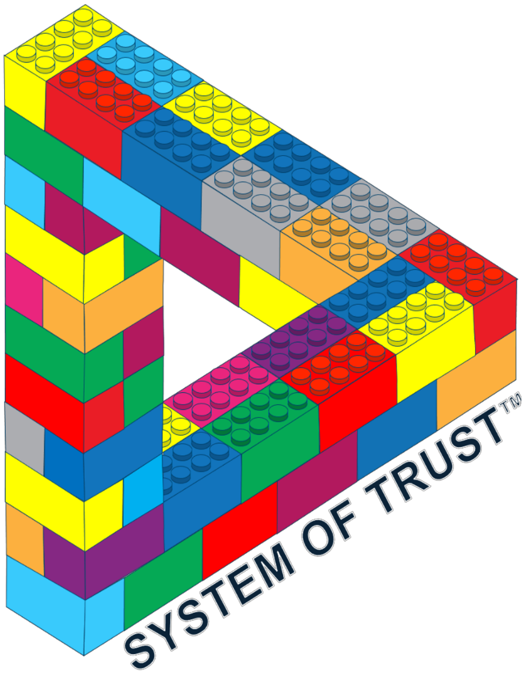
MITRE’S System of Trust™
Body of Knowledge

VERSION 1.4



May 8, 2025

System of Trust Body of Knowledges as a Hierarchy

System of Trust Risk Hierarchy in Table Form

Level 1	**(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-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-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.			
Level 2	**(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-77) Supply Malicious Taint**	**(RC-9) Supply Counterfeit**	**(RC-8) Supply Hygiene Risks**	**(RC-287) Service Quality Risks**	**(RC-289) Service Resilience Risks**	**(RC-286) Service Security Risks**	**(RC-288) Service Integrity Risks**
Level 3	(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-155) Supply Chain Management Integrity Risks	(RC-54) Packaging Integrity Risks	(RC-214) Supply (product) Resilience 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-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/ Geopolitical Instability	(RC-26) Pattern of Criminal Behavior	(RC-534) Foreign Business Relationship Risks	(RC-149) Manufacturing Process Integrity Risks	(RC-127) Unsanctioned Manufacturing	(RC-213) Supply (product) Security 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-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-154) Geopolitical Integrity Risks	(RC-127) Unsanctioned Manufacturing	(RC-201) Supply (product) Quality Risks	(RC-300) Service Specific Quality Risks		(RC-296) Service Security Infrastructure Pedigree Risks	(RC-575) Service Integrity Infrastructure Provenance Risks
	(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-153) Functional Integrity Risks	(RC-126) Mislabeling		(RC-302) Service Specific Reliability Risks		(RC-295) Service Security Infrastructure Provenance 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-151) Logistics/Transportation Integrity Risks	(RC-118) Technical Authenticity Risks		(RC-587) Service Reliability Infrastructure Provenance Risks		(RC-10) Physical Access to Service Infrastructure Risks	
		(RC-400) Security Governance and Compliance Risks	(RC-23) Technical Susceptibility					(RC-152) Poor Reputation for Integrity	(RC-128) Copycat Manufacturing		(RC-588) Service Reliability Infrastructure Pedigree Risks			
								(RC-150) Facilities Integrity Risks						
								(RC-156) Maintenance Integrity Risks						

(RC-13) Supplier Financial Stability 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 of supplies (products) or services, including their supply chain, that may potentially impact consumers of those supplies (products) or services.

Level 3

(RC-257) Short-term Financial Health Risks

Definition: Risks that affect the financial health and stability of a supplier because of poor short-term liquidity, cashflows or profitability.

(RF-31) Supplier is not sufficiently profitable

Definition: This risk considers whether a company can fulfil its core objective as a business, namely to deliver value and return on investment to its shareholders in the form of profits.

Possible Measures:
(RM-1061) Does the company have an EBITDA margin <0%?
(RM-1062) Does the company have an EBITDA margin <10% but >0%?
(RM-1063) Does the company have an EBITDA margin >10%?

(RF-858) Supplier does not maintain adequate cashflow to sustainably support operations

Definition: This risk considers whether a company can generate money from business activities to continue operating on a week-to-week basis.

Possible Measures:
(RM-1066) Are days sales outstanding >55?
(RM-1067) Are days sales outstanding >40 but <55 days?
(RM-1068) Are days sales outstanding <40 days?

(RF-197) Supplier has concerning inventory turnover rate

Definition: This risk considers whether a company properly balances inventory levels to both meet demand and optimize warehousing expense.

Possible Measures:
(RM-421) Does the company have an inventory turnover rate <4?
(RM-422) Does the company have an inventory turnover rate >6?
(RM-423) Does the company have an inventory turnover rate >=4 and <=6?

(RF-200) Supplier does not maintain adequate liquidity

Definition: This risk considers whether a company maintains enough liquid assets to cover its liabilities in the short term.

Possible Measures:
(RM-414) Does the company have an average quick ratio <.90 for the last year?
(RM-415) Does the company have an average quick ratio > .90 and < 1.1 for the last year?

Level 3

(RC-256) Financial Stewardship Risks

Definition: Risks that affect the financial health and stability of a supplier because of poor business operations and the fiduciary responsibility to deliver value to owners/shareholders.

(RF-201) Supplier has history of late payments

Definition: This risk considers whether a company regularly makes payments to creditors and suppliers as they come due, while late payments may affect the ability of a company to maintain operations.

Possible Measures:
(RM-424) Does the company have a Cortera payment score <=367?
(RM-425) Does the company have a Cortera payment score >367 and <533?
(RM-426) Does the company have a Cortera payment score >=534?

(RF-55) Supplier management behavior contributes to financial instability

Definition: This risk considers whether a company's management leads the company to remain competitive and inspires its workforce to be great, or leads the company into financial distress.

Possible Measures:
(RM-1049) Does this company have a higher than industry average level of employee turnover coupled with negative employee reviews?

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

(RM-1050) Does this company have an employee turnover rate equivalent to the industry average coupled with neutral employee reviews?

(RF-28) Supplier has history of bankruptcies

Definition: This risk considers whether a company has filed for chapter 11 bankruptcy (or foreign equivalent) in the recent past, indicating that it may be in an unstable period of restructuring and rebuilding.

Possible Measures:
(RM-1036) Has the company had a bankruptcy less than 5 years ago?
(RM-1037) Has the company had a bankruptcy between 5 and 10 years ago?
(RM-1038) Has the company had a bankruptcy 10+ years ago?

(RF-29) Organization Supplier has history of financial regulatory agency (state, federal (or foreign counterpart) investigations.

Definition: This risk considers whether a company operates in a manner suspected to be in contravention of local laws regulating financial transparency, integrity, and competition.

Possible Measures:
(RM-1052) Has the company had a financial regulatory agency judgment declared against it or admitted guilt?
(RM-1053) Has the company been the subject of one or more financial regulatory agency investigations but not directly sanctioned or admitted guilt less than three years ago?
(RM-1054) Has the company been the subject of one or more financial regulatory agency investigations but not directly sanctioned or admitted guilt more than three years ago?

(RF-19) Supplier lacks currency in public filings

Definition: This risk considers whether a company regularly makes financial disclosures as required, indicating transparency into its financial position. This Risk Factor largely pertains to publicly traded companies.

Possible Measures:
(RM-10) Has the company filed a single late financial disclosure?
(RM-57) Has the company ever had to restate its financial statements?
(RM-1057) Has the company consistently filed its financial disclosures late?
(RM-1058) Has the company filed less than 5 financial disclosures late?

(RF-204) Supplier falls behind its competitors in R&D investment level

Definition: This risk considers how a company compares to its competitors in terms of investing in R&D to expand or improve its offerings to customers.

Possible Measures:
(RM-433) Is R&D as a percentage of company revenue or total sales <=80% of the industry average benchmark?
(RM-434) Is R&D as a percentage of company revenue or total sales >80% and <=90% of the industry average benchmark?
(RM-435) Is R&D as a percentage of company revenue or total sales >90% and <=110% of the industry average benchmark?

(RF-32) Supplier has poor credit rating

Definition: This risk considers whether a company has access to capital through lines of credit and outside investment.

Possible Measures:
(RM-1055) Does the company have a junk debt rating (Ba1/BB+ or lower)?
(RM-1056) Does the company have a medium investment grade debt rating (between Baa3/BBB- and A1/A+)?

(RF-33) Supplier has history of being target of lawsuits

Definition: This risk considers whether a company has been involved in lawsuits relating to safety or business practices, judgements and settlements from which could damage the financial position of the company. This includes class-action lawsuits against the company and criminal judgements.

Possible Measures:
(RM-1042) Has there been a criminal judgement against the company?
(RM-1043) Have there been or are there pending civil suits against the company related to safety of its products or operations?
(RM-1044) Is there a pending class action lawsuit with a judgment magnitude equal to or greater than the company revenue?
(RM-1045) Have there been or are there more pending civil suits against this company related to business practices than its industry peers?
(RM-1046) Is there a pending class action lawsuit with a judgment magnitude greater than 50% of the company revenue?
(RM-1047) Have there been or are there about the same or less pending civil suits against this company related to business practices than its industry peers?
(RM-1048) Is there a pending class action lawsuit with a judgment magnitude less than 50% of the company revenue?
(RM-1358) Have there been or are there more pending civil suits against this company related to business practices than its industry peers within the last 5 years?
(RM-1359) Have there been or are there more pending civil suits against this company related to business practices than its industry peers within the last year?

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

(RM-1360) Have there been or are there more pending civil suits against this company related to product safety than its industry peers within the last 5 years?
(RM-1361) Have there been or are there more pending civil suits against this company related to product safety than its industry peers within the last year?
(RM-1362) Are there any potential lawsuits not filed yet (e.g., known because of widespread news about serious incident(s))?

Level 3

(RC-260) Adverse Market Factors

Definition: This risk considers whether the industry sector in which the company operates is experiencing a decline in business which could hurt the company in question

(RF-59) Supplier is unable to maintain market share in relation to its competitors

Definition: This risk considers a company's competition for customers with other similar companies over time.

Possible Measures:
(RM-119) Is the company's market strength good in comparison to their competitors?

(RF-30) Supplier lacks depth of experience

Definition: This risk considers how long a company has been operating, the experience level of KMP in the company's market and the average experience level of employees.

Possible Measures:
(RM-110) Has the company been established less than 3 years?
(RM-1076) Has the company been established less than 10 years but more than 3 years?
(RM-1077) Has the company been established greater than 10 years?

(RF-58) Supplier has highly volatile stock price

Definition: This risk considers whether investor's perception of the company's value is decreasing, as measured by the company's stock price.

Possible Measures:
(RM-1078) Is the company's stock price standard deviation over the last year more than double their industry average?
(RM-1081) Is the company's stock price standard deviation over the last year greater than their industry average?
(RM-1082) Is the company's stock price standard deviation over the last year equivalent to their industry average?

(RF-61) Supplier financial stability vulnerable to market decline

Definition: This risk considers the market as a whole and whether a company's financial stability is significantly influenced by a market downturn.

Possible Measures:
(RM-120) Is the company's market weak?

(RF-867) Supplier operates in a declining industry

Definition: This risk considers whether the industry sector in which the company operates is experiencing a decline in business which could hurt the company in question.

Possible Measures:
(RM-1083) Is the predicted industry growth <=2% for the next year?
(RM-1084) Is the predicted industry growth <5% but >2% for the next year?
(RM-1085) Is the predicted industry growth >= 5% for the next year?

Level 3

(RC-258) Long-term Financial Health Risks

Definition: Risks that affect the financial health and stability of a supplier because of poor long-term solvency, capital expenditures and/or debt or equity management.

(RF-866) Supplier is unable to manage assets and maintain solvency

Definition: This risk considers whether a company is sustainably balancing earnings and assets with liabilities, to maintain viability over time horizons greater than two years.

Possible Measures:
(RM-1072) Does the company have an Altman Z score <1.8?
(RM-1073) Does the company have an Altman Z score >1.8 but <3?
(RM-1074) Does the company have an Altman Z score >3?

(RF-196) Supplier may be unable to service its debts

Definition: This risk considers whether a company is sustainably balancing earnings and assets with liabilities, to maintain viability over time horizons greater than two years.

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

Possible Measures:
(RM-1069) Does the company have a debt to equity ratio greater than 150% of their industry average?
(RM-1070) Does the company have a debt to equity ratio between 75% and 150% of their industry average?
(RM-1071) Does the company have a debt to equity ratio less than 75% of their industry average?

Level 3

(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-1086) Does the company have more than 50% of its contractual obligations in a country of concern?
(RM-1087) Does the company have between 25% and 50% of its contractual obligations in a country of concern?
(RM-1088) Does the company have contractual obligations in 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-1089) Does the company have greater than 10% of its financial interests in a country of concern?
(RM-1090) Does the company have less than 10% of its financial interests in a country of concern?
(RM-1091) Does the company have financial interests in a country 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-1283) Has there been any information indicating investigations targeting financial interests of the company by foreign government(s)?
(RM-1284) Has there been any information indicating investigations targeting financial interests of KMP of the company by foreign government(s)?
(RM-1285) Has there been any information indicating investigations targeting financial interests of the company by foreign government(s) of country/ies of concern?
(RM-1286) Has there been any information indicating investigations targeting financial interests of KMP of the company by foreign government(s) of country/ies of concern?
(RM-1287) Has there been any information indicating lawsuits targeting financial interests of the company by foreign government(s)?
(RM-1288) Has there been any information indicating lawsuits targeting financial interests of KMP of the company by foreign government(s)?
(RM-1289) Has there been any information indicating lawsuits targeting financial interests of the company by foreign government(s) of country/ies of concern?
(RM-1290) Has there been any information indicating lawsuits targeting financial interests of KMP of the company by foreign government(s) of country/ies of concern?
(RM-1291) Has there been any information indicating trade restrictions targeting financial interests of the company by foreign government(s)?
(RM-1292) Has there been any information indicating trade restrictions targeting financial interests of KMP of the company by foreign government(s)?
(RM-1293) Has there been any information indicating trade restrictions targeting financial interests of the company by foreign government(s) of country/ies of concern?
(RM-1294) Has there been any information indicating trade restrictions targeting financial interests of KMP of the company by foreign government(s) of country/ies of concern?

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

<table>
<tr><th></th><th colspan="7">Supply Chain Risks</th></tr>
<tr><td></td><td colspan="2"><b>(RC-1) Supplier Risks</b></td><td colspan="3">(RC-2) Supply Risks</td><td colspan="2">(RC-3) Service Risks</td></tr>
<tr><td></td><td>(RC-13) Supplier Financial Stability Risks</td><td><b>(RC-76) Supplier Organizational Security Risks</b></td><td>(RC-4) Supplier Susceptibility</td><td>(RC-20) Supplier Quality Culture Risks</td><td>(RC-105) Supplier Organizational Effectiveness Risks</td><td>(RC-7) Supplier Ethical Risks</td><td>(RC-6) Supplier External Influences</td></tr>
<tr><td></td><td colspan="7">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.</td></tr>
<tr><td>Level 3</td><td colspan="7">(RC-403) Technical Operations 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 security challenges posed by nature and complexity of supplier technical operations.</td></tr>
<tr><td></td><td colspan="7">(RF-432) Scope and management of assets
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to the volume and type of assets deployed.
Possible Measures:
(RM-1130) Does the supplier lack an accurate inventory of existing assets and deployed locations?
(RM-1131) Does the supplier lack sufficient capability to effectively manage existing assets (i.e., deployed assets and level of effort needed for adequate management exceeds supplier capabilities)?</td></tr>
<tr><td></td><td colspan="7">(RF-436) Insufficient maturity of operational management
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to poor and inadequate management of technical operations.
Possible Measures:</td></tr>
<tr><td></td><td colspan="7">(RF-431) Complex and non-standard technology architectures
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to excessive complexity or non-standard nature of deployed technology architectures.
Possible Measures:</td></tr>
<tr><td></td><td colspan="7">(RF-430) Inadequate technical policy, governance, and resourcing
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequacy of technical policy detail, management and resourcing.
Possible Measures:</td></tr>
<tr><td></td><td colspan="7">(RF-435) Age/complexity of technology systems
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to excessive age or complexity of deployed technology systems. This includes unplanned maintenance due to failures and also includes the risks associated with a diminishing base of support such as the ability to make repairs and updates to the underlying software and related physical components, particularly those needed to address new and evolving threats.
Possible Measures:
(RM-1363) Are a majority of deployed technology systems no longer fully supported by their vendor?
(RM-1364) Will vendor support for the majority of deployed technology systems end before the life expectancy of the manufacturing plant?
(RM-1365) Is the failure rate of the deployed technology systems increasing, i.e., indications of operating beyond useful life?</td></tr>
<tr><td></td><td colspan="7">(RF-434) Complex technical dependencies
Definition: This risk considers how vulnerable to malicious activity a supplier may be due to excessive complexity of dependencies between technology systems.
Possible Measures:</td></tr>
<tr><td>Level 3</td><td colspan="7">(RC-441) Cyber Threat Intelligence 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 intelligence on known threats derived from analysis of cyber threat activity.</td></tr>
</table>

(RF-533) Recent sightings of known active threats by relevant peers

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active cyber threats by relevant peers.

Possible Measures:

(RF-532) Known active threats against peers

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active campaign threats by the supplier.

Possible Measures:

(RF-530) Known active threats against relevant industry

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to analytic evidence of known potential active cyber threats against industries relevant to the supplier.

Possible Measures:

(RF-531) Known active threats against relevant geographies

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to analytic evidence of known potential active cyber threats within geographies relevant to the supplier.

Possible Measures:

(RF-538) Recent internal sightings of insider threat behaviors

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of insider threat behaviors by the supplier.

Possible Measures:

(RF-1224) Known active threats against relevant geopolitics

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to analytic evidence of known potential active cyber threats against particular geopolitical ideologies, policies or activities relevant to the supplier.

Possible Measures:

(RF-1234) Lack of cyber threat intelligence capability

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to a lack of capability and activity to collect, assess, and analyze cyber threat intelligence and to effectively leverage it in cyber threat defense decisions.

Possible Measures:

Level 4

(RC-442) Recent internal sightings of known active threats

Definition: Risks that increase the likelihood a supplier will be targeted by and be unable to resist and withstand cyber malicious actions due to recent direct observations of known potential active cyber threats by the supplier.

(RF-537) Recent internal sightings of known active threat actors

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active threat actors by the supplier.

Possible Measures:

(RF-536) Recent internal sightings of known active attack pattern threats

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active attack pattern threats by the supplier.

Possible Measures:

(RF-535) Recent internal sightings of known active threat campaigns

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active campaign threats by the supplier.

Possible Measures:

(RF-534) Recent internal sightings of known active malware threats

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to recent direct observations of known potential active campaign threats by the supplier.

Possible Measures:

Level 3

(RC-16) Security Training Deficiencies

Definition: Risks that increase how vulnerable to malicious activity a supplier may be because the type, level, and frequency of employee training on security SOPs and threats is inadequate.

(RF-428) Employee security training does not adequately prepare all employees to respond to security incidents

Definition: This risk considers how vulnerable to malicious activity a supplier may be because employees and directly managed contract staff including outsourced services such as janitorial, cafe, construction etc., are not adequately trained to recognize and respond to common types of security incidents.

Possible Measures:
(RM-1366) Does the supplier lack cybersecurity awareness training for all employees?
(RM-1367) Does the supplier lack cybersecurity awareness training for all contractors?
(RM-1368) Does the supplier lack cybersecurity awareness training for all maintenance service providers?
(RM-1369) Does the supplier lack cybersecurity awareness training for all visitors?

(RF-427) Employee security training does not cover full range of security disciplines

Definition: This risk considers how vulnerable to malicious activity a supplier may be because the supplier does not have relevant and impactful security training for employees across the full range of relevant security disciplines. E.g., a concentration on physical security only for security guards but not for janitorial staff, cyber security response training for a limited number of cybersecurity staff but a lack of it for network operators, managers, administrators, and staff.

Possible Measures:
(RM-1370) Does supplier lack specific cybersecurity training for every position within the Human Resources system?

(RF-57) There is not sufficient organic supply chain security awareness training for all levels of employees

Definition: This risk considers how vulnerable to malicious activity a supplier may be because of insufficient employee training for supply chain security awareness.

Possible Measures:
(RM-51) Does organic supply chain security awareness training exist per NIST 800-161 guidance?
(RM-52) Does organic supply chain security awareness training per NIST 800-161 guidance occur for all relevant personnel on a yearly basis?
(RM-53) Does organic supply chain security awareness training exist per ISO 28000 guidance?
(RM-54) Does organic supply chain security awareness training exist per C-TPAT guidance?
(RM-55) Does organic supply chain security awareness training exist per TAPA FSR guidance?
(RM-1371) Does awareness training for all employees fail to adequately address supply chain security?
(RM-1372) Does specific cybersecurity training fail to adequately address supply chain security, e.g., electrical engineering, instrument and controls engineering, IT specialists, network engineers, purchasing agents, etc.?

(RF-429) Employee security training is not frequent enough to maintain currency with threats.

Definition: This risk considers how vulnerable to malicious activity a supplier may be because employee security training lacks adequate frequency to stay current with emerging and evolving threats.

Possible Measures:
(RM-1373) Does supplier lack a rationale basis for updating courses and refresher training based on emerging and evolving threats?

(RF-1225) There are insufficient drills to evaluate efficacy of security training

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy evaluation of security training through tabletop or operational drills.

Possible Measures:

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.

(RF-414) Violation of Security Policy

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to frequency and severity of security policy violations.

Possible Measures:
(RM-850) Has the company had >1 security violations (of internal policy) per 100 employees within the last 12 months?
(RM-851) Has the company had >1 security violations (of internal policy) per 100 employees within the last 6 months?
(RM-852) Has the company had >1 security violations (of National Industrial Security Program Operating Manual (NISPOM)) per 100 employees within the last 12 months?
(RM-853) Has the company had >1 security violations (of National Industrial Security Program Operating Manual (NISPOM)) per 100 employees within the last 6 months?

(RF-517) Insufficient level of operational authority for security concerns

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate level of authority to make operational decisions in regard to security concerns.

Possible Measures:

(RF-518) Insufficient visibility and integration between security operations and technical operations

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of cooperative integration between company technical operations and security operations.

Possible Measures:

Level 4

(RC-410) Software Assurance Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software assurance processes and practices.

Level 5

(RC-416) Software code analysis risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate code analysis practices.

(RF-485) Inadequate mitigation or remediation of software code analysis findings

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate mitigation or remediation of security risks identified by software code analysis.

Possible Measures:

(RF-482) Inadequate Manual-Pattern secure code review

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of Manual-Pattern software secure code review.

Possible Measures:

(RF-483) Inadequate software static analysis

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software static code analysis.

Possible Measures:

(RF-484) Inadequate software dynamic analysis

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software dynamic code analysis.

Possible Measures:

Level 5

(RC-417) Software security testing risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software security testing practices.

(RF-486) Inadequate security testing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software security testing.

Possible Measures:

(RF-487) Inadequate fuzz testing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software fuzz testing.

Possible Measures:

(RF-488) Inadequate penetration testing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software security penetration testing.

Possible Measures:

(RF-489) Inadequate mitigation or remediation of software security testing findings

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate mitigation or remediation of security risks identified by software security testing.

Possible Measures:

Level 5

(RC-419) Software secure integration and deployment risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software secure integration and deployment practices.

(RF-494) Inadequate security design of software integration and deployment process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequacy of the security design of the software integration and deployment process.

Possible Measures:

(RF-495) Insufficient security protection of software integration and deployment process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient security protection of the software integration and deployment process.

Possible Measures:

Level 5

(RC-422) Third party component risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate third party software component selection and management practices.

(RF-500) Insufficient security vetting of third party components

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of security vetting of leveraged third party software components.

Possible Measures:

Level 6

(RC-423) Open source software risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate security vetting and management of leveraged open source software components

(RF-501) Insufficient security review of open source software

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of security review of leveraged open source software components.

Possible Measures:

(RF-502) Insufficient security testing of open source software

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of security testing of leveraged open source software components.

Possible Measures:

(RF-504) Inadequate maintenance for open source software

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate maintenance for leveraged open source software components.

Possible Measures:

(RF-503) Inadequate contribution control for open source software

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate contribution control for leveraged open source software components.

Possible Measures:

Level 5

(RC-411) Software Assurance process risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequately defined and implemented software assurance processes.

(RF-473) Inadequately implemented software secure development lifecycle (SDLC)

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequately implemented software secure development lifecycle (SDLC).

Possible Measures:

(RF-474) Insufficiently effective software secure development lifecycle (SDLC)

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of the implemented software secure development lifecycle (SDLC).

Possible Measures:

(RF-472) Inadequately specified software secure development lifecycle (SDLC)

Definition: Inadequately specified software secure development lifecycle (SDLC)

Possible Measures:

Level 5

(RC-421) Software pedigree and provenance risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software pedigree and provenance practices.

(RF-498) Insufficient visibility and transparency of software pedigree and provenance

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of visibility and transparency of software pedigree and provenance.

Possible Measures:
(RM-1132) Do results from an up-to-date Software Component Analysis of supplier leveraged software not exist?
(RM-1134) Does an up-to-date Software Bill of Material (SBOM) of supplier leveraged software not exist?

(RF-499) Insufficient management of software pedigree and provenance

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient management of software pedigree and provenance.

Possible Measures:

Level 5

(RC-420) Software secure update risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software secure update practices.

(RF-497) Insufficient security protection of software update process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient security protection of the software update process.

Possible Measures:

(RF-496) Insufficient software update process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient software update processes.

Possible Measures:

Level 5

(RC-413) Software security requirements risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate definition and review practices for software security requirements.

(RF-475) Inadequate consistency in explicit specification of security requirements

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate consistency in explicit specification of software security requirements.

Possible Measures:

(RF-476) Inadequate security requirements review

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of review of software security requirements.

Possible Measures:

Level 5

(RC-418) Software secure build risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software secure build practices.

(RF-490) Inadequate security design of software build process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequacy of the security design of the software build process.

Possible Measures:

(RF-491) Choices of software build toolchain insufficiently justified for security

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient security justification for the software build toolchain choices.

Possible Measures:
(RM-1374) Are there known vulnerabilities in the chosen software build toolchain?
(RM-1375) Are there known architecture/design security issues in the chosen software build toolchain?
(RM-1376) Are there known operational security issues in the chosen software build toolchain?
(RM-1377) Have known security issues in the chosen software build toolchain not been fully mitigated?
(RM-1378) Has a threat assessment not been performed on the chosen software build toolchain?

(RF-493) Insufficient security protection of software build process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient security protection of the software build process.

Possible Measures:

(RF-492) Insufficient consistency of software build process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient consistency of the software build process.

Possible Measures:
(RM-1379) Does the defined software build process lack a defined audit process?
(RM-1380) Are there unresolved audit findings regarding the defined software build process?

Level 5

(RC-415) Software coding language risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of underlying security issues in coding languages utilized by suppler.

(RF-480) Choices of utilized coding languages insufficiently justified for security

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient consideration and justification of security concerns with the supplier's choice of utilized software coding languages.

Possible Measures:

(RF-481) Utilization of insufficiently secure coding languages

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to utilization of software coding languages with known security concerns.

Possible Measures:

Level 5

(RC-414) Software architecture and design security risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate definition and review practices for software architecture and design security.

(RF-477) Insufficient software architecture security review

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of security review of software architecture.

Possible Measures:
(RM-1381) Has the software architecture not been reviewed against known relevant security risk patterns?
(RM-1382) Are there unresolved security risk findings regarding the software architecture?

(RF-478) Insufficient software design security review

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of security review of software design.

Possible Measures:

(RF-479) Insufficient software threat modeling

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an insufficient level of software threat modeling.

Possible Measures:
(RM-1383) Does the defined software development process lack threat modeling as a key activity?
(RM-1384) Has a threat modeling assessment not been performed on the software architecture?
(RM-1385) Does the defined software development process lack an audit work process to ensure that threat modeling occurs?

Level 4

(RC-70) Vulnerability Management Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of poor awareness, management and mitigation of security vulnerabilities.

(RF-441) Inadequate patching of known relevant vulnerabilities

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate execution of patching for known relevant vulnerabilities.

Possible Measures:

(RF-438) Supplier lacks effective vulnerability management process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequately implemented and executed process for managing known vulnerabilities.

Possible Measures:

(RF-437) Supplier lacks formal vulnerability management process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequately defined and consistent process for managing known vulnerabilities.

Possible Measures:

(RF-439) Supplier inadequately tracks relevant vulnerabilities for their technical ecosystem

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to lack of awareness and explicit tracking of known vulnerabilities that are relevant to their technical ecosystem.

Possible Measures:
(RM-1386) Does the supplier lack or fail to follow a defined process to track known security vulnerabilities relevant to their technical ecosystem?
(RM-1387) Does the supplier take more than one day to note and assess published vulnerabilities from MITRE's CVE and vulnerability advisories from the US Cybersecurity & Infrastructure Security Agency (CISA)?

(RF-440) Inadequate mitigation planning for known relevant vulnerabilities

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate planning for mitigation of known relevant vulnerabilities.

Possible Measures:

Level 4

(RC-408) Inadequate technical security solutions

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of choice, implementation, configuration, deployment and operation of technical security solutions.

(RF-464) Insufficiently effective sandboxing solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated code isolation sandboxing solutions.

Possible Measures:

(RF-456) Insufficiently effective anti-malware solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated anti-malware solutions.

Possible Measures:
(RM-1388) Does the supplier lack any implemented anti-malware solutions?
(RM-1389) Does the supplier lack or fail to follow an audit program that measures implementation of anti-malware capabilities versus defined performance expectations?
(RM-1390) Does the supplier take more than one day to update anti-malware solutions with appropriate published updates and patches?

(RF-465) Insufficiently effective network traffic analysis solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated network traffic analysis solutions.

Possible Measures:
(RM-1391) Does the supplier lack approved baseline documentation for all allowable traffic?
(RM-1392) Does the supplier lack or fail to follow a work process to assess unexpected traffic that involves a risk assessment if it is decided not to shut the traffic down?

(RF-458) Insufficiently effective email security solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated email security solutions.

Possible Measures:

(RF-461) Insufficiently effective security information and even management (SIEM) solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated security information and even management (SIEM) solutions.

Possible Measures:

(RF-467) Insufficiently effective encryption and public key infrastructure (PKI) solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated encryption and public key infrastructure (PKI) solutions.

Possible Measures:

(RF-460) Insufficiently effective intrusion prevention system (IPS) solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated intrusion prevention system (IPS) solutions.

Possible Measures:

(RF-457) Insufficiently effective endpoint security solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated endpoint security solutions.

Possible Measures:

(RF-455) Insufficiently effective firewall solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated firewall solutions.

Possible Measures:
(RM-1393) Do any supplier facility communications interface with the internet without transiting a firewall, unidirectional gateway or data diode?

(RF-462) Insufficiently effective anomaly detection solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated anomaly detection solutions.

Possible Measures:
(RM-1394) Does the supplier lack an implemented security anomaly detection capability?
(RM-1395) Does the supplier fail to log all detected security anomalies?
(RM-1396) Does the supplier lack a means to rapidly determine the importance of detected security anomalies?
(RM-1397) Does the supplier lack defined responses for significant anomalies?
(RM-1398) Does the supplier lack training with respect to determination of significance and response for significant anomalies?
(RM-1399) Does the supplier lack or fail to follow an audit program that measures performance (e.g., time to respond, improper significance determination, etc.) against defined objectives for significant detected anomalies?

(RF-466) Insufficiently effective virtual private network (VPN) solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated virtual private network (VPN) solutions.

Possible Measures:

(RF-459) Insufficiently effective application security solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated application security solutions.

Possible Measures:

(RF-463) Insufficiently effective wireless security solutions

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of chosen, implemented, configured, deployed and operated wireless security solutions.

Possible Measures:

Level 4

(RC-424) Hardware Assurance Risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequately defined and implemented hardware assurance processes.

Level 5

(RC-430) Hardware fabrication risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate hardware fabrication practices.

(RF-512) Inadequate hardware fabrication process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware fabrication processes.

Possible Measures:

Level 5

(RC-432) Hardware system integration risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate hardware system integration practices.

(RC-427) Hardware logic design risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate definition and review practices for hardware logic design.

