#RSAC

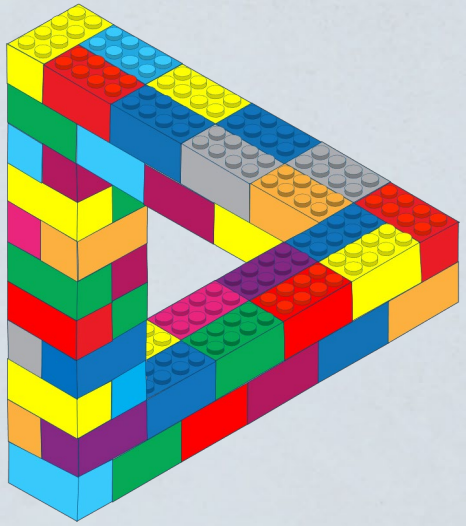
RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PDSC-T08**

Addressing Supply Chain Security Risks - MITRE's System of Trust™



MITRE | System of Trust™

Robert Martin

Sr. Software and Supply Chain Assurance Prin. Eng.
Cross Cutting Solutions and Innovation Dept.
Cyber Solutions Innovation Center
MITRE Labs

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Disclaimer

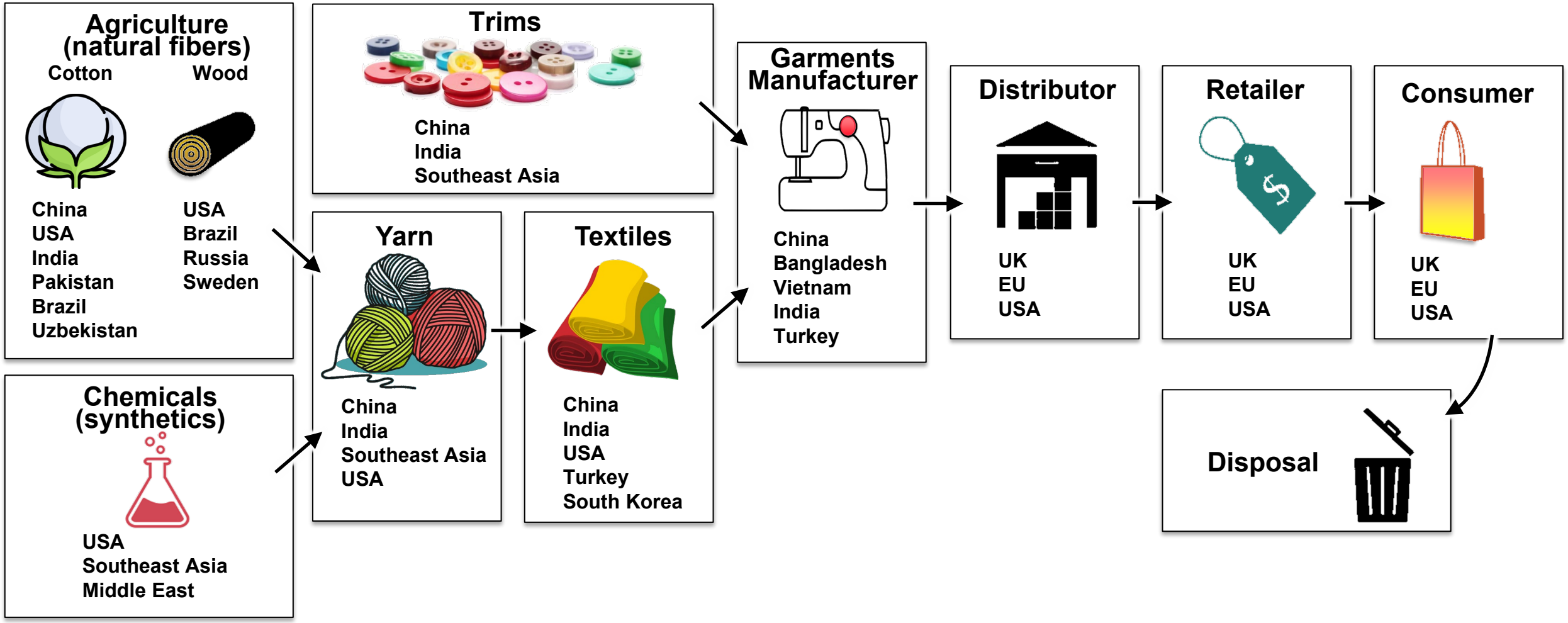
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chain Example – Consumer Clothing

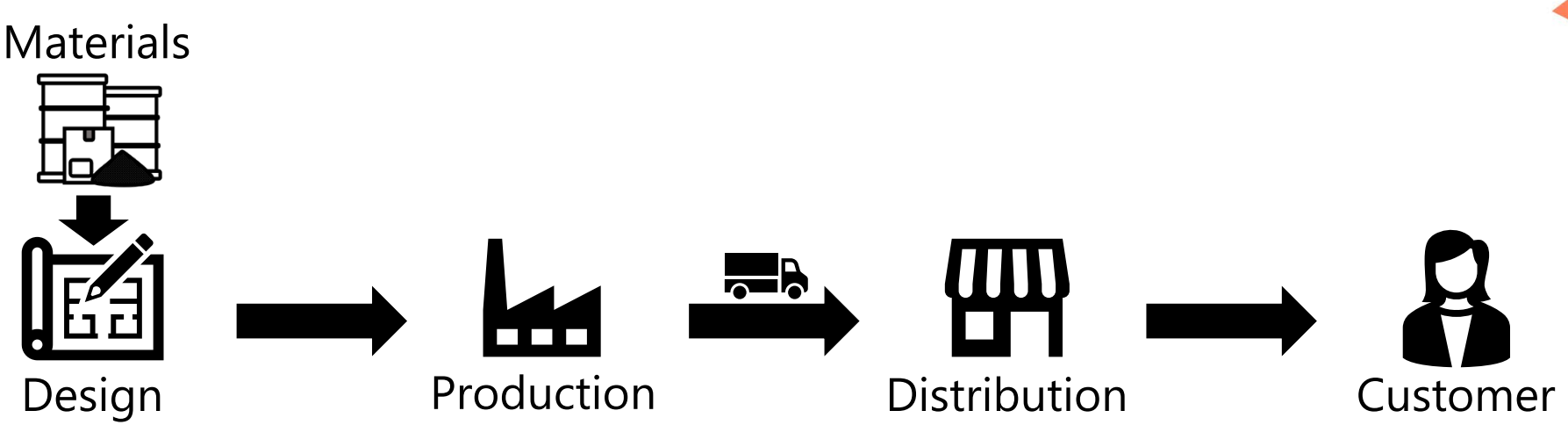


https://imgs.mongabay.com/wp-content/uploads/sites/20/2020/04/23100736/FF_Supplychain.png

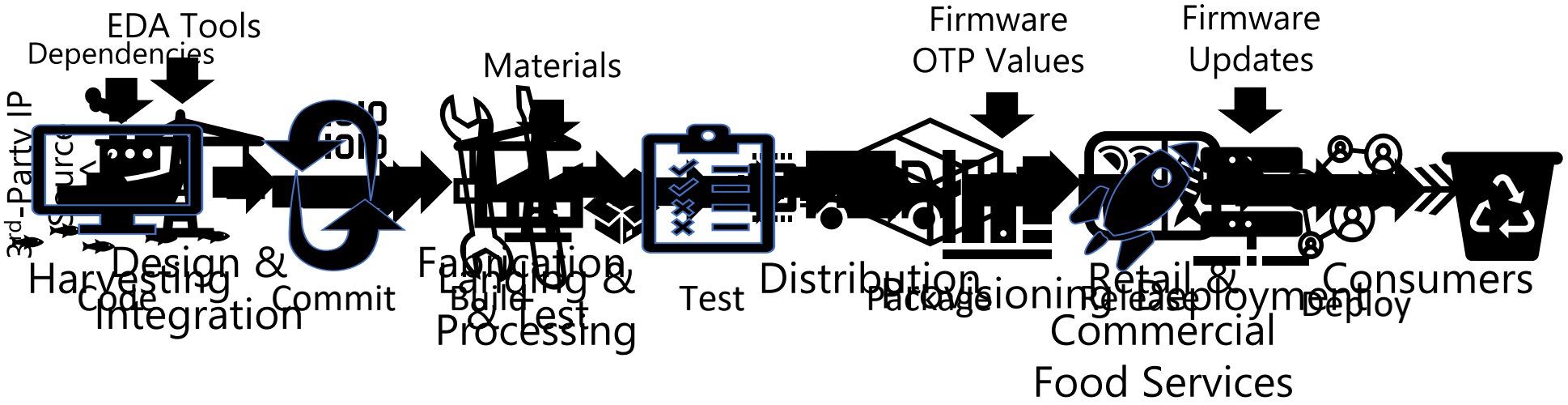
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chains

Generic Supply Chain

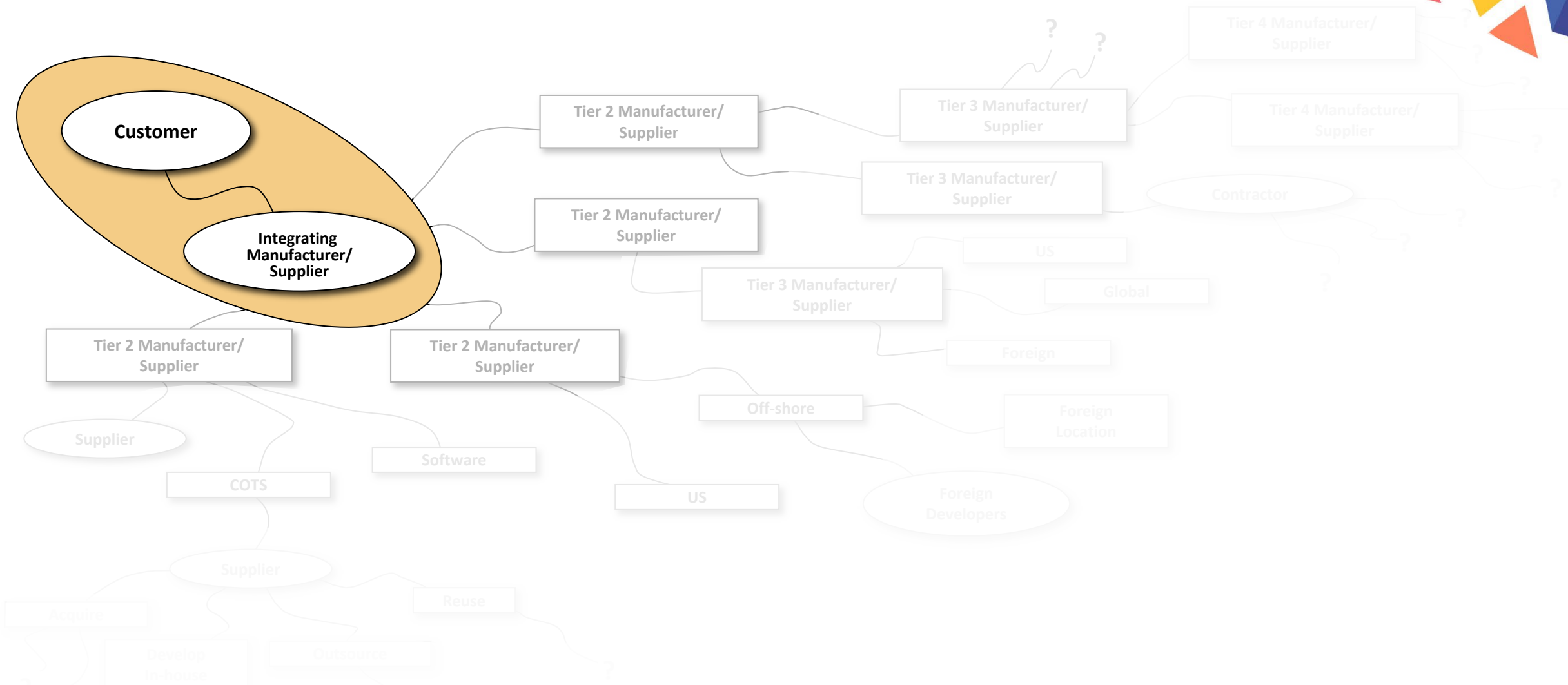


Micro-Electronics Supply Chain

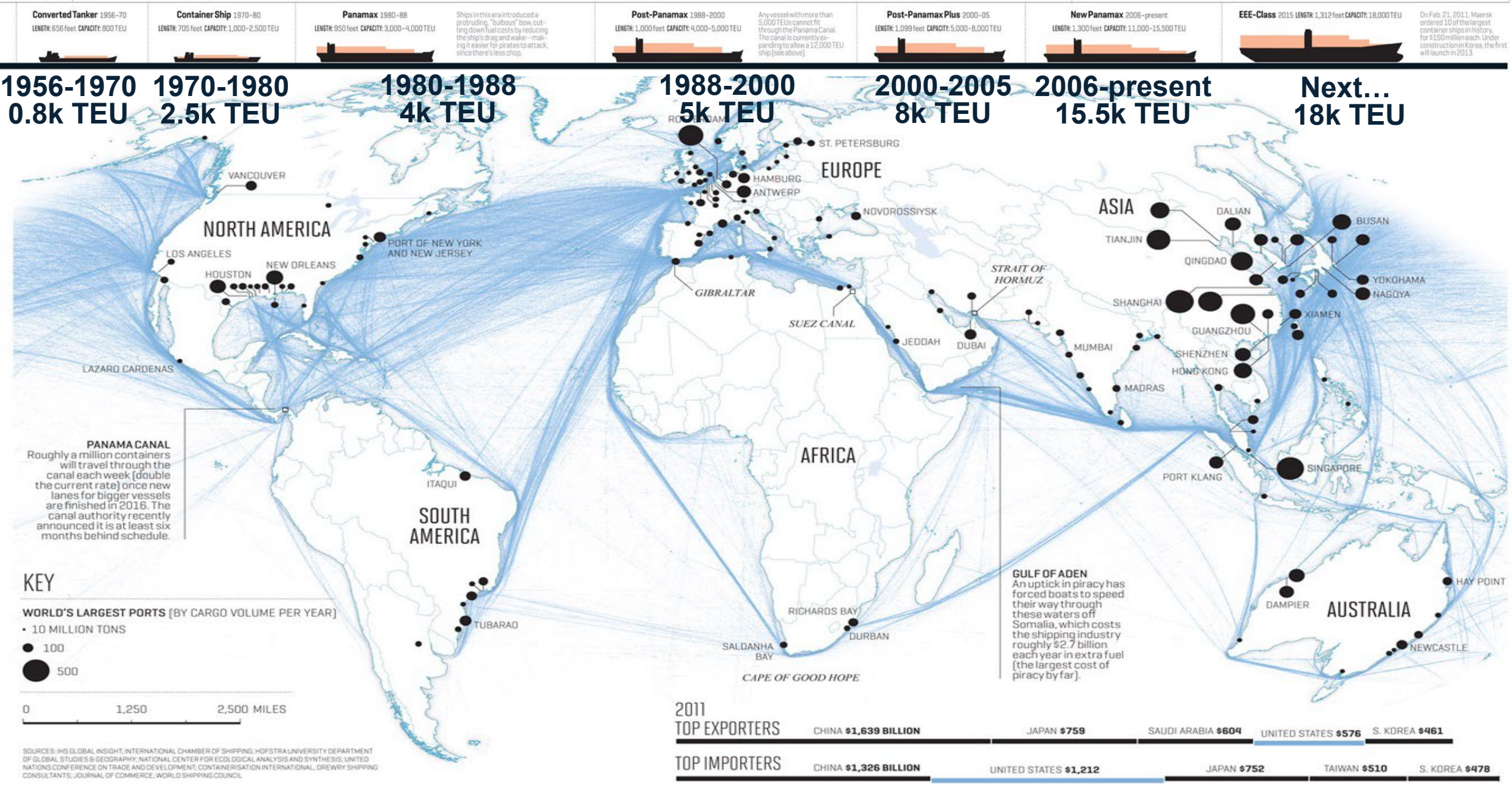


© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chains are Complex and Opaque



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Software is Ubiquitous, Assembled, and Critical

IT Risk → **Operational Risk**

Loss of data or capability | **Loss of safety or reliability** | **Loss of property or lives**

Scratch Built Software → Assembled Software

Majority of products built with no 3rd Party dependencies

Use of open source and 3rd party libraries, modules, frameworks, and services
Multi-party software updating/patching

Traditional Computers → Software Enabled Everything

Servers	databases
Desktops	office apps
Laptops	e-mail
Tablets	browsers
Switches	Routers

Healthcare	Implantable Medical	Smart Munitions
Aeronautics	Smart Manufacturing	Intelligent Vehicles
Smart Energy	Water Treatment	Intelligent Shipping
Oil & Gas	Hydro Power	Dam Management
Microgrids	Smart Cities	Building Management
		Autonomous Systems

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Software Enabled Critical Infrastructure and Mission Capabilities…

