North American Transmission Forum

NATF Supply Chain Risk Controls and Monitoring

Open Distribution for Supply Chain Materials

The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

Version 1.0
Document ID: 1813
Approval Date: 1/30/2026

Versioning

Revision History

Date	Version	Notes
1/30/2026	1.0	Initial version

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

1. Purpose

After entities have carefully collected information and conducted a thorough risk assessment on a current or potential supplier, how can they ensure that their efforts are properly memorialized and effectively used to reduce the amount of risk they face? This document seeks to help answer that question by providing specific guidance and practical examples of how entities can implement controls to mitigate supplier risk, and equally important, suggested practices for how those controls may be documented and monitored.

An important driver of this document is the *2023 Lessons Learned from Commission-led CIP Reliability Audits* [1] report by the Federal Energy Regulatory Commission (FERC)*,* which highlighted instances where entities lacked a documented process to respond to supplier risks that were previously identified. This observation was consistent with the CIP-013-2 Standard Authorization Request (SAR) submitted by the North American Electric Reliability Corporation (NERC) in September 2023 [2] which cited industry's variable response to implementing controls to supplier risks once they were identified, as well as a general lack of rigor in tracking residual risks posed by a supplier.

More recently, FERC's Order 912 on Supply Chain Risk Management Reliability Standards Revisions [3] notes continued concern regarding the sufficiency of an entity's Supply Chain Risk Management (SCRM) plans in appropriately identifying, assessing, and responding to supply chain risks. Beyond any regulatory requirements, however, it is imperative that entities have effective processes in place to address the threats that modern day supply chains can pose to their operations.

It is these ever-present concerns regarding SCRM that has led the North American Transmission Forum (NATF) to create a series of publicly available resources for industry use and adoption. In particular, the *NATF Supply Chain Security Assessment Model* [4] (the "NATF Model") provides a step-by-step approach to accomplishing effective SCRM. Some NATF resources, such as the *NATF Supply Chain Security Criteria* [5] and the *Energy Sector Supply Chain Risk Questionnaire* [6] focus on collecting information (step 1 of the NATF Model), whereas other resources such as the *NATF Supply Chain Risk Assessment Guidance (*"Risk Assessment Guidance") [7] focus on assessing the risks present (step 3 of the NATF Model).

Accordingly, this document seeks to provide guidance on implementing controls on suppliers and highlight practices for monitoring changes to supplier risk posture. These activities correspond to *Step 5: Implement controls and monitor risks* of the NATF Model. However, this document does not create, replace, or change any requirements in the NERC Reliability Standards or other applicable criteria, nor does it create binding norms by which compliance with NERC Reliability Standards is monitored or enforced. Implementation of NATF practices does not ensure compliance with the NERC Reliability Standards. In addition, this document is not intended to take precedence over any company or regional procedure. It is recognized that individual companies may use alternative and/or more specific approaches that they deem more appropriate.

2. Scope

This guidance is written primarily for entities and their staff responsible for procuring products and services from suppliers. Accordingly, most of the discussion and examples provided throughout this document use the term "entities" to denote the party obtaining goods or services. However, this guidance may also be useful for suppliers who are themselves customers or clients of another supplier and seek to better understand their own supply chains and manage sources of risk. In such cases, "entity" may be construed as "customer" or "client" instead.

The scope of this guidance is focused on "Step 5: Implement Controls and Monitor Risks" of the *NATF Supply Chain Security Model* [4]. Specifically, this guidance is intended to broadly support and further explore the two main sub-steps listed:

> *The entity should have a plan to monitor:*
>
> - *Risks and controls associated with the purchase throughout the lifecycle of the products or services.*
> - *The supplier for any changes that could affect products or services (e.g., corporate changes or changes to the supplier's supply chain) as well as for any breaches or compromises.*

To maintain focus for this document, other aspects of supply chain risk management, such as contract negotiation, assessing supplier risk, and soliciting information from a (potential) supplier to aid in risk assessment are expressly out of scope. While these are worthy considerations, they more naturally map to other parts of the NATF Model [4] and are not addressed in this specific document. Additional resources for consideration are cited throughout this document for the interested reader.

3. Supply Chain Risk Controls

Today's diverse supply chain represents one of the most significant vectors of risk for entities, as many different types of risk are contained within it. For example, cybersecurity vulnerabilities may be contained within a product or service that is provided to an entity. Privileged access that a supplier has into an entity's network may be infiltrated by a malicious third party. Even the information that a supplier maintains on their customers may represent a risk to entities if the supplier's information systems are breached and the information leaked.

Geopolitical risks, outside the ability of suppliers or entities to control, are another form of risk to the supply chain that may be manifested via tariffs, bans, regulation, taxes, forced divestment or seizure, and other scenarios that are difficult to predict. Even regional issues like material shortages, labor strikes, and natural disasters can have global impacts if only a handful of suppliers produce a given product.

These are only some of the risks that an entity may identify while performing a supplier risk assessment. After these risks have been identified and impacts assessed, controls must be put into place to address these sources of material risk. Indeed, the CIP-013 Reliability Standard [8] also emphasize the need for proactive measures to mitigate these threats, not only by identifying inherent risks but also by addressing residual risk after initial safeguards are applied (such as the disclosure of a vulnerability or incident that impacts the entity).

Implementing controls such as supplier risk assessments, contractual security requirements, and continuous monitoring ensures that entities maintain resilience against evolving threats. By layering controls to reduce both primary and residual risk, entities can strengthen their defensive posture and reduce the impact of supply chain risks to their organization.

Supplier Risk Tiering

Entities are encouraged to adopt a risk tiering methodology that best fits their organizational needs and risk appetite. Classifying a given supplier into a specific risk tier is performed during "Step 3: Conduct the Risk Assessment" of the NATF Model. Accordingly, this section serves as a refresher on the concept of supplier risk tiering and provides an expanded discussion on the implications of different tiers, particularly given the foundational roles that different risk tiers serve when entities decide which supply chain risk controls to implement.

