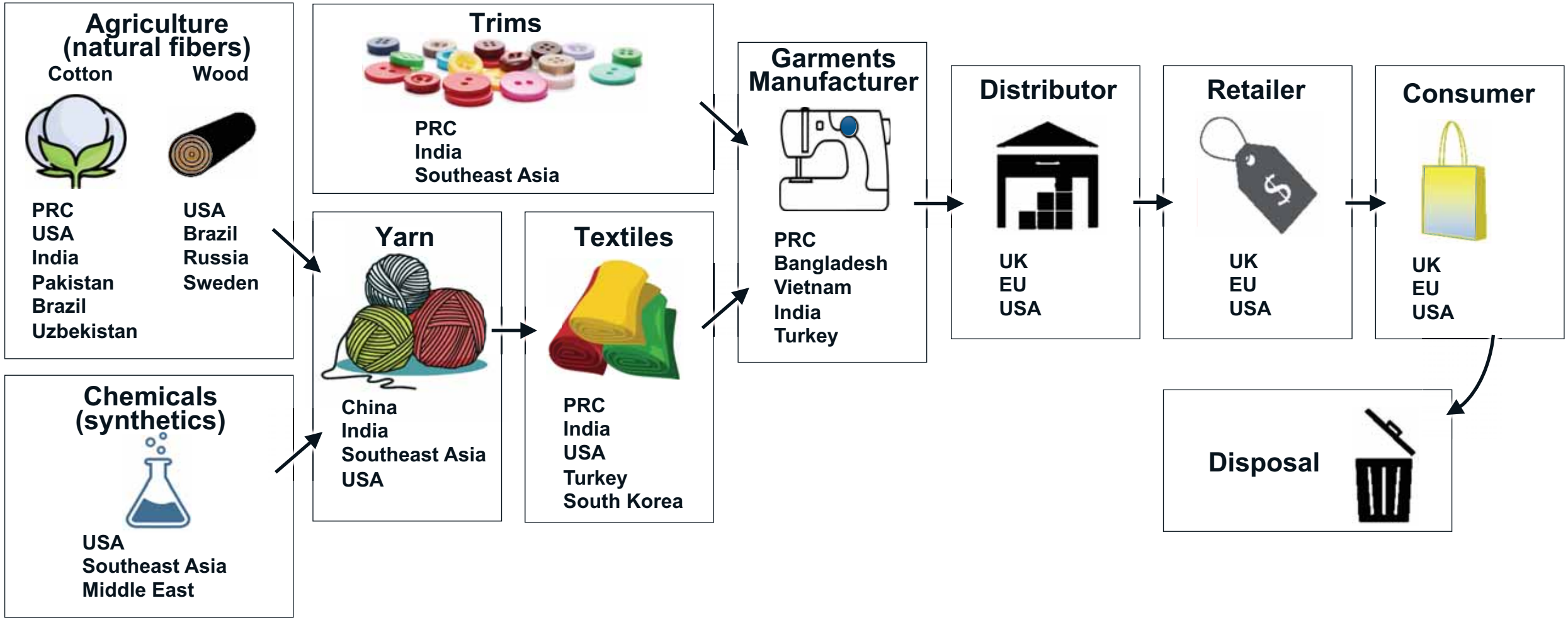
MITRE's System of Trust™ Framework and Community

Robert Martin
Sr. Software and Supply Chain Assurance Prin. Eng.
Cyber Solutions Innovation Center
MITRE Labs

Presented to the Software and Supply Chain Assurance Forum on 1 June 2023

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Supply Chain Example – Consumer Clothing



https://imgs.mongabay.com/wp-content/uploads/sites/20/2020/04/23100736/FF_Supplychain.png

MITRE

Supply Chain Risk Areas

Natural Disasters and Hazards

Floods
Avalanche
Drought
Winds
Heavy Rains
Pandemics
Earthquake
Volcanoes
Tornadoes
Forest Fires
Snow
Thunderstorms
Tsunamis

Icons thanks to freepik

Human Hazards

Hijacking

Corporate Corruption

Traffic Congestion

Civil Disruption

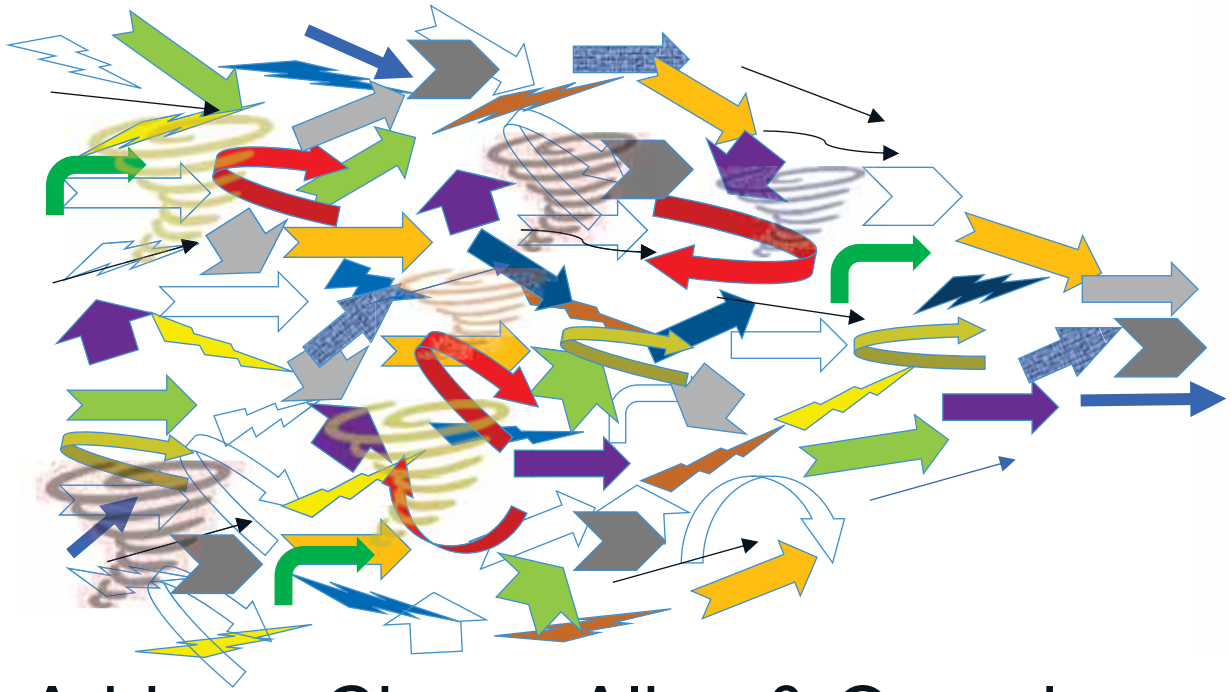
Interdependent Supply Chains

National Corruption

Supply Chain Security (SCS) System of Trust (SoT)

"What Supply Chain Risks to Manage?"

SoT - a strategic, widely-adoptable, holistic, data-driven analysis platform to assess supply chain security risks



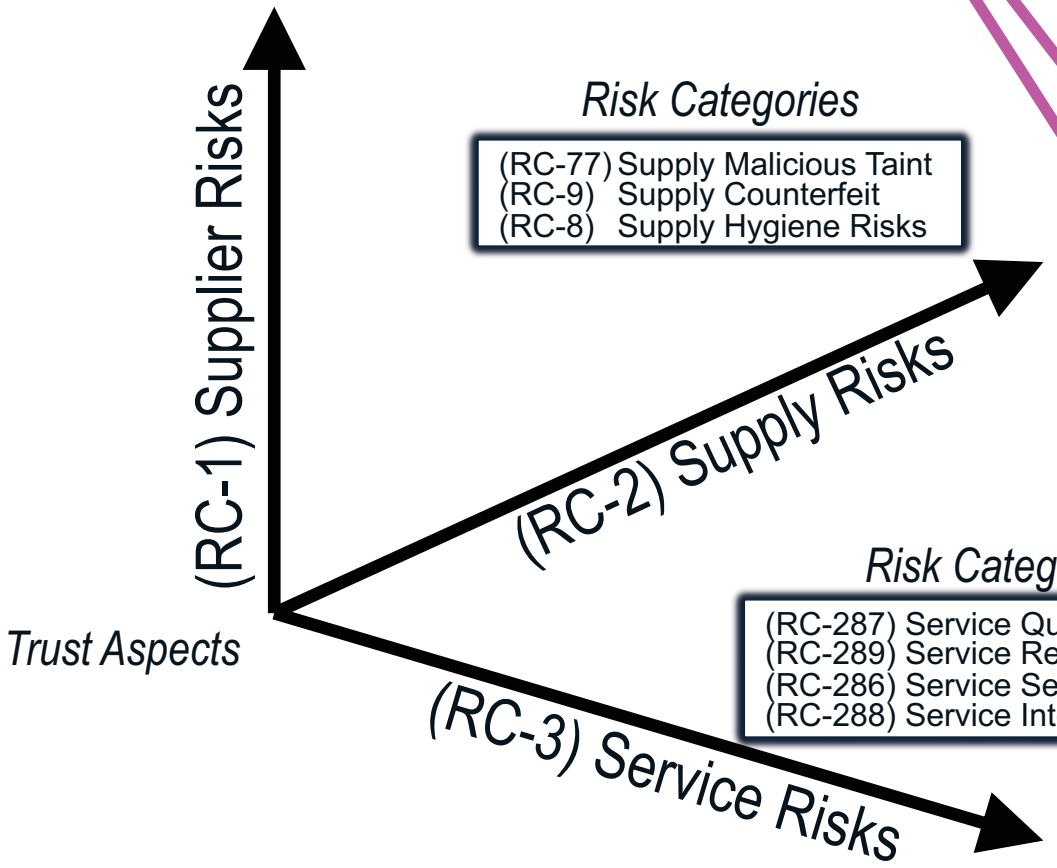
Address Chaos, Align & Organize

Simplify, Tailor & Use

Basis of Trust

Risk Categories

(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



Risk Categories

(RC-77) Supply Malicious Taint
(RC-9) Supply Counterfeit
(RC-8) Supply Hygiene Risks

Risk Categories

(RC-287) Service Quality Risks
(RC-289) Service Resilience Risks
(RC-286) Service Security Risks
(RC-288) Service Integrity Risks

(RC-13) Supplier Financial Stability Risks
(RC-257) Short-term Financial Health Risks
(RC-256) Financial Stewardship Risks
(RC-260) Adverse Market Factors
(RC-258) Long-term Financial Health Risks
(RC-262) Foreign Financial Obligations

(RC-76) Supplier Organizational Security Risks
(RC-403) Technical Operations Risks
(RC-441) Cyber Threat Intelligence Risks
(RC-16) Security Training Deficiencies
(RC-346) Security Capabilities and Operations Risks
(RC-434) Cyber Threat Activity Risks
(RC-400) Security Governance and Compliance Risks

(RC-105) Supplier Organizational Effectiveness Risks
(RC538) Structural & Operational Instability
(RC-537) Geographical/Geopolitical Instability

(RC-7) Supplier Ethical Risks
(RC-15) Association with Foreign Intelligence Service or Foreign Military Entity
(RC-26) Pattern of Criminal Behavior

(RC-6) Supplier External Influences
(RC-5) Ownership and Control Risks
(RC-534) Foreign Business Relationship Risks
(RC-536) Adverse Corporate Influences

MITRE

MITRE Supply Chain Security System of Trust Risk Areas* **

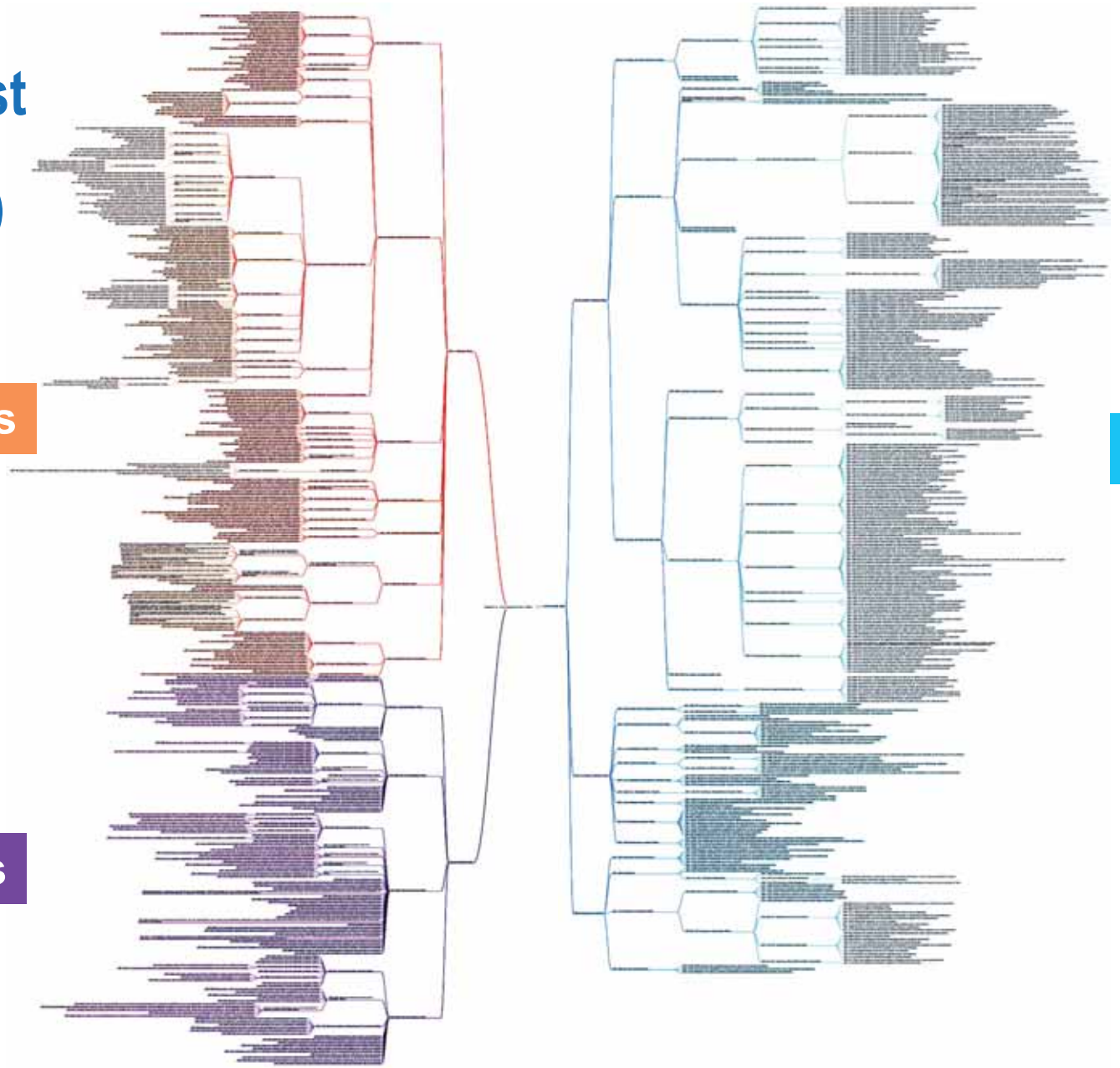
Supply Chain Risks																
(RC-1) Supplier Risks							(RC-2) Supply Risks			(RC-3) Service Risks						
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Culture Risks	(RC-105) Supplier Organizational Effectiveness Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences	(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			
(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-127) Unsanctioned Manufacturing	(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-126) Mislabeling	(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-118) Technical Authenticity Risks	(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-128) Copycat Manufacturing		(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-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-588) Service Reliability Infrastructure Pedigree Risks						
							(RC-150) Facilities Integrity Risks									
							(RC-54) Packaging Integrity Risks									
							(RC-156) Maintenance Integrity Risks									