Medical

Buildings

Aeronautics

Manufacturing

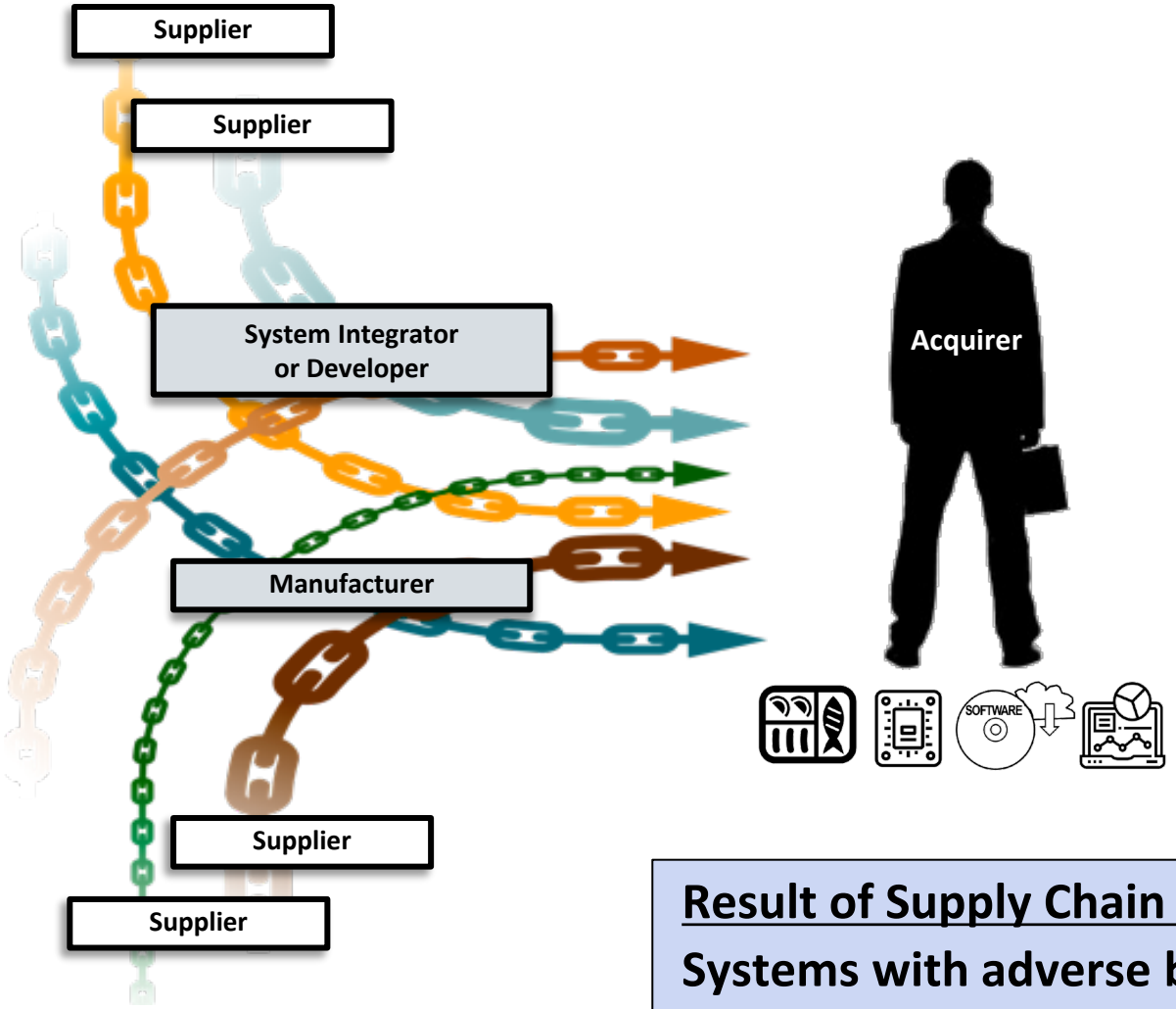
Vehicles

Energy

Shipping

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Whether for Fish, Chips, or Software
Supply Chain Trustworthiness: Intentional and Unintentional Acts



Based on SEI/CMU materials

Intentional acts

- Counterfeit products
- Disruption, hijacking, theft, civil unrest,…
- Malicious taint or insertion

Unintentional acts

- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/weaknesses and/or known vulnerabilities)

Result of Supply Chain Attacks:

Systems with adverse behaviors including functional degradation, data exfiltration, espionage, adversarial control and disruption.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chain Security Risk Management: Elements of Practice

Traditional SCRM (Logistics)

- Supplier Economic Viability
- Fitness for Purpose (form, fit, function)
- Source of Materials (non electronic)
- Inventory Management/Just-in-time
- Vendor/supplier payment
- Third-party service providers
- Anti-Tamper
- Shipping/Receiving

Organizational Operations and Risk Management

- Training/Professional Education/Awareness
- Legal Authorities and Policy (General Counsel)
- Human Resources
- Physical Security
- Logistics

Cyber-Supply Chain Risk Management (C-SCRM)

- Risk evaluation of tier 1 – tier n supplier
- Flow-down of requirements to sub-tiers
- Source of materials (ICT/IoT) analysis
- Alternative sources (contingency planning)
- Transit/warehouse/loading dock security
- Bill of materials – analysis and tracking
- Blind buy strategies
- S/W and H/W risk analysis
- SCADA, IoT, IIoT lifecycle management
- Disposal/retirement planning and execution
- Sustainment strategy/delegation to service provider
- Cloud (SAAS, PAAS, IAAS) services
- Anti-Tamper

Traditional Cyber Security/Risk Management

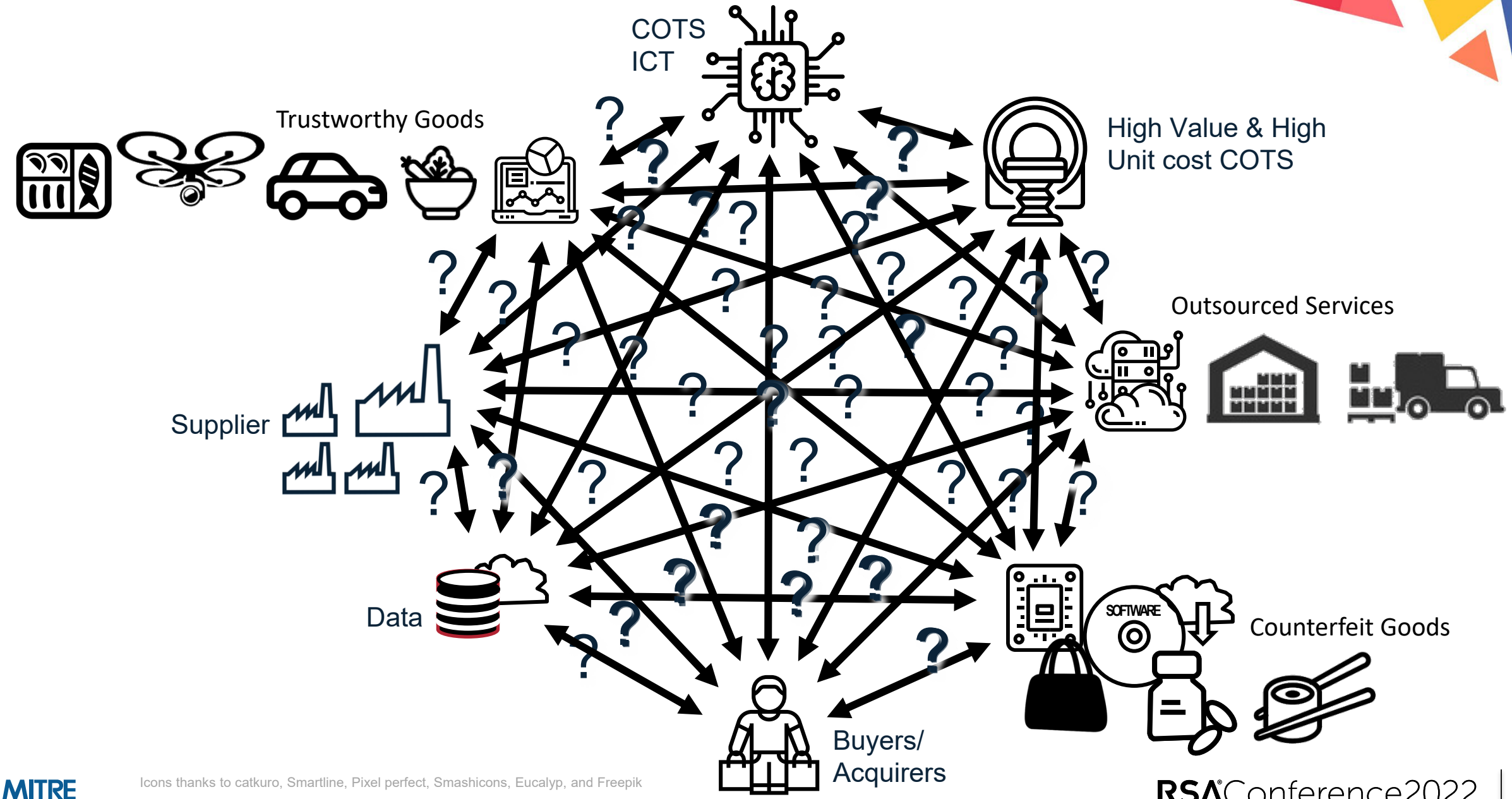
- Security architecture
- Privacy
- Data security
- Phishing & Social Engineering
- Criticality and dependency analysis
- Network/workstation security
- Insider threats/Employee misconduct
- Product hygiene/Application of patches

Acquisition/Procurement

- Statutory compliance
- Submission of documents
- Program Protection Planning
- Budget/resource consideration

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

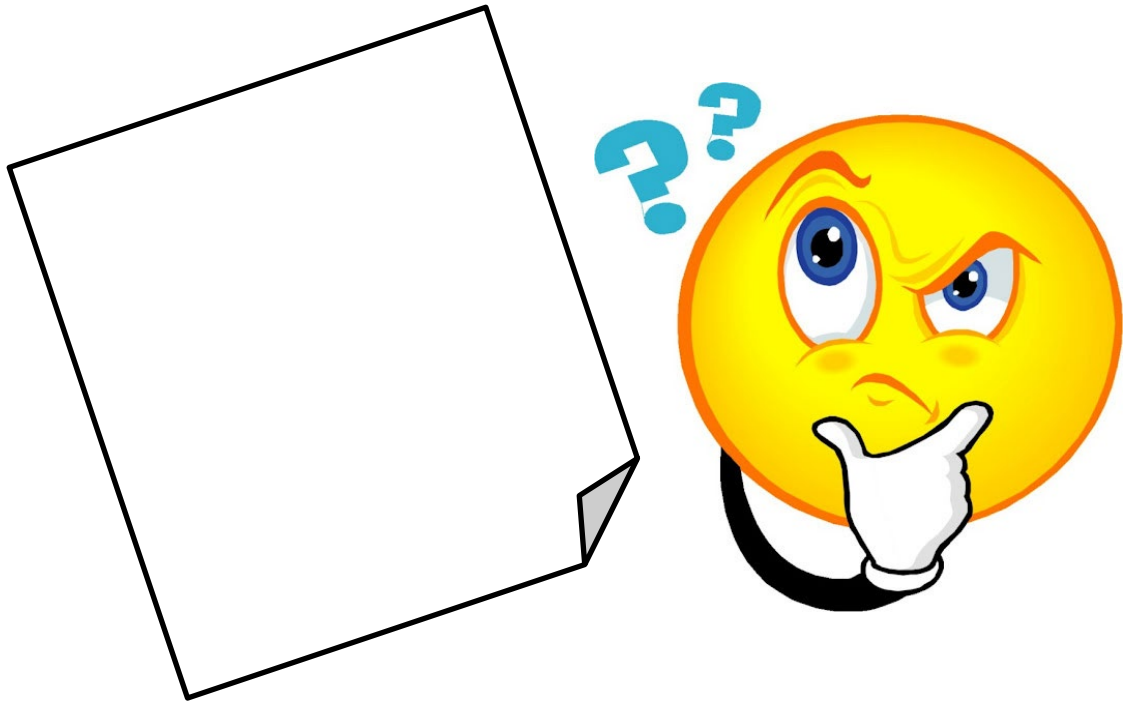
Open Question: What Supply Chain Risks to Manage?

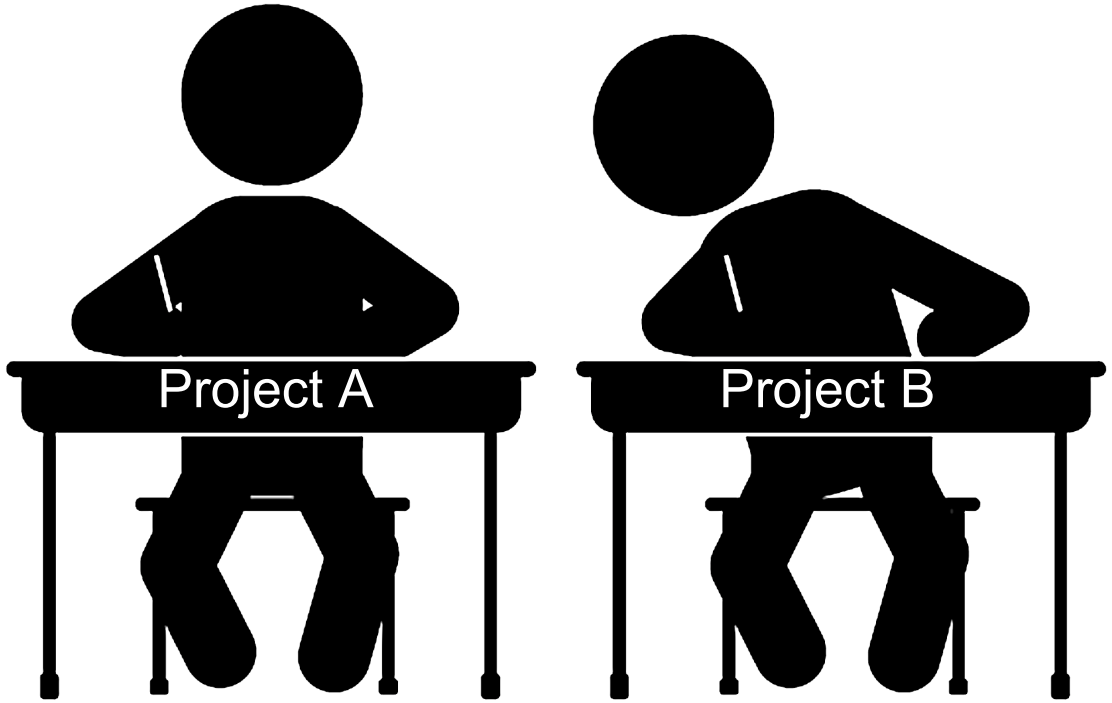


Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Open Question: What Supply Chain Risks to Manage?





© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chain Risk Areas

Natural Disasters and Hazards

Icons thanks to freepik

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

Quality Culture of the Supplier

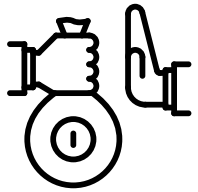
External Influences of the Supplier

Financial Stability of the Supplier
Organizational Stature of the Supplier
Susceptibility of the Supplier

Maliciousness of the Supplier
Organizational Security

Human Hazards

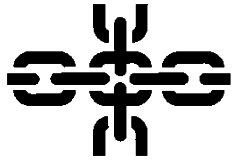
Hijacking



Corporate Corruption

Traffic Congestion

Civil Disruption



Interdependent Supply Chains

National Corruption

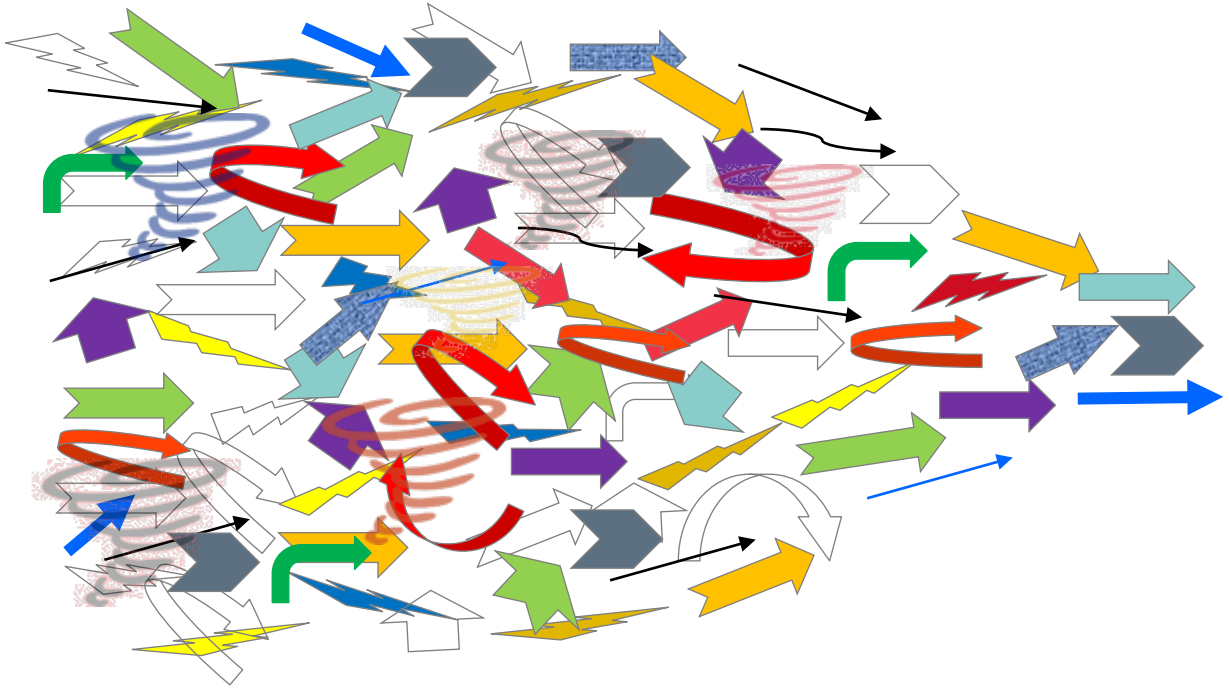
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

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

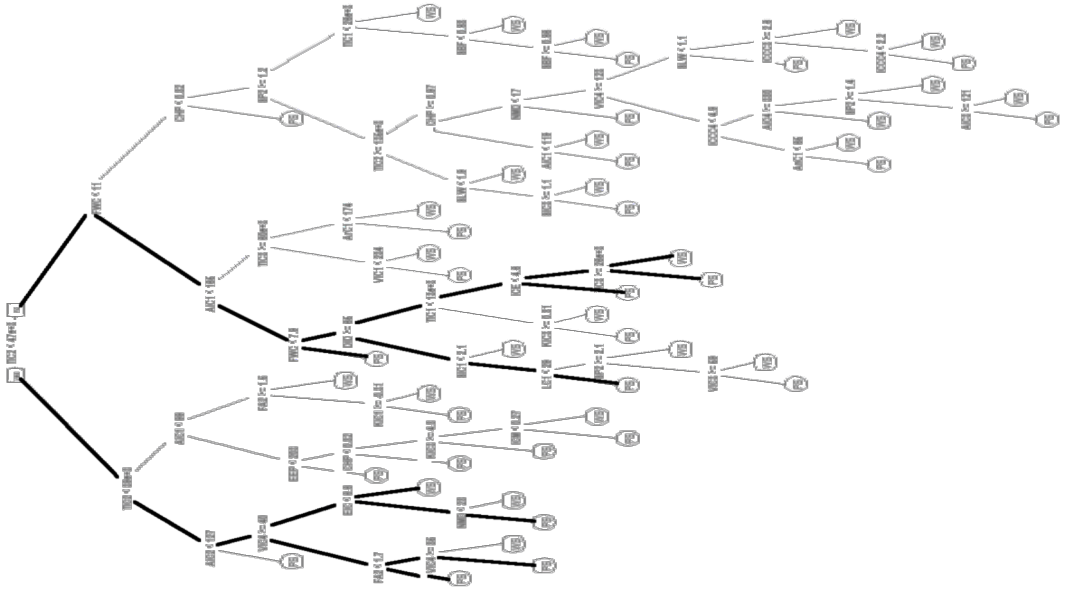
"What Supply Chain Risks to Manage?"

