Journal of Innovation
August 2024 | 25th Edition

Object Management Group

Guiding Supply Chain Security in Aeronautic Development

Authors:

Robert A. Martin
MITRE Corporation
ramartin@mitre.org

Sean Barnum
MITRE Corporation
sbarnum@mitre.org

Aaron Phillips
Boeing Intelligence and Analytics
aaron.r.phillips@boeing.com

CONTENTS

FIGURES

In the Aeronautics industry, assessing supply chain elements for security, financial, ethical, geographical, resilience, quality and integrity risks is complicated by: (1) the lack of standard sets of risks to potentially assess; (2) a lack of standard practices for how to evaluate those risks in a consistent, structured, and defendable manner; and (3) no clear way to convey the results.[1] [2]

This paper proposes an approach leveraging System of Trust™ (SoT) as a body of knowledge of supply chain-relevant risks and shows how this can be applied to the supply chain risk assessments that the Aeronautics industry conduct. An assessment, with at-a-glance illustration of the findings and detailed assessment data for measures used, is included as an example for others to leverage.

While supply chain security issues loom large in organizations, they lack a demonstrable, scalable, repeatable, and defensible approach to perform due-diligence assessments of their supply chain partners that can communicate to leadership who meets their risk appetite and why. Real-world consequences within the aeronautic field were demonstrated by the Advanced Air Mobility (AAM) supply chain working group by NASA Aeronautics Research Institute (NARI). The AAM supply chain group provided evidence on Boeing and Airbus showing contractual cost consequences due to supply structure changes and supply volatility.[3] This new work leverages MITRE's history of efforts to clarify and standardize security measurement and demonstrates the presentation of its application and findings outcomes.

1 Supply Chain Security Issues in Aerospace

Most current supply chain security practices lack uniformity and scoping for supply chain risk management. Framing a supply chain risk for leadership personnel often requires a specific security education to enable decision making. In the past, software development and cybersecurity were independent fields of study and application.

With the introduction of DevSecOps, which fuses both software development and cybersecurity goals into a single blended perspective, came positions devoted to its integrated implementation and the study of its practical benefits. Acquisition, requirements building, and engineering parts selection are currently going through a similar fusion of supply chain and security perspectives. Supply Chain Security is at the forefront of cybersecurity topics, leading discussions on how to solve and prepare the industry for the known problems that have evolved. Leadership needs to

[1] *https://www.cutter.com/article/supply-chain-security-system-trust-framework-concerns-blocking-trust-supplies-suppliers*

[2] *https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2021/winter/defining-system-trust-sot-a-keystone-tool-supply-chain-security/*

[3] *https://nari.arc.nasa.gov/sites/default/files/attachments/2021-09-09%20AeroDynamic%20Advisory%20AAM%20Supply%20Chain%20Working%20Group%20Presentation.pdf*

understand the state its supply chain is in, and the consequences derived from the risks of that state.

Risks vary widely on the supply chains involved and become more complex the larger the project. Each part, when viewed in tiers of acquisition, expands. Simply given, one part selection may have three to five tiers down to its material sources. A large scale project potentially has upwards of a million parts, vendors, and transitive modes to track. Each part has a supply chain that services that part. Add more parts and your supply chains grow like a seed taking root. The more mature the project, the more intertwined these supply chains get. Rooting out a bad supply chain or risk involved within each part becomes a task load beyond one company's capability. This becomes ever more realized when other key factors like safety become mixed into the engineering process.

Aerospace is a growing industry bolstered by space exploration, commercial travel, weather tracking, new technology, and the increase of contracting. The abilities of planes, rockets, and satellites are growing tremendously. Once simple avionic projects are now housing a multitude of sensors and smart logic bearing devices, with complex programs to manage everything. Multiple systems rely on key data. With the introduction of new parts, more cost, and new supply chains without the ability to evaluate the increase of supply chain problems, effective and informed decisions cannot be made. With more moving parts, simpler attacks become easier to employ.

Exemplifying the changing world of Aerospace supply chains, NASA has moved to a contracting approach for the Space Launch System.[4] This creates new and unique multi-party supply chains where the government must now rely on the contractor for visibility, trusting not only the contractor but the sub-contracts and vendor management of the company selected. Any failure when tracking the vendors may lead to inaccurate cost projections as well as safety and reliability issues unknown to such organizations unless they have a framework that implements accountability measures in place for the contract.

The competing concerns of industry, contractors, and government shape supply chain requirements and the resiliency the system needs to face. Supply chains can be constrained through regulation with the Trade Act Agreements or sole United States of America and Ally manufacturing processes, increasing the legal factors companies will face. Increased legal considerations for supply chains combined with stakeholders outside of a specific company's control, such as the Federal Aviation Agency or Congress, pose competing interests on how a company can meet demands.

[4] *https://www.nasa.gov/news-release/nasa-prepares-for-space-launch-system-rocket-services-contract/*

Supply chain attacks target not only physical procurement but also digital. This enhances the difficulties of monitoring and measuring the attack profile of a supply chain. Embedding dependencies to software chains, counterfeiting hardware, and tampering with logic bearing devices become the weak links of system resiliency. Software Supply Chain concerns versus Hardware Supply Chain concerns span unique risk conditions and should be identified within a company's product.

Practitioners of supply chain security, cybersecurity engineering, and risk management need to understand this growing complexity and initiate a strategy to frame the importance of key supply chain aspects to leadership. With accurate company framing and leadership buy-in, the ability to assess, respond, and monitor these key areas becomes a part of everyday operations. Supply chain security has grown to the point where no single department should be offloaded the task. Acquisitions cannot make parts decisions, nor does the engineer have the same goals as a cyber analyst. Even with more moving parts, once responsibility is spread appropriately across an organization, attacks become more difficult to successfully execute.

Adversarial engagements and foreign actors are becoming more relevant as competing state actors have both funding and time to target these expanded attack vectors. Per the Mandiant M-Trends 2022 Report, supply chain vectors rose by seventeen percent rising to the second most common initial attack vector.[5] Additionally, within this report they cite the geographical conflicts of Ukraine and Russia as a key driver to increased threat actors. [6] Having a capability that can reduce or highlight the foreign influence of a company can make or break part selection. Implementing a standard knowledge base to frame key risk areas to leadership and implementing this standard throughout the company can evolve not only the companies processes but the trust its consumers have with its product.

Supply Chain Security is expanding in research with evolving standards. Current practices are not up to the rigor requisite of handling complex supply chain attacks. The complex systems within Avionics, like Fly-By-Wire, Autopilot Programs, Traffic Control Tower Interfaces by themselves are often reliable and safe components. Often such components are implemented with triple to quadruple redundancies.

The current structure works only under the assumption that adversarial engagements are not targeting the supply chains. Counterfeiting is a common type of attack but does not fully exemplify the depth that threat actors are utilizing in current day environments. If a software or hardware in the redundancy system is legitimate but tampered with, then the resiliency of the system overall collapses. This type of system failure has been observed but not only by an intentional attack but rather by faulty development procedures causing four of the five

[5] *https://cloud.google.com/blog/topics/threat-intelligence/russia-invasion-ukraine-retaliation*

[6] *https://services.google.com/fh/files/misc/m-trends-report-2022-en.pdf*

redundant flight systems on the Space Shuttle to fail.[7] Mandiant released a report showing a breakdown of an attack targeting a software supply chain, providing in-depth analysis on how a threat actor executed a supply chain compromise by using a prior network/system compromise and then laterally moving to the company's legitimate software development environments and thus eventually affecting unaware consumers.[8] Without a framework to evaluate companies and their products, the industry will continue to lack critical information and resiliency within the supply chain.