MITRE's Supply Chain Security System of Trust™ https://sot.mitre.org/

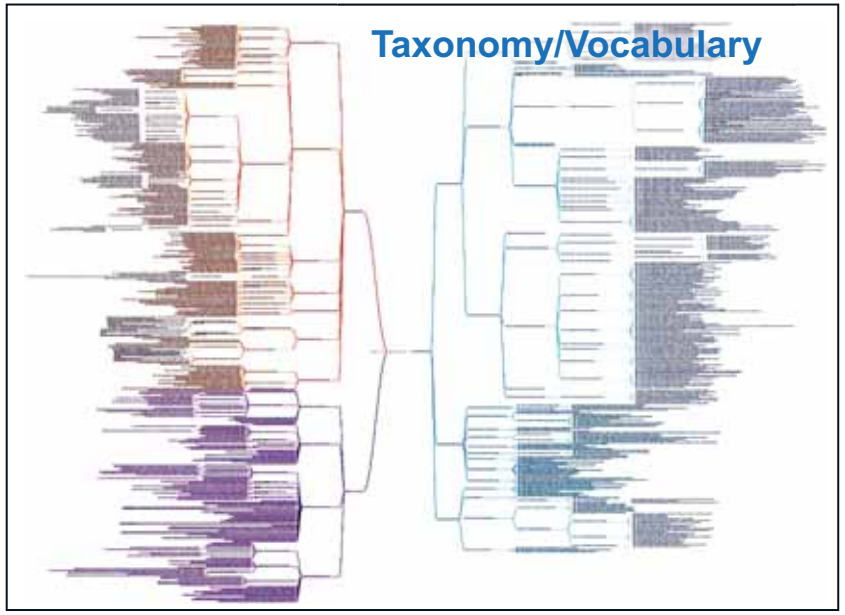
* Supply Chain Security Top 78 Risk Areas Levels 1-3
** System of Trust Expanding to Pharma, Food, and other types of Products

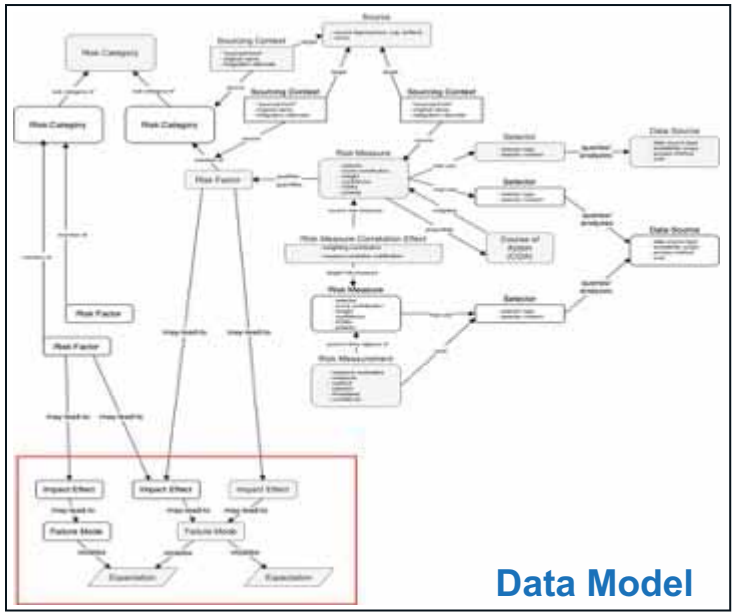
MITRE

MITRE Supply Chain Security System of Trust Risk Catalog at 7 levels (aka Taxonomy/Vocabulary)