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

MITRE | System of Trust™



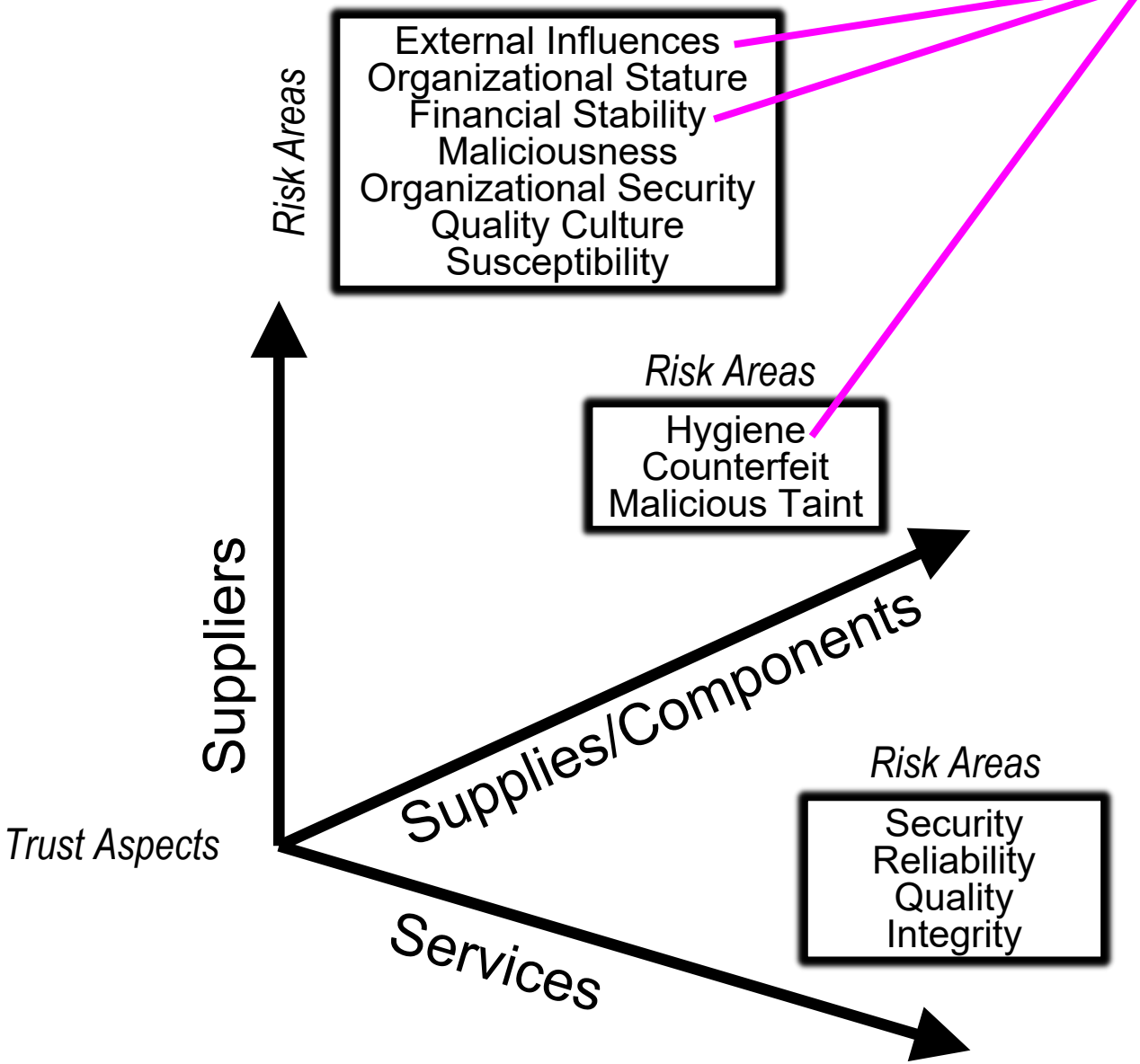
Address Chaos, Align & Organize



Simplify, Tailor & Use

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Basis of Trust

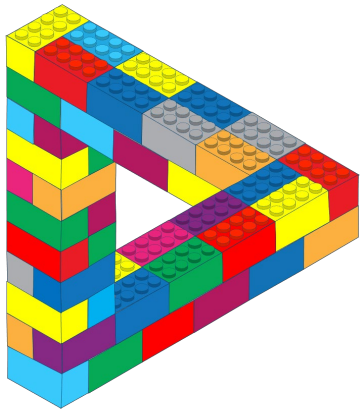


- **Product Quality**
  - ICT Hardware Product Quality
  - Product Quality Requirements
  - Software Product Quality
    - Software Anomaly Control
    - Software Consistency
    - Software Design Simplicity
    - Software Provenance & Pedigree
    - …
- **Product Resilience**
  - ICT Hardware Product Resilience
  - Software Product Resilience
- **Product Security**
  - ICT Hardware Product Security
  - Inadequate protection for controlled unclassified information
  - Information on product manufacturer information systems not backed up regularly
  - Misconfigured access controls on product manufacturer information systems
  - Sensitive information in digital form not encrypted while in physical transit either to or from product manufacturer
  - Users of product manufacturer information systems do not receive cybersecurity training
  - Weak identification and authentication controls on product manufacturer information systems
  - …

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

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

Supply Chain Risks													
Supplier Risks							Supply Risks			Services Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service Delivered	Reliability of Service Delivered	Security of Service Delivered
Company foreign relationships with countries of concern	Questionable debt management	Corporate ownership reputation	Customers	Company has a low CMMI rating	Foreign Intelligence Service (FIS) influence	Concerns regarding facility access	Product quality	Facilities integrity	Copycat manufacturing	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree
Company operational locations in countries of concern	Questionable financial stewardship	Diversity and inclusion	Industry sector	Internal company QC, SCRM policy & practice	Fraud and corruption	Concerns regarding software access	Product resilience	Functional integrity	Mislabeling	Service Infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance
Foreign registration/incorporation	Questionable future outlook	Geographic concentration	Location	Subcontractor supply chain health / risk	Legal/law issues	Concerns regarding hardware access	Product security	Geopolitical integrity	Packaging integrity	Service specific integrity	Service specific quality	Service specific reliability	Service specific security
Geopolitical instability	Questionable profitability	Mergers & acquisitions frequency	Personnel		Sanction list status	Cyber threat activity		Logistics / transportation integrity	Technical authenticity				Susceptibility to manipulation of service infrastructure via physical access/touch
Key Management Personnel (KMP) and non-person entity relationships of concern	Vulnerability of financial stability to foreign influence	Natural disasters	Technical susceptibility			Data security status		Maintenance integrity	Unsanctioned manufacturing				Susceptibility to manipulation of service infrastructure via remote/virtual access/touch
National corruption	Vulnerability of financial stability to market factors	Operational volatility				Type/ level /frequency of security training		Manufacturing process integrity					
National governance	Vulnerability to takeover	Sustainability				Vulnerabilities		Packaging integrity					
Organization ownership and control								Reputational integrity					
Politically Exposed Persons (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													

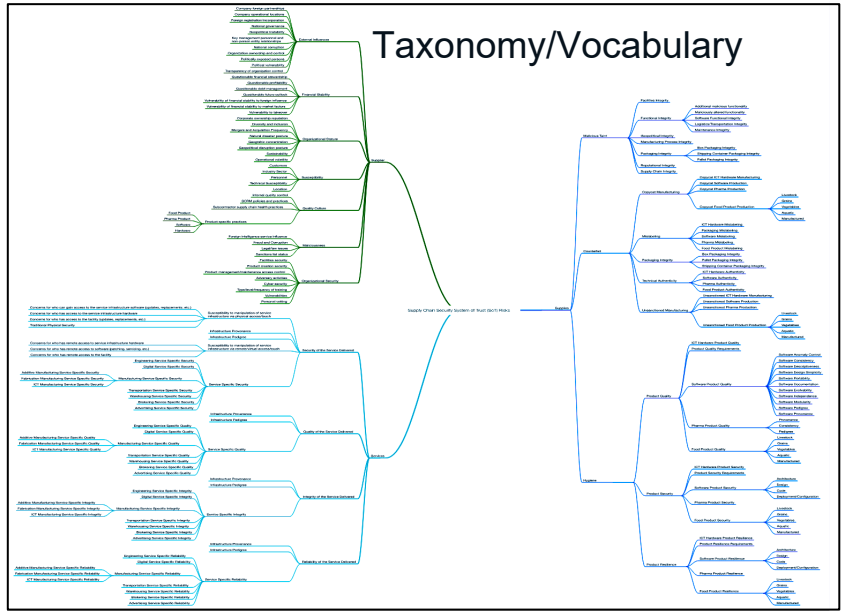


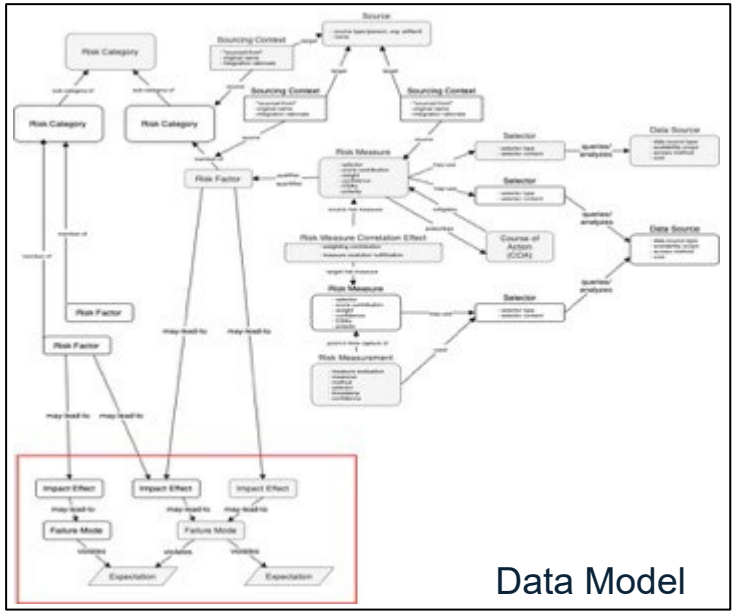
MITRE | System of Trust™

MITRE's Supply Chain Security System of Trust™
https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach

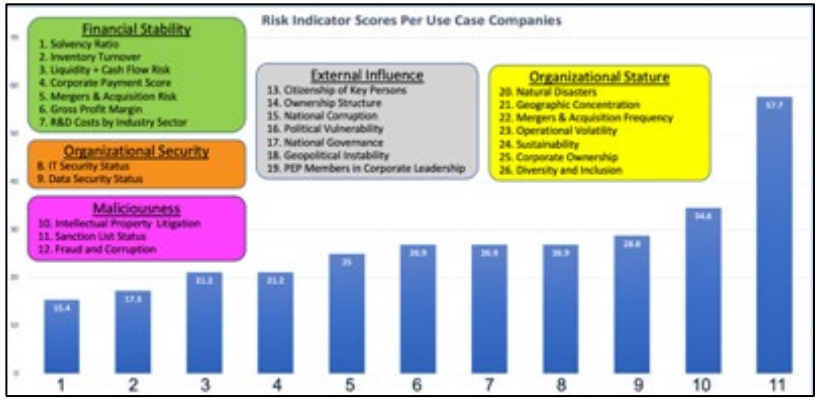
* Supply Chain Security Top 75 Risk Areas Levels 1-4
** System of Trust Expanding to Pharma, Food, and other types of Products

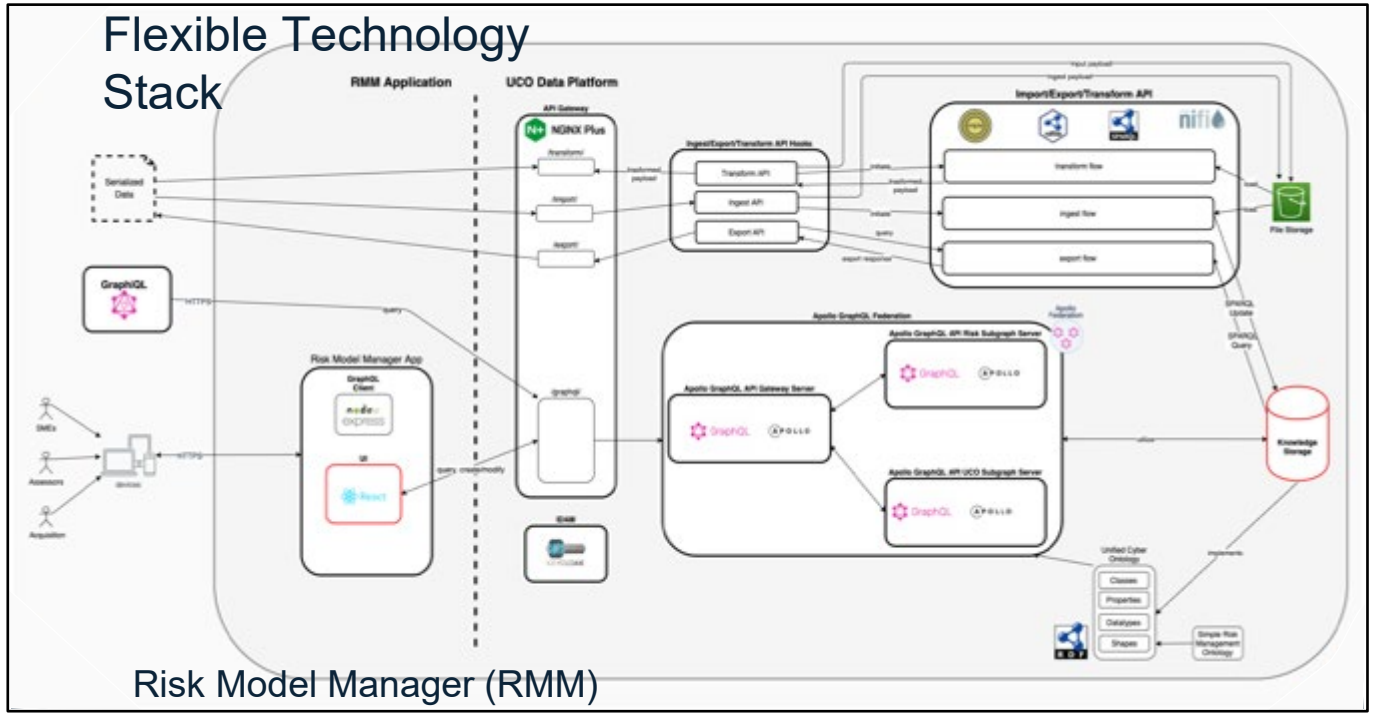
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88