(RF-509) Inadequate hardware logic design process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware logic design processes.

Possible Measures:

Level 5

(RC-431) Hardware packaging and testing risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate hardware packaging and testing practices.

(RF-513) Inadequate hardware packaging and testing process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware packaging and testing processes.

Possible Measures:

Level 5

(RC-425) Hardware assurance process risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequately defined and implemented hardware assurance processes.

(RF-506) Inadequately implemented system engineering development process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequately implemented system engineering development process.

Possible Measures:

(RF-507) Insufficiently effective system engineering development process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient efficacy of the implemented system engineering development process.

Possible Measures:

(RF-505) Inadequately specified system engineering development process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequately specified system engineering development process.

Possible Measures:

Level 5

(RC-429) Hardware verification risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate hardware verification practices.

(RF-511) Inadequate hardware verification process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware verification processes.

Possible Measures:

Level 5

(RC-426) Hardware specification risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate definition and review practices for hardware specifications.

(RF-508) Inadequate hardware specification process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware specification processes.

Possible Measures:

Level 5

(RC-428) Hardware physical design risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate definition and review practices for hardware physical design.

(RF-510) Inadequate hardware physical design process

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate hardware physical design processes.

Possible Measures:

Level 4

(RC-409) Insufficient Security Vetting

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of insufficient vetting of security policy, procedures, implementations and operations.

(RF-471) Insufficient security vetting of relevant personnel

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate security assessment and evaluation of relevant personnel.

Possible Measures:
(RM-1400) Have background checks not been performed for any employees or contractors?
(RM-1401) Does supplier not monitor employees and contractor social media for radicalization?

(RM-1402) Are background checks for employees and contractors not periodically performed after the initial check?

(RF-413) Insufficient security vetting of supplier facilities

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate assessment and evaluation of the security of relevant facilities.

Possible Measures:
(RM-849) Does the company hold an active Facility Clearance (FCL) issued under the US National Industrial Security Program (NISP)?
(RM-1403) Has a site vulnerability assessment not been performed for each relevant supplier or contractor site?

(RF-470) Insufficient security vetting of supplier security operations

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate assessment and evaluation of security operations.

Possible Measures:
(RM-886) Does the supplier lack an up-to-date passing external assessment against the industry standards?
(RM-887) Does the supplier lack yearly externally conducted cyber risk assessments?
(RM-888) Does the supplier lack quarterly externally conducted cyber risk assessments?

Level 4

(RC-407) Insufficient Access Control

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate control of who can access supplier environments, assets and data.

(RF-453) Users of supplier networks are not subject to roles-based privileges/access

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate implementation, configuration and application of identity and access management (IDAM) capabilities.

Possible Measures:

(RF-452) Information about sensitive programs is made available to those without a need-to-know

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to insufficient data security and operations security practices allowing access to sensitive program information by personnel without appropriate need-to-know.

Possible Measures:
(RM-1404) Does the supplier not have a data classification policy in place?
(RM-1405) Can the supplier not define least privilege on an individual basis?

(RF-448) Unauthorized personnel can gain access to the facility

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate control of who can access relevant facilities.

Possible Measures:
(RM-146) Are unauthorized personnel able to physically access the facility?
(RM-185) Is not all personnel access to the facility logged?
(RM-904) Are not all facility access logs reviewed and audited?

(RF-449) Unauthorized personnel can gain access to software

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate control of who can access relevant software.

Possible Measures:
(RM-160) Are unauthorized personnel able to physically access the software?

(RF-104) Unauthorized personnel can gain access to hardware

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate control of who can access relevant hardware.

Possible Measures:
(RM-136) Are unauthorized personnel able to work on the hardware?
(RM-1406) Is physical access to hardware not controlled in accordance with least privilege?

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 no 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?
(RM-1407) Does any two-way communication occur outside of firewall control?
(RM-1408) Are unidirectional gateways or data diodes not used when there is a requirement to send but not receive information from the internet?

(RF-442) Supplier lacks a formal security controls plan

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate planning for selection and application of security controls.

Possible Measures:

(RF-444) Inappropriately configured security controls

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to a failure to appropriately configure security controls for their intended use and effect.

Possible Measures:
(RM-1409) Does the supplier lack or fail to follow a work process to periodically compare actual security control configurations to the approved design specification?
(RM-1410) Does the supplier lack or fail to follow a work process to ensure any detected security control configuration discrepancies are fixed?

Level 4

(RC-433) Security Staffing risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate staffing of security-focused personnel.

(RF-515) Inadequate levels of relevant security training for security-focused staffing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate levels of relevant security training for security-focused staff.

Possible Measures:

(RF-516) Inadequate levels of relevant security certification for security-focused staffing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate levels of relevant security certification for security-focused staff.

Possible Measures:

(RF-514) Inadequate levels of security-focused staffing

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate levels of staffing for security-focused roles.

Possible Measures:

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.

(RF-529) Efficacy of courses of action (control, mitigation, remediation, etc.)

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to ineffective choice and execution of security courses of action such as controls, mitigations, remediations, etc.

Possible Measures:

Level 4

(RC-435) External 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 outside the company.

(RF-521) External Security Compromises/Breaches Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to the frequency and severity of externally observed successful cyber security compromises or breaches.

Possible Measures:

(RF-519) External Cyber Threat Activity Trending Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to the direction and level of trending in externally observed relevant cyber threat actions.

Possible Measures:

(RF-520) External Cyber Security Incidents Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to the frequency and severity of externally observed cyber security incidents.

Possible Measures:

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-525) Internal Security Compromises/Breaches Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to historical or ongoing evidence of previous successful security compromises/breaches.

Possible Measures:
(RM-443) Within the last 5 years, were there reports of 3 or more breaches?
(RM-444) Within the last 5 years, were there reports of 1 or 2 breaches?
(RM-791) Has the company ever been successfully breached?

(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?

(RF-522) Cyber Alerts Risks

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to level and frequency of historical or ongoing cyber security alerts (indications of potential cyber threat activity affecting the company).

Possible Measures:

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?
(RM-1411) Is there observed network traffic from company infrastructure to country/ies of concern in the last year?
(RM-1412) (RM-1411) Is there observed network traffic from company infrastructure to country/ies of concern in the last year? 55 Proposed these don't hone in on 'unintended' but should. Also recommend combining with 'to/from' vs. separate RMs. why separate RMs for 12, 6, 1 mo. and 1 week? 67 Is there observed network traffic from company infrastructure to country/ies of concern in the last 6 months?
(RM-1413) Is there observed network traffic from company infrastructure to country/ies of concern in the last 1 month?
(RM-1414) Is there observed network traffic from company infrastructure to country/ies of concern in the last 1 week?
(RM-1415) Is there observed network traffic from country/ies of concern to company infrastructure in the last year?
(RM-1416) Is there observed network traffic from country/ies of concern to company infrastructure in the last 6 months?
(RM-1417) Is there observed network traffic from country/ies of concern to company infrastructure in the last 1 month?
(RM-1418) Is there observed network traffic from country/ies of concern to company infrastructure in the last 1 week?
(RM-1419) Is there observed unintended network traffic from company infrastructure to country/ies of concern in the last year?
(RM-1420) Is there observed unintended network traffic from company infrastructure to country/ies of concern in the last 6 months?
(RM-1421) Is there observed unintended network traffic from company infrastructure to country/ies of concern in the last 1 month?
(RM-1422) Is there observed unintended network traffic from company infrastructure to country/ies of concern in the last 1 week?
(RM-1423) Is there observed unintended network traffic from country/ies of concern to company infrastructure in the last year?
(RM-1424) Is there observed unintended network traffic from country/ies of concern to company infrastructure in the last 6 months?
(RM-1425) Is there observed unintended network traffic from country/ies of concern to company infrastructure in the last 1 month?
(RM-1426) Is there observed unintended network traffic from country/ies of concern to company infrastructure in the last 1 week?

Level 6

(RC-672) Suspicious Application 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 application activity.

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?

(RF-424) Supplier does not meet basic cyber security standards.

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to lack of effectively implemented cyber security capabilities to even a basic level as specified in independent standards.

Possible Measures:

(RF-425) Supplier has a poor security and compliance track record

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to a lax security culture, as demonstrated by a history of failed audits and poor compliance with required controls, actions, and standards.

Possible Measures:

(RF-426) Inadequate governance processes for security policies and procedures

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to inadequate administration and control of its security policies and procedures.

Possible Measures:

(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.

(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) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via front companies in the past 36 months?
(RM-820) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via front companies in the past 12 months?
(RM-821) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via front companies in the past 6 months?
(RM-822) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via straw purchasing in the past 36 months?
(RM-823) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via straw purchasing in the past 12 months?
(RM-824) Is there evidence the company has been the target of state attempts to bypass regulations (ITAR) via straw purchasing in the past 6 months?

(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?

(RC-22) Susceptibility due to Location

Definition: Risks related to supplier direct or indirect operational activity in particular geolocations that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

(RF-239) Supplier operational locations in countries with problematic national governance

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to location-based geopolitical instability and the potential for violence.

Possible Measures:
(RM-494) Is the WGI Government Effectiveness (GE) <= -1.00 for the country hosting the company?
(RM-495) Is the WGI Government Effectiveness (GE) >-1.00 and <0.00 for the country hosting the company?
(RM-496) Is the WGI Government Effectiveness (GE) >0.00 for the country hosting the company?

(RF-226) Supplier operational locations in country/ies of concern

Definition: 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.

Possible Measures:
(RM-121) Is the geographic footprint of company facilities (including warehouse and storage locations) in a country/ies of concern?
(RM-767) Is the geographic footprint of company offices in a country/ies of concern?
(RM-1213) Is the geographic footprint of company HQ in a country/ies of concern?

(RF-549) Supplier's sub-suppliers are in country/ies of concern

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to the supplier's sub-suppliers operating in country/ies of concern.

Possible Measures:
(RM-1267) Has there been any information indicating details of proprietary manufacturing data/trade secrets have been inappropriately altered by unauthorized parties?

(RC-4) Supplier Susceptibility in Table Form

(RF-2) Manufacturing/R&D occurs in country/ies of concern

Definition: 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.

Possible Measures:
(RM-122) Is the geographic footprint of company manufacturing in a country/ies of concern?
(RM-123) Is the geographic footprint of company R&D sites in a country/ies of concern?
(RM-1427) Is there a known likelihood that supplier facilities will be nationalized?

(RF-237) Supplier operational locations in countries with prevalency of national corruption

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to the propensity for corruption in the countries where the supplier operates.

Possible Measures:
(RM-488) Is the Corruption Perceptions Index <= 25 for the country hosting the company?
(RM-489) Is the Corruption Perceptions Index >25 and <50 for the country hosting the company?
(RM-490) Is the Corruption Perceptions Index >= 50 for the country hosting the company?

Level 3

(RC-25) Susceptibility due to Industry sector

Definition: Risks related to supplier participation in particular industry sectors that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

(RF-547) Supplier operates within commonly targeted industry sector

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to the supplier operating within commonly targeted industry sectors.

Possible Measures:
(RM-1428) Is there a history of threatening activist activity within the company's industry sector?
(RM-1429) Is there current threatening activist activity within the company's industry sector?
(RM-1430) Is there a history of ransomware attacks within the company's industry sector?
(RM-1431) Are there current ransomware attacks within the company's industry sector?
(RM-1432) Is the company's industry sector a target due to actual or potential cyber warfare between nation states?
(RM-1433) Is the company's industry sector a potential target for terrorists?

Level 3

(RC-21) Susceptibility due to Personnel

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

(RF-23) Personal financial situation of any key management personnel (KMP) is of concern

Definition: 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) having concerning personal financial situation.

Possible Measures:
(RM-33) Have any key management personnel (KMP) declared bankruptcy, do any KMP have heavy indebtedness or have/are subject to SEC investigation(s) or if foreign under an SEC counterpart investigation(s)?

(RF-52) Presence of foreign employees on visas who are from country/ies of concern

Definition: 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) having concerning personal financial situation.

Possible Measures:
(RM-23) Are a majority of the company's foreign employees on work visas from country/ies of concern?

(RF-17) Citizenship of key management personnel (KMP) and employees is in country/ies of concern

Definition: 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.

Possible Measures:
(RM-22) Are any key management personnel (KMP) or employees citizens of country/ies of concern?
(RM-1273) Are employees, contractors and/or sub-contractor staff who are involved in leadership citizens of country/ies of concern?
(RM-1274) Are employees, contractors and/or sub-contractor staff who are involved in government contracts (especially foreign governments) citizens of country/ies of concern?
(RM-1275) Are employees, contractors and/or sub-contractor staff who have access to the company’s key IT and technology citizens of country/ies of concern?

(RC-4) Supplier Susceptibility in Table Form

(RM-1276) Are employees, contractors and/or sub-contractor staff who work on site at the company’s location in foreign countries citizens of country/ies of concern? (RM-1277) Are employees, contractors and/or sub-contractor staff who are on an Excluded Parties List citizens of country/ies of concern? (RM-1435) Do any key management personnel (KMP) or employees who are citizens of a country of concern have close or active relationships with the government of that country? (RM-1436) Do any key management personnel (KMP) or employees who are citizens of a country of concern have close or active relationships with any non-government malicious actors in that country?

(RC-4) Supplier Susceptibility in Table Form

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) Is there evidence the company has been the target of commercial espionage activity in the past 36 months?
(RM-814) Is there evidence the company has been the target of commercial espionage activity in the past 12 months?
(RM-815) Is there evidence the company has been the target of commercial espionage activity in the past 6 months?

(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) Is there evidence the company has been the target of state espionage activity in the past 36 months?
(RM-817) Is there evidence the company has been the target of state espionage activity in the past 12 months?
(RM-818) Is there evidence the company has been the target of state espionage activity in the past 6 months?
(RM-1215) Is there evidence the company has been the target of state espionage by a country/ies of concern activity?
(RM-1216) Is there evidence the company has been the target of state espionage activity?
(RM-1217) Is there evidence the company has been the target of state espionage by a country/ies of concern activity in the past 36 months?
(RM-1218) Is there evidence the company has been the target of state espionage by a country/ies of concern activity in the past 12 months?
(RM-1219) Is there evidence the company has been the target of state espionage by a country/ies of concern activity in the past 6 months?

Level 3

(RC-24) Susceptibility due to Customers

Definition: Risks related to supplier customer base involving particular customers that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

(RF-554) Supplier customer affiliation with high-value commercial entities

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer affiliation with high-value commercial entities.

Possible Measures:

(RF-555) Supplier customer base is in foreign countries

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer base being in foreign countries.

Possible Measures:

(RF-49) Supplier customer base is in country/ies of concern

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer base being in country/ies of concern.

Possible Measures:
(RM-78) Is the location of a majority of the customer base in country/ies of concern?

Level 4

(RC-47) Supplier customer affiliation with governmental entities

Definition: Risks related to supplier customer base involving governmental entities that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

(RF-552) Supplier customer affiliation with intelligence service entities

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer affiliation with the intelligence service entities.

Possible Measures:

(RC-4) Supplier Susceptibility in Table Form

(RF-553) Supplier customer affiliation with law enforcement entities

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer affiliation with the law enforcement entities.

Possible Measures:

(RF-551) Supplier customer affiliation with military entities

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer affiliation with military entities.

Possible Measures:

(RF-53) Public disclosure of supplier customer affiliation with the federal government

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to supplier customer affiliation with the federal government.

Possible Measures:
(RM-84) Is the company's association with the federal government revealed in any gov't website or publication?
(RM-171) Does the company have in it's publicly released material an association with the federal government?

Level 3

(RC-23) Technical Susceptibility

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

Level 4

(RC-84) Technology dependencies

Definition: Risks related to supplier dependency on particular technology choices that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

(RF-565) Supplier leverages technology platforms shared with high-value commercial entities.

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to utilization of technology platforms shared with high-value commercial entities.

Possible Measures:
(RM-1437) Have industry data indicated attacks within the last year on technology platforms company shares utilization of with high-value commercial entities?
(RM-1438) Have government sources indicated attacks within the last year on technology platforms company shares utilization of with high-value commercial entities?

(RF-564) Supplier leverages technology platforms shared with governmental entities.

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to utilization of technology platforms shared with governmental entities.

Possible Measures:

(RF-50) Risks related to supplier dependency on particular technology choices that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to dependence on open source software, freeware and/or shareware developed in country/ies of concern.

Possible Measures:
(RM-37) Can software components be associated with a company name?
(RM-42) Is open source, freeware, or shareware software produced or dependent upon (incorporated in their own products) by the company developed in country/ies of concern?
(RM-111) Are developers of this software associated with malicious software activities?

(RF-563) Development of operational technology used by the supplier occurs in country/ies of concern.

Definition: This risk considers the likelihood of a supplier being targeted, compromised or otherwise adversely affected by malicious actors due to dependence on operational technology developed in country/ies of concern.

Possible Measures:

(RC-4) Supplier Susceptibility in Table Form

(RM-1439) Have industry data indicated attacks on company utilized operational technology developed in country/ies of concern?

(RC-20) Supplier Quality Culture 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 ability to reliably deliver appropriate quality supplies (products) and/or services.

(RF-43) Company has a low Capability Maturity Model Integration (CMMI) Rating

Definition: This risk considers the level to which a supplier is or is not managing and optimizing their business processes and organization, a lack of which could result in poor delivery of supplies and services.

Possible Measures:
(RM-165) Does the company have a low (or no) CMMI rating?
(RM-1135) Is there a lack of an appraisal result from a CMMI appraisal led by a certified Lead Appraiser?

Level 3

(RC-630) Subcontractor Supply Chain Hygiene Risks

Definition: Risks that contract language that addresses subcontractor supply chain hygiene is not adequate to address current risks, hygiene requirements are not complied with by subcontactor, or subcontractors are not audited for compliance by contracting organization. This may result from "boilerplate" language that both sides recognize as unenforceable, impractical, or contrary to market factors such as product timeliness.

(RF-56) Subcontractor lacks unambiguous guidance and expectations of the contractor's hygiene requirements

Definition: Risks related to the diligence of the supplier to set, document, and propagate to their subcontractors, their requirements that address and set standards for hygiene of subcomponents and services acquired from their subcontractors.

Possible Measures:
(RM-77) Do company contracts for ICT with sub-contractors lack a clause requiring SCRM hygiene?
(RM-1137) Is there a lack of specific quality thresholds in contract language?

(RF-1106) Supplier does not conduct effective audits of subcontractor hygiene

Definition: Risks related to the diligence of the supplier to verify the hygiene of their subcontractors using audit functions.

Possible Measures:
(RM-1440) Does supplier lack records of subcontractor audits that can be assessed for effectiveness?
(RM-1441) Does supplier not compare successive audit results for evidence of continuous improvement by the subcontractor?

Level 3

(RC-82) Supplier has performance issues on contracts with other companies

Definition: Risks that increase the likelihood that a supplier may be unreliable in fulfilling the requirements of their contracts

(RF-18) Supplier has had one or more contracts terminated

Definition: This risk considers whether a supplier is more likely to fail to fulfill the requirements of their contracts due to a history of contract terminations, particularly terminations for cause.

Possible Measures:
(RM-20) Have contracts been terminated and under what circumstances?
(RM-40) Have one or more company contracts been terminated for default/cause?

(RF-46) Supplier has unusual growth compared with its peers

Definition: This risk considers whether there are indications a supplier has gone through structural changes of inexplicable nature, which may negatively impact contract performance.

Possible Measures:
(RM-30) Is the level of company growth within its peers unusually high or low?

(RC-20) Supplier Quality Culture Risks in Table Form

(RF-20) Supplier has demonstrated an inability to execute on contracts it has with others

Definition: This risk considers whether a supplier is more likely to fail to fulfill the requirements of their contracts due to a history of unreliability, change orders, and contract renegotiation.

Possible Measures:
(RM-12) Has the company's past performance demonstrated an inability to deliver goods and/or services that meet generally accepted industry standards?
(RM-21) Has the company's prior contract history demonstrated an inability to execute contract performance requirements and specifications adequately?

Level 3

(RC-18) Subcontractor Supply Chain Security Risks

Definition: Risks that increase the likelihood a supplier will be unable to reliably deliver quality supplies (products) and/or services because of poor subcontractor quality standards and/or inadequate subcontractor supply chain security requirements.

(RF-1103) Supplier uses subcontractors that mis-represent meeting or adhering to quality standards

Definition: Risk that the company doesn't verify the claim by a subcontractor/supplier of having met quality standards and is maintaining that level of quality.

Possible Measures:
(RM-1442) Does supplier not assess subcontractors for adequacy of their standards and practices?
(RM-1443) Does supplier not assess subcontractors for evidence of conformance to their standards and practices?

(RF-1100) Supplier relies on an industry sector that has a history of inconsistent or poor quality subcomponents or services

Definition: This risk considers the likelihood that inconsistent/poor quality is endemic across the supplier's upstream supply chain and that the company may be exposed to security risks even if they strive to deliver high quality.

Possible Measures:

(RF-1101) Supplier's low margins on product/services sales affect quality of subcomponents they use

Definition: This risk considers that a supplier may compromise the security of their product or service when profit margins don't meet profitability targets by using lower quality subcomponents.

Possible Measures:

(RF-1102) Supplier uses subcontracted staff and their tenure is lower than industry or local standards

Definition: The consistent use of short-term subcontracted staff to provide services may indicate a culture of poor quality services particularly when service demand is higher. For example, firms that bring in subs to meet surge requirements may not be able to ensure quality standards are met because of a lack of incentives for quality, a lack of inspections/inspectors, etc.

Possible Measures:
(RM-1138) More than 75% of subcontracted staff lack appropriate certifications for their role?
(RM-1140) Less than 75% and more than 25% of subcontracted staff lack appropriate certifications for their role?
(RM-1141) Less than 25% and more than 0% of subcontracted staff lack appropriate certifications for their role?
(RM-1444) Does supplier lack short term personnel requirements for quality and competence consistent with tasks to be performed?
(RM-1445) Does supplier lack or fail to follow a process for collecting and evaluating evidence that short term personnel deliver the quality and competence required?

Level 3

(RC-19) Internal Quality Control Risks

Definition: Risks that increase the likelihood a supplier will be unable to reliably deliver quality supplies (products) and/or services because of poor quality control practices that result in products and services not meeting expected standards, specifications and/or requirements.

(RF-1107) Market cycles are so short that quality is commonly sacrificed.

Definition: The risk that particular components typically have low quality due to "time to market" factors and that this is widely tolerated by customers.

Possible Measures:

(RF-1109) Supplier consistently fails to resolve competing priorities in favor of supply (product) quality

Definition: The risk that a supplier does not consider quality to have value as high or higher than other factors. Supplier has demonstrated a preference to avoid addressing quality concerns and failures commonly by replacing defective products with existing stock or new version rather than providing service.

Possible Measures:

(RC-20) Supplier Quality Culture Risks in Table Form

(RF-1108) Supplier specifically aims at having the least expensive product in a market, focusing on public perception of cost rather than quality.

Definition: The risk that a supplier seeks to drive the use of quality-related standards out of a market so as to compete only on cost.

Possible Measures:

Level 3

(RC-632) Internal SCRM Policy and Practices Risks

Definition: Risks that increase the likelihood a supplier will be unable to reliably deliver quality supplies (products) and/or services because of poor internal SCRM policies and practices that result in products and services not meeting expected standards, specifications and/or requirements.

(RF-1110) Supplier lacks formal, documented policies and procedures for SCRM that results in poor or inconsistent quality.

Definition: Risks resulting from a lack of documented policies and procedures that define standards for supply chain risk elements such as integrity, quality, security, reliability, etc. Such guidance is needed to guide interactions and transactions with external parties and the components, materials, or services they provide or purchase. While a lack of such guidance might be expected in companies with very small numbers of staff, e.g., less than 10, even small businesses that have other formal, documented policies and procedures can be expected to be able to provide the same level of control and rigor to SCRM.

Possible Measures:
(RM-1446) Does supplier lack documented supply chain quality requirements?
(RM-1447) Does supplier lack a formal requirement to perform a risk assessment of their supply chain?
(RM-1448) Does supplier lack or fail to follow a formal work process to follow up on recommendations that result from a supply chain risk assessment?
(RM-1449) Does supplier lack or fail to follow an on-going audit program for the supply chain?

(RF-1111) Supplier's guidance to staff regarding SCRM policies and procedures may result in poor or inconsistent quality

Definition: Risks that the supplier does not have or cannot demonstrate an effective program of training and awareness of SCRM-related policies and procedures that can result in quality risks to both the supplier and to the supplier's customers.

Possible Measures:
(RM-1450) Does supplier lack training for employees in supply chain policies and procedures?

(RF-1113) Supplier's guidance in the form of policies, processes and procedures do not adequately address SCRM

Definition: Risks that the supplier's SCRM policies and procedures are inadequate, not enforced, arbitrary, or are not based on standards or norms applicable to the industry that the supplier serves.

Possible Measures:
(RM-1451) Does supplier lack or fail to follow a formal work process to follow up on recommendations that result from a supply chain risk assessment?
(RM-1452) Is there evidence that recommendations from supply chain risk assessment(s) have not been implemented?

(RC-105) Supplier Organizational Effectiveness 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 geographical, geopolitical, structural or operational characteristics of a supplier that affect its potential to operate in an efficacious and resilient manner.

(RF-247) Corporate Ownership has a poor reputation

Definition: This risk considers that negative public, social or media reputation of supplier ownership may negatively impact supplier's effectiveness.

Possible Measures:
(RM-518) Have there been >=3 open source and social media (OSSM) negative reports about the company leadership chain (President, CEO, COO, CFO, etc. and primary Board Members)?
(RM-519) Have there been >0 and <3 open source and social media (OSSM) negative reports about the company leadership chain (President, CEO, COO, CFO, etc. and primary Board Members)?

Level 3

(RC-538) Structural & Operational Instability

Definition: Risks that may affect a supplier's effectiveness due to changing structural or operational conditions internal to the company.

(RF-244) Supplier has frequently restructured through mergers & acquisitions

Definition: This risk considers that a supplier undergoing multiple mergers and acquisitions events within a given time frame can lead to issues (integration risk, overpayment, culture clash, etc.) that can negatively impact supplier's effectiveness.

Possible Measures:
(RM-509) Has the company undergone >10 mergers & acquisitions (M&As) within a 5-year time window?
(RM-510) Has the company undergone >=5 and <=10 mergers & acquisitions (M&As) within a 5-year time window?
(RM-511) Has the company undergone <5 mergers & acquisitions (M&As) within a 5-year time window?

(RF-245) Supplier has high operational volatility

Definition: This risk considers that high operational volatility (the likelihood that company operations are unstable and inconsistent over time) can negatively impact supplier's effectiveness.

Possible Measures:
(RM-512) Over the prior 5 years or less, is the normalized deviation of the turnover rate >=25%?
(RM-513) Over the prior 5 years or less, is the normalized deviation of the turnover rate >15%? and <25%?
(RM-514) Over the prior 5 years or less, is the normalized deviation of the turnover rate <15%?

Level 3

(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)?

(RF-238) Supplier facilities are located in areas prone to political instability

Definition: This risk considers whether political conditions in the locations where a company operates (such as government transparency, information rights, and civic participation) may negatively affect the ability of the supplier to operate effectively.

Possible Measures:
(RM-491) Is the World Justice Project (WJP) rating <= 0.45 for the country hosting the company?
(RM-492) Is the World Justice Project (WJP) rating >0.45 and <0.55 for the country hosting the company?
(RM-493) Is the World Justice Project (WJP) rating >= 0.55 for the country hosting the company?

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

(RF-240) Supplier facilities are located in areas prone to geopolitical instability

Definition: This risk considers that the physical location of key company facilities in areas prone to geopolitical instability and volatility can negatively impact a supplier's reliability, quality, and security.

Possible Measures:
(RM-497) Is the short-term political risk rating >=5 for the company's headquarters' country?
(RM-498) Is the short-term political risk rating 3 or 4 for the company's headquarters' country?
(RM-499) Is the short-term political risk rating <=2 for the company's headquarters' country?

(RF-243) Supplier facilities have a high geographic concentration

Definition: This risk considers that the larger the geographic spread of a company, the lesser the effects of an adverse event would be on the company and that the smaller and more concentrated the geographic footprint is, the greater the effects of an adverse event might be on the company.

Possible Measures:
(RM-506) Are the company HQ and branches in a single state (or similar sized region)?
(RM-507) Are the company HQ and branches in >1 and <=5 states (or similar sized regions)?
(RM-508) Are the company HQ and branches in >5 states (or similar sized regions)?

(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.

(RF-72) Company does not adhere to business compliance norms

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to a demonstrated history of not adhering to business compliance norms.

Possible Measures:
(RM-164) Does the company adhere and register to business compliance norms, e.g., ISO 9000?

(RF-209) Supplier sanction list status

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to its presence on any relevant governmental sanctions lists.

Possible Measures:
(RM-16) Is the company and/or key management personnel (KMP) listed on any sanctions list (if so, which ones and for what reason)?

(RF-208) Intellectual property litigation involving supplier

Definition: This risk considers how a supplier could negatively impact its customers, clients, partners or market due to a history of supplier involvement in intellectual property litigation.

Possible Measures:
(RM-445) Is the ratio of the number of litigated patents to the number of controlled patents greater than or equal to 10%, or is one of the litigating company's countries on the US Trade Representative (USTR) Priority Watch List (PWL)?
(RM-446) Is the ratio of the number of litigated patents to the number of controlled patents <10% and >5%?
(RM-447) Is the ratio of the number of litigated patents to the number of controlled patents <=5%?

Level 3

(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-1221) Has there been any information from open public sources indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?
(RM-1222) Has there been any information from commercial sources indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?
(RM-1223) Has there been any information from internal company sources indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?

(RC-7) Supplier Ethical Risks in Table Form

(RM-1224) Has there been any information from general confidence government sources indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?
(RM-1225) Has there been any information from high confidence government sources indicating company and/or key management personnel (KMP) cooperation with a foreign intelligence service?
(RM-1226) Has there been any information indicating company direct involvement in intelligence gathering for a foreign intelligence service?
(RM-1227) Has there been any information indicating company direct support to intelligence gathering for a foreign intelligence service?
(RM-1228) Has there been any information indicating company indirect support to intelligence gathering for 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:

(RC-7) Supplier Ethical Risks in Table Form

(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 4

(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-39) Supplier and/or key management personnel (KMP) have engaged in industrial espionage

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

Possible Measures:
(RM-15) Has there been a conviction, or solid evidence, of the company and/or key management personnel (KMP) for foreign or domestic industrial espionage?

(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 business-related 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-38) Supplier and/or key management personnel (KMP) have demonstrated malicious intent

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

Possible Measures:
(RM-19) Are there any convictions, or solid evidence, of the company and/or key management personnel (KMP) actions of malicious intent?

(RF-40) Supplier and/or key management personnel (KMP) have knowingly sold counterfeit parts or tainted parts (e.g., containing malware)

Definition: 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).

Possible Measures:
(RM-14) Is there information to indicate that either the company itself, or one or more key management personnel (KMP), has sold counterfeit, or tainted parts?

(RF-114) Software has malicious attributes hidden so as to be responsive to some triggering condition

Definition: 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.

Possible Measures:
(RM-1229) Does software have hidden triggerable malicious attributes/logic that could result in inappropriate exposure of data?
(RM-1230) Does software have hidden triggerable malicious attributes/logic that could result in inappropriate modification of data?
(RM-1231) Does software have hidden triggerable malicious attributes/logic that could result in inappropriate destruction of data?
(RM-1232) Does software have hidden triggerable malicious attributes/logic that could result in unauthorized remote access and control of the software?
(RM-1233) Does software have hidden triggerable malicious attributes/logic that could result in blocking of access to data or software logic?
(RM-1234) Does software have hidden triggerable malicious attributes/logic that could result in physical alteration, degradation or destruction at a limited and local operational scope?
(RM-1235) Does software have hidden triggerable malicious attributes/logic that could result in physical alteration, degradation or destruction at an extended organizational or broader tactical scope?
(RM-1236) Does software have hidden triggerable malicious attributes/logic that could result in physical alteration, degradation or destruction at an economy-wide, nation-wide or global strategic scope?
(RM-1453) Does supplier lack or fail to follow a work process in place to allow customers to specifically test and inspect software for malicious hidden attributes?

(RC-7) Supplier Ethical Risks in Table Form

(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) Are there >3 past criminal investigations conducted by the US or registered by the US department of justice or European equivalent?
(RM-451) Are there <4 and >1 past criminal investigations conducted by the US or registered by the US department of justice or European equivalent?