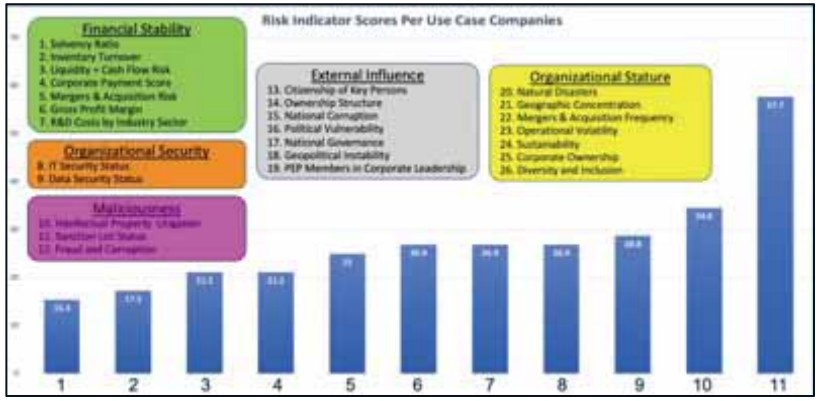


MITRE

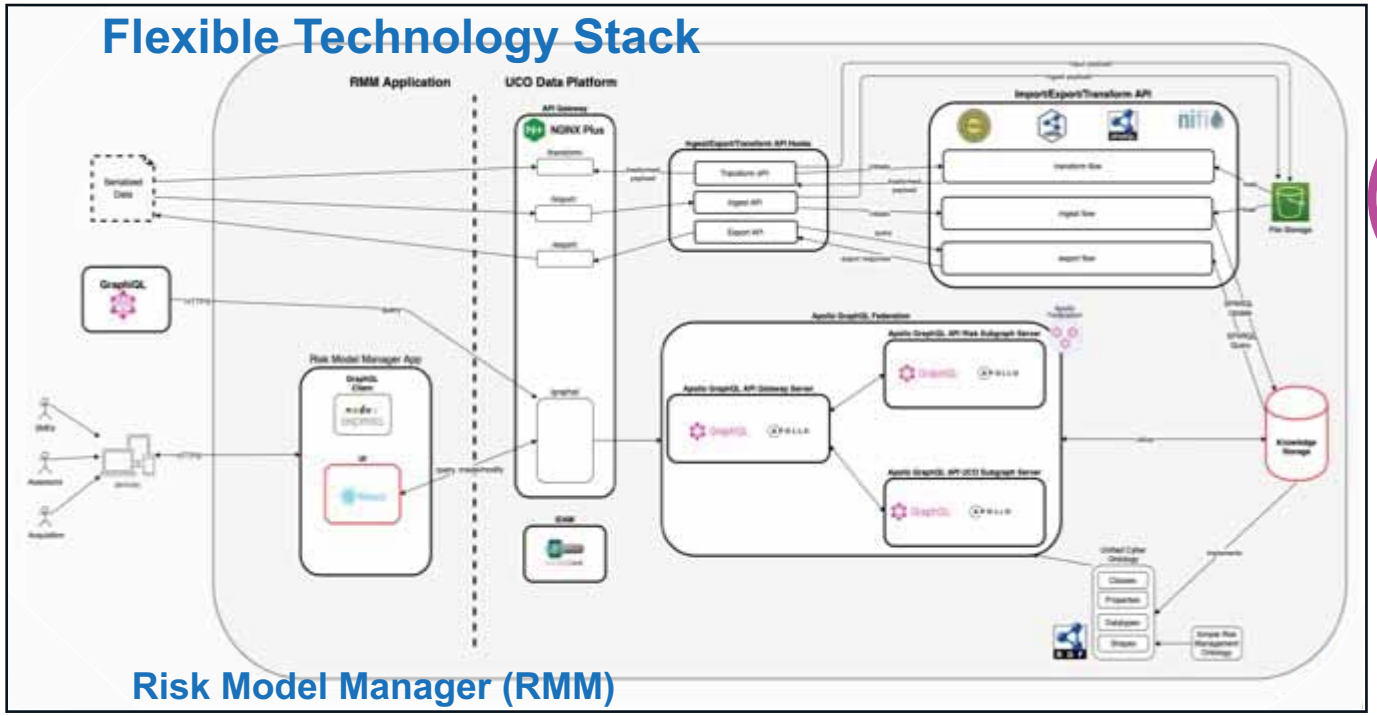




Analytic Methods

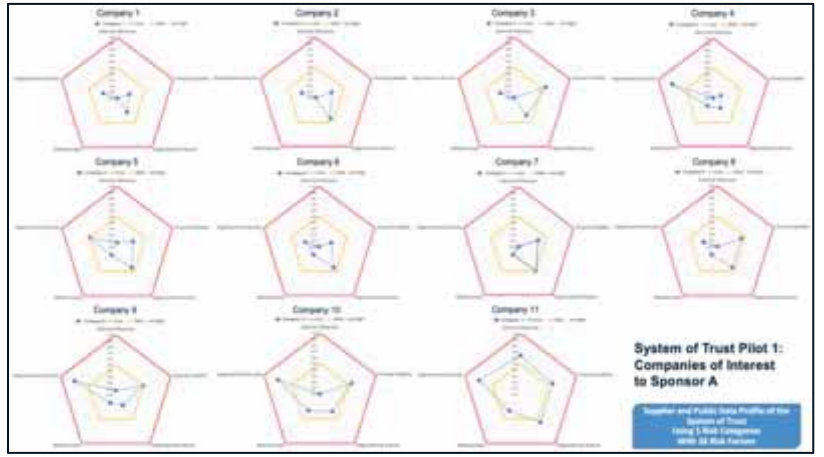


Flexible Technology Stack

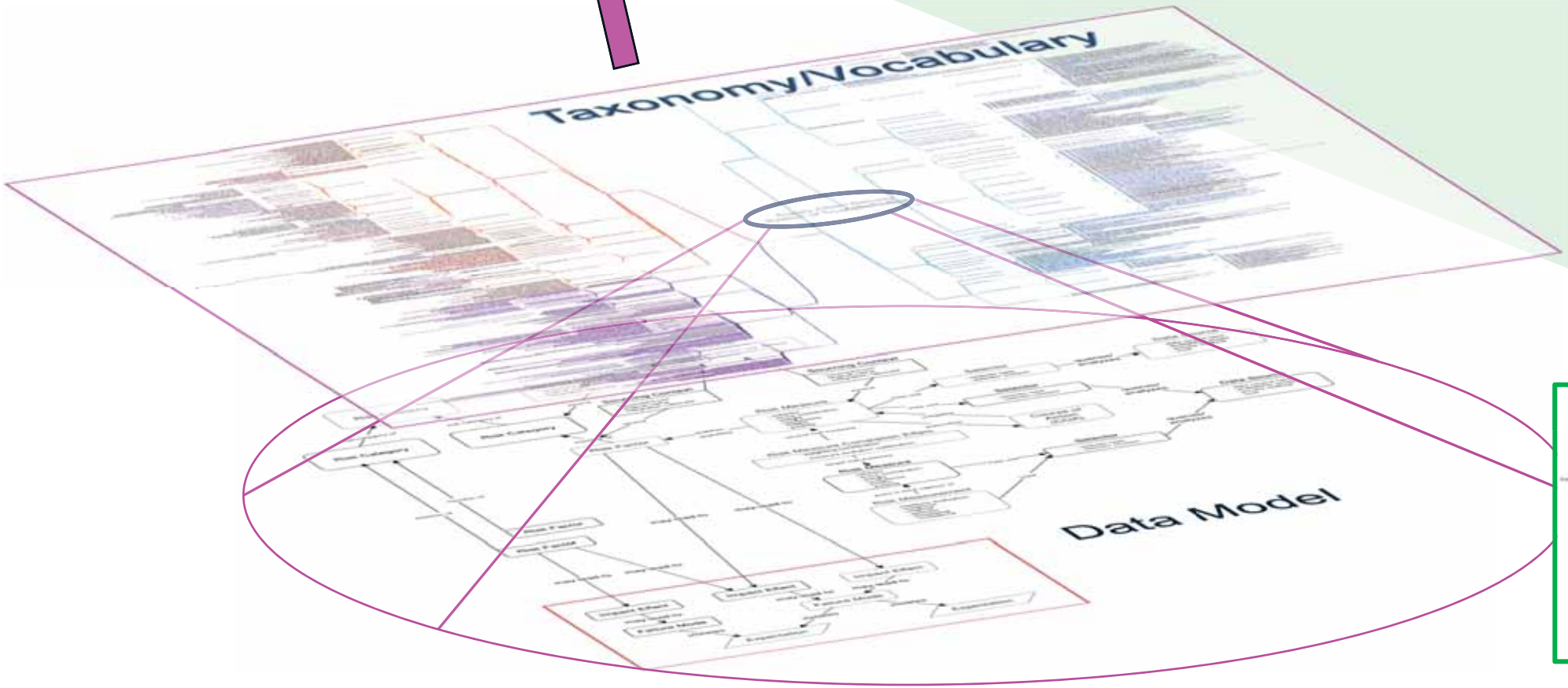


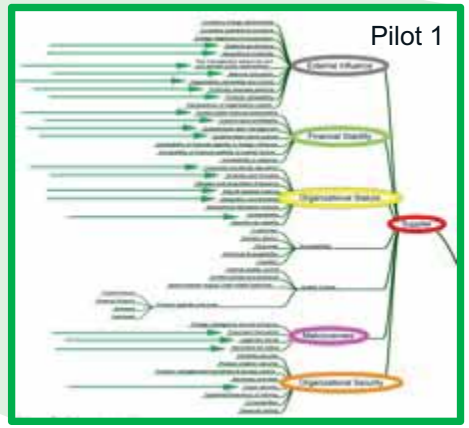
Piloting
On-going

Export to Spreadsheet for "Offline" Assessment

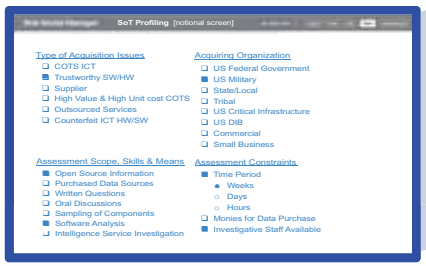


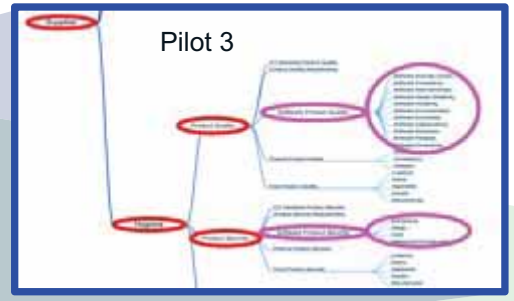
Tying together SoT and RMM

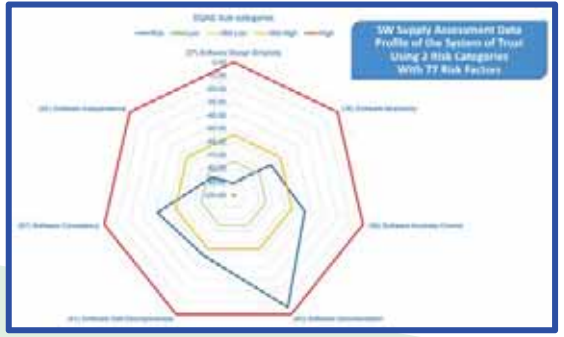


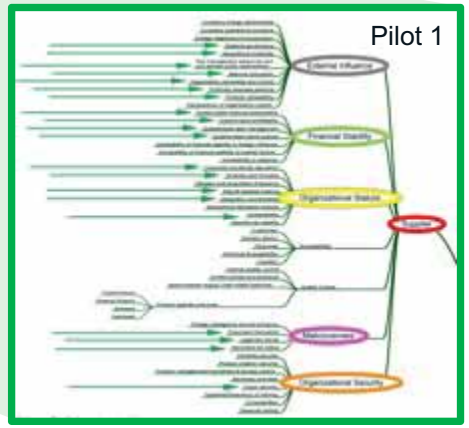


Tying together SoT and RMM









(RC-76) Supplier Organizational Security Risks → (RC-434) → (RC-435) → (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.
- **Data Source :**
  - Source: EDGAR, SEC, Wikipedia
  - Security and Exchange and Commission: https://www.sec.gov/edgar/searchedgar/companysearch.html
  - EDGAR database
  - Enforcement actions: https://www.sec.gov/litigation/suspensions.shtml
  - https://en.wikipedia.org/wiki/List_of_data_breaches
- **Risk Measures:**

4 issues found

  - High Risk: Have there been reported and documented security issues, with three or more security incidents? Yes
  - Moderate Risk: Have there been reported and documented security issues, with at least one to two security incidents? No
  - Low Risk: Have there been no reported and documented security issues? No

(RC-76) Supplier Organizational Security Risks → (RC-434) → (RC-435) → (RF-520) External Cyber Security Incidents Risks

- **Definition:**
  - This risk consid
    severity of exte
- **Data Source :**
  - Source: EDGA
  - Security and E
    https://www.sec
  - EDGAR databa
  - Enforcement a
  - https://en.wikip
- **Risk Measures:**
  - High Risk: Hav
    incidents? Yes
  - Moderate Risk:
    security incider
  - Low Risk: Have

(RC-105) Supplier Organizational Effectiveness Risks → (RC-538) → (RF-244) Supplier has frequently restructured through mergers & acquisitions

- **Rationale:**
  - Number of merg
    culture clash, siz
- **Data Source :**
  - Source: BvD, In
  - BvD Corporate
  - Investopedia: ht
    can-affect-comp
  - Harvard Busines
    15 M&A Risk Fa
- **Risk Measures:**
  - High Risk: Has t
    window? No
  - Moderate Risk:
  - Low Risk: Has t

(RC-7) Supplier Ethics Risks → (RC-13) → (RC-26) → (RF-568) Supplier and/or key management personnel (KMP) have been targets of national or international criminal investigation

- **Rationale:**
  - A company is lik
    illegal acts in the
- **Data Source :**
  - Source: Justice.
- **Risk Measures:**
  - High Risk: Is the
    registered by the
  - Moderate Risk:
    the US or regist
  - Low Risk: Is the
    department of ju

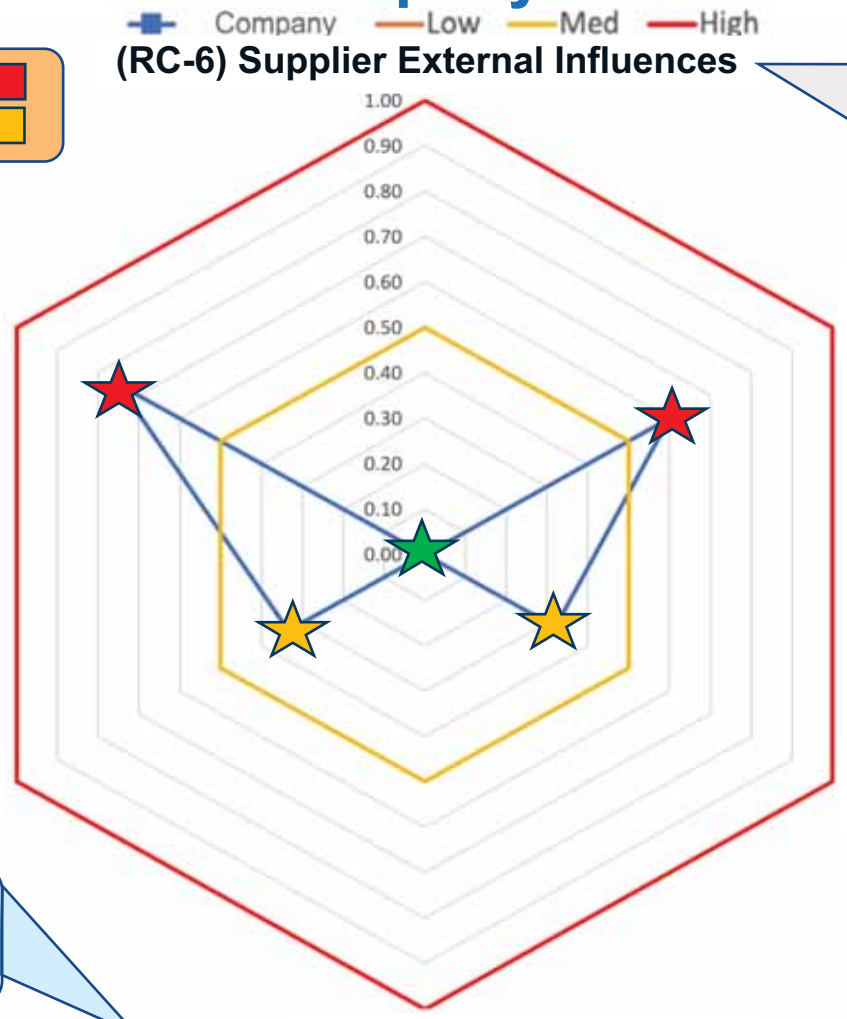
(RC-6) Supplier External Influences → (RC-5) → (RF-230) Supplier is wholly or partially owned by a foreign entity

- **Rationale:**
  - The likelihood that company operations are subject to antagonistic national interest is indicated by the potential allegiance of key partners and stakeholders.
- **Data Source :**
  - Source: Orbis BvD
  - From the Orbis Corp database, a list of stakeholders and their respective country was obtained (i.e., see Orbis Corp DB/ Report/ Corp Ownership/ Current Shareholders/). The list was then analyzed to determine the percentage of stakeholders from adversary and watch list countries.
- **Risk Measures:**
  - High Risk: Does this company have key stakeholder nationality of >= 15% from adversary or US Treasury watch list countries? No
  - Moderate Risk: Does this company have key stakeholder nationality of < 15% and > 5% from adversary or US Treasury watch list countries? No
  - Low Risk: Does this company have key stakeholder nationality of <= 5% from adversary or US Treasury watch list countries? Yes

None from adversary or US Treasury watch list country

MITRE

Company 10



(RC-6) Supplier External Influences

13. Ownership and Control Risks
14. National Corruption
15. Political Vulnerability
16. National Governance Risks
17. Geopolitical Instability
18. PEP Members in Corporate Leadership

7. External Cyber Security Incidents Risks
8. External Security Compromises/Breaches Risks

(RC-76) Supplier Organizational Security Risks

(RC-13) Supplier Financial Stability Risks

1. Supplier may be unable to service its debts
2. Supplier has concerning inventory turnover rate
3. Supplier does not maintain adequate liquidity
4. Supplier has history of late payments
5. Supplier is not sufficiently profitable
6. Supplier falls behind its competitors in R&D investment level

9. Intellectual property litigation involving supplier
10. Supplier sanction list status
11. Supplier and/or key management personnel (KMP) have been targets of national or international criminal investigation

(RC-7) Supplier Ethics Risks

(RC-105) Supplier Organizational Effectiveness Risks

19. Natural Disaster Risks
20. Geographic Concentration Risks
21. Mergers & Acquisition Frequency Risks
22. Operational Volatility Risks
23. Sustainability Risks
24. Corporate Ownership Risks
25. Diversity and Inclusion Risks