Analytic Methods

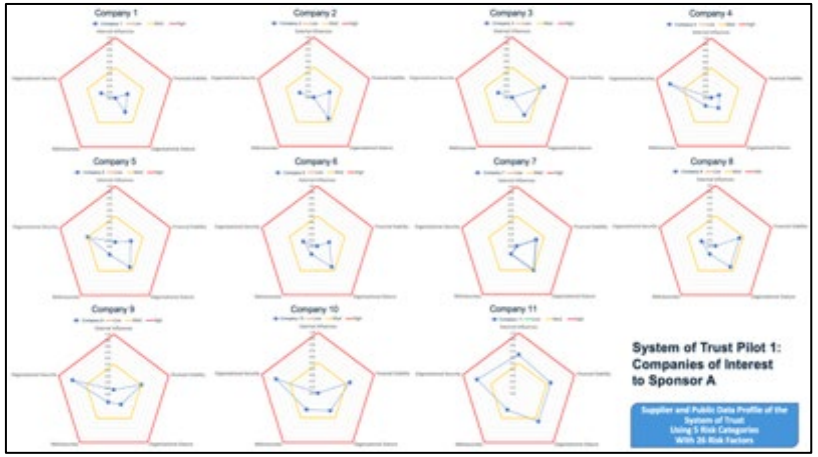




Piloting

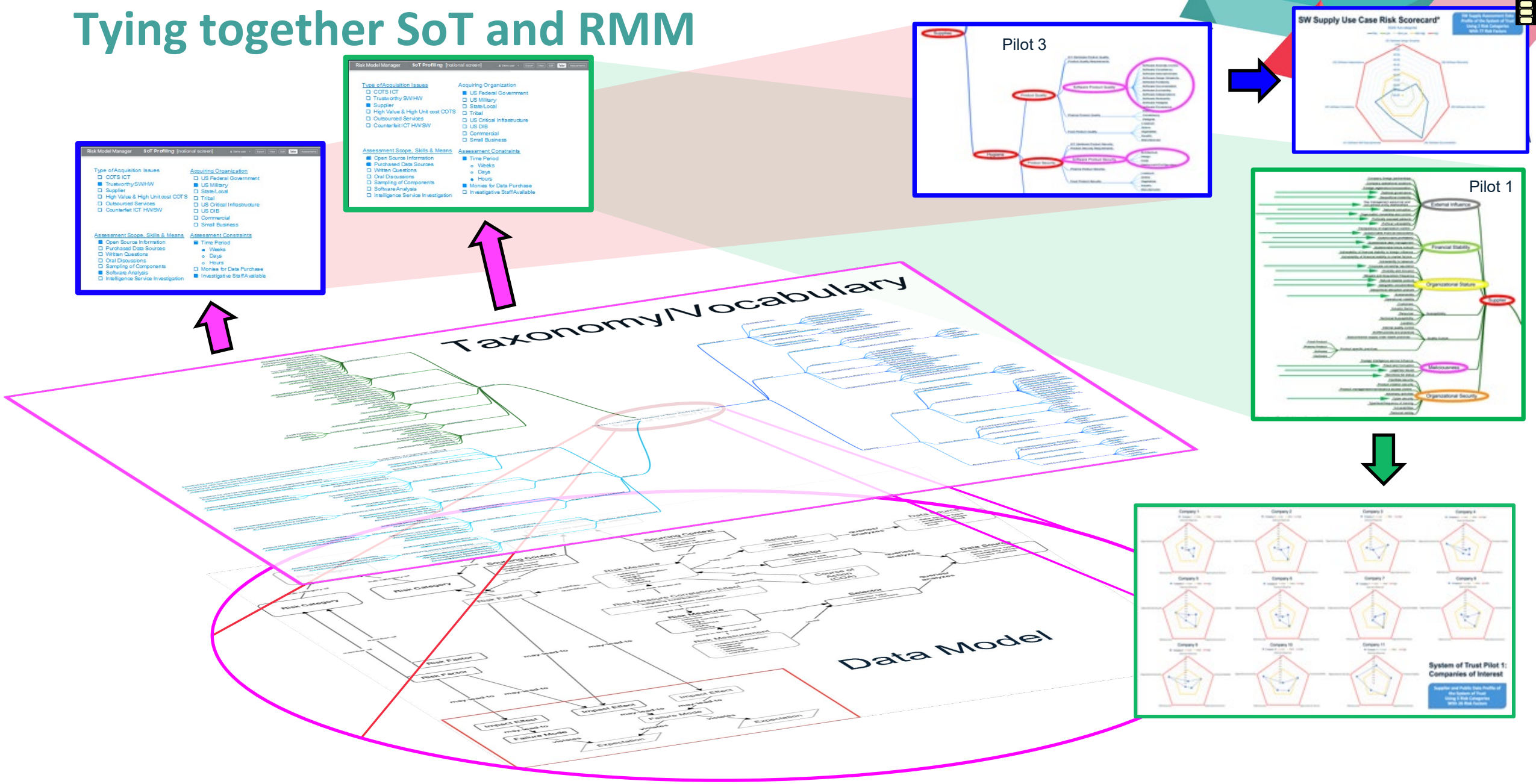
11, 3, 1, 6, 22, 12, …

Export to Spreadsheet for "Offline" Assessment

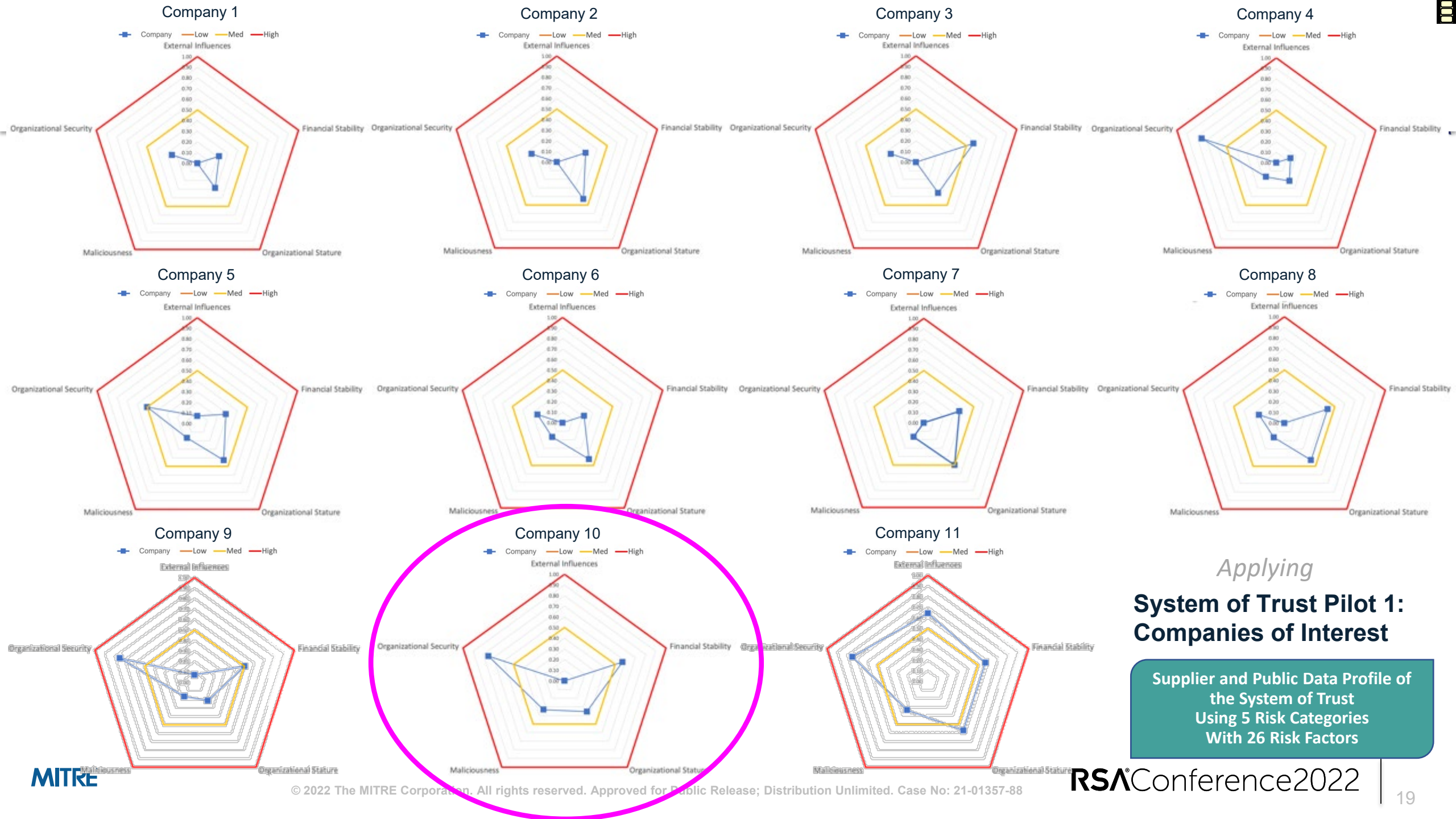


© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Tying together SoT and RMM



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88



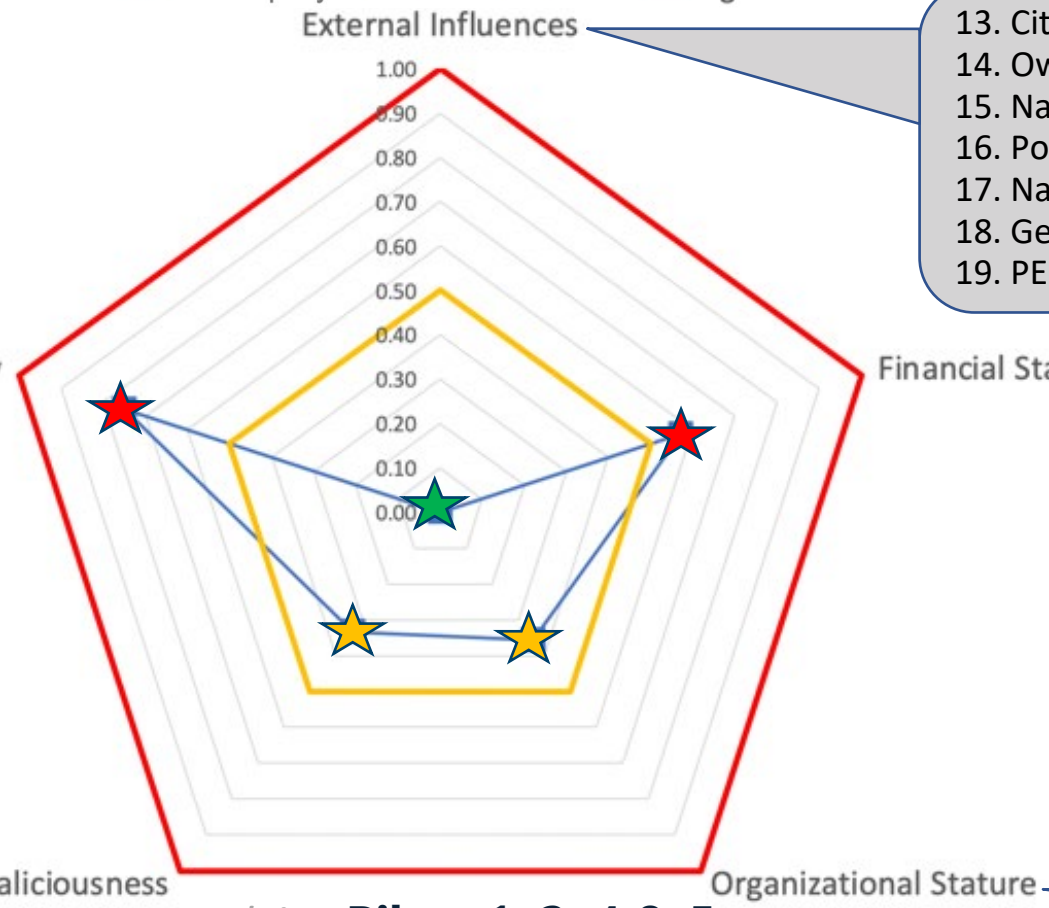
Applying

System of Trust Pilot 1: Companies of Interest

Supplier and Public Data Profile of the System of Trust Using 5 Risk Categories With 26 Risk Factors

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Company 10



13. Citizenship of Key Persons
14. Ownership Structure
15. National Corruption
16. Political Vulnerability
17. National Governance
18. Geopolitical Instability
19. PEP Members in Corporate Leadership

1. Solvency Ratio
2. Inventory Turnover
3. Liquidity + Cash Flow Risk
4. Corporate Payment Score
5. Mergers & Acquisition Risk
6. Gross Profit Margin
7. R&D Costs by Industry Sector

8. IT Security Status
9. Data Security Status

Applying **Pilots 1, 2, 4 & 5**

10. Intellectual Property Litigation
11. Sanction List Status
12. Fraud and Corruption

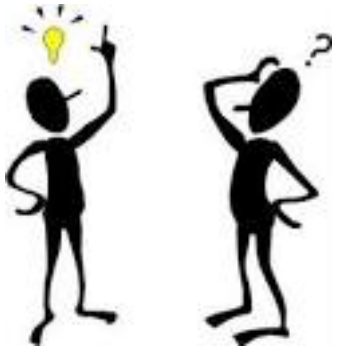
Supplier and Public Data Profile of the System of Trust Using 5 Risk Categories With 26 Risk Factors

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

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

SoT's Risk Model Manager "Modes" – An Analogy

We should do a survey – we need a questionnaire!



Okay, but what questions should we ask?

here are all the questions you could potentially ask about supply chain security risks

View

nice but I see something I want to change for the purposes of my survey

Edit (optional)

now I just need a subset of these questions to create my questionnaire

Tailor

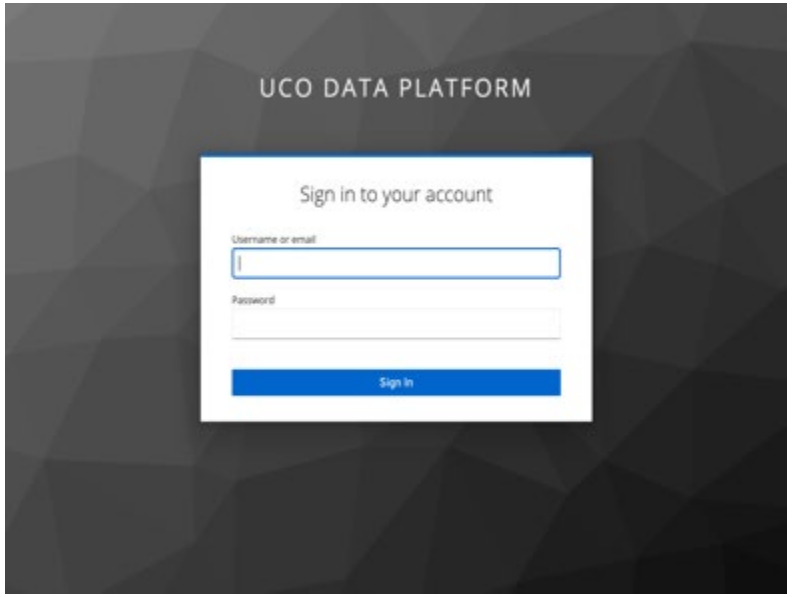
profiles

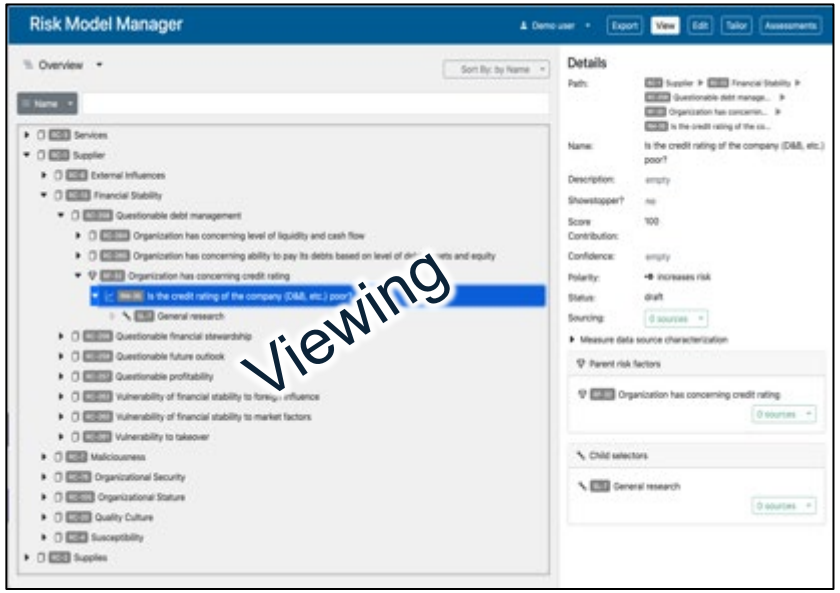
now I just need to fill one of these out for every person I interview!

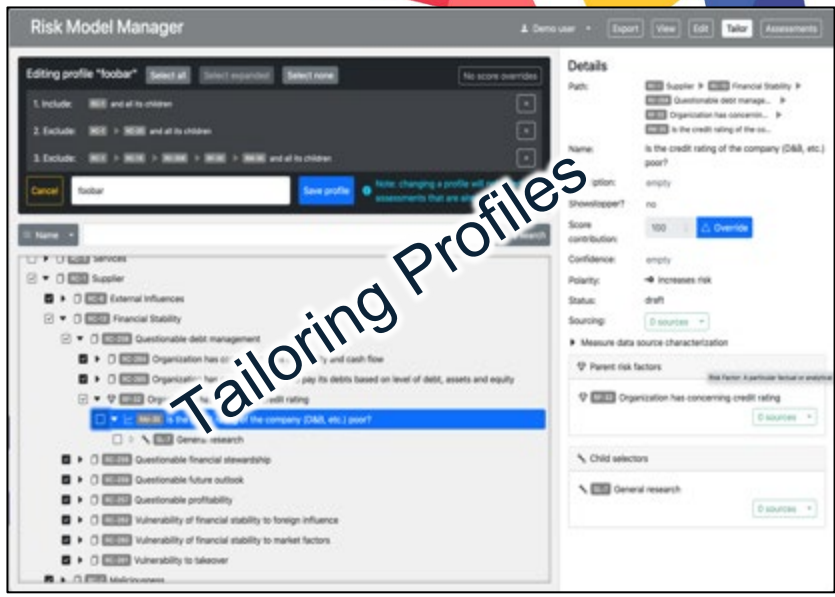
Assessments

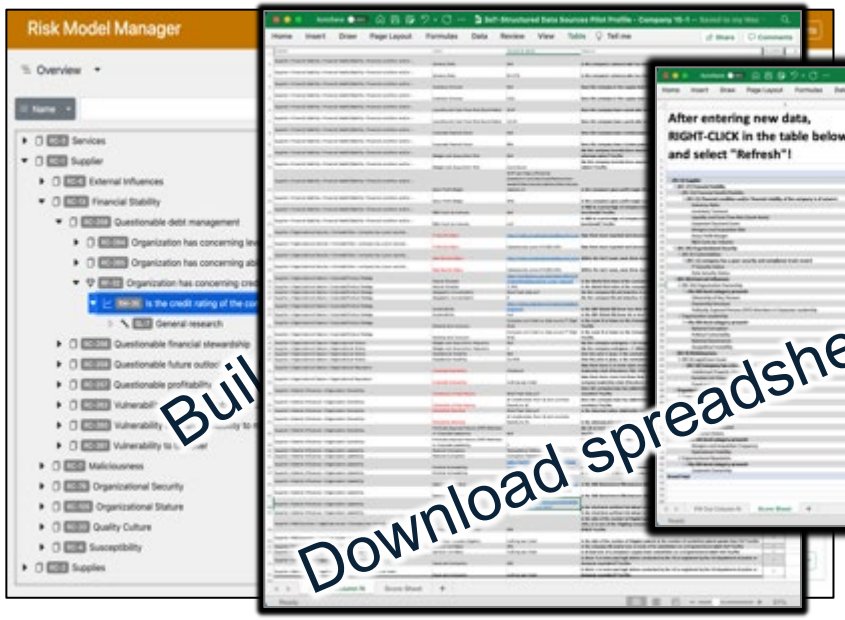
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

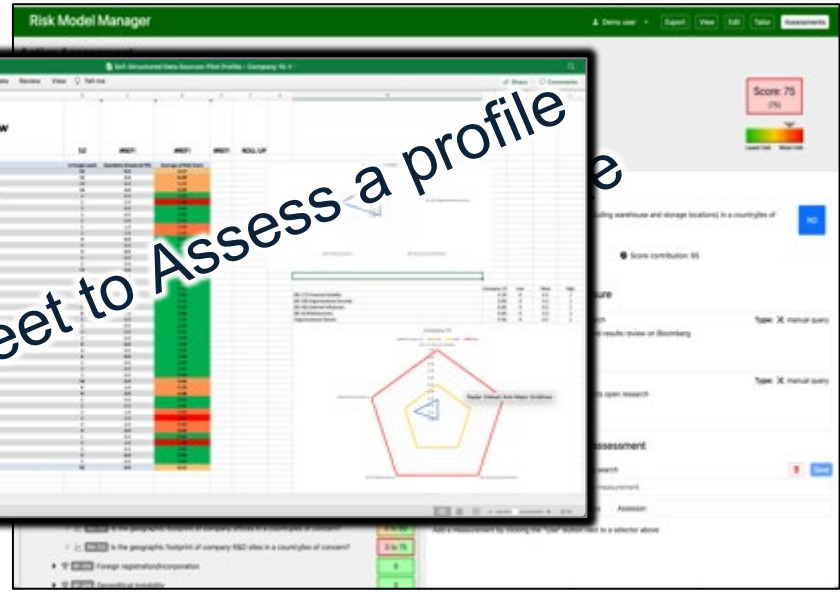
SoT.MITRE.org Set of Tools – Risk Model Manager