System of Trust™ identifies the standard frameset for supply chain security risk. Industry and government partners all have the responsibility to implement or audit their supply chains. No single locus within this interconnected web can fully address supply chain security alone.

2 Similarities with Supply Chain Security (SCS) Issues in Other Domains

Every type of supply chain has suppliers, items of supply and services, and involves the assembly and movement of the item being passed along to either a consumer/user or another supply chain link. Most supply chains also include a disposal phase which may include the reuse or recycling of an item no longer needed as shown in Figure 2-1. If the application of the re-furbished or recycled component is in the same grade application (as opposed to a lower grade application which may also not be in aerospace or aviation), then the visibility and security of the refurbishing or recycling process must also be part of the supply chain security.

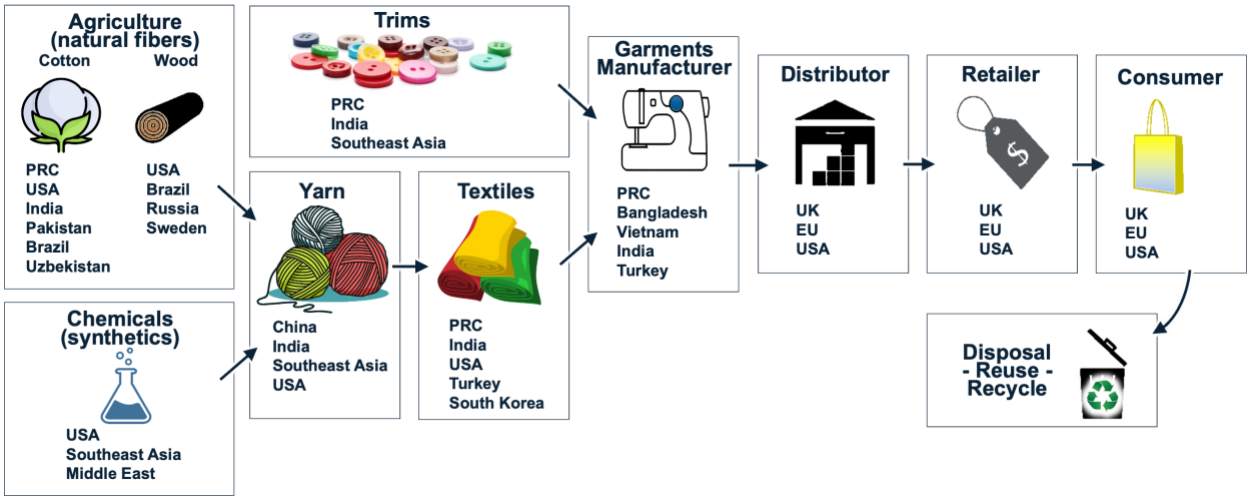

Figure 2-1: Supply chain flow example.

One reason supply chains are a focus of attention is the capacity to ship or move goods cheaply across the United States or the world, as shown in Figure 2-2. This means that most supply chains can include items and actors from anywhere.

[7] *https://web.archive.org/web/20200115234428/https://apps.dtic.mil/dtic/tr/fulltext/u2/679158.pdf*

[8] *https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/*

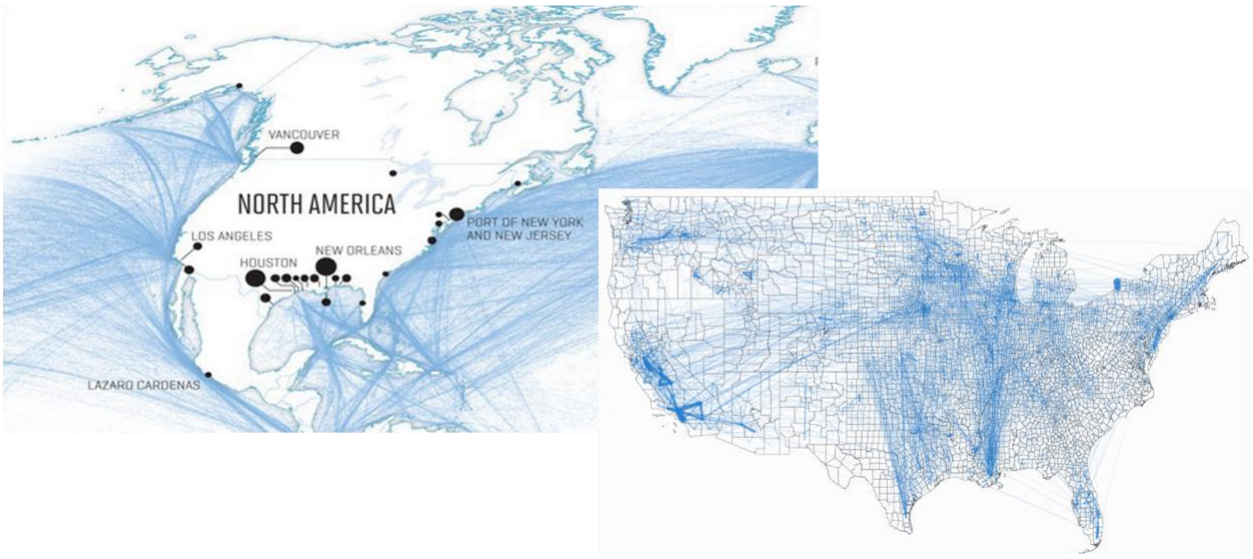

Figure 2-2: Global and United States shipping and cargo routes.

The challenge this brings is that most organizations, without full local visibility, have a hard time envisioning all the problems that could occur across their supply chains. Most do not have a good handle on what risks they may encounter through their supply chain, never mind how to manage those risks. The understanding of what risks may come from a supply chain through the suppliers involved, the supply items themselves, or the services involved is the focus of MITRE's System of Trust™ effort.

3 Crafting a Common Framework to Consistently Assess SCS Risks

With more than half a century of experience in working with MITRE's customers in the various areas of risk that face supply chains for the military, healthcare, and critical infrastructure, it has been apparent that while we, as a community, have collectively established norms about how to manage supply chain and cyber risks,[9] [10] [11] [12] [13] we have never assembled a master list of the supply chain risks we may want to manage.

This lack of an explicit basis of risk often leads to inconsistency and incompletion of risk management efforts. With the establishment of an explicit and organized Body of Knowledge, the various players in a supply chain can make use of the Body of Knowledge as a dictionary of various potential supply chain risks as well as a starting point to determine which risks they choose to address for a particular transaction, agreement, or interaction with a supplier.

[9] *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf*

[10] *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf*

[11] *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf*

[12] *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf*

[13] *https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/520044p.pdf*

To date, MITRE has gathered and shared over 650 measurable risks with over 1300 measures against them. Risks are organized into a hierarchical set of risk categories that start with supplier, supply, and service risks. Risk categories are broken down into 15 top-level risk subcategories of 7, 4, and 4 respectively for supplier, supply and service risks. Subcategories are then further spread into almost 230 lower level risk categories, as illustrated in Figure 3-1.

