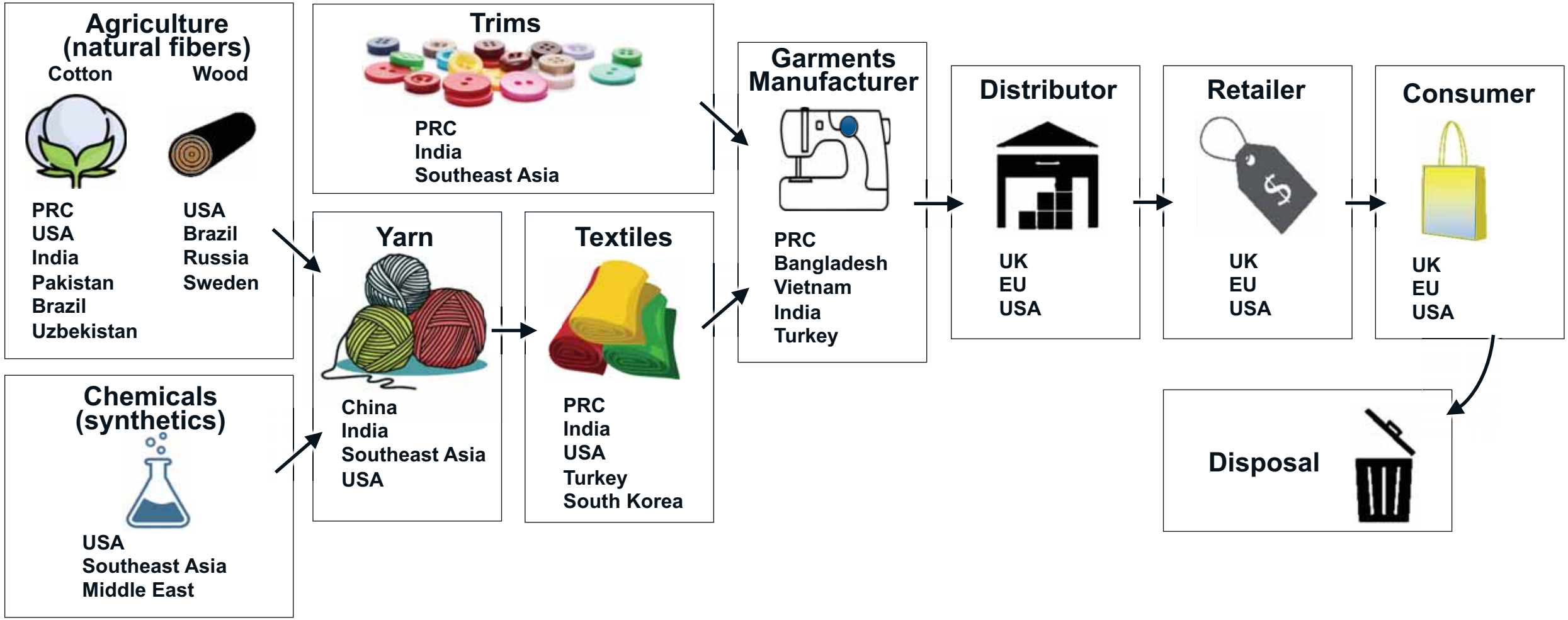
Supply Chain Security: MITRE's System of Trust™, SCITT & SBOMs

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

Presentation to BlackBerry PSEC
30 November 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

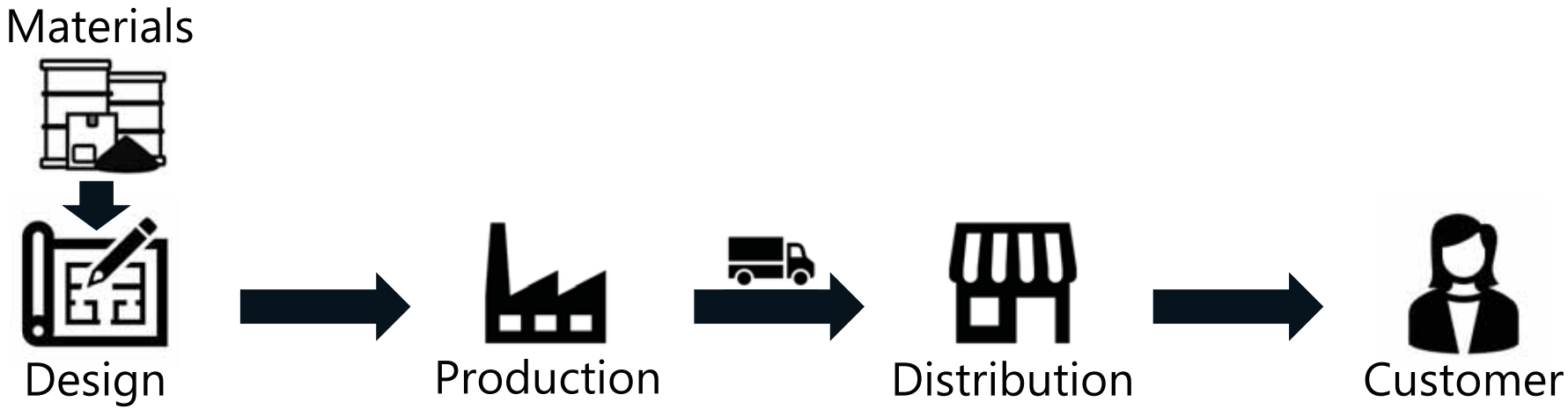
Supply Chain Example – Consumer Clothing



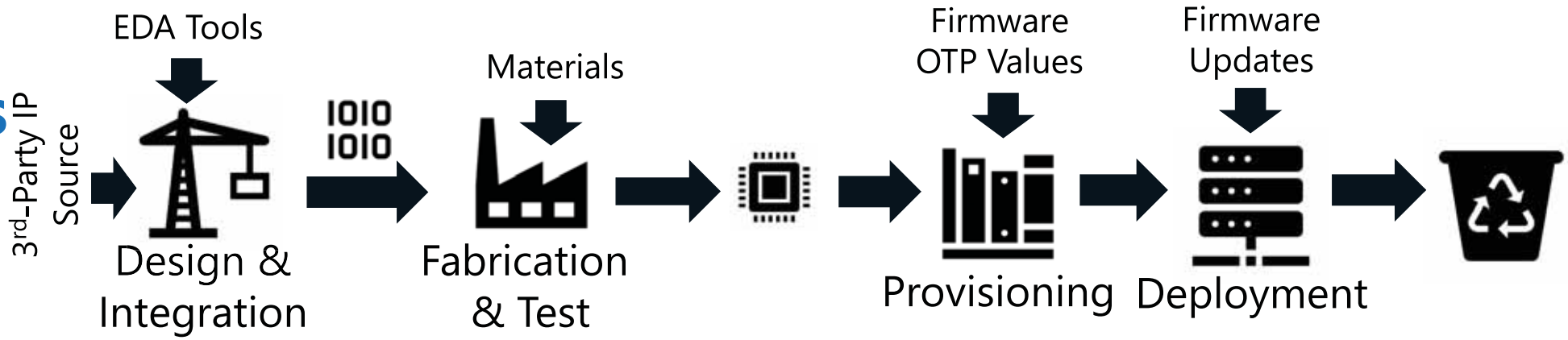
https://imgs.mongabay.com/wp-content/uploads/sites/20/2020/04/23100736/FF_Supplychain.png

