving the objectives of each component of the Cyber Supply Chain Risk Management framework (as defined in Section 2: Cyber Supply Chain Risk Management).*

Delete this instruction and all other instructions from your final version of the document.]

3.1 Integrate C-SCRM Across the Organization

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-1: Integrate C-SCRM Across the Organization Implementation Summary

Integrate C-SCRM Across the Organization Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Integrate C-SCRM Across the Organization*** step is to ensure all applicable requirements and business perspectives are included in the decision-making processes for C-SCRM at the organizational level, which applies all flow down requirements to independent business units. This also ensures that all independent business units are integrated into a unified Cyber Supply Chain Risk Management process.

***[INSTRUCTIONS:** This section describes the organization's approach to meeting the objectives of the **Integrate C-SCRM Across the Organization** step. Sub-sections should demonstrate how the organization:*

- *Fosters collaboration across the enterprise in managing supply chain risk.*
- *Provides oversight to supply chain risk management (e.g., C-SCRM steering committee, advisory council, leadership team, etc.)*
- *Incorporates perspectives of key stakeholders from diverse groups associated with Cyber Supply Chain Risk Management (procurement, IT, legal, operations, executive team, etc.)*
- *Socializes the organization's C-SCRM practices to applicable personnel across the organization (e.g., policies, procedures, standards, guidelines, training, and education)*
- *Aligns Cyber Supply Chain Risk Management with cybersecurity risk management and enterprise risk management.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.2 Establish a Formal C-SCRM Program

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-2: Establish a Formal C-SCRM Program Implementation Summary

Establish a Formal C-SCRM Program Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Establish a Formal C-SCRM Program*** step is to establish organizational accountability for managing supply chain risks. This should include defined, documented, and disseminated policies, standards, procedures, processes, and tools that have been socialized throughout the organization to the applicable personnel.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Establish a Formal C-SCRM Program*** *step. Sub-sections should demonstrate how the organization:*

- *Demonstrates that C-SCRM is a top business priority for executives.*
- *Formalizes governance for C-SCRM activities.*
- *Maintains appropriate contractual and business agreements with third parties that articulate legal, business and compliance requirements.*
- *Vets third parties from a cybersecurity perspective*
- *Establishes security requirements for third parties.*
- *Implements appropriate technical safeguards for third parties.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.3 Know and Manage Critical Suppliers

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-3: Know and Manage Critical Suppliers Implementation Summary

Know and Manage Critical Suppliers Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Know and Manage Critical Suppliers*** step is to ensure organizations inventory critical suppliers and assess the risk to the organization based on the services or products offered, their role in the organization, the terms of the contracts, etc.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Know and Manage Critical Suppliers*** *step. Sub-sections should demonstrate how the organization:*

- *Maintains an inventory of suppliers.*
- *Identifies suppliers who are critical to the organization.*
- *Understands and tracks the data and systems that are shared and inter-connected between the organization and its suppliers.*
- *Assesses risk of each supplier to the organization*
- *Manages risks from each supplier.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.4 Understand the Organization's Supply Chain

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-4: Understand the Organization's Supply Chain Implementation Summary

Understand the Organization's Supply Chain Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Understand the Organization's Supply Chain*** step is to understand the depth and breadth of their supply chain, including sub-suppliers and how technology and data is managed at every step throughout the system lifecycle.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Understand the Organization's Supply Chain*** *step. Sub-sections should demonstrate how the organization:*

- *Recognizes its role in the supply chain.*
- *Determines its reliance upon suppliers to support key business processes.*
- *Understands the entirety of the supply chain, including the suppliers' reliance upon sub-suppliers.*
- *Requires sub-suppliers also comply with supplier cybersecurity requirements.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.5 Closely Collaborate with Key Suppliers

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-5: Closely Collaborate with Key Suppliers Implementation Summary

Closely Collaborate with Key Suppliers Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Closely Collaborate with Key Suppliers*** step is to ensure organizations partner with their key suppliers to mature processes and increase efficiencies.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Closely Collaborate with Key Suppliers*** *step. Sub-sections should demonstrate how the organization:*