12. Citizenship of key management personnel (KMP) and employees is in country/ies of concern

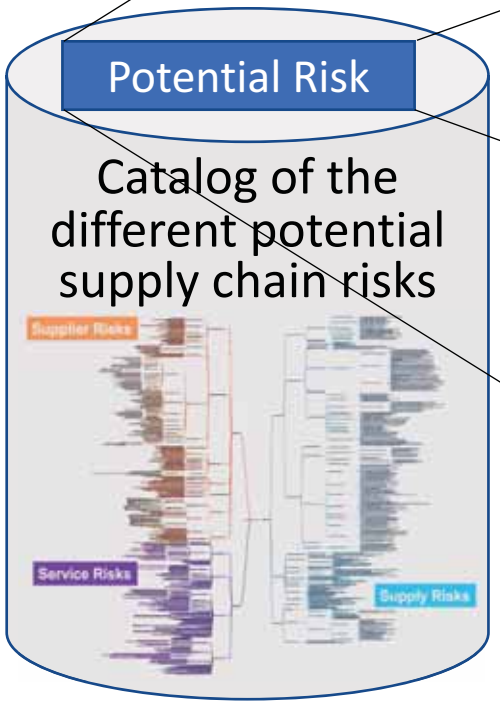
(RC-4) Supplier Susceptibility

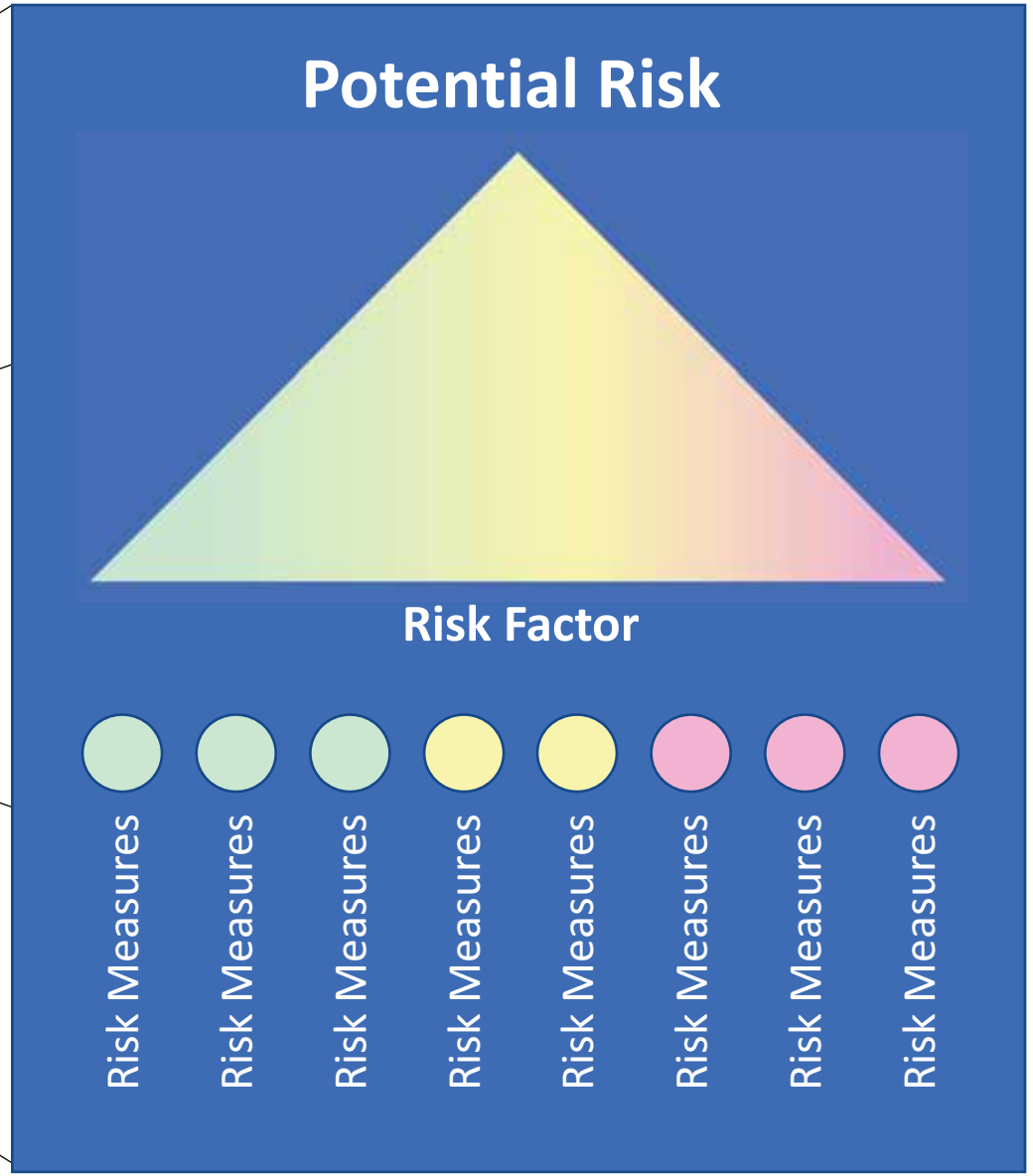
Supplier and Public Data Profile

Using 6 Risk Categories With 25 Risk Factors

MITRE

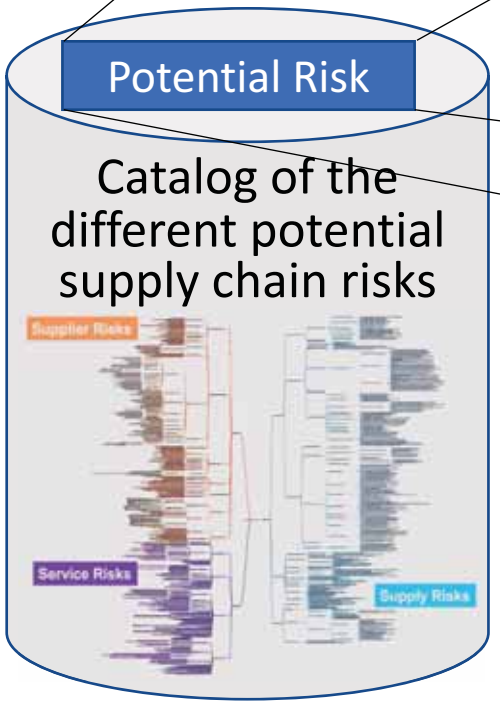
Risk Measures Bring Data to the Assessment of Risks



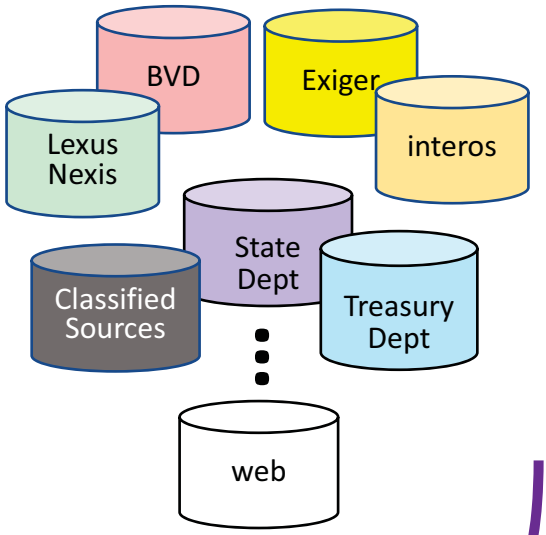


MITRE

Pulling it Together



Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information



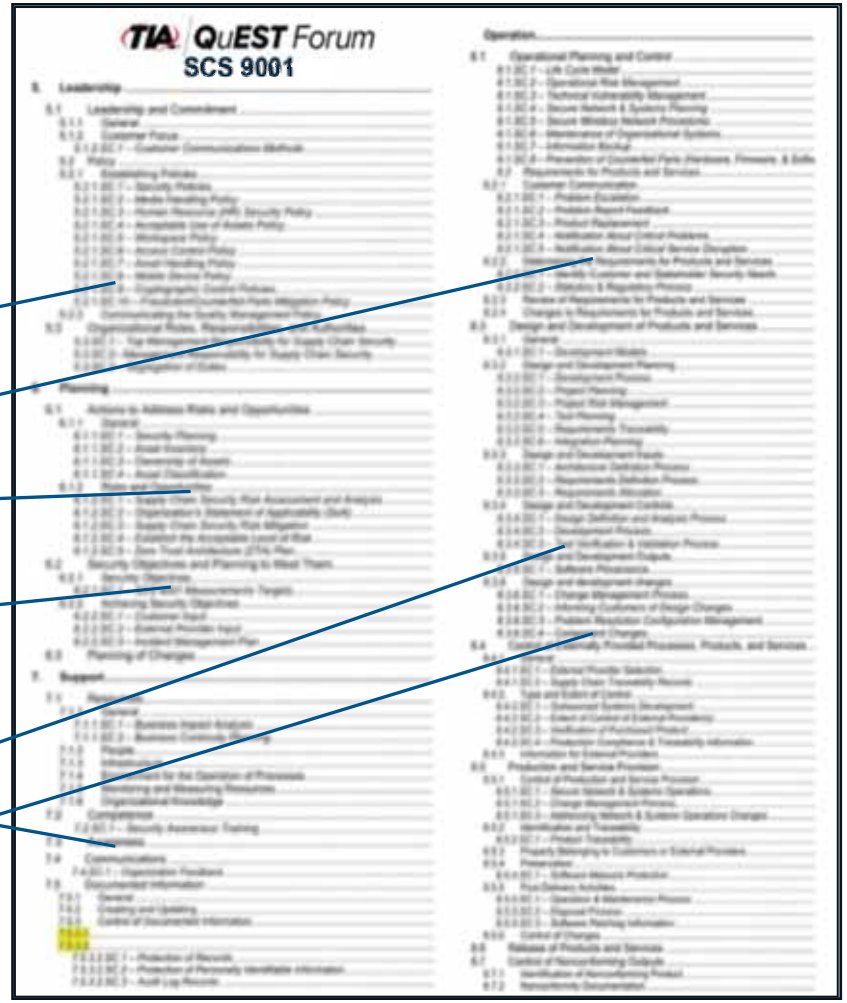
Mapping SoT Risks to Assessment Information Sources / Standards

Supplier Risks

Supply Risks

Service Risks

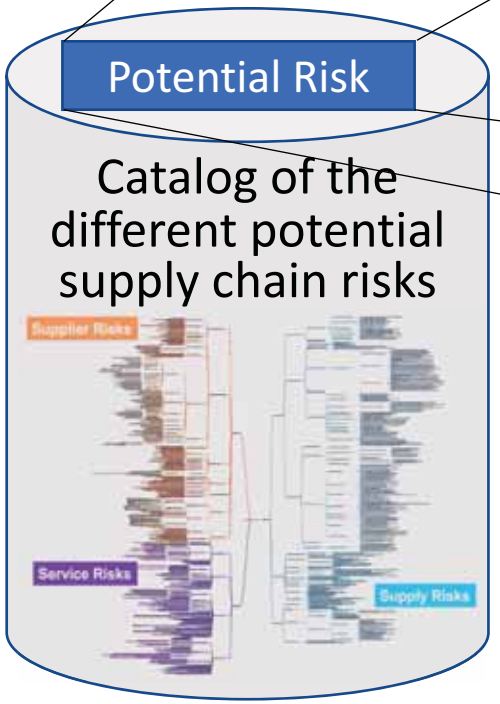
NOTIONAL



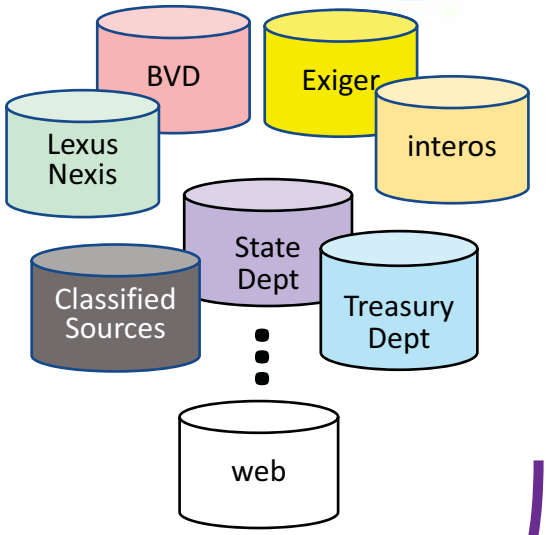
TIA SCS 9001, ISA/IEC 62443, , ISA/IEC 62443 or ISO/IEC 27001/2, ISO/IEC 27036, ISO/IEC 20243, ISO/IEC 27036, NIST CSF 1.1, NIST 800-37, NIST SP 800-161, NIST 800-53, NIST 800- 171, CMMC Level 3-5 Assessment, ITAR, NDAA Section 889, TAPA FSR, NISP Facility Clearance, C-TPAP, SAE AS649, SAE AS6171, SOC 2 Type 2

MITRE

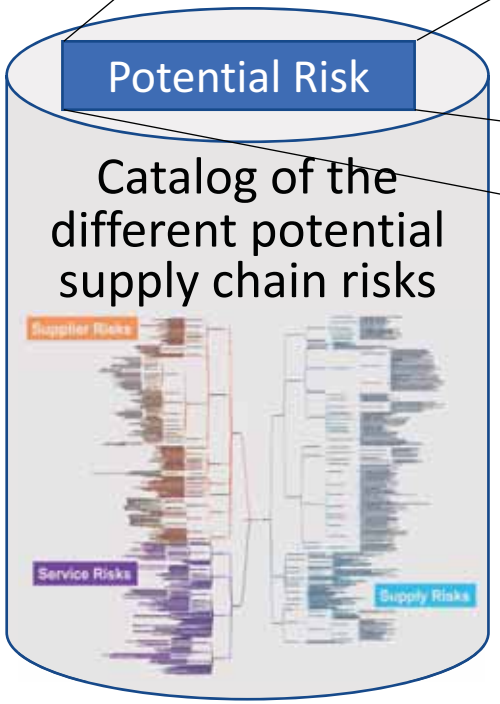
Pulling it Together

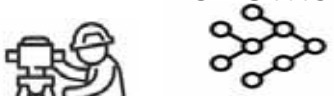


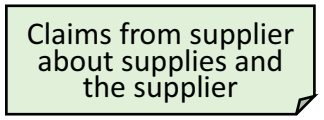
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information