Supply Chains

Generic Supply Chain

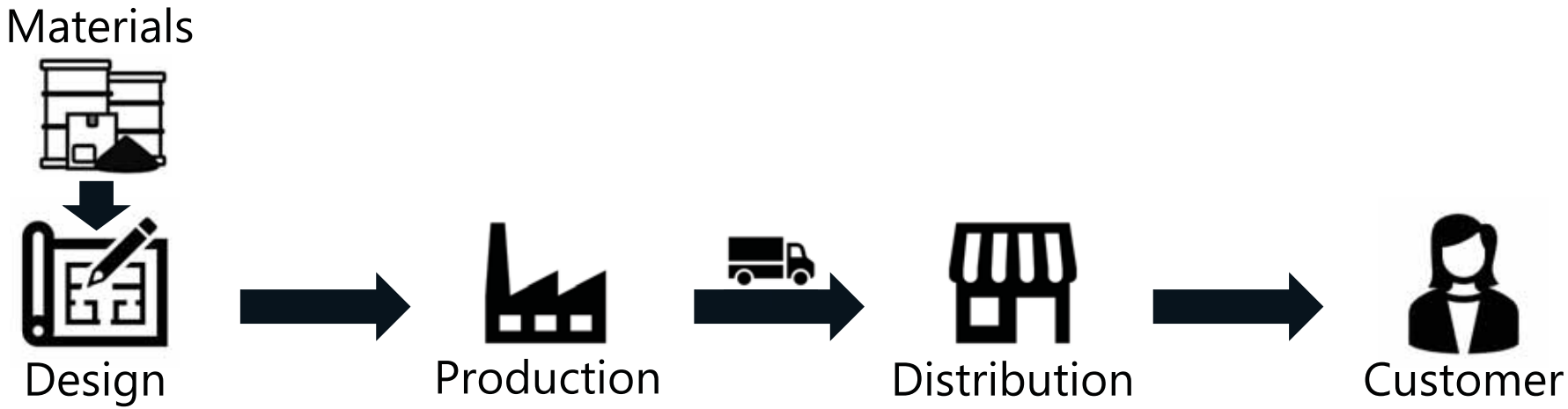


Micro-electronics Supply Chain

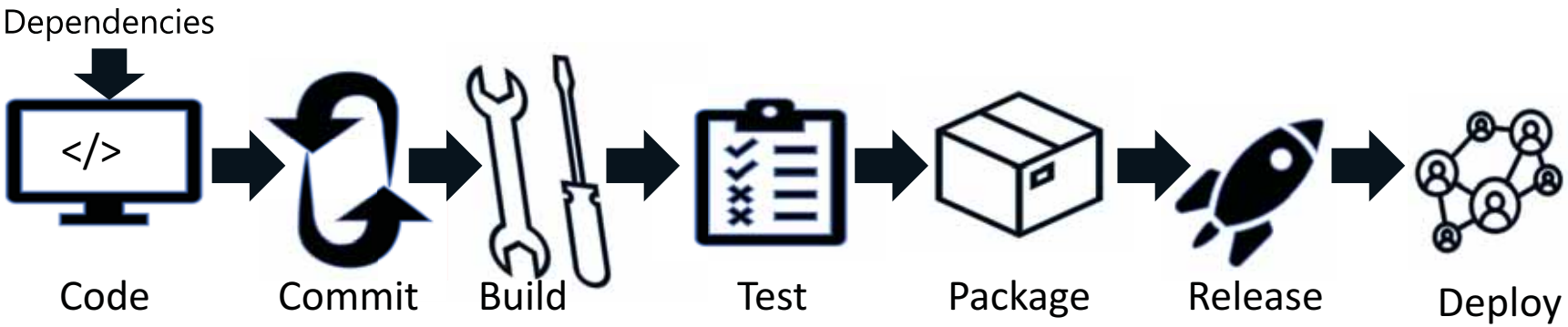


Supply Chains

Generic Supply Chain

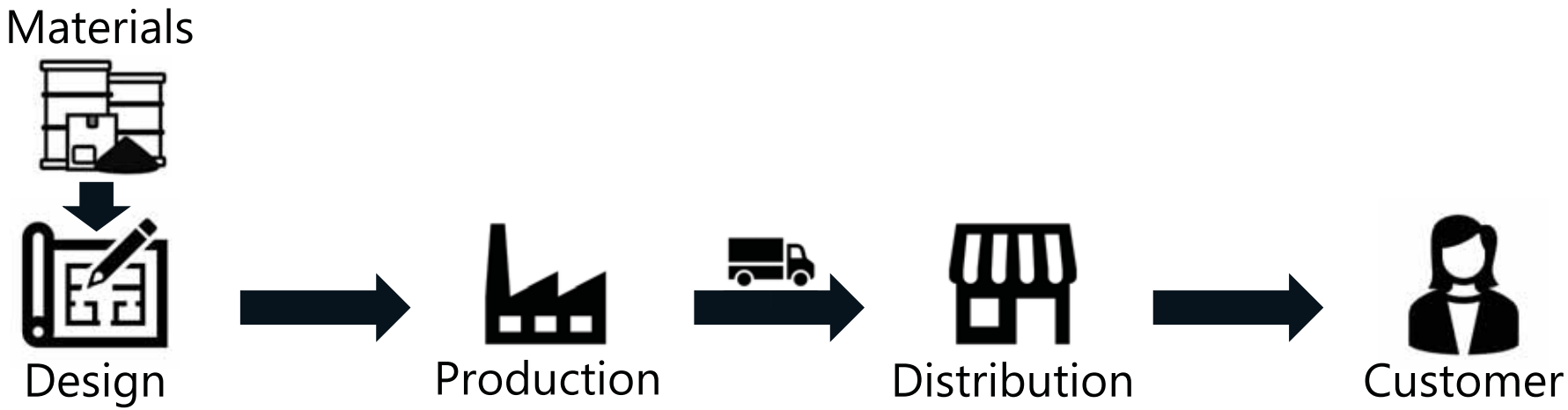


Software Supply Chain

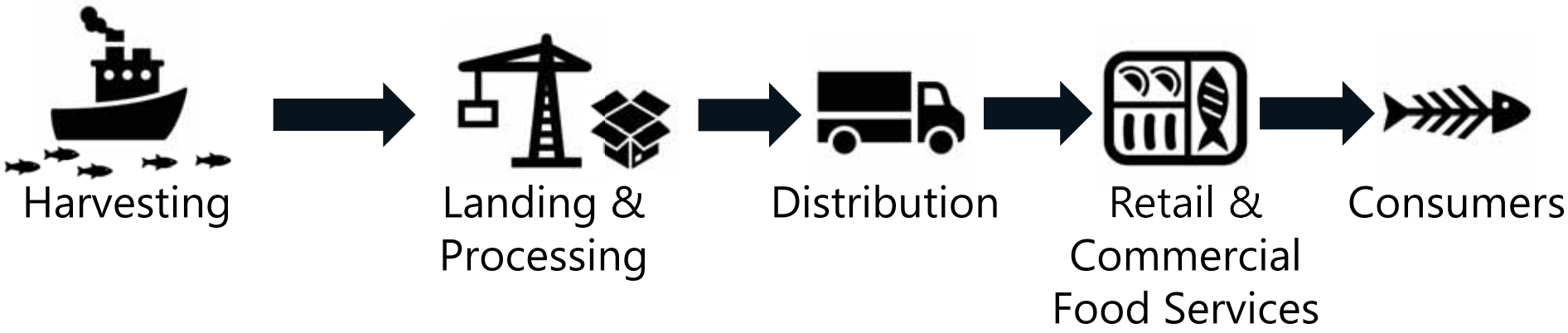


Supply Chains

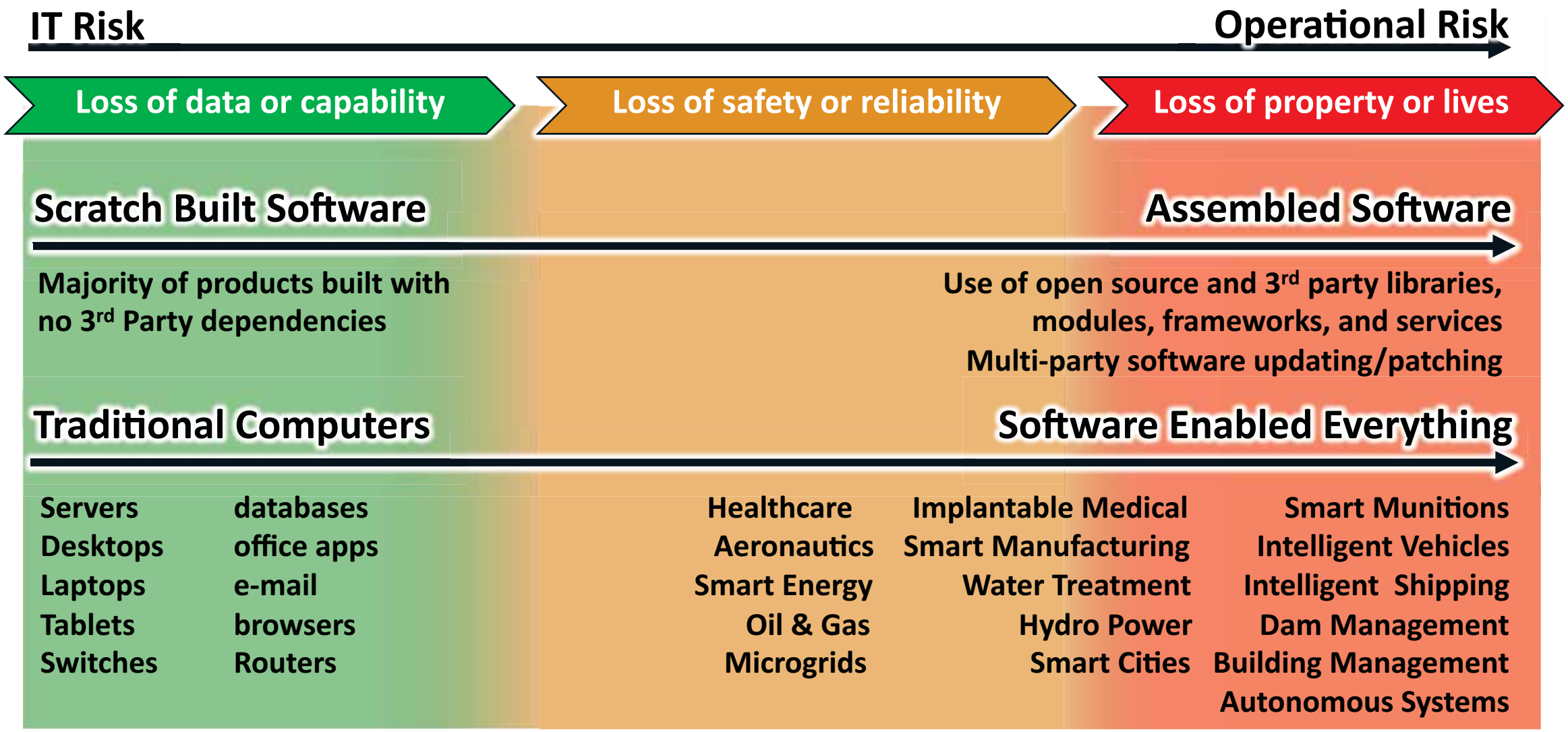
Generic Supply Chain



Seafood Supply Chain



Software is Ubiquitous, Assembled, and Critical