- *Delineates and communicates roles and responsibilities for cybersecurity requirements within the supply chain.*
- *Shares information with upstream and downstream third parties regarding cybersecurity, threats, risks, and best practices*
- *Communicates information about vulnerabilities and incidents to upstream and downstream third parties.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.6 Include Key Suppliers in Resilience and Improvement Activities

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-6: Include Key Suppliers in Resilience and Improvement Activities Implementation Summary

Include Key Suppliers in Resilience and Improvement Activities Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Include Key Suppliers in Resilience and Improvement Activities*** step is to ensure the role that suppliers play in supporting resilience is fully accounted for, tested, and managed.

Collaboration between the organization and its suppliers is key to success in this area and to identify areas of improvement.

***[INSTRUCTIONS:** This section describes the organization's approach to meeting the objectives of the **Include Key Suppliers in Resilience and Improvement Activities** step. Sub-sections should demonstrate how the organization:*

- *Collaborates with its suppliers on identifying vulnerabilities, risks, and threats that could impact the delivery of critical services.*
- *Accounts for the role that suppliers play in its incident response, business continuity, disaster recovery and contingency plans.*
- *Collaborates with suppliers on lessons learned after incidents or business interruptions.*
- *Includes suppliers in activities designed to improve resilience.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.7 Assess and Monitor Throughout the Supplier Relationship

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-7: Assess and Monitor Throughout the Supplier Relationship Implementation Summary

Assess and Monitor Throughout the Supplier Relationship Implementation Summary	
Implementation Status (check all that apply):	**Responsible Role:**
☐ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan
If not implemented, what is the implementation plan?	**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]	DD Month YYYY

The purpose of the ***Assess and Monitor Throughout the Supplier Relationship*** step is to ensure all applicable requirements and business perspectives are included in the decision-making processes for C-SCRM at the organizational level which applies all flow down requirements to independent business units. This also ensures that all independent business units are integrated into a unified Cyber Supply Chain Risk Management process.

***[INSTRUCTIONS:** This section describes the organization's approach to meeting the objectives of the **Assess and Monitor Throughout the Supplier Relationship** step. Sub-sections should demonstrate how the organization:*

- *Tracks changes in regulatory, industry and third-party requirements that could impact processes, systems, or data that its suppliers handle.*
- *Monitors supplier performance*
- *Validates supplier compliance with applicable cybersecurity and regulatory requirements.*
- *Assesses vendor risk status on a regular basis.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

3.8 Plan for the Full Life Cycle.

[INSTRUCTIONS: Update the table below with implementation status of controls in this section.]

Table 3-8: Plan for the Full Life Cycle Implementation Summary

Plan for the Full Life Cycle Implementation Summary			
Implementation Status (check all that apply):		**Responsible Role:**	
☐ Implemented ☐ Partially Implemented ☐ Planned	☐ Alternative Implementation ☐ Not Applicable	[Named Role(s)] **Instruction:** Ensure this role matches roles defined earlier in the plan	
If not implemented, what is the implementation plan?			**Planned Date for Full Implementation:**
[If applicable, insert text or replace with "N/A"]			DD Month YYYY

The purpose of the ***Plan for the Full Life Cycle*** step is to ensure all applicable requirements and business perspectives are included in the decision-making processes for C-SCRM at the organizational level which applies all flow down requirements to independent business units. This also ensures that all independent business units are integrated into a unified Cyber Supply Chain Risk Management process.

[INSTRUCTIONS: *This section describes the organization's approach to meeting the objectives of the* ***Plan for the Full Life Cycle*** *step. Sub-sections should demonstrate how the organization:*

- *Plans for unexpected interruptions to the supply chain*
- *Securely onboards and offboards suppliers.*
- *Integrates cybersecurity into the entire lifecycle for any systems or data procured from, managed by, or handled by third parties.*
- *Establishes requirements for secure removal of sensitive data when a supplier relationship is terminated.*

Delete this instruction and all other instructions from your final version of the document.]

