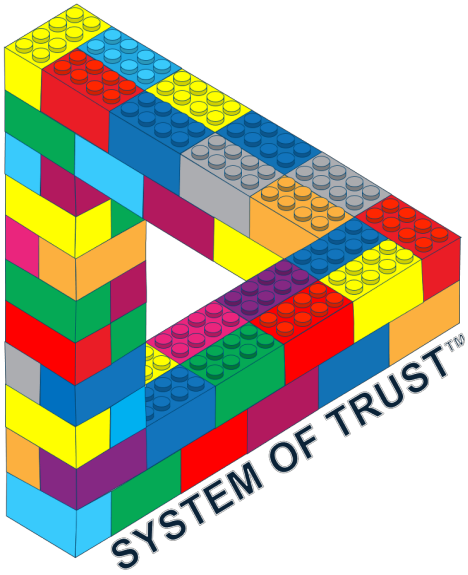
“High Sensitivity to Foreign Influence” Profile of MITRE’S System of Trust™ Body of Knowledge (v1.3) (Discussion DRAFT)



June 24, 2023

Table of Content for the Initial draft of a “High Sensitivity to Foreign Influence” SoT Profile

Introduction **2**

Profiles – A First Example **2**

System of Trust Body of Knowledge Risk Hierarchy in Table Form **3**

(RC-13) Supplier Financial Stability Risks in Table Form **3**

(RC-4) Supplier Susceptibility in Table Form **6**

(RC-105) Supplier Organizational Effectiveness Risks in Table Form **7**

(RC-6) Supplier External Influences in Table Form **12**

System of Trust Glossary **15**

Introduction

Since the introduction of System of Trust™ (SoT) at RSA2022, there has been a growing level of engagement with industry and standards bodies to evolve SoT into the standard of practice for supply chain security risk efforts. Through collaborations to add and evolve the body of supply chain risk knowledge as well as mapping and correlating existing standards and sources of supply chain risk information, the MITRE SoT effort is engaging with the broad audience of supply chain participants across the world.

The SoT Community, shown on the SoT web site [sot.mitre.org] has over 40 organizations like Intel, Micron, Microsoft, Hitachi, Dell, Raytheon, General Motors, Siemens, Synopsys, MasterCard, Cisco, BlackBerry, BSI, TIA, The Open Group, ISA, Schneider Electric, Exiger, in-teros, Stryker, and NASA SEWP that are helping to evolve SoT to address the risks they face through their supply chains. Version 1.3 of the System of Trust Body of Knowledge incorporated comments and suggestions from the SoT Community with more changes coming.

The SoT framework offers a comprehensive, consistent, and repeatable methodology – for evaluating suppliers, supplies, and service offerings alike – that is a combination of decades of MITRE's supply chain security experience and deep insights into the complex challenges facing the procurement and operations communities along with the daily experiences and insights from those running and managing supply chains across the world. By creating and curating a community-enabled structured corpus of concerns that are important for trusting organizations, products, and components, and service offerings that can be adopted, taught, and utilized by any organization involved in a supply chain, SoT offers a framework for focusing concise and rapid attention onto those risks most relevant and actionable to the parties involved in exchanging goods and services.

Organized into potential risks from Suppliers, Supplies, and Services with 7, 3, and 4 top-level risks categories in each respectively, spread into 228 individual risk categories with 642 specific measurable risk factors that can be evaluated with information.

Profiles – A First Example

SoT incorporates a mechanism for winnowing down and tailoring SoT to a set of investigative questions that consider the 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 access the different aspects of their supply chain that concerns them. This document reflects the insights and experience of our work with System of Trust with industry and sponsors that are concerned with "High Sensitivity to Foreign Influence" and is offered for discussion and evolution from those wishing to offer their thoughts. The subset of SoT represented by this draft profile is shown as bolded boarders for the relevant cells in the table on the next page. The pages following include names and definitions for the specific risk categories, sub-categories, and measurable risk factor for this profile along with a draft of measurements for the risk factors.

The Risk Model Manager (RMM) is the prototype application being used to create and work with the catalog of the potential supply chain risks cataloged in SoT. The RMM applications functions primarily as a content management capability and learning environment capturing and organizing the SoT catalog of supply chain risks. The SoT content in RMM also includes the communities' insights and knowledge about how these risks are related and what information / evidence is needed to evaluate the individual risk factors at the bottom of the hierarchy.

The RMM prototype is available to anyone wishing to explore the SoT content. There is a page to register for an account on the SoT web site.