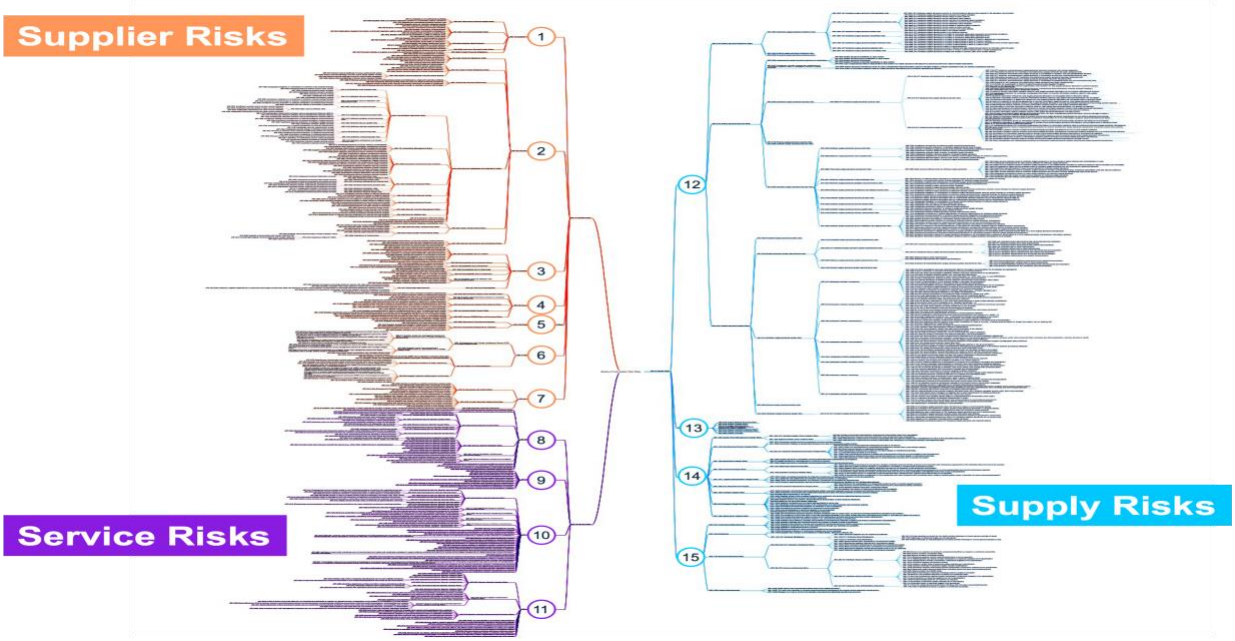

Figure 3-1: Hierarchical vocabulary of supplier, supply and service risks.

Each category of risk has a definition, a list of sub-categories of the specific risk area, and any measurable risks (risk factors) that are applicable to that category. The risk factors not only have definitions, but also have a listing of potential concrete risk measures that can be used to assess them.

Risk measures are specific conditions, expressed as yes/no questions, that can be evaluated utilizing appropriate data from relevant data sources to determine if the criteria of the condition have been met. When evaluated as true, various risk measures for a given risk factor may convey differing levels of risk qualification/quantification for the risk factor. These risk measures capture the experience and insights of subject matter experts to support practical measurement of the specific risks.

Figure 3-2 shows a screen shot from MITRE's content management system for the System of Trust body of knowledge with several risk categories (RC), risk factors (RF), and risk measures (RM) in the Supplier Financial Stability Risk area, illustrating the relationships and details of the SoT materials.

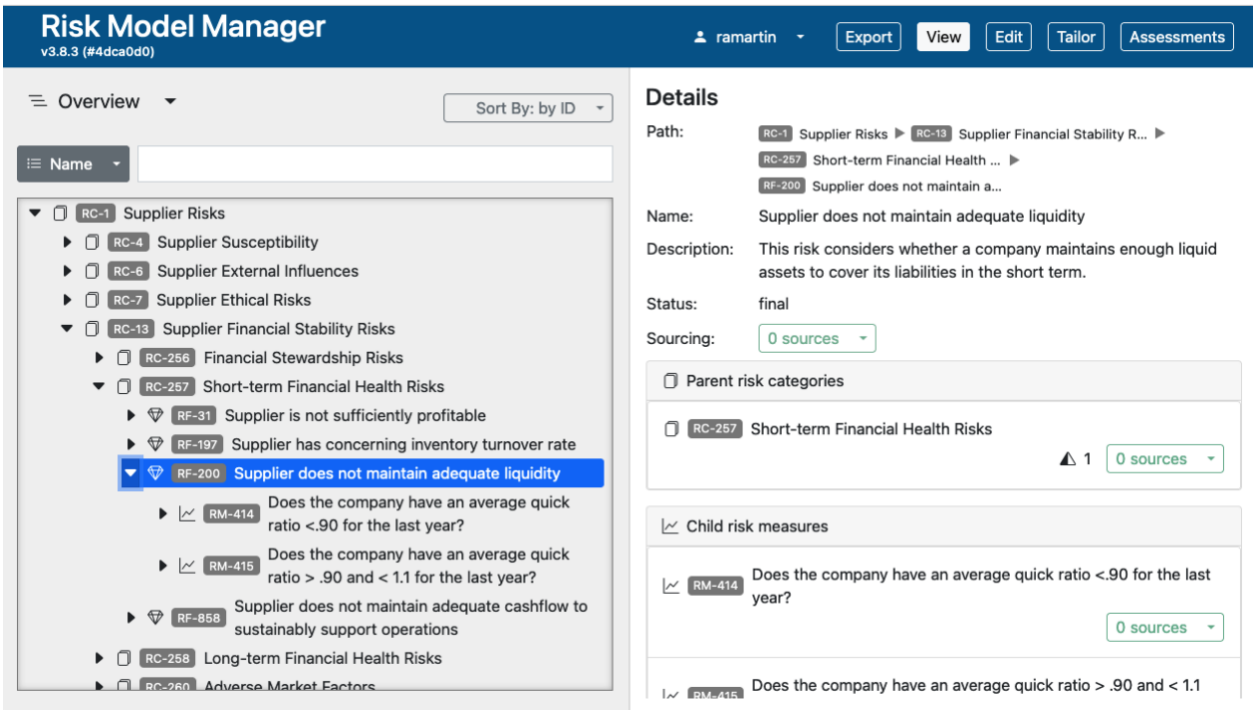

Figure 3-2: Screenshot of MITRE's content creation tool illustrating SoT knowledge.

Having a large, comprehensive, detailed list of the risks you may potentially need to address from your suppliers, supplies, or services is good, but leaves two areas open that must also be addressed. The first area is how to find the data to measure the risks you identify as relevant to your organization. The second area is how to select an appropriate subset of the overall risks to create a "profile" of the System of Trust Body of Knowledge that fits the environment, scope, and capabilities of the decisions being made.

4 IDENTIFYING SOURCES FOR ASSESSMENT DATA

When discussing sources of risk data about supply chain risks many think of public [14] [15] [16] [17] [18] [19] and commercial [20] [21] [22] [23] [24] [25] data providers that are available. These references are just some of the many sources available and each may offer useful data, if that data supports evaluation of a supply chain risk you care about and plan to use to drive your decision making. Figuring out which risks are the most important and practical for making decisions, as discussed in the next section, is key to helping determine which sources of data will best address the risks you will be assessing.