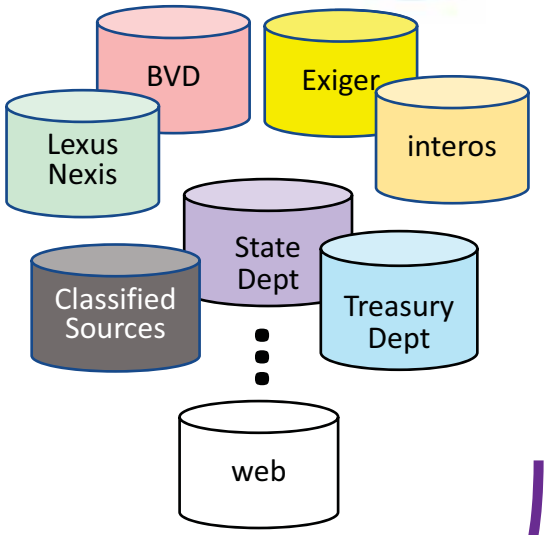


Pulling it Together



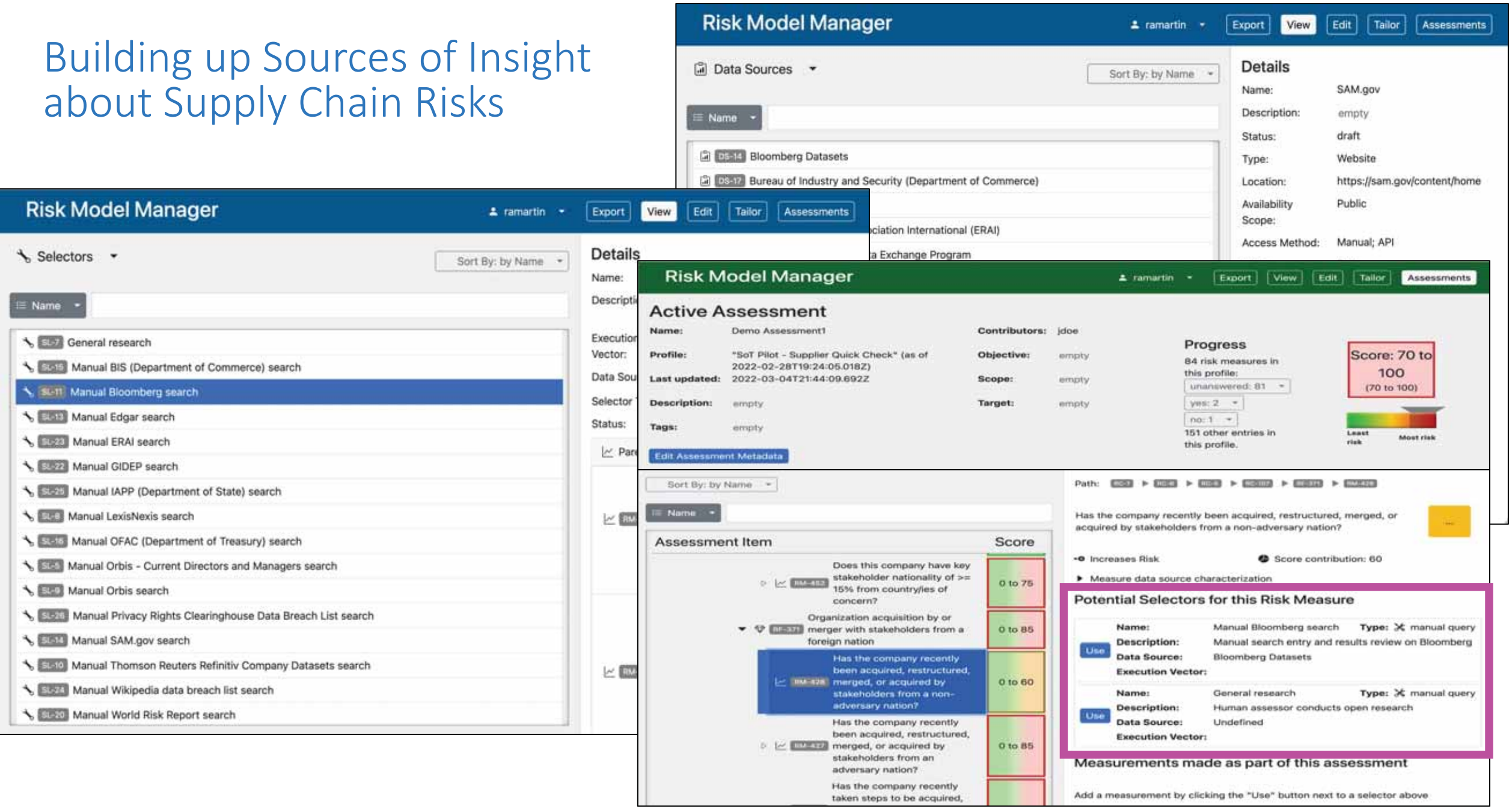






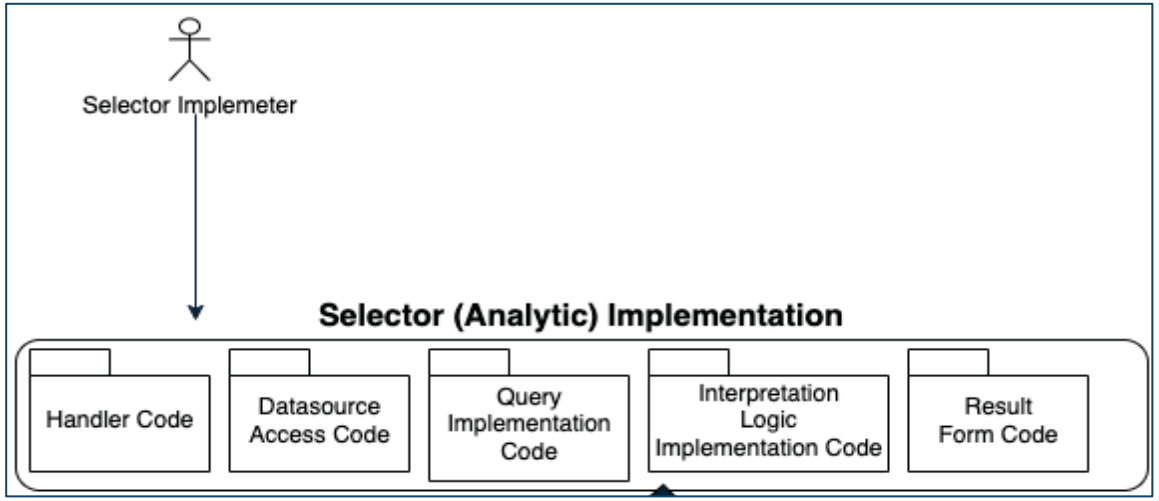
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information
Data / information

Building up Sources of Insight about Supply Chain Risks



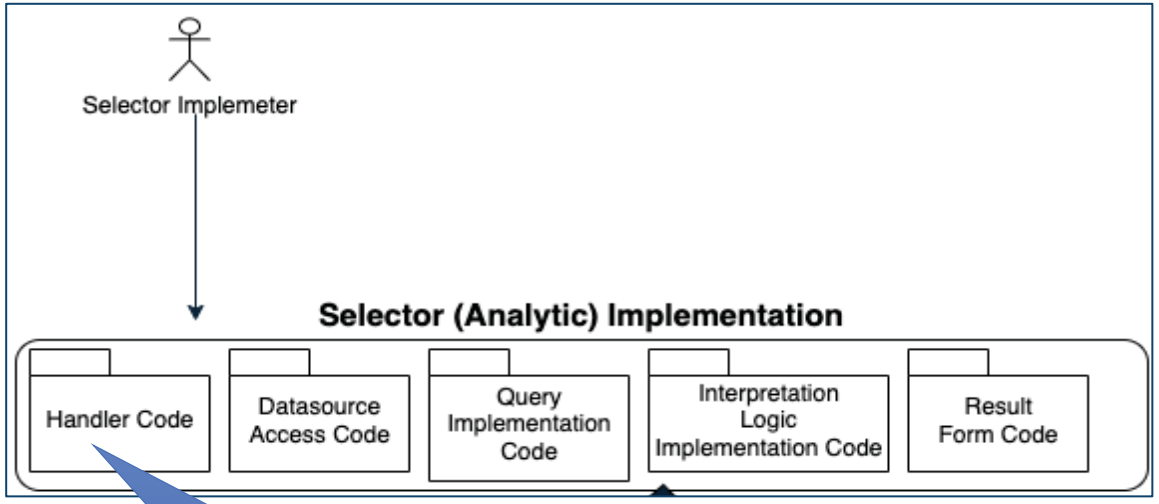
SoT Risk Model Manager Automation Technical Approach

Connecting to structured data



SoT Risk Model Manager Automation Technical Approach

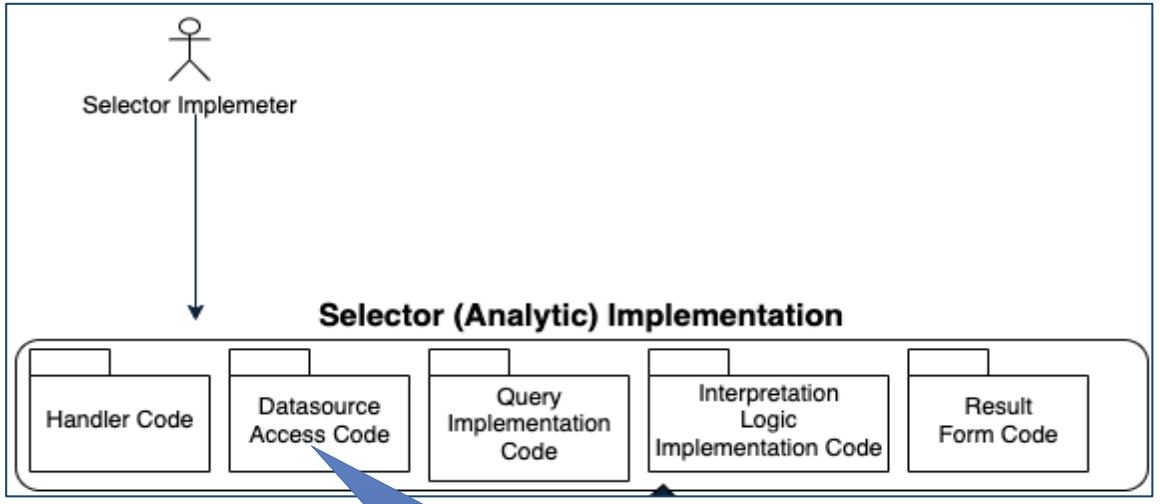
Connecting to structured data



Where do I go to get the data about a particular risk factor?

SoT Risk Model Manager Automation Technical Approach

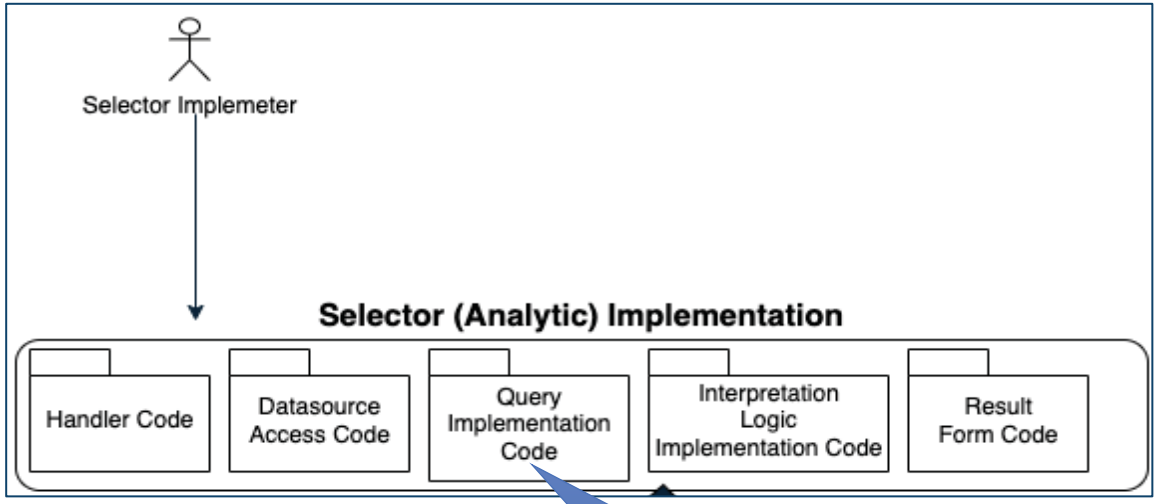
Connecting to structured data



How do I get access to the data?

SoT Risk Model Manager Automation Technical Approach

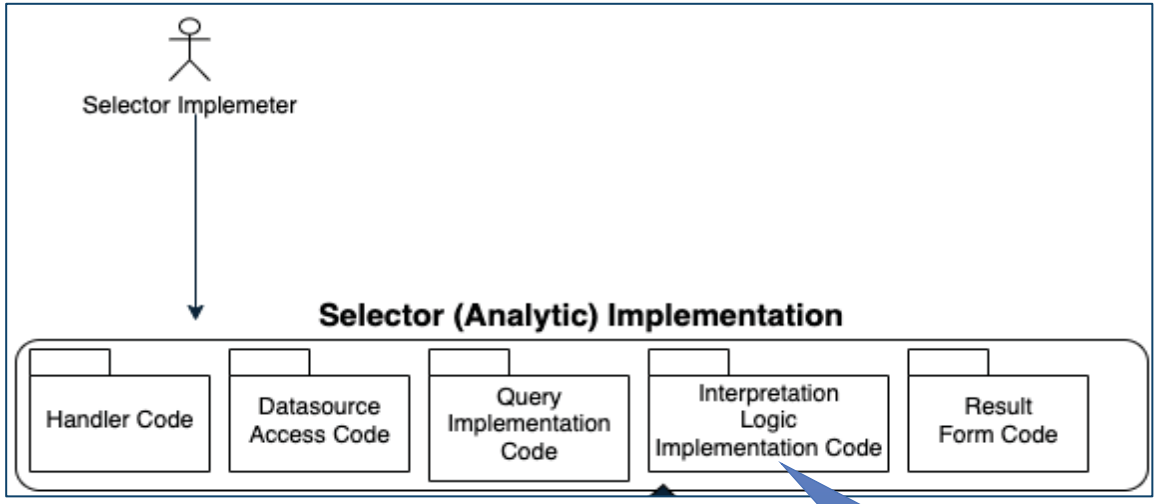
Connecting to structured data



What are the details for retrieving the data?