Level 5

(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 5

(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**

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.

Level 3

(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-230) Supplier is wholly or partially owned by a foreign entity

Definition: 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.

Possible Measures:
(RM-466) Is a minority percentage of company ownership held by foreign individuals and/or non-person entities?
(RM-467) Is a majority percentage of company ownership held by foreign individuals and/or non-person entities?
(RM-468) Is a plurality percentage of company ownership held by foreign individuals and/or non-person entities?
(RM-469) Is a minority percentage of company ownership held by individuals and/or non-person entities with affiliations to a country/ies of concern?
(RM-470) Is a majority percentage of company ownership held by individuals and/or non-person entities with affiliations to a country/ies of concern?
(RM-471) Is a plurality percentage of company ownership held by individuals and/or non-person entities with affiliations to a country/ies of concern?
(RM-486) Is <= 50% and >=5% of company ownership held by individuals and/or non-person entities from country/ies of concern?
(RM-487) Is <5% of company ownership held by individuals and/or non-person entities from country/ies of concern?

(RF-211) Degree of key stakeholder citizenship from country/ies of concern

Definition: The likelihood that company operations are subject to antagonistic national interest is indicated by the potential allegiance of key partners and stakeholders.

Possible Measures:
(RM-452) Does this company have key stakeholder nationality of >= 15% from country/ies of concern?
(RM-453) Does this company have key stakeholder nationality of <15% and >5% from country/ies of concern?
(RM-454) Does this company have key stakeholder nationality of >0 and <= 5% from country/ies of concern?

(RF-231) Supplier's KMP or owners cannot be identified

Definition: This risk considers whether a company's ownership and/or leadership can or cannot be clearly identified.

Possible Measures:

(RM-24) Does supplier have no identifiable KMP or owners?
(RM-36) Does supplier have limited KMP or owner information available?

(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) Are >=10 of the corporation leadership (CEO, staff, or Board of Directors) flagged as potential PEPs?
(RM-501) Are >=3 and <=9 of the corporation leadership (CEO, staff, or Board of Directors) flagged as potential PEPs?
(RM-502) Are <=2 of the 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?

(RC-6) Supplier External Influences in Table Form

(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?

(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?

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?

(RC-6) Supplier External Influences in Table Form

(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?

(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) Does >25% of company income come from foreign sources?
(RM-836) Does >50% of company income come from foreign sources?
(RM-837) Does >75% of company income come from foreign sources?
(RM-838) Does >25% of company income come from country/ies of concern?
(RM-839) Does >50% of company income come from country/ies of concern?
(RM-840) Does >75% of 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:

(RC-77) Supply Malicious Taint in Table Form

Supply Chain Risks		
(RC-1) Supplier Risks	**(RC-2) Supply Risks**	(RC-3) Service Risks
(RC-77) Supply Malicious Taint	(RC-9) Supply Counterfeit	(RC-8) Supply Hygiene Risks

Definition: Risks related to the integrity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms to cause harm.

Level 3

(RC-155) Supply Chain Management Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of integrity issues with supply chain management.

Level 4

(RC-159) ICT Hardware Supply Chain Integrity Risks

Definition: Risks that increase the likelihood an ICT hardware supply (product) may have been tampered with because of integrity issues with supply chain management.

(RF-99) Printed circuit board manufacturer receives and uses tainted chips from subsupplier

Definition: This risk considers whether a printed circuit board supply may be tainted due to tainted subcomponent chips provided to the PCB manufacturer by an upstream supplier, whether intentionally or inadvertently.

Possible Measures:
(RM-201) Is there evidence that a supplier of chips has ever provided tainted chips to printed circuit board manufacturer?
(RM-1454) Does supplier lack or fail to follow a quality assurance program suitable to their business?
(RM-1455) Does supplier lack effective circuit board testing capabilities to reveal tainted chips?
(RM-1456) Does subsupplier lack or fail to follow a quality assurance program suitable to their business?

(RF-16) Chip fabrication receives and uses tainted IP core components from subsupplier

Definition: This risk considers whether a chip supply may be tainted due to tainted subcomponent IP core or IP block components provided to the foundry by an upstream supplier, whether intentionally or inadvertently. The supplier does not recognize the tainted supplies and uses them in production.

Possible Measures:
(RM-91) Is there evidence that supplier of IP cores (IP blocks) has ever provided tainted IP cores (IP blocks) to chip manufacturers?
(RM-1457) Does supplier lack effective circuit board testing capabilities to reveal tainted IP core components?

Level 4

(RC-162) Software Supply Chain Integrity Risks

Definition: Risks that increase the likelihood a software supply (product) may have been tampered with because of integrity issues with supply chain management.

(RF-1093) Manufacturer outsources the functions associated with the external supply chain management for input to the manufacturing process

Definition: Risk that the manufacturer no longer controls the quality of the inputs to manufacturing. If the manufacturer limits their span of control to the product production and outsources the identification and procurement of raw materials, including delivery, then the manufacturer may be more exposed to tampering of those raw materials, including those advanced/sophisticated "raw material" components needed for the particular manufacturer of interest such as in a multi-step, multi-vendor, product.

Possible Measures:
(RM-1335) Does the company outsource the quality management function for input materials to the manufacturing process?
(RM-1458) Does supplier lack or fail to follow an independent audit program for any functions associated with the external supply chain management for input to the manufacturing process?

(RF-1094) Manufacturer outsources the functions associated with distribution or movement between manufacturing sites.

Definition: Risk that the manufacturer no longer controls the care and handling of the ouputs from manufacturing. The manufacturer still retains ownership and control of the manufacturing process.

Possible Measures:
(RM-1336) Does the company outsource processes or services for transportation of intermediate goods between manufacturing sites?
(RM-1459) Does supplier lack or fail to follow an independent audit program for any functions associated with distribution or movement between manufacturing sites?

Level 3

(RC-149) Manufacturing Process Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of inadequate manufacturing or development process integrity controls.

(RC-77) Supply Malicious Taint in Table Form

(RF-1050) Manufacturing of the supply depends on subcomponents sourced from a country of concern

Definition: This risk is specific to the production of subcomponents that could be either very unique, critical to the product or are fungible with subcomponents that could be sourced from various locations. When those subcomponents are sourced from a country of concern, even if the component isn't logic bearing, the subcomponent could pose unknowable risks and render the final product untrustworthy.

Possible Measures:

(RF-1051) Production quality control is inadequate to ensure product integrity

Definition: Concerns about the efficacy of quality control in the production environment including the establishment of a formal, documented QC process and the adherence to that process.

Possible Measures:
(RM-1103) Does the company not have a documented quality control process that is reviewed with and trained to all employees, regardless of function?
(RM-1104) Does the company not employ in-process quality checks to ensure quality of work in process material?
(RM-1105) Does the company not employ end-of-line testing and quality audits to ensure quality of finished good material?
(RM-1106) Does the company not track Key Performance Indicators (KPIs) through the use of Statistical Process Control (SPC)?
(RM-1107) Does the company not have a Manufacturing Execution System (MES)?
(RM-1108) Does the company not leverage a Manufacturing Operations Management (MOM) system?
(RM-1109) Does the company not enforce the use of Poka-Yoke safeguards throughout the production process?
(RM-1110) Does the company not track the number of defects per million?
(RM-1111) Does the company not track scrap?
(RM-1460) Does supplier have significant nonconformance findings from an ISA 62443-4-1 assessment?
(RM-1461) Does supplier have minor (not significant) nonconformance findings from an ISA 62443-4-1 assessment?
(RM-1462) Are there any outstanding recommendations from an ISA 62443-4-1 assessment that have not been formally closed out?
(RM-1463) Does supplier lack an audit program to ensure conformance to ISA 62443-4-1 is sustained?

(RF-1052) Production integrity is questionable because of a lack of intermediate quality checks

Definition: This is a risk that intermediate stages of production may be flawed and such a flaw is not or cannot be discovered leading to integrity concerns of an unknown quantity of the final product.

Possible Measures:

Level 4

(RC-28) ICT Hardware Manufacturing Process Integrity Risks

Definition: Risks that increase the likelihood that ICT hardware which includes electrical, electromechanical, and electronic components may have been tampered with because of inadequate manufacturing or development process integrity controls.

(RF-87) Printed circuit board fabrication/assembly process is not secure

Definition: Risk that one or more processes are insecure. This could be exploitable vulnerabilities in the tools used for fabrication/assembly or in the actual fabrication/assembly process. Such vulnerabilities can allow malicious insertion or control of a process.

Possible Measures:
(RM-130) Is use of printed circuit board fabrication/assembly equipment restricted to authorized personnel?
(RM-187) Is access to printed circuit board manufacturer fabrication/assembly areas restricted to authorized personnel?
(RM-1464) Does supplier have significant nonconformance findings from an ISA 62443-4-1 assessment relevant to printed circuit board fabrication/assembly?
(RM-1465) Does supplier have minor (not significant) nonconformance findings from an ISA 62443-4-1 assessment relevant to printed circuit board fabrication/assembly?
(RM-1466) Are there any outstanding recommendations relevant to printed circuit board fabrication/assembly from an ISA 62443-4-1 assessment that have not been formally closed out?
(RM-1467) Does supplier lack audits that confirm printed circuit board fabrication/assembly policies, processes and procedures are being followed?

(RF-1057) Chips are manufactured or assembled by equipment sourced from a non-trusted supplier

Definition: This risk considers the ability for malicious actors to disrupt, tamper with, or surveil the wafer manufacture and assembly process for semiconductor supplies via the equipment used.

Possible Measures:
(RM-1268) Is equipment used in manufacture or assembly of chips (supply) sourced from non-trusted domestic supplier?
(RM-1269) Is equipment used in manufacture or assembly of chips (supply) sourced from non-trusted foreign supplier?
(RM-1270) Is equipment used in manufacture or assembly of chips (supply) sourced from non-trusted supplier owned/controlled by country/ies of concern?
(RM-1468) Does non-trusted supplier have significant nonconformance findings from an ISA 62443-4-1 assessment relevant to chip manufacture or assembly?
(RM-1469) Does non-trusted supplier have minor (not significant) nonconformance findings from an ISA 62443-4-1 assessment relevant to chip manufacture or assembly?

(RC-77) Supply Malicious Taint in Table Form

(RM-1470) Are there any outstanding recommendations relevant to chip manufacture or assembly from an ISA 62443-4-1 assessment of non-trusted supplier that have not been formally closed out?
(RM-1471) Does supplier lack an audit program to ensure non-trusted supplier conformance to ISA 62443-4-1 is sustained?

(RF-96) Chips may be tainted or maliciously tampered with

Definition: This risk considers the ability for malicious actors to taint a semiconductor supply during the manufacturing process or intercept and tamper with the supply between production and delivery, such that it does not perform required functionality or performs unwanted functionality

Possible Measures:

(RF-1059) Quantitative testing shows chips do not match design or intended functionality

Definition: Risks that a post fabrication test process indicates a discrepancy in design and/or functionality between tested samples and the approved baseline. Such a discrepancy, if not immediately recognized as a quality escape, may be an indication of malicious insertion or alteration.

Possible Measures:
(RM-72) Is there evidence from quantitative testing to show that a fabricated integrated circuit (e.g., ASIC or FPGA chip) accurately implements its electrical design?
(RM-73) Is there evidence from quantitative testing to show that a fabricated integrated circuit (e.g., ASIC or FPGA chip) accurately implements its functional design?
(RM-74) Is there evidence from quantitative testing to show that a packaged integrated circuit (e.g., ASIC or FPGA chip) implements or provides only its intended functionality?
(RM-75) Is there evidence from quantitative testing to show that an integrated circuit (e.g., ASIC or FPGA chip), once integrated into a printed circuit board, retains its intended functionality?
(RM-76) Is there evidence from quantitative testing to show that an integrated circuit (e.g., ASIC or FPGA chip), once integrated into a printed circuit board, does not acquire additional capabilities?

(RF-14) Chip fabrication process is not secure

Definition: This risk considers the exposure of elements in the fabrication or quality control process to be subverted by malicious actors during wafer manufacture and assembly with the result being tainted semiconductor supplies

Possible Measures:
(RM-70) Is access to chip fabrication areas in foundry restricted to authorized personnel?
(RM-71) Is use of foundry fabrication equipment restricted to authorized personnel?

(RF-1058) Chip manufacturing process is staffed with subcontractors that are not accountable to the manufacturer

Definition: Risks that a manufacturer subcontracts labor and may not have the same level of background checking and accountability to the manufacturer that may be common for the regular employee of the manufacturer and that this increases the risk that a staff member with malicious intent is able to gain access to the manufacturing process.

Possible Measures:

(RF-1060) Quantitative testing shows chips in produced boards do not match design or intended functionality

Definition: Risks that a post fabrication/assembly test process indicates a discrepancy in design and/or functionality between tested samples and the approved baseline. Such a discrepancy, if not immediately recognized as a quality escape, may be an indication of malicious insertion or alteration.

Possible Measures:
(RM-197) Is there evidence from quantitative testing to show that chips incorporated into printed circuit board cannot engage in malicious acts against other chips on the same board?
(RM-198) Is there evidence from quantitative testing to show that fabricated/assembled printed circuit board accurately implements its electrical design?
(RM-199) Is there evidence from quantitative testing to show that fabricated/assembled printed circuit board accurately implements its functional design?
(RM-200) Is there evidence from quantitative testing to show that fabricated/assembled printed circuit board implements or provides only its intended functionality?

Level 3

(RC-154) Geopolitical Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of geopolitical conditions that negatively affect the pedigree or provenance of the supply (product).

(RF-1087) Supply (product) is identifiable as being associated with a geopolitical circumstance

Definition: Risk that the product could be maliciously harmed. This could include being targeted for having text or images on packaging that makes it conspicuous for association with a geopolitically significant event, movement, person, or belief. This could be as simple as "made in USA" or "made in China" or as nuanced as a particular packaging color since colors may be associated with such circumstances.

(RC-77) Supply Malicious Taint in Table Form

Possible Measures:

(RF-27) Supply (product) is manufactured in a country of concern

Definition: Risk that the manufacturing process is untrustworthy due to where it is manufactured. This risk applies to the substantive components which may include any or all phases of the manufacturing process. When products are assemblies of components with differing sources and pedigrees, this risk may still renders the product untrustworthy.

Possible Measures:
(RM-114) Is the country where manufacturing takes place a country of concern?
(RM-1472) Does supply lack quality assurance testing by parties other than those in the country of concern?
(RM-1473) Does supply lack evaluation and testing for backdoors?
(RM-1474) Does software supply lack evaluation and testing for potentially malicious code?

(RF-1088) Supply (product) is identifiable as being associated with an environmental issue

Definition: Risk that the product could be maliciously harmed. This could include being targeted due to an association with global climate change, environmental waste impacts, use of "blood" minerals, etc.

Possible Measures:

Level 3

(RC-153) Functional Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because it does not perform desired functions or performs functions not desired.

(RF-1077) Is the product known or suspected to have properties that if tampered with, expose some feature that is not intended.

Definition: Risk that illicit tampering with a product may go beyond the intent of the tampering and expose vulnerabilities that are either outside the scope of the intended operational parameters or in some cases, could not be foreseen.

Possible Measures:

(RF-1078) Is the product known or suspected to have properties that when tampered with to override some safety or quality control, make it desirable for some unintended purpose?

Definition: Risk that unintended functionality can be exposed when bypassing a security or safety control. For example, safety seals or limiting controls that prevent the user from exceeding approved limitations. This might include capabilities that are turned 'off" in settings or via some physical barrier, which preclude the user from enabling an unapproved or unsafe capability. Just that fact that such controls exist mean that there is a risk of tampering of those controls and render the product less safe or of lower quality.

Possible Measures:

Level 4

(RC-167) Maliciously altered functionality

Definition: Risks that the processes used to produce, assemble, compose, compile, and test products may be manipulated to maliciously alter the function of produced supplies.

(RF-1084) Manufacturer/developer has a rigorous integrity verification process but the process is not executed with a frequency appropriate to the criticality of the end use of the product

Definition: This risk considers the impact of parts that are not adequately tested or examined to verify integrity before being sold which could allow a malicious actor cause harm to customers knowing that the verification process is unlikely to catch defects or intentional corruption of the manufacturing process. This also considers the risk of having adequate processes and procedures but not following them as intended.

Possible Measures:
(RM-1112) Does the company not leverage per-piece audits for in-process and finished good materials?

(RF-1082) Risk that supply (product) integrity is vulnerable to corrupted or compromised production process.

Definition: This risk considers that a product's dependency during production on a tool or manufacturing process that could be corrupted to insert malicious functionality without the knowledge or complicity of the manufacturer/developer. This risk relates to both the accessibility of elements in the production environment to malicious insertion/control that could lead to compromise of the product as well as the awareness by the manufacturer/developer of the need to verify the integrity/trustworthiness of the production environment. This describes a key step in the SolarWinds exploit.

Possible Measures:
(RM-1475) Does supplier have significant nonconformance findings from an ISA 62443-4-1 assessment relevant to production process integrity?

(RC-77) Supply Malicious Taint in Table Form

(RM-1476) Does supplier have minor (not significant) nonconformance findings from an ISA 62443-4-1 assessment relevant to production process integrity? (RM-1477) Are there any outstanding recommendations relevant to production process integrity from an ISA 62443-4-1 assessment that have not been formally closed out? (RM-1478) Does supplier lack audits to ensure compliance with procedures? (RM-1479) Does software supply lack quality assurance testing of supply throughout the production process?
(RF-1083) Supplier lacks a rigorous integrity verification process for all elements of the production environment Definition: This risk is specific to the integrity verification process for production elements such as robotic assemblers, compliers, etc., that could allow malicious insertion or alterations while masking them so as to avoid detection. Manufacturer/developer may lack a rigorous integrity verification process for all elements of the production environment with the capability to maliciously insert functionality or alter the product functionality undetectably. This describes a key step in the SolarWinds exploit. Possible Measures: (RM-1334) Has there been information indicating any element of the production environment is susceptible to insertion or alteration without detection? (RM-1480) Does supplier have significant nonconformance findings from an ISA 62443-4-1 assessment relevant to production environment integrity? (RM-1481) Does supplier have minor (not significant) nonconformance findings from an ISA 62443-4-1 assessmentrelevant to production environment integrity? (RM-1482) Are there any outstanding recommendations relevant to production environment integrity from an ISA 62443-4-1 assessment that have not been formally closed out? (RM-1483) Does supplier lack audits to ensure compliance with procedures? (RM-1484) Does software supply lack quality assurance testing of the production environment?

(RC-77) Supply Malicious Taint in Table Form

Level 4

(RC-165) Software Functional Integrity Risks

Definition: Risks that increase the likelihood a software supply (product) may have been tampered with because it does not perform desired functions or performs functions not desired.

(RF-112) Software has attributes intentionally hidden by the developer and in violation of approved procedures so as to be undetectable that can be maliciously exploited

Definition: This risk considers whether software contains unpublished functions, unused attributes, "dead" code, developer backdoors, "easter eggs," etc., which may indicate an attempt at deliberate malicious taint. It can be considered malicious by the fact that such attributes are commonly prohibited by policies due to the potential financial and reputational liability. It may still be a practice among coders to violate such guidance for various reasons without intending harm for example as a time-saving measure, but the knowledge that such practices exist in a particular coder community could allow threat actors to have privileged knowledge that these hidden functions exist. This could lead to covert exploitation.

Possible Measures:

(RF-113) Software supply (product) includes components that were known to have exploitable vulnerabilities at the time it was in development

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to leveraging of third party software supply (product) components that were known to have exploitable vulnerabilities at the time it was in development.

Possible Measures:
(RM-1337) Is there information to indicate that the supply (product) contains components known to have exploitable vulnerabilities at the time of development?
(RM-1485) Do utilized versions of any software supply components have published vulnerabilities in MITRE CVE?

(RF-114) Software has malicious attributes hidden so as to be responsive to some triggering condition

Definition: 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.

Possible Measures:

Level 3

(RC-151) Logistics/Transportation Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of inadequate integrity controls around the movement and transportation of the supply (product).

(RF-1067) Chain of custody procedures for products in transit are not aligned with industry norms and standards

Definition: Risk that implemented chain of custody procedures/instructions are not aligned with industry norms and standards.

Possible Measures:

(RF-1071) Shipment risk statements are misused, miscommunicated, or misleading

Definition: This risk considers whether a supplier may exploit freight-on-board (FOB) or cost-insurance-freight (CIF) caveats to transfer in-transit shipment risks to downstream entities.

Possible Measures:

(RF-1069) Chain of custody procedures are unknown, unenforced or unaudited by logistics staff.

Definition: Risks that the logistics organization(s) don't inform staff about chain of custody procedures or implement enforcement and auditing of them.

Possible Measures:
(RM-1114) Does the company not leverage a Transportation Management Systems (TMS)?

(RF-1070) Products requiring greater security during movements and temporary storage are not handled appropriately.

Definition: Risk that products may be exposed to threats while not in the custody of the owner during movement/transit. For example, being mistakenly comingled with products that have lower security requirements or being warehoused in unbonded storage.

Possible Measures:

Level 3

(RC-152) Poor Reputation for Integrity

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of poor reputation for supply (product) integrity.

(RC-77) Supply Malicious Taint in Table Form

(RF-64) Supplier has history of malicious tampering with its supplies

Definition: Risk that the supplier continues to have inadequate controls to prevent malicious tampering following one or more episodes of such problems. When a supplier does not take impactful measures to prevent malicious tampering, allowing it to happen again, this indicates the supplier is not managing risk properly.

Possible Measures:

(RF-1073) Related supplies have been maliciously tainted

Definition: This risk considers whether a similar supply from another supplier, or related supply from the same supplier, have been known to be tainted in the past, thus increasing the risk the supply at hand will be maliciously tainted.

Possible Measures:
(RM-1271) Has there been any information indicating that a previous version of the supply (product) has been known to be maliciously tainted?
(RM-1272) Has there been any information indicating that a related supply (product) from the same supplier has been known to be maliciously tainted in the past?

Level 4

(RC-175) ICT Hardware Reputational Integrity Risks

Definition: Risks that increase the likelihood an ICT hardware product such as an electrical, electromechanical, or electronic component may have been tampered with because of poor reputation for supply (product) integrity.

(RF-15) Foundry is not a participant in a recognized trusted foundry or trusted supplier program

Definition: This risk considers whether a semiconductor supply was fabricated by a foundry that does not hold a third-party certification of trust, such as the US DoD's Trusted Foundry program or other US Govt. approved trusted supplier program.

Possible Measures:
(RM-90) Has the foundry producing integrated circuits (e.g., ASIC or FPGA chips) been accredited by the Defense Microelectronics Activity (DMEA) for membership in DoD’s Trusted Foundry/Trusted Supplier Program?
(RM-1486) Does supplier lack any independent and competent 3rd party attestation to the veracity of their manufacturing and supply security capabilities?

(RF-1076) Foundry cannot demonstrate or verify conformance to international quality standards

Definition: This risk considers the willingness of the foundry to seek, maintain, and adhere to internationally approved quality standards that are relevant to competitors.

Possible Measures:

Level 3

(RC-150) Facilities Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of inadequate facility physical security measures.

(RF-1065) Production environment cannot physically isolate or provide separate zones for products with different levels of security needs

Definition: Risk that security facets such as criticality, susceptibility to tampering, exposure to weather, etc. are not taken into account while products are moving through production.

Possible Measures:
(RM-1487) Does supplier have significant risk findings relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-3-2 risk assessment?
(RM-1488) Does supplier have minor (not significant) risk findings relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-3-2 risk assessment?
(RM-1489) Are there any outstanding recommendations relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-3-2 risk assessment?
(RM-1490) Does supplier have significant findings relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment?
(RM-1491) Does supplier have minor (not significant) risk findings relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment?
(RM-1492) Are there any outstanding recommendations relevant to physical isolation or separation of security level zones of the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment?

(RC-77) Supply Malicious Taint in Table Form

(RF-1064) Production environment has inadequate physical and cyber security processes to ensure product integrity Definition: Risk that the environment where production takes place are exposed to threats, either physical or cyber, and that the uncertainty associated with such risk may call the product integrity into question. Possible Measures: (RM-1493) Does supplier have significant risk findings relevant to physical and cyber security processes for the production environment from an ISA 62443-3-2 risk assessment? (RM-1494) Does supplier have minor (not significant) risk findings relevant to physical and cyber security processes for the production environment from an ISA 62443-3-2 risk assessment? (RM-1495) Are there any outstanding recommendations relevant to physical and cyber security processes for the production environment from an ISA 62443-3-2 risk assessment? (RM-1496) Does supplier have significant findings relevant to physical and cyber security processes for the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment? (RM-1497) Does supplier have minor (not significant) risk findings relevant to physical and cyber security processes for the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment? (RM-1498) Are there any outstanding recommendations relevant to physical and cyber security processes for the production environment from an ISA 62443-2-1 and ISA 62443-3-3 assessment?
(RF-24) Manufacturing facility is not secure Definition: This risk considers the ability for malicious actors to disrupt, tamper with, or surveil the manufacturing facility. Possible Measures: (RM-79) Is there controlled access for personnel (positive identification) to manufacturing facilities? (RM-1499) Does supplier have significant risk findings relevant to manufacturing facility security from an ISA 62443-3-2 risk assessment? (RM-1500) Does supplier have minor (not significant) risk findings relevant to manufacturing facility security from an ISA 62443-3-2 risk assessment? (RM-1501) Are there any outstanding recommendations relevant to manufacturing facility security from an ISA 62443-3-2 risk assessment? (RM-1502) Does supplier have significant findings relevant to manufacturing facility security from an ISA 62443-2-1 and ISA 62443-3-3 assessment? (RM-1503) Does supplier have minor (not significant) risk findings relevant to manufacturing facility security from an ISA 62443-2-1 and ISA 62443-3-3 assessment? (RM-1504) Are there any outstanding recommendations relevant to manufacturing facility security from an ISA 62443-2-1 and ISA 62443-3-3 assessment?

(RC-77) Supply Malicious Taint in Table Form

Level 3

(RC-54) Packaging Integrity Risks

Definition: Risks that increase the likelihood a supply (product) lacks authenticity or integrity because of inadequate tamper protection or evidence of tampering with the packaging of the supply (product).

(RF-1000) Supplier doesn't offer a support capability for customers with product integrity/tampering concerns

Definition: This risk concerns the ability of a customer to easily find and access a resource to distinguish, investigate, and resolve potential tampering incidents.

Possible Measures:

(RF-77) Box packaging does not have anti-tamper measures

Definition: This risk considers the increased likelihood that a supply has been tampered with or touched by malicious actors if the box does not have anti-tamper measures, such as shrink wrapping

Possible Measures:
(RM-167) Does the contract not call for shrink wrapping or other protective measures?
(RM-1116) Does the company not require the use of tamper-evident packaging for all of its products?
(RM-1119) Does the company not require the use of tamper-evident packaging by sub-suppliers?
(RM-1122) Does the company not perform inspections upon receipt of sub-supplier material and packaging?
(RM-1124) Does the company not inspect sub-supplier packaging against pre-defined specifications on a per component and per container basis?

(RF-992) Supplier doesn't use tamper resistant/proofing technologies on their products effectively

Definition: This risk concerns the customer's perspective that a supplier's tamper resistant/proofing is missing, inconsistent, easily replicated, etc.

Possible Measures:

(RF-84) Pallets do not have anti-tamper measures

Definition: This risk considers the increased likelihood that a supply has been tampered with or touched by malicious actors if the pallet does not have anti-tamper measures, such as shrink wrapping.

Possible Measures:
(RM-167) Does the contract not call for shrink wrapping or other protective measures?
(RM-1116) Does the company not require the use of tamper-evident packaging for all of its products?
(RM-1119) Does the company not require the use of tamper-evident packaging by sub-suppliers?
(RM-1122) Does the company not perform inspections upon receipt of sub-supplier material and packaging?
(RM-1124) Does the company not inspect sub-supplier packaging against pre-defined specifications on a per component and per container basis?

(RF-1002) Supplier's products are not clearly distinguishable in some way

Definition: This risk concerns the company's ability to distinguish brand and authenticity with a visual attribute including those of subcomponents.

Possible Measures:

(RF-1001) Materials used to protect the die or the components of a semiconductor lack functional integrity

Definition: This is intended to cover a wide range of packaging risks from the compounds used, the process to apply the packaging material, the bonding to connectors, etc.

Possible Measures:

(RF-1004) Packaging of mechanical supplies for shipment is not as expected

Definition: This risk considers whether the external packaging in which mechanical supplies were received, such as pallets and shipping containers, match the packaging typically used by the OEM.

Possible Measures:

(RC-77) Supply Malicious Taint in Table Form

(RF-1003) Packaging of electrical supplies for shipment is not as expected

Definition: This risk considers whether the external packaging in which electrical supplies were received, such as pallets and shipping containers, match the packaging typically used by the OEM.

Possible Measures:

(RF-1005) Internal packaging of electrical supplies is not as expected

Definition: This risk considers whether the internal packaging of electrical supplies, such as boxes, trays, tubes, or reels, match the packaging typically used by the OEM, and if the supplies were packaged correctly.

Possible Measures:

(RF-85) Shipping container does not have anti-tamper measures

Definition: This risk considers the increased likelihood that a supply has been tampered with or touched by malicious actors if the shipping container does not have anti-tamper measures, such as seals.

Possible Measures:
(RM-167) Does the contract not call for shrink wrapping or other protective measures?
(RM-1116) Does the company not require the use of tamper-evident packaging for all of its products?
(RM-1119) Does the company not require the use of tamper-evident packaging by sub-suppliers?
(RM-1122) Does the company not perform inspections upon receipt of sub-supplier material and packaging?
(RM-1124) Does the company not inspect sub-supplier packaging against pre-defined specifications on a per component and per container basis?

Level 3

(RC-156) Maintenance Integrity Risks

Definition: Risks that increase the likelihood a supply (product) may have been tampered with because of maintenance issues, including the update of software.

(RF-1098) The maintenance process requires elevated privileges such as "super user" or exposure of tamper-protected elements of the product.

Definition: The risk that firms which significantly undercut standard maintenance costs be subsidized by entities seeking to tamper the product or who pose other risks to product trustworthiness.

Possible Measures:

(RF-1097) The existence of firms that claim to provide maintenance/support, but which charge less than manufacturer-provided or manufacturer-approved options.

Definition: The risk that firms which significantly undercut standard maintenance costs be subsidized by entities seeking to tamper the product or who pose other risks to product trustworthiness.

Possible Measures:

(RF-1095) The vendor/manufacturer retains control of the maintenance process and the provisioning of that maintenance.

Definition: This is the risk of over-trusting the manufacturer who may have motives that are not in the best interests of the owner. For example, the owner's trust can be exploited to sell new features or capabilities having dubious or limited value. or recommending replacement when a repair would be more prudent.

Possible Measures:

(RF-1096) The product requires specialized support, e.g., specialized training or qualification.

Definition: Risks associated with having to rely on the maintenance provider having the knowledge, skills, and qualifications needed to perform the maintenance function.

Possible Measures:

(RC-9) Supply Counterfeit in Table Form

Supply Chain Risks		
(RC-1) Supplier Risks	**(RC-2) Supply Risks**	(RC-3) Service Risks
(RC-77) Supply Malicious Taint	**(RC-9) Supply Counterfeit**	(RC-8) Supply Hygiene Risks

Definition: Risks related to the authenticity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms.

Level 3

(RC-127) Unsanctioned Manufacturing

Definition: Risks that increase the likelihood a supply (product) is not authentic because of manufacturing by authorized entities outside of their authorized scope.

(RF-1045) Supplier lacks effective oversight and auditing of manufacturing materials to detect and prevent unsanctioned manufacturing

Definition: This risk considers the likelihood of unsanctioned manufacturing if the supplier lacks effective oversight and auditing of manufacturing materials to detect and prevent unsanctioned manufacturing.

Possible Measures:

(RF-1043) Supplier operates the manufacturing line at a tempo in excess of what is authorized

Definition: This risk considers the likelihood of unsanctioned manufacturing if the supplier operates the manufacturing line at a tempo in excess of what is authorized. This could lead to quality control and product accountability errors.

Possible Measures:
(RM-1127) Does the company not have a Manufacturing Execution System (MES) that can enforce authorized line tempo?
(RM-1128) Does the company not leverage a Manufacturing Operations Management (MOM) system that can manage and audit authorized line tempo?
(RM-1129) Is the company's manufacturing line not controlled via Programmable Logic Controllers (PLCs)?