[UPDATE]

4 KEY TERMINOLOGY

***[Instructions:** This section includes definitions for key terminology that are referenced in previous sections of this document. Review and adjust terms and definitions as necessary.]*

In the realm of IT security terminology, the NIST, IR 7298, Revision 1, Glossary of Key Information Security Terms, is the primary reference document that [ISP Vendor] uses to define common IT security terms. The key terminology to be aware of includes the following:'

Table 4-1: Key Terminology Definitions

Term	Definition
Control	This is a term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help [ISP Vendor] accomplish stated goals or objectives. All controls map to standards, but not all standards map to controls.
Data	This is a term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies provides guidance on data classification and handling restrictions.
Guidelines	This is a term describing recommended practices that are based on industry-recognized leading practices. Unlike standards, guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.
Information Security	This is a term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability (CIA) of data.
Policy	This is a term describing a formally established requirement to guide decisions and achieve rational outcomes. A policy is a statement of expectation that is enforced by standards and further implemented by procedures.
Procedure	This is a term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts

Term	Definition
	that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Sensitive Data	This is a term that covers categories of data that must be kept secure. Examples of sensitive data includes PII, electronic protected health information (ePHI) and all other forms of data classified as restricted or confidential in nature.
Personally Identifiable Information (PII):	This is a term that is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: • Social Security number (SSN)/Taxpayer Identification Number (TIN)/National Identification Number (NIN) • Driver license (DL) or other government-issued identification number (e.g., passport, permanent resident card) • Financial account number • Payment card number (e.g., credit or debit card)
Standard	This is a term describing formally established requirements regarding processes, actions, and configurations.
Supplier	A vendor, third party, contractor, service provider or other entity that supplies a product or service.

Term	Definition
Supply Chain Attack	Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.
Supply Chain Risk	The potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. Cybersecurity risk in supply chains is the result of threats that exploit vulnerabilities or exposures within 1) products and services that traverse supply chains; or 2) supply chains themselves
System	This is a term describing an asset; an information system or network that can be defined, scoped, and managed. These include, but are not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

APPENDIX A: NISTIR 8276 GUIDANCE

Included below is the guidance from NISTIR 8276 for each of the C-SCRM categories. This can be referenced for additional context regarding objectives of the Cyber Supply Chain Risk Management Plan. The full text of NISTIR 8276 "Key Practices in Cyber SCRM: Observations from Industry" can be found here: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

Integrate C-SCRM Across the Organization

A number of organizations have established Supply Chain Risk Councils (or Supply Chain Leadership Risk Councils) that include executives from supply chain/procurement, information technology, cybersecurity, operations, legal, enterprise risk management (ERM), and other functional and leadership areas of the organization, depending on the organization's business and structure. These Councils proactively review relevant risks and risk mitigation plans, set priorities, direct sharing of best practices throughout the enterprise, and pilot initiatives. They also result in informal networks of leaders that facilitate trust and accountability in complex business environments. The benefit of Councils is the shared risk decision-making that ensures all perspectives are addressed.

Collaborative C-SCRM is not limited to the executive suite. Mature C-SCRM programs facilitate closer collaboration between cybersecurity, product security, physical security, enterprise risk management, and, of course, supply chain/procurement. Specifically, the level of integration of supply chain, cybersecurity, product security, and physical security increases with C-SCRM practice maturity. More mature companies have explicit roles that bridge these functions and also integrate them with enterprise risk management. Such internal alignment facilitates the efficiency and effectiveness of delivering products and services while appropriately managing C-SCRM risks. For example, these integrated functions share information, metrics, and program objectives to reduce C-SCRM risks. This often results in a more nuanced and comprehensive understanding of cybersecurity risks by business executives, as well as better strategic decisions that take CSCRM into consideration.

