North American Transmission FORUM

Community Confidentiality Candor Commitment

Supply Chain Security Assessment Model

Open Distribution for Supply Chain Materials

The NATF permits the use of the content contained herein ("Content"), without modification; however, any such use must include this notice and reference the associated NATF document name & version number. The Content is provided on an "as is" basis. The NATF makes no and hereby disclaims all representations or warranties (express or implied) relating to the Content. The NATF shall not be liable for any damages arising directly or indirectly from the Content or use thereof. By using the Content, you hereby agree to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

Version 2.1
Document ID: 1302
Approval Date: 10/23/2023

Versioning and Acknowledgments

Contributing Organizations

American Public Power Association (APPA)

Con Edison Working Group (ConEd)

Edison Electric Institute (EEI)

Ernst & Young, LLP (E&Y)

GE Power

Hitachi-ABB Power Grids

ISO/RTO Council (IRC)

KPMG

Large Public Power Council (LPPC)

National Rural Electric Cooperative Association (NRECA)

North American Energy Standards Board (NAESB)

North American Generator Forum (NAGF)

North American Transmission Forum (NATF)

OSI

Schneider Electric

Schweitzer Engineering Laboratories, Inc.

Siemens Industry, Inc.

Transmission Access Policy Group (TAPS)

UL

With appreciation for the NATF Steering Team Members

- Ameren
- American Electric Power
- Duke Energy
- Exelon
- Nebraska Public Power District
- PJM
- Southern Company

Version History

Date	Version	Notes
01/31/2020	1.0	
03/30/2020	1.1	Updated document with revised copyright
06/04/2021	2.0	Updated document content, figures, and appendices
10/23/2023	2.1	Corrected broken hyperlinks.

Review and Update Requirements

- Update: as necessary
- Review: every 3 years

Contents

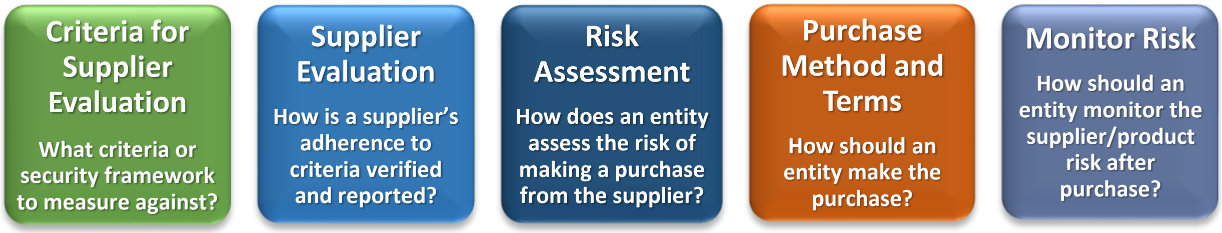
1. Purpose

The purpose of the Supply Chain Security Assessment Model (Model) is to provide a streamlined, effective, and efficient industry-accepted approach for entities to evaluate supplier supply chain security practices. The Model has been endorsed by the NATF-led Industry Organizations Team[1] and is supported by solution providers[2] and, if applied widely, will reduce the burden on suppliers, provide entities with more and better information, and improve supply chain security. The tools contained in the Model and supporting services offered by solution providers will provide critical information for entities to consider when conducting risk assessments for potential suppliers of products and services.

The overall objectives of this work were to 1) streamline common approaches to evaluating a supplier's security practices, 2) provide for flexibility within common approaches, 3) ensure the common approaches are scalable to include all suppliers and purchasing entities, and 4) while focusing on good supply chain security practices, address compliance requirements.

2. The Model

The Model addresses supply chain risk management through five lifecycle phases (shown in Figure 1), taking each phase of the lifecycle into an action (shown in Figure 2).


Criteria for Supplier Evaluation

What criteria or security framework to measure against?

Supplier Evaluation

How is a supplier's adherence to criteria verified and reported?

Risk Assessment

How does an entity assess the risk of making a purchase from the supplier?

Purchase Method and Terms

How should an entity make the purchase?

Monitor Risk

How should an entity monitor the supplier/product risk after purchase?

Figure 1: The Supply Chain Security Risk Assessment Lifecycle

The five-step Model provides a solid foundation for identifying, assessing, and mitigating supply chain risks, provides for inclusion of suppliers and solution providers depending upon each entity's needs, and provides for flexibility of each entity's implementation. Further, the Model and complementary products from other participating organizations[3] provide tools that support good supply chain security practices. When executed properly and with a focus on security, the Model will assist entities with meeting the compliance requirements

[1] The NATF-led "Industry Organizations Team" includes representatives from energy industry trade organizations and forums, NATF member utility representatives, key electric sector suppliers, and third-party assessors. A list of participants on the Industry Organizations Team is located on the NATF public website at: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/contributing-organizations.

[2] A solution provider is an organization that collects and provides supplier information and may provide additional services to assist companies with supplier risk assessments. See Appendix 3 for process detail.