Software Enabled Critical Infrastructure and Mission Capabilities…

Medical

Buildings

Aeronautics

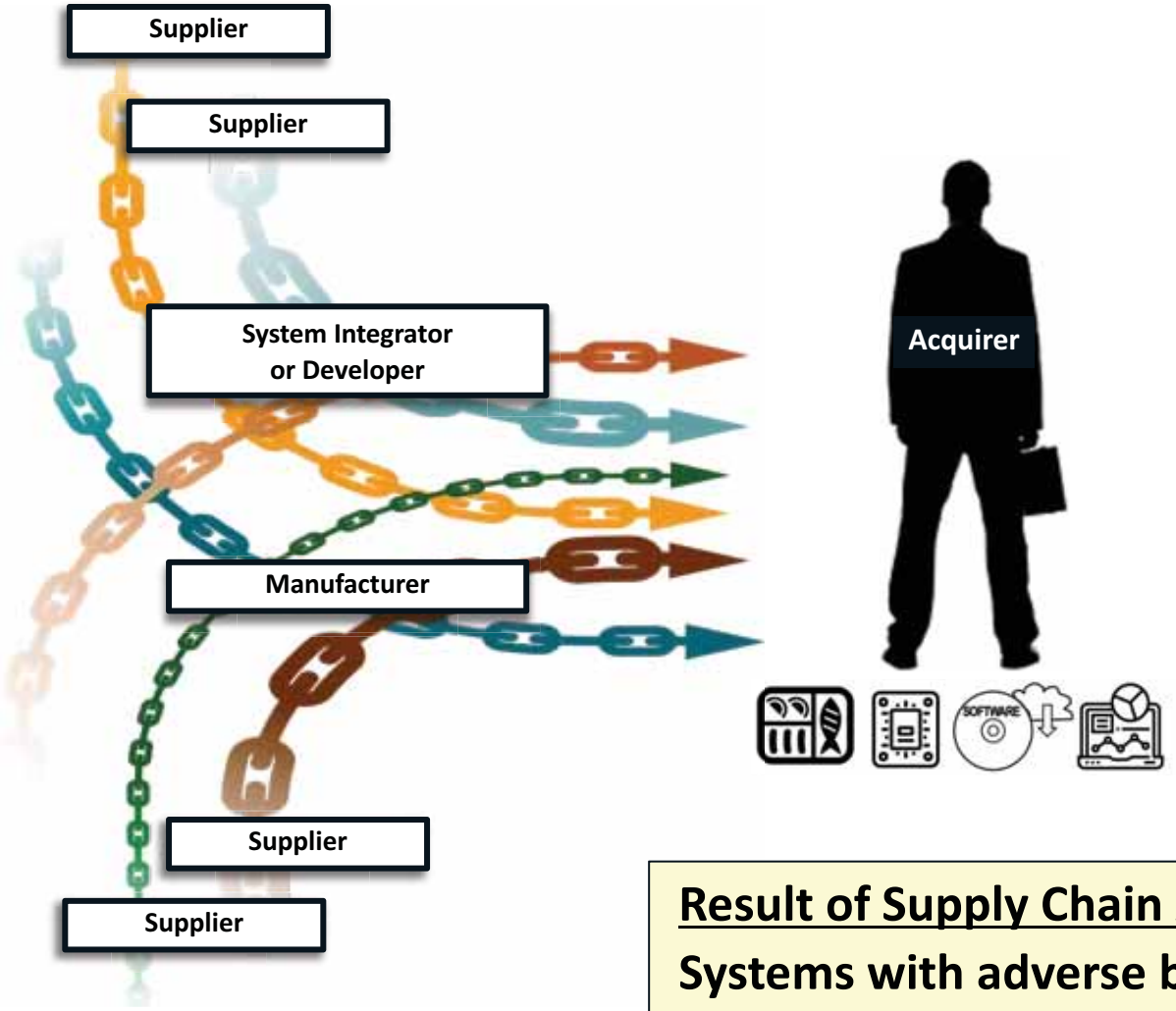
Manufacturing

Vehicles

Energy

Shipping

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



Based on SEI/CMU materials

Intentional acts

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

Unintentional acts

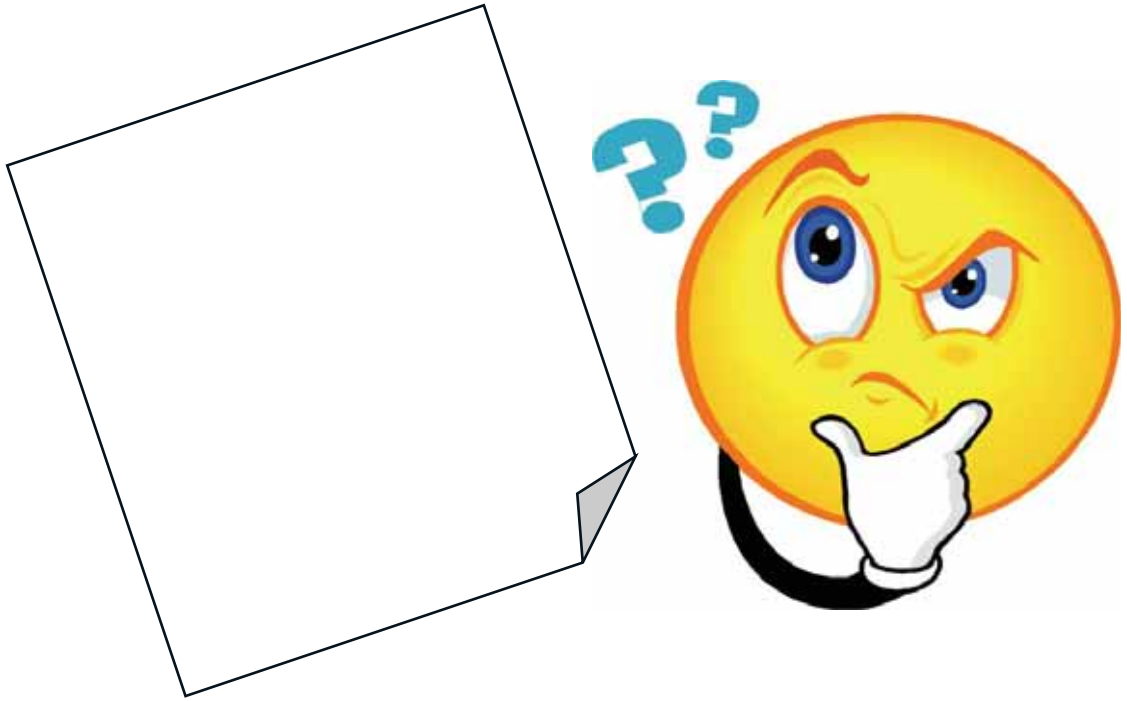
- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/weaknesses and/or known vulnerabilities)