As noted in the NATF's Supply Chain Risk Assessment Guidance [7], a common and effective approach is to classify suppliers into three risk tiers – such as high, medium, and low – representing the varying degrees of risk that a supplier presents to the entity. Such a methodology provides clarity and supports consistent risk management practices across the organization.

While other descriptors may be used (such as Level I, Level II, Level III), this document will use High, Medium, and Low for consistency. Similarly, though this document suggests three tiering levels, entities may choose to use a different number of tiers (such as two in a Tier 1/Tier 2 configuration). In all cases, entities are free to tailor the number of levels, naming conventions, and assessment factors to their unique context.

Below are recommended definitions for high, medium, and low risk suppliers that may be used to aid in control implementation and supplier monitoring. For example, if new information is discovered during supplier monitoring, these definitions may be useful if risk re-classification (and re-assessment) is warranted.

High-risk Supplier

A supplier whose failure or compromise could cause significant operational, financial, regulatory, or reputational harm. These suppliers are often single-source or sole-source, provide critical components or services, or have access to sensitive systems/data. They also may be in high-risk regions or have a history of compliance issues. Examples of high-risk suppliers may include:

- The sole provider of a mission-critical software platform for grid operations.
- A manufacturer supplying unique, custom-engineered parts with no immediate alternatives.
- A supplier with direct access to company networks or sensitive customer data.
- A supplier operating in a politically unstable country or subject to frequent regulatory changes.
- A strategic partner whose disruption would halt production or service delivery.

Medium-risk Supplier

A supplier whose disruption would cause moderate impact—delays, increased costs, or operational inconvenience—but for whom alternatives exist or the supplied goods/services are less critical. These suppliers may provide important but not unique products, or have some exposure to risk factors (e.g., moderate financial health, partial compliance gaps). Examples of medium-risk suppliers may include:

- A regional distributor of standard electrical components, with other distributors available.
- A service provider supporting non-core business functions (e.g., IT helpdesk, facility maintenance).
- A supplier with some history of late deliveries but no major compliance issues.
- A backup supplier for critical materials (not the primary source).

Low-risk Supplier

A supplier whose failure would have minimal impact on operations, finances, or reputation. These suppliers typically provide non-critical goods or services, are easily replaceable, and have little or no access to sensitive systems or data. Examples of low-risk suppliers may include:

- An office supply company providing pens, paper, and other commodities.
- A local catering service for company events.
- A supplier of promotional items or branded merchandise.
- A supplier used for non-critical one-off purchases with no ongoing relationship.
- Distributors and resellers with no access to the products and services being sold.

Periodic Review of Supplier Risk Tier and Reassessment

To ensure that the assigned supplier risk tier remains accurate and relevant, entities should periodically reassess their suppliers and, if warranted, reclassify their suppliers into a different risk tier using a risk-based approach. For example, a high-risk supplier of significant criticality to the entity may be reassessed every year to ensure that emerging risks are quickly identified and addressed, whereas a low-risk supplier that poses little impact on the entity’s operations or core functions may only be assessed every three years. The entity may tailor the frequency and depth of review based on regulatory requirements or organizational risk appetite.

In most cases, risk tier reclassifications will occur during an entity's routine supplier risk reassessment. However, entities may discover new information when implementing supply chain controls or while monitoring their suppliers that may warrant an out-of-cycle reassessment and reclassification. It is imperative that entities remain vigilant to changing circumstances and watchful for triggers that may indicate a change in a supplier's risk posture. Accordingly, whether they are routine or out-of-cycle, all supplier reassessments should:

- Assess the effectiveness of existing risk controls and mitigation strategies.
- Incorporate lessons learned from incidents, audits, or industry developments.
- Evaluate any changes in the supplier's operations, ownership, financial health, regulatory environment, or the criticality of the goods and services provided.
- Recalculate the supplier's risk tier based on current facts and circumstances.
- Update the associated risk controls, control owners, and internal processes as necessary to reflect changes in risk tiering or newly identified risks.

Entities may also consider integrating supplier risk reassessments with broader organizational risk management activities, such as annual business planning or compliance reviews, to ensure alignment and efficiency. A structured, periodic review process helps entities proactively identify emerging risks, maintain compliance, and ensure that supplier risk management practices remain robust and effective. Additional discussion on risk assessment triggers and supplier risk tiering is provided in the NATF's Risk Assessment Guidance [7].

Control Implementation

Supplier risk assessments will often provide valuable insight into where additional protections are needed. By carefully analyzing assessment results, entities can pinpoint specific risks such as weak authentication, inadequate patch management, or unclear incident response processes and implement targeted controls to address them. For example, if a supplier lacks strong access safeguards, an entity might require multi-factor authentication and session monitoring. Similarly, poor findings related to software integrity could lead to contractual requirements for secure development practices and vulnerability testing.

Thus, after conducting a thorough supplier risk assessment (or reassessment), controls should be identified to address the risks identified. While compliance with the CIP-013 Reliability Standard provides a strong baseline set of controls, entities are encouraged to go beyond the minimum requirements to strengthen their supply chain security posture further. Selecting which controls to use, however, presents its own unique series of challenges:

- What controls are most relevant to the risks identified?
- Which controls are most cost-effective?
- What controls should be implemented by the entity, supplier, or outsourced to a third party?

The answers to these questions may be further modulated by entities' available resources. For example, if a given risk is best addressed by onsite inspections of the supplier, but the entity cannot perform these inspections due to cost, the entity will need to determine the next-best control (or combination of controls) that still effectively addresses the risk.

It is important that entities use a carefully designed process that takes such questions into account at the beginning of the control implementation process. Doing so provides the basis for an effective and efficient supplier risk management program that carefully stewards the finite resources of an entity for risk management. This approach also ensures that controls are not generic but are tailored to actual and specific risks, thus helping to reduce the total and residual risk that an entity is exposed to and strengthening their overall supply chain security.