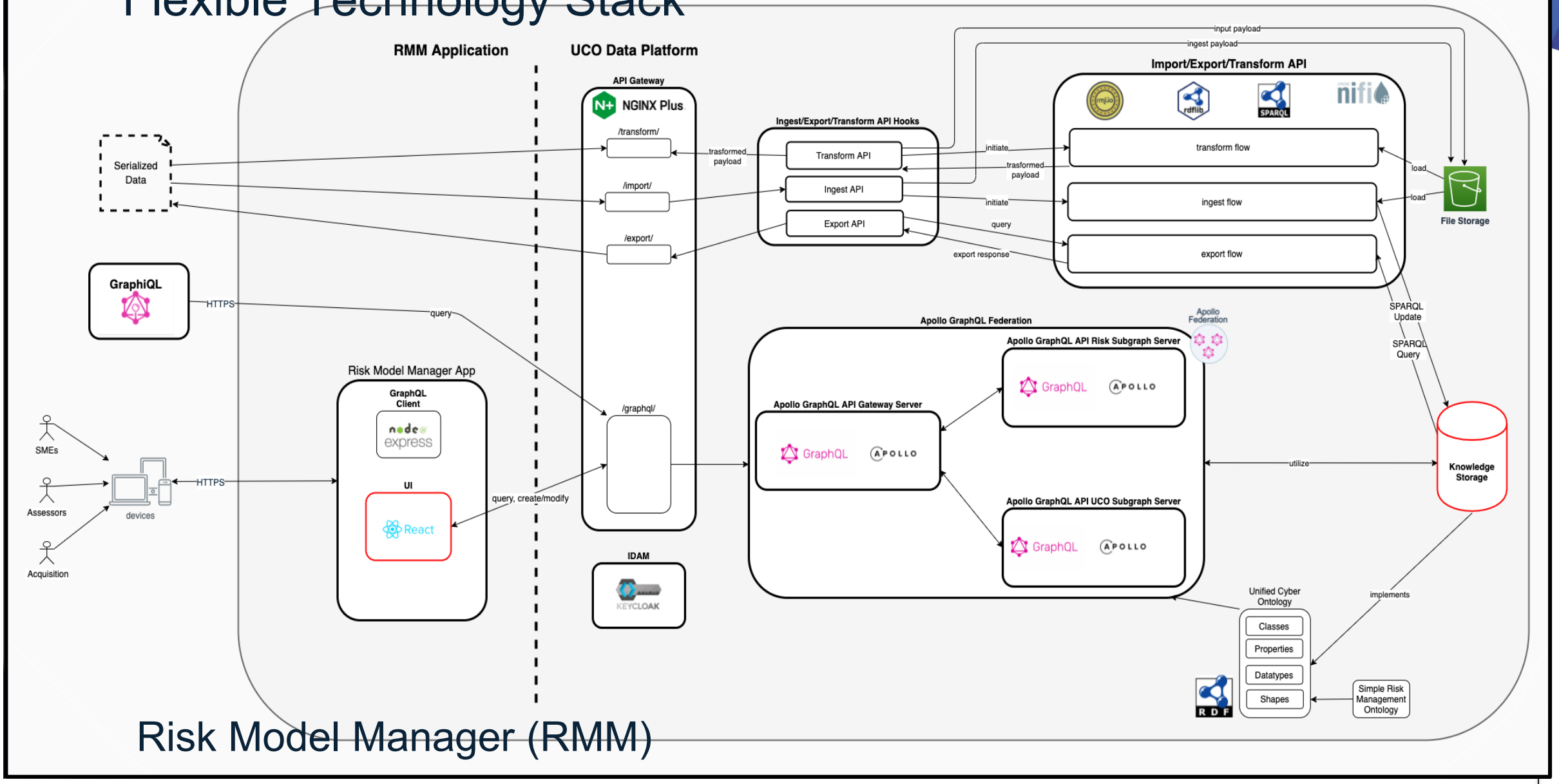




© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

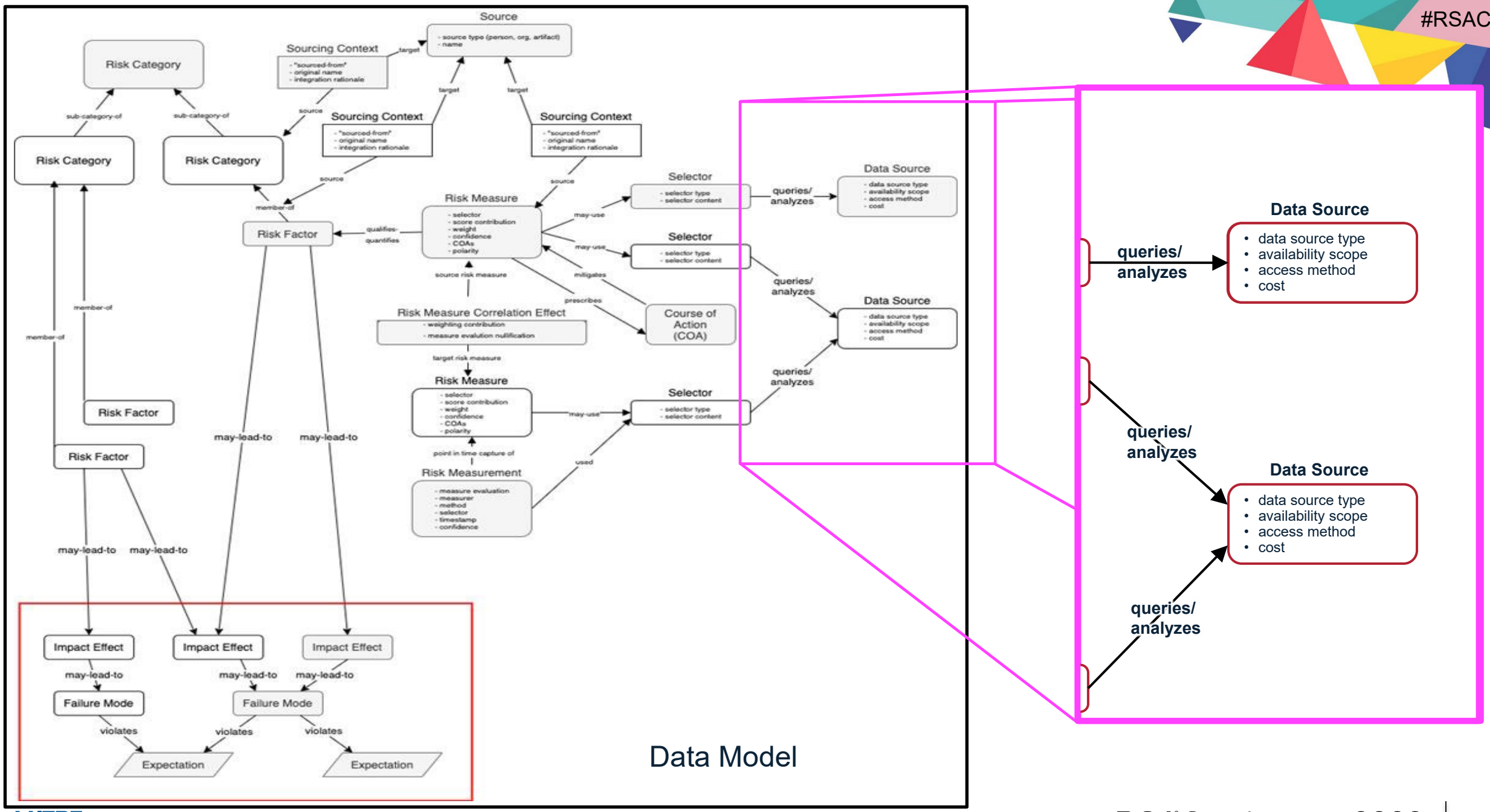
SoT Risk Model Manager Platform Technical Architecture

Flexible Technology Stack



Risk Model Manager (RMM)

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88



Data Model

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Building up Sources of Insight about Supply Chain Risks

Risk Model Manager

ramartin | Export | View | Edit | Tailor | Assessments

Data Sources | Sort By: by Name

Name

DS-14 Bloomberg Datasets

DS-17 Bureau of Industry and Security (Department of Commerce)

ciation International (ERAI)

a Exchange Program

Details

Name: SAM.gov

Description: empty

Status: draft

Type: Website

Location: https://sam.gov/content/home

Availability Scope: Public

Access Method: Manual; API

Risk Model Manager

ramartin | Export | View | Edit | Tailor | Assessments

Selectors | Sort By: by Name

Name

SL-7 General research

SL-15 Manual BIS (Department of Commerce) search

SL-11 Manual Bloomberg search

SL-13 Manual Edgar search

SL-23 Manual ERAI search

SL-22 Manual GIDEP search

SL-25 Manual IAPP (Department of State) search

SL-8 Manual LexisNexis search

SL-16 Manual OFAC (Department of Treasury) search

SL-5 Manual Orbis - Current Directors and Managers search

SL-9 Manual Orbis search

SL-26 Manual Privacy Rights Clearinghouse Data Breach List search

SL-14 Manual SAM.gov search

SL-10 Manual Thomson Reuters Refinitiv Company Datasets search

SL-24 Manual Wikipedia data breach list search

SL-20 Manual World Risk Report search

Details

Name:

Descripti

Execution Vector:

Data Sou

Selector

Status:

Pare

RM-

RM-

Risk Model Manager

ramartin | Export | View | Edit | Tailor | Assessments

Active Assessment

Name: Demo Assessment1

Profile: "SoT Pilot - Supplier Quick Check" (as of 2022-02-28T19:24:05.018Z)

Last updated: 2022-03-04T21:44:09.692Z

Description: empty

Tags: empty

Contributors: jdoe

Objective: empty

Scope: empty

Target: empty

Edit Assessment Metadata

Progress

84 risk measures in this profile:

unanswered: 81

yes: 2

no: 1

151 other entries in this profile.

Score: 70 to 100 (70 to 100)

Least risk — Most risk

Sort By: by Name

Name

Assessment Item	Score
RM-452 Does this company have key stakeholder nationality of >= 15% from country/ies of concern?	0 to 75
RF-371 Organization acquisition by or merger with stakeholders from a foreign nation	0 to 85
RM-428 Has the company recently been acquired, restructured, merged, or acquired by stakeholders from a non-adversary nation?	0 to 60
RM-427 Has the company recently been acquired, restructured, merged, or acquired by stakeholders from an adversary nation?	0 to 85
Has the company recently taken steps to be acquired,	

Path: RC-1 ▶ RC-6 ▶ RC-5 ▶ RC-107 ▶ RF-371 ▶ RM-428

Has the company recently been acquired, restructured, merged, or acquired by stakeholders from a non-adversary nation?

Increases Risk — Score contribution: 60

▶ Measure data source characterization

Potential Selectors for this Risk Measure

Use — **Name:** Manual Bloomberg search — **Type:** manual query
Description: Manual search entry and results review on Bloomberg
Data Source: Bloomberg Datasets
Execution Vector:

Use — **Name:** General research — **Type:** manual query
Description: Human assessor conducts open research
Data Source: Undefined
Execution Vector:

Measurements made as part of this assessment

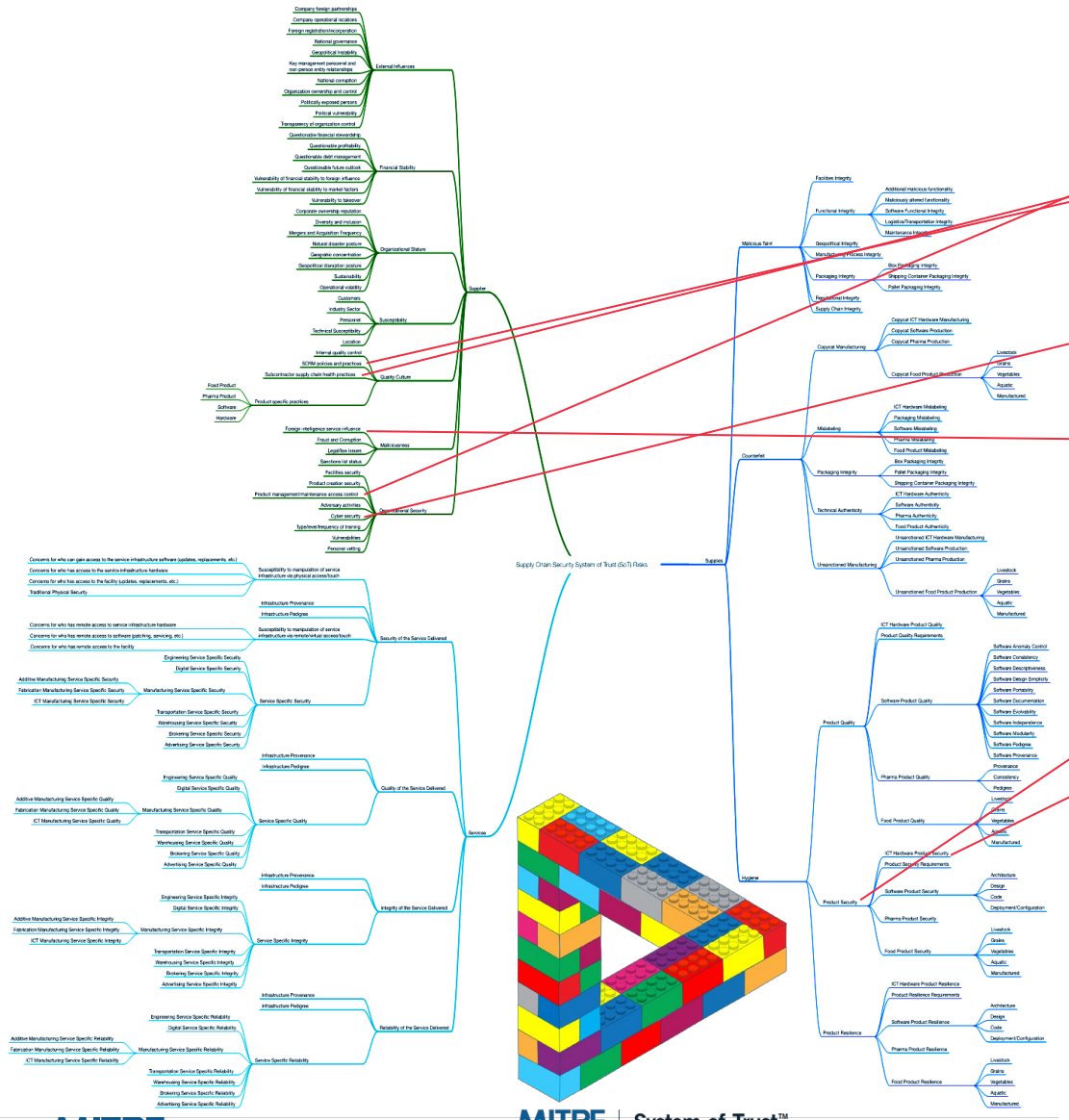
Add a measurement by clicking the "Use" button next to a selector above

MITRE

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

RSAConference2022

Mapping SoT Risks to Assessment Information Sources / Standards



Along with DHS ICT SCRM Task Force Vendor Template, ISO/IEC 62443, and others, …

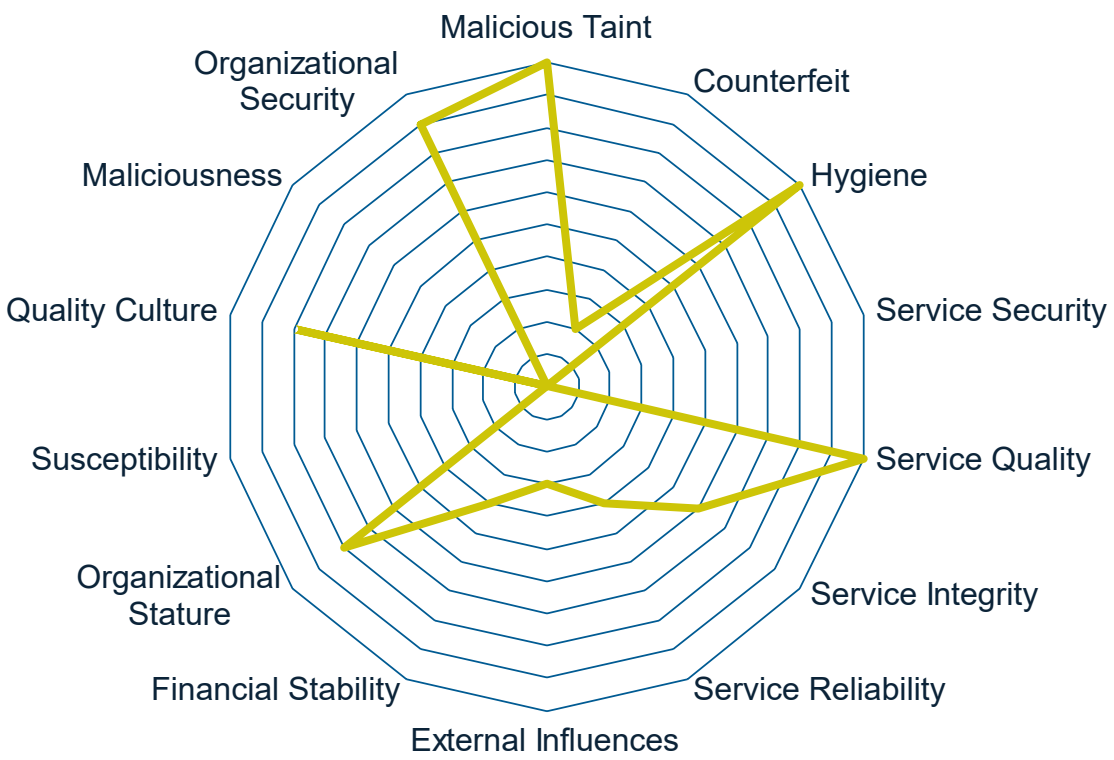
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

