NATF Supply Chain Risk Assessment Guidance

Version 1.0
Document ID: 1731
Approval Date: 3/11/2025

Versioning

Revision History

Date	Version	Notes
3/11/2025	1.0	Initial version

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

Versioning 2
Contents 3
1. Purpose 4
2. Scope 5
3. Definitions 5
4. Supplier Risk Assessment Methodologies 6
5. Additional Assessment Considerations 12
6. Risk Dispositions 16
7. Documentation Practices 17
8. Integration with Enterprise Risk Management 20
9. Conclusion 21
References 22

1. Purpose

In today's increasingly interdependent global economy, supply chains have grown into complex networks of suppliers, integrators, manufacturers, contractors, service providers, resellers, subcontractors, and other related providers that serve an ever-increasing array of customers. In this dynamic and shifting landscape, how can entities ensure that their suppliers – many of which are themselves customers of other suppliers with their own unique set of requirements – are sufficiently secure and resilient and do not pose undue risk to the mission and function of the entity?

In this document, various methodologies for performing supplier risk assessments are examined, along with a discussion on the relative advantages and disadvantages of each method. As even the best risk assessment would be of limited value unless it is also properly recorded, various documentation techniques are discussed along with suggested risk dispositions and definitions. Finally, a brief review of how supplier risk assessments fit into a larger Supply Chain Risk Management (SCRM) program is provided, along with additional resources to help entities implement and expand upon the approaches described in this guidance.

This document may be considered a logical expansion of "Step 3: Conduct the Risk Assessment" of the *NATF Supply Chain Security Assessment Model* [1], which calls for purchasing entities to have a methodology for performing supplier risk assessments and to document the results of their risk assessments.

Given the diverse business needs of entities, the technologies involved, and varying tolerances for risk, performing an effective risk assessment of current and potential suppliers is not always a straightforward task. Likewise, keeping such assessments current, documenting results consistently, and incorporating findings into actionable plans can also be a challenge for some entities.

These realities were evident in the report from the Federal Energy Regulatory Commission (FERC), *2023 Lessons Learned from Commission-led CIP Reliability Audits*, which found that "Audit staff observed that some entities lacked consistency and effectiveness when evaluating vendors and procuring vendor-supplied equipment and software" [2, p. 17]. FERC also observed challenges in follow-up, noting in the same report that "In some cases, staff found that entities' supply chain risk management plans did not include processes or procedures to respond to risks once identified" [2, pp. 17-18].

Accordingly, it is apparent that entities may benefit from specific guidance on how to effectively conduct risk assessments and document their findings in a way that facilitates follow-on risk mitigation activities. It is in the spirit of continuous improvement that the recommendations in this guidance are offered; 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 most applicable to entities who rely on the products and services of suppliers and are responsible for their procurement. Accordingly, most of the discussion and examples provided use the term "entities" to denote the party performing the risk assessment. 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 identify sources of risk. By better understanding the unique obligations of entities, suppliers can also be more responsive to the needs of their customers.

As fundamental risk assessment principles are widely applicable to entities and suppliers serving different sectors and subsectors, this guidance is being provided to industry with the intention of enhancing an organization's capability to effectively identify, assess, and document supplier risk regardless of size, program maturity, or region.

The scope of this guidance is focused on "Step 3: Conduct the Risk Assessment" of the *NATF Supply Chain Security Model* [1, p. 9]. In particular, this guidance supports and further explores the two main sub-steps listed therein:

- The entity should have a methodology to perform supplier risk assessments.
- The entity should document the results of risk assessments.

An important note is that although this guidance in some cases references product risks to illustrate risk assessment principles and provide example scenarios, this guidance is primarily focused on supplier risk assessments. An entity may elect to perform a supplier risk assessment, a product risk assessment, or both, depending on the individual procurement and compliance requirements.

In order to maintain focus on these subjects, other aspects of supply chain risk management, such as how an entity may decide to accept risk, who in the organization can (or should) accept risk, or specific methods of tracking a supplier's performance over time are not in scope for this guidance. While these are worthy considerations, they more naturally map to other parts of the *NATF Supply Chain Security Model* and so are not addressed herein. Resources for additional consideration are referenced throughout the document for the interested reader.

3. Definitions

FERC

Federal Energy Regulatory Commission

NERC

North American Electric Reliability Corporation

4. Supplier Risk Assessment Methodologies

The following section describes a variety of assessment methodologies that may be used to identify supplier risk. The examples provided are not intended to be an exhaustive or exclusive listing of all possible methodologies, but rather a showcase of various effective strategies. Alternative approaches not listed may also be similarly effective as those contemplated here, and it is expected that any methodology will require some degree of customization to fit the unique needs, process, and organizational structure of the entity.

Although different entities will invariably have different risk assessment processes, there are certain elements which appear in many environments that represent good general practice. These steps have been compiled into a simplified example workflow, shown in Figure 1, as a roadmap for understanding the general risk assessment process and how different methodologies may be incorporated within various review steps.