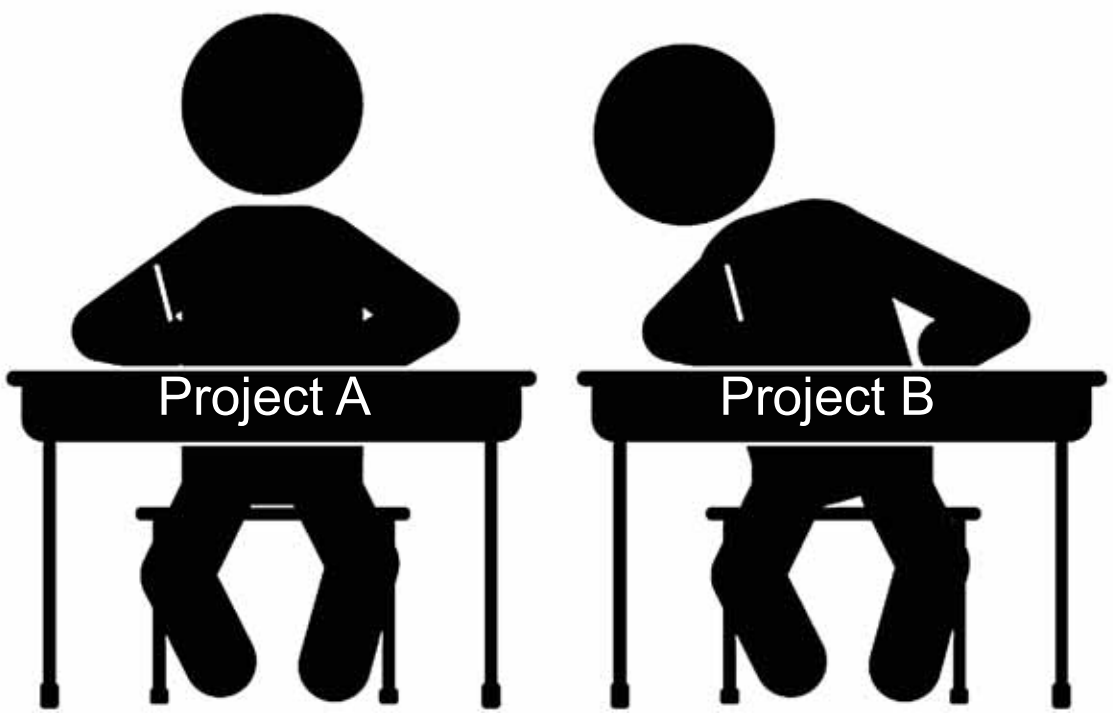
<u>Result of Supply Chain Attacks:</u>

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

MITRE

Open Question: What Supply Chain Risks to Manage?