MITRE is seeking help from the community to bring the catalog forward in richness and coverage similar to how MITRE has developed the Common Weakness Enumeration (CWE) initiative, Common Attack Pattern Enumeration and Classification (CAPEC) initiative, and ATT&CK framework with the community. System of Trust will be a similar enhancement of and leverageable resource for industry, government, and academia, just as these previous efforts are.

System of Trust Body of Knowledge Risk Hierarchy in Table Form

Supply Chain Risks

Level 1 Level 2 Level 3

(RC-1) Supplier Risks

Definition: Risks related to characteristics of a supplier of supplies (products) or services, including their supply chain, that may potentially impact consumers of those supplies (products) or services.

(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences
(RC-257) Short-term Financial Health Risks	(RC-403) Technical Operations Risks	(RC-22) Susceptibility due to Location	(RC-630) Subcontractor Supply Chain Hygiene Risks	(RC-538) Structural & Operational Instability	(RC-15) Association with Foreign Intelligence Service (FIS) or Foreign Military Entity	(RC-5) Ownership and Control Risks
(RC-256) Financial Stewardship Risks	(RC-441) Cyber Threat Intelligence Risks	(RC-25) Susceptibility due to Industry Sector	(RC-82) Supplier has Performance Issues on Contracts with other Companies	(RC-537) Geographical/Geo political Instability	(RC-26) Pattern of Criminal Behavior	(RC-534) Foreign Business Relationship Risks
(RC-260) Adverse Market Factors	(RC-16) Security Training Deficiencies	(RC-21) Susceptibility due to Personnel	(RC-18) Subcontractor Supply Chain Security Risks			(RC-536) Adverse Corporate Influences
(RC-258) Long-term Financial Health Risks	(RC-346) Security Capabilities and Operations Risks	(RC-448) Susceptibility due to Espionage	(RC-19) Internal Quality Control Risks			
(RC-262) Foreign Financial Obligations	(RC-434) Cyber Threat Activity Risks	(RC-24) Susceptibility due to Customers	(RC-632) Internal SCRM Policy and Practices Risks			
	(RC-400) Security Governance and Compliance Risks	(RC-23) Technical Susceptibility				

(RC-2) Supply Risks

Definition: Risks related to characteristics of a supply (product), including their supply chain provenance and pedigree, that may potentially impact consumers of that supply (product).

(RC-77) Supply Malicious Taint	(RC-9) Supply Counterfeit	(RC-8) Supply Hygiene Risks
(RC-155) Supply Chain Management Integrity Risks	(RC-54) Packaging Integrity Risks	(RC-214) Supply (product) Resilience Risks
(RC-149) Manufacturing Process Integrity Risks	(RC-127) Unsanctioned Manufacturing	(RC-213) Supply (product) Security Risks
(RC-154) Geopolitical Integrity Risks	(RC-126) Mislabeling	(RC-201) Supply (product) Quality Risks
(RC-153) Functional Integrity Risks	(RC-118) Technical Authenticity Risks	
(RC-151) Logistics/Transportation Integrity Risks	(RC-128) Copycat Manufacturing	
(RC-152) Poor Reputation for Integrity		
(RC-150) Facilities Integrity Risks		
(RC-156) Maintenance Integrity Risks		

(RC-3) Service Risks

Definition: Risks related to characteristics of a service, including their supply chain provenance and pedigree, that may potentially impact consumers of that service.

(RC-287) Service Quality Risks	(RC-289) Service Resilience Risks	(RC-286) Service Security Risks	(RC-288) Service Integrity Risks
(RC-563) Service Quality Infrastructure Pedigree Risks	(RC-598) Service Infrastructure Redundancy Risks	(RC-294) Service Specific Security Risks	(RC-301) Service Specific Integrity Risks
(RC-562) Service Quality Infrastructure Provenance Risks	(RC-599) Service Infrastructure Diversity Risks	(RC-11) Remote/Virtual Access to Service Infrastructure Risks	(RC-576) Service Integrity Infrastructure Pedigree Risks
(RC-300) Service Specific Quality Risks		(RC-296) Service Security Infrastructure Pedigree Risks	(RC-575) Service Integrity Infrastructure Provenance Risks
(RC-302) Service Specific Reliability Risks		(RC-295) Service Security Infrastructure Provenance Risks	
(RC-587) Service Reliability Infrastructure Provenance Risks		(RC-10) Physical Access to Service Infrastructure Risks	
(RC-588) Service Reliability Infrastructure Pedigree Risks			

Boarder indicates portion of overall System of Trust Catalog of Potential Risks within the draft "High Sensitivity to Foreign Influence" profile

(RC-13) Supplier Financial Stability Risks in Table Form

Level 3

Supply Chain Risks						
(RC-1) Supplier Risks		(RC-2) Supply Risks			(RC-3) Service Risks	
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences

Definition: Risks related to characteristics of a supplier of supplies (products) or services, including their supply chain, that may potentially impact consumers of those supplies (products) or services.