Establish a Formal C-SCRM Program

A formal C-SCRM program ensures organizational accountability for managing cyber supply chain risks. Mature organizations have formal programs with established governance, policies and procedures, processes, and tools. It should be noted that smaller organizations may not need the structure required by larger organizations. For example, a small manufacturing organization may not need as many formal processes as a large technology company. The following is a list of high-level characteristics of a formal C-SCRM program that organizations can consider implementing when establishing a formal C-SCRM program:

Table A-1: Establish a Formal C-SCRM Program Considerations

Establish a Formal C-SCRM Program Considerations
Considerations
1. Increased Executive Board or Executive Level involvement for establishing C-SCRM as a top business priority and to ensure proper oversight
2. Clear governance of C-SCRM activities that includes cross-organizational roles and responsibilities with clear definitions and designation/distribution of these roles among

Establish a Formal C-SCRM Program Considerations
enterprise risk management, supply chain, cybersecurity, product management and product security (if applicable), and other relevant functions appropriate for the organization's business.
3. Standards-based policies and procedures that provide guidance to different business units detailing their C-SCRM activities.
4. Same policies used internally and with suppliers
5. Integration of cybersecurity considerations into the system and product development life cycle
6. Use of cross-functional teams to address specific enterprise-wide risks
7. Clear definition of roles of individuals responsible for cybersecurity aspects of supplier relationships (which may be different than those responsible for procurement activities with specific suppliers)
8. Establishment of centers of excellence to identify and manage best practices
9. A set of measures of success used to facilitate decision-making, accountability, and improvement
10. Approved and banned supplier lists
11. Use of software and hardware component inventory (e.g., bill of materials) for third-party components
12. Prioritization of suppliers based on their criticality
13. Establishment of testing procedures for the most critical components
14. Establishment of a known set of security requirements or controls for all suppliers, especially robust security requirements for critical suppliers to be used in procurement (sometimes known as master specifications)
15. Service-level agreements (SLA) with suppliers that state the requirements for adhering to the organization's cybersecurity policy and any controls required of the supplier
16. Establishment of intellectual property rights agreements
17. Shared supplier questionnaires across like organizations, such as within the same critical infrastructure sector
18. Upstream propagation of acquirer's security requirements within the supply chain to sub-tier suppliers
19. Assurance that suppliers have only the access they need in terms of data, capability, functionality, and infrastructure; bounding this access by specific time frames during which suppliers need it
20. Use of escrow services for suppliers with a questionable or risky history
21. Provision of organization-wide training for all relevant stakeholders within the organization, such as supply chain, legal, product development, and procurement; this training may also be extended to key suppliers
22. Identification of alternative sources of critical components to ensure uninterrupted production and delivery of products
23. Secure requirements guiding disposal of hardware that contains regulated data (e.g., personally identifiable information [PII] or protected health information [PHI]) or otherwise sensitive information (e.g., intellectual property)

Establish a Formal C-SCRM Program Considerations
24. Protocols for securely terminating supplier relationships to ensure that all hardware containing acquirer's data has been properly disposed of and that the risks of data leakage have been minimized

Know and Manage Critical Suppliers

Critical suppliers are those suppliers which, if disrupted, would create a negative business impact on the organization. Critical suppliers are also those suppliers that provide critical components (products or services) that support the critical business missions of the organization. Identifying such suppliers requires organizations to first identify and prioritize critical missions, assets, systems, processes, and data and then identify suppliers that either have access to or provide infrastructure for critical assets, systems, processes, and data.

Several criteria can be used to determine component and supplier criticality:

- Revenue contribution of suppliers
- Whether a supplier processes critical data belonging to the acquirer, such as regulated data (e.g., PII, PHI) or intellectual property.
- Volume of data a supplier has access to or hosts.
- Whether a supplier has access to the acquirer's system and network infrastructure
- Whether a supplier can become an attack vector by being compromised and allowing threat actors access to the acquirer
- For technology companies, whether a supplier can become an attack vector for the technology company's products or services delivered to customer.

There is a number of NIST and industry resources that can be used to identify critical suppliers:

- NIST has made available a free tool that helps identify the impact of suppliers to the organization; The tool is described in NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks, along with instructions on how to use it [NISTIR 8272].
- NISTIR 8179, Criticality Analysis Process Model, provides a comprehensive methodology for determining project and product criticality that can be used as an input in determining system, component, and supplier criticality [NISTIR 8179
- The Business Impact Analysis (BIA) described in NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, can also be used to determine supplier criticality [SP 800-34].
- The Business Continuity Planning booklet published by the FFIEC (Federal Financial Institutions Examination Council) provides a process and list of considerations that can be adapted to determine supplier criticality [FFIEC BCP].