There are many other sources of supply chain security data, as shown in Figure 4-1. One important thought to contemplate is whether you want a supplier organization to be aware that you are assessing the risks about them, their offerings, and services. Passive/In-direct information sources are shown in the top branches of Figure 4-1, whereas the Active/Direct engagement approaches are shown in the lower branches.

[14] *https://www.sec.gov/edgar.shtml*

[15] *https://sam.gov/*

[16] *https://www.bis.doc.gov/*

[17] *https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information*

[18] *https://www.sec.gov/enforcement-litigation/trading-suspensions*

[19] *https://www.gleif.org/*

[20] *https://www.refinitiv.com/en/financial-data/company-data*

[21] *https://www.exiger.com/*

[22] *https://www.interos.ai/*

[23] *https://global.craft.co/*

[24] *https://www.bvdinfo.com/en-gb/our-products/data/international/orbis*

[25] *https://www.lexisnexis.com/en-us/*

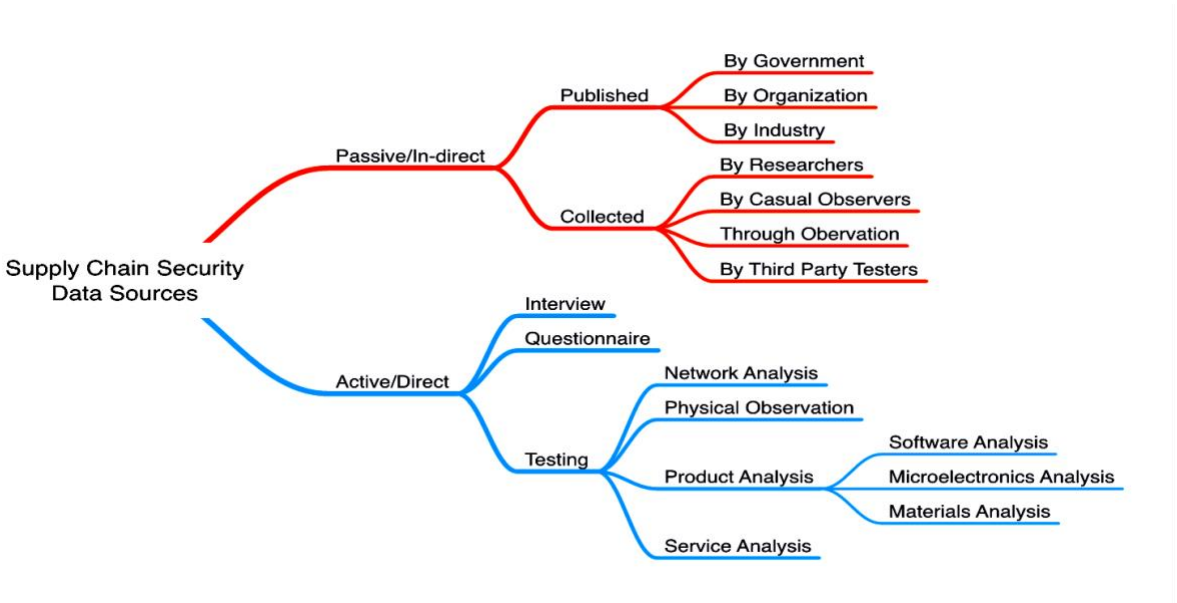

Figure 4-1: Types of passive and active supply chain security data sources.

The government and commercial sources are usually passive, in that the organization is not aware of your specific interest in them when you obtain data through those sources. If you are planning on teaming with an organization or having them be a critical part of your on-going efforts, you may eventually make use of active methods to get current detailed and specific data regarding particular risks you are concerned about.

The frequency of collection/publication of these different types of data and their "freshness" or "validity" is also a dimension to consider when selecting a data source. Briefly, some of the criteria to consider when selecting data sources include whether the data source provides data relevant to risks you care about, the appropriateness of the level of detail in the data provided, the ease of use of the data source, the visibility of the use of the data source, and how accurate and recent the data provided is.

5 Driving Down the Breadth and Depth of Topics and Risk Aspects in Scope

SoT incorporates a mechanism for winnowing down and tailoring the overall SoT Body of Knowledge of potential risks to a particular set of relevant risks and investigative questions that consider the context and resources of your organization, the significance of the system or service to its operations, and the consequences that could result from failing to fully vet supply chain risks. This "profile" is a proper subset of the overall System of Trust that an organization can repeatedly use to assess the different risk aspects of their supply chain that concern them.

The Risk Model Manager (RMM) is the prototype application being used to create and work with the Body of Knowledge of potential supply chain risks captured and curated in SoT. The RMM application functions primarily as a content management capability and learning environment

capturing and organizing the SoT Body of Knowledge of supply chain risks. The SoT content in RMM also includes insights and knowledge from various supply chain risk communities about how these risks are related and what information / evidence is needed to evaluate the individual risk factors and measures at the ends of the hierarchy branches.

Creating a profile for your own situation will require your team to consider what risks they really care to understand relative to a particular supplier, their supplies, and any services. We have found that different formats/approaches of presentation of the risks in SoT are better aligned to some aspects of creating a profile than others. The SoT web site's Pilot page[26] provides a discussion of these approaches as well as how to present the results, which we will refer to and use in the remainder of this paper.

6 AUTOMATED APPROACHES TO DEVELOPING AND DEFINING SOT PROFILES

An additional capability of RMM provides one structured way to formally define or review profiled subsets of the overall Body of Knowledge of potential risks. To do this you use the "Tailor" mode, as shown in Figure 6-1, to either select a previously created profile or start a new one. Once you start a new profile you can use the selection boxes to bring individual items into or out of scope of that profile, including whole risk categories. You can also bring in a risk category but select sub-parts of it to be out of scope.

[26] *https://sot.mitre.org/resources/papers/System_of_Trust_Body_of_Knowledge_Risk_Catalog_v1.3-Draft_Profile_of_High_Sensitivity_to_Foreign_Influence.pdf*