(RC-262) Foreign Financial Obligations

Definition: Risks that affect the financial health and stability of a supplier because of exposure to foreign entities through financial vehicles and relationships.

(RF-42) Financial interests of supplier are subject to contractual obligations to a country of concern

Definition: This risk considers whether a company's financial stability may be affected by direct contractual obligations to a foreign government of or other companies based a country of concern.

Possible Measures:
RM-4: Does the indebtedness threaten the viability or profitability of the company?
RM-3: Does the company have contracts, agreements, understandings, or arrangements with or indebtedness to a country of concern?

(RF-47) Financial interests of supplier are located in a country of concern

Definition: This risk considers the potential that a company's financial stability may be affected by its financial interests located within a country of concern.

Possible Measures:
RM-2: Are any of the company's interests located in countries of concern?

(RF-60) Financial interests of supplier are targeted by foreign government action

Definition: This risk considers whether a company is a target of foreign government actions that can include investigations, lawsuits, and trade restrictions that may impact its financial stability.

Possible Measures:
RM-9: Are there any indications that the company may be nationalized?

(RC-76) Supplier Organizational Security Risks in Table Form

Supply Chain Risks						
(RC-1) Supplier Risks		(RC-2) Supply Risks		(RC-3) Service Risks		
(RC-13) Supplier Financial Stability Risks	**(RC-76) Supplier Organizational Security Risks**	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences

Definition: Risks related to characteristics of a supplier's personnel, facilities, transport and cyber security capabilities, policies, and practices that affect the potential to resist and withstand malicious actions and the impact on customers.

Level 3

(RC-346) Security Capabilities and Operations Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of insufficiently implemented and managed security operational capabilities and practices.

Level 4

(RC-406) Security Controls Management Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of poor selection, application and management of appropriate security controls.

(RF-405) Exposure of internet facing assets

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inappropriately exposed or inadequately protected internet facing assets.

Possible Measures:

RM-780: Company lacks correctly configured firewalls?
RM-781: Company lacks correctly implemented/configured external access policies?
RM-782: Are any internet facing assets of product versions that are end-of-life and not longer supported?
RM-783: Are any internet facing assets of product versions that are known to be commonly targeted for attack?
RM-784: Are any internet facing assets of product versions that have recent security notifications?

Level 3

(RC-434) Cyber Threat Activity Risks

Definition: Risks that increase the likelihood a supplier will be targeted by and be unable to resist and withstand cyber malicious actions due to past or current evidence of such actions.

Level 4

(RC-436) Internal Cyber Threat Activity Risks

Definition: Risks that increase the likelihood a supplier will be targeted by and be unable to resist and withstand cyber malicious actions due to past or current evidence of such actions observed inside the company.

(RF-381) Internal Cyber Security Incidents Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to level and frequency of historical or ongoing security incidents.

Possible Measures:

RM-436: Have there been reported and documented security issues, with >=3 security incidents?
RM-437: Have there been reported and documented security issues, with 1 or 2 security incidents?
RM-438: Have there been reported and documented security issues, with no security incidents?

(RC-76) Supplier Organizational Security Risks in Table Form

Level 5

(RC-283) Indications of Compromise

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand cyber malicious actions or may be currently under the influence of such actions due to historical or ongoing indications of such activity.

(RF-384) Supplier resources/information illicitly available online

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to historical or ongoing evidence of supplier resources/information inappropriately available online (e.g., supplier IP or personnel info found on pastebin).

Possible Measures:

RM-715: Are company credential dumps available online?
RM-716: Are company data dumps available online?
RM-794: Are credential dumps available online containing credentials for company key management personnel (KMP)?
RM-795: Are credential dumps available online containing credentials for company privileged users?

Level 6

(RC-440) Suspicious Network Traffic

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand cyber malicious actions or may be currently under the influence of such actions due to historical or current observations of suspicious network traffic.

(RF-526) Supplier communicates with known malicious ICT

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to historical or ongoing evidence of communication with known malicious ICT.