The control implementation process naturally progresses through *Identify Controls*, *Assign Owners*, and *Implement Controls* phases, each of which is discussed in additional detail in the following sections. While these phases are typically linear such that one is completed before proceeding to the next one, flexibility to adjust prior decisions should be maintained when proceeding through the phases. If, for example, a supplier is found to be unable or unwilling to adequately execute a supplier-assigned control during the *Implement Controls* phase, the earlier phases may need to be repeated to address the risk posed by the incomplete or ineffective implementation of the control.

Identify Controls

Before supply chain controls can be implemented, entities must first identify controls that are commensurate and responsive to the specific results of the supplier risk assessment. High risk suppliers may require more stringent controls, while low risk suppliers may need baseline measures. For any identified risks where the entity has decided to mitigate or outsource the risk, a corresponding control should be identified to address it.

During the *Identify Controls* phase, entities answer the question of which controls are most relevant and appropriate to address the risks previously identified during the supplier risk assessment. This phase also includes feasibility considerations, as relevant controls will be of little value if the corresponding resources are not available to implement them in practice. For example, an entity may have a control that requires potential suppliers to conduct enhanced background checks of their employees before the purchase of any service. If a potential supplier is unable or willing to pay for the costs of increased vetting, the control's lack of feasibility may cause the entity to look for an alternate supplier or re-evaluate the use of this control.

When identifying which controls to implement, it may be helpful to first identify categories or "families" of controls based on the risk each control represents (or is designed to address). Doing so may speed up the process of control identification, particularly for risks that are unique or not previously encountered by the entity. For situations where the right risk control is initially difficult to develop, the larger control family will typically be easier to identify, which may aid in narrowing the scope of possible controls to consider.

While the specifics of individual controls may vary greatly between entities, the larger categories or families of risk they correspond to are largely the same across industry, even if referred to by different names that cover slightly different areas. Accordingly, it is anticipated and expected that each entity will develop their own internal library of controls to draw from – and add to – when conducting the identify controls phase.

Suggested categories of controls that entities should consider, along with representative examples of individual controls that each category might contain, are as follows:

- Identity and access management
    - Multi-factor authentication is required for all remote access by supplier
    - Entity limits supplier remote access to needed systems only

  - Communication channels between entity and supplier are encrypted
- Asset management
  - Critical hardware components use tamper-evident seals placed by supplier
  - Entity maintains asset inventory (including hardware/software)
  - Entity verifies firmware authenticity and integrity before installation
- Configuration management
  - Supplier changes to entity systems are reviewed by entity for impact before implementation
  - Entity documents and tracks any system changes
  - Back-out or rollback plans are developed prior to any change and reviewed by entity
- Continuous supplier monitoring
  - Suppliers are monitored using third-party risk management services
  - Entity signs up to receive supplier vulnerability announcement notifications
  - Entity leverages private information sharing networks (e.g., E-ISAC) for early warning of potential supplier incidents
- Disaster recovery and business continuity
  - Supplier maintains and implements business continuity and disaster recovery plans
  - Alternative supplier(s) are pre-selected by entity in case of supplier unavailability
  - Entity maintains enough spares for critical products
- Incident response
  - Suppliers are required to report incidents promptly
  - Supplier conducts periodic incident response exercises or drills
  - Secure communication protocols are established by supplier and entity
- Legal and compliance
  - Suppliers are required to indemnify a certain amount
  - Entity maintains ownership of data and product outputs
  - Entity maintains the right to audit supplier processes and facilities
- Policy and governance
  - Supplier maintains a documented cybersecurity program
  - Periodic risk reassessments on suppliers are performed
  - Supplier’s policies are routinely reviewed and updated
- Workforce management
  - Periodic security awareness training is provided to supplier staff

- Supplier staff have initial and ongoing background checks
- Supplier promptly notifies entity of any terminated staff with entity access

This list is non-exclusive in nature and is not intended to limit an entity but rather to serve as a minimum basis for consideration. Different entities may choose to categorize risks and controls in a variety of ways, and while there is no singular “correct” approach, this list should be evaluated to determine if any controls or categories are described for which an entity does not have a corresponding or equivalent entry.

Assign Owners

The *Assign Owners* phase addresses the question of who is responsible for executing the control. Some control assignments may be implied by the work done previously during the *Identity Controls* step. A control to implement multi-factor authentication for all remote access to an entity’s systems, for example, may be seen to clearly be the responsibility of the supplier to implement.

However, even seemingly straightforward control assignments may involve additional effort on the part of the entity or another party to be effective. In the example just provided, the supplier may be responsible for implementing multi-factor authentication, but the entity may have to independently provide the second factor of authentication for each new remote connection into an entity’s systems. Therefore, while it may be tempting to neatly categorize all controls into the exclusive responsibility of entity, supplier, or some other third party, the practicalities of implementation may dictate a more nuanced and collaborative approach.

One way of quickly and effectively assigning control owners is via the use of role-based assignments. Rather than naming individuals, unique centers of risk and business function are used to develop roles, stratify responsibilities, and define areas of risk coverage. Assigning the responsibilities for controls to roles rather than individuals also allows for greater flexibility and continuity when individuals change roles, departments are reconfigured, or reporting relationships change. Suggested roles to consider when assigning controls are:

- **Business Continuity/Disaster Recovery (BCDR):** Maintains contingency plans and ensures coordinated response
- **Compliance:** Provides regulatory coordination, adherence, and recordkeeping controls
- **Cybersecurity:** Maintains technical security controls (e.g., access management, monitoring)
- **Operations:** Provides controls related to the intended use of the product or service
- **Physical security:** Maintains physical security controls (e.g., patrols, motion sensors)
- **Procurement:** Maintains controls related to supplier selection and contract clauses
- **Risk management:** Maintains controls that support the larger enterprise risk framework
- **Safety:** Maintains safety-related controls to avoid injury or damage to life and property

These functional roles may not always map into the existing organizational layout or reporting structure of an entity. Specific roles may be carried out by more than one department or via a cross-functional team comprised of representatives from multiple departments. Additionally, new roles may be developed by the entity to reflect other functions or unique sources of risk not captured by those offered here.