GOAL for use of SoT in Industry and Government…

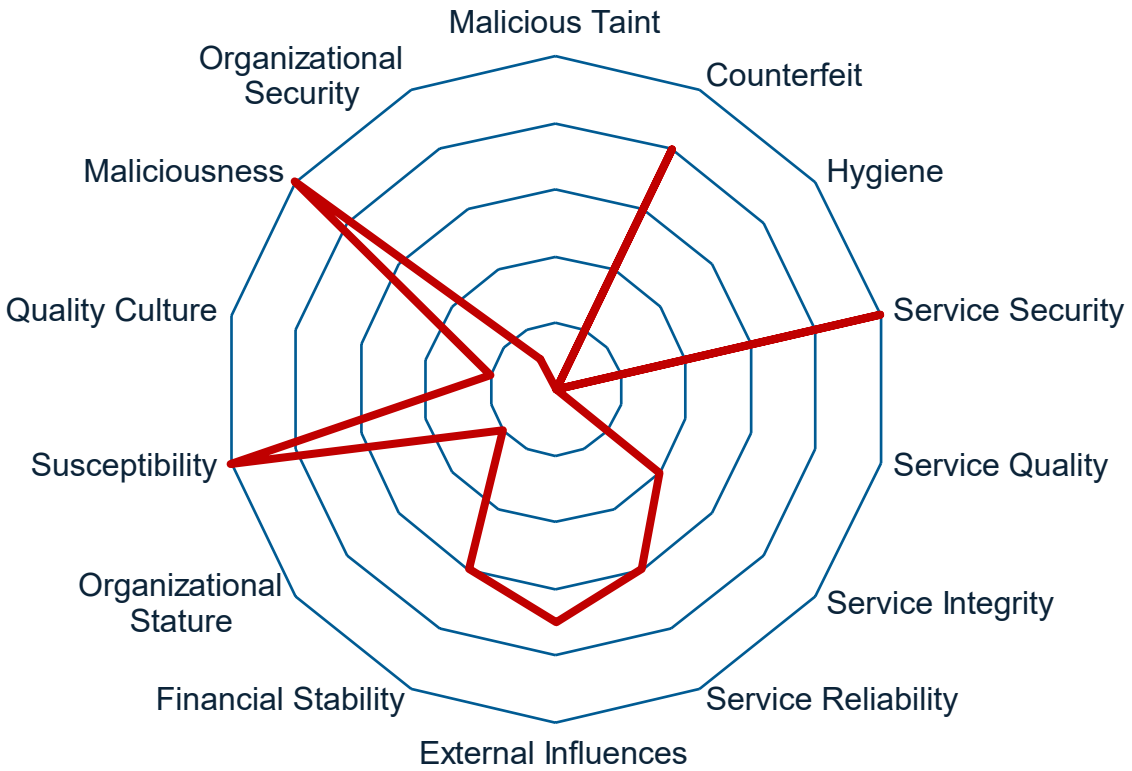
Risk Model Manager

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

Top-Level Concerns Vendor/Product A

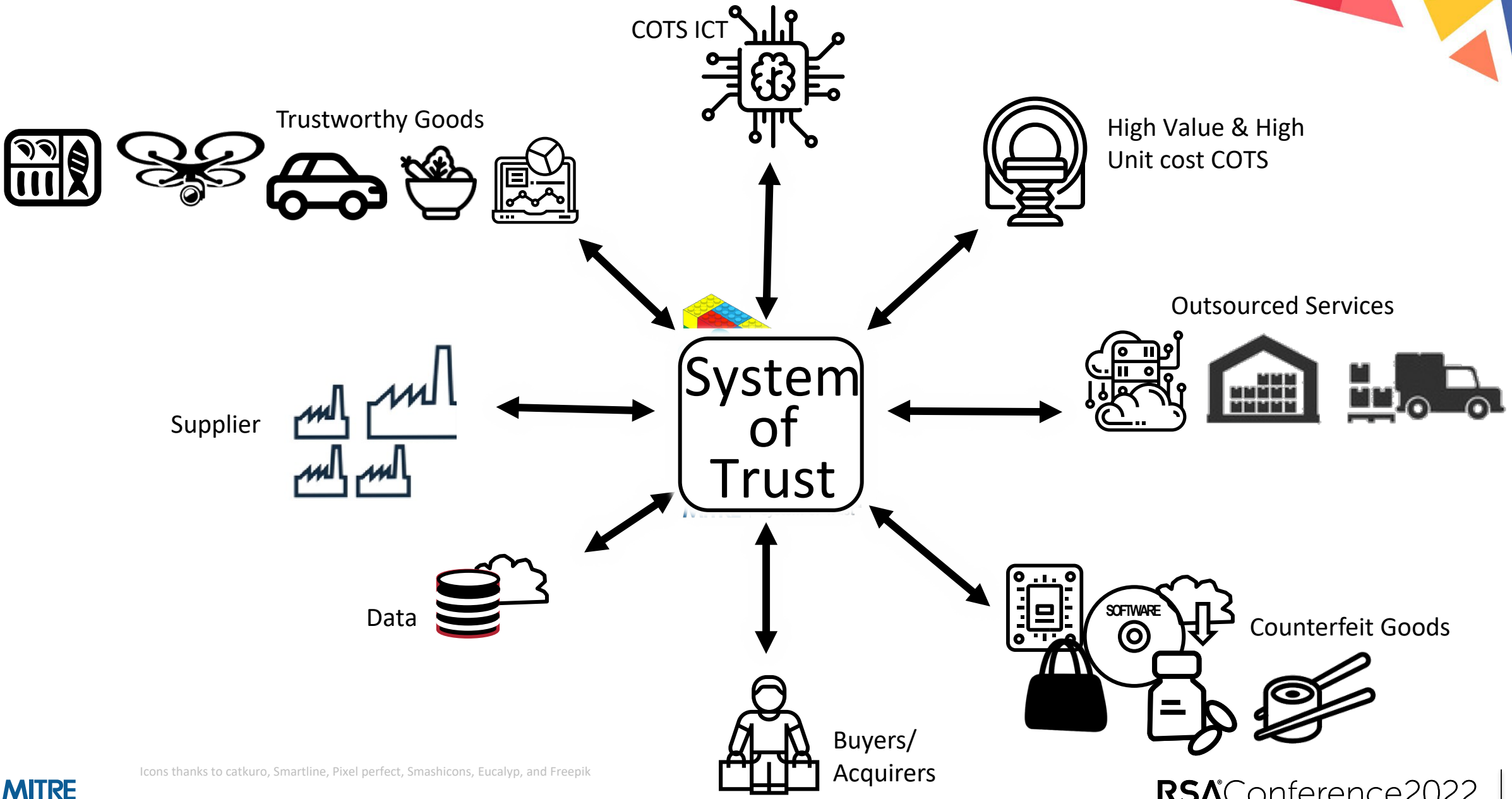


Top-Level Concerns Vendor/Product B



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Effective Supply Chain Trust Interactions



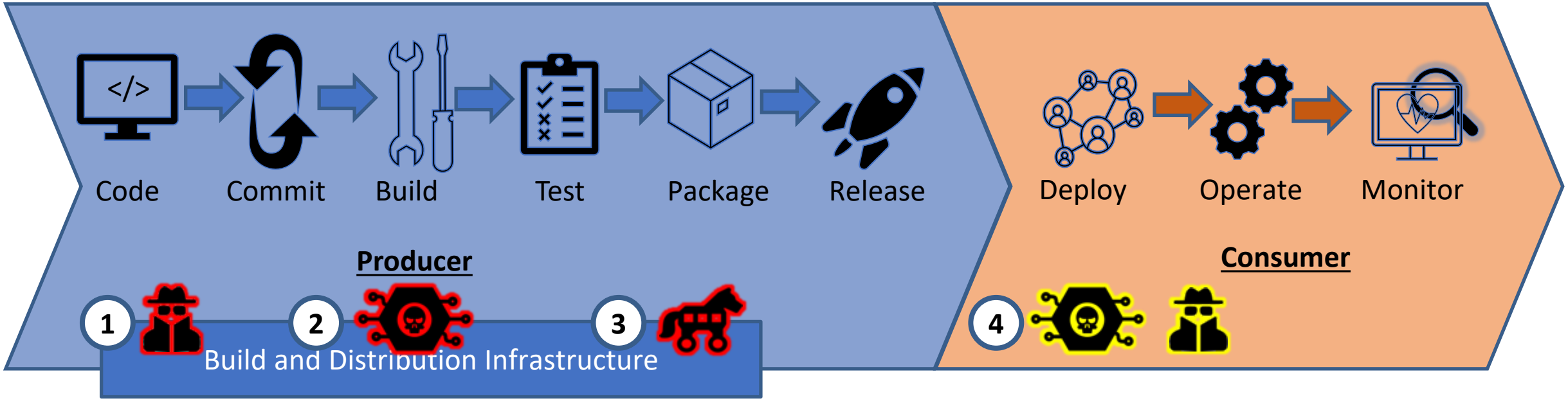
Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-91

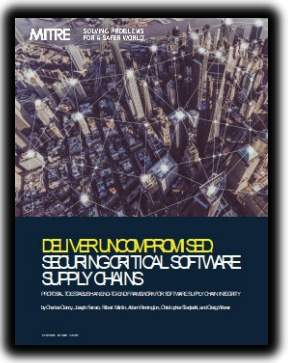
Software Supply Chain Integrity Attack

(a.k.a SolarWinds)

1. Preparatory compromises at SolarWinds date back to October 2019. (Refs 11 & 12)
2. At some point there was a compromise of the build environment itself.
3. Malicious code sent in SolarWinds updates released between March and at least June 2020. (Refs 32 & 33)
4. Approximately 18,000 organizations receive the tainted updates and may have been targeted and impacted.

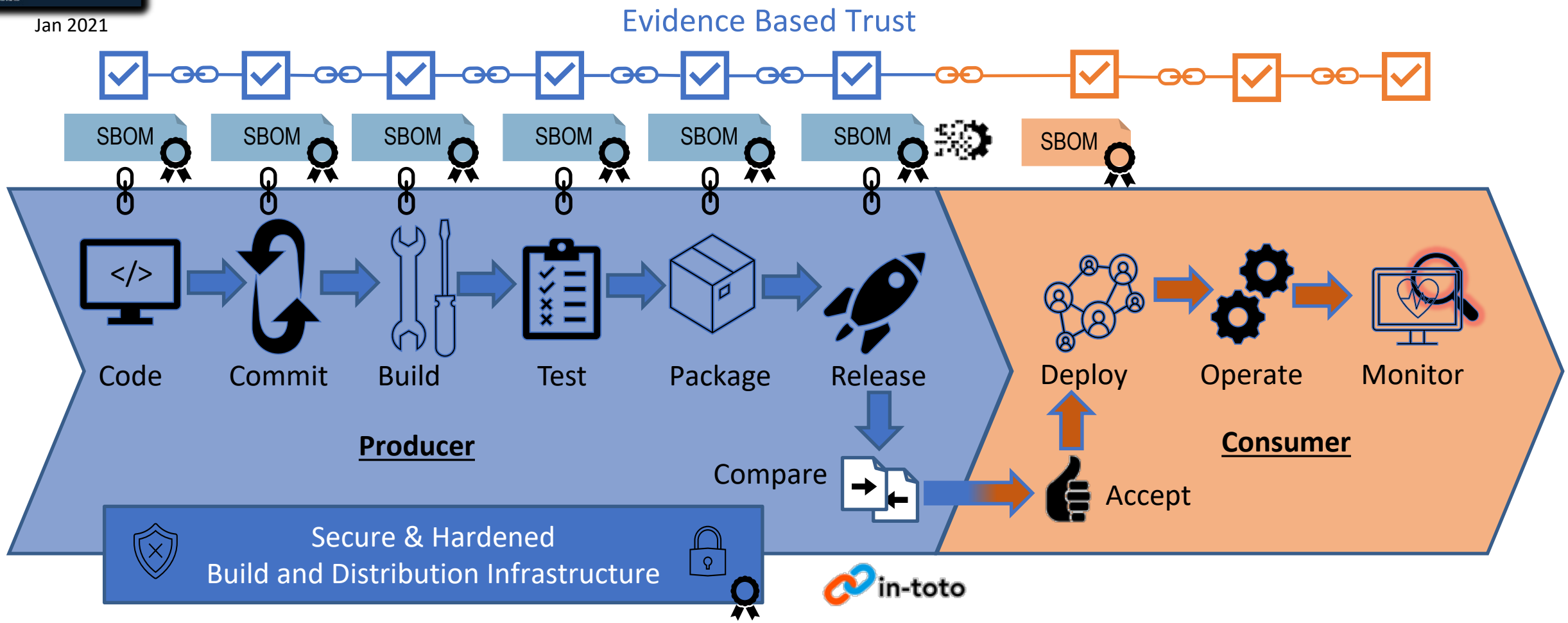


© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88



Jan 2021

Software Supply Chain Integrity

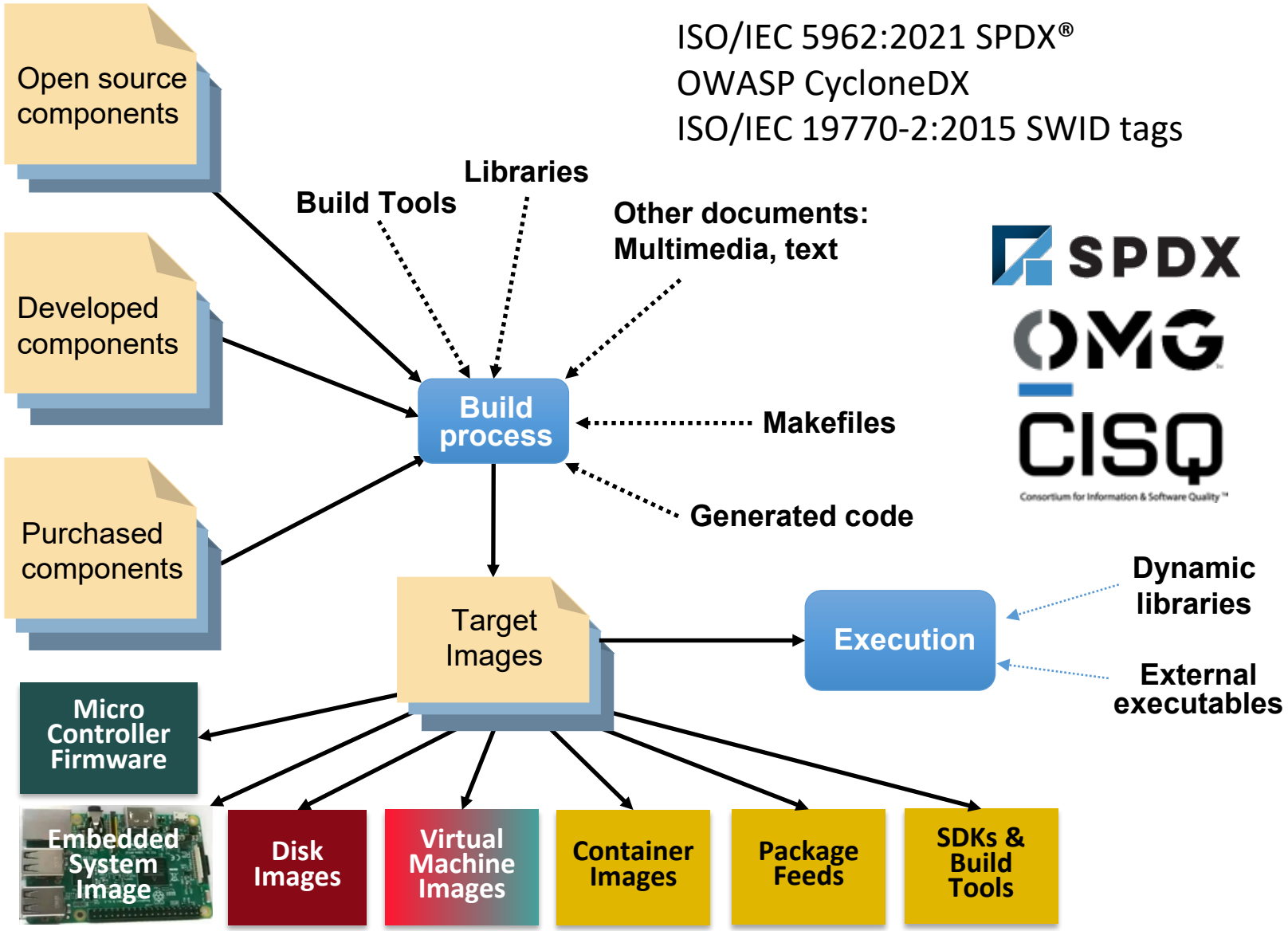


https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Software Bill of Materials Standardization

ISO/IEC 5962:2021 SPDX®
OWASP CycloneDX
ISO/IEC 19770-2:2015 SWID tags



SPDX
OMG
CISQ
Consortium for Information & Software Quality™

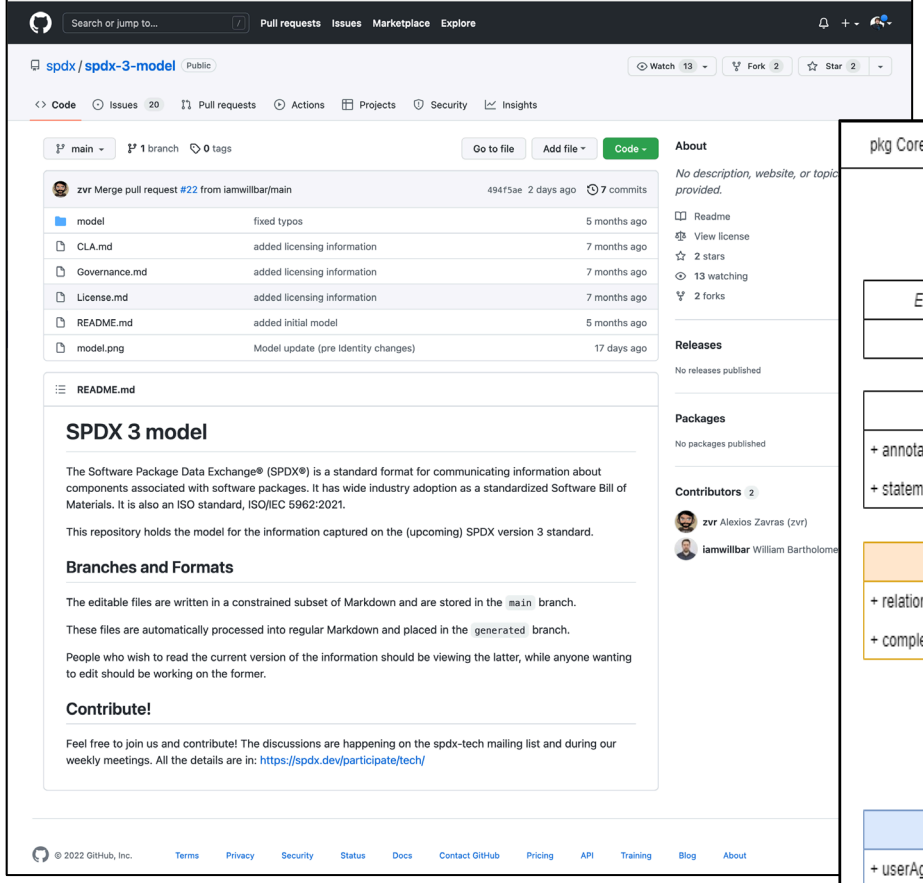
Usage Scenarios Around SBOMs

- **Refer, Transfer or Purchase** (definition of what it is)
- **Pedigree** (history of how it was produced)
- **Provenance** (chain of custody of it)
- **Integrity** (cryptographic basis of unalteredness)
- **Proper and Legal** (conditions about its use)
- **Known Sw Vulns** (known fixes are applied to it)
- **Assurance** (safe-secure-resilient)
- **SBoM of a SW Service** (SBoM of sw delivering service)
- **Supply Chain Sequence Integrity**