(RF-1044) Supplier lacks effective security and oversight of manufacturing line to detect and prevent unsanctioned manufacturing

Definition: This risk considers the likelihood of unsanctioned manufacturing if the supplier lacks effective security and oversight of manufacturing line to detect and prevent unsanctioned manufacturing.

Possible Measures:

(RF-1041) Supplier's production line is not fully utilized even though raw materials are available

Definition: Risk that the idle production line may allow for unauthorized production. If the supplies (raw materials) needed for component production are available but the workforce and production systems are not being utilized, the risk that unauthorized manufacturing will occur increases.

Possible Measures:

(RF-1040) Supplier's manufacturing line is not 24/7

Definition: Risk that a production line that is not in continuous operation offers the opportunity for unauthorized production. It would be almost impossible to produce supplies that are "off-the-books" or unauthorized if manufacturing systems and are in use or at least monitored around the clock.

Possible Measures:

(RF-1042) Supplier operates an extra unauthorized shift on the manufacturing line

Definition: This risk considers the likelihood of the manufacturing of perfect but unsanctioned products if the supplier tolerates an unauthorized shift on the manufacturing line.

Possible Measures:

Level 3

(RC-126) Mislabeling

Definition: Risks that increase the likelihood a supply (product) is not authentic because the printed markings identifying the supply (product) are not as expected.

(RF-1035) Nameplate indicators of mechanical supplies are not as expected

Definition: This risk considers whether nameplates on mechanical parts appear to be genuine, or if they show signs of alteration or application by a malicious actor.

(RC-9) Supply Counterfeit in Table Form

Possible Measures:
(RM-1510) Does supplier lack or fail to follow procedures to conduct investigation of nameplates showing signs of alteration or application by a malicious actor?

(RF-1034) Supplier has a history of inconsistency in label design, placement, texture, etc.

Definition: Risk that inconsistency in labeling makes it more difficult to identify authentic products. Companies with multiple divisions or in the merger and acquisition process, may fail to have consistent printed labeling leading to uncertainty as to authenticity.

Possible Measures:
(RM-1511) Does management of change work process not include changes to labeling?
(RM-1512) Does supplier lack documentation of label changes?
(RM-1513) Does supplier lack an assessment of actual changes to confirm conformance to documented change process?

(RC-131) ICT Hardware Mislabeling

Definition: Risks that increase the likelihood an ICT hardware supply (product) is not authentic because the printed markings identifying the supply (product) are not as expected.

(RF-1036) Electrical supplies are not marked as expected

Definition: This risk considers whether markings on electrical supplies, such as date codes, lot numbers, or logos, match those typically used by the OEM.

Possible Measures:
(RM-1514) Does supplier lack or fail to follow procedures to conduct an investigation in the event electrical supplies are found not marked as expected?

(RF-1037) Markings on electrical supply are not permanent

Definition: This risk considers whether markings on electrical supplies, such as date codes, lot numbers, or logos, were applied in the permanent manner typical of a genuine part.

Possible Measures:
(RM-1515) Does supplier lack or fail to follow procedures to conduct an investigation in the event markings on electrical supply are not permanent?

Level 5

(RC-139) ICT Hardware Board Mislabeling

Definition: Risks that increase the likelihood an ICT hardware board supply (product) is not authentic because the printed markings identifying the supply (product) are not as expected.

(RF-261) Printed markings on board do not match printed markings on known genuine sample of board

Definition: This risk considers whether printed markings on an ICT hardware board supply, such as date codes, lot numbers, or logos, appear as expected in comparison to known genuine samples of the ICT hardware board supply.

Possible Measures:
(RM-560) Are manufacturer's markings on the board permanent and clean with no indications of remarking?
(RM-561) Are there laser burn marks visible on the board that could have been made during a remarking process?
(RM-562) Are there signs of original, faded or obscured manufacturer part markings behind newer appearing markings the board?
(RM-563) Do printed markings on board differ from markings on a known genuine sample of board by having incorrect country of origin?
(RM-564) Do printed markings on board differ from markings on a known genuine sample of board by having incorrect font and size for letters?
(RM-565) Do printed markings on board differ from markings on a known genuine sample of board by having incorrect font and size for numbers?
(RM-566) Do printed markings on board differ from markings on a known genuine sample of board by having incorrect logo?
(RM-567) Do printed markings on board differ from markings on a known genuine sample of board by having incorrect part number?
(RM-568) Do printed markings on board differ from markings on a known genuine sample of board by having misspelled words?
(RM-1516) Does supplier lack or fail to follow procedures to conduct an investigation in the event printed markings on board do not match printed markings on known genuine sample of board?

Level 5

(RC-140) ICT Hardware Chip Mislabeling

Definition: Risks that increase the likelihood an ICT hardware chip supply (product) is not authentic because the printed markings identifying the supply (product) are not as expected.

(RF-89) Printed markings on chip package do not match printed markings on known genuine sample of chip

Definition: This risk considers whether printed markings on an ICT hardware chip supply, such as date codes, lot numbers, or logos, appear as expected in comparison to known genuine samples of the ICT hardware chip supply.

Possible Measures:
(RM-102) Do printed markings on chip differ from markings on a known genuine sample of chip by having incorrect font and size for letters?
(RM-103) Do printed markings on chip differ from markings on a known genuine sample of chip by having incorrect font and size for numbers?

(RC-9) Supply Counterfeit in Table Form

(RM-104) Do printed markings on chip differ from markings on a known genuine sample of chip by having misspelled words?
(RM-105) Do printed markings on chip differ from markings on a known genuine sample of chip by having incorrect part number?
(RM-106) Do printed markings on chip differ from markings on a known genuine sample of chip by having incorrect logo?
(RM-107) Do printed markings on chip differ from markings on a known genuine sample of chip by having incorrect country of origin?
(RM-124) Are manufacturer's markings on the chip's package permanent and clean with no indications of remarking?
(RM-128) Are there laser burn marks visible on the chip's package that could have been made during a remarking process?
(RM-129) Are there signs of original, faded or obscured manufacturer part markings behind newer appearing markings the chip's package?
(RM-1517) Does supplier lack or fail to follow procedures to conduct an investigation in the event printed markings on chip package do not match printed markings on known genuine sample of chip?

Level 3

(RC-118) Technical Authenticity Risks

Definition: Risks that increase the likelihood a supply (product) is not authentic because of other-than-expected technical characteristics.

Level 4

(RC-604) Non-ICT Hardware Authenticity Risks

Definition: Risks that relate to authenticity of mechanical parts, to include large products such as pressure vessels or engine blocks, subcomponents such as valves or fittings, and piece parts such as bolts.

(RF-1008) Valves indicate poor manufacture of mechanical supply

Definition: This risk considers whether valves in mechanical supplies contain flaws or inconsistencies that may indicate the part is not genuine or not to specifications

Possible Measures:
(RM-1518) Does supplier lack or fail to follow a quality assurance process to inspect valves for flaws or inconsistencies versus specification?
(RM-1519) Does supplier lack or fail to follow procedures to correct any valves with flaws or inconsistencies versus specification?

(RF-1007) Mechanical supplies indicate poor manufacture quality

Definition: This risk considers whether the mechanical supply contains flaws or inconsistencies that may indicate the part is not genuine or not to specifications

Possible Measures:
(RM-1520) Does supplier lack or fail to follow a quality assurance process to inspect poor manufacture quality?
(RM-1521) Does supplier lack or fail to follow procedures to correct poor manufacture quality when found?

(RF-1009) Small hardware indicates poor manufacture of mechanical supply

Definition: This risk considers whether small hardware in mechanical supplies contain flaws or inconsistencies that may indicate the part is not genuine or not to specifications.

Possible Measures:
(RM-1522) Does supplier lack or fail to follow a quality assurance process to ensure authenticity of mechanical supply and inspection for flaws or inconsistencies versus specification?
(RM-1523) Does supplier lack or fail to follow procedures to reject any non-authentic parts?
(RM-1524) Does supplier lack or fail to follow procedures to correct any flaws or inconsistencies of parts versus specification?

(RF-1010) Roller bearings indicate poor manufacture of mechanical supply

Definition: This risk considers whether roller bearings in mechanical supplies contain flaws or inconsistencies that may indicate the part is not genuine or not to specifications

Possible Measures:
(RM-1525) Does supplier lack or fail to follow a quality assurance process to ensure authenticity of roller bearings and inspection for flaws or inconsistencies versus specification?
(RM-1526) Does supplier lack or fail to follow procedures to reject any non-authentic roller bearings?
(RM-1527) Does supplier lack or fail to follow procedures to correct any flaws or inconsistencies of roller bearings versus specification?

(RF-1006) Mechanical supplies include documentation that is not as expected

Definition: This risk considers whether the documentation included with mechanical parts does not appear genuine upon inspection

Possible Measures:
(RM-1528) Does supplier lack or fail to follow procedures to conduct an investigation in the event the documentation included with mechanical parts does not appear genuine upon inspection?

Level 4

(RC-30) ICT Hardware Authenticity Risks

Definition: Risks that relate to the authenticity of ICT hardware and their electric/electronic subcomponents.

(RC-9) Supply Counterfeit in Table Form

(RF-1022) Electrical supplies do not match known-good examples

Definition: This risk considers whether an electrical component does not appear to be the same as known-good parts previously purchased from the manufacturer, and may indicate it is not genuine or out of specification.

Possible Measures:
(RM-1529) Does supplier lack or fail to follow procedures to conduct an investigation in the event electrical supplies do not match known-good examples?

(RC-9) Supply Counterfeit in Table Form

(RF-1011) Electrical supplies include documentation that is not as expected

Definition: This risk considers whether the documentation included with ICT supplies does not appear genuine upon inspection.

Possible Measures:
(RM-1535) Does supplier lack or fail to follow procedures to conduct an investigation in the event the documentation included with electrical supplies does not appear genuine upon inspection?

(RF-1017) Radiological/X-ray testing reveals composition of electrical supplies not to specification

Definition: This risk considers whether radiological/x-ray testing reveals features of the electrical component that may indicate it is not genuine or out of specification.

Possible Measures:
(RM-93) Does X-ray inspection of chip reveal that there are bond wires missing between the die and its bonding pad, an indicator of recycling?
(RM-94) Does X-ray inspection of chip reveal one or more broken bond wires between the die and its bonding pad, an indicator of recycling?
(RM-95) Does X-ray inspection of chip reveal bond wire terminations on the die's bonding pad are double balled, an indicator of die repackaging?
(RM-96) Does X-ray inspection of chip reveal the die is missing?
(RM-97) Does X-ray inspection of chips from the same lot reveal inconsistent die sizes?
(RM-98) Does X-ray inspection of chips from the same lot reveal inconsistent leadframe designs?
(RM-1536) Does supplier lack or fail to follow a documented work process as to what response is expected when radiological/x-ray testing reveals features of the electrical component that may indicate it is not genuine or out of specification?

(RF-1019) Decapsulation reveals composition of electrical supplies not to specification

Definition: This risk considers whether decapsulation reveals features of the electrical component that may indicate it is not genuine or out of specification.

Possible Measures:
(RM-1537) Does supplier lack or fail to follow a documented work process as to what response is expected when decapsulation reveals electrical supplies are not to specification?

(RF-1021) Electrical supplies are prone to failure

Definition: This risk considers whether the failure rate of electrical supplies may indicate it is not genuine or out of specification

Possible Measures:

(RF-1015) Leads or solder balls of electrical supply indicate poor manufacture

Definition: This risk considers whether the leads or solder balls of electrical components contains flaws or inconsistencies that may indicate the part is not genuine or not to specifications.

Possible Measures:

(RF-1023) Surface markings of electrical supply indicate modifications

Definition: This risk considers whether the surface markings of electrical components have indications that they have been modified from appropriate manufacture.

Possible Measures:
(RM-1540) Does supplier lack quality insurance inspection of surface markings of electrical components for indications that they have been modified from appropriate manufacture?
(RM-1541) Does quality insurance inspection of surface markings of electrical components indicate that they have been modified from appropriate manufacture?
(RM-1542) Does supplier lack or fail to follow a documented work process as to what response is expected when electrical components have indications that they have been modified from appropriate manufacture?

(RF-1018) Scanning acoustic microscopy reveals composition of electrical supplies not to specification

Definition: This risk considers whether scanning acoustic microscopy reveals features of the electrical component that may indicate it is not genuine or out of specification

Possible Measures:
(RM-100) Does acoustic microscope scanning of chip reveal laser etching underneath blacktopping, a sign that resurfacing was used to cover up original markings?
(RM-1543) Does supplier lack or fail to follow a documented work process as to what response is expected when scanning acoustic microscopy reveals electrical supplies are not to specification?

(RF-1016) X-ray fluorescence testing reveals composition of electrical supplies not to specification

(RC-9) Supply Counterfeit in Table Form

Definition:	This risk considers whether x-ray fluorescence testing reveals features of the electrical component that may indicate it is not genuine or out of specification.
Possible Measures:	

(RC-9) Supply Counterfeit in Table Form

(RF-1012) Dimensions of electrical supplies are not to specification

Definition: This risk considers whether the electrical components received appear to match the components purchased in size & shape.

Possible Measures:
(RM-1551) Does supplier lack or fail to follow a documented work process as to what response is expected when dimensions are out of specification?

(RF-1020) Programmable parts do not function as required

Definition: This risk considers whether a programmable part cannot be programmed correctly and may indicate the electrical supply is not genuine or out of specification.

Possible Measures:

(RF-1013) Surface of electrical supply indicates poor manufacture

Definition: This risk considers whether the surface of electrical components contains flaws or inconsistencies that may indicate the part is not genuine or not to specifications.

Possible Measures:
(RM-978) Does the surface marking of electrical supply have incomplete or missing data?
(RM-979) Does the surface marking of electrical supply have preprinted labels that show typed entries?
(RM-980) Does the surface of electrical supply have markings in a different location or orientation than normal?
(RM-981) Does the surface marking of electrical supply have missing manufacturer's standard markings, stamps, or logos, or with irregular stamping or inconsistent font?
(RM-982) Does the surface marking of electrical supply have atypically multiple logos or seals?
(RM-1552) Does supplier lack quality insurance inspection of surfaces of electrical supply for indications that they have been modified from appropriate manufacture?

(RF-1014) Surface finish of electrical supply is not permanent

Definition: This risk considers whether the surface finish of electrical components is not applied permanently, as would be expected of genuine supplies, and may indicate the part is not genuine or not to specifications

Possible Measures:
(RM-126) Are texture differences in finish visible between the top and side surfaces of the chip package, an indicator of blacktopping?
(RM-1553) Does supplier lack quality insurance inspection of the surface finish of electrical components for indications that they have been modified from appropriate manufacture?

Level 5

(RC-62) ICT Hardware Device Authenticity

Definition: Risks related to the authenticity of ICT hardware which includes subcomponents such as power supplies and capacitors.

(RF-83) Device is or contains an electronic component identified as suspect or confirmed counterfeit

Definition: Risk that a device is or contains an electronic component reported to, investigated, substantiated as suspect/confirmed counterfeit, and disseminated by an authoritative entity, e.g., Government-Industry Data Exchange Program (GIDEP), Independent Distributors of Electronics Association (IDEA), Electronic Resellers Association International (ERAI)

Possible Measures:
(RM-553) Has a Field Programmable Gate Array (FPGA) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-554) Has a Graphics Processing Unit (GPU) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-555) Has a Microcontroller (µC or Microcontroller Unit (MCU)) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-556) Has a Microprocessor (µP or Microprocessor Unit (MPU)) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-557) Has a Programmable System on Chip (SoC) (or SoC Field Programmable Gate Array (FPGA)) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-558) Has a System on Chip (SoC) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-559) Has an Application Specific Integrated Circuit (ASIC) chip in a device produced by the device manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-1530) Does supplier lack or fail to follow a documented work process as to what response is expected when a device is or contains counterfeit parts?

(RF-260) Device contains counterfeit chips

Definition: Risk that a device is untrustworthy because it has counterfeit chips.

Possible Measures:

(RC-9) Supply Counterfeit in Table Form

(RM-1531) Does supplier lack a mechanism to determine if chips are counterfeit?
(RM-1532) Does supplier lack or fail to follow a documented work process as to what response is expected when a chip is counterfeit?

(RF-259) Device contains counterfeit boards

Definition: Risk that a device is untrustworthy because it has counterfeit printed circuit boards.

Possible Measures:
(RM-1533) Does supplier lack a mechanism to determine if printed circuit boards are counterfeit?
(RM-1534) Does supplier lack or fail to follow a documented work process as to what response is expected if printed circuit boards are counterfeit?

Level 5

(RC-73) ICT Hardware Board Authenticity

Definition: Risks related to the authenticity of ICT hardware boards.

(RF-254) Board has visible physical deformities indicating board has been resurrected/recycled

Definition: Risk of the board being untrustworthy due to appearance of having been resurrected/recycled from used or scrap electronics.

Possible Measures:
(RM-545) Are marks such as scuffs or scratches visible on top or side surfaces of the board?
(RM-546) Does magnified inspection of board reveal visible delamination on any of its surfaces?
(RM-547) Does the board show physical wear and tear?
(RM-548) Does the color of the board appear faded when compared to the color of other same or similar boards known to be authentic?
(RM-1544) Does supplier lack or fail to follow procedures to conduct an investigation in the event that a board has visible physical deformities indicating board has been resurrected/recycled?

(RF-258) Board contains counterfeit chips

Definition: Risk that a printed circuit board contains a chip reported to, investigated, substantiated as suspect/confirmed counterfeit, and disseminated by an authoritative entity, e.g., Government-Industry Data Exchange Program (GIDEP), Independent Distributors of Electronics Association (IDEA), Electronic Resellers Association International (ERAI).

Possible Measures:
(RM-1545) Has a chip on a board produced by the board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-1546) Does supplier lack or fail to follow a documented work process as to what response is expected when a board is or contains counterfeit chip(s)?

(RF-255) Board resurfacing is detected indicating board is suspect counterfeit

Definition: Risk of the board being untrustworthy due to appearance of having been resurfaced.

Possible Measures:
(RM-549) Are texture differences in finish visible between the top and side surfaces of the board?
(RM-550) Does acoustic microscope scanning of board reveal laser etching underneath blacktopping, a sign that resurfacing was used to cover up original markings?
(RM-551) Has the board been resurfaced (blacktopped)?
(RM-552) If board was resurfaced (blacktopped), was resurfacing performed by an entity other than its original manufacturer?
(RM-1547) Does supplier lack or fail to follow procedures to conduct an investigation in the event that a board has indication of resurfacing leading to suspicion of being counterfeit?

(RF-79) Board is not authentic because it contains non-authentic parts

Definition: Risk that Printed circuit board is untrustworthy because it is or contains parts reported to, investigated, substantiated as suspect/confirmed counterfeit, and disseminated by an authoritative entity, e.g., Government-Industry Data Exchange Program (GIDEP), Independent Distributors of Electronics Association (IDEA), Electronic Resellers Association International (ERAI).

Possible Measures:
(RM-150) Has a System on Chip (SoC) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-152) Has a Field Programmable Gate Array (FPGA) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-157) Has an Application Specific Integrated Circuit (ASIC) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-158) Has a Programmable System on Chip (SoC) (or SoC Field Programmable Gate Array (FPGA)) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-162) Has a Microprocessor (µP or Microprocessor Unit (MPU)) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?

(RC-9) Supply Counterfeit in Table Form

(RM-163) Has a Graphics Processing Unit (GPU) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-209) Has a Microcontroller (µC or Microcontroller Unit (MCU)) chip on a printed circuit board produced by the printed circuit board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-1548) A new risk measure t8hkw5Has a part on a board produced by the board manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-1549) Does supplier lack or fail to follow a documented work process as to what response is expected when a board is or contains non-authentic parts?

Level 5

(RC-31) ICT Hardware Chip (FPGA/ASIC) Authenticity

Definition: Risks related to the authenticity of ICT hardware chips

(RF-91) Chip has visible physical deformities indicating chip has been resurrected/recycled

Definition: Risk of the chip being untrustworthy due to appearance of having been resurrected/recycled from used or scrap electronics.

Possible Measures:
(RM-108) Does the chip show physical wear and tear, including bent leads?
(RM-109) Does the color of the chip package appear faded when compared to the package color of other same or similar chips known to be authentic?
(RM-112) Does magnified inspection of chip reveal visible delamination on any of its surfaces?
(RM-125) Are marks such as scuffs or scratches visible on top or side surfaces of the chip's package?
(RM-1554) Does supplier lack or fail to follow procedures to conduct an investigation in the event that there are visible physical deformities indicating chip has been resurrected/recycled?

(RF-118) Chip is identified as being a suspect or confirmed counterfeit.

Definition: Risk that a chip reported to, investigated, substantiated as suspect/confirmed counterfeit, and disseminated by an authoritative entity, e.g., Government-Industry Data Exchange Program (GIDEP), Independent Distributors of Electronics Association (IDEA), Electronic Resellers Association International (ERAI) rendering it untrustworthy.

Possible Measures:
(RM-115) Has a Graphics Processing Unit (GPU) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity?
(RM-116) Has a System on Chip (SoC) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-117) Has a Programmable System on Chip (SoC) (or SoC Field Programmable Gate Array (FPGA)) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-118) Has a Microcontroller (µC or Microcontroller Unit (MCU)) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-207) Has an Application Specific Integrated Circuit (ASIC) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-208) Has a Microprocessor (µP or Microprocessor Unit (MPU)) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-210) Has a Field Programmable Gate Array (FPGA) chip produced by the chip manufacturer been reported to, investigated, substantiated, and disseminated by an authoritative entity?
(RM-1555) Has a chip supply been reported to, investigated, substantiated, and disseminated by an authoritative entity, e.g., GIDEP, IDEA, ERAI?
(RM-1556) Does supplier lack or fail to follow a documented work process as to what response is expected when a chip is identified as being a suspect or confirmed counterfeit?

(RC-128) Copycat Manufacturing

Definition: Risks that increase the likelihood a supply (product) is not authentic because of manufacturing by unauthorized entities to mimic an authentic supply (product).

(RF-1046) OEM reports that unauthorized copies exist of the supply (product)

Definition: This risk considers whether known, unauthorized copies of a supply exist, thus requiring greater inspection and testing to ensure the product son hand are in fact genuine.

Possible Measures:

(RF-1048) The tools and capability to produce copycat products exist beyond the bounds of the authorized manufacturer.

Definition: This risk considers the likelihood of copycat manufacturing if the tools and capability to produce copycat products exist beyond the bounds of the authorized manufacturer.

Possible Measures:

(RC-9) Supply Counterfeit in Table Form

(RF-1049) Release of or loss of control of proprietary manufacturing data/trade secrets has occurred

Definition: This risk considers the likelihood of copycat manufacturing if any release of or loss of control of relevant proprietary manufacturing data/trade secrets has occurred. This could indicate a malicious insider or an undiscovered data breach.

Possible Measures:

(RM-1265) Has there been any information indicating details of proprietary manufacturing data/trade secrets are accessible to unauthorized parties?
(RM-1266) Has there been any information indicating details of proprietary manufacturing data/trade secrets have been inappropriately altered by unauthorized parties?

(RC-8) Supply Hygiene Risks in Table Form

Supply Chain Risks		
(RC-1) Supplier Risks	**(RC-2) Supply Risks**	(RC-3) Service Risks
(RC-77) Supply Malicious Taint	(RC-9) Supply Counterfeit	**(RC-8) Supply Hygiene Risks**

Definition: Risks affecting the ability of a supply (product) to perform as expected. This involves characteristics related to establishing and maintaining the quality, security, resilience, etc. of the supply (product).

Level 3

(RC-214) Supply (product) resilience risks

Definition: Risks affecting the ability of a supply (product) to continue to conform structurally and functionally, within unexpected and changing environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 4

(RC-487) Hardware supply (product) resilience risks

Definition: Risks affecting the ability of a hardware supply (product) to continue to conform structurally and functionally, within unexpected and changing environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 5

(RC-242) ICT hardware supply (product) resilience risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to continue to conform structurally and functionally, within unexpected and changing environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 6

(RC-497) ICT hardware supply (product) interoperability risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to remain operationally effective in its interoperation with other supplies (products).

(RF-645) ICT hardware supply (product) is prone to communications failures when placed in the operation environment.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective in its operational environment without degraded communications with other supplies (products).

Possible Measures:

Level 6

(RC-490) ICT hardware supply (product) cybersecurity resilience risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

(RF-630) ICT hardware supply (product) cannot recover from cyber stresses

Definition: This risk considers how an ICT hardware supply (product) may fail to recover from cyber stresses.

Possible Measures:

(RF-628) ICT hardware supply (product) cannot adapt to cyber attacks

Definition: This risk considers how an ICT hardware supply (product) may fail to adapt to cyber attacks.

Possible Measures:

(RF-625) ICT hardware supply (product) cannot withstand cyber attacks

Definition: This risk considers how an ICT hardware supply (product) may fail to withstand cyber attacks.

Possible Measures:

(RF-629) ICT hardware supply (product) cannot recover from adverse cyber conditions

Definition: This risk considers how an ICT hardware supply (product) may fail to recover from adverse cyber conditions.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

(RF-623) ICT hardware supply (product) cannot withstand adverse cyber conditions

Definition: This risk considers how an ICT hardware supply (product) may fail to withstand adverse cyber conditions.

Possible Measures:

(RF-624) ICT hardware supply (product) cannot withstand cyber stresses

Definition: This risk considers how an ICT hardware supply (product) may fail to withstand cyber stresses.

Possible Measures:

(RF-626) ICT hardware supply (product) cannot adapt to adverse cyber conditions

Definition: This risk considers how an ICT hardware supply (product) may fail to adapt to adverse cyber conditions.

Possible Measures:

(RF-627) ICT hardware supply (product) cannot adapt to cyber stresses

Definition: This risk considers how an ICT hardware supply (product) may fail to adapt to cyber stresses.

Possible Measures:

(RF-631) ICT hardware supply (product) cannot recover from cyber attacks

Definition: This risk considers how an ICT hardware supply (product) may fail to recover from cyber attacks.

Possible Measures:

Level 6

(RC-498) ICT hardware supply (product) safety risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to fail in a safe and secure manner.

(RF-646) ICT hardware supply (product) fails in an unsafe manner.

Definition: This risk considers how an ICT hardware supply (product) may fail in an unsafe manner when pushed past its intended operational limits.

Possible Measures:
(RM-1295) Does functional or structural failure of the ICT hardware supply (product) result in safety concerns to users or the general public?

(RF-647) ICT hardware supply (product) fails in an insecure manner.

Definition: This risk considers how an ICT hardware supply (product) may fail in an insecure manner when pushed past its intended operational limits.

Possible Measures:
(RM-1296) Does functional or structural failure of the ICT hardware supply (product) result in negative impact on confidentiality?
(RM-1297) Does functional or structural failure of the ICT hardware supply (product) result in negative impact on integrity?
(RM-1298) Does functional or structural failure of the ICT hardware supply (product) result in negative impact on availability?
(RM-1299) Does functional or structural failure of the ICT hardware supply (product) result in negative impact on authenticity?
(RM-1300) Does functional or structural failure of the ICT hardware supply (product) result in negative impact on non-repudiation?

Level 6

(RC-494) ICT hardware supply (product) robustness risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to remain operationally effective in the face of errors, faults and varying environmental conditions.

(RF-641) ICT hardware supply (product) is not able to overcome reasonably expected environmental conditions.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective in the face of reasonably expected environmental conditions.

Possible Measures:

(RF-639) ICT hardware supply (product) is not able to overcome reasonably expected errors.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective in the face of reasonably expected errors.

Possible Measures:

(RF-640) ICT hardware supply (product) is not able to overcome reasonably expected faults.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective in the face of reasonably expected faults.

Possible Measures:

Level 6

(RC-493) ICT hardware supply (product) tamper tolerance risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to maintain integrity and trustworthy operation when targeted by intentional tampering.

(RF-638) ICT hardware supply (product) is not able to demonstrate a Root of Trust for upgrade &/or maintenance.

Definition: This risk considers how an ICT hardware supply (product) may be unable to demonstrate a Root of Trust for upgrade &/or maintenance when targeted by intentional tampering.

Possible Measures:

(RF-637) ICT hardware supply (product) is not able to demonstrate a Root of Trust for runtime.

Definition: This risk considers how an ICT hardware supply (product) may be unable to demonstrate a Root of Trust for runtime when targeted by intentional tampering.

Possible Measures:

(RF-635) ICT hardware supply (product) is not able to demonstrate a Root of Trust for instantiation from a known good state.

Definition: This risk considers how an ICT hardware supply (product) may be unable to demonstrate a Root of Trust for instantiation from a known good state when targeted by intentional tampering.

Possible Measures:

(RF-636) ICT hardware supply (product) is not able to demonstrate a Root of Trust for boot.

Definition: This risk considers how an ICT hardware supply (product) may be unable to demonstrate a Root of Trust for boot when targeted by intentional tampering.

Possible Measures:

(RF-634) ICT hardware supply (product) unable to resist tampering.

Definition: This risk considers how an ICT hardware supply (product) may be unable to resist intentional tampering.

Possible Measures:

Level 6

(RC-495) ICT hardware supply (product) capacity risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to remain operationally effective under expected levels, duration, and volatility of operational loads.

(RF-643) ICT hardware supply (product) fails under normally expected operational loads.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective under expected levels of operational loads.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

Level 6

(RC-491) ICT hardware supply (product) survivability risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to survive physical damage due to intentional physical attack or unintentional safety hazards.

Level 7

(RC-492) ICT hardware supply (product) kinetic attack survivability risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to survive a kinetic attack.

(RF-633) ICT hardware supply (product) is not able to remain mission capable after a single engagement.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain mission capable after a single engagement.

Possible Measures:

(RF-632) ICT hardware supply (product) is fragile and unable to function after minor kinetic attacks.

Definition: This risk considers how an ICT hardware supply (product) may be unable to function as expected after minor kinetic attacks.

Possible Measures:

Level 6

(RC-496) ICT hardware supply (product) longevity risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to remain operationally effective for its full intended useful life span.

(RF-644) ICT hardware supply (product) is prone to defects and age related failures before its intended useful life span.

Definition: This risk considers how an ICT hardware supply (product) may be unable to remain operationally effective for its full intended useful life span and not succumb to age related defects and failures.

Possible Measures:

Level 4

(RC-499) Pharma supply (product) resilience risks

Definition: Risks affecting the ability of a pharma supply (product) to continue to conform structurally and functionally, within unexpected and changing environmental or usage parameters, to a specific expected standard or other set of requirements.

(RC-500) Foodstuff supply (product) resilience risks

Definition: Risks affecting the ability of a foodstuff supply (product) to continue to conform structurally and functionally, within unexpected and changing environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 3

(RC-213) Supply (product) security risks

Definition: Risks affecting the ability of a supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RF-305) Lack of appropriate network segmentation and isolation for supply (product) manufacture to prevent access from network based adversaries

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to lack of appropriate network segmentation and isolation for the digital environment used for its manufacture in order to prevent access from network based adversaries.

Possible Measures:
(RM-661) Are the product manufacturer's information systems protected from network based adversaries through appropriate network segmentation and isolation?
(RM-1557) Does supplier lack a comprehensive network segmentation plan for supply (product) manufacture identifying and structured by explicit zones and conduits?
(RM-1558) Does supplier lack effective comprehensive network segmentation implementing an explicit comprehensive network segmentation plan for supply (product) manufacture?

(RF-1252) Inappropriate supply (product) data communication

Definition:

Possible Measures:
(RM-1199) Does the supply (product) transmit data to infrastructure in country/ies of concern?

(RF-1253) Inappropriate supply (product) command and control

Definition:

Possible Measures:
(RM-1200) Does the supply (product) receive, accept, and obey command and control imperatives from infrastructure in country/ies of concern?

(RF-1254) Concerns for who has remote access to supply (product) functionality and configuration

Definition:

Possible Measures:
(RM-1201) Are personnel in country/ies of concern able to remotely access the supply (product) functionality or configuration?
(RM-1202) Are personnel in country/ies of concern able to remotely modify the supply (product) functionality or configuration?
(RM-1203) Are personnel in country/ies of concern able to remotely leverage system administrator privileges for the supply (product) functionality or configuration?