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

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

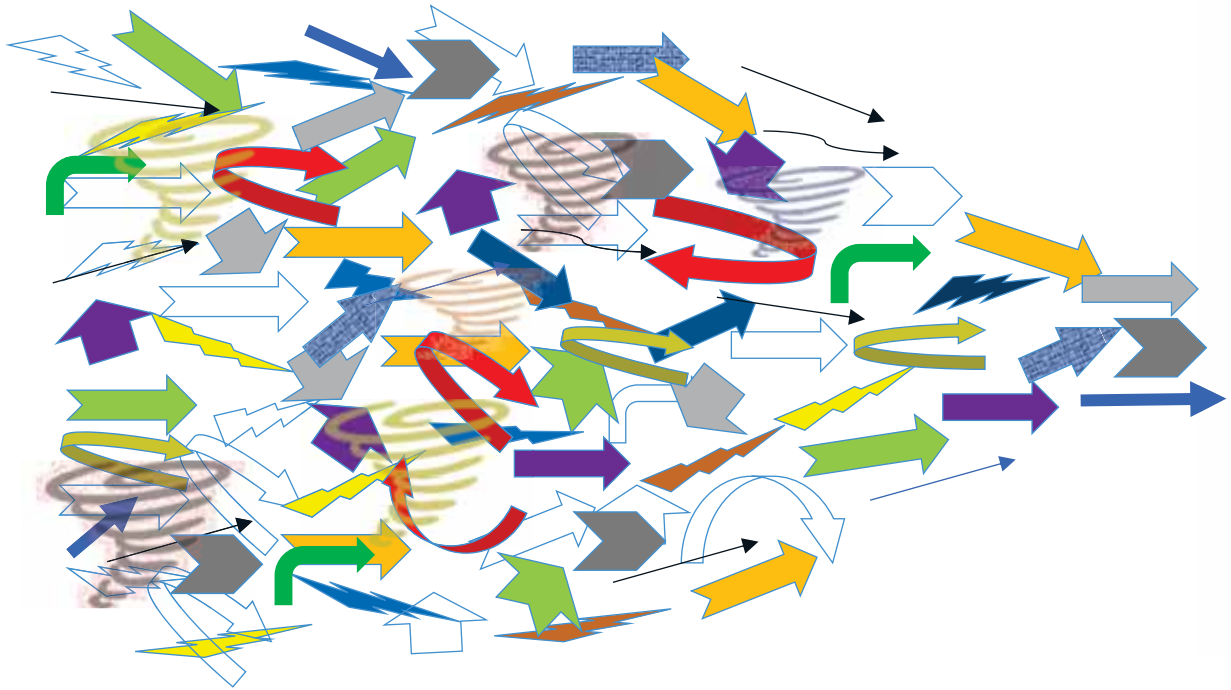
National Corruption

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™

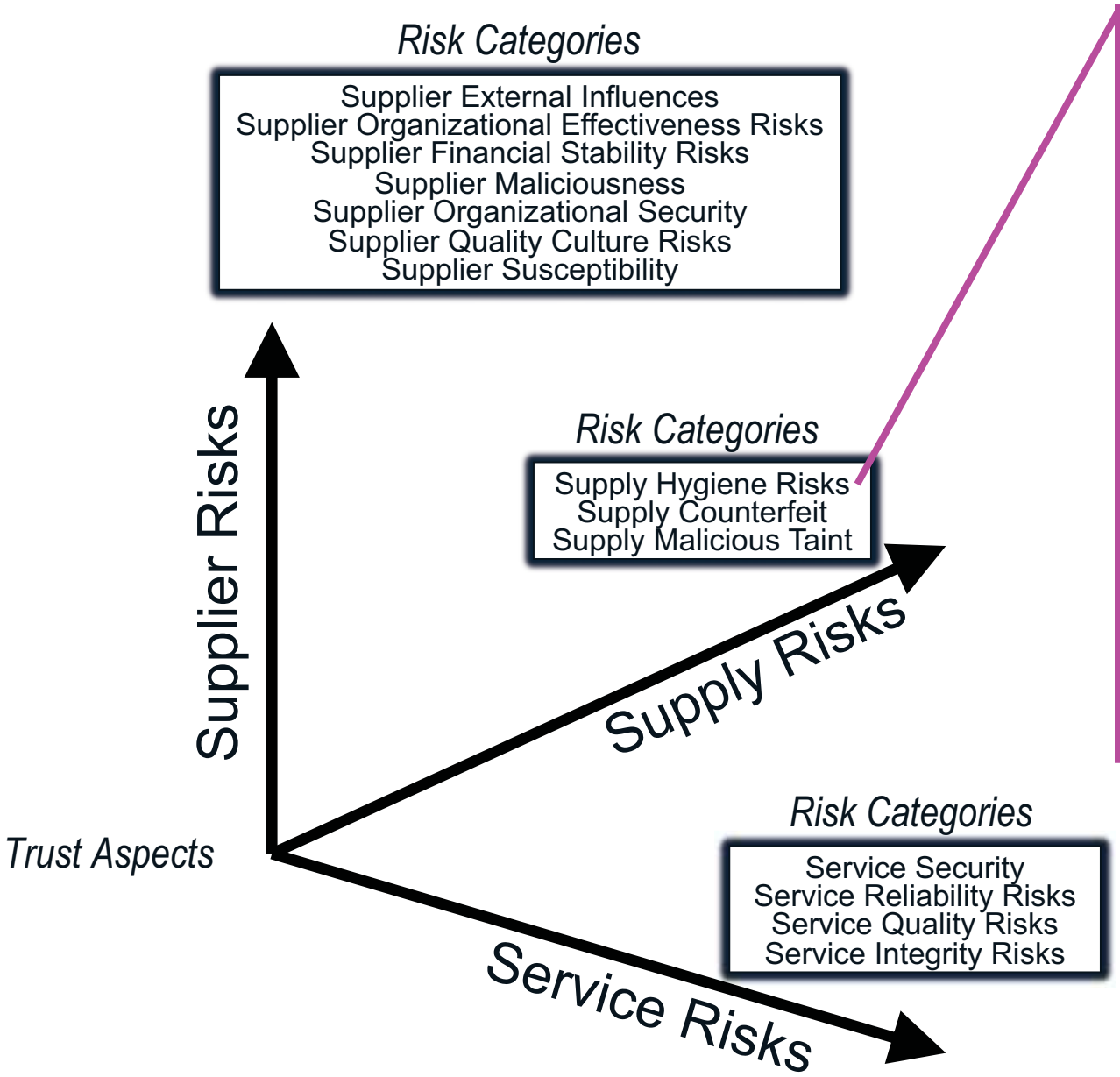


Address Chaos, Align & Organize

Simplify, Tailor & Use

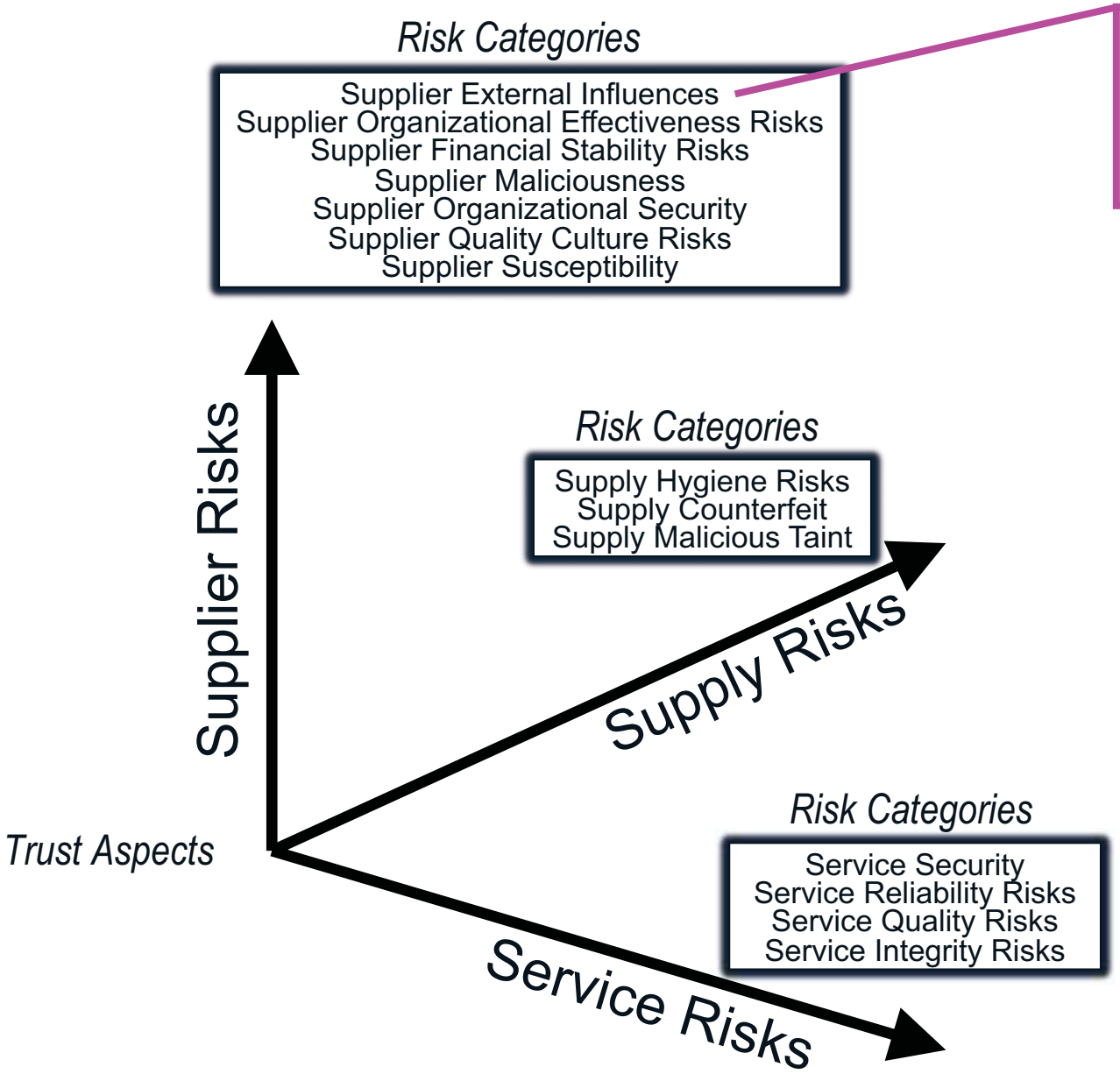
MITRE

Basis of Trust



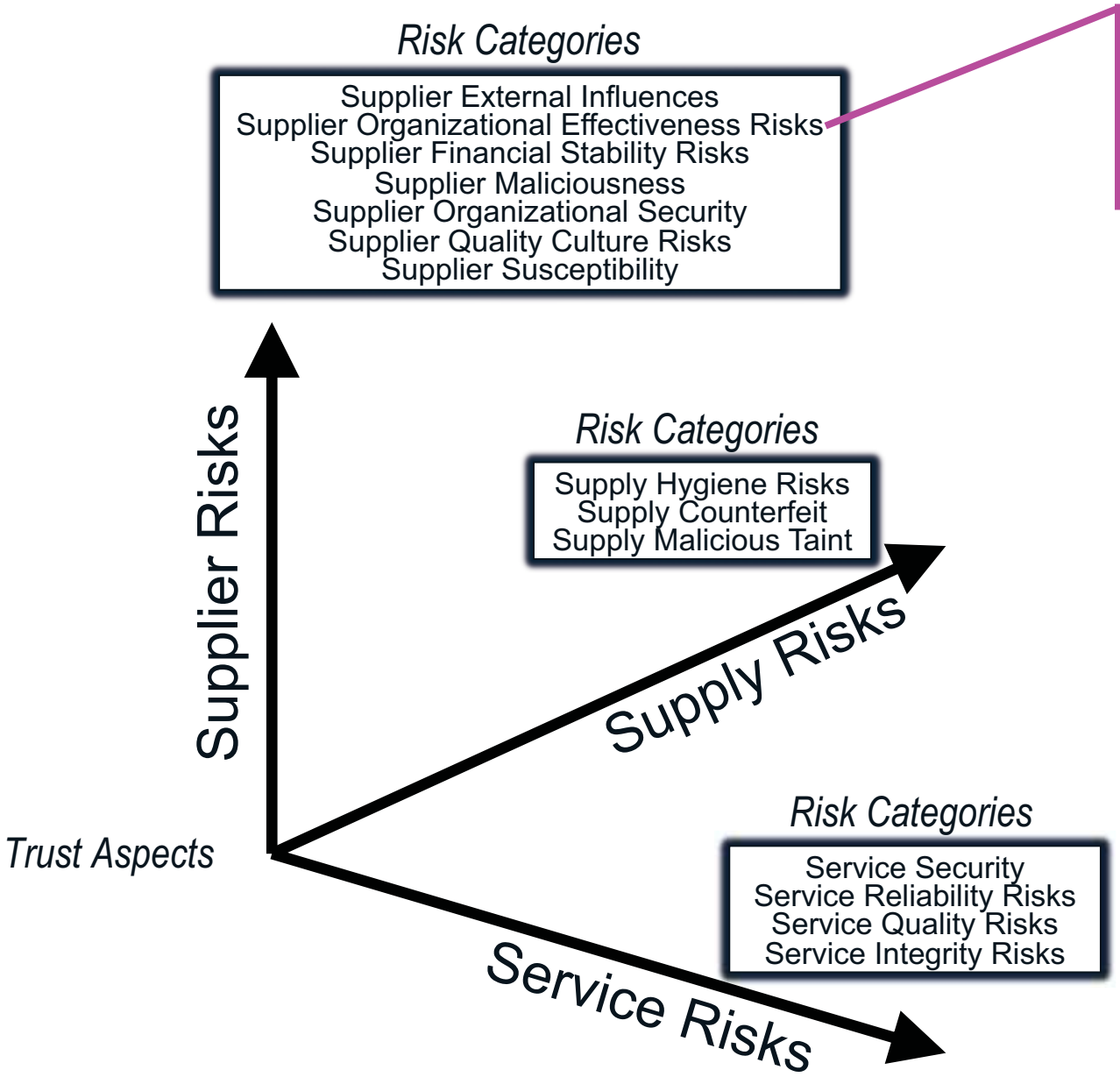
- **Product Quality Risks**
  - ICT Hardware Product Quality
  - Product Quality Requirements
  - Software Product Quality
  - Pharma Product Resilience
  - Food Product Resilience
- **Product Resilience Risks**
  - ICT Hardware Product Resilience
  - Software Product Resilience
  - Product Resilience Requirements
  - Pharma Product Resilience
  - Food Product Resilience
- **Product Security Risks**
  - ICT Hardware Product Security
  - Software Product Security
  - Product Security Requirements
  - Pharma Product Security
  - Food Product Security