[3] Complimentary products from other organizations are posted on the NATF public website at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

of the NERC supply chain reliability standards,[4] which initially became effective on October 1, 2020 and are revised from time to time.[5] The five steps of the Model are depicted below in Figure 2, and each step is examined in more detail in the next section.[6]

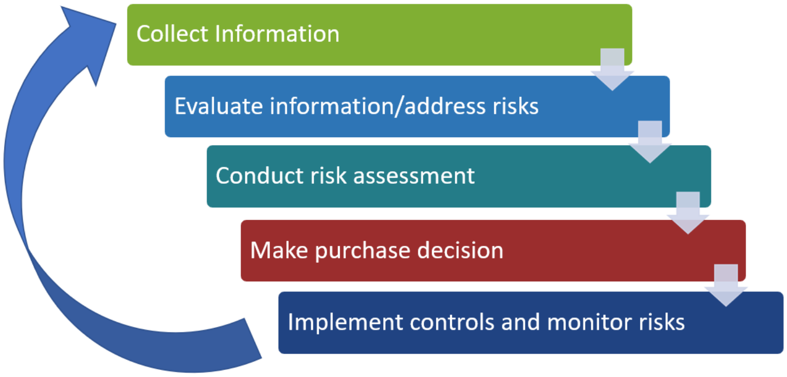

Collect Information
Evaluate information/address risks
Conduct risk assessment
Make purchase decision
Implement controls and monitor risks

Figure 2: The Supply Chain Security Assessment Model

3. The Five Steps of the Model

The five steps of the Model provide a strong foundation to mitigate supply chain risks by encapsulating the necessary actions and components of supply chain risk, without regard to whether the purchase is for IT, OT, software, firmware, hardware, equipment, components, or services. The actions contained within each step are outlined in the following sections.

1. Collect Information

The Model provides the following tools for collecting information:

1. The NATF Supply Chain Security Criteria (NATF Criteria), which can be used to collect information from a supplier or can be used as a basis for measuring a supplier's security posture/practices (i.e., a "best practices" list), and

2. the Energy Sector Supply Chain Risk Questionnaire (NATF Questionnaire) to obtain more granular information on a supplier's supply chain risk performance.

Either tool can be used to collect information regarding the supplier's risk management at the supplier's corporate level, for a specific product or service, and/or at the development system level.

[4] In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed new Reliability Standard CIP-013-1 and modified Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards."

[5] Information on the most current version of the supply chain standards can be located on the NERC website: https://www.nerc.com/Pages/default.aspx.

[6] A detailed illustration featuring the inputs to each step of the Model is provided in Appendix 4, Figure 6.

The NATF Criteria and the NATF Questionnaire are tools for collecting information from suppliers. The NATF Criteria are "best practices" by which to measure a supplier's security posture. The Questionnaire provides questions to assist entities in obtaining necessary information to use in the evaluations. These are not pass/fail lists; they are designed to identify risks and provide an opportunity for mitigation.

Entities should provide the entire NATF Criteria and/or the entire NATF Questionnaire to a supplier. Entities may request that suppliers provide responses to all or some of the questions or criteria, and items not required to be completed by the supplier should be clearly identified by the entity. However, the supplier should have the option to provide answers to all questions or criteria even if not required by the entity. Requesting responses in their entirety assists suppliers in recognizing the tools, having responses prepared, and thus being able to provide responses in a timely manner. Since they will be working with many entities across the industry and in most cases will be providing all the responses, providing all of responses may simplify their ability to respond, meeting the entities' needs and encouraging adoption across the industry. The entity can determine which responses they use in their risk assessments based on the supplier and the risk of the product or service being procured. When entities have additional questions, or need a question modified, those may be provided to the supplier as an addendum to the NATF Questionnaire or Criteria.

The entity's risk assessment process determines the risk that could derive from a procurement, with input from sources such as the NATF Criteria, NATF Questionnaire, certifications to existing frameworks/standards, independent assessments/audits from qualified third-parties, open-source information, shared entity assessments, other data sources, or a combination of these sources. Supplier answers to specific criteria or questions may or may not prevent the entity from procuring a product from the supplier. The information from these various sources, as available, should be viewed as input to the risk assessment process documented by each entity, and is not intended as a checklist of items to require mitigation. The entity's risk assessment process should identify risk and provide an opportunity for any mitigation the entity deems appropriate.

> *Entities should <u>obtain information</u> from, or about, suppliers <u>AND</u> verify that the <u>information is accurate.</u>*

The information received from or about a supplier can be verified in several ways:

The supplier could provide a security framework report from a qualified independent third-party
This would include either a certification to, or assessment of, a supplier's performance to a security framework from a <u>qualified</u> auditor or assessor. An entity should verify that the certification or assessment report addresses all of questions or criteria needed to analyze risk for the purchase, which can be done by reviewing the report's Statement of Applicability. Mapping is provided to selected security frameworks in the NATF Criteria. Examples include:

- *Certification* - The supplier could provide a certification to an existing security framework (e.g., IEC 62443, ISO 27001)[7]

[7] See Appendix 1 for process detail

- *Independent assessment or audit* - The supplier could provide its report from an independent assessment (e.g., SOC2) or audit[8] by a qualified auditor or assessor

Entity could procure a report from an independent third-party

This would include either a report or audit conducted by a third-party professional organization or entity. The receiving entity should verify that the information collected addresses all the questions or criteria needed to analyze risk for the purchase and should understand how the accuracy of the information was verified by the third-party.