(RF-1256) Concerns for where sensitive customer data is remotely processed or retained by the supply (product)

Definition:

Possible Measures:
(RM-1207) Does the supply (product) process or retain customer PII data on infrastructure in country/ies of concern?
(RM-1208) Does the supply (product) process or retain customer BII data on infrastructure in country/ies of concern?
(RM-1209) Does the supply (product) process or retain customer financial information on infrastructure in country/ies of concern?

Level 4

(RC-533) Inappropriate supply (product) exposure or exploitation

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to evidence of its exposure or direct technical exploitation of its structure and/or function.

(RF-392) Supply (product) availability on gray market

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to evidence of its direct exposure and availability on the gray market.

Possible Measures:
(RM-722) Is the product available on the gray market?
(RM-723) Are other company products illicitly available on gray market?
(RM-724) Is there a history of company products illicitly available on gray market?

(RF-407) Supply (product) clone availability on gray market

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to evidence of its indirect exposure on the gray market via availability of a supply (product) clone.

Possible Measures:
(RM-807) Is clone of the product available on the gray market?
(RM-808) Are clone of other company products available on gray market?
(RM-809) Is there a history of clones of company products available on gray market?

(RF-406) Supply (product) Exploitation

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to evidence of its direct technical exploitation (e.g., reversing or deconstructive analysis) exposing its technical structure and/or function.

Possible Measures:
(RM-800) Are there known instances of exploitation of the product?
(RM-801) Are there active (in-the-wild) exploits of the product?
(RM-802) Does the product have known direct vulnerabilities?
(RM-803) Does the product have known indirect vulnerabilities due to associated risks demonstrated as exploitable in other products?

(RF-393) Supply (Product) counterfeit availability on gray market

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to evidence of its indirect exposure on the gray market via availability of a supply (product) counterfeit.

Possible Measures:
(RM-725) Is counterfeit of the product available on the gray market?
(RM-726) Are counterfeits of other company products available on gray market?

(RC-8) Supply Hygiene Risks in Table Form

(RM-727) Is there a history of counterfeits of company products available on gray market?

Level 4

(RC-531) Inadequate security training and certification for information systems users or managers involved in supply (product).

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to inadequate security training and certification for information systems users or managers involved in board supply (product) manufacture.

(RF-295) Supply (product) manufacture does not have a designated cyber/information security manager holding a relevant certification from an industry-recognized authority.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to lack of a cyber/information security manager (holding a relevant certification from an industry-recognized authority) being designated for its manufacture.

Possible Measures:
(RM-655) Does the product manufacturer have a full-time cyber/information security manager holding a relevant certification from an industry-recognized authority (e.g., International Information System Security Certification Consortium (ISC2))?

(RF-310) Users of information systems used for supply (product) manufacture do not receive cybersecurity training.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to insufficient security training for users of information systems used for its manufacture.

Possible Measures:
(RM-666) Do users of the product manufacturer's information systems receive cybersecurity training at least annually?
(RM-1559) Does the the supplier lack a clearly documented cyber security training program for all personnel using information systems used for supply manufacture?
(RM-1560) Does the supplier lack documented proof of cyber security training performed/completed for all personnel using information systems used for supply manufacture?
(RM-1561) Does the supplier lack yearly refresher cyber security training performed/completed for all personnel using information systems used for supply manufacture?

Level 4

(RC-502) Hardware supply (product) security risks

Definition: Risks affecting the ability of a hardware supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

Level 5

(RC-238) ICT hardware supply (product) security risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

Level 6

(RC-513) ICT hardware microelectronics supply (product) security risks

Definition: Risks affecting the ability of an ICT hardware microelectronic supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

Level 7

(RC-514) ICT hardware microelectronics supply (product) integrity risks

Definition: Risks affecting the ability of an ICT hardware microelectronic supply (product) to maintain its intended properties in the face of intentional malicious action without violating its integrity.

(RF-710) ICT hardware microelectronics supply (product) has been tampered with during integration.

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to it being tampered with during integration.

Possible Measures:

(RF-707) Fabrication tooling for ICT hardware microelectronics supply (product) has been tampered with.

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its fabrication tooling being tampered with.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

(RF-703) ICT hardware microelectronics supply (product) is susceptible to radiation (not rad-hardened/fail rad test).

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its susceptibility to radiation (not rad-hardened/fail rad test).

Possible Measures:

(RF-704) ICT hardware microelectronics supply (product) is susceptible to heat (not insulated/fail thermal test).

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its susceptibility to heat (not insulated/fail thermal test).

Possible Measures:

(RF-708) Fabrication process for ICT hardware microelectronics supply (product) has been tampered with.

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its fabrication process being tampered with.

Possible Measures:

(RF-709) ICT hardware microelectronics supply (product) packaging has been tampered with.

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its packaging being tampered with.

Possible Measures:

(RF-705) ICT hardware microelectronics supply (product) is susceptible to magnetic fields (not non-ferrous/fail mag test).

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its susceptibility to magnetic fields (not non-ferrous/fail mag test).

Possible Measures:

(RF-706) Designs for ICT hardware microelectronics supply (product) have been tampered with.

Definition: This risk considers how an ICT hardware microelectronics supply (product) may be unable to maintain its security properties due to its designs being tampered with.

Possible Measures:
(RM-1562) Does the supplier lack effective integrity validation of ICT hardware microelectronics supply (product) designs?

Level 6

(RC-27) ICT hardware chip supply (product) security risks

Definition: Risks affecting the ability of an ICT hardware chip supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RF-11) Foundry not a participant in DoD's Trusted Foundry/Trusted Supplier Program

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to its fabrication foundry not being a participant in the US Department of Defense Trusted Foundry/Trusted Supplier Program.

Possible Measures:
(RM-68) Has the foundry been accredited by the Defense Microelectronics Activity (DMEA) for membership in DoD's Trusted Foundry/Trusted Supplier Program?

(RF-26) Lack of the appropriate network segmentation and isolation for chip supply (product) fabrication to prevent access from network based adversaries.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to lack of appropriate network segmentation and isolation for the digital environment used for its fabrication in order to prevent access from network based adversaries.

Possible Measures:
(RM-82) Are the foundry's information systems protected from network based adversaries through appropriate network segmentation and isolation?
(RM-1563) Does supplier lack a comprehensive network segmentation plan for supply (product) fabrication identifying and structured by explicit zones and conduits?

(RC-8) Supply Hygiene Risks in Table Form

(RM-1564) Does supplier lack effective comprehensive network segmentation implementing an explicit comprehensive network segmentation plan for supply (product) fabrication?

Level 7

(RC-510) Inadequate foundry information system security configuration, operations and management used for chip supply (product) fabrication.

Definition: Risks affecting the ability of an ICT hardware chip supply (product) to maintain its intended security properties due to inadequate security configuration, operation and management of relevant information systems.

(RF-3) Foundry information system software used for chip supply (product) fabrication not kept current.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to failure to keep software current on foundry information systems used for its manufacture.

Possible Measures:
(RM-58) Does the foundry have a designated person responsible for software configuration management of its information systems?
(RM-59) Is software on foundry information systems managed to current revision levels?
(RM-60) Is software on foundry information systems managed to current patch levels?

(RF-6) Users not required to set strong passwords on foundry information systems used for chip supply (product) fabrication.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to failure to require users to set strong passwords on foundry information systems used for its manufacture.

Possible Measures:
(RM-86) Are users required to set strong passwords on foundry information systems following password creation guidelines described in NIST 800-63 Password Guidelines?
(RM-1573) Does supplier lack an explicit password standard for foundry information systems used for chip supply (product) fabrication?
(RM-1574) Does supplier have an explicit password standard for foundry information systems used for chip supply (product) fabrication that lacks strong password requirements?

(RF-4) Misconfigured access controls on foundry information systems used for chip supply (product) fabrication.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to misconfigured access controls on foundry information systems used for its manufacture.

Possible Measures:
(RM-61) Do foundry information systems implement access controls consistent with access control AC-3 ACCESS ENFORCEMENT described in NIST SP 800-53r4?
(RM-1579) Does supplier lack explicitly specified configurations for access controls on foundry information systems used for chip supply (product) fabrication?
(RM-1580) Does supplier lack an explicit policy for managing configurations for access controls on foundry information systems used for chip supply (product) fabrication?
(RM-1581) Does supplier lack an audit program to ensure implemented configurations for access controls on foundry information systems used for chip supply (product) fabrication conform to specified configurations?

(RF-5) Weak identification and authentication controls on foundry information systems used for chip supply (product) fabrication.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to weak identification and authentication controls on foundry information systems used for its manufacture.

Possible Measures:
(RM-62) Do foundry information systems implement identification and authentication controls consistent with identification and authentication control IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) described in NIST SP 800-53r4?

(RF-12) Information on foundry information systems used for chip supply (product) fabrication not backed up regularly.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to failure to regularly back up information on foundry information systems used for its manufacture.

Possible Measures:
(RM-69) Is information on foundry information systems involved in chip manufacturing backed up to an alternative site (offline storage) at least once daily?
(RM-1582) Does the supplier lack an explicit policy for backing up information on foundry information systems used for chip supply (product) fabrication?
(RM-1583) Does the supplier have an explicit policy for backing up information on foundry information systems used for chip supply (product) fabrication that lacks a requirement for specific frequency of backup?
(RM-1584) Does the supplier have an explicit policy for backing up information on foundry information systems used for chip supply (product) fabrication that lacks a requirement for specific duration of retention of backed up information?
(RM-1585) Does the supplier lack explicitly defined procedures for backing up information on foundry information systems used for chip supply (product) fabrication?
(RM-1586) Does the supplier lack periodic integrity testing of backed up information on foundry information systems used for chip supply (product) fabrication?
(RM-1587) Does the supplier lack periodic restoration testing of backed up information on foundry information systems used for chip supply (product) fabrication?

(RF-25) Foundry information systems used for chip supply (product) fabrication do not run anti-malware software.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to failure to run anti-malware software on foundry information systems used for its manufacture.

Possible Measures:
(RM-85) Are foundry information systems required to and verified as running software that blocks execution of unauthorized code to include viruses, trojans, and other forms of malware?
(RM-1575) Does supplier lack an explicit policy for running anti-malware software on foundry information systems used for chip supply (product) fabrication?
(RM-1576) Does supplier lack an explicit policy for managing anti-malware software on foundry information systems used for chip supply (product) fabrication?

(RF-51) Foundry information systems used for chip supply (product) fabrication running anti-malware software are not running current versions.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to failure to run current versions of anti-malware software on foundry information systems used for its manufacture.

Possible Measures:
(RM-204) Do foundry information systems running anti-malware software run current versions that include patches, builds, signature identification, and heuristic patterns?
(RM-1575) Does supplier lack an explicit policy for running anti-malware software on foundry information systems used for chip supply (product) fabrication?
(RM-1576) Does supplier lack an explicit policy for managing anti-malware software on foundry information systems used for chip supply (product) fabrication?
(RM-1577) Does supplier have an explicit policy for managing anti-malware software on foundry information systems used for chip supply (product) fabrication that lacks a requirement for running the latest version?
(RM-1578) Does the supplier lack explicitly defined procedures for updating anti-malware software on foundry information systems used for chip supply (product) fabrication?

Level 7

(RC-511) Inadequate security training and certification for foundry information systems users or managers involved in chip supply (product) fabrication

Definition: Risks affecting the ability of an ICT hardware chip supply (product) to maintain its intended security properties due to inadequate security training and certification for information systems users or managers involved in board supply (product) manufacture.

(RF-100) Chip supply (product) fabrication does not have a designated cyber/information security manager holding a relevant certification from an industry-recognized authority.

(RC-8) Supply Hygiene Risks in Table Form

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to lack of a cyber/information security manager (holding a relevant certification from an industry-recognized authority) being designated for its fabrication.

Possible Measures:
(RM-81) Does the foundry have a full-time cyber/information security manager holding a relevant certification from an industry-recognized authority (e.g., International Information System Security Certification Consortium (ISC2))?

(RF-7) Users of foundry information systems used for chip supply (product) fabrication do not receive cybersecurity training.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to insufficient security training for users of information systems used for its fabrication.

Possible Measures:
(RM-64) Do users of foundry information systems receive cybersecurity training at least annually?
(RM-1565) Does the the supplier lack a clearly documented cyber security training program for all personnel using foundry information systems used for supply fabrication?
(RM-1566) Does the supplier lack documented proof of cyber security training performed/completed for all personnel using foundry information systems used for supply fabrication?
(RM-1567) Does the supplier lack yearly refresher cyber security training performed/completed for all personnel using foundry information systems used for supply fabrication?

Level 7

(RC-512) Inadequate foundry data security protection used for chip supply (product) fabrication.

Definition: Risks affecting the ability of an ICT hardware chip supply (product) to maintain its intended security properties due to inadequate security protections for data relevant to its manufacture.

(RF-13) Inadequate protection for controlled unclassified information on foundry information systems used for chip supply (product) fabrication.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to inadequate protection for controlled unclassified foundry information on information systems used for its manufacture.

Possible Measures:
(RM-63) Does the foundry implement NIST SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations?
(RM-83) Do foundry information systems running anti-malware software receive regular updates of malware definitions/signatures?
(RM-87) Do foundry information systems running antivirus software receive regular updates of virus signatures?
(RM-1568) Does the supplier lack an explicit information classification policy for information on foundry information systems used for chip supply (product) fabrication?
(RM-1569) Does the supplier lack explicitly defined procedures for handling different classifications of information on foundry information systems used for chip supply (product) fabrication?

(RF-9) Sensitive information relevant to chip supply (product) fabrication not encrypted while in electronic transit.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information while in electronic transit either to or from information systems used for its fabrication.

Possible Measures:
(RM-66) Is sensitive information related to the manufacture of the chip, including chip specifications and architecture designs, encrypted while in electronic transit between the manufacturer and any other point?
(RM-1570) Does supplier lack an explicit encryption standard for information relevant to chip supply (product) fabrication while in electronic transit?

(RF-8) Sensitive information stored on foundry information systems used for chip supply (product) fabrication not encrypted.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information stored on information systems used for its fabrication.

Possible Measures:
(RM-65) Is sensitive information related to the manufacture of the chip, including chip specifications and architecture designs, stored encrypted on foundry information systems?
(RM-1571) Does supplier lack an explicit encryption standard for information relevant to chip supply (product) fabrication while stored on foundry information systems used for chip supply (product) fabrication?

(RF-10) Sensitive information in digital form relevant to chip supply (product) fabrication not encrypted while in physical transit.

Definition: This risk considers how an ICT hardware chip supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information in digital form while in physical transit either to or from printed circuit board fabrication.

Possible Measures:
(RM-67) Is sensitive information related to the manufacture of the chip, including chip specifications and architecture designs, encrypted while in physical transit between the manufacturer and any other point?
(RM-1572) Does supplier lack an explicit encryption standard for information relevant to chip supply (product) fabrication while in physical transit?

Level 6

(RC-44) ICT hardware board supply (product) security risks

Definition: Risks affecting the ability of an ICT hardware board supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RF-95) Lack of appropriate network segmentation and isolation for printed circuit board supply (product) manufacture to prevent access from network based adversaries.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to lack of appropriate network segmentation and isolation for the digital environment used for its manufacture in order to prevent access from network based adversaries.

Possible Measures:
(RM-213) Are the printed circuit board manufacturer's information systems protected from network based adversaries through appropriate network segmentation and isolation?
(RM-1598) Does supplier lack a comprehensive network segmentation plan for printed circuit board supply (product) manufacture identifying and structured by explicit zones and conduits?
(RM-1599) Does supplier lack effective comprehensive network segmentation implementing an explicit comprehensive network segmentation plan for printed circuit board supply (product) manufacture?

Level 7

(RC-506) Inadequate information system security configuration, operations and management used for board supply (product) manufacture.

Definition: Risks affecting the ability of an ICT hardware board supply (product) to maintain its intended security properties due to inadequate security configuration, operation and management of relevant manufacturing and quality verification information systems.

(RF-76) Information systems used for printed circuit board supply (product) manufacture do not run anti-malware software.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to failure to run anti-malware software on information systems used for its manufacture.

Possible Measures:
(RM-143) Are printed circuit board manufacturer's information systems required to and verified as running software that blocks execution of unauthorized code to include viruses, trojans, and other forms of malware?
(RM-1600) Does supplier lack an explicit policy for running anti-malware software on information systems used for printed circuit board supply (product) manufacture?
(RM-1601) Does supplier lack an explicit policy for managing anti-malware software on information systems used for printed circuit board supply (product) manufacture?

(RF-93) Information systems used for printed circuit board supply (product) manufacture running anti-malware software are not running current versions.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to failure to run current versions of anti-malware software on information systems used for its manufacture.

Possible Measures:
(RM-206) Do printed circuit board manufacturer's information systems running anti-malware software run current versions that include patches, builds, signature identification, and heuristic patterns?
(RM-1600) Does supplier lack an explicit policy for running anti-malware software on information systems used for printed circuit board supply (product) manufacture?
(RM-1601) Does supplier lack an explicit policy for managing anti-malware software on information systems used for printed circuit board supply (product) manufacture?
(RM-1602) Does supplier have an explicit policy for managing anti-malware software on information systems used for printed circuit board supply (product) manufacture that lacks a requirement for running the latest version?
(RM-1603) Does the supplier lack explicitly defined procedures for updating anti-malware software on information systems used for printed circuit board supply (product) manufacture?

(RF-94) Information on information systems used for printed circuit board supply (product) manufacture not backed up regularly.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to failure to regularly back up information on information systems used for its manufacture.

Possible Measures:
(RM-188) Is information on the printed circuit board manufacturer's information systems involved in printed circuit board manufacturing backed up to an alternative site (offline storage) at least once daily?

(RC-8) Supply Hygiene Risks in Table Form

(RM-1608) Does the supplier lack an explicit policy for backing up information on information systems used for printed circuit board supply (product) manufacture? (RM-1609) Does the supplier have an explicit policy for backing up information on information systems used for printed circuit board supply (product) manufacture that lacks a requirement for specific frequency of backup? (RM-1610) Does the supplier have an explicit policy for backing up information on information systems used for printed circuit board supply (product) manufacture that lacks a requirement for specific duration of retention of backed up information? (RM-1611) Does the supplier lack explicitly defined procedures for backing up information on information systems used for printed circuit board supply (product) manufacture? (RM-1612) Does the supplier lack periodic integrity testing of backed up information on information systems used for printed circuit board supply (product) manufacture? (RM-1613) Does the supplier lack periodic restoration testing of backed up information on information systems used for printed circuit board supply (product) manufacture?
(RF-63) Users not required to set strong passwords on information systems used for printed circuit board supply (product) manufacture. Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to failure to require users to set strong passwords on information systems used for its manufacture. Possible Measures: (RM-137) Are users required to set strong passwords on the printed circuit board manufacturer's information systems following password creation guidelines described in NIST 800-63 Password Guidelines? (RM-1614) Does supplier lack an explicit password standard for foundry information systems used for printed circuit board supply (product) manufacture? (RM-1615) Does supplier have an explicit password standard for foundry information systems used for printed circuit board supply (product) manufacture that lacks strong password requirements?
(RF-69) Misconfigured access controls on information systems used for printed circuit board supply (product) manufacture. Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to misconfigured access controls on information systems used for its manufacture. Possible Measures: (RM-144) Do the printed circuit board manufacturer's information systems implement access controls consistent with access control AC-3 ACCESS ENFORCEMENT described in NIST SP 800-53r4? (RM-1616) Does supplier lack explicitly specified configurations for access controls on foundry information systems used for printed circuit board supply (product) manufacture? (RM-1617) Does supplier lack an explicit policy for managing configurations for access controls on foundry information systems used for printed circuit board supply (product) manufacture? (RM-1618) Does supplier lack an audit program to ensure implemented configurations for access controls on foundry information systems used for printed circuit board supply (product) manufacture conform to specified configurations?
(RF-70) Information system software used for printed circuit board supply (product) manufacture not kept current. Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to failure to keep software current on information systems used for its manufacture. Possible Measures: (RM-170) Does the printed circuit board manufacturer have a designated person responsible for software configuration management of its information systems? (RM-191) Is software on the printed circuit board manufacturer's information systems managed to current patch levels? (RM-192) Is software on the printed circuit board manufacturer's information systems managed to current revision levels? (RM-1619) Does supplier lack an explicit policy for managing all software on information systems used for printed circuit board supply (product) manufacture? (RM-1620) Does supplier have an explicit policy for managing all software on information systems used for printed circuit board supply (product) manufacture that lacks a requirement for running the latest versions? (RM-1621) Does the supplier lack explicitly defined procedures for updating software on information systems used for printed circuit board supply (product) manufacture?
(RF-98) Weak identification and authentication controls on information systems used for printed circuit board supply (product) manufacture. Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to weak identification and authentication controls on information systems used for its manufacture. Possible Measures: (RM-148) Do the printed circuit board manufacturer's information systems implement identification and authentication controls consistent with identification and authentication control IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) described in NIST SP 800-53r4?

(RC-8) Supply Hygiene Risks in Table Form

Level 7

(RC-507) Inadequate security training and certification for information systems users or managers involved in board supply (product) manufacture.

Definition: Risks affecting the ability of an ICT hardware board supply (product) to maintain its intended security properties due to inadequate security training and certification for information systems users or managers involved in board supply (product) manufacture.

(RF-102) Printed circuit board supply (product) manufacture does not have a designated cyber/information security manager holding a relevant certification from an industry-recognized authority.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to lack of a cyber/information security manager (holding a relevant certification from an industry-recognized authority) being designated for its manufacture.

Possible Measures:
(RM-205) Does the printed circuit board manufacturer have a full-time cyber/information security manager holding a relevant certification from an industry-recognized authority (e.g., International Information System Security Certification Consortium (ISC2))?

(RF-97) Users of information systems used for printed circuit board supply (product) manufacture do not receive cybersecurity training.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to insufficient security training for users of information systems used for its manufacture.

Possible Measures:
(RM-154) Do users of the printed circuit board manufacturer's information systems receive cybersecurity training at least annually?
(RM-1590) Does the the supplier lack a clearly documented cyber security training program for all personnel using foundry information systems used for printed circuit board supply (product) manufacture?
(RM-1591) Does the supplier lack documented proof of cyber security training performed/completed for all personnel using foundry information systems used for printed circuit board supply (product) manufacture?
(RM-1592) Does the supplier lack yearly refresher cyber security training performed/completed for all personnel using foundry information systems used for printed circuit board supply (product) manufacture?

Level 7

(RC-508) Inadequate board supply (product) data security protection

Definition: Risks affecting the ability of an ICT hardware board supply (product) to maintain its intended security properties due to inadequate security protections for data relevant to its manufacture.

(RF-68) Sensitive information not encrypted while in electronic transit either to or from information systems used for printed circuit board supply (product) manufacture.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information while in electronic transit either to or from information systems used for its manufacture.

Possible Measures:
(RM-189) Is sensitive information related to the manufacture of the printed circuit board, including board specifications and architecture designs, encrypted while in electronic transit between the manufacturer and any other point?
(RM-1593) Does supplier lack an explicit encryption standard for information relevant to printed circuit board supply (product) manufacture while in electronic transit?

(RF-67) Sensitive information stored on information systems used for printed circuit board supply (product) manufacture not encrypted.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information stored on information systems used for its manufacture.

Possible Measures:
(RM-183) Is sensitive information related to printed circuit board manufacturing, including board specifications and architecture designs, stored encrypted on the printed circuit board manufacturer's information systems?
(RM-1594) Does supplier lack an explicit encryption standard for information relevant to printed circuit board supply (product) manufacture while stored on foundry information systems used for chip supply (product) fabrication?

(RF-71) Sensitive information in digital form relevant to printed circuit board supply (product) manufacture not encrypted while in physical transit either to or from printed circuit board manufacturer.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information in digital form while in physical transit either to or from printed circuit board manufacturer.

Possible Measures:
(RM-190) Is sensitive information related to the manufacture of the printed circuit board, including board specifications and architecture designs, encrypted while in physical transit between the manufacturer and any other point?

(RC-8) Supply Hygiene Risks in Table Form

(RM-1595) Does supplier lack an explicit encryption standard for information relevant to printed circuit board supply (product) manufacture while in physical transit?

(RF-111) Inadequate protection for controlled unclassified information on information systems used for printed circuit board supply (product) manufacture.

Definition: This risk considers how an ICT hardware board supply (product) may be unable to maintain its security properties due to inadequate protection for controlled unclassified information on information systems used for its manufacture.

Possible Measures:
(RM-132) Does the printed circuit board manufacturer implement NIST SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations?
(RM-1596) Does the supplier lack an explicit information classification policy for information on information systems used for printed circuit board supply (product) manufacture?
(RM-1597) Does the supplier lack explicitly defined procedures for handling different classifications of information on information systems used for printed circuit board supply (product) manufacture?

Level 4

(RC-515) Pharma supply (product) security risks

Definition: Risks affecting the ability of a pharma supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RC-516) Foodstuff supply (product) security risks

Definition: Risks affecting the ability of a foodstuff supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RC-239) Software supply (product) security risks

Definition: Risks affecting the ability of a software supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

Level 5

(RC-524) Software supply (product) secure build risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate software supply (product) secure build practices.

(RF-734) Insufficient consistency of software supply (product) build process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient consistency of the software supply (product) build process.

Possible Measures:
(RM-1622) Does supplier lack an explicitly defined and documented software supply (product) build process?
(RM-1623) Does supplier lack an automated software supply (product) build process?
(RM-1624) Does supplier lack explicit policy for managing software supply (product) build process definition, documentation, and automation?
(RM-1625) Does supplier lack explicitly defined procedures for managing software supply (product) build process definition, documentation, and automation?
(RM-1626) Does supplier lack an explicitly defined audit process for software supply (product) build process implementation and execution?
(RM-1627) Are there open and unresolved audit findings regarding software supply (product) build process implementation and execution?
(RM-1628) Does supplier lack an active work process underway to resolve open and unresolved audit findings regarding software supply (product) build process implementation and execution?

(RF-735) Insufficient security protection of software supply (product) build process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient security protection of the software supply (product) build process.

Possible Measures:

(RF-733) Choices of software supply (product) build toolchain insufficiently justified for security

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient security justification for the software supply (product) build toolchain choices.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

(RF-732) Inadequate security design of software supply (product) build process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequacy of the security design of the software supply (product) build process.

Possible Measures:

Level 5

(RC-522) Software supply (product) code analysis risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate code analysis practices utilized for the software supply (product).

(RF-725) Inadequate software static analysis of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of software static code analysis utilized for the software supply (product).

Possible Measures:
(RM-1629) Has there been no security-focused static analysis of the software supply (product) performed?

(RF-726) Inadequate software dynamic analysis of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of software dynamic code analysis utilized for the software supply (product).

Possible Measures:
(RM-1630) Has there been no security-focused dynamic analysis of the software supply (product) performed?

(RF-727) Inadequate mitigation or remediation of software code analysis findings for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate mitigation or remediation of security risks identified by software code analysis of the software supply (product).

Possible Measures:
(RM-1631) Does supplier lack explicitly defined process and procedures for mitigation or remediation of software supply (product) code analysis findings?
(RM-1632) Does supplier lack explicit policy for mitigation or remediation of software supply (product) code analysis findings?

(RF-724) Inadequate Manual-Pattern secure code review of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of Manual-Pattern software secure code review utilized for the software supply (product).

Possible Measures:
(RM-1633) Has there been no security-focused manual analysis of the software supply (product) performed?

Level 5

(RC-528) Third party supply (product) component risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate third party software supply (product) component selection and management practices.

(RF-113) Software supply (product) includes components that were known to have exploitable vulnerabilities at the time it was in development

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to leveraging of third party software supply (product) components that were known to have exploitable vulnerabilities at the time it was in development.

Possible Measures:

(RF-743) Insufficient security vetting of third party software supply (product) components

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of security vetting of leveraged third party software supply (product) components.

Possible Measures:

Level 6

(RC-529) Open source software risks for software supply (product)

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate security vetting and management of leveraged open source software supply (product) components.

(RC-8) Supply Hygiene Risks in Table Form

(RF-750) Open-source software used for software supply (product) is not fuzz tested to detect defects and vulnerabilities in code.

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to lack of fuzz testing to detect defects and vulnerabilities in code of leveraged open source software supply (product) components.

Possible Measures:

(RF-747) Inadequate maintenance for open source software for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate maintenance for leveraged open source software supply (product) components.

Possible Measures:

(RF-751) Open-source software used for software supply (product) is not independently checked for malicious behavior before changes are committed.

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to failure to independently check for malicious behavior before change commits to leveraged open source software supply (product) components.

Possible Measures:
(RM-1639) Does supplier lack explicitly defined process and procedures for reviewing all open source software leveraged by the software supply (product) for malicious behavior before changes are committed?

(RF-752) Pull requests to Open-source software used for software supply (product) are not reviewed for malicious behavior.

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to failure to review pull requests for malicious behavior for leveraged open source software supply (product) components.

Possible Measures:
(RM-1640) Does supplier lack explicitly defined process and procedures for reviewing pull requests of all open source software leveraged by the software supply (product) for malicious behavior?

(RF-745) Insufficient security testing of open source software for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of security testing of leveraged open source software supply (product) components.

Possible Measures:

(RF-749) Open-source software used for software supply (product) contains unexpected binaries containing executable code that may be malicious.

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to leveraged open source software supply (product) components containing unexpected binaries containing executable code that may be malicious.

Possible Measures:

(RF-748) Open-source software used for software supply (product) has not been recently updated and may not be secure.

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to lack of recent updates to leveraged open source software supply (product) components.

Possible Measures:
(RM-1638) Does supplier lack explicit policy for managing maintenance and updating of all open source software leveraged by the software supply (product) performed?
(RM-1646) Is any open source software leveraged by the software supply (product) not currently up to date on its security patches?
(RM-1647) Are there any currently known unresolved security vulnerabilities in any open source software leveraged by the software supply (product)?

(RF-746) Inadequate contribution control for open source software for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate contribution control for leveraged open source software supply (product) components.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

(RF-744) Insufficient security review of open source software for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of security review of leveraged open source software supply (product) components.

Possible Measures:

Level 5

(RC-521) Software supply (product) coding language risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of underlying security issues in coding languages utilized for the software supply (product).

(RF-722) Choices of utilized coding languages for software supply (product) insufficiently justified for security

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient consideration and justification of security concerns with the supplier's choice of software coding languages utilized for the software supply (product).

Possible Measures:

(RF-723) Utilization of insufficiently secure coding languages for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to software supply (product) utilization of software coding languages with known security concerns.

Possible Measures:

Level 5

(RC-527) Software supply (product) pedigree and provenance risks

Definition: Risks that increase the likelihood a supplier will be unable to resist and withstand malicious actions because of inadequate software supply (product) pedigree and provenance practices.

(RF-741) Insufficient visibility and transparency of software supply (product) pedigree and provenance

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of visibility and transparency of software supply (product) pedigree and provenance.

Possible Measures:
(RM-1142) Do results from an up-to-date Software Component Analysis of supplier produced software not exist?
(RM-1143) Does an up-to-date Software Bill of Material (SBOM) of supplier produced software not exist?

(RF-742) Insufficient management of software supply (product) pedigree and provenance

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient management of software supply (product) pedigree and provenance.

Possible Measures:

Level 5

(RC-520) Software supply (product) architecture and design security risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate definition and review practices for its software architecture and design security.

(RF-720) Insufficient software supply (product) threat modeling

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of software threat modeling against it.

Possible Measures:
(RM-1648) Does supplier lack explicit policy for threat modeling analysis of the software supply (product)?
(RM-1649) Does supplier lack explicitly defined process and procedures for threat modeling analysis of the software supply (product)?

(RC-8) Supply Hygiene Risks in Table Form

(RF-718) Insufficient software supply (product) design security review

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of security review of its software design.

Possible Measures:

(RF-717) Inadequate mitigation or remediation of software supply (product) architecture security review findings for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate mitigation or remediation of security risks identified by architecture security review of the software supply (product).

Possible Measures:
(RM-1650) Does supplier lack explicit policy for mitigation or remediation of software supply (product) architecture security review analysis findings?
(RM-1651) Does supplier lack explicitly defined process and procedures for mitigation or remediation of software supply (product) architecture security review analysis findings?

(RF-716) Insufficient software supply (product) architecture security review

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an insufficient level of security review of its software architecture.

Possible Measures:
(RM-1652) Does supplier lack explicit policy for architecture security review analysis of the software supply (product)?
(RM-1653) Does supplier lack explicitly defined process and procedures for architecture security review analysis of the software supply (product)?