Basis of Trust



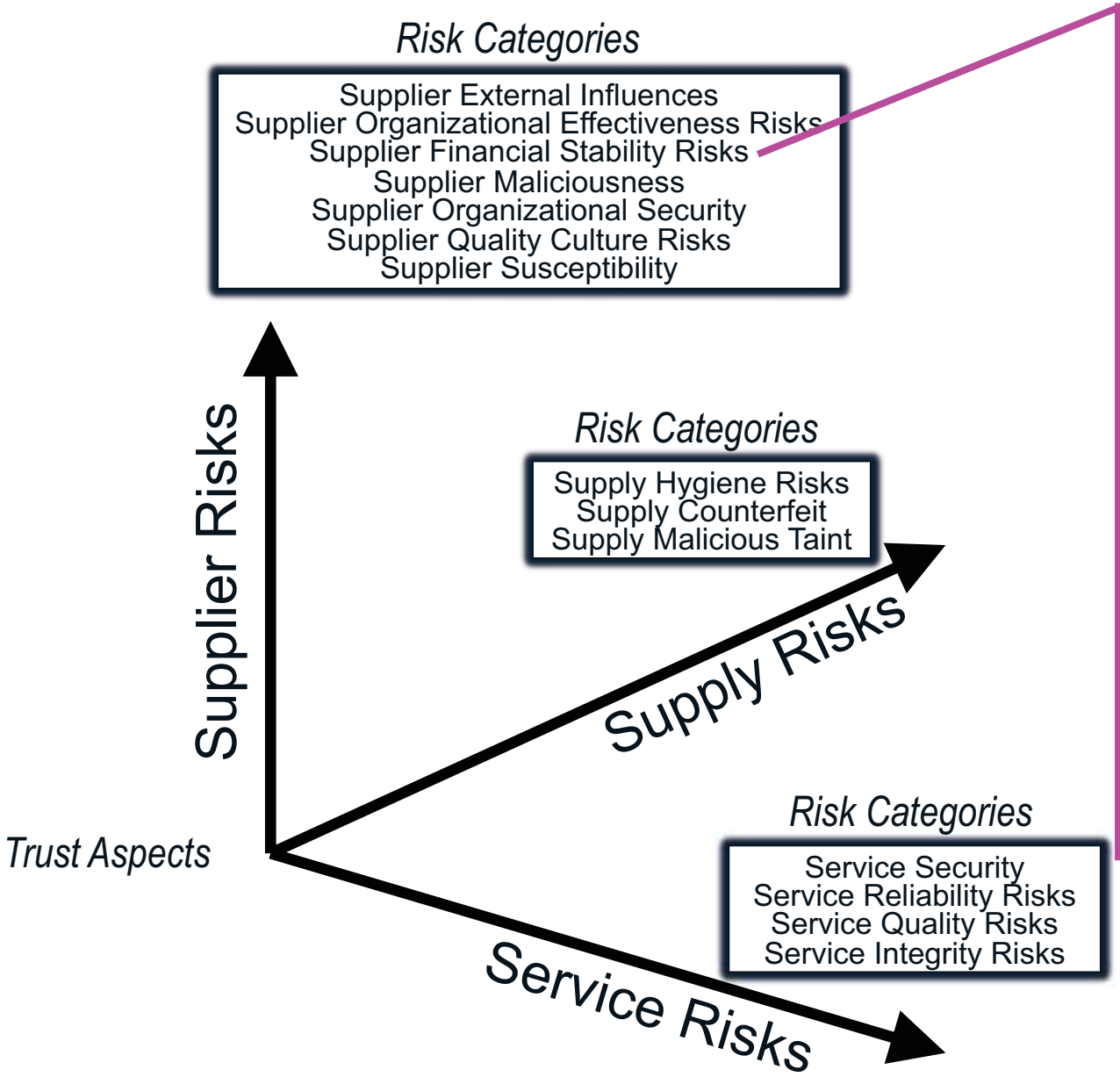
- **Ownership and Control Risks**
- **Foreign Business Relationship Risks**
- **Adverse Corporate Influences**

Basis of Trust



- **Environmental, Social, & Governance Risk**
- **Geographical / Geopolitical Instability**
- **Structural & Operational Instability**

Basis of Trust



- **Short-term Financial Health Risks**
  - Organization has concerning level of liquidity and cash flow
  - Organization has concerning ability to pay its debts based on level of debt, assets and equity
  - Gross profit margin is of concern
  - Organization is not showing a profit
- **Financial Stewardship Risks**
  - Organization has history of bankruptcy or liens
  - Organization has history of being target of lawsuits
  - Organization has history of explicit findings/ratings of financial instability due to stewardship issue
  - Organization has history of late payments
  - Organization has history of SEC (or foreign counterpart) investigations
  - Organization lack of currency in public filings
- **Long-term Financial Health Risks**
  - Company has concerning R&D investment level
  - Organization has concerning inventory turnover rate
- **Foreign Financial Obligations**
  - …

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

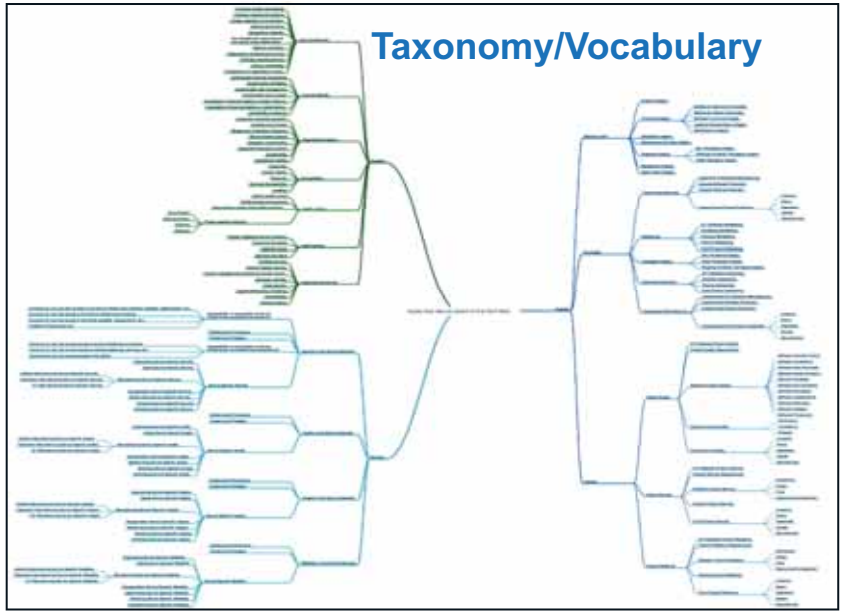
Supply Chain Risks														
Supplier Risks							Supply Risks			Service Risks			
Supplier External Influences	Supplier Financial Stability Risks	Supplier Organizational Effectiveness Risks	Supplier Susceptibility	Supplier Quality Culture Risks	Supplier Maliciousness	Supplier Organizational Security Risks	Supply Hygiene Risks	Supply Malicious Taint	Supply Counterfeit	Service Integrity Risks	Service Quality Risks	Service Reliability Risks	Service Security
Ownership and Control Risks	Financial Stewardship Risks	Environmental, Social, & Governance Risks	Customer Related Risks	Internal SCRM Policy and Practices Risks	Foreign Intelligence Service or Foreign Military Influence	Security Training Deficiencies	Product Quality Risks	Facilities Integrity Risks	Packaging Integrity Risks	Service Infrastructure Pedigree Risks	Service Infrastructure Pedigree Risks	Service Infrastructure Pedigree Risks	Service Infrastructure Pedigree Risks
Foreign Business Relationship Risks	Short-term Financial Health Risks	Geographical/Geopolitical Instability	Industry Related Risks	Internal Quality Control Risks	Avoidance of Sales Restrictions	Control Compliance & Vulnerability Management	Product Resilience Risks	Functional Integrity Risks	Technical Authenticity Risks	Service Infrastructure Provenance Risks	Service Infrastructure Provenance Risks	Service Infrastructure Provenance Risks	Service Infrastructure Provenance Risks
Adverse Corporate Influence	Long-term Financial Health Risks	Structural & Operational Instability	Susceptible Location	Subcontractor Supply Chain Security Risks	Legal / Law Issues	Cyber Threat Activity	Product Security Risks	Geopolitical Integrity Risks	Mislabeling	Service Specific Integrity Risks	Service Specific Quality Risks	Service Specific Reliability Risks	Service Specific Security Risks
	Adverse Market Factors		Susceptible Personnel			Security Operations		Logistics / Transportation Integrity Risks	Unsanctioned Manufacturing				Physical Access to Service Infrastructure
	Foreign Financial Obligations		Technical Susceptibility			Insufficient Security Operations		Maintenance Integrity Risks	Copycat Manufacturing				Remote / Virtual Access to Service Infrastructure
								Manufacturing Process Integrity Risks					
								Packaging Integrity Risks					
								Poor Reputation for Integrity					
								Supply Chain Management Integrity Risks					