SoT Risk Model Manager Automation Technical Approach

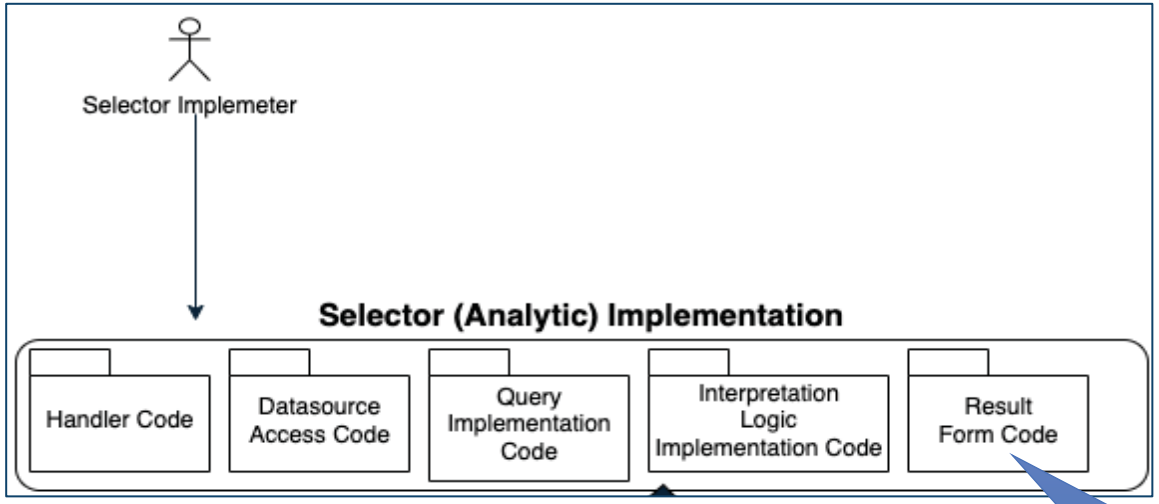
Connecting to structured data



How do I interpret the data to determine if the risk is present?

SoT Risk Model Manager Automation Technical Approach

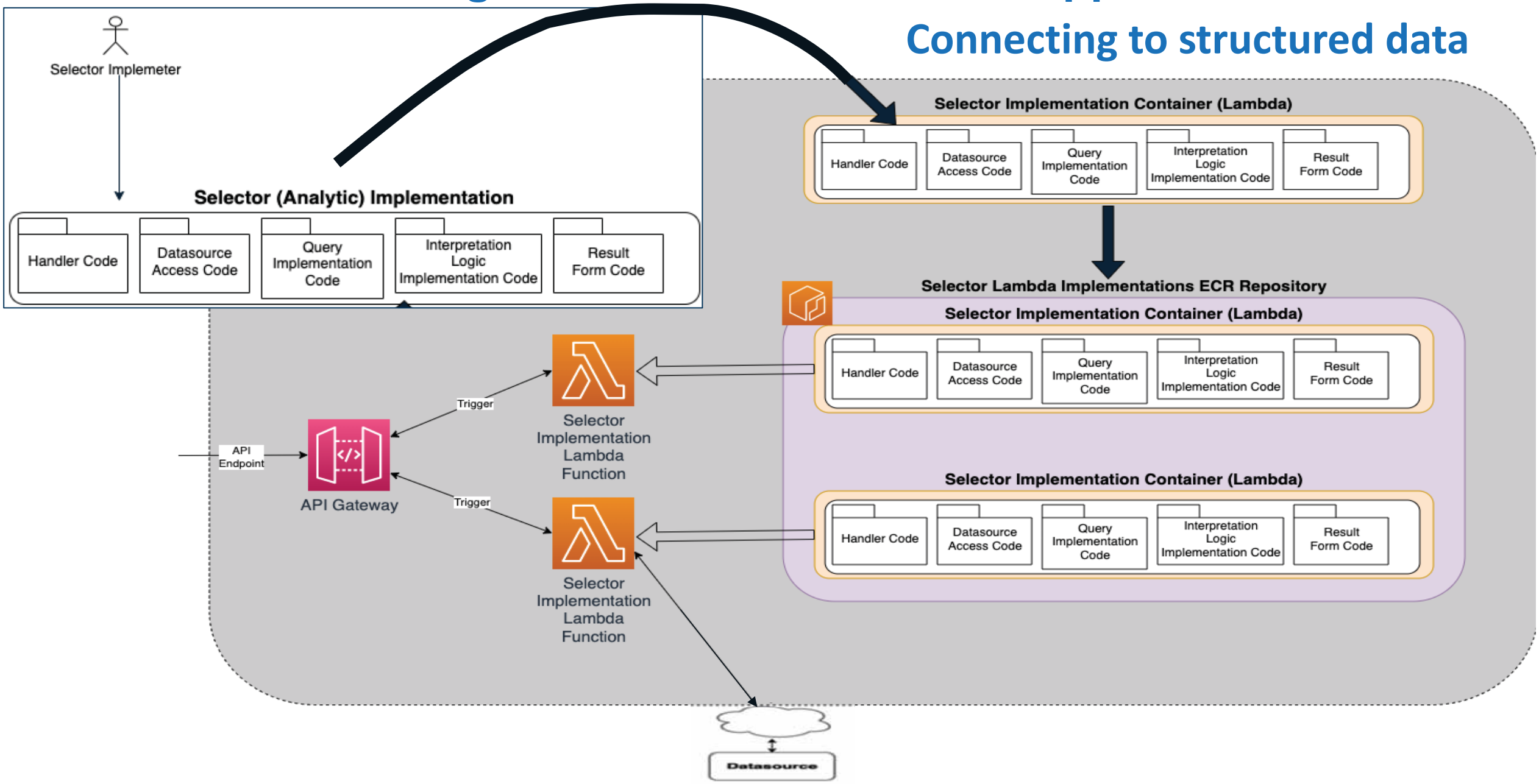
Connecting to structured data



Structure the answer and supporting data to send back to the RMM application.

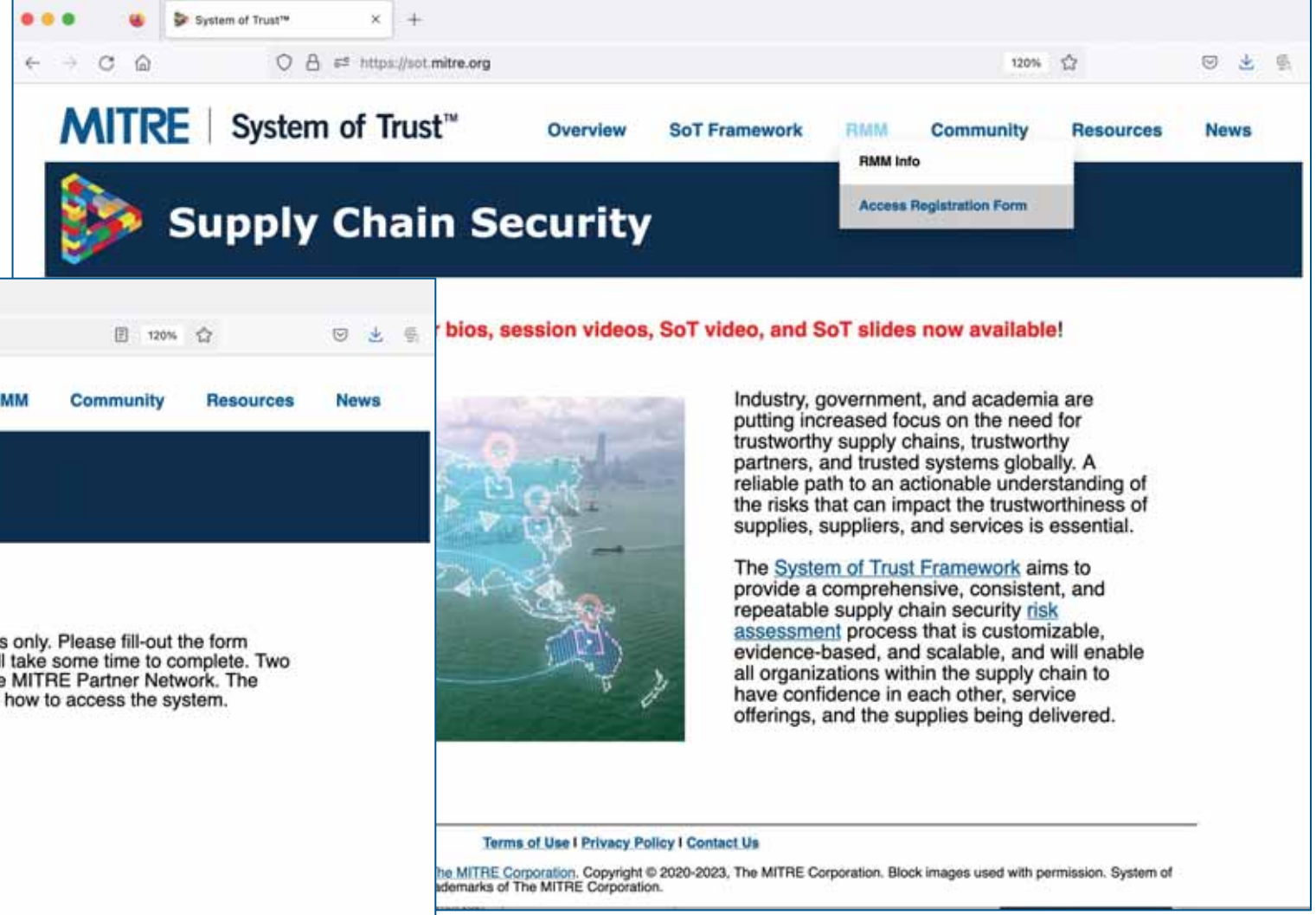
SoT Risk Model Manager Automation Technical Approach

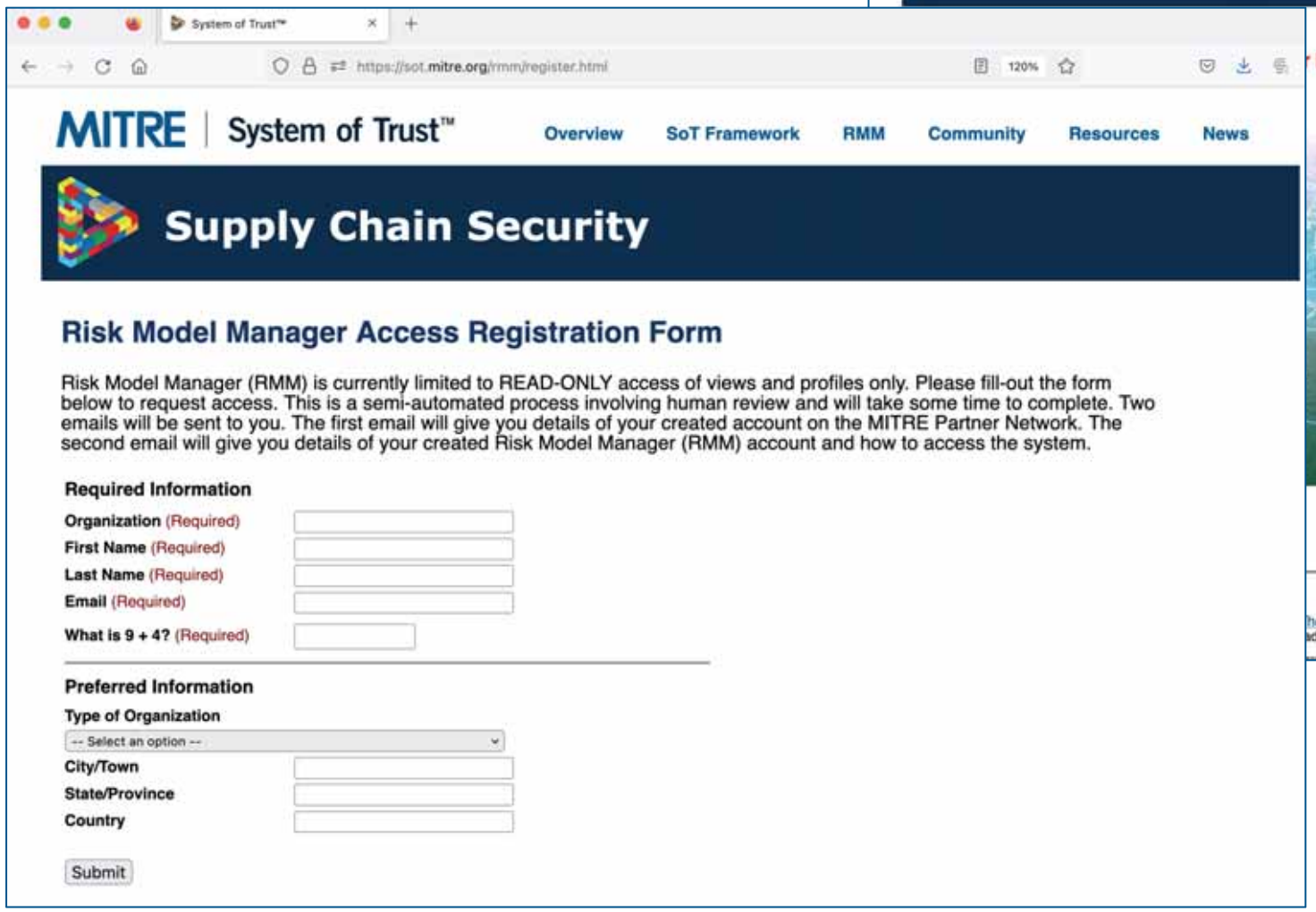
Connecting to structured data



Getting Access to RMM

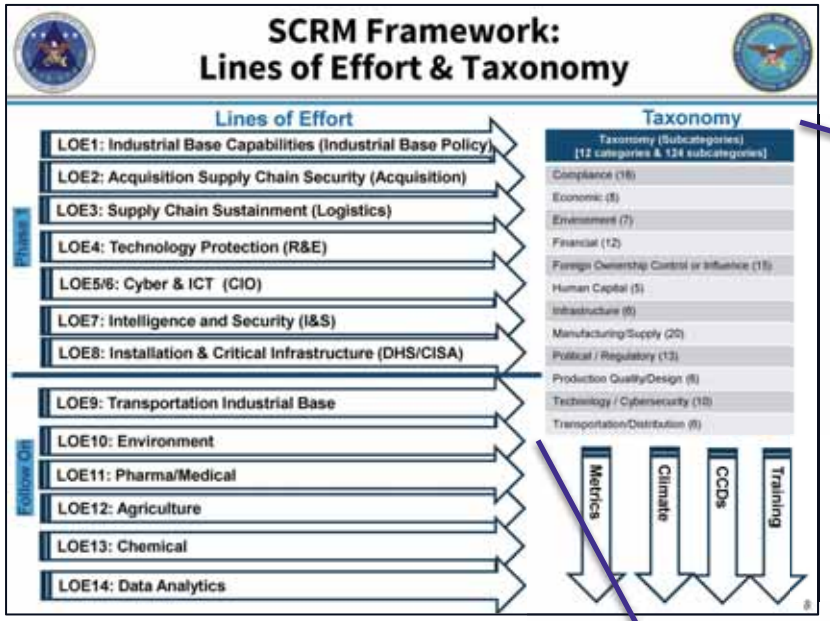
https://sot.mitre.org/rmm/register.html





SOT.MITRE.ORG

DoD Supply Chain Resiliency Work Group (DoD SCRM Taxonomy)