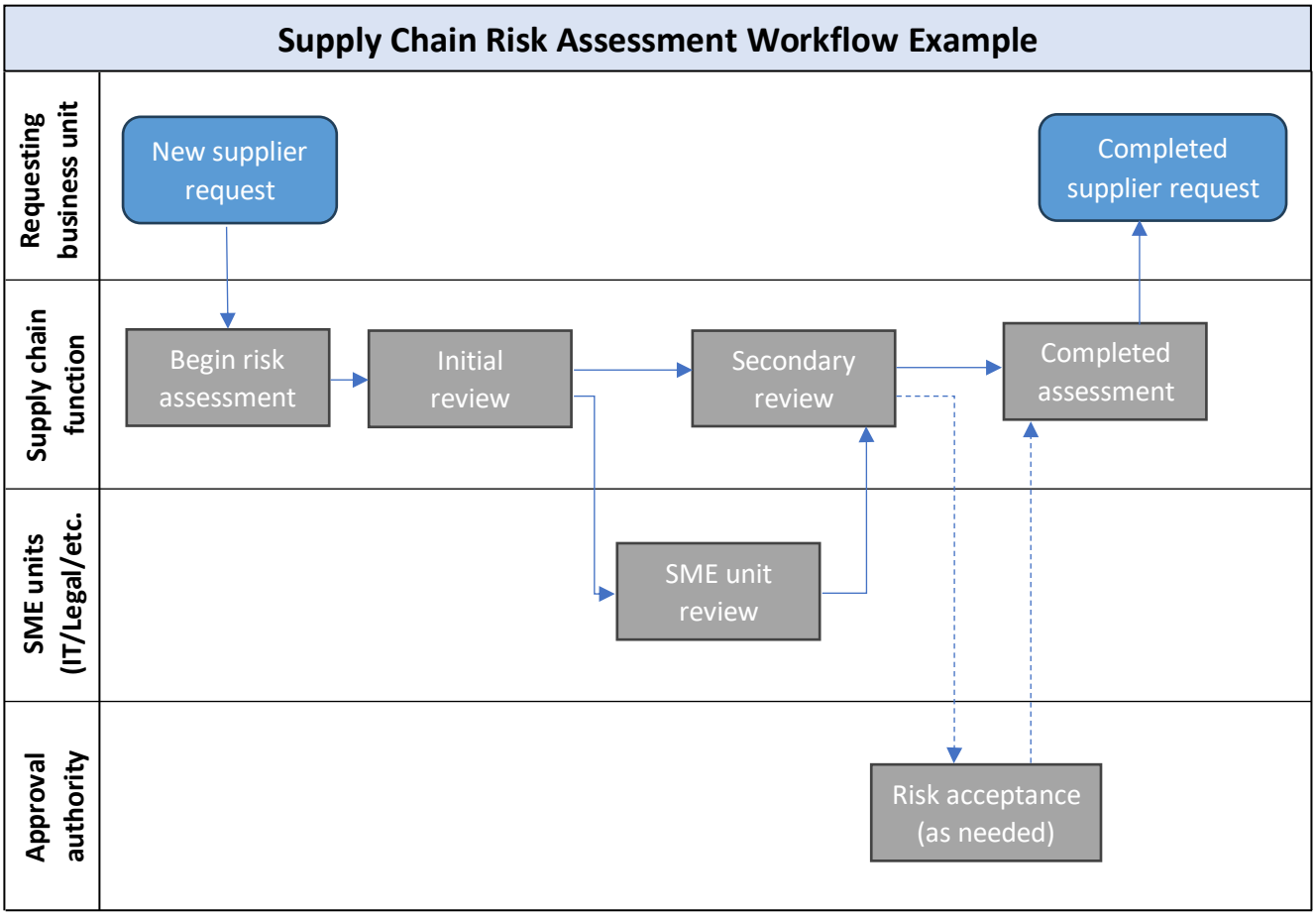

Figure 1: Supply Chain Risk Assessment Workflow Example

The “Supply chain function” in the example workflow above refers to whichever department, team, or organizational unit has primary responsibility for supply chain risk assessments. Notably, this general risk assessment workflow applies whether or not there are compliance requirements. Although there may be additional decision points and processes that are specific to compliance obligations, the overall workflow should follow the same major steps regardless to maintain consistency. However accomplished, it is imperative that each potential procurement, product, or service be consistently evaluated for the risks they may pose.

Point System Method

The point-based method is a structured approach for evaluating supplier risk by assigning scores to predefined risk factors and calculating a total risk score. This method allows entities to objectively assess and compare multiple suppliers and quickly identify high-risk suppliers.

One of the most common and effective implementations of the point-based method involves entities adopting a supplier risk questionnaire or similar tool that specifies predetermined risk factors to analyze. The questionnaire is provided to the supplier to respond to and return to the entity. Points are then assigned by the entity based on how satisfactory the entity considers a given supplier's response on each questionnaire item. Additionally, some questionnaires allow certain questions to have a higher or lower weight to represent areas of greater or lesser importance to the entity.

Both answers and weighting (if offered) are typically assigned values on a numerical scale which are computed for each question and summed to provide a total risk score. Because expertise in different risk areas may be distributed throughout an entity, some sections may be assigned to various subject matter experts (SMEs) or departments to score.

One questionnaire that provides for rapid scoring is the *Energy Sector Supply Chain Risk Questionnaire* [3], a simplified version of which is shown in Figure 2. This questionnaire offers answer and weight values for each question in a Likert scale (1 – 5) that automatically re-calculates as the questionnaire is scored.

Energy Sector Supply Chain Risk Questionnaire Open Distribution for Supply Chain Materials			**Answer**	**Weight**	**Score**
Change and Configuration Management		**Primary or Supporting for NATF Criteria**	**Category Score**		**149**
CHNG-01	Do you have a documented and currently followed change management process (CMP) for the systems and networks under your control?		4	5	20
CHNG-02	Does your organization have policies and/or procedures to ensure that only application software verifiable as authorized, tested, and approved for production is placed into production and/or released for client use?	Supports (53, 54)	3	3	9
CHNG-03	Do you have a process to assess and apply security patches in your environment within a predetermined timeframe?	Primary (50)	3	3	9
CHNG-04	Do you provide a specific list of, and justifications for, required logical ports (which may include limited ranges) and services required for its deliverables (either products or services)?	Primary (56)	2	3	6

Figure 2: Excerpt from Energy Sector Supply Chain Risk Questionnaire

Once scores are determined, they should remain static for the remainder of the risk assessment process to ensure consistency. "Grading on a curve" or similar post-assessment adjustments should be avoided to ensure the assessment remains objective and reliable. A limited exception may exist where responses were misunderstood by the scorer or there are other fundamental errors of fact.

After the score has been calculated for several potential suppliers, scores may be plotted on a bar chart or similar graphing technique to easily demonstrate the difference in risk. An example is provided in Figure 3.