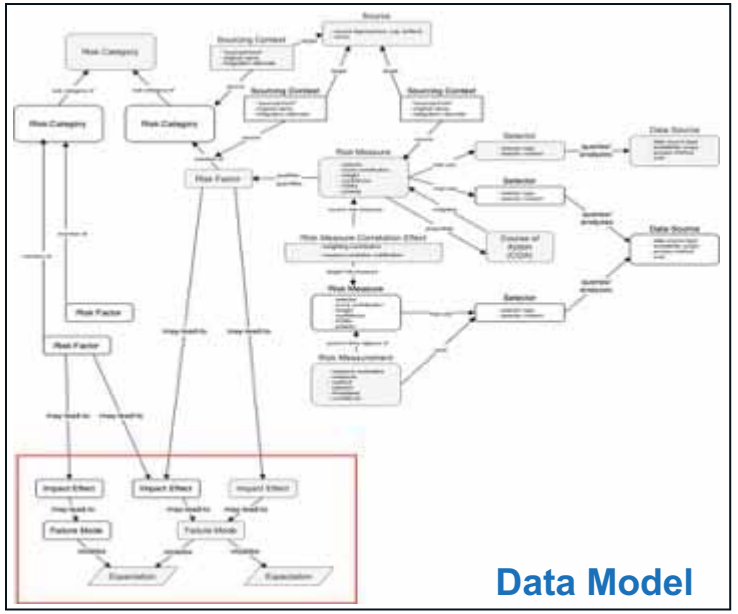
MITRE | System of Trust™

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

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

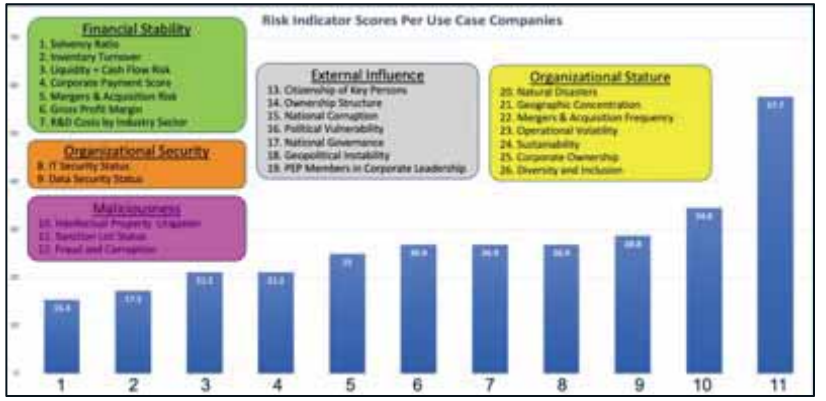
Taxonomy/Vocabulary



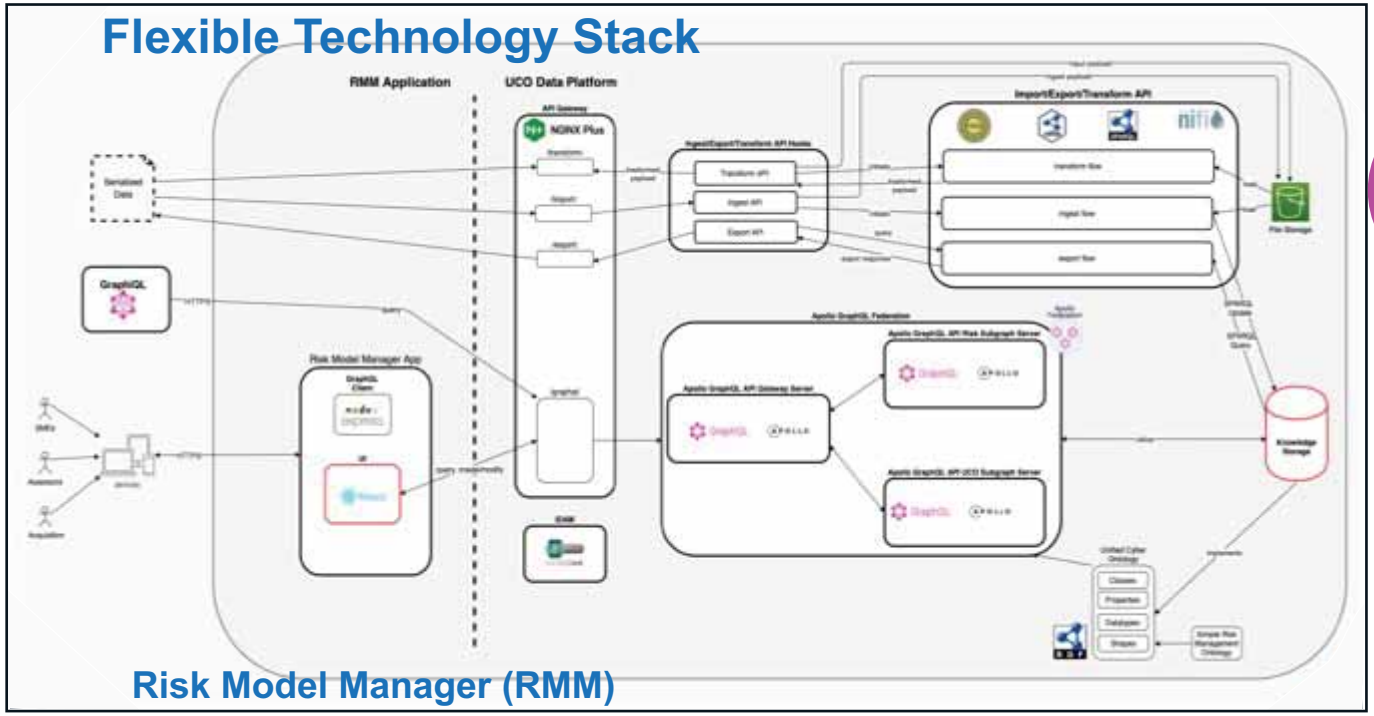


Data Model

Analytic Methods



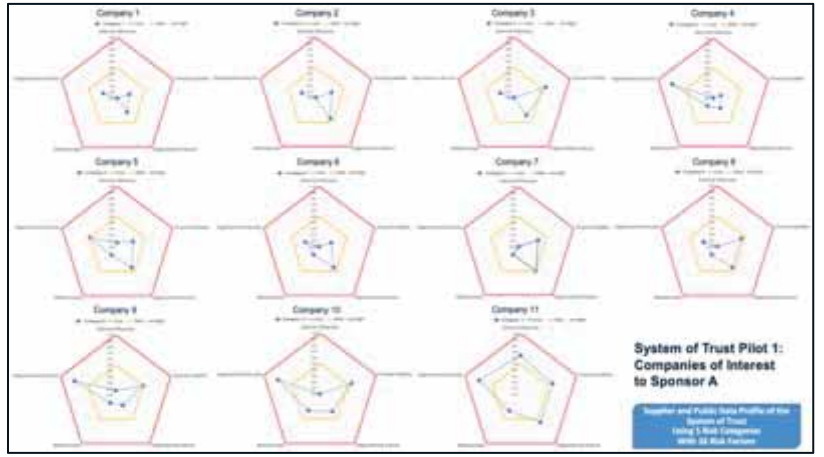
Flexible Technology Stack



Risk Model Manager (RMM)

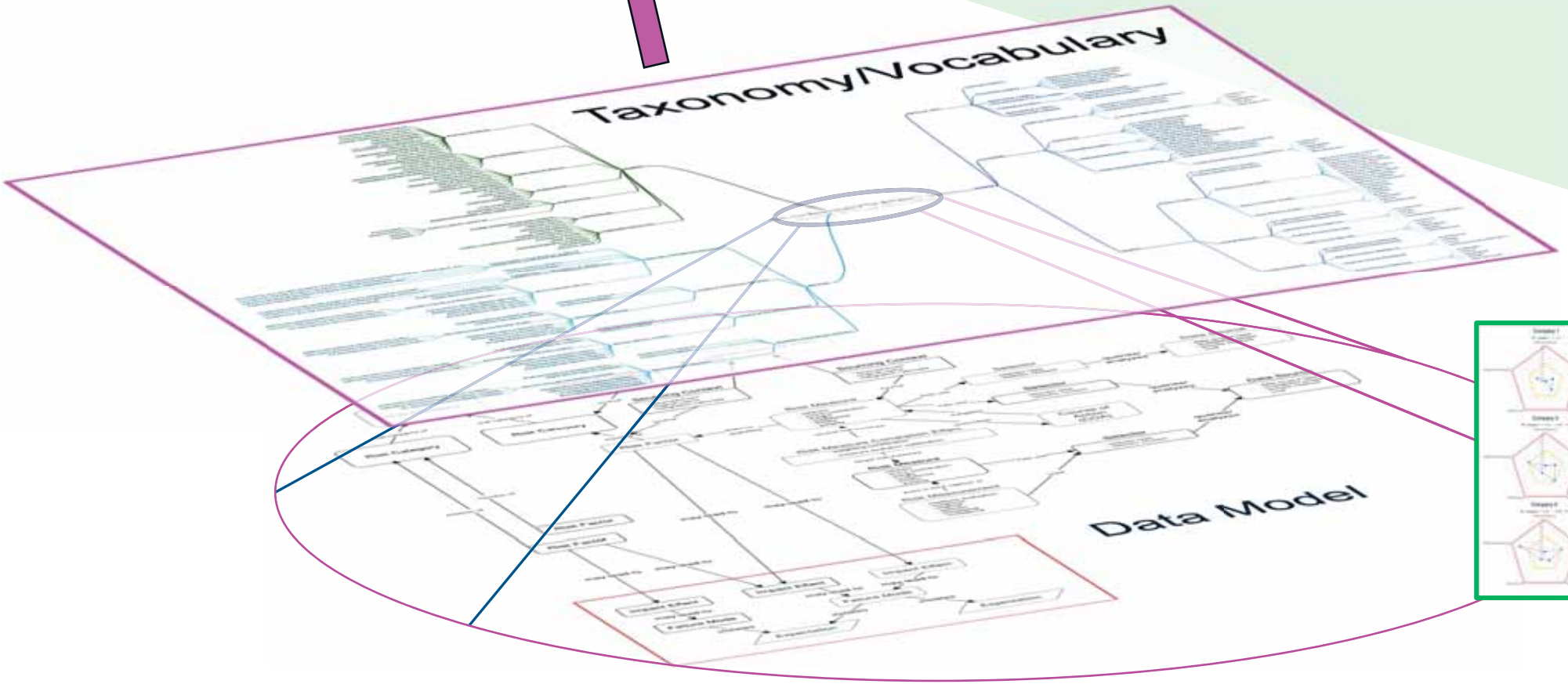
Piloting
11, 3, 1, 6, 22, 12, …

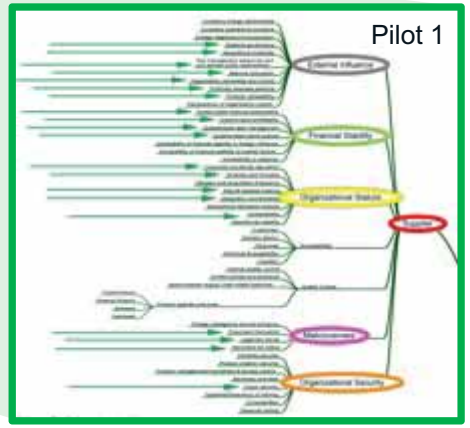
Export to Spreadsheet for "Offline" Assessment