- *Solution Provider*– Procure information and verification through a solution provider
- *Sharing prior purchaser audit* – An audit or assessment another purchaser had conducted previously that could be obtained from the prior purchaser/entity, from the supplier, or from a solution provider

The supplier could provide verification of accuracy with the information

This would consist of a self-attested response to the NATF Criteria or Questionnaire with supporting evidence that the purchasing entity could review.

If the supplier cannot or will not provide information, a purchasing entity can seek information from other sources

- Investigate other external evaluations of the supplier (e.g., a Department of Defense maturity ranking)
- Investigate open or private sources to verify supplier’s responses, including suppliers’ security policy statements or trust-center webpages, financial reporting services, obtaining references from other entities that purchase from the supplier, etc.
- Use other verification methods, such as hardware, firmware and software security assessments or testing

Mapping to Third-Party Certifications and Assessments/Audits

The NATF Criteria are provided on a spreadsheet and are mapped to several existing security frameworks. This is not an all-inclusive list. The criteria are intentionally provided in this format so that an entity could use it to map the criteria to an additional security framework or certification. As entities add additional frameworks, their mapping could be included on the master NATF Criteria workbook to allow other entities to benefit from their work. The critical observation would be to see which criteria are not addressed by the security framework, so an entity could use other methods, which may include a second security framework, to verify the suppliers’ performance to those criteria.

[8] See Appendix 2 for process detail

2. Evaluate the Information/Address Risks

When evaluating the information collected, an entity can determine:

1. Whether the level of the supplier's adherence to the NATF Criteria or the responses to the Questionnaire identify any risks pertinent to the product or service being purchased

2. Whether the level of assurance or verification of the accuracy of the supplier information is sufficient for the product or service being purchased

3. Whether any identified risks could be mitigated by the supplier or the entity, or if the risk could be accepted.

The purchasing entity can determine, based on the information and assurance provided, if any of the supplier's security practices raise a concern (i.e., are a risk) and whether that risk can be mitigated or accepted.[9] Considerations include:

An evaluation of the supplier's adherence to the NATF Criteria and/or response to the Questionnaire
Does the supplier fully conduct all of the pertinent actions contained in the criteria and/or questionnaire or are there some pertinent actions that the supplier conducts partially? For any pertinent actions that are not fully conducted, the entity can determine whether the non-action constitutes a risk.

An evaluation of the level of assurance the supplier has provided for its responses
Was the supplier able to provide the purchasing entity with assurance that it performs as reported? Depending upon the potential impact the specific product or service could have on the Bulk-Power System, the purchasing entity may require more assurance.

An evaluation of the significance of any identified risks and how they could be addressed
The purchasing entity can ascertain whether it or the supplier could take actions or implement controls to mitigate any identified risks or if the risks can be accepted.

Mitigation of Risks

Identified risks are evaluated for potential mitigations that would result in a lower residual risk or an elimination of the risk. Mitigations could be implemented by the supplier or by the entity. In some cases, the risk may be such that it can be accepted. Through entities and suppliers working together on solutions for identified risk, it is anticipated that repeated identification of the same risks and implementation of mitigating activities will bring an overall increase in security, as depicted by the figure below:

[9] The NERC Supply Chain Working Group (SCWG) has developed a series of supply chain security guidelines that provide guidance for evaluating supplier information and in determining whether or how to mitigate risks. These are concise three-page documents that provide a high-level summary of issues to be aware of and potential methods of addressing them. The guidelines are available on the NERC website: https://www.nerc.com/comm/RSTC/Pages/SCWG.aspx and can be linked to from the NATF website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