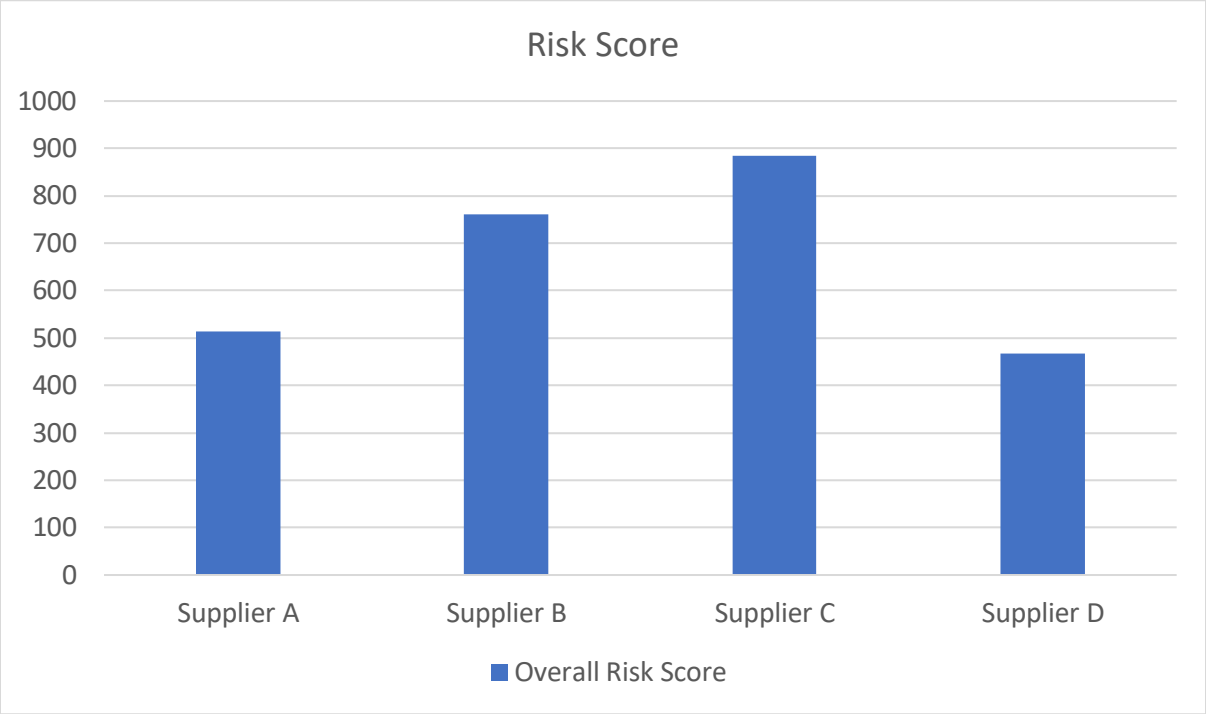

Figure 3: Example risk scoring chart

Committee Method

Supply chain risk assessments can be difficult to complete by a single person. It is challenging for one individual to have diverse knowledge of the many systems that a product or service may involve and to understand how those systems integrate with existing assets. Individuals with the appropriate expertise may be in different organizational groups or may be contracted out. Additionally, an entity will rarely share the same organizational structure or risk tolerance as another entity. One entity may view a risk as unacceptable while another entity may accept such risk without exception. Therefore, forming a diverse team that incorporates a variety of expertise is often beneficial in the risk evaluation process to ensure key concerns are not overlooked.

For example, a cyber analyst may have knowledge of the best cyber asset for security but may not understand how that asset will function or integrate with other assets to perform the intended function. An engineer may have knowledge of the desired outcome and performance of the cyber asset but may not understand the security vulnerabilities that it may introduce into the environment. A procurement specialist can provide information on prohibited purchases, availability, and the best strategy to obtain cyber assets and purchases but may not be familiar with the latest vulnerabilities affecting the product. Accordingly, forming a committee with a diverse background can provide a comprehensive approach for performing risk assessments in an efficient and cost-effective manner.

Some areas of expertise to consider when developing a team or committee approach are:

- Security (Cyber/Physical/Data Protection)
- Compliance
- Engineering
- IT/networking/telecommunications
- Procurement
- Supply/warehouse
- Legal

It is also important to consider the time a committee may spend in meetings and reviewing risk assessments. In some cases, a smaller team may be more appropriate for performing the risk assessment, with a larger team involved in any subsequent approval process. In other cases, the reverse may be true. Entities may also have separate teams, depending on the criticality (e.g., high/medium/low impact BES Cyber Systems), geographic region, or other considerations. In all cases, it is important to keep the dual tenants of efficiency and completeness in mind when developing committees and their memberships to avoid making the risk assessment process more onerous or time-consuming than is warranted.

Finally, a committee approach may also be able to incorporate other risk elements, such as risks to an entity's procurement strategy, that may be difficult to capture via other methodologies. For example, a business unit may wish to purchase a new or different item than planned to expedite progress on a project, but it is important to consider downstream risks, such as the modified cost of maintaining the asset, need to maintain a reserve or emergency storm supply, and future potential acquisition difficulties. While separate from the direct risk that a given product may pose, these indirect risks can nonetheless represent a threat to an entity's operational capabilities and should be incorporated into a holistic risk analysis. A committee approach to the risk assessment evaluation can thus be an excellent way to incorporate these concerns.

Third-Party Risk Assessor Method

This approach utilizes a third-party assessor to complete an independent assessment of a supplier. This is based upon the ERO-endorsed practice of relying on the work of others as a means of supporting reasonable assurance that defined reliability and security objectives are being met by suppliers. The third-party assessor should use a security framework, NATF Questionnaire, or other predetermined criteria as a baseline for their assessment. The result of the assessment is then used by the entity as an input to the risk assessment process to identify risk and mitigate as appropriate.

In NERC's Compliance Monitoring and Enforcement Program (CMEP) document *ERO Enterprise CMEP Practice Guide: Using the Work of Others* [4], NERC acknowledges the benefit of using third-party risk assessors as part of a holistic supply chain risk management program, but cautions that the mere use of such a resource by itself is not sufficient. The entity must be able to demonstrate how the information obtained from third-party risk assessors is used to effectively meet the goals of their program, and that the provider themselves is qualified to perform these activities through sufficient independence, credentials, and certifications.

As part of this approach, the entity should understand how the thirty-party assessor collects and verifies the accuracy of the information obtained from the supplier. Controls must be in place to monitor the quality of the third-party risk assessor and the qualifications of the individuals conducting the assessment. For example, an entity may consider reviewing sample reports, participating in question sessions with the supplier, reviewing third-party assessor training, and employing other information gathering techniques. The assessor should also

have a process for updating their questions in alignment with any updates made to the frameworks they may use.