Possible Measures:

RM-714: Is there observed network traffic between company infrastructure and known botnet infrastructure?
RM-792: Is there observed network traffic between company infrastructure and known malicious infrastructure within the last 6 months?

(RF-527) Unintended supplier communications with foreign networks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to historical or ongoing evidence of communication with foreign ICT networks.

Possible Measures:

RM-713: Is there observed network traffic from company infrastructure to country/ies of concern?
RM-778: Is there observed network traffic from country/ies of concern to company infrastructure?

Level 3

(RC-400) Security Governance and Compliance Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of insufficient management and compliance of security policies and processes.

(RF-404) Inadequate maturity/formality/efficacy of security policies and procedures

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequacy of explicitly defined security policies and procedures that meet a level of maturity specified in relevant independent standards.

Possible Measures:

RM-779: Company lacks explicit definition of external access policies?

(RC-4) Supplier Susceptibility in Table Form

Supply Chain Risks						
(RC-1) Supplier Risks			(RC-2) Supply Risks		(RC-3) Service Risks	
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	**(RC-4) Supplier Susceptibility**	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences

Definition: Risks related to characteristics of a supplier that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

Level 3

(RF-410) Susceptibility due to indirect purchasing

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier being the target of illicit activity via indirect purchasing.

Possible Measures:

RM-819, RM-820, RM-821: Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via front companies?
RM-822, RM-823, RM-824: Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via straw purchasing

(RF-411) Susceptibility due to targeted corporate acquisitions

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to the supplier being the target of corporate acquisition activity.

Possible Measures:

RM-825: Is there evidence the company has been the target of a corporate acquisition by another company solely for the purposes of acquiring their IP?
RM-826: Is there evidence the company has been the target of a corporate acquisition by a foreign company solely for the purposes of acquiring their IP?
RM-827: Is there evidence the company has been the target of a corporate acquisition by a foreign company (from a country of concern) solely for the purposes of acquiring their IP?

Level 3

(RC-448) Susceptibility due to espionage

Definition: Risks related to potential espionage activities targeting supplier that affect the likelihood of them being compromised or otherwise adversely affected by malicious actors. Actors can include those associated with nation-states as well as transnational and criminal organizations.

(RF-408) Supplier targeted by commercial espionage

Definition: This risk considers the likelihood of a supplier being compromised or otherwise adversely affected by malicious actors due to potential commercial espionage activities targeting the supplier.

Possible Measures:

RM-813, RM-814, RM-815: Is there evidence the company has been the target of commercial espionage activity

(RF-409) Supplier targeted by state-sponsored espionage

Definition: 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.

Possible Measures:

RM-816, RM-817, RM-818: Is there evidence the company has been the target of state espionage activity

(RC-105) Supplier Organizational Effectiveness Risks in Table Form

Level 3

Supply Chain Risks						
(RC-1) Supplier Risks		(RC-2) Supply Risks		(RC-3) Service Risks		
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	**(RC-105) Supplier Organizational Effectiveness Risks**	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences

Definition: Risks related to geographical, geopolitical, structural or operational characteristics of a supplier that affect its potential to operate in an efficacious and resilient manner.

(RC-537) Geographical/Geopolitical Instability

Definition: Risks related to a supplier's operational locations that may pose an impediment to successful operation of the company, outside of the control of the company.

(RF-242) Supplier facilities are located in areas prone to natural disasters

Definition: This risk looks at the locations of major supplier facilities and their exposure to natural hazards (cyclones, droughts, earthquakes, foods, and sea-level rise). This risk is especially high wherever natural events hit vulnerable societies.

Possible Measures:

RM-503: Is the World Risk Index of the company HQ's country >7.1%?
RM-504: Is the World Risk Index of the company HQ's country >=5.5% and <=7.1%?
RM-505: Is the World Risk Index of the company HQ's country <5.5%?
RM-857: Is the geographic footprint of company facilities in regions susceptible to extreme weather events?
RM-858: Is the geographic footprint of company facilities in regions susceptible to extreme environmental disturbances (earthquakes, floods, volcanos, etc)?

(RC-7) Supplier Ethical Risks in Table Form

Supply Chain Risks						
(RC-1) Supplier Risks			(RC-2) Supply Risks		(RC-3) Service Risks	
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	**(RC-7) Supplier Ethical Risks**	(RC-6) Supplier External Influences

Definition: Risks related to characteristics of a supplier that could negatively impact its customers, clients, partners or market through explicit intent, whether internally or externally driven, to violate legal/business norms or to cause harm.

