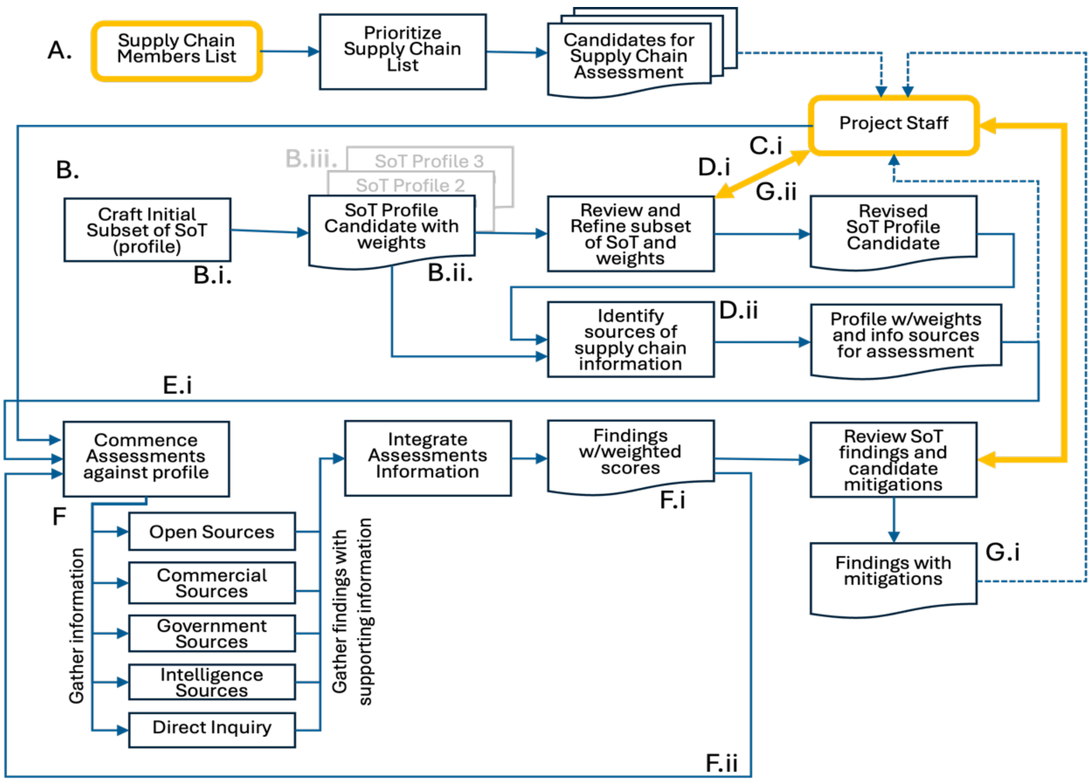
SoT Supply Chain Assessment Process

Supply chains are increasingly complex and vulnerable to a wide range of disruptions due to many different risks, including geopolitical instability, cyber threats, and other types of impacts to supplier operations. To assess these challenges within a program, we have leveraged MITRE's System of Trust (SoT), a robust framework for identifying, evaluating, and mitigating risks, and used it to define an overall supply chain assessment process. This paper presents a step-by-step methodology for how SoT can be used for identifying which risks to the supply chain should be in scope for assessment and investigation (developing risk profiles), identifying the relative importance of the risks, determine how and where to obtain the information to assess the risks, perform the assessments of those risks, and implementing mitigation strategies for the security and resilience of the supply chains that allow us to bring the best suite of tools and capabilities to bear on this complex challenge.

The below discussion lays out the overall process, illustrated in Figure 1: Supply Chain Assessment Task, and provides explanatory details. Items shaded green are already completed; gold ones involve outside parties.

Figure 1: Supply Chain Assessment Task Flow


A.
Supply Chain Members List
Prioritize Supply Chain List
Candidates for Supply Chain Assessment
Project Staff
B.
B.iii.
SoT Profile 3
SoT Profile 2
C.i
D.i
G.ii
Craft Initial Subset of SoT (profile)
SoT Profile Candidate with weights
Review and Refine subset of SoT and weights
Revised SoT Profile Candidate
B.i.
B.ii.
Identify sources of supply chain information
D.ii
Profile w/weights and info sources for assessment
E.i
Commence Assessments against profile
Integrate Assessments Information
Findings w/weighted scores
Review SoT findings and candidate mitigations
F
F.i
Open Sources
Commercial Sources
Government Sources
Intelligence Sources
Direct Inquiry
Gather information
Gather findings with supporting information
Findings with mitigations
G.i
F.ii

For an assessment we would produce several items. One is a version of the System of Trust (SoT) Body of Knowledge (BoK) showing the subset identified as most pertinent to this effort. This subset is referred to as a candidate profile of System of Trust and is normally shown with a red bordered around items in a word document containing the full set of the SoT BoK for context.