Other capabilities to consider when using a third-party assessor are whether they offer continuous monitoring and notification of supplier risks, dashboard visibility, integration with internal contract tracking tools, and tracking of supplier mitigations. While these capabilities are not required to use this methodology, they can assist in other aspects of supply chain risk management and enhance overall program effectiveness. Additionally, resources like the ERO-endorsed *NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors* [5] provides practical consideration for when use of independent third-party judgement is beneficial, such as during program inception or to supplement constrained internal resources. The use of third-party risk assessors provides a structured approach with standardized risk assessments.

Other use cases for third-party risk assessors may include:

- Performing high-volume tasks for lower risk suppliers, freeing internal staff to concentrate on more complex assessments.
- Performing specialized complex tasks such as analysis of product software bill of materials (SBOMs).
- Performing repetitive tasks such as continuous monitoring of high-risk suppliers.

Phase-Based Method

A phase-based approach (also known as a "funnel") involves the use or two more distinct segments of evaluation as part of an overall risk assessment. Typically, each phase has its own set of requirements that must be met in order for a potential supplier to remain eligible for consideration. Suppliers that do not meet such requirements are set aside as other suppliers continue through the risk evaluation process.

This approach is very similar to the phase-based approach commonly used for procurements generally. In this example, an entity may identify the need for an industry-provided solution and issue a Request for Information (RFI) to several suppliers to learn more about their specific offerings. After evaluation, some suppliers may be dropped from consideration as their offerings do not meet the project requirements. The remaining suppliers are then issued a Request for Proposal (RFP) to solicit bids for the project, where again some may be dropped based on their bid. Finally, a demo of each supplier's solution is provided, after which the final supplier is selected. Each major step, or phase, of this example is shown on Figure 4.

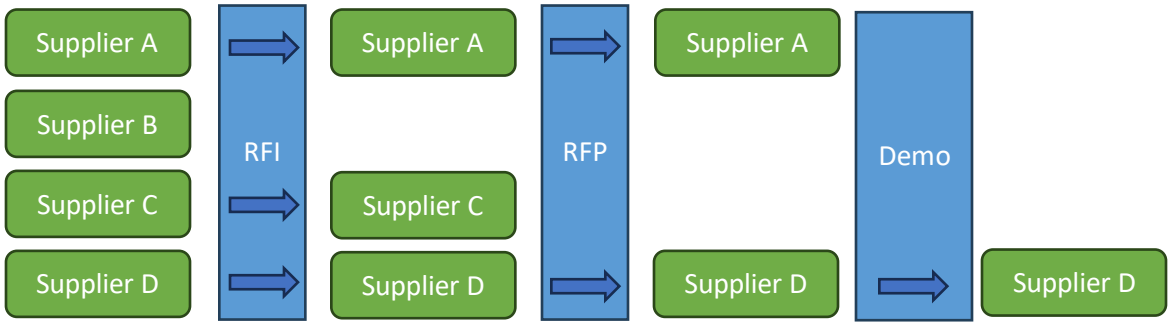

Figure 4: Example phased-based workflow for procurement

A phase-based approach to risk assessments works in a similar fashion. For example, four potential suppliers for a given procurement are identified by an entity and evaluated based on what public information is available via open-source intelligence (OSINT) collection. After review, Supplier B is found to operate in a geographical region that the entity has chosen not to do business in and is dropped from further consideration. The remaining three suppliers are then submitted for evaluation by the entity's third-party risk management (TPRM) solution provider. After reviewing the reports generated by the TPRM provider, Supplier C is found to have had several recent breaches and exceeds the entity's tolerance for risk, leaving only Supplier A and D for further consideration. The two remaining suppliers are sent the entity's risk questionnaire, and after an evaluation of their responses by the entity's Subject-Matter Experts (SME Eval), Supplier D is found to have the lower overall risk and is the one recommended for procurement. Figure 5 shows this example's workflow.

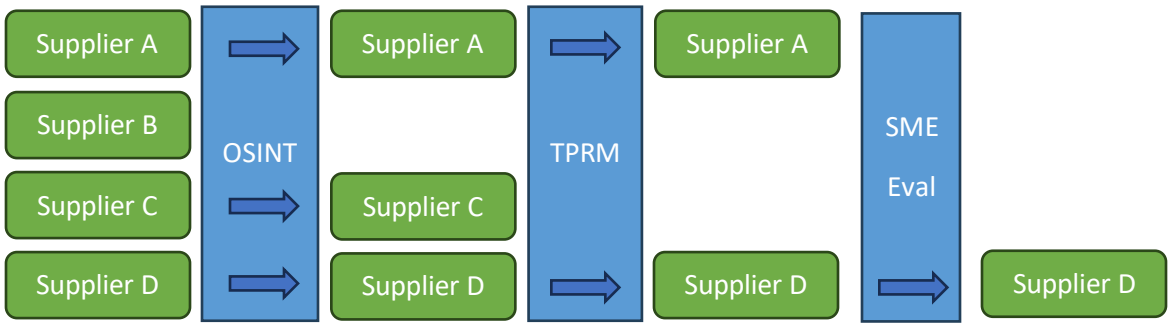

Figure 5: Example phased-based workflow for risk assessment

In practice, a phase-based methodology may have more or fewer phases than those described in this example and may involve different review processes than those listed here, but in general, the principle of a staggered and stepwise evaluation process remains the same.

Consideration should also be given to the level of effort required to complete each phase by both the requesting entity and the potential supplier. As each phase is delimited by a decision from the requesting entity, care should be taken to balance the number of phases with the entity's ability to effectively and efficiently conduct reviews and make decisions.

Likewise, consideration should be given to suppliers and the level of effort needed to respond to such requests, balancing the entity's desire for extensive information with the suppliers' ability to provide it. Using standard industry resources, such as the *NATF Supply Chain Security Criteria* [6] or *Energy Sector Supply Chain Risk Questionnaire* [3] can help reduce the administrative burden for suppliers and increase the likelihood of a complete response.

Additional examples of phased-assessment workflows are illustrated in Figure 6.