Control assignments may be recorded by use of a dedicated governance, risk, and compliance (GRC) tool or enterprise resource planning (ERP) solution that supports risk management functions. As these tools can be costly to implement and maintain, alternative approaches may be utilized instead. Workflow management software, databases, or even basic spreadsheets may be used to track who is responsible for which control. Further information on documenting control assignments is provided in the following section, "4. Supply Chain Control Documentation."

Implement Controls

The *Implement Controls* phase addresses the activities related to control deployment and integration into an entity's operations. For some controls, this may be as simple as updating a step in an existing standard operating procedure (SOP), distributing the updated SOP via usual documentation update processes, and relying on entity staff to perform the additional step when they get to that part of the process. In other cases, it may be as involved as complex contract negotiations lasting several months to implement a control incorporated into contract language.

Additionally, some controls can be more effective if used as part of an overall lifecycle instead of a single instance. For example, an internal control may stipulate that any contemplated purchase from a single supplier that would result in a yearly expenditure beyond a fixed dollar amount must have a risk assessment conducted within the last three years before any purchase orders are issued. This is representative of a lifecycle control, as it exists independent of any individual purchase or supplier, is continuously evaluated, is proactive in nature, and may result in the identification and creation of additional controls.

By contrast, a control that requires a supplier's creditworthiness to be evaluated after a certain amount has been paid is more representative of a targeted control, as it only occurs once, is reactive in nature (occurring after the expenditure takes place), and is limited to a single factor (financial risk) instead of multiple factors.

In practice, a combination of both lifecycle and targeted controls is needed to effectively manage supplier risk. Additional practices to consider for control implementation include:

- Writing controls directly into contracts with suppliers
- Using automation or configurable workflows to embed controls into procurement processes, supplier onboarding, and contract management functions
- Preferentially selecting controls (where possible) that can be independently verified
- Scheduling periodic reviews of existing controls
- Conduct tabletop exercises to simulate control effectiveness in different situations

In addition to implementing controls, it is also important to establish mechanisms to independently verify that these controls are working as intended. Having an independent department whose primary mission is to validate the effectiveness of implemented controls (such as Internal Audit, although other names may be used) can provide an additional level of assurance and strengthen accountability. Peer checking, the practice of having a second person continuously verify that the actions taken by an individual are correct, should also be incorporated into critical control implementation and verification processes to catch potential gaps early and promote consistency. Together, these steps help ensure that controls are effective and working as designed to reduce supply chain risk.

Address Residual Risk

Despite the best efforts of an entity to reduce the amount of risk faced, there will always be a remnant that cannot be eliminated. This remnant, known as residual risk, is the level of risk remaining after all planned risk mitigation measures and controls have been implemented. Residual risk can be determined by first identifying the level of inherent risk – the level of risk before any controls – and then applying the appropriate type of control (technical, administrative, contractual, etc.) to reduce the risk. Whatever risk remains after all controls have been implemented is the residual risk.

By way of example, a supplier risk assessment may indicate a high risk of unauthorized access due to insecure login mechanisms. To address this inherent risk, the entity may implement technical and contractual controls such as multi-factor authentication and incident notification requirements. While the likelihood and impact of unauthorized access may decrease, it will not be zero, as there is a non-zero chance that an attacker has already compromised the supplier before the multi-factor authentication control was implemented. This possibility that cannot be eliminated is known as the residual risk.

Examples of supply chain risk residuals that entities may encounter include:

- Limited visibility to supplier subcontractors
    - Even if entities require suppliers to disclose their subcontractors and security practices, entities may not have full visibility into the subcontractors' downstream suppliers.
- Incomplete assurance of software integrity
    - Many software integrity verification methods rely on supplier-provided checksums, signatures, or other measures to validate the integrity of software packages. However, there is often no way to verify that these measures have not been tampered with or created by an attacker inside the supplier's environment.
- Supplier business email compromise
    - Despite the best efforts of a supplier to implement effective information security controls, an attacker may compromise one (or more) of a supplier's email accounts and use those accounts to selectively target entities in additional attacks. As this risk may be reduced but never eliminated, entities must remain continuously vigilant for attackers that attempt to compromise and abuse a trusted entity-supplier relationship.
- Delayed patch deployment
    - Even with contractual requirements defining a required timeframe in which suppliers must apply (or issue) patches for newly discovered vulnerabilities, there will typically exist some window of time – however slight or significant – that the system, product, or service is unpatched and vulnerable to attack.
- Insider threat in supplier organizations
    - Background checks and personnel risk assessments can reduce the threat of insider risk, but they cannot eliminate the possibility of a malicious (or negligent) insider at a supplier impacting an entity's systems.

- Supply chain disruption risks
  - Disruptions caused by geopolitical issues, natural disasters, pandemics, trade issues, and similar national or multi-national risks can result in significant risk residuals that are resistant to mitigation efforts.

Although many risks can be managed or mitigated, there are no perfect controls that can prevent all possible negative outcomes. As some remaining exposure will always exist, the entity must determine if the residual risk is acceptable. If it is, the entity may decide to formally accept the residual risk. If it is not, however, this may indicate that not all controls have been implemented and more are needed. In rare cases, the residual risk may be considered too great even after additional mitigation measures have been implemented, resulting in the entity refusing the risk and canceling the procurement.

Accept and Document Residual Risk

Once controls have been implemented to mitigate risk to a level the entity finds acceptable, the entity should act to formally accept and document the residual risk that has been identified. While the residual risk faced by the entity remains the same regardless of formal acceptance and documentation, the benefit of these actions lies in the ability to demonstrate awareness of the risks and to serve as a baseline against which future changes in residual risk can be measured and re-evaluated.

The methods of accepting and documenting residual risk will vary between entities and organizational processes, but they should fundamentally follow the same process that is used for standard, non-residual sources of risk. This ensures that such risks are not forgotten and receive the same level of tracking and care as other, more traditional types of risk.

When documenting the acceptance of residual risk, it is important to also record the justification. It may be that the risks are deemed to be so small, the entity is willing to tolerate the possibility of an adverse event occurring because the anticipated impact is minor. Conversely, the risks may be significant, but the entity is unable to reduce it any further. In scenarios such as these where the supplier, product, or service involved is critical to the entity's operations and for which no suitable alternative can be found, the entity may decide to accept a high degree of residual risk.