12 Categories &
124 subcategories

DoD Notional SC Risk Taxonomy Categories

Compliance	Political/Regulatory	Economic	Foreign Influence	Manufacturing/Supply	Financial	Human Capital
Contractor Misconduct	Political Government Changes	Demand Shocks	Weaponized Merger/Acquisition	Obsolescence/Diminishing Manufacturing Sources and Material Shortages (DMSMS)	Liquidity	Industrial Unrest, Labor Dispute
Past Suspension or Debarment	Interstate Conflict	Currency Fluctuations	Partnership with State Owned Entity	Throughput, Production Delays	Cyclical Risk	Loss of Talent
Defective Pricing, Price Fixing	Terrorism	Economic	Industrial Espionage	Outsourcing	Unstable Payment Performance	Lack of access to workforce
Security Enforcement Actions	Corruption	High Unemployment	Proprietary Info-Theft of Trade Secrets	Extended Lead Times	Lack of Funding	Work Stoppage
Conflict Minerals in the Supply Chain	Border Delays	Inflation/Hyperinflation/Stagflation/Wage Danger	Executive Pressure	Inventory or Capacity Incidents	Dependency on Contracts	Boycotts/Societal Risks
Anti-Trust/Monopolistic Practices	Government Shutdowns	Price Volatility/Market Risk	Sabotage	Equipment Downtime	Bankruptcy	**Transportation/Distribution**
Import, Export Violation	Territorial Disputes	Recession, economic slowdown	Violent Unrest	Sole Source	Profitability Measures	Transportation Network Disruption
Fraud (Procurement, Government)	New Regulations/Changes in Policy	Economic Instability	Cyber Espionage	Concentration	Cost Overruns	Poor On-Time Delivery Performance (On-time delivery, right location)
Ethics Violations	Trade War Restrictions	**Technology/Cybersecurity**	Counterintelligence	Inventory Shortages/Material Shortages	Off-shore Leaks/Database	Poor Shipment accuracy (Correct)
–Human Rights Violations (Ethics Violations)	Watch List	Critical HW/SW Vulnerability	Counterintelligence Analysis	Material Sources	Financial Crime	Loss of Cargo
–Forced Labor (Ethics Violations)	Potential Political Exposure	Cyber Attack Espionage	Counterintelligence Collection	Parts/Spares Inventory Shortages		Accidents
–Trafficking in Persons (Ethics Violations)	Environmental Protection	IT Disruption, Connectivity Issues	Foreign Intelligence Entity	Single Sources		Change in Trade Policy (Containers in Ports)
Workers Health & Safety – OSHA (Ethics Violations)	**Government Policies**	Loss or Theft of Personally Identifiable Information	Nationalization	Order Fulfillment/Requisitions		
–Insider Threat (Ethics Violations)	**Environment**	Unsecure Disposal	**Production Quality/Design**	Industrial Capacity		
Legal and Reputational	Natural Disaster	Operational Security Violations	Counterfeit Parts	Industrial Capability		
Occupational Safety and Health	Extreme Weather	Malicious Intrusion	System Failure	Reclamation/Utilization		
Contract Non-Compliance	Pandemic	IT Implementation Failures	Non-Conformance	Adjacency Risk		
	Wildfire	Data Breach	Non-MIL Commercial			
	Chemical Spill/Release Risk	Obsolescence	Unreported Supplier Recalls			
	Climate					
	Man-made Risk					

MITRE SYSTEM OF TRUST

DoD SCRM TAXONOMY

RC: Financial

SC: Liquidity

(RC-1) Supplier Risks

(RC-13) Supplier Financial Stability Risks

(RC-257) Short-term Financial Health Risks

(RC-256) Financial Stewardship Risks

(RC-260) Adverse Market Factors

(RC-258) Long-term Financial Health Risks

(RC-262) Foreign Financial Obligations

(RF-31) Supplier is not sufficiently performing

(RF-197) Supplier has concerning inventory rate

(RF-200) Supplier does not maintain adequate liquidity

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

(RM-416) Quick Ratio > 1?

(RM-415) Quick Ratio = 1?

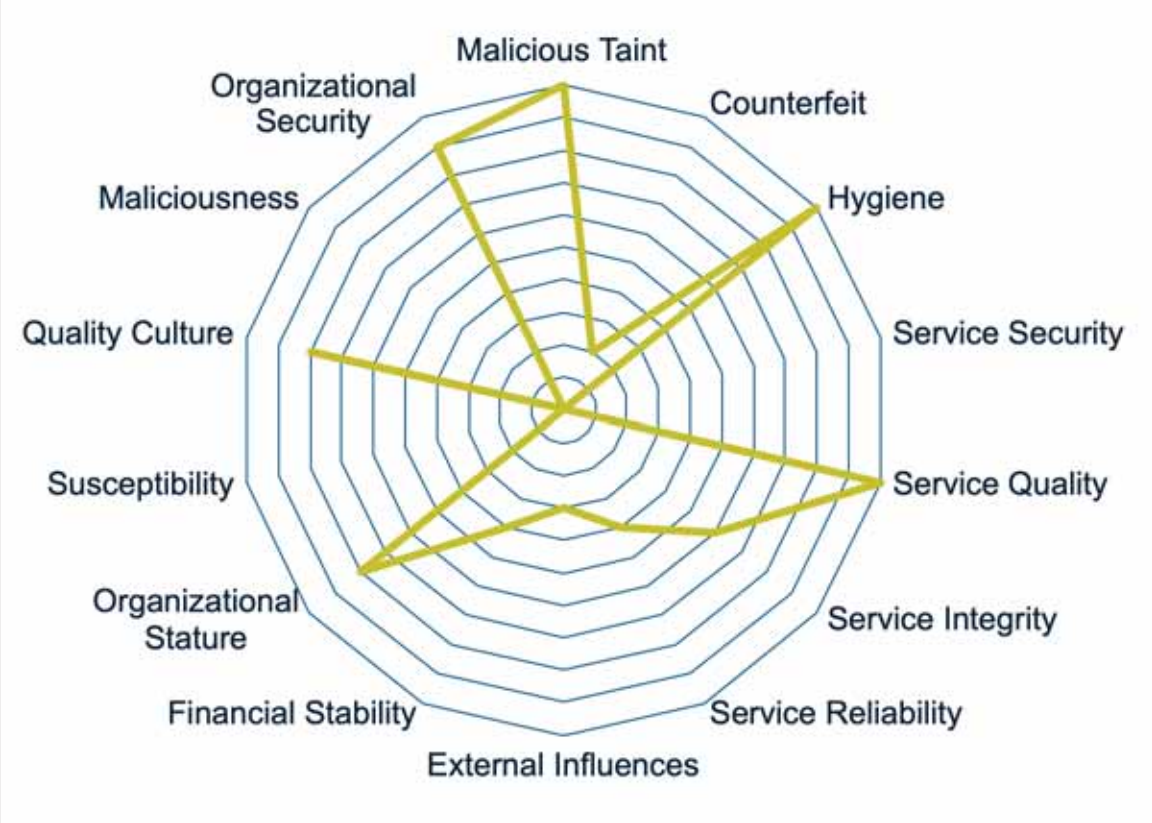
(RM-414) Quick Ratio < 1?

GOAL for use of SoT in Industry and Government…

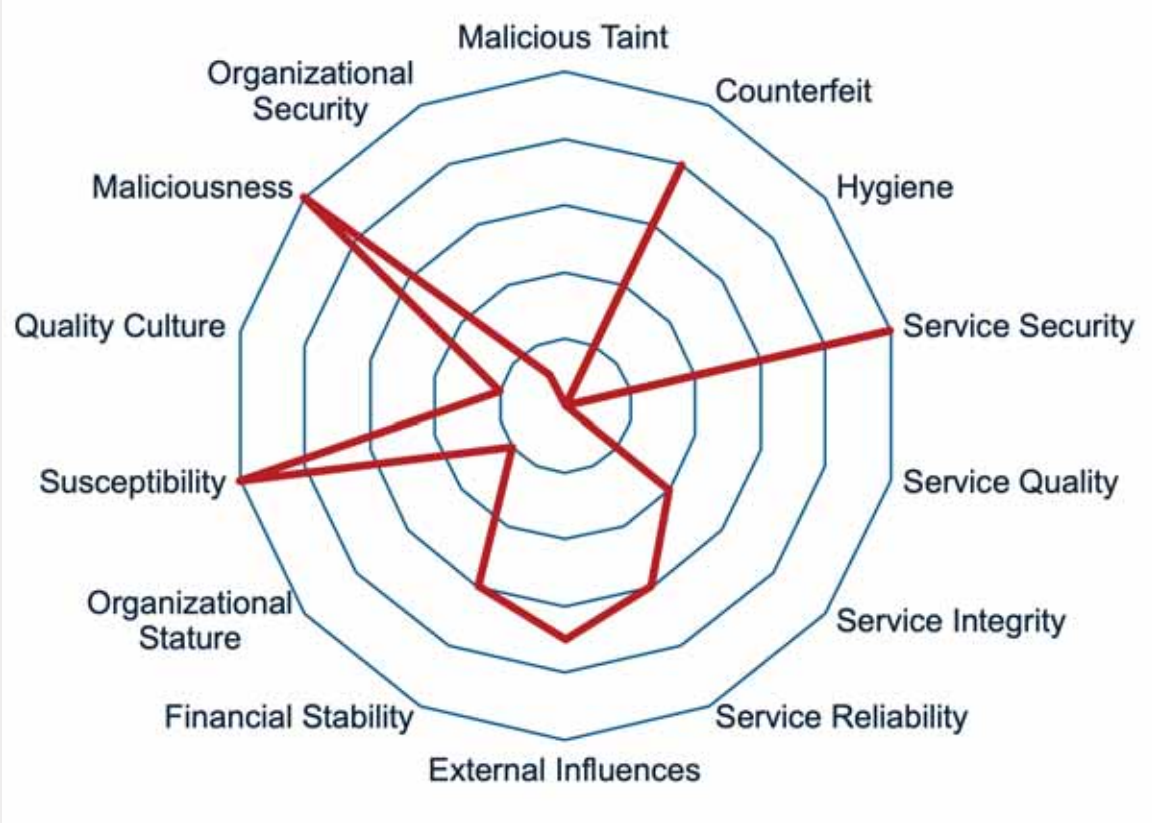
Risk Model Manager

Demo user | Export | View | Edit | Tailor | Assessments

Top-Level Concerns Vendor/Product A

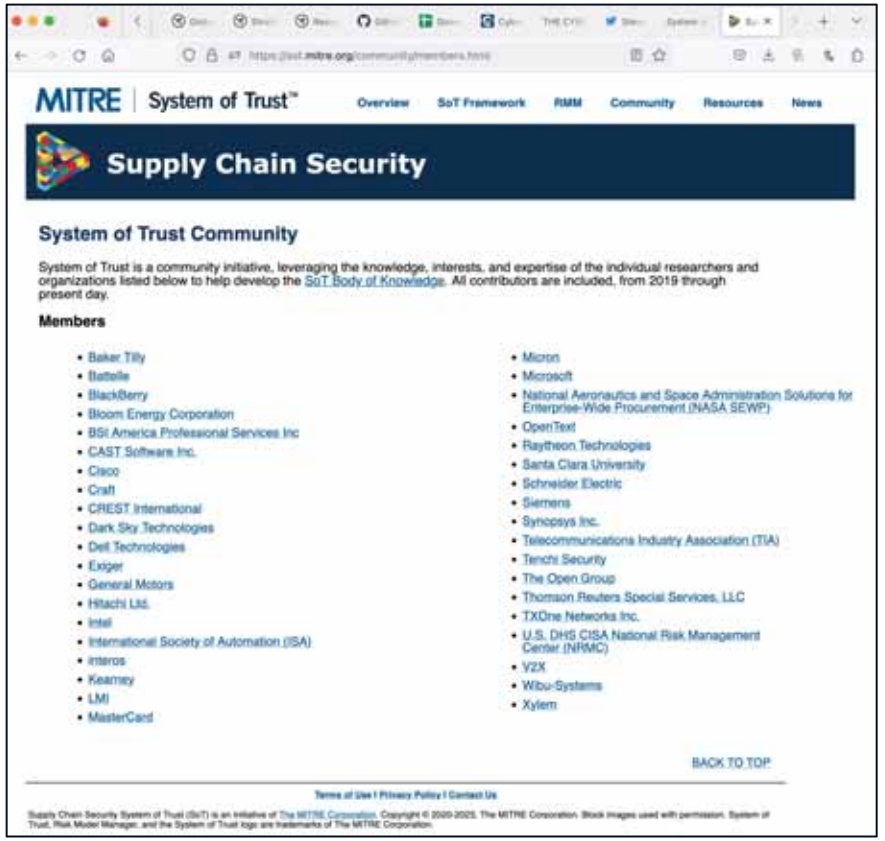


Top-Level Concerns Vendor/Product B



MITRE

System of Trust™ Community



System of Trust risk catalog out for community review

MITRE'S System of Trust™ Body of Knowledge

REVIEW VERSION 1.2

January 17, 2022

System of Trust Body of Knowledges as a Hierarchy

(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 st

(RF-31) Supplier is not sufficiently profitable

Definition: This risk considers whether a company c shareholders in the form of profits.