Once suppliers are identified, risks can be assessed, and suppliers can be prioritized by their criticality. Best practice organizations have established supplier requirements by criticality and include the use of master specifications for security requirements. These requirements are used in supplier contracts (e.g., Terms and Conditions), and adherence to these requirements is monitored during the supplier relationship life cycle.

Understand the Organization's Supply Chain

To manage cybersecurity risks that originate from supply chains, organizations need to understand their supply chains, including multiple layers of sub-suppliers. Today's supply chains are extended, extensive, and include multiple organizations across the globe. In this environment, the risks may stem from suppliers' connectivity to their suppliers, component sourcing for hardware and software suppliers, technologies shared upstream and downstream within supply chains, and processes and people within those supply chains.

Best practice organizations establish real-time visibility into the production processes of their outsourced manufacturers with the capacity to capture not only defect rates but causes of failure and, therefore, prevent a supplier's ability to shortcut testing requirements before shipment. This includes the use of software and hardware component inventory as well as tools and methods to audit provenance claims at any point in the supply chain. Such visibility and transparency reduce the risk of tampering and counterfeiting and improve the security, and the quality, of the resulting products. Additionally, best practice organizations have insight into how their supplier's vet their personnel, who they are outsourcing to and who has access to the acquirer's data.

Closely Collaborate with Key Suppliers

Best practice organizations establish close relationships with their suppliers up to and including creating shared ecosystems between acquirers and suppliers to increase coordination and simplify the management of complex shared supply chains. Increasingly, organizations are treating their suppliers as members of their ecosystem and closely collaborating in a variety of ways:

- Acquirers maintain close working relationships through frequent visits and communications.
- Acquirers mentor and coach suppliers on C-SCRM and actively help suppliers improve their cybersecurity and supply chain practices.
- Acquirers and suppliers invest in common solutions.
- Acquirers require the use of the same standards within the acquirer organizations and by suppliers, thereby simplifying communications about cybersecurity risk and mitigations and helping to achieve a uniform level of quality throughout the ecosystem.

The sophistication and level of formality of acquirer-supplier relationships increase with the maturity of the C-SCRM practices. For example, smaller businesses establish and maintain close relationships with their key suppliers by conducting frequent visits, phone calls, and other forms of informal communication. Larger and more mature organizations use more documented processes and procedures and hold multiple formal meetings with their suppliers. Acquirers and suppliers within the ecosystem coach each other upstream and downstream. Because most organizations find themselves in the roles of acquirers and suppliers, the presence of more mature acquirers in the overall ecosystem increases the maturity of the entire ecosystem. An example of this effect is when executives join Executive Boards of more mature organizations and become exposed to the practices deployed there, as well as the questions and topics discussed at Executive Board meetings. Executives then bring those practices and topics to their own organizations and advocate for adoption. A similar effect is achieved when organizations belong to industry groups, information-sharing organizations, and roundtables where individuals and organizations can learn from each other. Another method for acquirers and suppliers to coach each other is through the use of supplier questionnaires, which are used to identify opportunities for additional supplier mentoring and training. Some suppliers also use acquirer questionnaires to shape security requirements that suppliers apply to their products and services.