(RC-15) Association with Foreign Intelligence Service (FIS) or Foreign Military Entity

Definition: Risks related to known associations, cooperation or coordination with a foreign intelligence service or foreign military entity that could negatively impact its customers, clients, partners or market.

Level 4

(RC-71) Supplier and/or key management personnel (KMP) have an association with a Foreign Intelligence Service (FIS)

Definition: Risks related to known associations, cooperation or coordination with a foreign intelligence service that could negatively impact its customers, clients, partners or market.

(RF-36) Any known or presumed associations of key management personnel (KMP) family members or their known associates with a foreign intelligence service

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known or presumed associations of key management personnel (KMP) family members or their known associates with a foreign intelligence service.

Possible Measures:

RM-48: Has there been any information indicating know associates of key management personnel (KMP) having associations with a foreign intelligence service?

(RF-37) Any known or presumed involvement of supplier and/or key management personnel (KMP) cooperation with a foreign intelligence service in intelligence gathering

Definition: 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.

Possible Measures:

RM-26: Has there been any information indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?

(RF-35) Any known or presumed associations of key management personnel (KMP) with a foreign intelligence service

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known or presumed associations of key management personnel (KMP) with a foreign intelligence service.

Possible Measures:

RM-49: Has there been any information indicating key management personnel (KMP) and/or family member associations with a foreign intelligence service?

(RF-34) Any convictions or solid evidence of supplier and/or key management personnel (KMP) involvement in espionage activities for a foreign government

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any convictions or solid evidence of supplier and/or key management personnel (KMP) involvement in espionage activities for a foreign government.

Possible Measures:

RM-25: Is there credible information regarding the company and/or key management personnel (KMP) espionage activities for a foreign government?

(RF-386) Any known direct coordination with a foreign intelligence service

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known direct coordination between the supplier and a foreign intelligence service.

Possible Measures:

RM-717: Has there been any information indicating company is/was in direct coordination with a foreign intelligence service?

Level 4

(RC-285) Supplier and/or key management personnel (KMP) have an association with a foreign military entity

Definition: Risks related to known associations, cooperation or coordination with a foreign military entity that could negatively impact its customers, clients, partners or market.

(RF-34) Any convictions or solid evidence of supplier and/or key management personnel (KMP) involvement in espionage activities for a foreign government

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any convictions or solid evidence of supplier and/or key management personnel (KMP) involvement in espionage activities for a foreign government.

Possible Measures:

RM-25: Is there credible information regarding the company and/or key management personnel (KMP) espionage activities for a foreign government?

(RF-389) Any known or presumed associations of key management personnel (KMP) family members or their known associates with a foreign military entity

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known or presumed associations of key management personnel (KMP) family members or their known associates with a foreign military entity.

Possible Measures:

RM-719: Has there been any information indicating know associates of key management personnel (KMP) having associations with a foreign military entity?

(RF-388) Any known or presumed associations of key management personnel (KMP) with a foreign military entity

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known or presumed associations of key management personnel (KMP) with a foreign military entity.

Possible Measures:

RM-718: Has there been any information indicating key management personnel (KMP) and/or family member associations with a foreign military entity?

(RF-390) Any known or presumed involvement of a supplier and/or key management personnel (KMP) cooperation with a foreign military entity in intelligence gathering

Definition: 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 military entity in intelligence gathering.

Possible Measures:

RM-720: Has there been any information indicating company and/or key management personnel (KMP) cooperation with a foreign military entity?

(RF-391) Any known direct coordination with a foreign military entity

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to any known direct coordination between the supplier and a foreign military entity.

Possible Measures:

RM-721: Has there been any information indicating company is/was in direct coordination with a foreign military entity?

Level 3

(RC-26) Pattern of Criminal Behavior

Definition: Risks related to patterns of criminal behavior by the supplier that could negatively impact its customers, clients, partners or market.

(RF-41) Supplier and/or key management personnel (KMP) have been convicted of criminal activities

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to demonstrated history of criminal convictions.

Possible Measures:

RM-18: Have any key management personnel (KMP) been convicted of criminal activity?
RM-921: Have any key management personnel (KMP) been convicted of non-business-related criminal activity?
RM-923: Has the supplier been convicted of business-related criminal activity?
RM-924: Has the supplier been convicted of non-business-related criminal activity?

(RF-568) Supplier and/or key management personnel (KMP) have been targets of national or international criminal investigation

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to a history of being the target of national or international criminal investigations.