While the specifics of implementations vary, a benefit of a phase-based assessment is that potential for risk is evaluated through a greater number of perspectives, leading to a fuller picture of the actual risk that a potential supplier represents. The main drawbacks of incorporating additional assessment methodologies are the additional resources required to perform them, along with the additional time that such assessments may require. These additional time and resource costs may be partially mitigated by technological, process, or workflow capabilities. For example, a potential supplier's responses to a risk questionnaire could be partial or entirely scored, following the point-based approach. Alternatively, a supplier's responses could be automatically routed to multiple designated internal teams (e.g., legal, IT, compliance) for manual review, allowing the teams

to work asynchronously and avoiding the scheduling bottlenecks that can sometimes occur when attempting to gather many teams together at the same time in a traditional committee approach. Ultimately, the ideal approach is one that strikes an appropriate balance between the level of review required and the available resources of the organization.

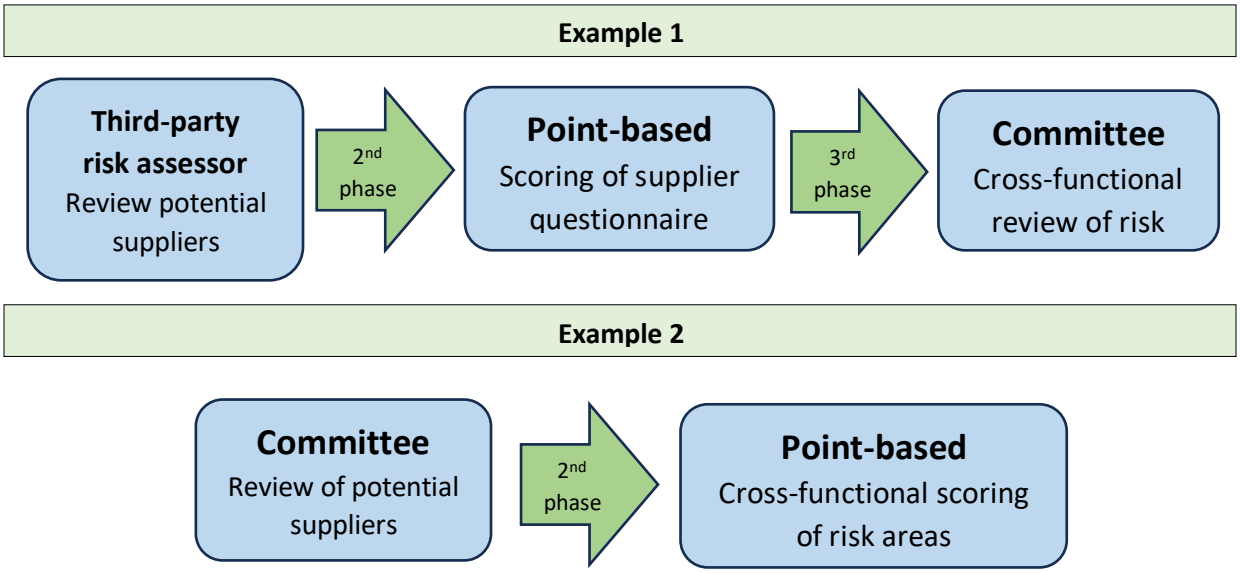

Figure 6: Phase-based assessment examples

5. Additional Assessment Considerations

Apart from the specific methodologies that an entity may use to perform risk assessments, there are a number of other considerations that should be addressed as part of a mature supply chain risk management program. A selection of key assessment considerations is provided below.

Cross-Functional Review

Each organization has a unique business structure that is distinct to its mission, culture, and regulatory environment. Many organizations are matrixed in functional responsibilities, whereas others may have indirect, "dotted line" reporting structures that denote a certain level of responsibility to various other organizational units. Regardless of the approach taken, it is unlikely that any individual business unit will possess the expertise needed to perform a complete risk assessment independent of the input from other business units. It is this scenario that requires comprehensive and consistent cross-functional reviews.

When designing an effective supply chain risk management program, it is important that the risk assessment process incorporates experts from various fields, such as legal, supply chain, information technology (IT), cybersecurity, physical security, business owners/unit, procurement, compliance, and other relevant areas. While not every procurement requires the same level of review or effort from each department, it is important that each area understands their role in the review process.

While cross-functional reviews may often be used in a committee approach, such as an advisory committee with representation from multiple departments or business areas, it may also take other forms, such as each department using their own point-based system to calculate an area risk score, with scores from the various areas added to calculate a total risk score.

Risk Mitigation

Risk mitigation, which may be formalized as risk memos, risk letters, or similar documents, may be utilized to document risks that the supplier will not or cannot immediately remediate. For each risk assessment by the entity, risk mitigations should be created if risks are not adequately mitigated by contract language and/or supplier security capabilities, policies, or procedures. Documentation should include identification of the risk to be mitigated, how the risk will be mitigated, and the major steps to be taken to mitigate the risk. Some risk mitigations may be incorporated into an entity's risk assessment documentation, whereas others – particularly for large-scale procurements – may exist as a separate document. For any risks that will be accepted without further mitigation actions, the justification and approval for accepting the risk must be documented; documenting risks is further explored in section 7: Documentation Practices.

Questions to consider when developing risk mitigations include:

- What are the open findings and how do they impact the entity?
- What is the business impact of severing the relationship with the supplier?
- Are there alternative suppliers able to provide the needed services/good without risk acceptance (or perhaps a lesser degree of risk acceptance)?

Risk Exception Handling

Risk exceptions are created to ensure critical risks are accounted for and properly considered for those risks that will not or cannot be fully mitigated via other measures. Risk exceptions may also be referred to as "risk acceptance" or similar wording. Regardless of terminology, the outcome is the same: the entity is formally recognizing that a risk exists and is willing to tolerate its continued existence. In some entities, different degrees of risk acceptance may require different levels of leadership approval; a risk identified as "critical" may require the approval of a vice president of a certain department, for example. At other entities, all risk exception requests, regardless of severity, may need to be accepted by a senior leadership figure. Different entities follow different processes, depending on their regulatory environment, services offered, and appetite for risk. Regardless of approach, a defined risk acceptance process should be in place with senior leadership support and oversight.