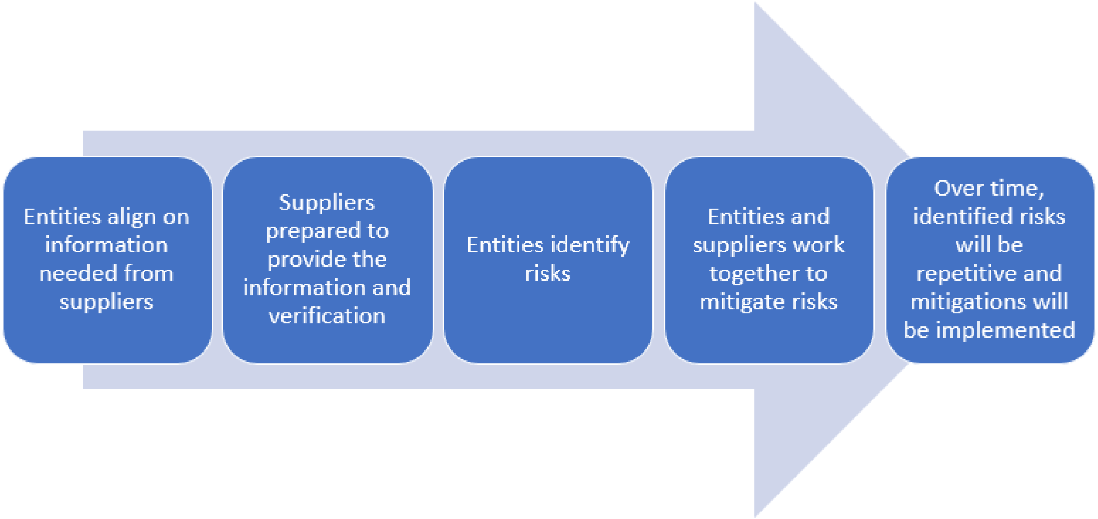

Entities align on information needed from suppliers
Suppliers prepared to provide the information and verification
Entities identify risks
Entities and suppliers work together to mitigate risks
Over time, identified risks will be repetitive and mitigations will be implemented

Figure 3: The Vision for Alignment

Document the Determinations

Maintaining the supplier's responses and documenting the evaluations will help the purchasing entity to monitor risks after the purchase as well as demonstrate compliance.

3. Conduct the Risk Assessment

1. *The entity should have a methodology to perform supplier risk assessments.*[10]
2. *The entity should document the results of risk assessments.*

The entity can then conduct a risk assessment to determine which suppliers could provide the desired product or service with the least amount of residual risk. There are a variety of methods that could be used to conduct a risk assessment.[11] Some entities use the suppliers' responses to the criteria in a staged approach, or gates, determining which criteria are the most critical for the product or service and assessing supplier risk in phases. Other entities use a rating and ranking methodology, and some use a combination of both.

[10] The American Public Power Association, an Industry Organizations participating member, has developed a guide for conducting risk assessments: *Cyber Supply Chain Risk Management*, available on the APPA website: https://www.publicpower.org/resource/cyber-supply-chain-risk-management and is linked on the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/all-resources.

[11] *Id.*

4. Make Purchase Decision

1. *Develop a cross functional process to include the information from the supplier risk assessment into the entity's purchase procedure.*

2. *Consider other entity-identified factors and the entity's risk appetite in supplier selection.*

3. *When making a purchase decision and entering into a purchase agreement or contract an entity should consider whether implemented or agreed upon mitigations can be supported by contract terms and conditions.*

The results from the supply chain risk assessment are one input into the entity's procurement process and includes consideration of any mitigations that would need to be implemented and monitored. Depending upon the nature of the mitigations and the risk associated with a failure of the mitigations, entities may include terms and conditions to support the mitigation activities in procurement contracts or purchase order terms and conditions.

The information obtained through this Model does not dictate purchasing decisions for the purchasing entity; rather it provides risk information to consider and weigh along with other factors. This Model does not address what factors a purchasing entity should consider (and these may vary by purchase) or how the entity should weigh their considerations. Factors may include, among others:

- Financial
- Operational
- Supplier support levels
- Reputational
- Regulatory requirements
- The entity's inherent risks
- The entity's risk appetite
- Other information or factors as determined by the entity

Cross Functional Process

Cross-functional processes are required for the supplier risk evaluation, mitigation, the development of contractual terms and conditions, procurement, and monitoring. Often there is not a single responsible department, so entities can develop controls to ensure processes are implemented as intended across multiple functions.

5. Implement Controls and Monitor Risks

The entity should have a plan to monitor:

1. Risks and controls associated with the purchase throughout the lifecycle of the products or services.

2. 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.

Supply chain risk is not limited to the purchase, completion of the service, or the installation of the product, and needs to be monitored through the lifecycle of the product or service purchased. A supplier’s supply chain security posture can be dynamic, requiring an entity to have controls in place and monitor risks.

Controls and Monitoring Risk

Any mitigations that have been implemented will need to be monitored to ensure that the mitigating actions remain effective, and the purchased product or service should be evaluated for any changes in risk resulting from implementation. In addition, new supply chain risks (such as concerns regarding a country of origin) may arise, and an entity may need to evaluate how these identified risks pertain to or affect existing or inventoried equipment, components, software, etc., and whether those risks can be mitigated.

Review of Supplier Risk Assessment

How often an entity reviews or refreshes a supplier’s risk assessment may be approached differently depending upon the supplier, whether or how the supplier is being monitored for purchased products or services, or whether the supplier is being considered for a new purchase. Entities may conduct supplier monitoring themselves or may employ a solution provider to conduct continuous monitoring.

4. Conclusion

Supply chain exploitation is not just a potential risk but has become reality. Now more than ever, industry needs to take actions to prevent attacks and breaches, be knowledgeable of breaches that have occurred, and know how to identify if a compromise has infiltrated its systems. The NATF and the Industry Organizations Team have developed this Supply Chain Security Assessment Model to encapsulate the necessary actions and components for supply chain risks.

The Model can assist entities in management of supply chain risks. It takes advantage of existing methods to provide entities with a streamlined, effective, and efficient approach while providing flexibility for each entity’s implementation. Entities can build upon this Model as they mature in their processes and as new aspects of supply chain risk are identified. This Model is available for industry stakeholders and adoption of the Model will provide entities with a strong foundation to address supply chain security.