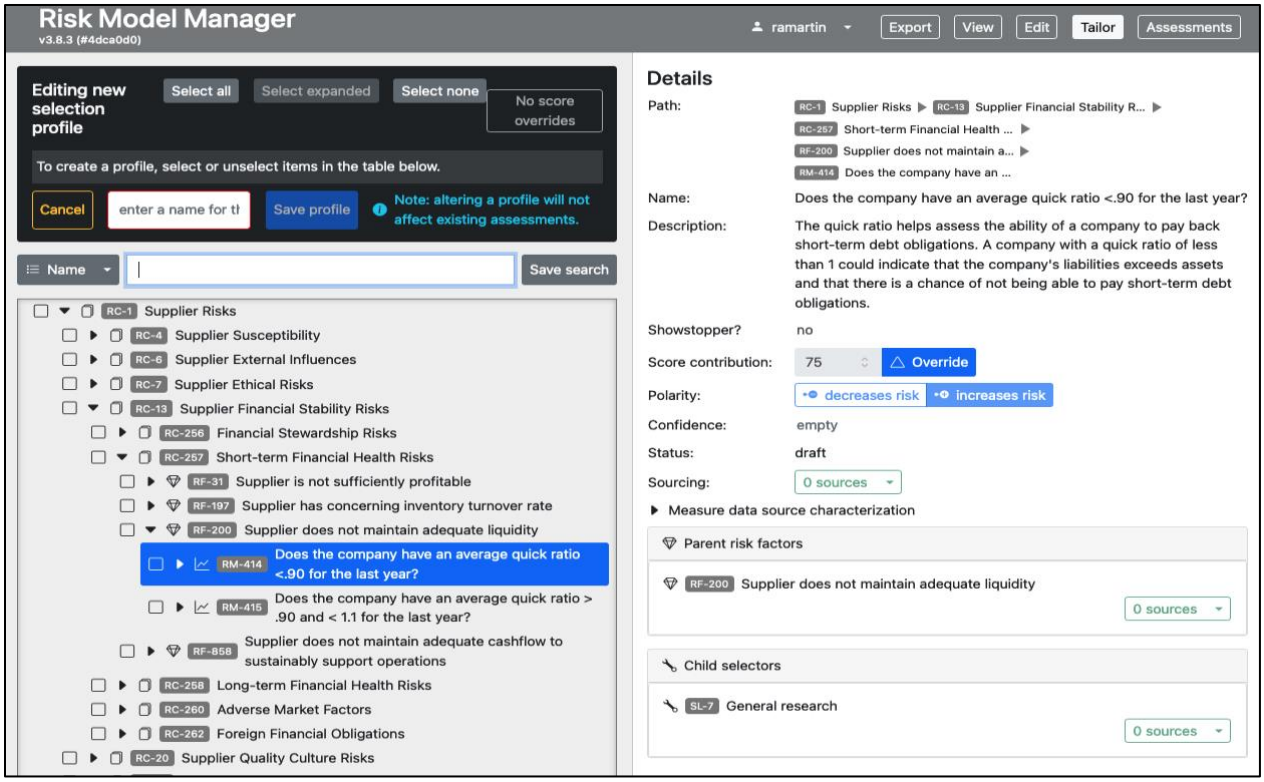

Figure 6-1: Tailor mode of RMM initial screen for making or selecting profiles of System of Trust.

7 Approaches to Presenting and Reviewing SoT Profiles

It is also possible to define SoT profile subset scopes of risks relevant for a given context using more manual document-based approaches. Whether using automated or manual approaches for defining an SoT profile, deciding which risk factors and risk measures will be appropriate for the sort of assessments you wish to perform will require a strong understanding of what sort of risks are and are not relevant for you. This understanding will serve as a filter to review the set of potential risks available within the full SoT risk Body of Knowledge.

While it is practical for an individual to review SoT risk material, we have found that viewing the material directly in the RMM is not the best way to review those risk concerns and discuss them amongst a group. Rather, we have found that Tabular Text and Spreadsheet versions of the material, as shown in Figure 7-1, are more useful. This approach is more digestible for the wide range of participants who can provide insight on relevant supply chain risks.

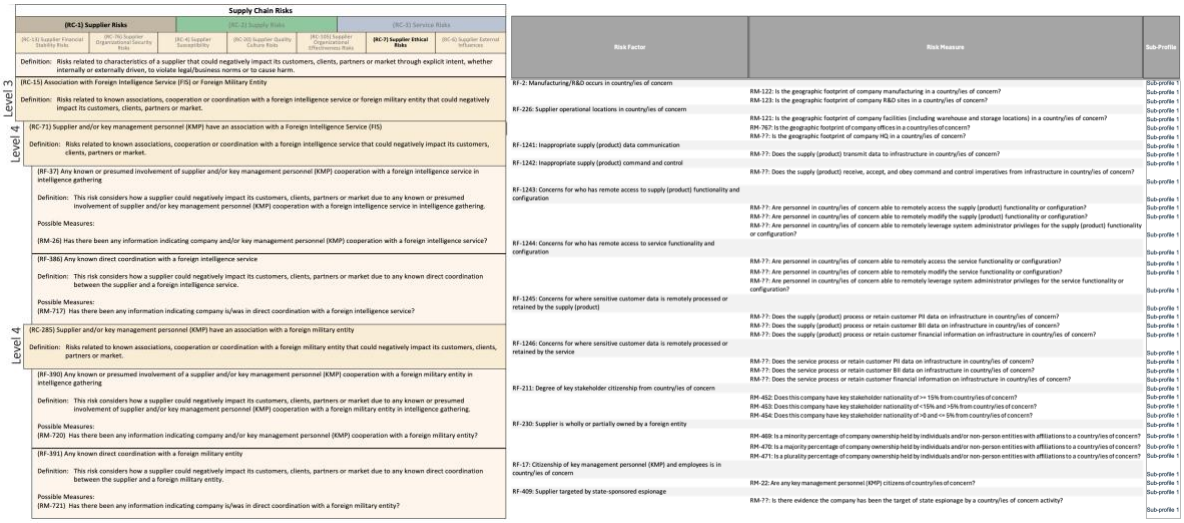

Figure 7-1: Examples of System of Trust content in tabular text and spreadsheet forms.

For sharing and discussing the risks to select profiles, we have found a tabular text version (using Word) most useful as a read-ahead and leave-behind. This approach has the full detail of the content, a built-in capability to invoke track changes, and allows the people to take things out of scope as well as make comments about them.

While useful for in-depth review of profile selection choices, this approach is not recommended for collaborative discussions or quick review meetings given the extensive detail. For getting a quick overview of risk factors and their component risk measures we have found a focused spreadsheet version of the materials to be very effective and a good way of supporting a collaborative meeting where the items could be discussed.

Once a team has culled through the overall System of Trust Body of Knowledge and created their profile or profiles of interest that reflect their effort's needs, interests, risk appetite, and available resources, they will need to be able to convey the profile(s) to others in presentations, reports, and discussions.

We found that, for profiles with more than a dozen risk factors this can be a difficult task with any of the above mechanisms (tabular text, spreadsheet, or table) and have developed a hierarchical heatmap illustration approach, shown in Figure 7-2, that can handle up to 70-80 risk factors. The heatmap can be read left-to-right with the highest level of abstraction/categorization on the left and increasing levels of deeper abstraction/categorization as you move to the right.