Additionally, processes must also be in place to allow for the procurement of assets, products, or services during an emergency. Such risk may be temporarily accepted in order to restore service or core business functions but should follow the organization's established risk assessment process as soon as is feasible. The emergency procurement function should be well-defined in advance of use (including what conditions qualify for emergency procurement) and have the necessary internal approvals to avoid unnecessary or inappropriate purchases.

Risk Tiering

Although risks do not naturally align themselves into convenient quantities, it may be nonetheless useful to compartmentalize identified risks into defined levels, or tiers. Some entities recognize three tiers of risk, such as High, Medium and Low, or perhaps alternatively, Level I, II, and III. Others may simplify to only two tiers, such as High or Low risk, and still others recognize four (or more) tiers. The right level of depth depends on the

organization's desire for granularity and tolerance for complexity. A two-tier system is simpler but provides less granularity for degrees of risk; four (or more) tiers provides high granularity but adds complexity, as each tier must have their own corresponding definitions and required actions to be meaningful.

Tier assignments can be highly subjective if definitions are vaguely defined, so it is worth considering factors that are more objective when developing or refining your organization's risk tiers. Some examples are:

- Level of dependence on supplier
- Level of mitigations likely needed
- Point-based risk score (based on questionnaire or similar)
- Data breach within the previous five years
- Location of data hosting (on premise vs off premise)
- Integration with entity's network (API, persistent VPN, as-needed access, etc.)
- Elevated permissions to key systems
- Foreign ownership or offshore hosting of data

Suppliers can be categorized based upon the risk the relationship poses to the entity's systems and data. Additional criteria that may be considered are the entity's information protection programs (which may use names such as Information Management, Data Privacy, Data Protection, or similar) that may pose their own requirements to help define tiers of risk.

Risk Assessment Triggers

Although it is crucial to perform risk assessments initially, it is equally important to understand how frequently such assessments should be repeated, as well as any other triggers that might necessitate their performance outside of their usual cadence. Indeed, a risk assessment performed ten years ago provides little assurance that such risks are still the same today. Therefore, each entity should have a pre-defined frequency on how often to repeat a risk assessment. Such periodic risk assessments are often based on the level of risk that a given supplier or engagement is assessed as having and are frequently associated with the concept of risk tiering.

For example, a risk assessment that places a supplier in a low tier of risk may be repeated every three years, whereas a supplier in a high tier of risk may be assessed each year. An example of risk tiering and risk reassessment cadence is provided below, though entities should adjust as needed to match their operational needs, organizational tolerance for risk, and regulatory requirements:

- Low risk: Every three years
- Medium risk: Every two years
- High risk: Every year

Outside of a scheduled risk assessment, however, there should also be a mechanism whereby new information, or a novel circumstance, can mandate the immediate reassessment of a supplier. Such scenarios may be considered risk assessment triggers and should be given priority whenever they occur, regardless of typical risk

assessment cadence. A non-exclusive list of risk assessment triggers to consider are provided below, though it is ultimately up to the organization to determine which are most appropriate and useful:

- Significant cybersecurity incident or data breach
- Breach of contract
- Merger, acquisition, or divestment
- Significant performance/deliverability issues
- Financial instability
- Criminal charges
- Significant change in geopolitical risk
- Supply chain constraints
- Changes in types of procurement from supplier
- Lack of response to risk questionnaires or inquiries

It is important to note that at any point, the risk profile or tiering of a supplier may change when new information is revealed, or existing information is shown to no longer be current.

For example, a supplier may initially present as a Low tier risk, with products procured and stored under that understanding. However, new information may come to light – such as a deficiency or breach in the supplier's development practices – that warrant a re-analysis of the risk and possible change in risk tiering. Although the previously procured products have not changed since they entered the entity's inventory, the knowledge they were procured under has changed, thus necessitating a fresh look at the potential risk they may represent.

Lack of response

Despite the best efforts of an entity, suppliers may not always respond to requests to complete a risk questionnaire or similar risk assessment tool. Alternatively, a supplier may refuse to respond to an entity's designated third-party risk assessor, only respond to a portion of the entity's request, or provide answers that are incomplete. When this occurs, it can be challenging for the entity to properly assess the risk posed by the supplier and/or their product(s). While there is no one perfect approach for such a scenario, certain factors may be considered to provide a relative measure of inferred risk in the event of an inadequate response from a supplier. Some factors to consider include:

- Size of supplier – A large, multinational corporation with many industry clients may have more mature processes than a small, local company with few clients.
- Third-party risk assessors – These services may be able to provide a relative assessment of risk.
- Open-source information – Data gathered directly from the supplier's website, compliance or regulatory filings, and relevant news articles may provide insight into a supplier's operations and risk profile.
- Supplier certifications – Certifications that are validated by an independent third-party can provide a degree of confidence that the measures stipulated by those certifications are being followed.

While it is always preferrable to obtain responses from the supplier directly, entities should consider developing a contingency plan for how to consistently assess supplier risk when such information is incomplete or not forthcoming.

6. Risk Dispositions

After performing the risk assessment, it is important that the effort made during such analysis is not lost or forgotten and is properly recorded. In particular, each identified risk should have a corresponding disposition indicating what course of action, if any, the entity believes is warranted in response. Accordingly, having a defined glossary of dispositions is invaluable in ensuring that identified risks are consistently responded to and can aid in future risk tracking and mitigation efforts. A glossary of suggested risk dispositions along with definitions and example scenarios is provided below, although entities may wish to define additional dispositions or have definitions that vary from those provided.

No Risk Identified

No risk was identified with the given response. This may be because the risk is not germane to the supplier or solution being evaluated, or that any such risk is exceedingly low. For example, a supplier whose core purpose is to pour concrete pads for transformers may have "No Risk Identified" regarding a risk assessment question that pertains to obtaining remote access to the entity's network.