Producing this document entailed creating an initial subset by the assessment team that would then be reviewed with a broader set of project staff from the other project management staff. Subsequently we created the first draft of possible sources of information to support assessing the risks in the profile.

Below is a narrative description of the methodology and activities depicted in Figure 1, the Supply Chain Assessment Task Flow.

Methodology

(A) Review supply chain(s) – Identify those to be assessed

Outputs from this phase will be the list of organizations for assessments against the supply chain profiles.

(B) Defining Initial Scope of Risks

The initial scope of risks is defined based on areas of concern, such as supplier reliability, geopolitical factors, or product vulnerabilities. This step ensures that the risk evaluation process is aligned with organizational priorities and objectives. The initial scoping will focus on the risks that come from the supplier of the goods. Subsequent profiles will address other supply chain participants, such as those providing services and the goods themselves as appropriate.

(Bi) Craft Initial Subset of SoT Risk Factors

The process element leverages a comprehensive framework of 701 measurable risk factors and 1,363 risk measures, used in the overall SoT Framework. These factors and measures are reviewed to identify a subset (profile) relevant to the specific supply chain under evaluation.

(Bii) SoT Profile Candidate

The initial focus for tailoring the process in this example is on supplier risks. This resulted in the identification of 116 risk factors (RFs) from SoT.

(Biii) Expanding Profiles

Additional profiles for product risks and service risks can be added, enabling an incremental holistic approach to supply chain risk management.

(C) Risk Profile

The resultant, aggregate risk profile is shared with stakeholders to validate the scope of risks.

(Ci) Refining the Profile

A walkthrough with project personnel would be conducted to trim or extend the profile details based on practical and security considerations. This step ensures that the profile is both comprehensive and actionable. As a result of this activity in our example the candidate profile now includes 183 risk factors with 445 risk measures, adding 67 risk factors and their risk measures as a result of the team review.

(D) Risk Assessment Preparation

Once initial steps have been performed to generate a profile, you are ready to prepare the profile for assessment.

(Di) Finalizing the Profile

The refined risk profile is prepared for assessment by incorporating feedback from stakeholders and project personnel to assign weights to elements that will be used for assessment. This step can be extended to craft mitigations for each of the risk areas for later use if the risks materialize out of the assessment.

(Dii) Information Sources and Methods

Profile-specific weights are assigned to each risk factor and measure, reflecting their relative importance and impact on the supply chain element under investigation. Sources are divided into two broad categories:

- **Public Sources:** Government reports, government public resources, open-source intelligence, academic studies, etc.
- **Private Sources:** Commercial databases, government sensitive resources, classified intelligence, law enforcement data, requests to organization being assessed, site visit to organization being assessed, direct assessment of goods, 3rd party assessments, etc.

(E) Tiered Evaluation Approach

With sources and methods identified, and the profile finalized, the evaluation process may or may not benefit from a tiered approach to optimize data collection necessary for assessment.

(Ei) Tiered Evaluation Execution

The tiered approach begins with autonomous collection, where Initial data is collection from publicly available sources. Subsequent data collection can then target organization-specific data collection from individual organizations of interest.

(F) Risk Evaluation

In this stage you begin the process of evaluating risks for an initial set of suppliers where data is available.

(Fi) Residual Risks

Not all risks will have data available for use in evaluation. These unevaluated risks are recognized as residual risks in the framework. In each case, risks are documented for further investigation and mitigation. Additionally, risk scoring can model these residual risks with weighting that recognizes the potential residual risks associated with these areas.

(Fii) Incremental Expansion

The evaluation process is expanded incrementally to cover additional tiers of the supply chain. This approach ensures scalability and adaptability.

(G) Results Review and Action Steps

The final stage of the process requires an evaluation of the results provided by these steps and integrated analysis components. Evaluation results are reviewed incrementally to identify patterns, trends, and areas requiring immediate attention.

(Gi) Mitigation Planning

Actions are planned to mitigate both evaluated risks and residual risks. Mitigation strategies can include any number of actions, both long, and short-term, including supplier diversification, enhanced monitoring, and contingency planning. Listed mitigations for the individual risks in SoT can form a starting point for this step.

(Gii) Profile Refinement

Risk profiles are refined based on lessons learned during the evaluation process. This iterative approach ensures continuous improvement and increased security. The overall risk management process is optimized to enhance efficiency, accuracy, and scalability.

Conclusion

The incremental approach to supply chain assessment outlined in this process provides a structured framework for identifying, evaluating, and mitigating risks in a data driven, repeatable and explainable way. By leveraging stakeholder input, tiered evaluations, and iterative refinements, organizations can enhance their resilience and adaptability in the face of evolving challenges from their supply chains.

This paper provides a comprehensive outline for implementing an incremental risk profiling and evaluation process in supply chain management that leverages the System of Trust framework. The methodology is adaptable to various supply chain structures, enabling organizations to proactively address vulnerabilities and ensure operational resilience.