If high levels of residual risk are identified, it is important to escalate quickly to the correct internal decision-making bodies (such as senior leadership, risk committees, etc.) to adjudicate, as careful deliberation and investigation may be required to better understand the potential issues. Coordinating with these parties early on can provide the time necessary to properly evaluate these issues and help avoid the predicament of attempting to conduct a thorough risk review right before an important procurement deadline.

Whether the residual risk is high or low, documenting the justification for residual risk acceptance memorializes the rationale for doing so and can serve as a critical piece of evidence should an adverse event occur. Where relevant, highlighting mitigation measures that are related to residual risks can be helpful for clarifying the boundary between where a compensating control is able to provide a level of protection and where the risk remains unmitigated (the residual).

4. Supply Chain Control Documentation

Once controls are implemented, the entity should document each one in a designated, centralized repository. Using a centralized repository ensures that controls will be readily accessible and reduce the risk of duplicative or “missing” controls as may occur in a fragmented, decentralized approach. The repository itself may take a variety of different forms.

Larger entities that have invested in an ERP solution may have a dedicated module that can be used to document risks, controls, and related materials. Alternatively, a dedicated GRC tool may be utilized instead, and may offer a feature set more fully dedicated to the function of risk controls. Entities that do not have these solutions may be able to accomplish the same result by the thoughtful use of workflow management tools, databases, and document repositories.

For example, a workflow management tool could be used as part of an entity’s procurement process to automatically notify designated personnel that a given supplier is ready to be assessed for risks and have controls developed. The personnel could record controls in a database and store artifacts related to the control implementation, contracts, and supplier attestations in a document repository. Although upfront setup and configuration will be required, the entity may be able to build such a system using the tools it already has (or for minimal added cost).

For smaller entities and for those with very limited resources, controls may be documented using basic spreadsheet software. While typically the simplest and cheapest solution, this approach can have difficulty scaling beyond a certain point and result in other inefficiencies caused by concurrent or conflicting edits and a lack of proper input validation. This approach can also risk data loss or corruption due to user errors.

When documenting controls, entities should identify a core set of data fields necessary to understand the function of each control. The system used to document controls should be configured, as is feasible, to validate the data provided when new controls are entered or existing ones updated. At a minimum, such checks should ensure that required data is not missing and that the data provided matches the format of the data requested. Suggested data fields for entities to consider including in their control documentation include:

- **Control ID:** A unique identifier used to reference the control. This may take the form of an alphanumeric string (XX-YYY-01), a brief name (“Require MFA”), or both.
- **Control description:** A clear statement of the control’s requirements, any steps required, and an explanation of what the control is intended to do.
- **Control objective:** The outcome that the control is intended to achieve (e.g., prevent unauthorized access).
- **Control owner:** The role responsible for executing the control (or overseeing its execution if performed by a third party, such as the supplier).
- **Associated risk:** The risk, threat, or compliance requirement that the control is intended to address (e.g., CIP-013).
- **Frequency:** How often the control is performed (e.g., continuously, quarterly, annually).
- **Control type:** The category of the control based on how it mitigates risk (e.g., preventive, detective, corrective, though other categorical schemes exist).
- **Implementation evidence:** Description of artifacts that can prove the control is in place (e.g., logs, reports, signed checklists) and where the evidence can be found.

- **Effectiveness:** Results of control assessments to determine effectiveness for mitigating the control's designated risk (this may not apply equally to every control).

Occasionally, controls can exist in unexpected places and so remain undocumented, leading to an incomplete risk mitigation picture. Some controls are referenced by procurement materials and frequently contain risk mitigation measures written directly into a document. Items such as contracts, purchase agreements, and statements of work (SOWs) often contain many such controls and should be included in an entity's control documentation.

For example, a control providing protection against unauthorized access may be embedded as a clause in an entity's master service agreement that requires multi-factor authentication for all remote access. Instead of having separate procedures, the control is built into the legal and operational framework of the entity-supplier relationship. When feasible, this approach can lessen the number of controls that must be defined elsewhere – leading to more efficient processes – while simultaneously increasing an entity's contractual protections.

Program Documentation

Although controls frequently receive the greatest attention for documentation efforts, entities should also consider how the various programmatic elements that support their controls are documented. Escalation pathways, supply chain risk management roles and responsibilities, and risk control review cycles are all examples of elements that should be documented in addition to the controls. At a minimum, entities should consider developing documentation for each of the following areas:

- **Policy and governance:** Creates the basic framework for identifying, assessing, and mitigating supply chain risks to protect the reliability, security, and compliance posture of the entity. Examples of relevant documents include:
    - Supply Chain Risk Management program charter
    - Supplier risk management policies, including evaluation criteria for suppliers, risk assessment requirements, justification for supplier approval or rejection, etc.
    - Procurement processes, standards, and guidelines
- **Procurement:** Enforces requirements in contractual language, maintains business records, and executes business processes to ensure obligations are legally enforceable. Examples of relevant documents include:
    - Contracts, including security clauses, audit rights, breach notification requirements, etc.
    - SOWs, especially technical and cybersecurity requirements
    - Purchase orders, including compliance-specific language for relevant suppliers
- **Monitoring and oversight:** Conducts ongoing supplier performance reviews to ensure that suppliers consistently meet contractual, operational, and compliance requirements throughout the entity-supplier relationship. Examples of relevant documents include:
    - Logs or reports from third-party risk monitoring services or tools
    - Internal audits of supply chain and procurement processes

    - External audits of suppliers, including supplier compliance reviews

- **Operations:** Executes the processes and procedures to provision, modify, and revoke suppliers' access to an entity's systems and restricted spaces. Examples of relevant documents include:
    - Supplier onboarding procedures
    - Access control processes for third-party personnel
    - Supplier offboarding procedures
- **Training and awareness:** Delivers training programs for procurement and supplier management teams to ensure that all stakeholders understand their roles, responsibilities, and the importance of the controls in place. Examples of relevant documents include:
    - Training records for internal supply chain risk management processes
    - Security briefings on supplier trends, incidents, and vulnerabilities
    - Compliance/regulatory training records for controls mandated by regulation or law

Ensuring that all aspects of supply chain risk controls, including program elements, are properly documented enhances the entity's ability to monitor and demonstrate the effectiveness of their supply chain risk management program.