Accept Risk

The entity has decided to take no further action on an identified risk. Acceptance may be formal, requiring the explicit approval of key individuals, or may be informal, whereby no additional approvals are required. Regardless of the level of formality, the entity understands the potential impact of the risk to the organization, has decided that it is willing to tolerate the risk, and concludes that no immediate action is necessary. For example, an entity may discover that a supplier is in financial duress but may decide to accept this risk because several alternate suppliers for the same product or service have already been reviewed and approved by the organization, and the loss of this supplier would not represent a hardship. Note that accepted risks may still go on to be monitored.

Mitigate Risk

Positive actions are undertaken to eliminate or reduce the identified risk. This may represent controls that the entity introduces or maintains, or it may represent controls that are introduced by the supplier to address the identified risk. In either case, the mitigation(s) must be sufficient to reduce the risk to a level deemed acceptable by the entity, with any remaining risk being implicitly accepted. For example, an entity may decide to introduce their own product testing and acceptance protocols to mitigate the risk of defective products produced by a supplier that does not have a robust testing process.

Transfer Risk

The identified risk is transferred to another in-house organizational entity (such as an affiliate or major department of the organization). It is important to recognize that transferred risks do not disappear, and the receiving organization must agree to formally receive the risk and must still provide a risk disposition. As this adds complexity to the risk assessment process and risk tracking, this disposition may be more appropriate for larger entities or those capable of robust risk tracking. For example, a critical supplier may not agree to the full

indemnification amount requested by the entity, and so the risk is formally transferred to entity's finance department, which agrees to Accept the risk posed by the lesser indemnification amount.

Outsource Risk

The risk is outsourced to an external organization or supplier. This disposition is distinct from Mitigate Risk in that a third party (and not the entity or supplier) is assigned to address the risk. This approach may be useful when neither the entity nor the supplier being assessed has the means or capability to fully mitigate the identified risk internally. For example, a supplier may not possess the necessary equipment and technical expertise to adequately sanitize physical media containing the entity's sensitive information, and so the entity outsources this risk to a contracted media disposal company who specializes in this work and can generate certificates of destruction.

Refuse Risk

The risk is deemed to be unacceptable by the entity. This is appropriate when other efforts to address the identified risk have failed and often results in a supplier not advancing in consideration. However, there may be certain situations in which the refused risk is specific to a particular service or product, and not the supplier generally. For example, a supplier who relies on a large contingent of foreign nationals may be precluded from certain types of work but permitted to perform other types. In other cases, a supplier that is based in a prohibited country may be precluded from consideration altogether.

7. Documentation Practices

In the never-ending effort to decrease risk and promote compliance, the development of clear documentation guidelines that support the process, decisions, and implementation of mitigation measures is key. As regulatory environments change over time, proper planning and detailed processes will help build defensible and auditable records.

This section details several approaches that have been successfully used by entities to document the results of their risk assessments along with considerations for each approach. It is not uncommon for multiple approaches to be in use at the same time. Such a situation is not inherently correct or incorrect, but there should be a strong emphasis on eliminating duplicative processes and unnecessary steps wherever possible.

However, do not let the "perfect" tool of tomorrow dissuade the use of a "good" tool today. If an entity does not yet have the resources for an expensive but capable enterprise resource planning (ERP) solution for documenting risk assessments, the key functions of documenting assessment results, risk findings, and risk decisions can still be accomplished via simpler means such as spreadsheets or even paper processes. Regardless of the approach used, care must be taken to ensure security controls are in place to ensure that sensitive assessment information is not accessible to unauthorized individuals.

Enterprise Resource Planning or Risk Management Systems

The use of ERP or similar risk management systems can vary greatly between entities. These tools can help manage lead times, define roles, responsibilities, and approval processes. Most ERP systems are built for inventory management and can leverage rating or scoring criteria. Integrating a library of approved suppliers – particularly those that comply with regulatory requirements, such as CIP-013 – into the ERP system can be an

extremely effective way to control procurement workflows. Approved suppliers can then be assigned a risk classification or tier to manage the frequency and level of risk assessments.

For example, a given tier 1 supplier which makes a critical product may be considered a high risk and require a new risk assessment on a more frequent basis, whereas a tier 2 supplier that is merely the reseller of that product may require a less frequent risk assessment. Where possible, risk assessments should be automatically assigned an expiration date that reflects their risk classification and provide sufficient notice to relevant staff so that a reassessment can be completed before the prior assessment's expiration date.

Key features to consider when evaluating or implementing ERP systems include:

- Automatic order controls (e.g., identifying an incorrect part number, over-ordering, etc.)
- Ability to flag suppliers as failing certain compliance requirements (CIP-013, etc.)
- Ability to assign suppliers, products, or services to tiers
- Correlating related purchase orders, shipments, and invoices
- Alerting based on exceptions or unexpected conditions
- Halting workflows based on specific criteria (e.g., order from a restricted supplier or country)

Some ERP systems can be configured to allow suppliers to directly access and complete a risk assessment questionnaire within the tool. The tool should ideally have the ability to automatically calculate scoring based upon criteria defined by the entity. Once completed, a group or committee can be established to review the responses.

A link between a risk assessment and the procurement must be established so that there is a trackable history when the requisition is submitted for procurement. A separate process should automatically attempt to reconcile the assessed requisitions with completed purchase orders to identify any orders that did not follow the entity's prescribed processes.

Different tools may provide more flexibility or customization than others. Whichever tool is selected, the ability to tie a given procurement with its corresponding risk assessment is a crucial feature that can greatly aid compliance efforts. However, no tool will address every process required, and it is important to consider which steps may be automated, and which are not a suitable fit for the capabilities of the ERP system.

Workflow Systems

If an entity does not have a robust ERP platform or risk management solution deployed, much can still be accomplished via the thoughtful setup of other productivity tools that offer workflow design and management. While such tools may not provide "out of the box" solutions to support an entity's risk assessment process, with some customizations, these tools can often be designed to automatically route documents and approval requests, greatly reducing the need for manual process, reducing error, and improving efficiency.

For example, a workflow may be set up that allows an entity to enter a potential supplier's contact information and automatically email the supplier using a prepared template, inviting them to upload a completed questionnaire to an entity's secure portal. The workflow could then detect if a week has passed without a response and send a reminder email to the potential supplier – or alternatively, notify the entity if the

questionnaire file has been uploaded and is ready for review. This is but one example of how a workflow system, if properly configured, can assist the routine but critical functions of the risk assessment process.