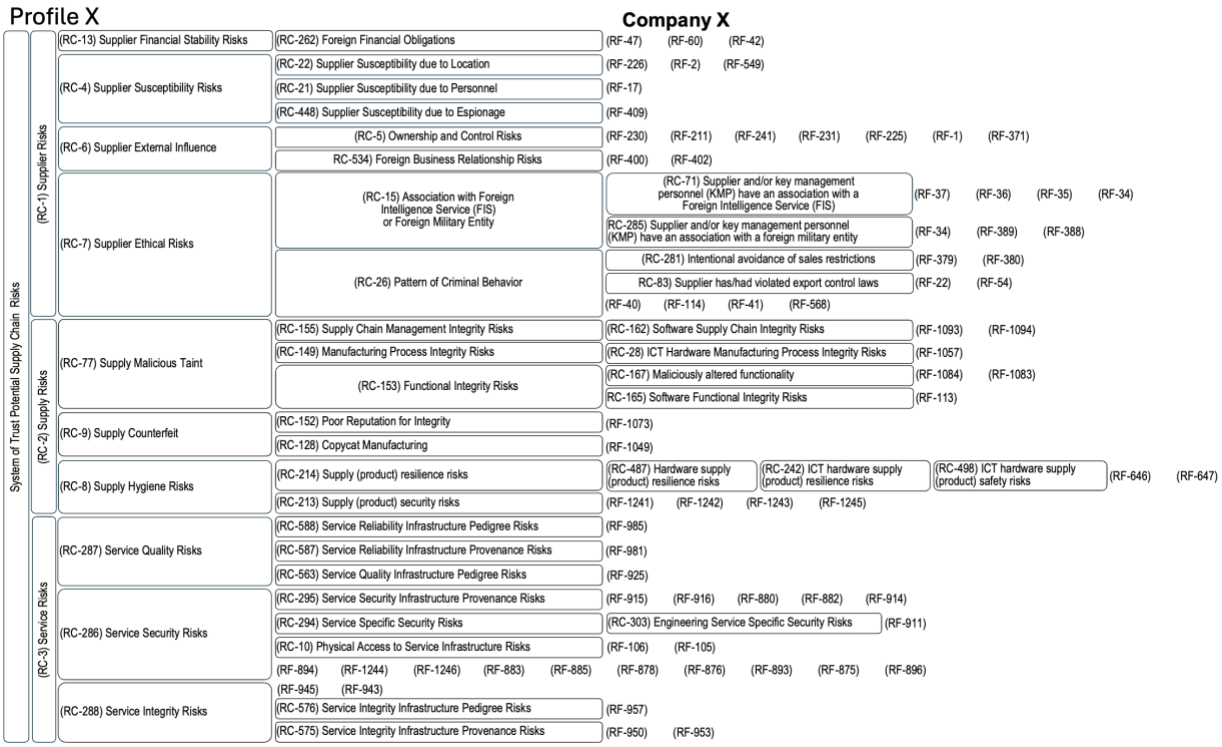

Figure 7-2: Hierarchical heatmap of profile with many risk factors.

On the SoT web site there is an example document[27] that contains a tabular text presentation of an SoT profile based on the insights and experience of our work utilizing System of Trust with various industry players and government sponsors that are concerned with the "High Sensitivity to Foreign Influence" of a supplier. In the online example document, the subset of SoT represented by this profile is shown with bolded borders and includes names and definitions for the specific risk categories, sub-categories, and measurable risk factors for this profile along with risk measurements for the risk factors.

8 PROOF-OF-CONCEPT: ASSESSING A COMPANY AGAINST A SET PROFILE OF RISKS

Once a profile has been defined and/or selected, including adequate and appropriate data sources for evaluating the relevant risk measures, the SoT process of assessment is straightforward. Assessors iteratively work through each risk measure within the scope of the assessment profile and leverage the appropriate data source to evaluate the risk measure condition to either a yes (the condition is true) or no (the condition is false). The scoring weights (either SoT defaults or profile-based overrides) for the risk measures evaluated as true are then used to calculate risk scores for the affected risk factors and roll-up weights are used to calculate risk scores for the relevant risk categories. Depending on which mechanism is being used for the assessment, these scoring calculations will be either automated or manual.

[27] *https://sot.mitre.org/framework/pilot.html*

When all risk measures within the scope of the profile have been evaluated, the assessors review across the assessment activities and findings to determine if the assessment has been successfully completed. Assessors then generate appropriate presentations of the findings, including assessment reports, to effectively convey the assessment findings to various relevant stakeholders. This may include high-level decision makers who are only interested in at-a-glance summaries as well as technical staff interested in full verbose detail to evaluate, select, and implement appropriate courses of action. We have found it important to recognize the relevant types of stakeholders in play and to craft presentations of findings appropriately.

9 Conveying Assessment Findings in a Consumable Manner

9.1 At-a-Glance Results Illustration – Hierarchical Scoring Heatmaps

The heatmaps described above for presenting profiles can be adorned with the assessment results for each of the risk factors in the profile as well as showing how those assessment results are bubbled up to summary assessments for risk categories that are in-scope for the profile being assessed. Figure 9-1 shows an example of doing this for the profile set of risk factors and risk categories that were shown in Figure 7-2. Note the key to the figure introduces the set of risk range depictions used in Figure 7-2.

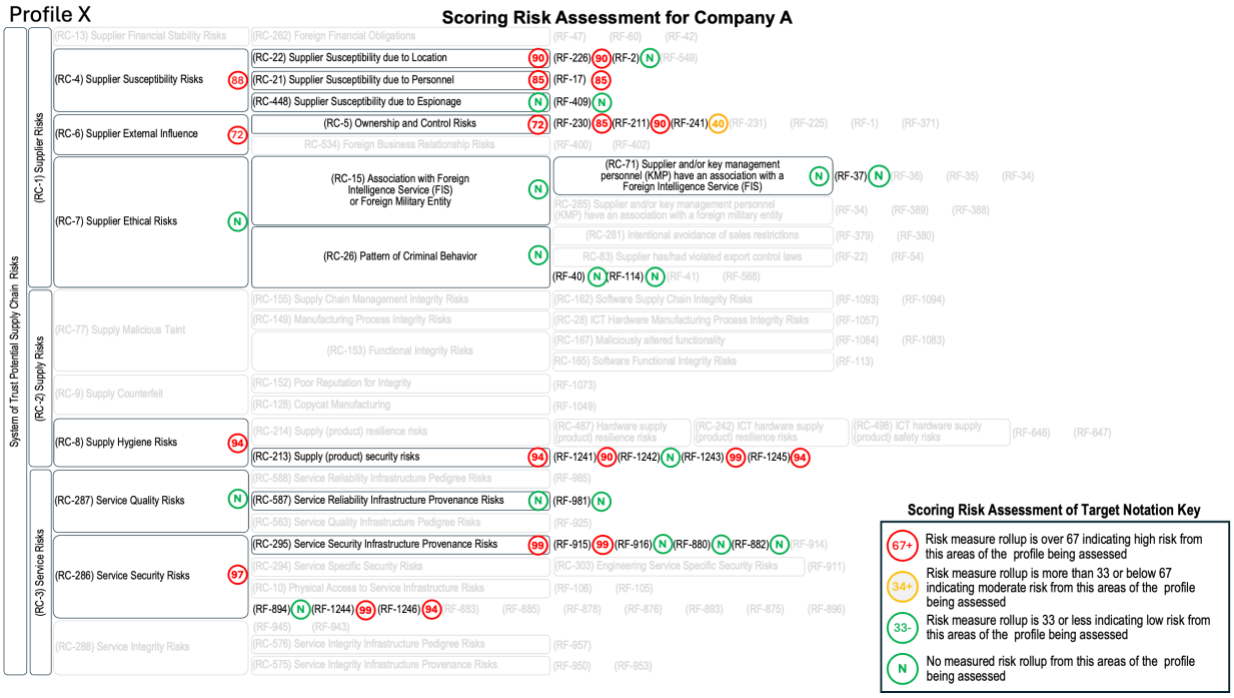

Figure 9-1: Hierarchical scoring heatmap of profile with many risk factors.