Possible Measures:

RM-450, RM-451: Are there past criminal investigations conducted by the US or registered by the US department of justice or European equivalent?

Rationale: A company is likely to be more susceptible to bribery or corruption if it has engaged in dubious or prior illegal acts in the recent past and has not changed executive leadership or ownership since then.

Level 4

(RC-281) Intentional avoidance of sales restrictions

Definition: Risks related to intentional avoidance of relevant sales restrictions by the supplier that could negatively impact its customers, clients, partners or market.

(RF-379) Supplier has intentionally avoided sales restrictions through use of front companies

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to intentional avoidance of sales restrictions through use of front companies.

Possible Measures:

RM-704: Has the company directly established front company for the purposes of selling products to parties blocked by sales restrictions?
RM-705: Has the company sold products to parties blocked by sales restrictions via front company established by the government of a country of concern?
RM-706: Has the company sold products to parties blocked by sales restrictions via front company established by a non-government third party?

(RF-380) Supplier has intentionally avoided sales restrictions through illicit use of technology brokers

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to intentional avoidance of sales restrictions through use of technology brokers.

Possible Measures:

RM-703: Has the company sold products to parties blocked by sales restrictions via illicit technology brokers?

Level 4

(RC-83) Supplier has/had violated export control laws

Definition: Risks related to violation of export control laws by the supplier that could negatively impact its customers, clients, partners or market.

(RF-22) Supplier and/or key management personnel (KMP) have partnerships with companies/countries that, according to credible and corroborated information, have violated export control laws or that have sold significant technology to a country of concern.

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to the supplier and/or key management personnel (KMP) having partnerships with companies/countries that have violated export control laws or that have sold significant technology to a country of concern.

Possible Measures:

RM-34: Is there information to indicate that either the company itself, or one or more key management personnel (KMP), have violated Export Control laws, or have sold technology to a country of concern?

(RF-54) There is credible and corroborated information that the supplier and/or key management personnel (KMP) participates/participated in intentional illegal technology transfers

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to the supplier and/or key management personnel (KMP) participation in intentional illegal technology transfers.

Possible Measures:

RM-13: Has there been a conviction, or solid evidence, of intentional illegal technology transfer by the company, key management personnel (KMP) or any of its partners or subsidiaries?

(RC-6) Supplier External Influences in Table Form

Supply Chain Risks

(RC-1) Supplier Risks			(RC-2) Supply Risks		(RC-3) Service Risks	
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	**(RC-6) Supplier External Influences**

Level 3

Definition: Risks related to characteristics of a supplier that make it susceptible to negative influence by external motivations or allegiances. In a nation-state context this is typically an issue of foreign influences and in the commercial context this would typically be a competitor's influence on a supplier.

(RC-5) Ownership and Control Risks

Definition: Risks that increase the likelihood a supplier will be internally susceptible to negative influence by an adversary because of ownership, control, and/or direction that is influenced by external motivations or allegiances.

(RF-241) Key Management Personnel (KMP) or owners are Politically Exposed Persons (PEP)

Definition: 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.

Possible Measures:

RM-500, RM-501, RM-502: Are corporation leadership (CEO, staff, or Board of Directors) flagged as potential PEPs?

(RF-225) Supplier restructures operations on behalf of a foreign entity

Definition: This risk considers whether a company is forced to restructure the way it manages and conducts operations, either locally or globally, in response to foreign government influence. This includes the required installation of foreign nationals in leadership and the nationalization of a company.

Possible Measures:

RM-28: Are company actions with regard to their partners of interest having connections to foreign ownership and/or influence of concern?
RM-29: Are company actions of their subsidiaries with regard to foreign ownership and/or influence of concern?
RM-31: Are company actions towards foreign ownership and/or influence significant enough to be of concern?

(RF-232) Supplier is registered or incorporated in a foreign country

Definition: This risk considers whether a company may be negatively influenced due to registration or incorporation in a foreign country.

Possible Measures:

RM-43: Is the supplier incorporated or registered in a foreign country of concern?
RM-44: Is the country of registration/ incorporation for non-person entities that have an ownership or controlling relationship to the company in a country of concern?
RM-1101: Is the supplier incorporated or registered in a foreign country not of concern?

(RF-1) Key Management Personnel (KMP) or owners have relationships to non-state organizations of concern

Definition: This risk considers whether a company's management may be susceptible to influence due to relationships with non-state organizations of concern such as non-state activists, terrorist organizations or ties with non-governmental organizations.