(RF-719) Inadequate mitigation or remediation of software supply (product) design security review findings for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate mitigation or remediation of security risks identified by design security review of the software supply (product).

Possible Measures:
(RM-1654) Does supplier lack explicit policy for design security review analysis of the software supply (product)?
(RM-1655) Does supplier lack explicitly defined process and procedures for design security review analysis of the software supply (product)?

(RF-721) Inadequate mitigation or remediation of software supply (product) threat modeling findings for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate mitigation or remediation of security risks identified by threat modeling of the software supply (product).

Possible Measures:
(RM-1656) Does supplier lack lack explicit policy for mitigation or remediation of software supply (product) threat modeling analysis findings?
(RM-1657) Does supplier lack explicitly defined process and procedures for mitigation or remediation of software supply (product) threat modeling analysis findings?

Level 5

(RC-518) Software supply (product) security process risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequately defined and implemented software supply (product) security processes.

(RF-712) Software supply (product) developed with an inadequately implemented software secure development lifecycle (SDLC)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to its development with an inadequately implemented software secure development lifecycle (SDLC).

Possible Measures:

(RF-713) Software supply (product) developed with an insufficiently effective software secure development lifecycle (SDLC)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to its development with an insufficiently effective software secure development lifecycle (SDLC) implementation.

Possible Measures:

(RF-711) Software supply (product) developed with an inadequately specified software secure development lifecycle (SDLC)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to its development with an inadequately specified software secure development lifecycle (SDLC).

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

Level 5

(RC-523) Software supply (product) security testing risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate software security testing practices in its development.

(RF-731) Inadequate mitigation or remediation of software security testing findings of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate mitigation or remediation of security risks identified by software security testing in its development.

Possible Measures:
(RM-1658) Does supplier lack explicit policy for mitigation or remediation of software supply (product) security testing findings?
(RM-1659) Does supplier lack explicitly defined process and procedures for mitigation or remediation of software supply (product) security testing findings?

(RF-729) Inadequate fuzz testing of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a supplier may be due to an inadequate level of software fuzz testing.

Possible Measures:
(RM-1660) Has there been no security-focused fuzz testing of the software supply (product) performed?
(RM-1661) Has there been no security-focused template or grammar-based fuzz testing of the software supply (product) performed?
(RM-1662) Has there been no security-focused guided fuzz testing of the software supply (product) performed?
(RM-1663) Has there been no security-focused advanced random fuzz testing of the software supply (product) performed?

(RF-728) Inadequate security testing of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of software security testing in its development.

Possible Measures:
(RM-1664) Does supplier lack explicit policy for security testing of the software supply (product)?
(RM-1665) Does supplier lack explicitly defined process and procedures for security testing of the software supply (product)?
(RM-1666) Does supplier lack explicit security requirements for the software supply (product)?
(RM-1667) Does supplier lack an explicit security test plan for the software supply (product)?

(RF-730) Inadequate penetration testing of software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of software security penetration testing in its development.

Possible Measures:
(RM-1668) Does supplier lack explicit policy for security penetration testing of the software supply (product)?
(RM-1669) Does supplier lack explicitly defined process and procedures for security penetration testing of the software supply (product)?
(RM-1670) Does supplier lack explicit security requirements with regards to penetration resistance for the software supply (product)?
(RM-1671) Does supplier lack an explicit security penetration test plan for the software supply (product)?

Level 5

(RC-526) Software supply (product) secure update risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate software supply (product) secure update practices.

(RF-740) Insufficient security protection of software supply (product) update process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient security protection of the software supply (product) update process.

Possible Measures:

(RF-78) Insufficient software supply (product) update process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient software supply (product) update processes.

Possible Measures:
(RM-147) Are software updates made on a timely basis?
(RM-672) Are software updates verified authentic?
(RM-673) Are software updates transmitted and applied in a secure fashion?

(RC-8) Supply Hygiene Risks in Table Form

Level 5

(RC-519) Software supply (product) security requirements risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate definition and review practices for software supply (product) security requirements.

(RF-715) Inadequate software supply (product) security requirements review

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to an inadequate level of review of its software security requirements.

Possible Measures:
(RM-1674) Does supplier lack explicit security requirements for the software supply (product)?
(RM-1675) Does supplier lack explicit policy for security requirements review of the software supply (product) performed?
(RM-1676) Does supplier lack explicitly defined process and procedures for security requirements review of the software supply (product) performed?

(RC-8) Supply Hygiene Risks in Table Form

(RF-714) Inadequate consistency in explicit specification of security requirements for software supply (product)

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequate consistency in explicit specification of its software security requirements.

Possible Measures:
(RM-1677) Does supplier lack explicit policy for security requirements specification for the software supply (product) performed?
(RM-1678) Does supplier lack explicitly defined process and procedures for security requirements specification for the software supply (product) performed?
(RM-1679) Does supplier lack explicit policy for auditing security requirements specification for the software supply (product) performed?
(RM-1680) Does supplier lack explicitly defined audit process and procedures for security requirements specification for the software supply (product) performed?

Level 5

(RC-525) Software supply (product) secure integration and deployment risks

Definition: Risks that increase the likelihood a software supply (product) will be unable to resist and withstand malicious actions because of inadequate software supply (product) secure integration and deployment practices.

(RF-737) Insufficient security protection of software supply (product) integration and deployment process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to insufficient security protection of the software supply (product) integration and deployment process.

Possible Measures:
(RM-1681) Does supplier lack explicit policy for software supply (product) integration and deployment?
(RM-1682) Does supplier lack explicitly defined process and procedures for integration and deployment of the software supply (product)
(RM-1683) Does supplier lack explicit security requirements for software supply (product) integration and deployment process?

(RF-736) Inadequate security design of software supply (product) integration and deployment process

Definition: This risk considers how vulnerable to malicious activity a software supply (product) may be due to inadequacy of the security design of the software supply (product) integration and deployment process.

Possible Measures:
(RM-1681) Does supplier lack explicit policy for software supply (product) integration and deployment?
(RM-1682) Does supplier lack explicitly defined process and procedures for integration and deployment of the software supply (product)
(RM-1683) Does supplier lack explicit security requirements for software supply (product) integration and deployment process?
(RM-1687) Does supplier lack explicit policy for security design analysis of software supply (product) integration and deployment process?
(RM-1688) Does supplier lack explicitly defined process and procedures for security design analysis of software supply (product) integration and deployment process?

Level 4

(RC-530) Pharma supply (product) security risks

Definition: Risks affecting the ability of a pharma supply (product) to maintain its intended properties in the face of intentional malicious action without violating its confidentiality, integrity, availability, accountability, or non-repudiation.

(RF-296) Supply (product) manufacturer information system software not kept current

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to failure to keep software current on information systems used for its manufacture.

Possible Measures:
(RM-656) Does the product manufacturer have a designated person responsible for software configuration management of its information systems?
(RM-657) Is software on the product manufacturer's information systems managed to current patch levels?
(RM-658) Is software on the product manufacturer's information systems managed to current revision levels?
(RM-1689) Does supplier lack explicit policy for managing maintenance and updating of the information systems used in the manufacture of the software supply (product)?
(RM-1690) Does supplier lack explicitly defined process and procedures for managing maintenance and updating of the information systems used in the manufacture of the software supply (product)?

(RF-294) Misconfigured access controls on information systems used for supply (product) manufacture.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to misconfigured access controls on information systems used for its manufacture.

Possible Measures:
(RM-654) Do the product manufacturer's information systems implement access controls consistent with access control AC-3 ACCESS ENFORCEMENT described in NIST SP 800-53r4?
(RM-1691) Does supplier lack explicitly specified configurations for access controls on information systems used for software supply (product) manufacture?
(RM-1692) Does supplier lack an explicit policy for managing configurations for access controls on information systems used for software supply (product) manufacture?

(RC-8) Supply Hygiene Risks in Table Form

(RM-1693) Does supplier lack an audit program to ensure implemented configurations for access controls on information systems used for software supply (product) manufacture conform to specified configurations?

(RF-297) Information systems used for supply (product) manufacture do not run anti-malware software

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to failure to run anti-malware software on information systems used for its manufacture.

Possible Measures:
(RM-659) Are product manufacturer's information systems required to and verified as running software that blocks execution of unauthorized code to include viruses, trojans, and other forms of malware?
(RM-1694) Does supplier lack an explicit policy for running anti-malware software on information systems used for software supply (product) manufacture?
(RM-1695) Does supplier lack an explicit policy for managing anti-malware software on information systems used for software supply (product) manufacture?

(RF-293) Information on information systems used for supply (product) manufacture not backed up regularly

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to failure to regularly back up information on information systems used for its manufacture.

Possible Measures:
(RM-653) Is information on the product manufacturer's information systems backed up to an alternative site (offline storage) at least once daily?
(RM-1700) Does the supplier lack an explicit policy for backing up information on information systems used for software supply (product) manufacture?
(RM-1701) Does the supplier have an explicit policy for backing up information on information systems used for software supply (product) manufacture that lacks a requirement for specific frequency of backup?
(RM-1702) Does the supplier have an explicit policy for backing up information on information systems used for software supply (product) manufacture that lacks a requirement for specific duration of retention of backed up information?
(RM-1703) Does the supplier lack explicitly defined procedures for backing up information on information systems used for software supply (product) manufacture?
(RM-1704) Does the supplier lack periodic integrity testing of backed up information on information systems used for software supply (product) manufacture?
(RM-1705) Does the supplier lack periodic restoration testing of backed up information on information systems used for software supply (product) manufacture?

(RF-309) Users not required to set strong passwords on manufacturer information systems used for supply (product) manufacture.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to failure to require users to set strong passwords on information systems used for its manufacture.

Possible Measures:
(RM-665) Are users required to set strong passwords on the product manufacturer's information systems following password creation guidelines described in NIST 800-63 Password Guidelines?
(RM-1706) Does supplier lack an explicit password standard for information systems used for software supply (product) manufacture?
(RM-1707) Does supplier have an explicit password standard for information systems used for software supply (product) manufacture that lacks strong password requirements?

(RF-298) Information systems used for supply (product) manufacture running anti-malware software are not running current versions

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to failure to run current versions of anti-malware software on information systems used for its manufacture.

Possible Measures:
(RM-660) Do product manufacturer's information systems running anti-malware software run current versions that include patches, builds, signature identification, and heuristic patterns?
(RM-1696) Does supplier lack an explicit policy for running anti-malware software on information systems used for software supply (product) manufacture?
(RM-1697) Does supplier lack an explicit policy for managing anti-malware software on information systems used for software supply (product) manufacture?
(RM-1698) Does supplier have an explicit policy for managing anti-malware software on information systems used for software supply (product) manufacture that lacks a requirement for running the latest version?
(RM-1699) Does the supplier lack explicitly defined procedures for updating anti-malware software on information systems used for software supply (product) manufacture?

(RF-311) Weak identification and authentication controls on manufacturer information systems used for supply (product) manufacture.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to weak identification and authentication controls on information systems used for its manufacture.

Possible Measures:

(RC-8) Supply Hygiene Risks in Table Form

(RM-667) Do the product manufacturer's information systems implement identification and authentication controls consistent with identification and authentication control IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) described in NIST SP 800-53r4?

Level 4

(RC-532) Inadequate supply (product) data security protection

Definition: Risks affecting the ability of a supply (product) to maintain its intended security properties due to inadequate security protections for data relevant to its manufacture.

(RF-306) Sensitive information in digital form relevant to supply (product) manufacture not encrypted while in physical transit either to or from supply (product) manufacturer.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information in digital form while in physical transit either to or from printed circuit board manufacturer.

Possible Measures:
(RM-662) Is sensitive information related to the manufacture of the product, including product specifications and architecture designs, encrypted while in physical transit between the manufacturer and any other point?
(RM-1708) Does supplier lack an explicit encryption standard for information relevant to supply (product) manufacture while in physical transit?

(RF-292) Inadequate protection for controlled unclassified information on information systems used for supply (product) manufacture.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to inadequate protection for controlled unclassified information on information systems used for its manufacture.

Possible Measures:
(RM-652) Does the product manufacturer implement NIST SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations?
(RM-1709) Does the supplier lack an explicit information classification policy for information on information systems used for supply (product) manufacture?
(RM-1710) Does the supplier lack explicitly defined procedures for handling different classifications of information on information systems used for supply (product) manufacture?

(RF-307) Sensitive information relevant to supply (product) manufacture not encrypted while in electronic transit either to or from supply (product) manufacturer information systems

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information while in electronic transit either to or from information systems used for its manufacture.

Possible Measures:
(RM-663) Is sensitive information related to the manufacture of the product, including product specifications and architecture designs, encrypted while in electronic transit between the manufacturer and any other point?
(RM-1711) Does supplier lack an explicit encryption standard for information relevant to supply (product) manufacture while in electronic transit?

(RC-8) Supply Hygiene Risks in Table Form

(RF-308) Sensitive information stored on information systems used for supply (product) manufacture not encrypted.

Definition: This risk considers how a supply (product) may be unable to maintain its security properties due to lack of encryption of sensitive information stored on information systems used for its manufacture.

Possible Measures:
(RM-664) Is sensitive information related to product manufacturing, including product specifications and architecture designs, stored encrypted on the product manufacturer's information systems?
(RM-1712) Does supplier lack an explicit encryption standard for information relevant to supply (product) manufacture while stored on information systems used for supply (product) manufacture?

Level 3

(RC-201) Supply (product) quality risks

Definition: Risks affecting the ability of a supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 4

(RC-215) Supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of a supply (product) to meet quality standards.

Level 5

(RC-474) Foodstuff supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of a foodstuff supply (product) to meet quality standards.

(RC-473) Pharma supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of a pharma supply (product) to meet quality standards.

(RC-234) ICT hardware supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of an ICT hardware supply (product) to meet quality standards.

(RF-284) ICT hardware fails to meet requirements

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:
(RM-89) Does the quality of the hardware meet the stated contractual requirements?
(RM-149) Are there any reported hardware failure incidents (through GIDEP Failure Experience reports or other reporting sources)?
(RM-649) Does the ICT hardware fail to meet the stated contractual requirements?

(RF-613) ICT hardware requirements lack structured test and evaluation

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to a lack of structured test and evaluation of requirements.

Possible Measures:

(RF-612) ICT hardware requirements lack explicit documentation

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:

Level 6

(RC-237) ICT hardware board supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of an ICT hardware board supply (product) to meet quality standards.

(RC-8) Supply Hygiene Risks in Table Form

(RF-608) ICT hardware board requirements lack structured test and evaluation

Definition: This risk considers how an ICT hardware board supply (product) may fail to meet quality standards due to a lack of structured test and evaluation of requirements.

Possible Measures:

(RF-66) ICT hardware boards fail to meet requirements

Definition: This risk considers how an ICT hardware board supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:
(RM-145) Does the quality of the boards in question meet the stated contractual requirements?

(RF-607) ICT hardware board requirements lack explicit documentation

Definition: This risk considers how an ICT hardware board supply (product) may fail to meet quality standards due to a lack of explicitly specified requirements.

Possible Measures:
(RM-1713) Does the supplier lack explicit documented requirements for the ICT hardware board supply(product)?

Level 6

(RC-45) ICT hardware device supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of an ICT hardware chip supply (product) to meet quality standards.

(RF-65) ICT hardware device fails to meet requirements

Definition: This risk considers how an ICT hardware device supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:

(RF-611) ICT hardware device requirements lack structured test and evaluation

Definition: This risk considers how an ICT hardware device supply (product) may fail to meet quality standards due to a lack of structured test and evaluation of requirements.

Possible Measures:

(RF-610) ICT hardware device requirements lack explicit documentation

Definition: This risk considers how an ICT hardware device supply (product) may fail to meet quality standards due to a lack of explicitly specified requirements.

Possible Measures:
(RM-1714) Does the supplier lack explicit documented requirements for the ICT hardware device supply(product)?

Level 5

(RC-232) Software supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of a software supply (product) to meet quality standards.

(RF-280) Software fails to meet requirements

Definition: This risk considers how a software supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:
(RM-169) Does the software meet the stated contractual obligations?

(RF-618) Software requirements lack explicit documentation

Definition: This risk considers how a software supply (product) may fail to meet quality standards due to a lack of explicitly specified requirements.

Possible Measures:
(RM-1716) Does the supplier lack explicit documented requirements for the software supply(product)?

(RC-8) Supply Hygiene Risks in Table Form

(RF-619) Software requirements lack structured test and evaluation

Definition: This risk considers how a software supply (product) may fail to meet quality standards due to a lack of structured test and evaluation of requirements.

Possible Measures:

Level 6

(RC-233) Software (firmware/bitstream) supply (product) quality requirements risks

Definition: Risks that inadequate requirements specification, management, evaluation or conformance will negatively affect the ability of a software (firmware/bitstream) supply (product) to meet quality standards.

(RF-615) Firmware/bitstream software requirements lack explicit documentation

Definition: This risk considers how a software (firmware/bitstream) supply (product) may fail to meet quality standards due to a lack of explicitly specified requirements.

Possible Measures:
(RM-1717) Does the supplier lack explicit documented requirements for the firmware/bitstream software supply(product)?

(RF-74) Firmware/bitstream software fails to meet requirements

Definition: This risk considers how a software (firmware/bitstream) supply (product) may fail to meet quality standards due to its failure to meet requirements.

Possible Measures:
(RM-135) Are there any reported firmware/bitstream incidents (through GIDEP or other reporting sources)?
(RM-168) Does the firmware/bitstream meet the stated contractual obligations/requirements?

(RF-616) Firmware/bitstream software requirements lack structured test and evaluation

Definition: This risk considers how a software (firmware/bitstream) supply (product) may fail to meet quality standards due to a lack of structured test and evaluation of requirements.

Possible Measures:

Level 4

(RC-217) Software supply (product) quality risks

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 5

(RC-87) Inadequate software consistency

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate consistency.

(RF-126) Are there quantitative accuracy requirements stated in the paper documentation for all software I/O operations?

Definition: currently under review

Possible Measures:
(RM-240) Does the paper documentation universally contain quantitative accuracy requirements for all software I/O operations?
(RM-241) Does the paper documentation consistently (but not to a defined standard) contain quantitative accuracy requirements for all software I/O operations?

(RC-8) Supply Hygiene Risks in Table Form

(RF-122) Is there a definition of standard I/O handling in the paper documentation?

Definition: currently under review

Possible Measures:
(RM-232) Is there a definition of standard I/O handling present and usage consistent throughout documentation?
(RM-233) Is there a definition of standard I/O handling present but usage inconsistent in documentation?

(RF-125) Does the paper documentation establish software accuracy requirements for all operations?

Definition: currently under review

Possible Measures:
(RM-238) Does the paper documentation establish/describe consistent software accuracy requirements for all operations?
(RM-239) Does the paper documentation establish/describe software accuracy requirements inconsistently or not for all operations?

(RF-117) Are there consistent software global, unit, and data type definitions?

Definition: currently under review

Possible Measures:
(RM-221) Do all programmers use both consistent and distinguishable global, unit and data type definition conventions?
(RM-222) Does at least one (but not all) programmer use both consistent and distinguishable global, unit and data type definition conventions?
(RM-223) Does at least one (but not all) programmer use either consistent or distinguishable (but not both) global, unit and data type definition conventions?

(RF-132) Are naming standards consistent across code languages (i.e., SQL, GUI, Ada, C, and FORTRAN)?

Definition: currently under review

Possible Measures:
(RM-255) Is 100% of all code leveraging consistent naming standards across code languages?
(RM-256) Is >=90% but <100% of all code leveraging consistent naming standards across code languages?
(RM-257) Is >=50% but <90% of all code leveraging consistent naming standards across code languages?

(RF-124) Is there a standard for software function naming in the paper documentation?

Definition: currently under review

Possible Measures:
(RM-236) Are software function standards present and usage/coverage consistent throughout documentation?
(RM-237) Are software function standards present but usage/coverage inconsistent throughout documentation?

(RF-129) Are naming standards consistent across software inter-process communication (IPC) calls?

Definition: currently under review

Possible Measures:
(RM-247) Is the ratio of the number of pairs of software IPC-interacting modules with inconsistent naming conventions to the number of pairs of software IPC-interacting modules examined >= .65?
(RM-248) Is the ratio of the number of pairs of software IPC-interacting modules with inconsistent naming conventions to the number of pairs of software IPC-interacting modules examined > .35 and < .65?
(RM-249) Is the ratio of the number of pairs of software IPC-interacting modules with inconsistent naming conventions to the number of pairs of software IPC-interacting modules examined <= .35?

(RF-121) Is there a representation of the software design in the paper documentation?

Definition: currently under review

Possible Measures:
(RM-230) Does the paper documentation contain a detailed software design?
(RM-231) Does the paper documentation contain a high-level but not detailed software design?

(RC-8) Supply Hygiene Risks in Table Form

(RF-130) Is the software implemented in accordance with its design documentation? Definition: currently under review Possible Measures: (RM-250) Is the software implemented in accordance to a detailed software design specified in documentation? (RM-251) Is the software implemented in accordance to a high-level but not detailed software design specified in documentation?
(RF-127) Are there quantitative accuracy requirements stated in the paper documentation for all constants? Definition: currently under review Possible Measures: (RM-242) Does the documentation universally contain quantitative accuracy requirements stated for all constants? (RM-243) Does the documentation consistently (but with no standard defined) contain quantitative accuracy requirements stated for all constants?
(RF-120) Is there a consistent implementation of external I/O protocol and format for all code units? Definition: currently under review Possible Measures: (RM-225) Do all programmers use both consistent and distinguishable external I/O protocol and format conventions in code implementation? (RM-226) Does at least one (but not all) programmer use both consistent and distinguishable external I/O protocol and format conventions in code implementation? (RM-229) Does at least one (but not all) programmer use consistent or distinguishable (but not both) external I/O protocol and format conventions in code implementation?
(RF-116) Are software code naming conventions consistent for functional groupings? Definition: currently under review Possible Measures: (RM-56) Do all programmers use names that are both distinguishable and consistent within functional groupings? (RM-88) Does at least one programmer (but not all programmers) use names that are both distinguishable and consistent within functional groupings? (RM-92) Does at least one programmer use names that either distinguishable or consistent but not both within functional groupings?
(RF-131) Are naming conventions consistent for software data types (e.g., constant, Boolean) etc.? Definition: currently under review Possible Measures: (RM-252) Is 100% of all code leveraging consistent naming conventions for software data types? (RM-253) Is >=90% but <100% of all code leveraging consistent naming conventions for software data types? (RM-254) Is >=50% but <90% of all code leveraging consistent naming conventions for software data types?
(RF-123) Are data naming standards specified in the paper documentation? Definition: currently under review Possible Measures: (RM-234) Are data naming standards present and usage/coverage consistent throughout documentation? (RM-235) Are data naming standards present but usage/coverage inconsistent in documentation?
(RF-128) Are the naming conventions in the software code consistent for usage (e.g., I/O)? Definition: currently under review Possible Measures: (RM-245) Are all software naming conventions consistently implemented following a standard appropriate for usage? (RM-246) Are all software naming conventions consistently implemented appropriate for usage but not following a defined standard?

(RC-8) Supply Hygiene Risks in Table Form

Level 5

(RC-37) Inadequate software design simplicity

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate design simplicity.

(RF-190) Is the code segmented into procedure bodies that can be understood easily?

Definition: currently under review

Possible Measures:
(RM-396) Are 100% of code procedure bodies less than two pages and less than 50 lines per page?
(RM-397) Are >=80% but <100% of code procedure bodies less than two pages?
(RM-398) Are >=50% but <800% of code procedure bodies less than two pages?

(RF-194) Do all Boolean expressions in the code avoid referring to both a predicate and its complement?

Definition: currently under review

Possible Measures:
(RM-408) Is the ratio of the number of mixed predicate (referring to both a predicate and its complement) boolean expressions to the total number of boolean expressions >= .65?
(RM-409) Is the ratio of the number of mixed predicate (referring to both a predicate and its complement) boolean expressions to the total number of boolean expressions > .35 and < .65?
(RM-410) Is the ratio of the number of mixed predicate (referring to both a predicate and its complement) boolean expressions to the total number of boolean expressions <= .35?

(RF-189) Is the software database (DB) interaction properly isolated?

Definition: currently under review

Possible Measures:
(RM-394) Are all software database (DB) interactions isolated in one functional group?
(RM-395) Are all software database (DB) interactions restricted to a few areas but not isolated in one functional group?

(RF-193) Have all Boolean expressions in the code been parenthesized to clarify mixed operator evaluations?

Definition: currently under review

Possible Measures:
(RM-405) Is the ratio of the number of convoluted (non-clearly parenthesized) boolean expressions in the code to the total number of boolean expressions in the code >= .65?
(RM-406) Is the ratio of the number of convoluted (non-clearly parenthesized) boolean expressions in the code to the total number of boolean expressions in the code > .35 and < .65?
(RM-407) Is the ratio of the number of convoluted (non-clearly parenthesized) boolean expressions in the code to the total number of boolean expressions in the code <= .35?

(RF-188) Is the source code of low complexity (e.g., McCabe Cyclomatic…)?

Definition: currently under review

Possible Measures:
(RM-391) Is the normalized average software cyclomatic complexity for all functions and procedures >= .65?
(RM-392) Is the normalized average software cyclomatic complexity for all functions and procedures > .35 and < .65?
(RM-393) Is the normalized average software cyclomatic complexity for all functions and procedures <= .35?

(RF-187) Do all software modules have singular entry and exit and avoid unconditional branching internally?

Definition: currently under review

Possible Measures:
(RM-388) Is the normalized average software flow complexity for all functions and procedures >= .65?
(RM-389) Is the normalized average software flow complexity for all functions and procedures > .35 and < .65?
(RM-390) Is the normalized average software flow complexity for all functions and procedures <= .35?

(RC-8) Supply Hygiene Risks in Table Form

(RF-184) Does the code avoid making non-linear jumps into or out of loops?

Definition: currently under review

Possible Measures:
(RM-379) Is the ratio of non-linear code jumps into or out of loops to total jumps >= .65?
(RM-380) Is the ratio of non-linear code jumps into or out of loops to total jumps > .35 and < .65?
(RM-381) Is the ratio of non-linear code jumps into or out of loops to total jumps <= .35?

(RF-191) Is all use of self-modifying code fully documented and justified?

Definition: currently under review

Possible Measures:
(RM-399) Is the ratio of the number of incompletely documented and justified instances of self-modifying code to the total occurrences of self-modifying code >= .65?
(RM-400) Is the ratio of the number of incompletely documented and justified instances of self-modifying code to the total occurrences of self-modifying code > .35 and < .65?
(RM-401) Is the ratio of the number of incompletely documented and justified instances of self-modifying code to the total occurrences of self-modifying code <= .35?

(RF-186) Do all software inter-process communications (IPCs) communicate over unique channels?

Definition: currently under review

Possible Measures:
(RM-385) Is the ratio of the number of reused IPC channels to the number of IPC channels >= .65?
(RM-386) Is the ratio of the number of reused IPC channels to the number of IPC channels > .35 and < .65?
(RM-387) Is the ratio of the number of reused IPC channels to the number of IPC channels <= .35?

(RF-185) Does the code avoid modifying loop indices?

Definition: currently under review

Possible Measures:
(RM-382) Is the ratio of code loop indices modifications to number of looping constructs >= .65?
(RM-383) Is the ratio of code loop indices modifications to number of looping constructs > .35 and < .65?
(RM-384) Is the ratio of code loop indices modifications to number of looping constructs <= .35?

(RF-192) Have all software procedures been structured to avoid excessive nesting?

Definition: currently under review

Possible Measures:
(RM-402) Is the ratio of 13 to the sum of the average nesting level squared and the standard deviation squared >= .65?
(RM-403) Is the ratio of 13 to the sum of the average nesting level squared and the standard deviation squared > .35 and < .65?
(RM-404) Is the ratio of 13 to the sum of the average nesting level squared and the standard deviation squared <= .35?

Level 5

(RC-42) Inadequate software independence

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate independence.

(RF-135) Are the languages and interface libraries selected standardized and portable (i.e., ANSI…)?

Definition: currently under review

Possible Measures:
(RM-264) Is the ratio of standard languages to total languages >= .65?
(RM-265) Is the ratio of standard languages to total languages > .35 and < .65?
(RM-266) Is the ratio of standard languages to total languages <= .35?

(RC-8) Supply Hygiene Risks in Table Form

(RF-134) Are system dependent functions, etc., in stand-alone modules (not embedded in the code)?

Definition: currently under review

Possible Measures:
(RM-261) Is the ratio of dependencies embedded in code (not stand-alone modules) to total dependencies >= .65?
(RM-262) Is the ratio of dependencies embedded in code (not stand-alone modules) to total dependencies > .35 and < .65?
(RM-263) Is the ratio of dependencies embedded in code (not stand-alone modules) to total dependencies <= .35?

(RF-133) Is the software free of machine, operating system, and vendor specific extensions?

Definition: currently under review

Possible Measures:
(RM-258) Does the software contain zero instances of machine, operating system or vendor specific extensions?
(RM-259) Do < 10% of the software packages contain machine, operating system or vendor specific extensions?
(RM-260) Do >= 10% and < 50% of the software packages contain machine, operating system or vendor specific extensions?

(RF-138) Are the commercial software components available on other platforms in the same level of functionality?

Definition: currently under review

Possible Measures:
(RM-271) Is the ratio of number of commercial software components not available on other platforms in the same level of functionality to the number of dependencies on commercial software components >= .65?
(RM-272) Is the ratio of number of commercial software components not available on other platforms in the same level of functionality to the number of dependencies on commercial software components > .35 and < .65?
(RM-273) Is the ratio of number of commercial software components not available on other platforms in the same level of functionality to the number of dependencies on commercial software components <= .35?

(RF-136) Does the software avoid the need for any unique compilation in order to run (e.g., a custom post processor to "tweak" the code to run on machine X)?

Definition: currently under review

Possible Measures:
(RM-267) Is 100% of all code compiled/compilable without any unique requirements in order to run (e.g., a custom post processor to "tweak" the code to run on machine X)?
(RM-268) Is >=90% but <100% of all code compiled/compilable without any unique requirements in order to run (e.g., a custom post processor to "tweak" the code to run on machine X)?
(RM-269) Is >=50% but <90% of all code compiled/compilable without any unique requirements in order to run (e.g., a custom post processor to "tweak" the code to run on machine X)?

(RF-137) Runtime independence of generated code

Definition: currently under review

Possible Measures:
(RM-270) Is the generated code (i.e., GUI Builders) able to run without a specific support runtime component?

(RF-140) Does the software code avoid all usage of specific pathnames/filenames?

Definition: currently under review

Possible Measures:
(RM-274) Is the ratio of the number of software packages containing literal pathname dependencies to the number of software packages using file I/O >= .65?
(RM-275) Is the ratio of the number of software packages containing literal pathname dependencies to the number of software packages using file I/O > .35 and < .65?
(RM-276) Is the ratio of the number of software packages containing literal pathname dependencies to the number of software packages using file I/O <= .35?

(RC-8) Supply Hygiene Risks in Table Form

(RF-141) Is the software data representation machine independent?

Definition: currently under review

Possible Measures:
(RM-277) Are 100% of software packages free of the use of byte packing, assumptions on integer length, and assumptions on the structure of strings?
(RM-278) Are >=90% but <100% of software packages free of the use of byte packing, assumptions on integer length, and assumptions on the structure of strings?
(RM-279) Are >=50% but <90% of software packages free of the use of byte packing, assumptions on integer length, and assumptions on the structure of strings?

Level 5

(RC-40) Inadequate software documentation

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate documentation.

(RF-160) Does the documentation explain the high level functionality of the system?

Definition: currently under review

Possible Measures:
(RM-320) Does the documentation contain a detailed explanation of the high-level functionality of the system?
(RM-321) Does the documentation contain some information (but not detailed, consistent or full coverage) regarding the high level functionality of the system?

(RF-151) Is the documentation structured per the development plan?

Definition: currently under review

Possible Measures:
(RM-301) Is there good correlation between the documentation and its intended structure per the development plan?
(RM-302) Is there loose (but not good) correlation between the documentation and its intended structure per the development plan?

(RF-163) Are the high-level flows of data into, out of, and through the system detailed?