5. Supply Chain Risk Monitoring

After information on a supplier has been collected, their risk assessed, and controls implemented, it may be tempting for an entity to conclude that the supply chain risk management process is complete. For one-off procurements where no continuing entity-supplier relationship exists, this may be true. In other cases, however, a continuing relationship may exist, even if not formally or contractually defined.

For example, one-off procurements may require ongoing monitoring to properly mitigate risk, particularly for products containing microprocessors or other advanced electronics, to address the risk that a new vulnerability is discovered in a previously purchased product. In other cases, certain material components or products may be later found to fail prematurely or suffer from a manufacturing defect. Therefore, it is imperative that the supply chain risk management lifecycle remain a continuous process.

To help address future sources of risk, entities should have in place a robust supply chain monitoring program to detect new potential sources of risk for their suppliers and respond if their suppliers' risk posture has materially changed since they were last evaluated. Such monitoring may be accomplished in a variety of ways. In most cases, however, effective monitoring will fall into either first-party or third-party categories. Considerations for effective monitoring are provided below.

First-party Monitoring

First-party monitoring refers to the practice of using resources internal to the entity to conduct ongoing supplier risk monitoring operations. For entities early on in their supply chain risk management journey or that face significant constraints in available resources, first-party monitoring may be the most cost-effective option. However, this apparent advantage can be diminished if there are too many suppliers that the entity wishes to monitor or if too high level of detail is desired.

A smaller entity with a limited number of key suppliers may be well-served by a small, in-house team of analysts who monitor public and private channels for signs of supplier risk. Additional practices that an entity may wish to consider implementing include:

- Negotiating terms and conditions with suppliers to require that the supplier notify the entity of a security incident within a defined timeframe and require the coordination of response between the entity and supplier for such incidents.
- Attending routine threat briefings (such as may be provided by the E-ISAC, law enforcement partners, or industry trade groups) to learn of security threats that affect suppliers that the entity uses for procurements. Multiple staff members can attend the briefings to help provide coverage during vacations or other conflicts with meeting schedules.
- Signing up to receive bulletins and information on emerging security threats, incidents, and newly discovered vulnerabilities. Multiple staff members can sign up and review the information as each is available.
- Engaging with regional and national security groups (cyber and physical), including the NATF. Involvement in these groups can help entities stay abreast of emerging security threats and issues. Regional security calls, such as the weekly Midwest Reliability Organization (MRO) Security Advisory Council Threat Forum (SACTF) calls, can be another valuable source of information.
- Monitoring social media feeds to be aware of security incidents that affect the suppliers the entity uses. Many security researchers use social media as a method of announcing their discoveries, and threat actors also sometimes use social media to highlight their latest victims. While a high degree of discernment is needed to assess the actual impact, social media channels can be a valuable early warning indicator for potential issues.
- Sharing information from the threat briefings, internal assessments, and security or threat briefing webinar(s) with other authorized entity employees. Information can be analyzed regarding the most relevant items for the entity (and the entity's current suppliers) and shared with the staff involved with procurement and supplier risk assessments.

In addition, other operational strategies exist to further maximize the effectiveness of first-party risk monitoring teams. Automation can play a pivotal role in driving efficiencies, reducing tedious or repetitive tasks, and acting as a force-multiplier for existing staff. In certain cases, staff augmentation via the use of temporary or contract employees can help demonstrate the value of additional staff before committing to the increased headcount. Finally, the use of checklists or SOPs can be invaluable in keeping processes efficient and effective. This can be particularly true for threat intelligence or analysis work, where staff are frequently required to balance their time between researching the scope and impact of a potential issue, preparing communications, and performing risk assessments.

Third-party Monitoring

In contrast to first-party monitoring, third-party monitoring involves the use of a contracted third party to review a selection of an entity's suppliers for changes in security posture, organizational changes (such as merger or acquisition), and other sources of risk, such as reputational, legal, regulatory, and financial. In addition, third-party monitoring services also typically provide a certain level of analysis with the service.

For example, a service may calculate a numerical score to represent the potential risk that a given supplier possesses, allowing risk decisions to be made based on the value of the score. In other cases, the service may offer to issue, receive, and analyze the results of a risk questionnaire or assessment. Other options may include the ability to conduct on-site assessments for an additional fee.

In all cases, entities must carefully consider their intended use of third-party monitoring services to ensure that they obtain the full value that they anticipate. Unlike first-party monitoring under the direct control of the entity where changes in scope, processes, and output can be made quickly, third-party monitoring services are much more fixed. Therefore, it is important for the entity to consider in advance how they wish to engage third-party monitoring services. Practices to consider implementing include:

- Conduct due diligence on the service provider
    - Evaluate the provider’s expertise, financial liability, certifications, and track record in third-party risk management
    - Benchmark against other entities to learn which third-party monitoring provider they are utilizing and their experience so far
    - Review the provider’s security controls, data handling practices, and incident response capabilities
    - Validate the provider’s ability to monitor suppliers continuously and effectively identify incidents
    - Involve several teams in the supplier evaluation process
- Define clear roles and responsibilities
    - Establish a detailed agreement outlining the scope of monitoring, reporting requirements, and escalation procedures
    - Establish roles and responsibilities for both the provider and internal teams
    - Consider identifying a dedicated staff liaison to interface between the entity and provider
- Implement questionnaire and continuous monitoring process
    - Work with the provider to determine areas of risk to be monitored
    - Where possible, use structured questionnaires and risk scoring models for initial and ongoing supplier evaluations
    - Provide a list of suppliers and any other parties that will be monitored on the platform
    - Align on cadence of questionnaire process and communication plan for supplier engagement and remediation
    - Require the use of real-time monitoring tools (e.g., automated vulnerability scanners, security ratings platforms, threat feeds updated no less than daily)
- Maintain visibility and oversight
    - Require regular reporting (including minimum update thresholds) on all monitored supplier’s security posture, including updated metrics, risk ratings, and remediation status