As discussed earlier in this article, one of the challenges to assessing against a System of Trust profile is finding appropriate sources for the data needed to evaluate the risk measures within the scope of the profile. So, another at-a-glance aspect of the report from an SoT assessment

that is useful is an analysis of the data sources used and documenting what risk measures and risk factors they were good sources of data for.

Figure 9-2 shows an assessment of a data source used in a proof-of-concept assessment of four companies. The heatmap is using Harvey Balls to indicate whether a risk factor's risk measures were able to be evaluated with the data from the data source for the four companies we assessed.

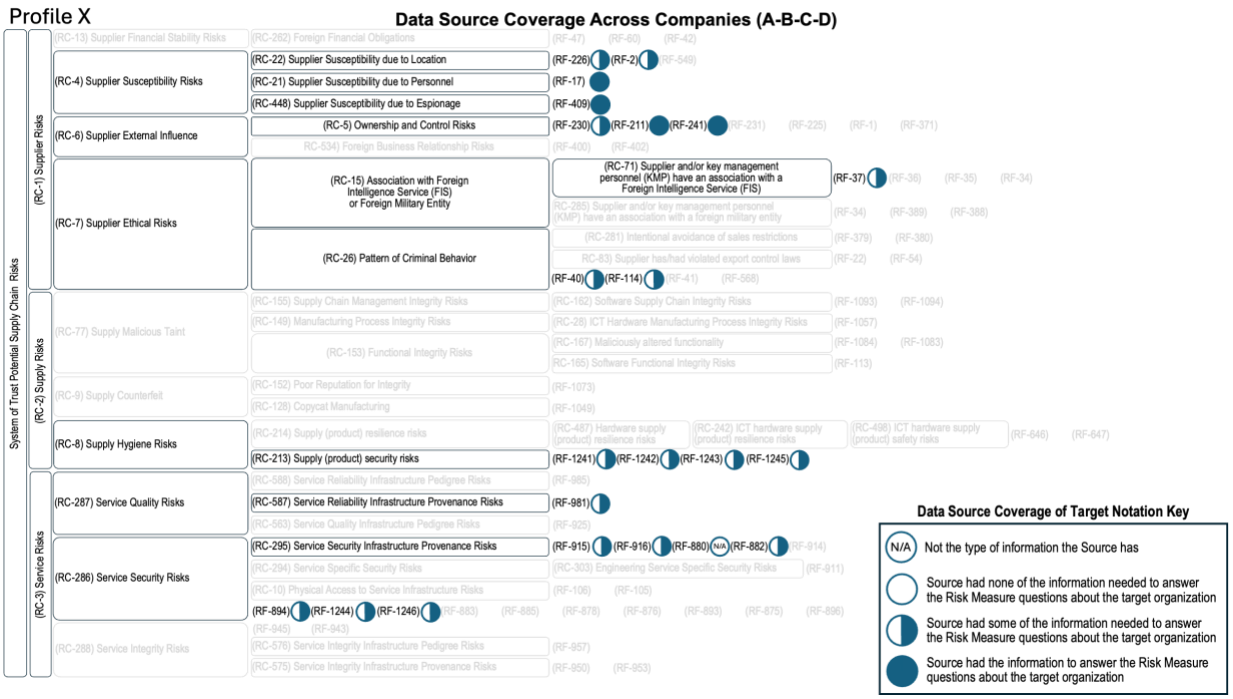

Figure 9-2: Depicting Source Coverage.

In addition to presenting the results of an assessment as a quick-glance presentation to be discussed and reviewed collaboratively, the results of an assessment will also typically be captured as a report. From our experience we suggest that the report have at least the sections, figures and tables shown below in Figure 9-3, to convey the work and findings in a consumable manner.

Table of Contents	List of Figures and Tables
1 Introduction	Table 1 Assessment Profile risk factors
2 Objectives of Assessment	Figure 1 Hierarchical scoring heatmap
3 Assessment Profile	Table 2 Scoring summary
4 Assessment Target Context	Figure 2 Hierarchical coverage heatmap
5 Profile Assessment Results	Table 3 Data source coverage summary
6 Conclusion/Recommendation	Table 4 Company overview info
Appendix – Assessment Target Organizational Context Information	Figure 3 Company ownership info

Figure 9-3: Outline and list of minimal figures and tables for an assessment report.

As indicated in Figure 9-3, tables can be another way of communicating System of Trust content. As shown in the example in Figure 9-4, tables have been found to be effective for providing an at-a-glance listing of the risk factors being used in an assessment profile, along with their definitions. These are good for inclusion in reports, but not an effective way of showing the broader hierarchical relationships between risk categories and risk measures.

Risk Factor
RF-2: Manufacturing/R&D occurs in country/ies of concern *This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier manufacturing and/or research and development occurring in country/ies of concern.*
RF-226: Supplier operational locations in country/ies of concern *This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier operations occurring in country/ies of concern.*
RF-1241: Inappropriate supply (product) data communication *This risk considers how a supply (product) may communicate sensitive or protected data to parties or locations outside of customer expectations or requirements.*
RF-1242: Inappropriate supply (product) command and control *This risk considers how a supply (product) may be influenced by command and control imperatives from parties or locations outside of customer expectations or requirements.*
RF-1243: Concerns for who has remote access to supply (product) functionality and configuration *This risk considers how a supply (product) may have its functionality and/or configuration controllable via remote access from parties outside of customer expectations or requirements.*
RF-1244: Concerns for who has remote access to service functionality and configuration *This risk considers how a service may have its functionality and/or configuration controllable via remote access from parties outside of customer expectations or requirements.*
RF-1245: Concerns for where sensitive customer data is remotely processed or retained by the supply (product) *This risk considers how a supply (product) may be unable to maintain its security properties due to where sensitive customer data is remotely processed or retained by the supply (product).*
RF-1246: Concerns for where sensitive customer data is remotely processed or retained by the service *This risk considers how a service may be unable to maintain its security properties due to where sensitive customer data is remotely processed or retained by the service.*
RF-211: Degree of key stakeholder citizenship from country/ies of concern *The likelihood that company operations are subject to antagonistic national interest is indicated by the potential allegiance of key partners and stakeholders.*
RF-230: Supplier is wholly or partially owned by a foreign entity *This risk considers whether a company may be influenced to operate in the interest of a foreign entity due to the level of foreign ownership.*
RF-17: Citizenship of key management personnel (KMP) and employees is in country/ies of concern *This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier key management personnel (KMP) or employees having citizenship in country/ies of concern.*
RF-409: Supplier targeted by state-sponsored espionage *This risk considers the likelihood of a supplier being compromised or otherwise adversely affected by malicious actors due to potential state-sponsored espionage activities targeting the supplier.*
RF-37: Any known or presumed involvement of supplier and/or key management personnel (KMP) cooperation with a foreign intelligence service in intelligence gathering *This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known or presumed involvement of supplier and/or key management personnel (KMP) cooperation with a foreign intelligence service in intelligence gathering.*
RF-114: Software has malicious attributes hidden so as to be responsive to some triggering condition *This risk considers how a supplier could negatively impact its customers, clients, partners or market due to production or distribution of software that has malicious attributes hidden so as to be responsive to some triggering condition.*
RF-894: Service provider steals intellectual property *Risk that a contracted service provider, or one of their subcontractors or employees, intentionally steals the intellectual property of the product during provision of the service. Any theft intellectual property can result in loss of a competitive edge in the market.*
RF-40: Supplier and/or key management personnel (KMP) have knowingly sold counterfeit parts or tainted parts (e.g., containing malware) *This risk considers how a supplier could negatively impact its customers, clients, partners or market due to a demonstrated history of knowingly selling counterfeit parts or tainted parts (e.g., containing malware).*
RF-915: Service requires all data to provide the service flow through hubs that are related to country/ies of concern *Services that require data flows through country(ies) of concern represent risks to provenance.*
RF-241: Key Management Personnel (KMP) or owners are Politically Exposed Persons (PEP) *This risk considers whether a company's management may be susceptible to influence due to a prominent public function a KMP holds or has held. This also includes political influence from stakeholders or non-controlling investment interests.*
RF-981: Tariffs, embargos or other governmental influence over market conditions *Services that utilize services or supplies that are subject to tariffs, embargo or other governmental influence represent risk to provenance.*
RF-880: Acquisition, sale or spin-off of critical assets to perform the service is of concern *Acquisition, sale or spin-off of critical assets to perform the service presents a security concern.*
RF-882: Service provider collects data about its customers that is beyond the control of those customers and could be leveraged or sold to a country of concern *Risks in services with hidden dual uses that include obvious uses or reasonable threats of any kind of data collection for use by others in country of concern.*
RF-916: Service provider relies on known-compromised infrastructure Services that must utilize known-compromised infrastructure to perform the service represent risk to infrastructure security of the service. Utilizing known-compromised infrastructure is fairly common at some level. However, controls and mitigations to the infrastructure can provide mechanisms for limiting risk. Nonetheless, utilizing known-compromised infrastructure is a factor in understanding risk to the service infrastructure.