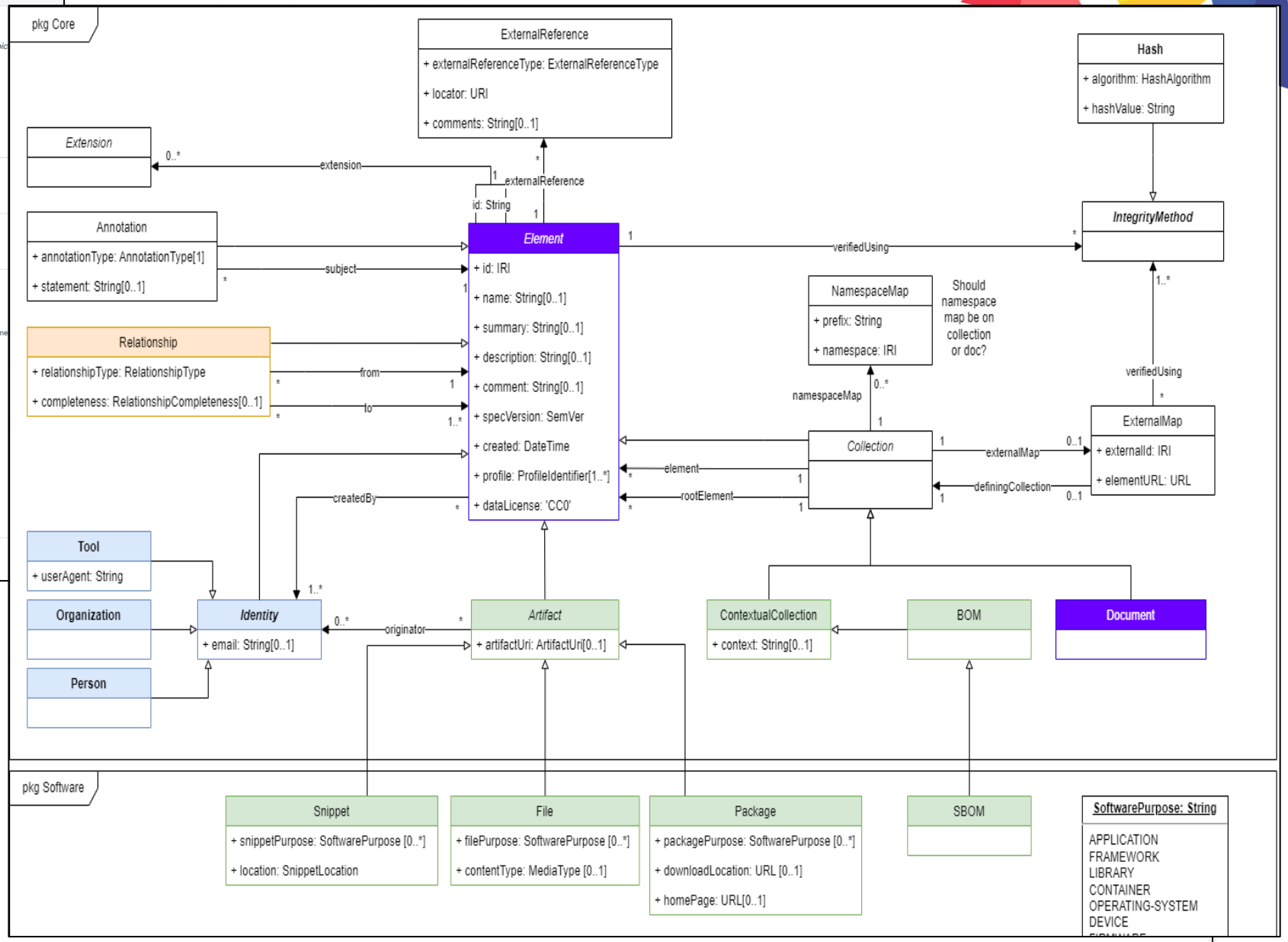
https://www.mitre.org/publications/technical-papers/standardizing-sbom-within-the-sw-development-tooling-ecosystem

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

SPDX 3.0 effort



https://github.com/spdx/spdx-3-model



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Lowering Adoption Hurdles for SBOMs and more

SBOMs

SBOMs

SBOMs

SBOMs

- Agriculture and Food
- Energy
- Transportation
- Chemical Industry
- Postal and Shipping

- Water
- Public Health
- Telecommunications
- Banking and Finance
- Key Assets

End Users in Industry, Government, and Commerce

Sectors

- Medical Devices
- Merchandise
- Automobiles
- Trains
- Vessels/Boats
- Building Mngt Sys
- Software

Product & Service Suppliers

Assets/ Capabilities

ICT SCRM Task Force
HBOM Working Group

INTEGRATED DEVELOPMENT ENVIRONMENTS (IDEs)

SOFTWARE COMPOSITION ANALYSIS

SOURCE CODE & PACKAGE REPOSITORIES

FRAMEWORKS

CLOUD TOOLS

BUILD CHOREOGRAPHY

LIC MNGT

Tools & Capabilities for Software

Software Ecosystems

INVENTORY MANAGEMENT SYSTEMS

PRODUCT LIFECYCLE MANAGEMENT (PLM) TOOLS

STANDARD OPERATING PROCEDURES

CAD SYSTEMS

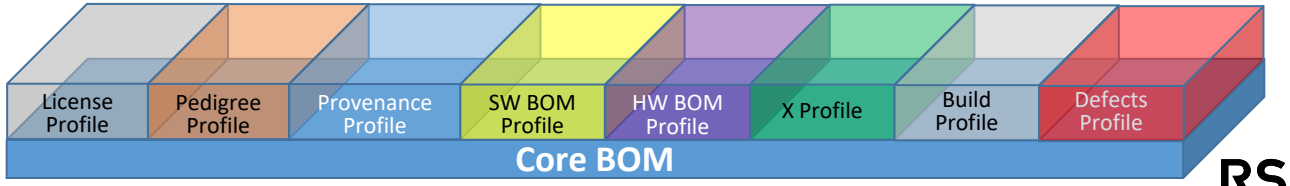
CATALOG BUILDERS

BOM MANAGEMENT SYSTEMS

Tools & Capabilities for Hardware

Hardware Ecosystems

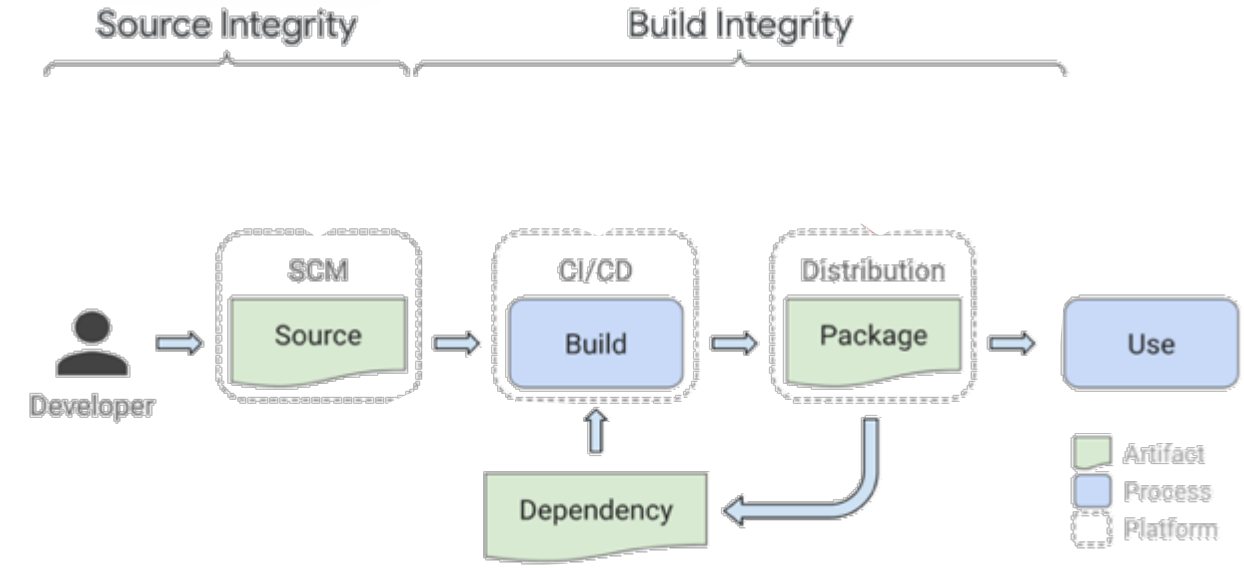
SPDX 3.0 effort



https://github.com/spdx/outreach/blob/main/SPDX and 3T-SBOM Intro.pptx

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply-chain Levels for Software Artifacts (SLSA)

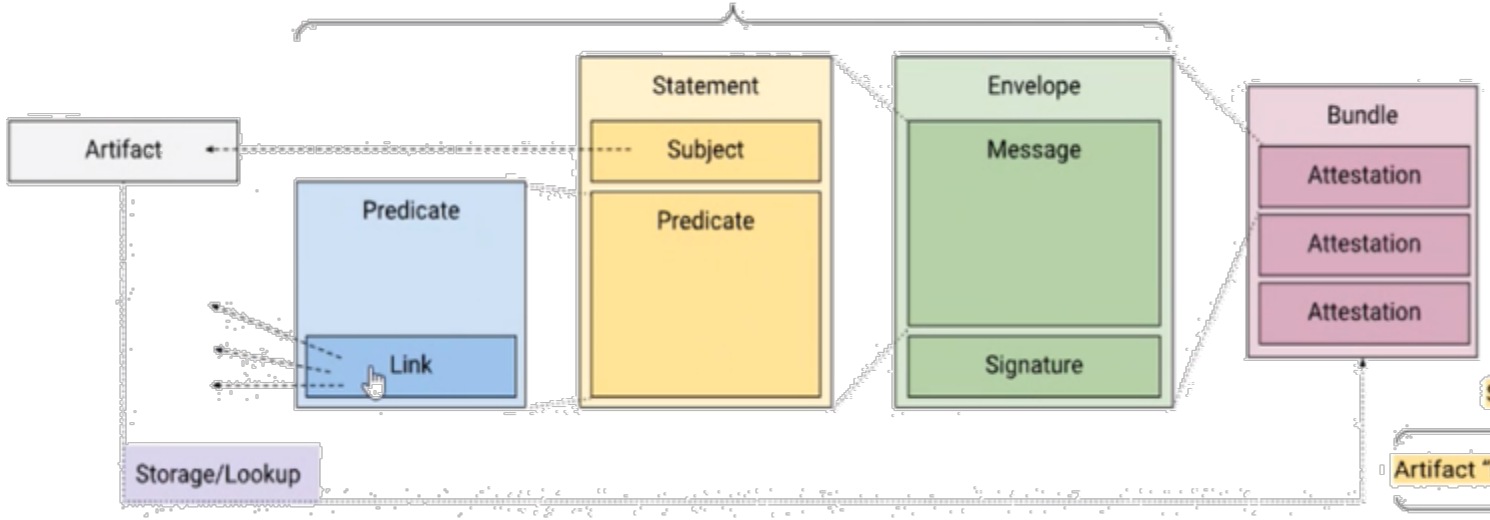


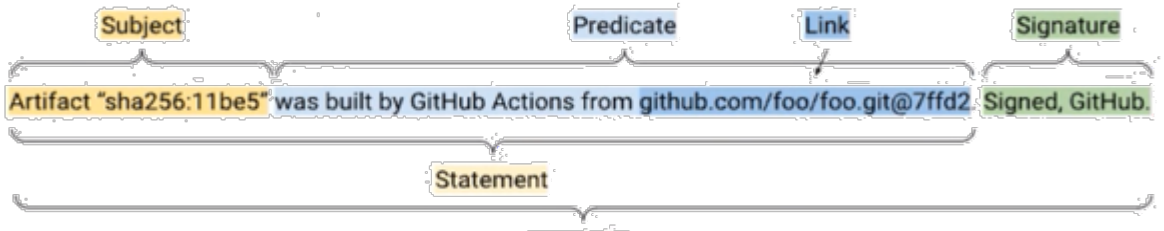
SLSA guidelines have 4 levels of incremental and actionable things that software producers can claim to do to protect against specific integrity attacks

https://github.com/slsa-framework/slsa

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version Controlled		✓	✓	✓
Source - Verified History			✓	✓
Source - Retained Indefinitely			18 mo.	✓
Source - Two-Person Reviewed				✓
Build - Scripted Build	✓	✓	✓	✓
Build - Build Service		✓	✓	✓
Build - Ephemeral Environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓
Build - Reproducible				○
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service Generated		✓	✓	✓
Provenance - Non-Falsifiable			✓	✓
Provenance - Dependencies Complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

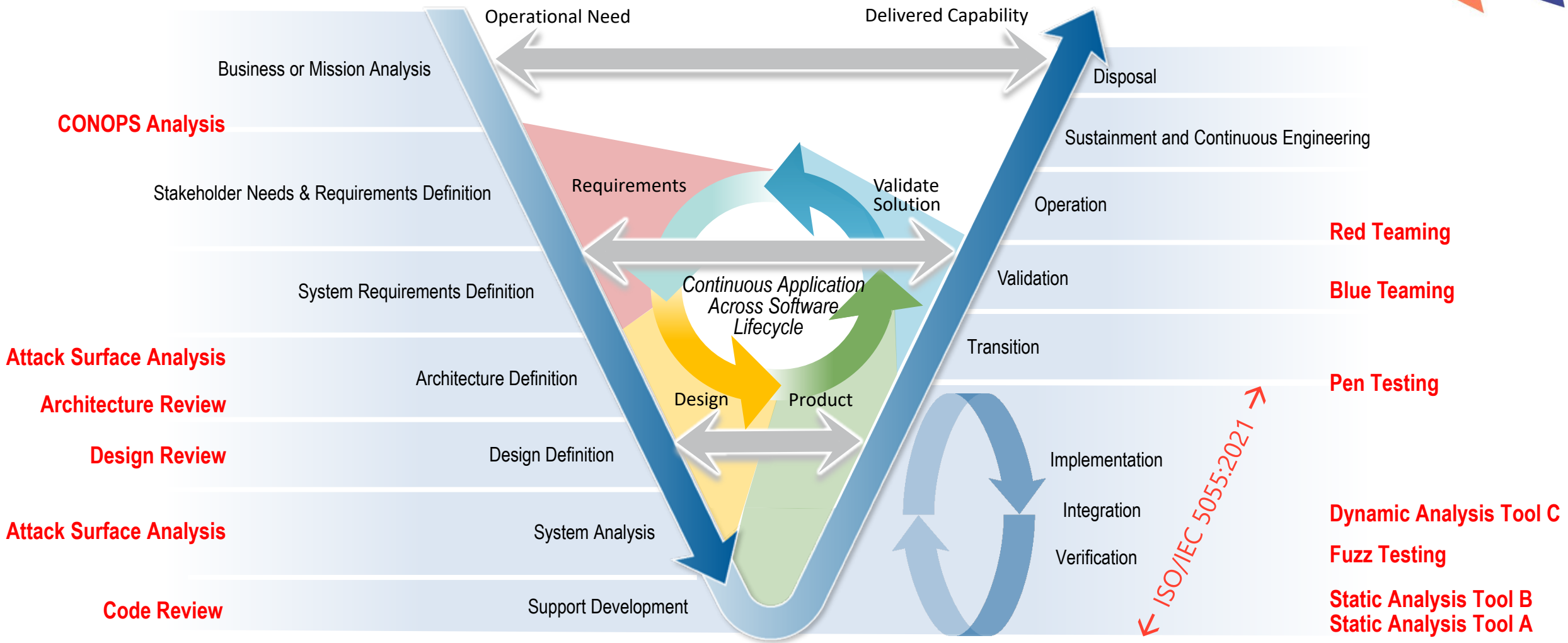
○ = required unless there is a justification





© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Software Development and Assurance Lifecycle Phases



NOTE: *Lifecycle processes typically occur simultaneously, **not** in sequence; see ISO/IEC 15288 & 12207*

NOTE: *Implementation, Integration & Verification are often performed continuously & simultaneously with the aid of Integrated Development Environments (IDEs) & other tools.*

Figure 3-2 from "Software Trustworthiness Best Practices," 2020, https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

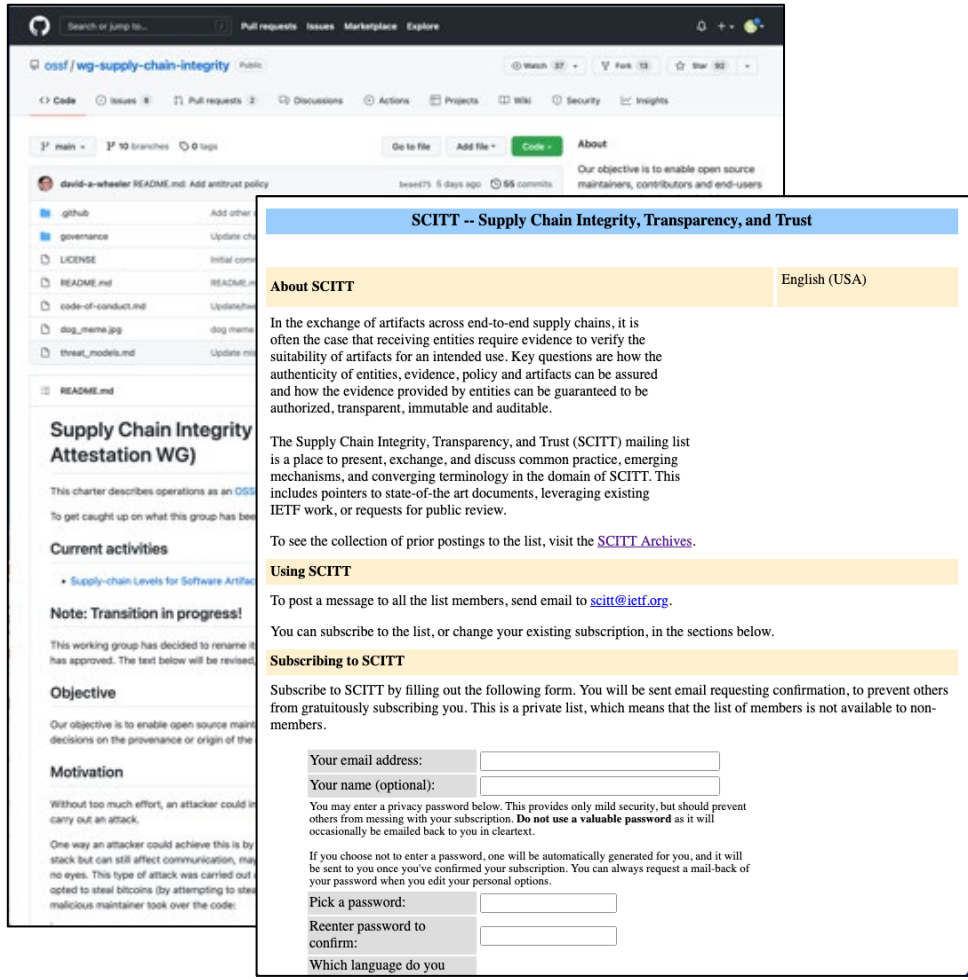
Supply Chain Integrity Transparency and Trust (SCITT)

Technologies leveraged:

- Claims/Evidence, Confidential Ledgers, Hardware Roots of Trust, BOMs, CBOR (RFC 8949) and COSE (RFC 8152)

SCITT:

- defines minimum standards around the:
  - preparation, storage, distribution, consumption, validation and evaluation of arbitrary claims/evidence about artifacts that are critical to maintaining the integrity of supply chains
- specifies an end-to-end system for validating arbitrary claim/evidence artifacts in terms of supply chains whose integrity has been proven.
- is applicable to both hardware (objects in the physical world) and software (digital) artifacts.
- does not define how artifacts are produced or distributed, nor the methods by which claims/evidence about artifacts are produced prior to preparation for inclusion in SCITT.