    - Ensure configurable alerts and dashboards are provided for customized visibility into changes in supplier risk posture
    - Implement dashboards or portals that allow internal teams to view real-time or periodic updates.
- Establish performance metrics and service level agreement (SLAs)
    - Define SLAs for monitoring frequency, issue resolution timeframes, and reporting accuracy
    - Include key performance indicators (KPIs) to measure effectiveness
    - Conduct weekly status calls and quarterly business reviews to track provider's performance and to provide ongoing feedback
    - Validate skill sets of entity staff to ensure understanding of information being asked and provided by the provider
- Integrate with internal risk management processes
    - Ensure the provider's findings are integrated into the entity's risk register and can influence internal decision-making
    - Align outsourced monitoring with your supplier lifecycle management processes
- Plan for incident response and escalation
    - Define how incidents involving suppliers will be communicated, escalated, and resolved
    - Ensure the provider has a tested incident response plan that includes coordination with your internal teams
- Review and update contracts periodically
    - Reassess the service agreement regularly to ensure it reflects current risks, technologies, and business needs
    - Include provisions for termination or transition in case of poor performance or strategic changes

These practices can be used to ensure that the use of third-party monitoring services deliver the value that the entity expects. As the service provider's capabilities, pricing, and expertise may change over time, so too may the needs and budget of the entity. Therefore, it is important that these practices are regularly executed to ensure that services and expectations are properly matched and continue to be of net benefit for both parties.

Hybrid Monitoring

When deciding between first-party and third-party monitoring, several factors need to be evaluated. Frequently, the choice depends on the level of risk associated with an entity's suppliers, the availability of internal resources, and the need for specialized expertise. First-party monitoring allows for deeper insight into internal processes and may be necessary for high-risk suppliers, whereas third-party monitoring can offer greater efficiency and scalability, especially when internal bandwidth is limited. Leveraging a third-party monitoring service can also help entities finish risk assessments faster, gain access to new tools and technologies, and redeploy internal staff to higher-value activities.

A balanced or hybrid approach that leverages both methods is a strong method that can help entities achieve a more robust monitoring program and provide more comprehensive oversight into an entity's biggest sources of supplier risk. Entities that pursue this approach should have a set of prepared criteria to decide when a supplier should be monitored using internal resources, a third-party, or both. Factors to consider when developing these criteria include:

- Efficiency - Third-party providers can frequently collect risk assessment data on an entity's behalf. This can allow an entity to move away from adding headcount and manual, one-off processes towards more automated methods and continuous monitoring.
- Expertise - Some third-party monitoring services can provide highly specialized expertise and may be able to leverage a team of dedicated experts (such as lawyers, cybersecurity engineers, financial advisors, etc.) to evaluate the impact of changes to a supplier's risk posture.
- Independence - Third-party providers can offer more independent judgement than first-party teams as there is no incentive to inflate a supplier's results (as may exist for an entity's critical supplier for which there is no market alternative).
- Knowledge - Internal staff often have more understanding in how a given supplier is used by the entity, whereas third-party providers may lack knowledge of internal security or business-specific product use and may not be as invested in accuracy.
- Resources – There may not be sufficient resources – monetary or otherwise – to pursue added headcount for improved first-party monitoring, or conversely, to hire the services of a third-party monitoring provider.
- Risk - High-risk suppliers may require first-party assessments to provide the level of detail necessary to properly assess risk.
- Technology - Third-party solutions may be able to offer fully built, plug-and-play integrations for management and tracking with the entities existing systems. Conversely, first-party teams may have built a mature and well-integrated technology ecosystem that is difficult or impossible to replicate externally.
- Urgency - Operational demands may force a selection of the option that can provide immediate (or near-immediate) results.

Supply chain processes have evolved from a simple procurement function into having a more strategic role in accelerating business growth. Accordingly, the careful use of first- and third-party monitoring approaches can be used to keep up with the increasing demand and operational tempo of modern supply chain procurement processes.

6. Supply Chain Risk Monitoring Documentation

If an entity's current supplier had a particularly serious incident five years ago, how would the entity's current supply chain personnel use this information to inform current business decisions and negotiations (such as during contract renewal)? Indeed, if the department responsible for performing supplier risk assessments had experienced significant turnover or reassignment in the intervening years, would the current staff know about the incident at all?

It is this scenario – and others like it – that effective risk monitoring documentation is designed to address. New risks that are identified during supplier monitoring should be tracked and documented using a predefined and repeatable process. Documenting these risks allows an entity to leverage their investment in supplier monitoring for future decision-making, making this historical data an appreciating asset from a risk perspective.

Documenting supplier incidents or newly identified supplier risks can be as simple as recording them into a spreadsheet, recording the basic details into a third-party risk monitoring or tracking service, or using a custom-made, internally developed tool that cross-references the entity's data, assets, and other resources with the supplier and incident. Regardless of the approach used, the overriding objective is to have a well-defined process and to follow it consistently each time a new incident or risk is identified during supplier monitoring.

After an entity conducts a supplier risk assessment, makes their purchase decision, and has implemented controls, there are a few options for an entity to consider if their monitoring program reveals a new supplier incident or risk during contract performance (or other ongoing business relationship) with the supplier. Primarily, these options include accepting the risk, mitigating the risk, and refusing the risk.

These options largely correlate to the definitions provided in the *Risk Dispositions* section of the *NATF Supply Chain Risk Assessment Guidance* [7], which provides further guidance on these options. However, there are some considerations that are specific to incidents occurring during supplier monitoring that are discussed next.

Acceptance

Depending on the level of risk created by a supplier's incident – and considering existing controls – the entity may decide to accept the risk that was identified through supplier monitoring. This may be accomplished via the use of formal risk acceptance letters or similar documents and workflows. For some entities, this risk is accepted by a senior representative of the business unit currently engaged with the supplier. For others, a centralized department – such as risk, legal, compliance, or a similar department – may accept the risk on behalf of the entire organization.