Possible Measures:
(RM-430) Is the company's gross profit margin <=90
(RM-432) Is the company's gross profit margin >90%
(RM-431) Is the company's gross profit margin <=11

(RF-858) Supplier does not maintain adequate cashf

Definition: This risk considers whether a company c

Possible Measures:

(RF-197) Supplier has concerning inventory turnove

Definition: This risk considers whether a company p

Possible Measures:
(RM-422) Does the company have an inventory turn
(RM-423) Does the company have an inventory turn
(RM-421) Does the company have an inventory turn

(RF-200) Supplier does not maintain adequate liquid

Definition: This risk considers whether a company n

Possible Measures:
(RM-416) Does the company have a quick ratio >17 quick ratio <17 quick ratio <17

(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 (p norms to cause harm.

Level 3 (RC-155) Supply Chain Management Integrity Risks

Definition: Risks that increase the likelihood a supply (

Level 4 (RC-159) ICT Hardware Supply Chain Integrity R

Definition: Risks that increase the likelihood ar chain management.

(RF-99) Printed circuit board manufacturer r

Definition: This risk considers whether a pri manufacturer by an upstream su

Possible Measures:

(RF-16) Chip fabrication receives and uses ta

Definition: This risk considers whether a chi foundry by an upstream supplier them in production.

Possible Measures:

Level 4 (RC-162) Software Supply Chain Integrity Risks

Definition: Risks that increase the likelihood a management.

(RF-1093) Manufacturer outsources the func

Definition: Risk that the manufacturer no lo the product production and outs may be more exposed to tampers the particular manufacturer of ir

Possible Measures:

(RF-1094) Manufacturer outsources the func

Definition: Risk that the manufacturer no lo ownership and control of the ma

Possible Measures:

Level 3 (RC-149) Manufacturing Process Integrity Risks

Definition: Risks that increase the likelihood a supply integrity controls.

System of Trust Risk Hierarchy in Table Form

System of Trust Body of Knowledge Risk Hierarchy in Table Form

Level 1 Level 2

(RC-1) Supplier Risks							(RC-2) Supply Risks			(RC-3) Service 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.							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).			Definition: Risks related to characteristics of a service, including their supply chain provenance and pedigree, that may potentially impact consumers of that service.			
(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 Reliability Risks	(RC-286) Service Security Risks	(RC-288) Service Integrity Risks
(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-127) Unsanctioned Manufacturing	(RC-214) Supply (product) Resilience Risks	(RC-563) Service Quality Infrastructure Pedigree Risks	(RC-598) Service Infrastructure Redundancy Risks	(RC-294) Service 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-126) Mislabeling	(RC-213) Supply (product) Security Risks	(RC-562) Service Quality Infrastructure Provenance Risks	(RC-302) Service Specific Reliability 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-118) Technical Authenticity Risks	(RC-201) Supply (product) Quality Risks	(RC-300) Service Specific Quality Risks	(RC-687) Service Reliability Infrastructure Provenance Risks	(RC-296) Service Security Infrastructure Pedigree Risks	(RC-575) Service Integrity Infrastructure Pedigree 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-128) Copycat Manufacturing			(RC-590) Service Infrastructure Diversity 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-588) Service Reliability Infrastructure Pedigree 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-150) Facilities Integrity Risks						
							(RC-54) Packaging Integrity Risks						
							(RC-156) Maintenance Integrity Risks						

1

(RC-287) Service Quality 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 Reliability Risks	(RC-286) Service Security Risks	(RC-288) Service Integrity Risks

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.

79

Examples of System of Trust Engagements

- DHS S&T Program Office
- American Bar Association (ABA) Technology Meeting
- Industry Technology & Innovation Roundtable
- Open Group July Member Meeting Plenary
- ABA IoT National Institutes Panel 2020
- DoD/DoE NNSA Software Assurance Community of Practice
- DHS S&T FVEYES Supply Chain Workshop
- EOP/OMB – Maria Roat (Dep Fed CIO at OMB)/ Camilo Sandoval (Fed CISO)
- EOP/OMB w/Lesley Field / Mathew Blum / Jeremy McCrary – OFPP Team
- Raytheon Technologies Product Cybersecurity Tech Exchange
- Senate Homeland Security and Governmental Affairs Committee staff
- IIC Winter 2020 Quarterly Member Meeting
- House Homeland Security Committee staff
- ABA SciTech Lawyer article – Winter 2021 Issue
- GAO Supply Chain Report Authoring Team
- ATIS 5G/SC Working Group
- House Armed Services Committee staff
- Senate Armed Services Committee staff
- House Oversight Committee staff
- Chris DeRusha (Fed CISO)
- Soraya Correa (DHS OCPO)
- DHS CSWG Supply Chain Subgroup
- USEA Energy Technology and Governance Program UCSI Working Group
- ABA IoT National Institute
- IIC Summer Meeting
- Manufacturing Industry Leadership Council meeting
- Global Industry Organizations' Smart Manufacturing Workshop
- SAE G-32 Hardware WG meeting
- New England Council event
- NSTAC Software Assurance Sub-Committee
- Aerospace Industries Association
- TIA | QuEST Forum Supply Chain Security 9001 Webinar
- Staff of Rep. Elissa Slotkin
- HASC critical defense supply chain TF report Staff
- ADM Mauger US Coast Guard Assistant Commandant for Prevention Policy (CG-5P)
- Navy Research, Development & Acquisition (ASN/RD&A)
- House Committee on Oversight and Reform
- Q3 IIC Information Day - Fuel Your Digital Transformation Journey
- CISA NRMC Supply Chain Trustworthiness Framework IPT
- CISA Standards Area Lead for C-SCRM
- MDA Ground Missile Defense PM
- DoE CESER Cybersecurity Senior Advisor

- House Permanent Select Committee on Intelligence
- Electric Power Research Institute (EPRI)
- Common Attack Pattern Enumeration (CAPEC) Workshop
- HHS ASPR RISC 2.0 Leadership Team
- DoC SCRM Team
- IIC March 2022 Event
- SW Supply Chain Integrity and SoT to ESF Team
- CMS CIO
- ELISA Workshop
- CISQ Webinar
- Software Supply Chain Security Webinar
- System of Trust with VA SCRM Team
- SW Supply Chain Integrity and SoT to RKVST Team
- SW Supply Chain Integrity and SoT to Dell Team
- American Bar Association (ABA) Technology Meeting
- RSA Conference 2022
- Open Group July Member Meeting Plenary
- Hacks In Taiwan Conference 2022
- Hot Topics in Supply Chain Security 2022 Summit
- NDIA Microelectronics Trust and Assurance Workshop
- ABA IoT National Institute 2022
- CISQ Resilience Summit
- Third Party Risk Management Symposium in Sao Paulo Brazil
- Global Semiconductor Alliance (GSA) Trusted IoT Ecosystem for Security (TIES)
- The Annual Computer Security Applications Conference (ACSAC)
- SC Magazine Paul's SC Weekly Podcast
- George Washington Univ. CoE in Public Leadership Video Roundtable
- DHS-NIST-DoD-GSA co-sponsored Software and Supply Chain Forum
- Advanced Technology Academic Research Center (ATARC) Supply Chain WG
- Cyber Physical Systems Symposium in Tokyo Japan
- IIC March 2023 Event
- MITRE Cybersecurity Days 2023
- Senate Sargeant at Arms Team
- Australian CISRO
- British Standards Institute BSI.Connect conference
- ABA Pre-RSA Tech Committee Meeting
- RSA Conference 2023
- House Committee on Oversight and Accountability
- Tenchi Security
- NDIA New England Annual Conference
- SSCA Spring Forum
- others...

Executive Acquisition

Congressional Groups

MITRE

System of Trust (SoT)

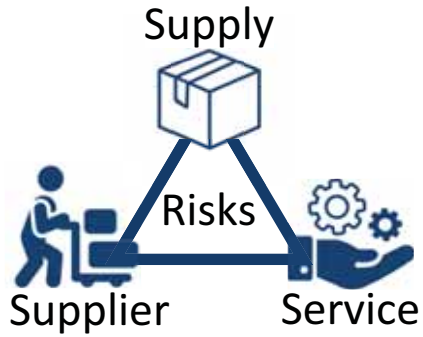
SoT is not:

- a magical database of supply chain information
- a Supply Chain Risk Management approach
- a Logistics Management approach
- a Cyber Supply Chain Risk Management approach

SoT is:

- a compliment to SP 800-161 and other risk management guidance by enumerating the supply chain risks that may need to be managed
- a strategic, widely-adoptable, tailorable, data-driven analysis framework to promote assessment of the appropriate elements of a supply chain
- a nexus of assessment capabilities, standards, & information sources that is leverageable by MITRE, government and industry for repeatable, impactful analysis required for supply chain hygiene & due-diligence

System of Trust Components



A Language / Catalog of Supply Chain Risks w/how to assess, contract, & COAs

Risk Model Manager

A Content Manager for the Risk Catalog

SoT Community

An external group working together on SoT

Public Website

An external place to share SoT capabilities

SoT Demonstrator

An Evaluation demo capability "art of the possible"

We Speak SoT™

SoT Compatibility

An Adoption Acceleration Program

A way to show supply chains

SoT Capability

SoT Risk Model Manager for customers/projects

MITRE

System of Trust Plans with Sponsors and the Community

Assessment Capabilities for Sponsors, Industry and Academia

Training Sponsors & Industry on the SoT methodology, content, and platform

Standards and best practices oriented around SoT

Evolving SoT Body of Knowledge with Domain SMEs to enhance Risk Factors

Mapping SoT to Industry and Government standards and assessment mechanisms

Active Feedback with communities on enhancements to SoT

No-Cost Licensing Risk Model Manager tool & SoT content to Industry for integration in their own assessment practices and offerings

For more information…


CUTTER Business Technology Journal

Management, Innovation, Transformation

Vol. 33, No. 5 2020 ● REPRINT

"A system of trust needs to have a pervasive, holistic approach to everything that can be of concern and needs to be truly effective in supporting our management of all items of concern."

The Supply Chain Security System of Trust:
A Framework for the Concerns Blocking Trust in Supplies, Suppliers, and Services

by Robert A. Martin

In this article, Robert A. Martin addresses the complete

https://www.cutter.com/offer/supply-chain-security-system-trust

SoT.MITRE.ORG

SoT@MITRE.ORG

TheSciTechLawyer WINTER 2021


TRUSTING OUR SUPPLY CHAINS:
A COMPREHENSIVE DATA-DRIVEN APPROACH

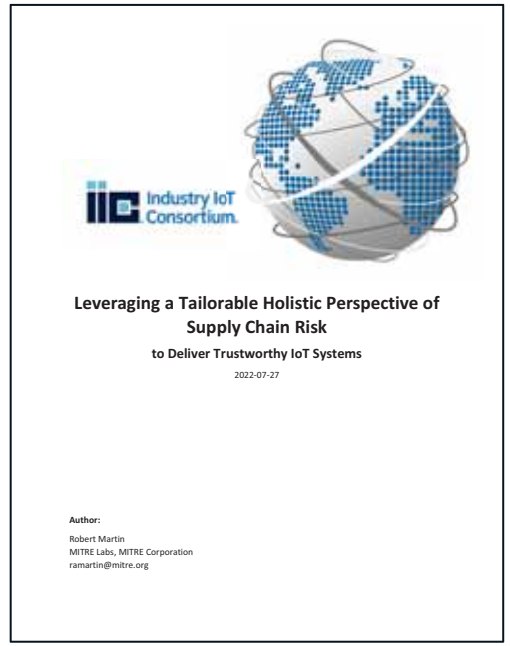
By Robert A. Martin

Trust and trustworthiness of supply chains is an issue confronting communities around the world, including U.S. government agencies and the thousands of commercial enterprises that support them.

Congressional Actions

MITRE

https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach


Industry IoT Consortium

Leveraging a Tailorable Holistic Perspective of Supply Chain Risk

to Deliver Trustworthy IoT Systems

2022-07-27

Author:

Robert Martin
MITRE Labs, MITRE Corporation
ramartin@mitre.org

https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/07/4-JOI_20220727_Leveraging_a_Tailorable_-Holistic_Perspective_of_Supply_Chain_Risks_to_Deliver_Trustworthy_IoT_Standalone-Systems_Standalone.pdf


SUPPLY CHAIN SECURITY – IT'S EVERYONE'S BUSINESS

For more than half a century, or for as long as the United States has had what has been described as a Military Industrial Complex, the U.S. Defense Industrial Base (DIB) has identified challenges, dedicated resources toward solving them, and attempted to learn from past mistakes.

https://www.mitre.org/publications/technical-papers/supply-chain-security-it's-everyone's-business

MITRE