For More Information

Webpage URL: http://www.natf.net/industry-initiatives/supply-chain-industry-coordination

NATF contact: supplychain@natf.net

List of key contacts for the Industry Organizations Team: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/contributing-organizations

Additional Resources:

Also see listing on the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- The NERC Supply Chain Working Group (SCWG) supply chain security guidelines: *Cyber Security Risk Management Lifecycle, Provenance, Risk Considerations for Open Source Software, Risks Related to Cloud Service Providers, Secure Equipment Delivery, Vendor Incident Response, Vendor Risk Management Lifecycle, Procurement Language*.
  - The guidelines are available on the NERC website: https://www.nerc.com/comm/RSTC/Pages/SCWG.aspx and can be linked to from the NATF website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

- The American Public Power Association[12], guide for conducting risk assessments: *Cyber Supply Chain Risk Management*
  - The guide is available on the APPA website: https://www.publicpower.org/resource/cyber-supply-chain-risk-management and can be reached from the NATF public website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/all-resources.

- The EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V3
  - The document is available on the EEI website: https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf and can be reached from the NATF website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[12] An Industry Organizations participating member.

Appendix 1: Certification to Existing Framework/Standard

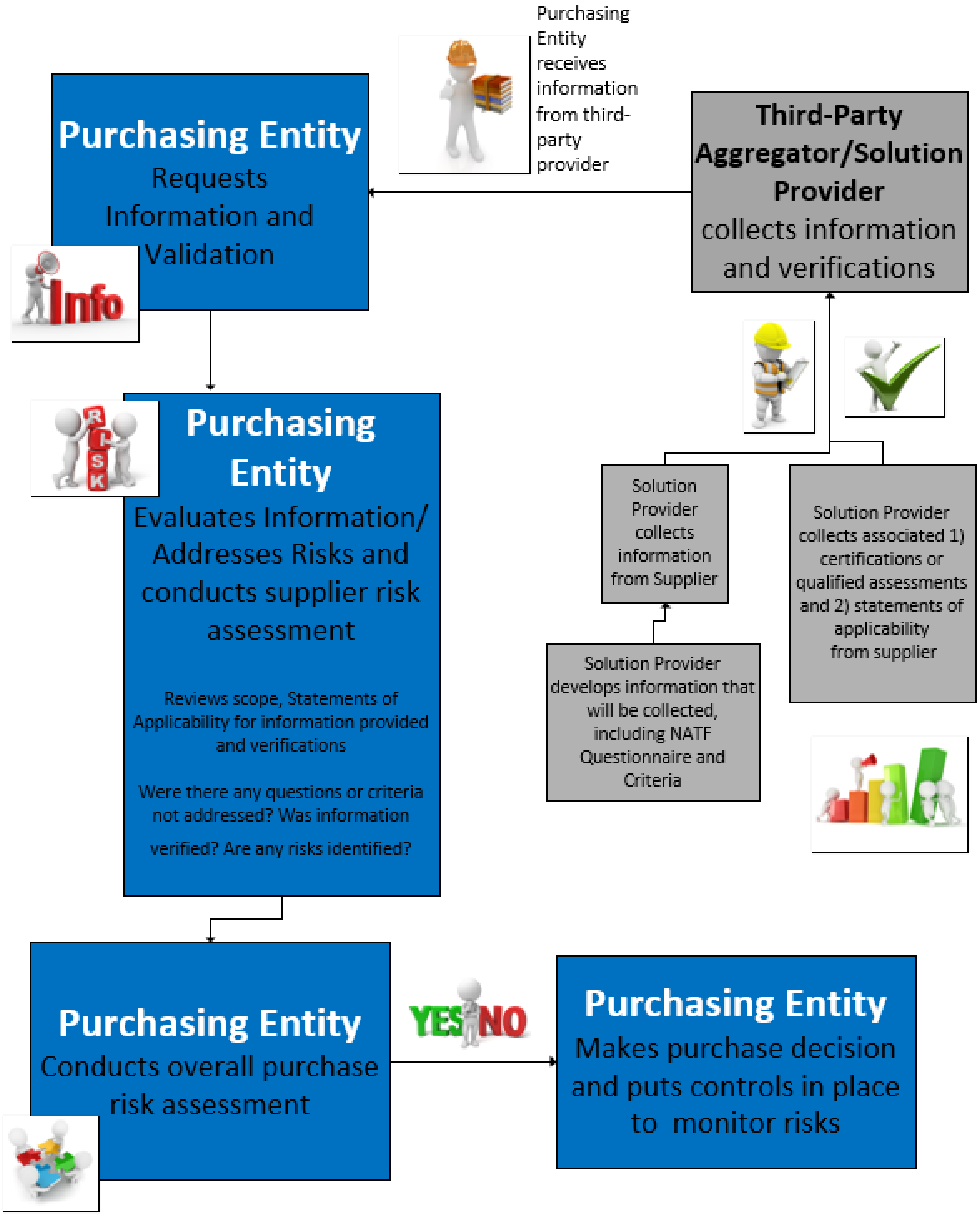

Purchasing Entity
Requests Information and Validation
Info
Purchasing Entity receives information from third-party provider
Third-Party Aggregator/Solution Provider
collects information and verifications
Purchasing Entity
Evaluates Information/ Addresses Risks and conducts supplier risk assessment
Reviews scope, Statements of Applicability for information provided and verifications
Were there any questions or criteria not addressed? Was information verified? Are any risks identified?
RISK
Solution Provider collects information from Supplier
Solution Provider collects associated 1) certifications or qualified assessments and 2) statements of applicability from supplier
Solution Provider develops information that will be collected, including NATF Questionnaire and Criteria
Purchasing Entity
Conducts overall purchase risk assessment
YES NO
Purchasing Entity
Makes purchase decision and puts controls in place to monitor risks