For documentation purposes, entities should note on the risk acceptance letter the supplier involved, details of the identified risk (including the results of any investigation), and any existing contracts or ongoing relationships with the supplier. The letter (or other record of risk acceptance) should be stored with the entity's existing records on the supplier. Maintaining records for such acceptance is critical, as multiple incidents with the same supplier – even if individually accepted – may cause the entity to take a different course of action if it becomes clear that a trend is developing, or if the aggregated risk becomes too high for the entity to continue to accept.

Mitigation

The purpose of mitigation is to work with the supplier to close any open findings discovered during supplier monitoring. Typically, this requires either the entity or their contracted third-party risk management assessor to work closely with the supplier to collaborate on improvements, and ideally to resolve the risk if possible. Using a standardized template can be an effective method to ensure that information on mitigation efforts is collected and recorded uniformly. Suggested elements to consider including when developing a mitigation template include:

- Detailed scope and description of the product or service – this helps decision makers better understand the risk to the entity (particularly if they were not present during meetings).

- Key information provided by the supplier – this may include their understanding of the incident or other relevant technical details (such as their cybersecurity posture).
- List of attendees during meetings – This can help prove participation and aid follow-up later. Entities may wish to ensure there is representation from their relevant business unit to explain how the product or service is used.
- Contract renewal date – Entities may use this date to determine the risk posed by the time remaining in the contract and serve as a reminder for when terms can be renegotiated.
- List of open findings (compared against last assessment if applicable) – Provides a current list of outstanding issues and how they compare to prior issues identified.
- Business impact – The potential effect on the entity if the relationship with the supplier were to be terminated.
- Customer impact – The potential effect on the entity's customers and their experience if the relationship with the supplier were to be terminated.

When conducting mitigation efforts with suppliers, it is important to have a defined process, along with maximum time limits, to ensure that remediation efforts do not unnecessarily linger without resolution. However, the dates and sequencing of steps may require modifications or exceptions based on extenuating circumstances.

Refusal

Typically, the refusal of a risk is fatal to a contract, as it indicates that the entity is not willing to accept or mitigate the risk. While refusing a risk during the initial risk assessment process may have little impact on the entity before any agreements are in place, refusing a risk during the performance of a contract with a supplier may have significant ramifications, including early termination fees or other penalties. Accordingly, the decision to refuse risk and terminate a contract mid-performance is a decision that should be carefully considered and well-documented. Elements that entities may wish to include are any triggering incidents or circumstances that led to the refusal, the justification for refusing the risk, and a listing of the affected contract, business units, and processes that would be affected by the refusal.

Additional Considerations

When pursuing any of the options above, entities may also wish to document key details of their decision via a database or other platform that can be easily searched, and which integrates with other risk management or procurement tools. As multi-page narrative documents may be a poor fit for such a purpose, an entity may wish to record another copy of their decisions in a leaner, more limited format that better supports these use cases. Fields to consider using, along with suggested values, include:

- Supplier name (name and/or internal ID to identify supplier)
- Coordinator (person leading entity response)
- Approver (for accepted risks)
- Status (In review; Pending acceptance; Pending mitigation; Pending risk assessment; Closed)
- Date reported (date issue was discovered)

- Estimated resolution date (when current efforts are expected to be complete)
- Due date (when the issue must be resolved per policy unless an exemption applies)
- Severity (High; Medium; Low)
- Resolution (Accepted; Mitigated; Refused; False positive; Unresolved)

7. Conclusion

The supply chain lifecycle of any modern entity is a highly complex and interdependent process that touches on many adjacent parts of the organization to function well. Multinational trade issues, security risks, and product scarcity are but some of an ever-increasing array of challenges that supply chain practitioners must navigate, frequently with significant constraints on their available resources. Accordingly, it is vital that entities take advantage of the resources available to them to improve efficiencies and reduce their level of supply chain risk.

The guidance provided in this document represents just one portion of a larger process, the *NATF Supply Chain Security Assessment Model* [4], that the NATF has developed to aid entities in their performance of effective supply chain risk management. Entities interested in learning more are encouraged to review this and other publicly available resources on the NATF's *Supply Chain Industry Coordination* website [9]. As supply chain risks continue to change and evolve, the NATF is committed to developing relevant guidance to keep the North American bulk power system safe, secure, reliable, and resilient.

References

[1] Federal Energy Regulatory Commission, "2023 Lessons Learned from Commission-led CIP Reliability Audits," 11 December 2023. [Online]. Available: https://www.ferc.gov/sites/default/files/2023-12/23_Lessons%20Learned_1211.pdf.

[2] North American Electric Reliability Corporation, "CIP-013 RSTC Letter and SAR 09-18-2023," 18 September 2023. [Online]. Available: https://www.nerc.com/globalassets/standards/approved-standards/cip/cip-013/cip-013-rstc-letter-and-sar-09182023.pdf.

[3] Federal Energy Regulatory Commission, "Docket Nos. RM24-4-000 and RM20-19-000; Order No. 912," 18 September 2025. [Online]. Available: https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20250918-3077.

[4] North American Transmission Forum, "NATF Supply Chain Security Assessment Model," 20 November 2024. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-supply-chain-security-assessment-model.pdf.

[5] North American Transmission Forum, "NATF Supply Chain Security Criteria," 20 May 2025. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-supply-chain-security-criteria.xlsx.

[6] North American Transmission Forum, "Energy Sector Supply Chain Risk Questionnaire," 20 May 2025. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire.xlsx.

[7] North American Transmission Forum, "NATF Supply Chain Risk Assessment Guidance," 11 March 2025. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/industry-initiatives/supply-chain/natf-supply-chain-risk-assessment-guidance.pdf.

[8] North American Electric Reliability Corporation, "Reliability Standards > CIP - Critical Infrastructure Protection," [Online]. Available: https://www.nerc.com/standards/reliability-standards/cip.

[9] North American Transmission Forum, "Supply Chain Industry Coordination," [Online]. Available: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.