Although there exist many workflow products and services, key features that an entity may wish to consider when selecting one include:

- Document storage: The ability to upload, store, retrieve, edit, and delete documents and incorporate them into workflows. This supports the analysis, archival, and scheduled deletion of critical files such risk questionnaire results, communications, and other records.
- Item/list management: The ability to store, sort, display, and manage lists of items. Note that this is a separate function than document storage, as the list - and list items - are considered independent entities that may represent a request (as opposed to a document) and can be used to direct workflows.
- Approval capabilities: The ability to designate a specified user (or group of users) with the ability to approve or reject selected documents or requests and affect their subsequent routing in the workflow.
- Notification capabilities: The ability to automatically alert users of the system that a document or request is ready for their review or approval, or to notify users when an exception has occurred (such as a rejection, too much time without a response, or other undesirable outcome).

This is not an exclusive list of useful features, and some solutions may provide more flexibility or customization than others. Regardless, it is more than likely that a workflow-based solution will represent some combination of both manual and automated processes. The extent of automation that can be applied is largely limited by the specific capabilities of the workflow solution and the risk assessment processes in place at an entity.

Manual Document Review

When a system is not available to support the supplier risk management process, a simple, manual process to document the results of a risk assessment using standard industry tools like a word processor, spreadsheet software, and document repository can suffice. The aim is to ensure that suppliers are assessed systematically, results are documented, and all documentation is stored for future reference. Suggestions for major components to include are noted below.

Use a tracking spreadsheet

A simple tracking spreadsheet can memorialize the important details about the supplier, the risk evaluation, and the risk evaluation results. This eases future supplier research and reporting.

- Record metadata about the supplier including name, supplier contact, product/services provided. It is helpful to identify an internal contact for future follow-up.
- Record details about the evaluation completed including date of completion, target date for re-review, risk categories, and individual risk ratings (e.g., high, medium, low). Consider including a future planned re-review date, if applicable.
- Record the final supplier risk determination (e.g. accepted, requires mitigation, rejected). Consider a color-coding system in the spreadsheet to visually represent risk levels (e.g., red for high risk, yellow for medium, green for low).
- Record risk mitigation activities to be completed including owner and target completion date.

Create a common documentation storage location

Consider storing all supplier review documentation in a common location that can be accessed by interested stakeholders. Organizing the repository by supplier name and evaluation date facilitates assessment progress tracking and ease collaboration among stakeholders. Limit access to this location to those with a need to know, since it may contain confidential information. Consider storing at least the following documents:

- Supplier questionnaire responses
- Supplier-provided supporting documentation. May include certifications (e.g., ISO-27001, IEC-62443, SOC2), audit reports, policies, etc.
- Third-party supplier assessments organized by the entity
- Internal risk assessment documents (e.g., scoring, risk level determination)
- Evidence of internal approval or rejection of supplier

Formalize assessment results

- Consider compiling a formal supplier risk assessment report summarizing the evaluation process and any identified risks. This report may include supplier services, assessment findings, recommendation mitigations, and overall risk rating.
- Store the supplier risk assessment report in the supplier documentation location.

Memorialize stakeholder approval

- Circulate the supplier risk assessment report to necessary individuals/groups for review and sign-off and/or convene a review committee, as appropriate for your organization.
- Store a record of individual sign-off(s) and/or committee approvals in the supplier documentation location. This may include emails and electronically or physically signed forms indicating whether residual risk regarding this supplier has been accepted.

8. Integration with Enterprise Risk Management

An enterprise risk management program is typically a company-wide effort that facilitates rapid identification, mitigation, and response to significant risks facing the organization. If done correctly, it allows entities to focus on rapidly changing business demands while ensuring material risks are properly managed. However, such a program is only effective if it has the proper visibility into key drivers of risk for the entity.

Therefore, whether required by compliance or not, it is worth ensuring that supply chain risk management is fully incorporated into a holistic, enterprise-wide risk management program. While traditional elements of risk, such as financial, legal, regulatory, reputational, and similar are often well-represented in a typical enterprise risk management plan, supply chain risks do not always have equal consideration, despite the outsize risk that supply chain issues can have on other areas.

For example, consider the following supply chain risks:

- What reputational risks might be faced by using a supplier that is badly and publicly compromised?
- What financial risks might there be if a supplier is sanctioned by a government agency?

- What regulatory impacts might there be if an entity's sensitive data is leaked by a supplier's breach?
- What operational impacts might there be if a critical supplier suddenly goes out of business or stops making a critical product?

While a full discussion on enterprise risk management is outside the scope of this document, supply chain risks are nonetheless an important factor to incorporate into any holistic risk management approach. One helpful resource that provides additional discussion on incorporating supply chain risk management into enterprise programs – including enterprise risk management, amongst others – is the American Public Power Association's *Cyber Supply Chain Risk Management* manual [7].

9. Conclusion

Although there is great variety in the supply chain processes used across industry, by consistently applying the guidance provided by this document and the rest of the NATF *Supply Chain Security Assessment Model* [1] steps, it is anticipated that entities and suppliers will be better prepared to identify and mitigate the risks present in their supply chains. As the supply chain risks facing the North American bulk power system continue to evolve, NATF remains committed to providing effective and relevant guidance to our members and industry.

References

[1] 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.

[2] 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.

[3] North American Transmission Forum, "Energy Sector Supply Chain Risk Questionnaire," 5 May 2024. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire.xlsx.

[4] ERO Enterprise, "ERO Enterprise CMEP Practice Guide - Using the Work of Others," 14 March 2023. [Online]. Available: https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Using%20the%20Work%20of%20Others.pdf.

[5] North American Transmission Forum, "NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors," 23 October 2023. [Online]. Available: https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013%20Using%20Independent%20Assessments%20of%20Vendors%20(NATF)%201.pdf.

[6] North American Transmission Forum, "NATF Supply Chain Security Criteria," 12 May 2024. [Online]. Available: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-supply-chain-security-criteria.xlsx.

[7] American Public Power Association, "Cyber Supply Chain Risk Management," December 2020. [Online]. Available: https://www.publicpower.org/resource/cyber-supply-chain-risk-management.