Figure 4: Process for obtaining a Security Framework Certification

Appendix 2: Independent Assessment from Qualified Third-Party

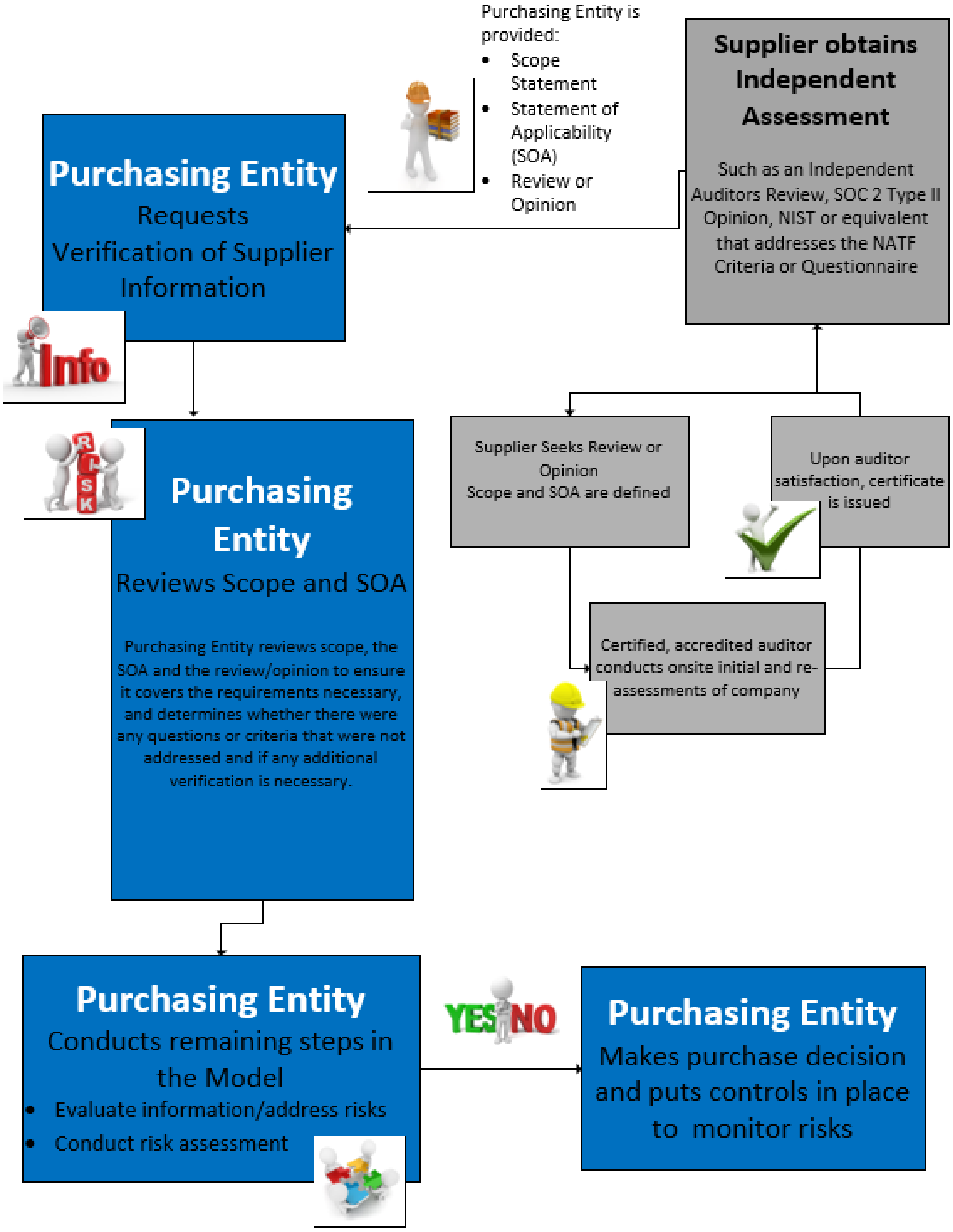
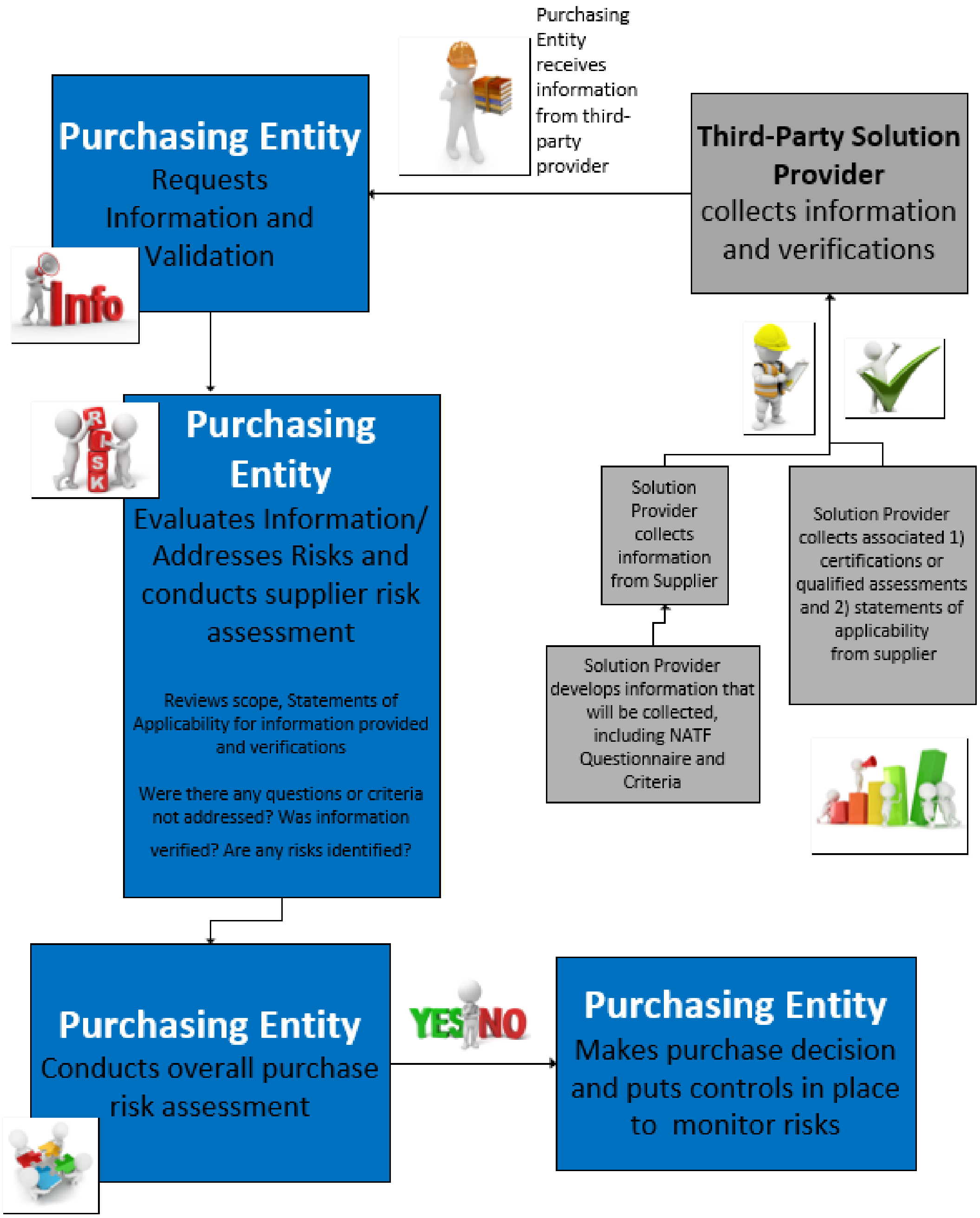