Definition: currently under review

Possible Measures:
(RM-326) Does the documentation contain good detail of the high-level flows of data into, out of, and through the system?
(RM-327) Does the documentation contain some information (but not detailed, consistent or full coverage) regarding the high-level flows of data into, out of, and through the system?

(RF-162) Are external software interfaces and systems depicted in the documentation?

Definition: currently under review

Possible Measures:
(RM-324) Does the documentation contain good depicted detail of all external software interfaces and systems?
(RM-325) Does the documentation contain some depicted information (but not detailed, consistent or full coverage) regarding any external software interfaces and systems?

(RF-157) Does the documentation contain comprehensive descriptions of all internal software operations?

Definition: currently under review

Possible Measures:
(RM-314) Does the documentation contain detailed comprehensive descriptions of all internal software operations?
(RM-315) Does the documentation contain some (but not detailed, consistent or full coverage) descriptions of all internal software operations?

(RC-8) Supply Hygiene Risks in Table Form

(RF-159) Does the paper documentation establish a requirement for commenting global data within a software unit to show where the data is derived, the data composition, and how the data is used? Definition: currently under review Possible Measures: (RM-318) Does the documentation establish a detailed requirement for commenting global data within a software unit to show where the data is derived, the data composition, and how the data is used? (RM-319) Does the documentation contain some information (but not detailed, consistent or full coverage) establishing a requirement for commenting global data within a software unit to show where the data is derived, the data composition, and how the data is used?
(RF-166) Are all software environmental variables and the default values clearly defined? Definition: currently under review Possible Measures: (RM-332) Is the ratio of the number of software environment variables that are not well defined with default values to the total number of software environment variables >= .65? (RM-333) Is the ratio of the number of software environment variables that are not well defined with default values to the total number of software environment variables > .35 and < .65? (RM-334) Is the ratio of the number of software environment variables that are not well defined with default values to the total number of software environment variables <= .35?
(RF-161) Does the documentation layout the functional allocation of the system to Computer Program Configuration Items (CPCIs)? Definition: currently under review Possible Measures: (RM-322) Does the documentation contain good detail of the functional allocation of the system to Computer Program Configuration Items (CPCIs)? (RM-323) Does the documentation contain some information (but not detailed, consistent or full coverage) regarding the functional allocation of the system to Computer Program Configuration Items (CPCIs)?
(RF-153) Does the design documentation depict data flow? Definition: currently under review Possible Measures: (RM-306) Does the documentation contain detailed design depictions of data flow? (RM-307) Does the documentation contain some (but not detailed, consistent or full coverage) design depictions of data flow?
(RF-165) Are all software inputs, process and outputs adequately defined in the documentation? Definition: currently under review Possible Measures: (RM-330) Are all software inputs, process and outputs defined in detail in the documentation? (RM-331) Are all software inputs, process and outputs defined at a high level but not in detail in the documentation?
(RF-158) Does the documentation contain comprehensive descriptions and justification of all software esoteric processing methods? Definition: currently under review Possible Measures: (RM-316) Does the documentation contain detailed comprehensive descriptions and justification of all esoteric processing methods OR does the software contain no software esoteric processing methods? (RM-317) Does software contain software esoteric processing methods and the documentation contain some (but not detailed, consistent or full coverage) comprehensive descriptions and justification of any software esoteric processing methods?

(RC-8) Supply Hygiene Risks in Table Form

(RF-152) Does the design documentation depict control flow to the CSU/CSC level?

Definition: currently under review

Possible Measures:
(RM-303) Does the documentation contain good detailed design depictions of control flow to the CSU/CSC level?
(RM-304) Does the documentation contain some detailed (but not highly detailed, consistent or full coverage) design depictions of control flow to the CSU/CSC level?
(RM-305) Does the documentation contain high-level only (but not detailed, consistent or full coverage) design depictions of control flow to the CSU/CSC level?

(RF-155) Is the documentation adequately indexed (functionality can be easily located in the code)?

Definition: currently under review

Possible Measures:
(RM-310) Does the documentation contain detailed indexing (functionality can be easily located in the code)?
(RM-311) Does the documentation contain some (but not detailed, consistent or full coverage) indexing (functionality can be easily located in the code)?

(RF-164) Does the documentation discuss/rationalize the usage of COTS, GOTS, and OS services?

Definition: currently under review

Possible Measures:
(RM-328) Does the documentation contain good detailed discussion/rationalization for the usage of COTS, GOTS, and OS services OR does the product contain no COTS, GOTS, or OS services?
(RM-329) Does the documentation contain some (but not detailed, consistent or full coverage) discussion/rationalization for the usage of COTS, GOTS, and OS services?

(RF-156) Does the documentation contain comprehensive descriptions of all system/software interfaces?

Definition: currently under review

Possible Measures:
(RM-312) Does the documentation contain detailed comprehensive descriptions of all system/software interfaces?
(RM-313) Does the documentation contain some (but not detailed, consistent or full coverage) descriptions of all system/software interfaces?

(RF-154) Do the design documents depict the task and system initialization hierarchy/relationships?

Definition: currently under review

Possible Measures:
(RM-308) Does the documentation contain detailed design depictions of the task and system initialization hierarchy/relationships?
(RM-309) Does the documentation contain some (but not detailed, consistent or full coverage) design depictions of the task and system initialization hierarchy/relationships?

Level 5

(RC-251) Inadequate software pedigree/provenance

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate tracking, management and transparency of pedigree/provenance.

(RF-312) Geopolitical concerns regarding software pedigree/provenance

Definition: This risk considers how a software supply (product) may fail to meet quality standards due to pedigree/provenance concerns relevant to the political considerations of particular geolocations.

Possible Measures:
(RM-196) Does the software contain code developed or modified in a particular country in violation of contractual restrictions?
(RM-668) Does the software contain code developed or modified in a country of concern?

Level 5

(RC-39) Inadequate software anomaly control

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate anomaly control.

(RF-179) Is the vendor's standard implementation of error handling consistently applied?

Definition: currently under review

Possible Measures:
(RM-369) Is an error handling standard defined and is it consistently followed in implementation?

(RC-8) Supply Hygiene Risks in Table Form

(RM-370) Is error handling implemented consistently but no error handling standard defined?

(RF-183) Are tasking and rendezvous exceptions handled in an orderly fashion?

Definition: currently under review

Possible Measures:
(RM-377) Does the system provide error handling and/or graceful exit for socket unavailability, corrupted data, AND unexpected process termination conditions?
(RM-378) Does the system provide error handling and/or graceful exit for some subset of but not all of the following conditions: socket unavailability, corrupted data, OR unexpected process termination?

(RF-180) Is there a defined statement of techniques for software error handling in the paper documentation?

Definition: currently under review

Possible Measures:
(RM-371) Is there a documented standard statement of techniques for software error handling?
(RM-372) Is there consistently documented techniques (with no defined standard) for software error handling?

(RF-182) Is the vendor's standard implementation of software input data handling consistently applied?

Definition: currently under review

Possible Measures:
(RM-375) Does the code consistently implement a documented standard for input data tolerance techniques?
(RM-376) Does the code consistently implement documented input data tolerance techniques without a specific documented standard?

(RF-181) Is there a defined statement of techniques for tolerance of input data in the paper documentation?

Definition: currently under review

Possible Measures:
(RM-373) Is there a documented standard for techniques for tolerance of input data?
(RM-374) Do techniques for tolerance of input data appear consistent but no explicit standard is defined?

Level 5

(RC-38) Inadequate software modularity

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate modularity.

(RF-143) Do the functional groupings of software units avoid calling units outside their functional area?

Definition: currently under review

Possible Measures:
(RM-282) Do the functional groupings of units strongly and consistently avoid calling units outside their functional area?
(RM-283) Do the functional groupings of units generally, but not strongly and consistently, avoid calling units outside their functional area?

(RF-144) Are machine dependent and I/O functions isolated and encapsulated?

Definition: currently under review

Possible Measures:
(RM-284) Is the ratio of multifunction software packages to total number of software packages containing ties to the system >= .65?
(RM-285) Is the ratio of multifunction software packages to total number of software packages containing ties to the system > .35 and < .65?
(RM-286) Is the ratio of multifunction software packages to total number of software packages containing ties to the system <= .35?

(RC-8) Supply Hygiene Risks in Table Form

(RF-146) Has code been structured to minimize coupling to global variables?

Definition: currently under review

Possible Measures:
(RM-289) Is the ratio of global variables in the software code to total variables in the software code >= .65?
(RM-290) Is the ratio of global variables in the software code to total variables in the software code > .35 and < .65?
(RM-291) Is the ratio of global variables in the software code to total variables in the software code <= .35?

(RF-142) Is the structure of the software design hierarchical in a top down design within tasking threads?

Definition: currently under review

Possible Measures:
(RM-280) Does the implemented code follow a crisp design hierarchy?
(RM-281) Does the implemented code follow a discernible but not crisp design hierarchy?

(RF-167) Are software symbolic constants defined in an isolated and centralized area?

Definition: currently under review

Possible Measures:
(RM-335) Is the ratio of the number of software packages using scattered symbolic constant definitions to the number of software packages defining symbolic constants >= .65?
(RM-336) Is the ratio of the number of software packages using scattered symbolic constant definitions to the number of software packages defining symbolic constants > .35 and < .65?
(RM-337) Is the ratio of the number of software packages using scattered symbolic constant definitions to the number of software packages defining symbolic constants <= .35?

(RF-145) Are all variables used exclusively for their declared purposes?

Definition: currently under review

Possible Measures:
(RM-287) Are 100% of all declared variables only ever used for their declared purposes?
(RM-288) Are > 95% but < 100% of all declared variables only ever used for their declared purposes?

(RF-150) Have software symbolic constants been used in place of explicit ones?

Definition: currently under review

Possible Measures:
(RM-298) Is the ratio of the number of instances of use of explicit constants to the total number of defined constants >= .65?
(RM-299) Is the ratio of the number of instances of use of explicit constants to the total number of defined constants > .35 and < .65?
(RM-300) Is the ratio of the number of instances of use of explicit constants to the total number of defined constants <= .35?

(RF-148) Are all commercial software interfaces & APIs, other than GUI Builders, isolated and encapsulated?

Definition: currently under review

Possible Measures:
(RM-293) Are all interactions with COTS interfaces implemented by the application calling the COTS interfaces?
(RM-294) Are interactions with COTS interfaces implemented by the application usually but not always calling the COTS interfaces?

(RF-147) Modification protection of interpreted code bodies (shell scripts and 4GL scripts)

Definition: currently under review

Possible Measures:
(RM-292) Are interpreted code bodies (shell scripts and 4GL scripts) protected from accidental or deliberate modification?

(RC-8) Supply Hygiene Risks in Table Form

(RF-149) Do all software functional procedures represent one function (one-to-one function mapping)?

Definition: currently under review

Possible Measures:
(RM-295) Do 100% of functional code procedures adhere to one-to-one function mapping (all functional procedures represent one function)?
(RM-296) Do >=90% and < 100% of functional code procedures adhere to one-to-one function mapping (all functional procedures represent one function)?
(RM-297) Do >=50% and < 90% of functional code procedures adhere to one-to-one function mapping (all functional procedures represent one function)?

Level 5

(RC-41) Inadequate software self-descriptiveness

Definition: Risks affecting the ability of a software supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to inadequate self-descriptiveness.

(RF-171) Is a standard format for organizations of modules implemented consistently?

Definition: currently under review

Possible Measures:
(RM-345) Are 100% of all software modules implemented conformant to a standard format for organization?
(RM-346) Are >=90% and < 100% of all software modules implemented conformant to a standard format for organization?
(RM-347) Are >=50% and < 90% of all software modules implemented conformant to a standard format for organization?

(RF-169) Does the software documentation standard prologue provide the following information: module name; version number; author; date; purpose; function; assumptions; limitations and restrictions; accuracy requirements; error handling; and COTS dependencies?

Definition: currently under review

Possible Measures:
(RM-339) Does the software documentation standard prologue provide the following information: module name; version number; author; date; purpose; function; assumptions; limitations and restrictions; accuracy requirements; error handling; and COTS dependencies?
(RM-340) Does the software documentation standard prologue provide the following information: module name; version number; author; date; purpose; function; assumptions; limitations and restrictions; but does not contain accuracy requirements; error handling; and COTS dependencies?
(RM-341) Does the software documentation standard prologue provide the following information: module name; version number; author; date; purpose; function; but does not contain assumptions; limitations and restrictions; accuracy requirements; error handling; and COTS dependencies?

(RF-172) Are comments set off from code and of consistent style throughout?

Definition: currently under review

Possible Measures:
(RM-348) Are 100% of comments in software set off from code and of consistent style throughout?
(RM-349) Are >=90% and < 100% of comments in software set off from code and of consistent style throughout?
(RM-350) Are >=50% and < 90% of comments in software set off from code and of consistent style throughout?

(RF-178) Do code generation tools (screen builders, DB query tools, etc.) produce reusable "source code" that is documented?

Definition: currently under review

Possible Measures:
(RM-367) Is "source code" generated from code generation tools both maintainable and documented?
(RM-368) Is "source code" generated from code generation tools either maintainable or documented (but not both)?

(RF-175) Has white space been managed for legibility and to allow identification of nesting constructs?

Definition: currently under review

Possible Measures:
(RM-358) Is 100% of white space in code managed for legibility and to allow identification of nesting constructs?
(RM-359) Is >=90% and < 100% of white space in code managed for legibility and to allow identification of nesting constructs?
(RM-360) Is >=50% and < 90% of white space in code managed for legibility and to allow identification of nesting constructs?

(RF-173) Are comments accurate and describe the "what's and whys?"

Definition: currently under review

Possible Measures:
(RM-351) Are 100% of comments in software accurate and describe the "what's and whys?'?

(RC-8) Supply Hygiene Risks in Table Form

(RM-352) Are >=90% and < 100% of comments in software accurate and describe the “what’s and whys?'?
(RM-354) Are >=50% and < 90% of comments in software accurate and describe the “what’s and whys?'?

(RF-176) Are function and variable names helpful in understanding the functionality of the code?

Definition: currently under review

Possible Measures:
(RM-361) Are 100% of function and variable names helpful in understanding the functionality of the code?
(RM-362) Are >=90% and < 100% of function and variable names helpful in understanding the functionality of the code?
(RM-363) Are >=50% and < 90% of function and variable names helpful in understanding the functionality of the code?

(RF-170) Is a standard prologue consistently implemented in code?

Definition: currently under review

Possible Measures:
(RM-342) Do 100% of software modules implement a standard prologue?
(RM-343) Do >=90% but <100% of software modules implement a standard prologue?
(RM-344) Do >=50% but <90% of software modules implement a standard prologue?

(RF-174) Are inputs, outputs and side effects (if any) clearly detailed for each software procedure?

Definition: currently under review

Possible Measures:
(RM-355) Do 100% of software procedures clearly detail all inputs, outputs and side effects (if any)?
(RM-356) Do >=90% but <100% of software procedures clearly detail all inputs, outputs and side effects (if any)?
(RM-357) Do >=50% but <90% of software procedures clearly detail all inputs, outputs and side effects (if any)?

(RF-177) Is any and all dead code clearly offset and the reason for its existence documented?

Definition: currently under review

Possible Measures:
(RM-364) Is the ratio of the amount of unjustified/hidden dead code to the amount of existing dead code >= .65?
(RM-365) Is the ratio of the amount of unjustified/hidden dead code to the amount of existing dead code > .35 and < .65?
(RM-366) Is the ratio of the amount of unjustified/hidden dead code to the amount of existing dead code <= .35?

(RF-168) Specification of standard prologue in documentation

Definition: currently under review

Possible Measures:
(RM-338) Does the documentation specify a standard prologue?

Level 4

(RC-484) Pharma supply (product) quality risks

Definition: Risks affecting the ability of a pharma supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

(RC-485) Foodstuff supply (product) quality risks

Definition: Risks affecting the ability of a foodstuff supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

(RC-464) Hardware supply (product) quality risks

Definition: Risks affecting the ability of a hardware supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

Level 5

(RC-216) ICT hardware supply (product) quality risks

Definition: Risks affecting the ability of an ICT hardware supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements.

(RF-599) ICT hardware supply (product) does not hold up to stress or environmental testing

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due failure to function as expected under stress or environmental testing.

(RC-8) Supply Hygiene Risks in Table Form

Possible Measures:
(RM-1718) Does the supplier lack explicit reliability, durability, and resilience requirements for the ICT hardware supply (product)?
(RM-1719) Does the supplier¬† lack an explicit policy for testing reliability, durability, and resilience requirements for the ICT hardware supply (product)?
(RM-1720) Does the supplier lack explicitly defined processes and procedures for testing reliability, durability, and resilience requirements for the ICT hardware supply (product)?

(RF-603) ICT hardware microelectronic supply (product) fails electrical parametric or property testing

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to inability to pass electrical parametric or property testing.

Possible Measures:
(RM-1724) Does the supplier lack an explicit policy for electrical parametric or property testing of the ICT hardware supply (product)?
(RM-1725) Does the supplier lack explicitly defined processes and procedures for electrical parametric or property testing of the ICT hardware supply (product)?

(RF-604) Components are improperly integrated into larger ICT hardware supply (product)

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due improper integration of components into larger ICT hardware supply (product).

Possible Measures:

(RF-598) Materials used in fabrication of ICT hardware supply (product) are not of required purity

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to the materials used in fabrication not being of required purity.

Possible Measures:
(RM-1721) Does the supplier lack explicit purity requirements for materials used in the fabrication of the ICT hardware supply (product)?
(RM-1722) Does the supplier lack an explicit policy for testing purity requirements for materials used in the fabrication of the ICT hardware supply (product)?
(RM-1723) Does the supplier lack explicitly defined processes and procedures for testing purity requirements for materials used in the fabrication of the ICT hardware supply (product)?

(RF-605) ICT hardware supply (product) contains faulty logic (fails logic testing)

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to it containing faulty logic (fails logic testing).

Possible Measures:
(RM-1726) Does the supplier lack an explicit policy for logic testing of the ICT hardware supply (product)?
(RM-1727) Does the supplier lack explicitly defined processes and procedures for electrical logic testing of the ICT hardware supply (product)?

(RF-597) ICT hardware supply (product) design process produces outside of specification components

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to an inadequate design process that produces outside of specification components.

Possible Measures:

(RF-601) Fabrication process produces too many ICT hardware supplies (products) out of control limits

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to fabrication process producing excessive out of control limits.

Possible Measures:

(RF-602) Validity of ICT hardware microelectronics supply (product)

Definition: Risks affecting the ability of an ICT hardware supply (product) to conform structurally and functionally, within expected environmental or usage parameters, to a specific expected standard or other set of requirements due to design validation issues.

Possible Measures:

(RF-600) Fabrication process produces ICT hardware supply (product) with material defects

Definition: This risk considers how an ICT hardware supply (product) may fail to meet quality standards due to faulty fabrication process producing material defects.

Possible Measures:

(RC-287) Service Quality Risks in Table Form

<table>
<tr><th colspan="6">Supply Chain Risks</th></tr>
<tr><td colspan="2"><b>(RC-1) Supplier Risks</b></td><td colspan="2">(RC-2) Supply Risks</td><td colspan="2"><b>(RC-3) Service Risks</b></td></tr>
<tr><td><b>(RC-287) Service Quality Risks</b></td><td colspan="2">(RC-289) Service Resilience Risks</td><td colspan="2">(RC-286) Service Security Risks</td><td>(RC-288) Service Integrity Risks</td></tr>
</table>

Definition: Risks related to the quality of a service delivered.

(RF-920) Subcontractor or third party is not accountable for sub-par service

Definition: Services that don’t hold their third party contractors accountable for sub-par services represent a risk to quality.

Possible Measures:

(RF-921) Service provider does not have an adequate quality assurance process.

Definition: Services that don't assess the quality of their own quality may provide sub-par service.

Possible Measures:

(RF-922) Service is oversold or oversubscribed to meet quality standards

Definition: Services that are oversold or oversubscribed represents a risk to service quality.

Possible Measures:

(RF-923) Service is not performed by sufficiently skilled personnel.

Definition: Services that are not performed by trained or experienced staff represent a risk to quality of the service in meeting obligations.

Possible Measures:

Level 3

(RC-300) Service Specific Quality Risks

Definition: Risks that increase the likelihood the quality of a service may be inadequate due to service specific quality issues.

Level 4

(RC-309) Digital Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a digital service.

(RF-932) Digital service provider does not have a regular update schedule.

Definition: With rapid changes associated with digital services, a provider must ensure that its offerings are up to date both from the perspective of compatibility, performance, reliability, and security.

Possible Measures:

Level 4

(RC-317) Transportation Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a transportation service.

(RF-938) Delays in transport of goods

Definition: Delays in transportation can result in the failure to meet customer expectations leading to loss of future business. In some cases, delated delivery can result in inventory loss (e.g., spoilage).

Possible Measures:

Level 4

(RC-329) Advertising Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of an advertising service.

(RC-287) Service Quality Risks in Table Form

(RF-926) Advertiser does not have clear performance metrics

Definition: Advertisers should be able to define and track the success of advertising campaigns. If undefined, or untracked, the advertiser may not provide the highest-quality service or may defraud its client.

Possible Measures:

(RF-928) Advertiser does not advertise on diverse collection of venues (e.g., multiple websites)

Definition: Advertisements are only effective if they are seen by possible consumers. By not advertising in a diverse set of venues, exposure to possible customers decreased.

Possible Measures:

(RF-929) Poor advertising impairs a client's effectiveness

Definition: Risk that an advertising service provider damages the reputation of a client or their products, degrades a client's market position, or undermines the goals of a client through poor advertising campaigns.

Possible Measures:

(RF-927) Advertiser does not have a robust quality control capability resulting in errors of advertising

Definition: Advertisers should render a service that is error-free and does not mislead customers or damage client reputation (e.g., distasteful jokes or inappropriate images).

Possible Measures:

Level 4

(RC-325) Brokering Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a pharmaceutical service.

(RF-930) Brokerage does not adequately vet its clients.

Definition: A broker's role is to connect two companies interested in working together. Clients should be able to trust that a broker vets its other clients' business health and product quality.

Possible Measures:

(RF-931) Poor brokering impairs a client's effectiveness.

Definition: Risk that a brokerage negatively affects the future business prospects of a client through the inability to find appropriate buyers or sellers for the client.

Possible Measures:

Level 4

(RC-572) Pharmaceutical Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a pharmaceutical service.

(RC-321) Warehousing Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a warehousing service.

(RF-939) Improper handling of warehoused goods

Definition: Improper handling of warehoused goods (e.g., storage location, temperature, humidity) can result in the degradation or destruction.

Possible Measures:
(RM-1728) Does the warehousing service provider lack explicit policy for proper handling of warehoused goods?
(RM-1729) Does the warehousing service provider lack explicitly defined processes and procedures for proper handling of warehoused goods?
(RM-1730) Does the warehousing service provider lack an explicitly defined audit process to ensure compliance with policies, processes and procedures regarding proper handling of warehoused goods?
(RM-1731) Are there open and unresolved audit findings regarding policies, processes and procedures regarding proper handling of warehoused goods?
(RM-1732) Does warehousing service provider lack an active work process underway to resolve open and unresolved audit findings regarding policies, processes and procedures regarding proper handling of warehoused goods?

(RC-287) Service Quality Risks in Table Form

Level 4

(RC-313) Manufacturing Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of a manufacturing service.

(RF-935) Manufacturing service provider does frequently assess the quality of the materials it receives from its suppliers.

Definition: A manufacturer must frequently assess the quality of the materials it receives from its suppliers as degraded quality in raw materials can result in the degraded quality of the end product.

Possible Measures:

(RF-936) Co-packing manufacturing does not meet the standard operating procedures to produce the product

Definition: Co-packing manufacturers who do not meet standard operating procedures in manufacturing the product represent a quality risk.

Possible Measures:

(RF-937) Poor manufacturing services damage a client's business

Definition: Risk that a manufacturer negatively affects the future business prospects of a client through the inability to manufacture quality goods.

Possible Measures:

(RF-934) Manufacturing service provider does not have robust QA processes

Definition: Quality assurance processes must be in place to ensure the continued delivery of products that meet client expectations.

Possible Measures:

Level 4

(RC-305) Engineering Service Specific Quality Risks

Definition: Risks that increase the likelihood of reduced quality of an engineering service.

(RF-933) Poor engineering services damage a client's business

Definition: Risk that an engineering firm damages the reputation of a client or their products, degrades the capability of a client's products or infrastructure, or creates cost and schedule overruns for a client due to poor quality engineering.

Possible Measures:

Level 3

(RC-563) Service Quality Infrastructure Pedigree Risks

Definition: Risks that increase the likelihood that the quality of a service is inadequate due to issues with the composition and certified authenticity of infrastructure necessary for the delivery of the service.

(RF-925) Service providers do not provide a full accounting of where open source components are used in service chain

Definition: Services that do not provide a full accounting of where open source components are used represent pedigree risk.

Possible Measures:
(RM-1319) Does the service provider no provide an accounting of whether open source components are used in the service chain?
(RM-1320) Does the service provider no provide a full accounting of where open source components are used in the service chain?

Level 3

(RC-562) Service Quality Infrastructure Provenance Risks

Definition: Risks that increase the likelihood the quality of a service is inadequate due to issues with the origin, evolution and chain of custody of infrastructure necessary for the delivery of the service.

(RF-924) Service provider does not consistently maintain chain of custody for service infrastructure assets affecting provenance

Definition: Services that involve the changes in the change of custody of infrastructure assets represent risk when not consistently maintained (e.g., service of securely disposing of equipment requires chain of custody of assets to disposal/wiping destruction).

Possible Measures:

(RC-287) Service Quality Risks in Table Form

Level 3

(RC-302) Service Specific Reliability Risks

Definition: Risks that increase the likelihood the reliability of a service may be inadequate due to service specific reliability issues.

Level 4

(RC-326) Brokering Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a brokering service.

(RF-988) Brokerage does not periodically assess its clients' health and offerings.

Definition: To offer a reliable service, a brokerage must ensure that the companies to which it is connecting customers are trustworthy in the delivery of their product. A client must trust that a brokering service is seeking-out reliable providers.

Possible Measures:

Level 4

(RC-306) Engineering Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of an engineering service.

(RC-314) Manufacturing Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a manufacturing service.

(RC-597) Pharmaceutical Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a pharmaceutical service.

(RF-991) Provider loses their license to provide the service (e.g., FDA, DEA, USDA license to operate/possess).

Definition: This risk considers the potential that a service provider may lose a license required to legally operate and perform the service thus impacting the reliability of the service.

Possible Measures:

Level 4

(RC-330) Advertising Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of an advertising service.

(RC-318) Transportation Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a transportation service.

(RF-989) Failure to perform appropriate vehicle maintenance according to schedule

Definition: This risk considers that not following an appropriate vehicle maintenance schedule may negatively impact the reliability of the service. (e.g. parking brake not routinely services and tested on vehicle).

Possible Measures:

Level 4

Level 3

(RC-310) Digital Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a digital service.

(RC-322) Warehousing Service Specific Reliability Risks

Definition: Risks that increase the likelihood of inadequate reliability of a warehousing service.

(RF-989) Failure to perform appropriate vehicle maintenance according to schedule

Definition: This risk considers that not following an appropriate vehicle maintenance schedule may negatively impact the reliability of the service. (e.g. parking brake not routinely services and tested on vehicle).

Possible Measures:

(RC-287) Service Quality Risks in Table Form

Level 3

(RC-587) Service Reliability Infrastructure Provenance Risks

Definition: Risks that increase the likelihood of inadequate reliability of a pharmaceutical service.

(RF-984) Contract is not tied to the provider's ability to perform the service

Definition: A contract should be tied to the performance of the service to ensure that it can be terminated if the service fails to deliver the promised capabilities.

Possible Measures:
(RM-1737) Does the service contract lack explicit performance requirements for services to be performed?
(RM-1738) Does service contract lack mechanism to terminate if services do not meet explicit performance requirements?

(RF-982) Service will not be supported by provider throughout entire expected length of life cycle

Definition: Given that a service is expected to perform over a certain period of time, if the provider discontinues support before the end of the expected lifecycle, the service may not perform as expected (including security and quality) or even remain available.

Possible Measures:

(RF-981) Tariffs, embargos or other governmental influence over market conditions

Definition: Services that utilize services or supplies that are subject to tariffs, embargo or other governmental influence represent risk to provenance.

Possible Measures:
(RM-1244) Does the service utilize services or supplies (products) that are subject to undue influence from country/ies of concern?
(RM-1328) Does the service utilize services or supplies (products) that are subject to undue foreign influence?
(RM-1329) Does the service utilize services or supplies (products) that are subject to tariffs?
(RM-1330) Does the service utilize services or supplies (products) that are subject to embargos?
(RM-1353) Does the service utilize services or supplies (products) that are subject to tariffs from country/ies of concern?
(RM-1354) Does the service utilize services or supplies (products) that are subject to embargos from country/ies of concern?

Level 3

(RC-588) Service Reliability Infrastructure Pedigree Risks

Definition: Risks that increase the likelihood a service is unreliable due to issues with the composition and certified authenticity of infrastructure necessary for the delivery of the service.

(RF-986) Service is reliant on potentially volatile commodities

Definition: A service heavily reliant on commodities may be heavily influenced by the vicissitudes of the market more so than others. For example, lumber shortages may disrupt a construction company's ability to finish a building.

Possible Measures:

(RF-987) Service subject to changes in tax codes or commodity regulations

Definition: Changes in tax codes and commodity regulations may place new burdens on a service or service provider that could result in degradation of performance or discontinuation of a service. For example, export/import laws could change and make a service unavailable in certain countries; or, tax increases could place a burden on a service provider that results in a prohibitive cost increase.

Possible Measures:

(RF-985) Service is forced to change to meet regulatory requirements

Definition: Services that change within the time period of performance for the service due to regulatory requirements represent risk. Government regulations affecting the user/customer change requiring them to change the way in which they interact with the service being provided.

Possible Measures:
(RM-1325) Has there been any information indicating that security-relevant characteristics of the service have changed in the past due to changes in domestic regulatory requirements without appropriate notification to customers?
(RM-1326) Has there been any information indicating that security-relevant characteristics of the service have changed in the past due to changes in foreign regulatory requirements without appropriate notification to customers?
(RM-1327) Has there been any information indicating that security-relevant characteristics of the service have changed in the past due to changes in foreign regulatory requirements from country/ies of concern without appropriate notification to customers?
(RM-1739) Does service contract language lack protection for forced changes to meet new regulatory requirements, e.g., force majeure?

(RC-289) Service Resilience Risks in Table Form

Supply Chain Risks			
(RC-1) Supplier Risks	(RC-2) Supply Risks	**(RC-3) Service Risks**	
(RC-287) Service Quality Risks	**(RC-289) Service Resilience Risks**	(RC-286) Service Security Risks	(RC-288) Service Integrity Risks

Definition: Risks related to the reliability of a service delivered.

(RF-980) Loss of key personnel or IP to spin-off

Definition: Service relies on the knowledge of a limited number of specific personnel, such that their departure would cause a break in service.

Possible Measures:

(RF-976) Service-provider unable to continue service through sustainment and end-of-life

Definition: Services that are not able to be sustained through the end-of-life of the service represent a risk to reliability of the service.

Possible Measures:
(RM-1733) Does the service provider lack an explicit “obsolescence plan” for the service?

(RF-977) Service supply chain lacks diversity

Definition: A failure at any point within a supply chain is likely to disrupt the availability of a service--redundancy can mitigate this risk. A diverse supply chain in which there are multiple supply sources is one that is more resilient and resistant to disruption.

Possible Measures:

(RF-972) Service provider does not have redundancy and mitigation plans to recover from a disruption in service

Definition: Services that do not have redundancy in performance or mitigations plans from disruption represent risk.

Possible Measures:
(RM-1734) Does the service provider lack an explicit business continuity plan for the service?

(RF-979) Manner of performance cannot be changed

Definition: With changes in law, technology, business needs and overall market, a performance contract that is too specific may tie users to an inflexible service that has become obsolete, illegal, or otherwise unnecessary. For example, a contract specifying that data is to be encrypted using AES-128 may not adapt as industry adopts AES-256.

Possible Measures:

(RF-975) Contract is not reviewed periodically to identify breaches, loopholes, and changing service requirements

Definition: Services that are not reviewed periodically to identify breaches, loopholes and changing service requirements represent risk to reliability.

Possible Measures:
(RM-1735) Is there a lack of explicitly defined processes and procedures for periodic review of service contract language?