Figure 9-4: Table version of System of Trust risk factor content.

10 NEXT STEPS IN SCS ASSESSMENTS FOR AEROSPACE AND AVIONICS IN GENERAL

Making defendable and repeatable data driven assessments of supply chain risks is important for the Aerospace and Avionics industry as well as other types of industries and government. Having a methodology to repeatably and effectively communicate assessment findings for supply chain assessment of suppliers, supplies and services will enable those organizations to better review and understand the details of the assessments, including their findings, to work through the implications and areas needing attention.

The hierarchical heatmaps used to convey System of Trust assessments of large sets of risk measurements at-a-glance while conveying the overall risks and their sub-elements helps meet the need for clarity about the findings from a data-driven assessment. More industries need to explore, adopt, and apply the methods in SoT before it can live up to its full potential to help all

of industry and government manage their supply chain risks more effectively, consistently, and concretely based on data.

The community of companies already working with the SoT team[28] includes organizations from many sectors and roles within those sectors but there is always room for more participation from those that have insights and problems that need solving. Only as a community can we evolve this capability for capturing and curating potential risks to ensure it offers full coverage to help us all manage, measure and mitigate supply chain risks.

11 REFERENCES

[1] Martin, R. A. "The Supply Chain Security System of Trust: A Framework for the Concerns Blocking Trust in Supplies." *Cutter Business Technology Journal, June 5, 2020. https://www.cutter.com/article/supply-chain-security-system-trust-framework-concerns-blocking-trust-supplies-suppliers-and*.

[2] Martin, R.A., Barsoum, Y., Hall, J.B., and Aisenberg, M.A. (Year). "Defining a System of Trust (SoT) as a Keystone Tool for Supply Chain Security." *SciTechLawyer, January 11, 2021*. *https//www/americanbar.org/groups/science_technology/publications/scitech_lawyer/2021/winter/defining-system-trust-sot-a-keystone-tool-supply-chain-security/*

(ABA membership required)

[3] *https://nari.arc.nasa.gov/sites/default/files/attachments/2021-09-09%20AeroDynamic%20Advisory%20AAM%20Supply%20Chain%20Working%20Group%20Presentation.pdf*

[4] National Aeronautics and Space Administration (NASA). "NASA Prepares for Space Launch System Rocket Services Contract." 26 July 2022. *https://www.nasa.gov/news-release/nasa-prepares-for-space-launch-system-rocket-services-contract/*

[5] Sadowski, James and Ryan Hall. "Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation | Mandiant | Google Cloud Blog." *Google*, Google, 4 Mar. 2022. *https://cloud.google.com/blog/topics/threat-intelligence/russia-invasion-ukraine-retaliation*

[6] *https://services.google.com/fh/files/misc/m-trends-report-2022-en.pdf*

[7] *https://web.archive.org/web/20200115234428/https://apps.dtic.mil/dtic/tr/fulltext/u2/679158.pdf*

[28] *https://sot.mitre.org/community/members.html*

[8] *https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/*

[9] National Institute of Standards and Technology (NIST) Special Publication. SP 800-53 rev 5. "Security and Privacy Controls for Information Systems and Organizations." September 2020. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf*

[10] Committee on National Security Systems Instruction (CNSSI) 1253. "Categorization and Control Selection for National Security Systems." 20 July 2022. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf*

[11] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 rev. 1. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." May 2022. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf*

[12] Department of Defense Instruction (DoDI) 4140.01. "DoD Supply Chain Material Management Policy." 6 March 2019. *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf*

[13] Department of Defense Instruction (DoDI) 5200.44. "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)." Incorporating Change October 3, 2018 (originally, November 5, 2012). *https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/520044p.pdf*

[14] Securities and Exchange Commission (SEC) Electronic Data Gathering, Analysis, and Retrieval system (EDGAR). *https://www.sec.gov/edgar.shtml*

[15] System for Award Management (SAM). *https://sam.gov/*

[16] Bureau of Industry and Security (BIS), U.S. Department of Commerce denied entities. *https://www.bis.doc.gov/*

[17] U.S. Department of the Treasury Office of Foreign Assets Control Sanctions List. *https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information*

[18] U.S. Securities and Exchange Commission Trading Suspensions. *https://www.sec.gov/enforcement-litigation/trading-suspensions*

[19] Global Legal Entity Identifier Foundation (GLEIF). *https://www.gleif.org/*

[20] Thomson Reuters Refinitiv Company Datasets. *https://www.refinitiv.com/en/financial-data/company-data*

[21] Exiger. *https://www.exiger.com/*

[22] Interos. *https://www.interos.ai/*

[23] Craft. *https://global.craft.co/*

[24] Orbis (Bureau van Dijk). *https://www.bvdinfo.com/en-gb/our-products/data/international/orbis*

[25] LexisNexis. *https://www.lexisnexis.com/en-us/*

[26] System of Trust web site. "Highly Sensitive to Foreign Influence" profile. *https://sot.mitre.org/resources/papers/System_of_Trust_Body_of_Knowledge_Risk_Catalog_v1.3-Draft_Profile_of_High_Sensitivity_to_Foreign_Influence.pdf*

[27] System of Trust Pilots web page. *https://sot.mitre.org/framework/pilot.html*

[28] System of Trust Community web page. *https://sot.mitre.org/community/members.html*

12 ACKNOWLEDGEMENTS

The views expressed in the *OMG Journal of Innovation* are the author's views and do not necessarily represent the views of their respective employers nor those of the Object Management Group® (OMG®).

- Return to *OMG Journal of Innovation landing page* for more articles and past editions.