Purchasing Entity is provided:
Scope Statement
Statement of Applicability (SOA)
Review or Opinion
Supplier obtains Independent Assessment
Such as an Independent Auditors Review, SOC 2 Type II Opinion, NIST or equivalent that addresses the NATF Criteria or Questionnaire
Purchasing Entity
Requests Verification of Supplier Information
Info
RISK
Purchasing Entity
Reviews Scope and SOA
Purchasing Entity reviews scope, the SOA and the review/opinion to ensure it covers the requirements necessary, and determines whether there were any questions or criteria that were not addressed and if any additional verification is necessary.
Supplier Seeks Review or Opinion
Scope and SOA are defined
Upon auditor satisfaction, certificate is issued
Certified, accredited auditor conducts onsite initial and re-assessments of company
Purchasing Entity
Conducts remaining steps in the Model
Evaluate information/address risks
Conduct risk assessment
YES NO
Purchasing Entity
Makes purchase decision and puts controls in place to monitor risks

Figure 5: Process for obtaining an Independent Assessment from a Qualified Third-Party

Appendix 3: Working with a Third-Party Solution Provider



Purchasing Entity Requests Information and Validation

Purchasing Entity receives information from third-party provider

Third-Party Solution Provider collects information and verifications

Solution Provider collects information from Supplier

Solution Provider collects associated 1) certifications or qualified assessments and 2) statements of applicability from supplier

Solution Provider develops information that will be collected, including NATF Questionnaire and Criteria

Purchasing Entity Evaluates Information/ Addresses Risks and conducts supplier risk assessment

Reviews scope, Statements of Applicability for information provided and verifications

Were there any questions or criteria not addressed? Was information verified? Are any risks identified?