(RF-974) Contract does not allow flexibility to prevent service-provider lock-in in the event of changing conditions for the service

Definition: Services that have an inability to change a contract due to changing conditions forces a risk of lock-in.

Possible Measures:

(RF-971) Service suffers from a lack of improvement or competition to improve.

Definition: Services that operate without change and without competition represent risks to the reliability of the service.

Possible Measures:

(RF-973) Service is specialized to the point that there are no adequate alternative service providers

Definition: Services that are so specialized lacking adequate alternative service providers represent risks to reliability of the service.

Possible Measures:

(RC-289) Service Reliability Risks in Table Form

(RF-978) Service contract cannot be terminated or modified

Definition: A service contract that can't be modified or terminated may limit a user's ability to adapt to changing business needs.

Possible Measures:
(RM-1736) Does the service contract language provide an explicit mechanism to modify or terminate the contract if necessary?

Level 3

(RC-598) Service Infrastructure Redundancy Risks

Definition: Risks that a service provider is vulnerable to outage because of non-redundant critical infrastructure.

(RC-599) Service Infrastructure Diversity Risks

Definition: Risks that a service provider is vulnerable to outage because of critical infrastructure that cannot be substituted by similar options.

(RC-286) Service Security Risks in Table Form

Supply Chain Risks			
(RC-1) Supplier Risks	(RC-2) Supply Risks	**(RC-3) Service Risks**	
(RC-287) Service Quality Risks	(RC-289) Service Resilience Risks	**(RC-286) Service Security Risks**	(RC-288) Service Integrity Risks
Definition: Risks related to the security of a service delivered.			

(RF-897) Service is not audited for security

Definition: Services that are not audited for security controls represent risk.

Possible Measures:

(RF-889) Access and Privilege incidents and violations are not actively monitored, reported, and effectively corrected

Definition: Access and Privilege incidents and violations are not actively monitored, reported, and effectively corrected creating risks to performance of the service.

Possible Measures:

(RF-884) Service is critical to all business or mission operations (a bottleneck or single point of failure/vulnerability).

Definition: Services that are critical to mission/business operate as a single point of failure represent a risk to the infrastructure security.

Possible Measures:

(RF-895) Service contract does not control what data can be sent back to service providers

Definition: Services that rely on data being sent back to service providers can represent a risk when the data sent could be to a location of concern.

Possible Measures:

(RF-899) Contract locks-in service-provider even if service is not in the best interest of the product

Definition: Contract lock-in to a service provider represents risks as the service may not be performed in a manner in the best interests of the product representing a security risk to the service.

Possible Measures:

(RF-892) Backups, recovery, and continuity of operations (COOP) practices are not defined, documented, and incorporated into the system design and operating procedures to support timely continuity of availability of Mission/Business critical Information, Functions, Services, and Assets through routine and crisis operations

Definition: Backups, recovery, and continuity of operations (COOP) practices are not defined, documented, and incorporated into the system design and operating procedures to support timely continuity of availability of Mission/Business critical Information, Functions, Services, and Assets through routine and crisis operations.

Possible Measures:
(RM-1734) Does the service provider lack an explicit business continuity plan for the service?
(RM-1741) Does the service provider lack an emergency response plan for the service?
(RM-1742) Does the service provider lack an explicit policy for backing up service information?
(RM-1743) Does the service provider have an explicit policy for backing up service information that lacks a requirement for specific frequency of backup?
(RM-1744) Does the service provider have an explicit policy for backing up service information that lacks a requirement for specific duration of retention of backed up information?
(RM-1745) Does the service provider lack explicitly defined procedures for backing up service information?
(RM-1746) Does the service provider lack periodic integrity testing of backed up service information?
(RM-1747) Does the service provider lack periodic restoration testing of backed up service information?

(RF-894) Service provider steals intellectual property

Definition: 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.

Possible Measures:
(RM-1237) Is there information to indicate that the service provider has inappropriately accessed customer intellectual property?

(RC-286) Service Security Risks in Table Form

(RM-1238) Is there information to indicate that the service provider has inappropriately leveraged stolen customer intellectual property for financial gain?
(RM-1239) Is there information to indicate that the service provider has inappropriately leveraged stolen customer intellectual property for political or military purposes?

(RF-883) Service provider monitors users without their permission or beyond what is necessary to provide the service

Definition: Services that allow the provider to monitor the users without their permission or beyond what is necessary to provide the service represent a risk to infrastructure security.

Possible Measures:
(RM-1306) Does the service provider unnecessarily monitor user access patterns to the service?
(RM-1307) Does the service provider unnecessarily monitor user interest, interactions, and queries to the service?

(RF-877) No provisions to mitigate changes in jurisdictions that affect the protection of the data/service

Definition: Jurisdiction changes affecting the protection of data/service represent security risks.

Possible Measures:
(RM-1748) Does service contract lack clear definition of relevant jurisdiction for protection of service data and allow for modification or termination of contract if there is a material change?

(RF-885) Sensitive information or context are exposed in performance of the service

Definition: As part of performing the service, sensitive aspects information or context are exposed in performance. (e.g., penetration testing reveals vulnerabilities, weaknesses in supply chain, legal exposures, etc.).

Possible Measures:
(RM-1308) Does the normal performance of the service inherently expose sensitive information or usage context?

(RF-881) Services involve multiple or significant number or parties to perform

Definition: Services that involve multiple or significant number of parties to perform represent risks.

Possible Measures:

(RF-875) Foreseeable technological improvements render the service less secure.

Definition: Changes in circumstances (technology, geo-political, etc.) render the service less secure (e.g., quantum computing).

Possible Measures:
(RM-1338) Has there been information indicating past technology choices for the service that were rapidly made less secure due to technology improvements?

(RF-878) Long service period exploited by adversaries through acquisition or infiltration

Definition: Long running (multiple years) contracts for services often lock parties into terms and conditions that could be targeted by adversaries through acquisitions or infiltration.

Possible Measures:
(RM-1303) Does the service provider have a minimum required contract period of >= 1 and < 3 year(s)?
(RM-1304) Does the service provider have a minimum required contract period of >= 3 and < 5 year(s)?
(RM-1305) Does the service provider have a minimum required contract period of > 5 year(s)?

(RF-879) Service contracts are not reviewed after service supplier business changes structure.

Definition: Risks that the service providers business structure changes without service review. This is meant to identify risks in context of loss of IP and MADO.

Possible Measures:

(RF-886) Identities of authorized individuals are not documented and vetted and credentials validated to support effective physical and electronic access and privilege management to Mission/Business critical information, services, and assets

Definition: Services that do not document users or validate users that manage critical mission or business assets represent risk to the service.

Possible Measures:
(RM-1339) Does the service lack documentation of which individuals are authorized for physical access and use of information, services, and assets that are Mission/Business critical for the service?
(RM-1340) Does the service lack vetting of individuals for authorized physical access and use of information, services, and assets that are Mission/Business critical for the service?
(RM-1341) Does the service lack validation of credentials for authorized individuals to physically access and use of information, services, and assets that are Mission/Business critical for the service?

(RC-286) Service Security Risks in Table Form

(RM-1342) Does the service lack documentation of which individuals are authorized for electronic access and use of information, services, and assets that are Mission/Business critical for the service?
(RM-1343) Does the service lack vetting of individuals for authorized electronic access and use of information, services, and assets that are Mission/Business critical for the service?
(RM-1344) Does the service lack validation of credentials for authorized individuals to electronically access and use of information, services, and assets that are Mission/Business critical for the service?

(RF-876) Export Control Risks

Definition: Performing the service violates the local export control laws/regulations requiring the provider to lessen the security to perform the service or violate the law/regulation.

Possible Measures:
(RM-1301) Is the service being provisioned at a lesser level of security in a foreign country due to export laws/regulations?
(RM-1302) Is the service being provisioned at a lesser level of security in a country/ies of concern due to export laws/regulations?

(RF-888) The processes for assessing and allowing access and privilege credentials are not based on documented, incorporated, and trained upon processes

Definition: Services that do not have documented, incorporated or followed processes to allow access and privileged credentials represent a risk to the service.

Possible Measures:

(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

Definition: 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.

Possible Measures:
(RM-1257) Does the service provider collect PII data about its customers that is beyond the control of those customers?
(RM-1258) Does the service provider collect BII data about its customers that is beyond the control of those customers?
(RM-1259) Does the service provider collect IP data about its customers that is beyond the control of those customers?

(RF-887) Service involves credentials that are not protected from loss, misuse, and manipulation

Definition: Services that do not protect credentials from loss, misuse and manipulation represent risk to the service. (e.g., service offers to save passwords but does not protect them).

Possible Measures:

(RF-891) Vulnerability scans are not conducted and patches and corrections are not documented and implemented to prevent and reduce opportunities for vulnerability exploitations that lead to the loss of Confidentiality, Integrity, or Availability of Mission/Business Critical Information, Functions, Services, and Assets through routine and crisis operations

Definition: Vulnerability scans are not conducted and patches and corrections are not documented and implemented to prevent and reduce opportunities for vulnerability exploitations that lead to the loss of Confidentiality, Integrity, or Availability of Mission/Business Critical Information, Functions, Services, and Assets through routine and crisis operations.

Possible Measures:

(RF-893) Vulnerability and Resilience Management incidents and violations are not actively monitored, reported, and effectively corrected

Definition: Vulnerability and Resilience Management incidents and violations are not actively monitored, reported, and effectively corrected enabling responsive actions to protect the service from risks.

Possible Measures:
(RM-1309) Does the service lack active and consistent monitoring to detect vulnerability and resilience management incidents and violations?
(RM-1310) Does the service lack an explicitly defined program for vulnerability disclosure?
(RM-1311) Does the service fail to consistently follow an explicitly defined program for vulnerability disclosure?
(RM-1312) Does the service fail to effectively address and correct known vulnerability and resilience management incidents and violations?

(RF-896) Service supplier process for vetting 3rd party suppliers lacks rigor affecting the security of the service

Definition: Services that lack rigor in vetting their vendors (3rd party) represent risk to the security of the infrastructure and delivery of the service.

Possible Measures:
(RM-1345) Does the service supplier lack an explicitly documented process for vetting of their 3rd party suppliers?
(RM-1346) Does the service supplier fail to follow an explicitly documented process for vetting of their 3rd party suppliers?
(RM-1347) Does the service supplier fail to follow an explicitly documented process for vetting of their 3rd party suppliers that has been demonstrated to effectively identify and avoid risky suppliers?

(RC-286) Service Security Risks in Table Form

(RF-890) Authentication and Access Control Practices are not incorporated into and enforced through service level agreements, contracts, policies, regulatory practices

Definition: Services that do not have incorporated service level agreements, contracts or regulatory practices incorporated in access and authentication control practices represent a risk to the service.

Possible Measures:
(RM-1749) Does the service provider lack explicit policy for authentication and access control for the service?
(RM-1750) Does the service provider lack explicitly defined processes and procedures for authentication and access control for the service?

(RF-880) Acquisition, sale or spin-off of critical assets to perform the service is of concern

Definition: Acquisition, sale or spin-off of critical assets to perform the service presents a security concern.

Possible Measures:
(RM-1245) Have critical assets required to perform the service been sold to a domestic entity?
(RM-1246) Have critical assets required to perform the service been sold to a foreign entity?
(RM-1247) Have critical assets required to perform the service been sold to an entity owned/controlled by country/ies of concern?
(RM-1248) Is the sale of critical assets required to perform the service to a domestic entity currently underway of planned for the future?
(RM-1249) Is the sale of critical assets required to perform the service to a foreign entity currently underway of planned for the future?
(RM-1250) Is the sale of critical assets required to perform the service to an entity owned/controlled by country/ies of concern currently underway of planned for the future?
(RM-1251) Has ownership/control of critical assets required to perform the service been spun-off into a separate domestic entity?
(RM-1252) Has ownership/control of critical assets required to perform the service been spun-off into a separate foreign entity?
(RM-1253) Has ownership/control of critical assets required to perform the service been spun-off into a separate entity owned/controlled by country/ies of concern?
(RM-1254) Is ownership/control of critical assets required to perform the service in process of being spun-off or planned to be spun-off into a separate domestic entity?
(RM-1255) Is ownership/control of critical assets required to perform the service in process of being spun-off or planned to be spun-off into a separate foreign entity?
(RM-1256) Is ownership/control of critical assets required to perform the service in process of being spun-off or planned to be spun-off into a separate entity owned/controlled by country/ies of concern?

(RF-898) Customers do not own intellectual property created using the service

Definition: In some cases, providers may contractually own IP developed with their service. In this scenario, businesses may be required to compensate or even relinquish full usage rights to the service provider.

Possible Measures:
(RM-1751) Does the service contract lack clearly defined ownership of intellectual property created using the service?

(RF-1255) Concerns for who has remote access to service functionality and configuration

Definition:

Possible Measures:
(RM-1204) Are personnel in country/ies of concern able to remotely access the service functionality or configuration?
(RM-1205) Are personnel in country/ies of concern able to remotely modify the service functionality or configuration?
(RM-1206) Are personnel in country/ies of concern able to remotely leverage system administrator privileges for the service functionality or configuration?

(RF-1257) Concerns for where sensitive customer data is remotely processed or retained by the service

Definition:

Possible Measures:
(RM-1210) Does the service process or retain customer PII data on infrastructure in country/ies of concern?
(RM-1211) Does the service process or retain customer BII data on infrastructure in country/ies of concern?
(RM-1212) Does the service process or retain customer financial information on infrastructure in country/ies of concern?

Level 3

(RC-294) Service Specific Security Risks

Definition: Risks that increase the likelihood that the security of a service may be inadequate due to service specific security issues.

Level 4

(RC-303) Engineering Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of an engineering service.

(RF-911) Engineering service provider seeks to own intellectual property to perform the engineering service

Definition: Services that rely on sharing the designs or composition of materials to perform the service represent a security risk where theft of intellectual property such as CAD drawings, formulas, or other intellectual property is shared and required to perform the service.

Possible Measures:
(RM-1313) Does the domestic engineering service provider require retained ownership of intellectual property rights for the results of their engineering service?
(RM-1314) Does the foreign engineering service provider require retained ownership of intellectual property rights for the results of their engineering service?
(RM-1315) Does the engineering service provider from country/ies of concern require retained ownership of intellectual property rights for the results of their engineering service?

Level 4

(RC-327) Advertising Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of an advertising service.

(RF-907) Advertising service collects or reveals personal information of users without explicit permission

Definition: Advertisers, especially digital advertisers, may have access to private information about the individuals that interact with or view their adds. It is a risk that the advertiser collects or otherwise improperly uses this data opening clients to potential legal issues.

Possible Measures:

(RF-906) Advertiser discloses sensitive or proprietary data to other clients or in advertisements

Definition: Advertisers may have privileged access to client data, proprietary information or other private information. It is a risk that the advertiser may provide or leak this data to another client or inadvertently include it in advertising.

Possible Measures:

Level 4

(RC-323) Brokering Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a brokering service.

(RF-908) Brokerage shares or fails to properly protect client's proprietary information with other clients

Definition: Brokering service providers may have privileged access to client data, proprietary information or other private information. It is a risk that the brokerage may provide this data to another client or inadvertently leak it due to improper security practices.

Possible Measures:

Level 4

(RC-311) Manufacturing Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a manufacturing service.

(RF-912) Manufacturing co-packer steals or attempts to own the formula or composition of materials to perform the service

Definition: Services where a manufacturing co-packer attempts to own the composition, formula or components that make up the product that represent a security risk.

Possible Measures:

Level 4

(RC-307) Digital Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a digital service.

(RF-909) Digital service provider does not employ (externally or internally) a data security team for response and recovery

Definition: Digital service providers must be able to properly protect client information and to do so they must leverage the experience of security professional, either by hiring an internal team or contracting to an external company for response and recovery.

Possible Measures:

(RF-910) Digital service provider does not disclose its data protection practices

Definition: Digital service providers that have access to client data are likely expected to keep it safe. Their security practices should be disclosed to the client including encryption processed and algorithms used.

Possible Measures:

(RC-286) Service Security Risks in Table Form

Level 4

(RC-560) Pharmaceutical Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a pharmaceutical service.

(RC-319) Warehousing Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a warehousing service.

(RF-913) Warehousing service provider's shipping services are not held to the same standards as others in securing locations

Definition: Security risks where a warehousing service provider's shipping services are not bound by the security standards as your own standards or across vendors (e.g., Fed Ex, UPS, Amazon allowed direct access where others need go through security).

Possible Measures:

Level 4

(RC-315) Transportation Service Specific Security Risks

Definition: Risks that increase the likelihood of inadequate security of a transportation service.

Level 3

(RC-11) Remote/Virtual Access to Service Infrastructure Risks

Definition: Risks that increase the likelihood the security of a service may be inadequate due to the ability to remotely or virtually access infrastructure for the delivery of the service.

(RF-108) Concerns for who has remote access to service infrastructure software for patching, servicing, etc.

Definition: An unapproved party with remote access and the permissions needed to update or otherwise alter the operation of service infrastructure may have access to sensitive customer information and could threaten the availability, reliability, and quality of the service.

Possible Measures:
(RM-141) Are unauthorized service personnel able to remotely access the service infrastructure software?
(RM-957) Are less than all service infrastructure remote access activity logs reviewed and audited?
(RM-1195) Is activity of remote access to service infrastructure software not always logged?

(RF-109) Concerns for who has remote access to the facility for servicing

Definition: Unapproved remote access to a service facility could allow a third-party to gain access to critical infrastructure, including security systems, within a facility which may expose critical customer information or threaten the availability, reliability and quality of a service. For example, a third party gaining access to a facility's camera system.

Possible Measures:
(RM-142) Are unauthorized service personnel able to remotely access the service infrastructure facility?
(RM-184) Is activity of remote access to service infrastructure facilities not always logged?
(RM-957) Are less than all service infrastructure remote access activity logs reviewed and audited?

(RF-103) Concerns for who has remote access to service infrastructure hardware for servicing

Definition: Unapproved remote access to service infrastructure could not only reveal sensitive customer information but could threaten the availability, reliability, and quality of the service.

Possible Measures:
(RM-140) Are unauthorized service personnel able to remotely access the service infrastructure hardware?
(RM-957) Are less than all service infrastructure remote access activity logs reviewed and audited?
(RM-1194) Is activity of remote access to service infrastructure hardware not always logged?

Level 3

(RC-296) Service Security Infrastructure Pedigree Risks

Definition: Risks that increase the likelihood the service is insecure due to issues with the composition and certified authenticity of infrastructure necessary for the delivery of the service.

(RF-918) Service is comprised of complex system of systems where the vendor provides the service and the supplies necessary for the service.

Definition: Services that are composed of complex systems of systems where the services and supplies are provided by the same vendor can represent infrastructure pedigree risk.

Possible Measures:

(RC-286) Service Security Risks in Table Form

(RF-917) Service introduces vulnerabilities to customers, or uses infrastructure with known vulnerabilities

Definition: Services that introduce vulnerabilities to customers, or use infrastructure that has known vulnerabilities to perform the service represent risk to the infrastructure pedigree.

Possible Measures:

(RF-919) In a merger, acquisition, divestiture and outsourcing context, services provided by any shared assets are needed to perform the service

Definition: Services that are performed in the midst of mergers, acquisitions, divestures, and outsourcing utilizing shared assets to perform the service represent a service pedigree risk.

Possible Measures:

Level 3

(RC-295) Service Security Infrastructure Provenance Risks

Definition: Risks that increase the likelihood a service may be insecure due to issues with the origin, evolution and chain of custody of infrastructure necessary for the delivery of the service.

(RF-914) Service is performed by persons not authorized to work for the customer.

Definition: Unauthorized personnel (potentially from country(ies) of concern) performing services as part of the overall service delivery is a security risk. Authorization could be defined by law, contract, export control rules, etc.).

Possible Measures:
(RM-1316) Does provision of the service involve performance by personnel who are domestic citizens and not authorized to work for the customer?
(RM-1317) Does provision of the service involve performance by personnel who are foreign citizens and not authorized to work for the customer?
(RM-1318) Does provision of the service involve performance by personnel who are citizens of country/ies of concern and are not authorized to work for the customer?

(RF-915) Service requires all data to provide the service flow through hubs that are related to country(ies) of concern

Definition: Services that require data flows through country(ies) of concern represent risks to provenance.

Possible Measures:

(RF-916) Service provider relies on known-compromised infrastructure

Definition: 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.

Possible Measures:
(RM-1260) Does the service provider utilize network infrastructure publicly disclosed or otherwise known to be compromised by malicious actors?
(RM-1261) Does the service provider utilize cloud infrastructure publicly disclosed or otherwise known to be compromised by malicious actors?
(RM-1262) Does the service provider utilize server infrastructure publicly disclosed or otherwise known to be compromised by malicious actors?
(RM-1263) Does the service provider utilize data infrastructure publicly disclosed or otherwise known to be compromised by malicious actors?
(RM-1264) Does the service provider utilize software infrastructure publicly disclosed or otherwise known to be compromised by malicious actors?

Level 3

(RC-10) Physical Access to Service Infrastructure Risks

Definition: Risks that increase the likelihood the security of a service may be inadequate due to the ability to physically access infrastructure for the delivery of the service.

(RF-106) Concerns for who has access to service infrastructure hardware for servicing

Definition: Unapproved physical access to service infrastructure could not only reveal sensitive customer information but could threaten the availability, reliability, and quality of the service.

Possible Measures:
(RM-138) Are unauthorized personnel able to physically access the service infrastructure hardware?

(RF-105) Concerns for who can gain access to the service infrastructure software (updates, replacements, etc.)

Definition: An unapproved party with physical access and the permissions needed to update or otherwise alter the operation of service infrastructure may have access to sensitive customer information and could threaten the availability, reliability, and quality of the service.

Possible Measures:
(RM-139) Are unauthorized personnel able to physically access the service infrastructure software?

(RC-286) Service Security Risks in Table Form

(RF-107) Concerns for who can gain access to the facility (updates, replacements, etc.)

Definition: Unapproved physical access to a service facility could allow a third-party to gain access to critical infrastructure, including security systems, within a facility which may expose critical customer information or threaten the availability, reliability and quality of a service.

Possible Measures:
(RM-161) Are unauthorized personnel able to physically access the service infrastructure facility?
(RM-947) Is not all personnel access to the service infrastructure facility logged?
(RM-950) Are not all service infrastructure facility access logs reviewed and audited?

(RC-288) Service Integrity Risks in Table Form

<table>
<tr><td colspan="12"><b>Supply Chain Risks</b></td></tr>
<tr><td colspan="4"><b>(RC-1) Supplier Risks</b></td><td colspan="4">(RC-2) Supply Risks</td><td colspan="4"><b>(RC-3) Service Risks</b></td></tr>
<tr><td colspan="3">(RC-287) Service Quality Risks</td><td colspan="3">(RC-289) Service Resilience Risks</td><td colspan="3">(RC-286) Service Security Risks</td><td colspan="3"><b>(RC-288) Service Integrity Risks</b></td></tr>
<tr><td colspan="12">Definition: Risks related to the integrity of a service delivered.</td></tr>
</table>

(RF-948) Risks are transferable to third-party subcontractors

Definition: Risk that a service provider will not be held accountable for failure to perform as its risks are transferred to a subcontractor.

Possible Measures:

(RF-946) Service doesn’t require reporting when there is a law enforcement request or government request

Definition: Services that doesn’t require reporting when there is a law enforcement or government request represent a risk to the service integrity.

Possible Measures:

(RF-941) Service-provider is not held accountable for lapses in service or meeting obligations

Definition: Service becomes less trustworthy over time due to the inability to hold provider accountable via changes in contract.

Possible Measures:

(RF-947) Service does not include a requirement to disclose changes to the terms of service (30/60/90) days before they occur

Definition: Services that do not provide agreed to time for changes in terms of services prior to implementation represent a risk to integrity of the service.

Possible Measures:

(RF-945) Service doesn’t define who owns the data or the data is solely owned by the platform on which it is created

Definition: Services that do not define who owns the data or where the data is solely owned but the on which it is created represent risks to integrity of the service.

Possible Measures:
(RM-1349) Does the service lack clear definition of who owns the data created using the service?
(RM-1350) Does the service assert ownership of all data created using the service?

(RF-944) Service is provided in a location or jurisdictions requiring disclosure of user information to the local government or partnering nations

Definition: Services that operate in locations or jurisdictions that require disclosure of user information in order to operate represent risk to the integrity of the service.

Possible Measures:

(RF-940) Service relies on software with known dual use issues

Definition: This risk considers that service integrity may be negatively affected for services that rely on software with known dual uses to perform the service. This dual use should be contemplated as a risk. "Dual use" to include a disconnect between users (esp. freeware) and customers (e.g., data buyers). (e.g., The Kali tool/Metasploit is used for vulnerability identification as well as hacking.)

Possible Measures:

(RF-943) Service does not require reporting of significant changes to how data is captured, stored, or shared to the customer.

Definition: Services that don’t report significant changes to the customer on how data is captured, stored, or shared represent risk.

Possible Measures:
(RM-1348) Does the service lack required customer reporting of significant changes to how data is captured, stored, or shared?

(RC-288) Service Integrity Risks in Table Form

(RF-942) Service includes creating information on platforms where reliance of security in data is dependent on the terms of service

Definition: Services that rely on Terms of Service to define the protection afforded to the data created on the service platform can represent a risk.

Possible Measures:

(RF-949) Provider shares with third parties critical information gathered through use of its service

Definition: Risk that critical information a provider can collect as part of the use of its service is released to adversaries or competitors.

Possible Measures:

Level 3

(RC-301) Service Specific Integrity Risks

Definition: Risks that increase the likelihood the integrity of a service may be inadequate due to service specific integrity issues.

Level 4

(RC-308) Digital Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a digital service.

(RC-304) Engineering Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of an engineering service.

(RC-586) Pharmaceutical Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a pharmaceutical service.

(RC-312) Manufacturing Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a manufacturing service.

(RF-970) Integrity risks when co-packing manufacturers do not carry liability insurance

Definition: Co-packing manufacturers should carry liability insurance to include products liability in order to cover liability claims as they are part of the overall manufacturing process and their negligence could affect the manufacturer.

Possible Measures:

(RF-969) Co-packing manufacturers claiming ownerships in the components/ingredients that make up the final product

Definition: Co-packing manufacturers have access and physical control over the intellectual property and the components/ingredients increasing the integrity risk of a co-packer claiming ownerships in the components/ingredients that make up the final product.

Possible Measures:

Level 4

(RC-320) Warehousing Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a warehousing service.

(RC-328) Advertising Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of an adverting service.

(RF-968) Advertiser plagiarizes another provider's unique advertising methods

Definition: The possibility of copyright infringement, or plagiarism in general could result in exposure to legal action and/or damage to client's reputation.

Possible Measures:

(RF-967) Advertiser defames other organizations or individuals.

Definition: Defamation in advertisement may expose a client to legal action and/or damage its reputation within the market.

Possible Measures:

(RC-288) Service Integrity Risks in Table Form

(RF-966) Advertiser fails to comply with regulations governing communication or advertising.

Definition: An advertiser that fails to comply with laws regarding communication may expose its clients to legal action and/or damage to their reputations.

Possible Measures:

Level 4

(RC-324) Brokering Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a brokering service.

(RC-316) Transportation Service Specific Integrity Risks

Definition: Risks that increase the likelihood of inadequate integrity of a transportation service.

Level 3

(RC-576) Service Integrity Infrastructure Pedigree Risks

Definition: Risks that decrease service integrity due to issues with the composition and certified authenticity of infrastructure necessary for the delivery of the service.

(RF-958) Supervisor of the service does not have the requisite knowledge to provide adequate oversight

Definition: Services that require requisite knowledge in order to manage/audit represent a risk when the provider does not have the requisite knowledge to oversee the service.

Possible Measures:

(RF-959) Supplier is not required to flow down obligations to sub-contractors

Definition: Services that do not require the same obligations on sub-contractors to the service provider represent risk.

Possible Measures:

(RF-956) Changes in business partnerships (M&A, joint ventures) are subject to review and approval.

Definition: New business partnerships should be subject to review and approval otherwise the service could be provided by parties associated with country(ies) of concern.

Possible Measures:

(RF-960) Service is impacted by consortium of providers

Definition: A consortium of providers could have influence over how a service is performed by an individual provider and therefore if that service meets the user's expectations.

Possible Measures:

(RF-957) Supplier is not required to declare the services it is receiving from other companies

Definition: Services that are not declared for source could come from companies that are controlled by countries of concern represent risk.

Possible Measures:
(RM-1321) Does the service provider fail to declare the subservices it utilizes for provision of the service?
(RM-1322) Does the service provider fail to declare the ownership/provider details of domestic subservices it utilizes for provision of the service?
(RM-1323) Does the service provider fail to declare the ownership/provider details of foreign subservices it utilizes for provision of the service?
(RM-1324) Does the service provider fail to declare the ownership/provider details of subservices it utilizes for provision of the service where the subservice is controlled or influenced by country/ies of concern?

(RC-577) Asset Inventory and Audit Management Practice [Asset and Audit] Risks

Definition: Risks that decrease service integrity due to inadequate asset inventory and audit management practices for composition of infrastructure necessary for the delivery of the service.

(RF-964) Asset Inventory and Audit data are not reviewed and assessed to support an effective known configuration of the system or remediated in a timely fashion

Definition: Service relies on assets that are not configured to a known configuration to support the service and remediated when the configuration deviates from that configuration.

Possible Measures:

(RF-962) Mission/Business Critical backup, reserve, and replacement assets are not inventoried, and periodically audited to assure their initial and continued pedigree, accountability and integrity

Definition: Service relies on the use of backup, reserve or replacement assets that are not audited for initial pedigree, accountability or integrity.

Possible Measures:

(RF-961) Mission/Business Critical operational assets are not inventoried and periodically audited to assure their initial and continued pedigree, accountability and integrity

Definition: Services relies on assets that are not inventories or periodically audited to assure initial pedigree, accountability and integrity.

Possible Measures:

(RF-963) Asset Inventory and Audit data are not protected from loss, corruption, or manipulation

Definition: Service relies on asset and inventory data that is not protected from loss, corruption or manipulation such that the reporting of these inventories would not be available or accurate.

Possible Measures:

(RF-965) Asset Inventory and Audit Management Practices are not incorporated into and enforced through service level agreements, contracts, policies, regulatory practices

Definition: Service relies on assets that are not audited and changes enforced for deviations from the agreed to service level agreement, policies or regulatory practices.

Possible Measures:

Level 3

(RC-575) Service Integrity Infrastructure Provenance Risks

Definition: Risks that decrease service integrity due to issues with the origin, evolution and chain of custody of infrastructure necessary for the delivery of the service.

(RF-954) End User License Agreement (EULA) changes don't require acknowledgement by customer

Definition: A change in a license agreement can include new permissions or requirements introduced by a provider that could alter how a service is performed or how a user's data is handled.

Possible Measures:

(RF-952) Contract does not address expectations for foreign outsourcing of third party subcontracting

Definition: A provider outsourcing to a foreign third party, if not previously discussed, could introduce risks into a supply chain depending on where the third party is located. A contract outlining the expectations for foreign outsourcing can help prevent this eventuality and give the user more control over whom is involved in the service delivery.

Possible Measures:

(RF-955) Service purports to provide protection for data or capability indefinitely

Definition: A service that offers protection of a user’s data should continue to do so for the length of the contract. Is there a time to live that's shorter than the purported period of protection so that the service dies before the protection expires?

Possible Measures:

(RF-950) Services provided where bribes and other unethical acts considered a normal business practice

Definition: Bribes and other unethical acts may be considered a normal business practice. A firm moving from one operation where such unethical practices are prohibited/banned may be at a disadvantage and forced to change its tolerance of such behavior.

Possible Measures:
(RM-1351) Is service infrastructure located in areas where bribes and other unethical acts considered a normal business practice?

(RC-288) Service Integrity Risks in Table Form

(RF-951) Services don’t seem bounded by time or some pre-condition that indicates a beginning and end.

Definition: Contracts should have a beginning, middle & end. There may be risks if the contract doesn't seem bounded by time or some pre-condition.

Possible Measures:

(RF-953) Service provider does not disclose the use of open source software

Definition: Open source solutions are not inherently risky; however, they do introduce certain risks that the customer may want to know about depending on how they are using a service. For example, an open source solution may enable adversaries to inject malicious code by participating in a contributor community.

Possible Measures:
(RM-1352) Does the service utilize open source software without the service provider disclosing its use?

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]
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]

System of Trust Glossary

Glossary Term	Glossary Definition
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.