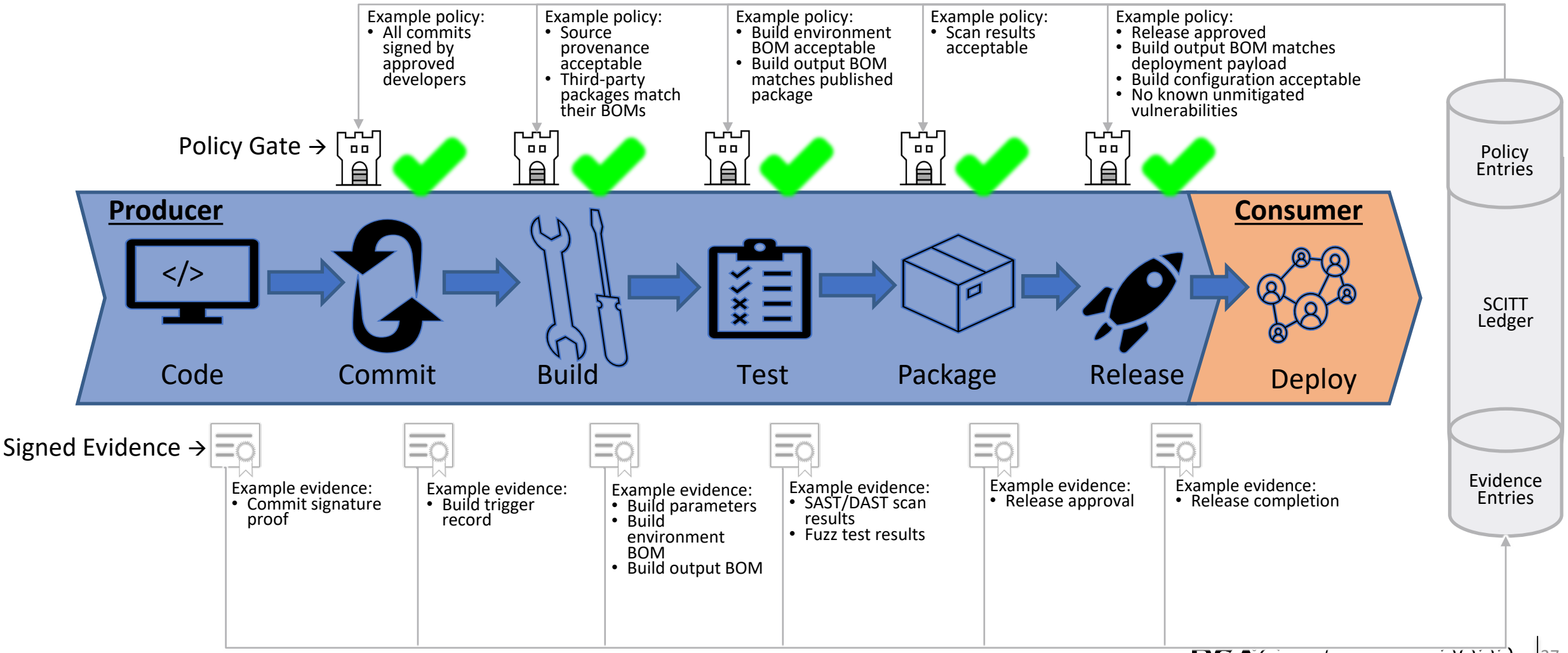


https://github.com/ossf/wg-supply-chain-integrity

https://www.ietf.org/mailman/listinfo/scitt

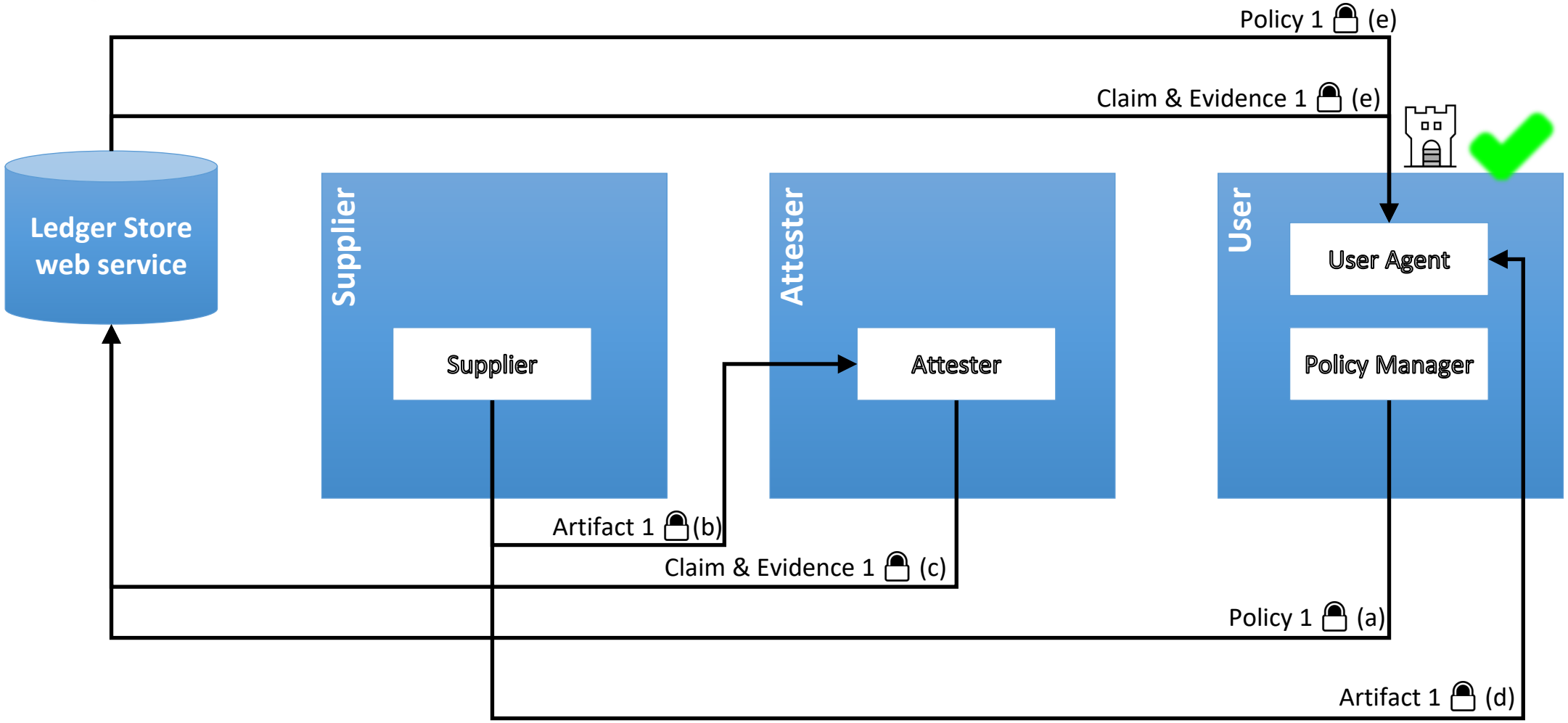
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chain Integrity
Software Supply Chain Security Risks
Transparency and Trust (SCITT)



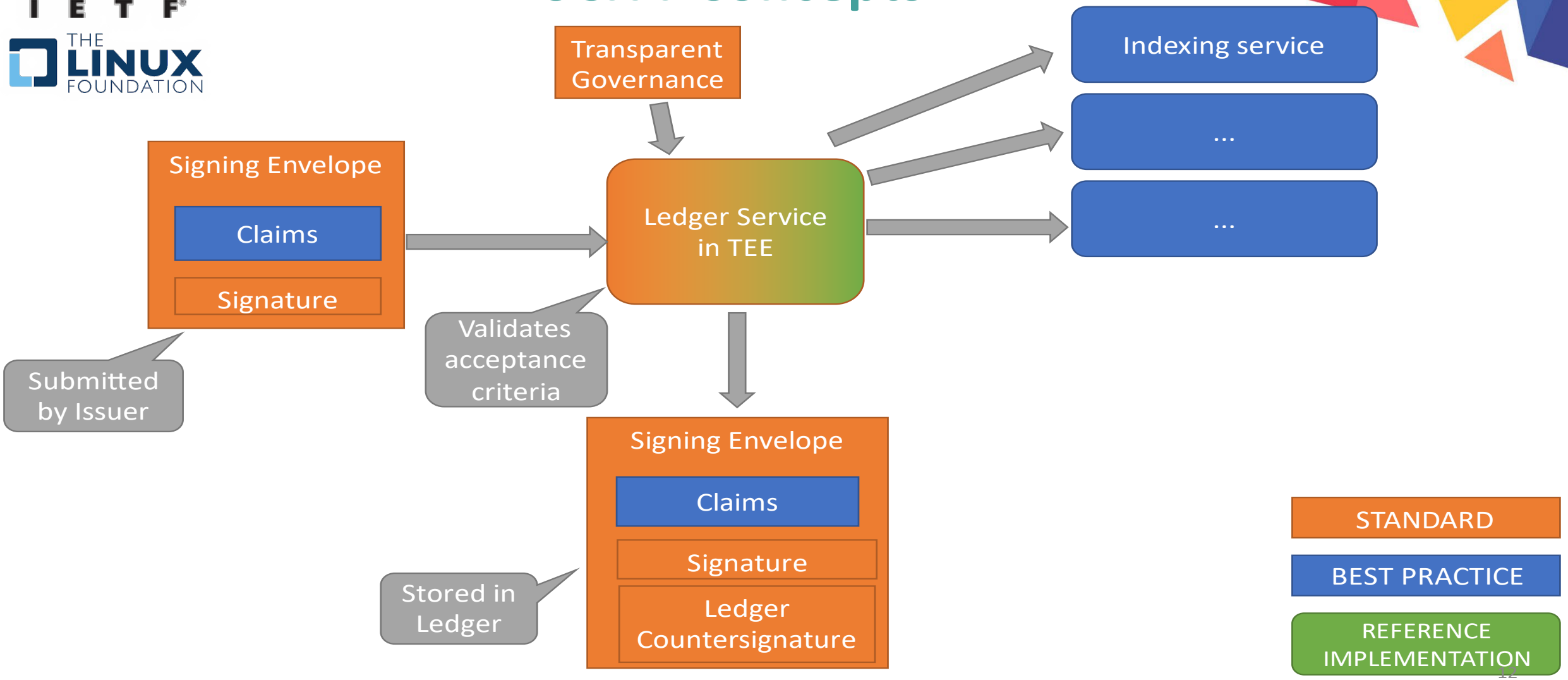
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-91

Example of SCITT in the Marketplace



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

SCITT Concepts

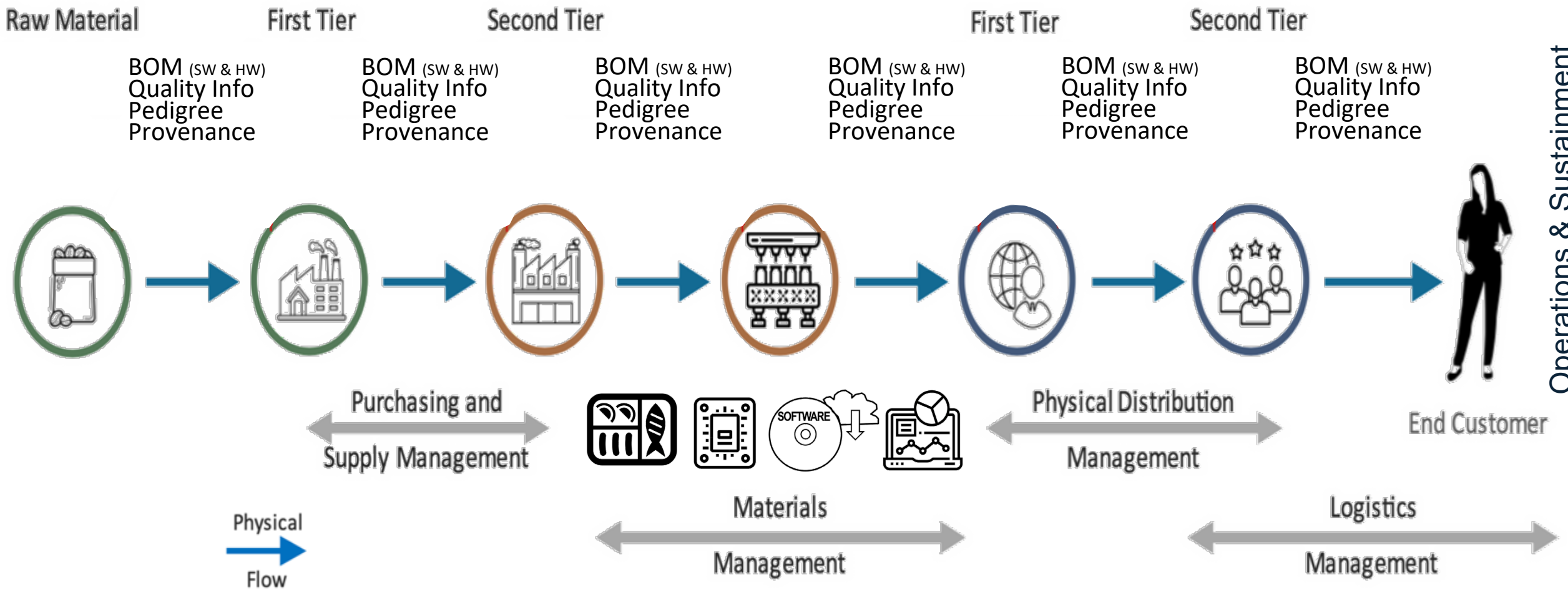


An Architecture for Trustworthy and Transparent Digital Supply Chains
https://datatracker.ietf.org/doc/html/draft-birkholz-scitt-architecture-00

Countersigning COSE Envelopes in Transparency Services
https://datatracker.ietf.org/doc/html/draft-birkholz-scitt-receipts-00

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chains – As multi-Stakeholder Network



https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

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
- 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
- RSA Conference 2022
- CISQ Resilience Summit
- others…

Executive Acquisition

Congressional Committees

MITRE

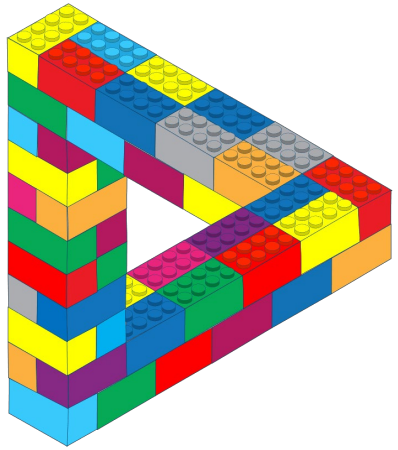
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

RSAConference

SYSTEM OF TRUST™

System of Trust Plans with Sponsors and Industry

- 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 BoK 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 RMM tool & SoT content to Industry for integration in their own assessment practices and offerings



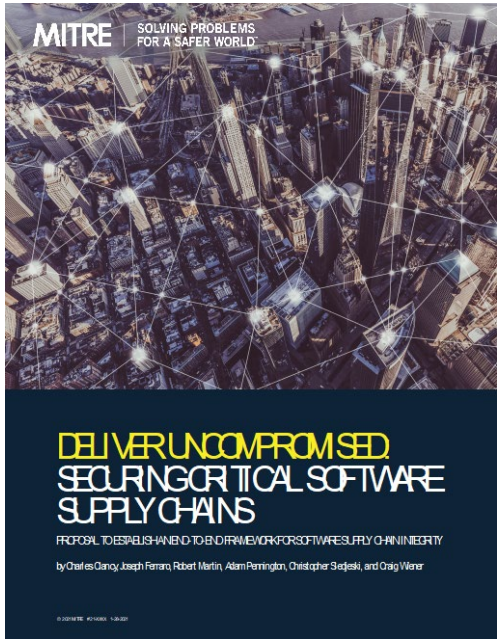
MITRE | System of Trust™

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Publications to date…

TheSciTechLawyer WINTER 2021

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



https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf

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

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

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88

Supply Chain Security - System of Trust™

Overview | System of Trust Framework | Pilot Results | Resources | News & Calendar

Industry, government, and academia are putting increased focus on the need for trustworthy supply chains, trustworthy partners, and trusted systems globally, a reliable path to an actionable understanding of the risks that can impact the trustworthiness of supplies, suppliers, and services is essential.

The System of Trust Framework aims to provide a comprehensive, consistent, and repeatable supply chain security risk assessment risk assessment process that is customizable, evidence-based, and scalable, and will enable all organizations within the supply chain to have confidence in each other, service offerings, and the supplies being delivered.

SoT@MITRE.ORG

Terms of Use | Privacy Policy | Contact Us

Supply Chain Security System of Trust (SoT) is an initiative of The MITRE Corporation. Copyright © 2020-2022, The MITRE Corporation. Lego block images used with permission. System of Trust, Risk Model Manager, and the System of Trust logo are trademarks of The MITRE Corporation.

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 21-01357-88