Possible Measures:

RM-38: Are any KMP or owners connected to non-state organizations of concern?
RM-1097: Are any former KMP or owners connected to non-state organizations of concern?

(RF-371) Supplier has merged with, acquired, or been acquired by a foreign entity

Definition: This risk considers whether a company may change towards the interest of a foreign entity due to merger & acquisition activity with a foreign company.

Possible Measures:

RM-427: Has the company recently been acquired, restructured or merged by stakeholders from an adversary nation?
RM-428: Has the company recently been acquired, restructured or merged by stakeholders from a non-adversary nation?
RM-774: Has the company recently taken steps to be acquired, restructured, or merged by stakeholders from a country of concern?
RM-775: Has the company recently taken steps to be acquired, restructured, or merged by stakeholders from a foreign state that is not a country of concern?

Level 3

(RC-534) Foreign Business Relationship Risks

Definition: Risks that increase the likelihood a supplier will be susceptible to negative influence by external motivations or allegiances because the supplier has business relationships, contracts, or reliance upon foreign entities.

(RF-400) Supplier does direct business with the government of a country of concern

Definition: This risk considers whether a company may be susceptible to influence by a foreign government (that is a country of concern) due to direct sales, purchases, or business agreements with related entities.

Possible Measures:

RM-748: Is there credible information indicating the company has sold directly to the government of a country of concern?
RM-749: Is there credible information indicating the company has purchased directly from the government of a country of concern?

(RF-399) Supplier does direct business with the government of a country that is not a country of concern

Definition: This risk considers whether a company may be susceptible to influence by a foreign government (that is not a country of concern) due to direct sales, purchases, or business agreements with related entities.

Possible Measures:

RM-746: Is there credible information indicating the company has sold directly to a foreign government that is not a country of concern?
RM-747: Is there credible information indicating the company has purchased directly from a foreign government that is not a country of concern?

(RF-44) Supplier has foreign relationship(s) with country/ies of concern

Definition: This risk considers whether a company may be susceptible to influence by a foreign government due to relationships with foreign entities.

Possible Measures:

RM-134: Does the company have ongoing partnerships, joint ventures and/or collaborations with companies that are owned or controlled by country/ies of concern, especially those companies who have aggressively sought out restricted US information and where IT and other technology, including unique manufacturing techniques, is involved in the relationship?
RM-694: Does the company have ongoing partnerships, joint ventures and/or collaborations with academic institutions that are funded or heavily influenced by country/ies of concern?
RM-695: Does the company have ongoing partnerships, joint ventures and/or collaborations with any non-company, non-government entity (think tank, industry consortium or council, etc.) that is funded or heavily influenced by country/ies of concern?
RM-696: Is the company involved in significant IP sharing with an entity that is funded or heavily influenced by country/ies of concern?
RM-697: Does the company share parts with an entity that is funded or heavily influenced by country/ies of concern?
RM-769: Is a subsidiary of the company involved in significant IP sharing with an entity that is funded or heavily influenced by country/ies of concern?

(RF-401) Supplier does indirect business with the government of a country that is not a country of concern

Definition: This risk considers whether a company may be susceptible to influence by a foreign government (that is not a country of concern) due to business relationships with entities that are linked to, but not directly controlled by, said government.

Possible Measures:

RM-750: Is there credible information indicating the company has sold indirectly to a foreign government that is not a country of concern via 3rd party proxy?
RM-751: Is there credible information indicating the company has purchased indirectly from a foreign government that is not a country of concern via a 3rd party proxy?

(RF-402) Supplier does indirect business with the government of a country of concern

Definition: This risk considers whether a company may be susceptible to influence by a foreign government (that is a country of concern) due to business relationships with entities that are linked to, but not directly controlled by, said government.

Possible Measures:

RM-752: Is there credible information indicating the company has sold indirectly to the government of a country of concern via a 3rd party proxy?
RM-753: Is there credible information indicating the company has purchased indirectly from the government of a country of concern via a 3rd party proxy?

(RC-6) Supplier External Influences in Table Form

(RF-412) Supplier income is from foreign sources

Definition: This risk considers whether a company may be obligated to a foreign political entity due to a substantial percentage of its revenue being derived from that country.

Possible Measures:

RM-835, RM-836, RM-837: Does company income come from foreign sources?
RM-838, RM-839, RM-840: Does company income come from country/ies of concern?

Level 3

(RC-536) Adverse Corporate Influences

Definition: Risks that increase the likelihood a supplier will be susceptible to negative influence by a non-state corporate entity because the supplier has business relationships, contracts, or competition with other players in the market.