Purchasing Entity Conducts overall purchase risk assessment

Purchasing Entity Makes purchase decision and puts controls in place to monitor risks

Figure 6: Third-Party Solution Provider Process

Appendix 4: Detailed Illustration of Model Steps

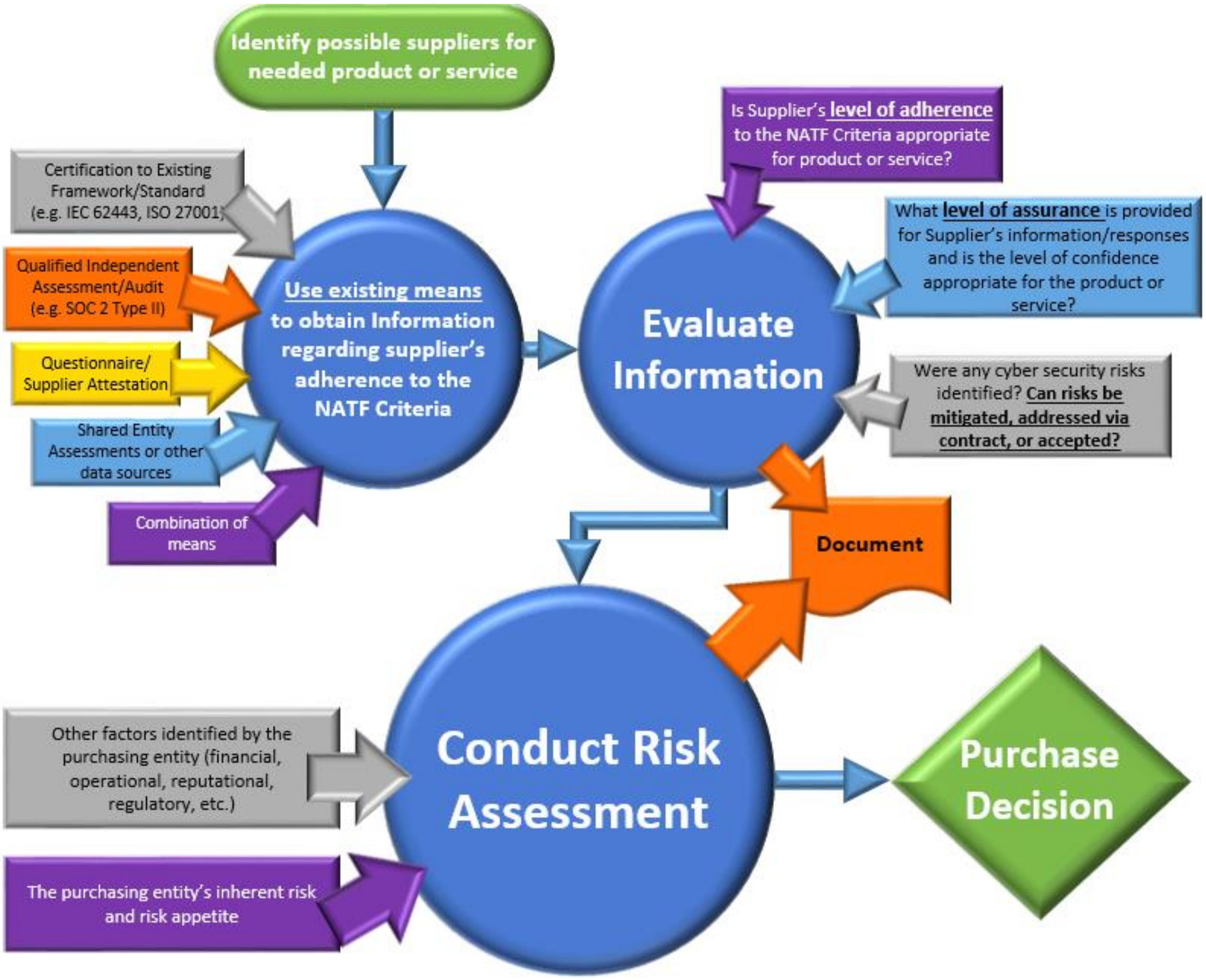

Identify possible suppliers for needed product or service
Certification to Existing Framework/Standard (e.g. IEC 62443, ISO 27001)
Qualified Independent Assessment/Audit (e.g. SOC 2 Type II)
Questionnaire/ Supplier Attestation
Shared Entity Assessments or other data sources
Combination of means
Use existing means to obtain Information regarding supplier's adherence to the NATF Criteria
Is Supplier's level of adherence to the NATF Criteria appropriate for product or service?
What level of assurance is provided for Supplier's information/responses and is the level of confidence appropriate for the product or service?
Evaluate Information
Were any cyber security risks identified? Can risks be mitigated, addressed via contract, or accepted?
Document
Other factors identified by the purchasing entity (financial, operational, reputational, regulatory, etc.)
The purchasing entity's inherent risk and risk appetite
Conduct Risk Assessment
Purchase Decision

Figure 7: The Supply Chain Security Assessment Model with Details