Include Key Suppliers in Resilience and Improvement Activities

Threat actors actively target acquirers through suppliers. In addition to cybersecurity risks, there are environmental risks, such as severe weather, and risks associated with geopolitical unrest, that continually threaten to disrupt the supply chain. Incidents will happen to even the most mature organizations, which makes resiliency planning essential. Mature organizations include their critical suppliers, products, and assets in their contingency planning, incident response, and disaster recovery. These organizations test such plans with key stakeholders, including suppliers, to guarantee the readiness of all involved parties and the effectiveness of the plans. This ensures that critical procedures and protocols are established and well-understood ahead of any significant event. Resilience and improvement activities include:

- Rules and protocols for information sharing between acquirers and suppliers, sometimes within larger critical infrastructure sector ecosystems.
- Joint development, review, and revision of incident response, business continuity, and disaster recovery plans
- Protocols for communicating vulnerabilities and incidents.
- Responsibilities for responding to cybersecurity incidents.
- Coordinated communication methods and protocols.
- Coordinated restoration and recovery procedures.
- Collaborative processes to review lessons learned.
- Updates of coordinated response and recovery plans based on lessons learned.

More mature acquirers have formal continuous improvement processes that include collecting lessons learned from supply chain incidents; sharing potential improvements throughout the ecosystem; incorporating results into planning, response, and recovery processes; and sharing them with appropriate organizations throughout the enterprise. This process includes stakeholders from the organization and suppliers to ensure that identified risks are remediated.

Assess and Monitor Throughout the Supplier Relationship

Organizations and their environments are continuously evolving. A supplier assessment conducted prior to bringing a supplier on board is a snapshot in time that becomes obsolete before it is completed. Mature acquirers establish supplier-monitoring programs that cover the entire supplier relationship life cycle and monitor a variety of risks, including security, privacy, quality, financial, and geopolitical risks, to name a few. This practice of monitoring and review includes validating that suppliers are meeting cybersecurity and other key SLA requirements, identifying any changes in supplier status (e.g., financial, legal, ownership), and mitigating the identified risks per mutually agreed upon remediation timelines.

Assessing supplier controls on a regular basis helps manage cyber supply chain risks by determining whether agreed-upon requirements and controls are being met, identifying improvements that may be required, and monitoring the completion of those improvement actions.

Acquirers deploy a variety of supplier assessment and monitoring mechanisms, such as self-assessment, supplier attestation, third-party assessments, formal certifications, and site visits. For most critical suppliers, acquirers use a combination of formal certifications, third-party assessments, and site visits. Assessments allow organizations to understand the changes in a supplier's status and discover changes in risks. The frequency and robustness of the assessments should be established based on supplier

criticality. Critical suppliers should be assessed more frequently, and more extensive assessment methods should be used to determine if there are any changes in risk.

Large organizations may rely on hundreds of supplier assessments every year, causing some suppliers to answer a burdensome number of questionnaires in turn. Shared assessments involve using a single supplier assessment to satisfy multiple acquirers and are an emerging practice within some critical infrastructure organizations. In a shared assessment, a number of acquirers create a single assessment methodology and questionnaire which may then be applied to thousands of suppliers that support a particular need. Suppliers can then reuse their answers to such questionnaires by providing them to multiple acquirers. Some critical infrastructure sectors have established entities to run third-party risk processes for industry segments, with C-SCRM being included in these processes. While this approach may save acquirers and suppliers significant time and resources, organizations should carefully consider whether shared assessments fit their own particular needs, including risk tolerance, operating environment, and regulatory obligations.

In addition to supplier assessments, organizations can deploy technical processes and technologies to monitor any changes in a supplier's risk status. If suppliers have dedicated connections to the acquirer's infrastructure, the acquirer's security operations center can monitor any changes to the supplier's connection to the acquirer's network and systems. Acquirers can also use a variety of cybersecurity risk-rating solutions to provide insights into cybersecurity risks posed by suppliers.

Plan for the Full Life Cycle

When organizations put technical solutions into their infrastructures, they expect those solutions to continue working for as long as they are needed by the organization. However, organizations should plan for unexpected interruptions to the supply chain to ensure business continuity. Examples of such interruptions include suppliers stopping support of obsolete hardware and software, discontinuing production of hardware components, or adopting a significant change of business direction caused by acquisition or changes in supplier ownership or management. Organizations should deploy a variety of practices to manage this particular risk, including purchasing reserve quantities of critical components and establishing relationships with approved resellers that are likely to stay in business. An innovative method deployed by digital companies is to bring ailing component manufacturers in-house to ensure an uninterrupted supply of critical components.