(RF-816) Supplier has merged with, acquired, or been acquired by another company which introduces potential external influences not previously present

Definition: This risk considers whether a supplier will be susceptible to negative influence due to merger & acquisition activity, especially with activist investors, private equity funds, or holding companies that introduce new forms of external influence.

Possible Measures:

RM-816: Supplier has merged with, acquired, or been acquired by another company which introduces potential external influences not previously present

Rationale: This risk considers whether a supplier will be susceptible to negative influence due to merger & acquisition activity, especially with activist investors, private equity funds, or holding companies that introduce new forms of external influence.

System of Trust Glossary

Glossary Term	Glossary Definition
Counterfeit	a supply (product) that does not conform to a standard and is intentionally mislabeled
Industrial Control System (ICS)	A collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes.
Industrial Sector	a segment of the economy made up of businesses that aid other businesses in manufacturing, shipping or producing their products
Industry	refers to a collection of companies that perform the same/similar business operations (e.g. telecoms, aerospace, etc.)
Integrity	property of accuracy and completeness [ISO/IEC 27000:2016]
MITRE System of Trust™ (SoT™)	A framework aimed at defining, aligning, and addressing the specific concerns and risks that stand in the way of organizations' trusting suppliers, supplies, and service providers.
Pedigree	The pedigree of an entity is a record of its essence (the "what" it is) and the history of that essence, which can be characterized as lineage. The essence of Z came from Y whose essence came from X. This includes the "how" the entity came to be "pre-origin" (this distinction is important) as it is part of the essence of the entity. The key here is pedigree is what we know about the essence of the entity up to the point of origin. In the example of a software library this would include details of what code is part of the library, where that code came from, details of its coding language, compilation and linking, etc. Details of what it was composed or derived from.
Provenance	Provenance of an entity is a record of what happened to the entity, who did it, where and when and why from its origin to its point of consumption/use/action/etc. Chain of custody is a key part of this but provenance is about more than just chain of custody. In the example of software, provenance would include details of who did the end consumer get the software from and who did they get it from, etc. But it would also include details of things like whether it was ever encrypted/decrypted or encoded/decoded/transcoded along the way, was it repackaged, not only "who" had it but "where" and "when" did they have it, etc. It is also important to note that Pedigree and Provenance are not disjoint from each other. The pedigree of a composed or aggregated entity includes both the pedigree and the provenance of each element of the composition/aggregation from its point of origin to its point of use within the composed/aggregated entity.
Quality	the degree to which a set of inherent characteristics of an object fulfils requirements [ISO 9000]

Glossary Term	Glossary Definition
Reliability	ability of a system or component to perform its required functions under stated conditions for a specified period of time [ISO/IEC 27040:2015]
Risk Category	A particular area of conditional concern that may potentially affect risk to an entity.
Risk Factor	A particular factual or analytical condition affecting risk to an entity.
Risk Measure	A specific assertion/question that can help quantify or qualify a particular risk factor.
Sector	typically refers to four large economic sectors under which industries are grouped: • Primary: Raw materials • Secondary: Manufacturing • Tertiary: Services • Quaternary: Information services • Quinary: Human services *sometimes included*
Security	property of being protected from unintended or unauthorized access, change or destruction ensuring availability, integrity and confidentiality [IIC]
Service	A particular activity that is required for a supply chain to function. Examples include transportation, warehousing, Software as a Service (SaaS), physical security, system administration, cloud services, accounting/fiscal
Supplier	An organization or entity that provides supplies and/or services. Examples include companies, manufacturers, government organizations, contractors, OEMs, wholesalers, import/export entities
Supply	A particular physical or digital object, entity, part, component or material. Examples include devices, chips/boards, software libraries and applications, consumer goods, raw and intermediate materials.
Supply Chain	A network of entities and people that work directly and indirectly to move a good or service from production to the final consumer.
Supply Chain Security (SCS)	The part of supply chain management that focuses on the risk management of external suppliers, vendors, logistics and transportation. Its goal is to identify, analyze and mitigate the risks inherent in working with other organizations as part of a supply chain. Supply chain security involves both the physical security relating to products and cybersecurity for software and services.
Supply Chain Risk Management (SCRM)	A discipline that addresses the threats and vulnerabilities of commercially acquired information and communications technologies within and used by government information and weapon systems.
Trustworthiness	To behave voluntarily in a way not to take advantage of the trustor's vulnerable position when faced with a self-serving decision that conflicts with the trustor's objective.