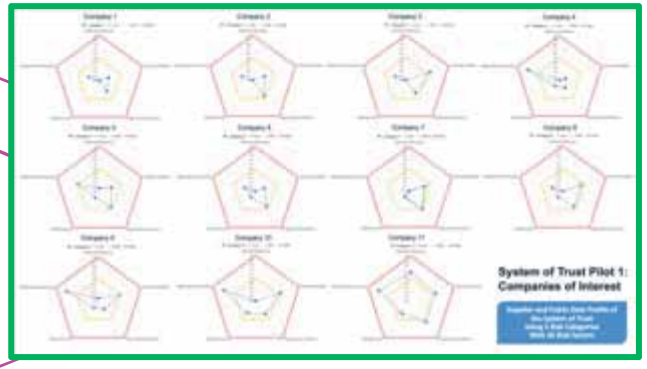


MITRE

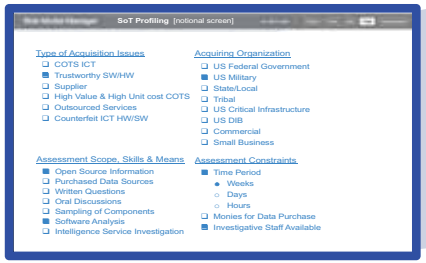
Tying together SoT and RMM

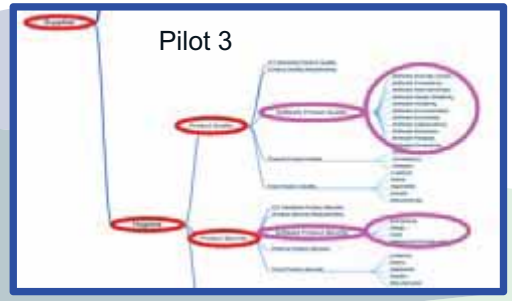


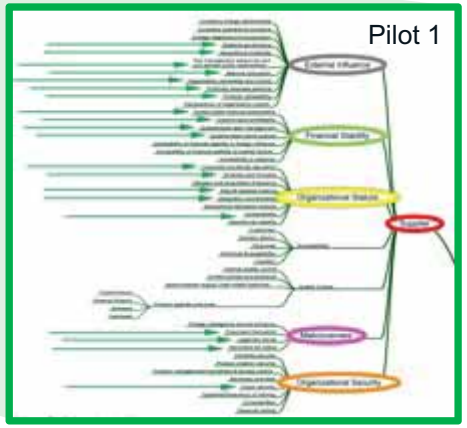


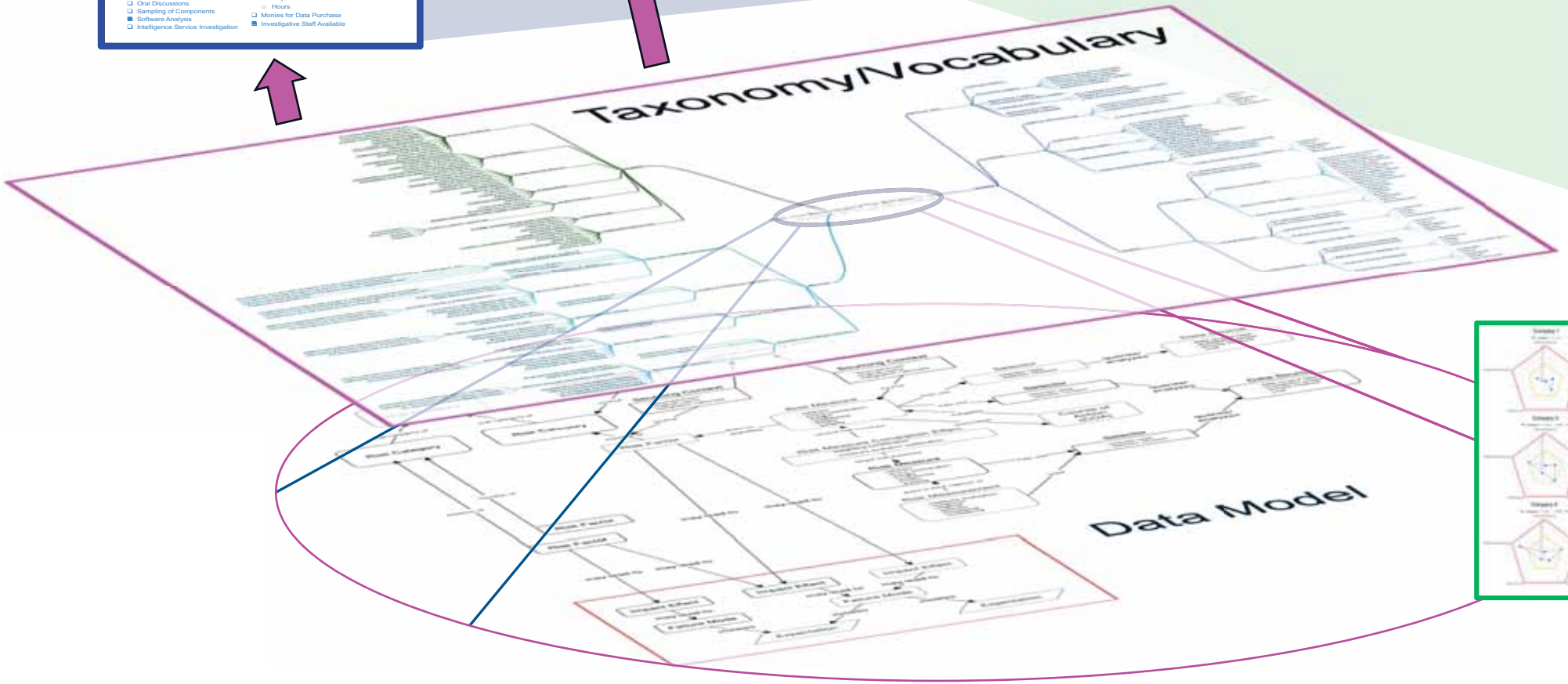


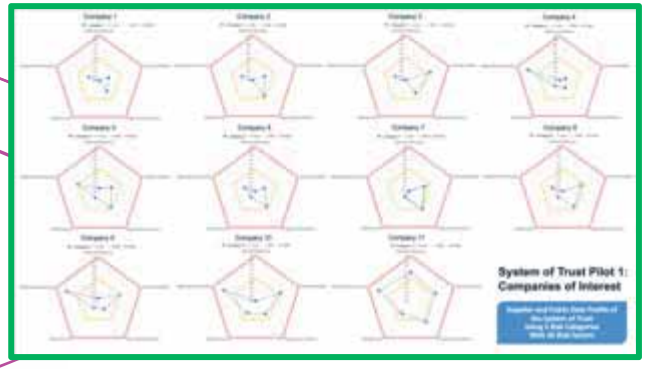
Tying together SoT and RMM



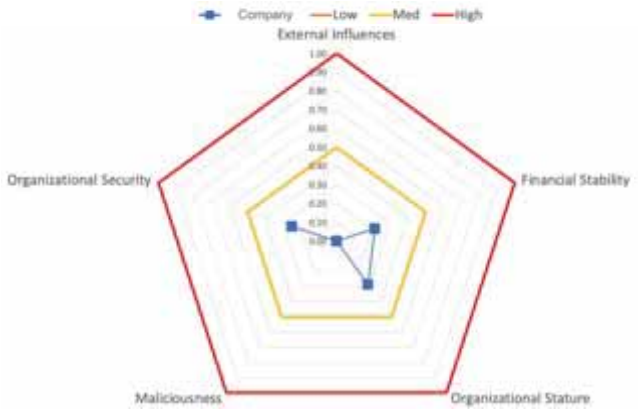




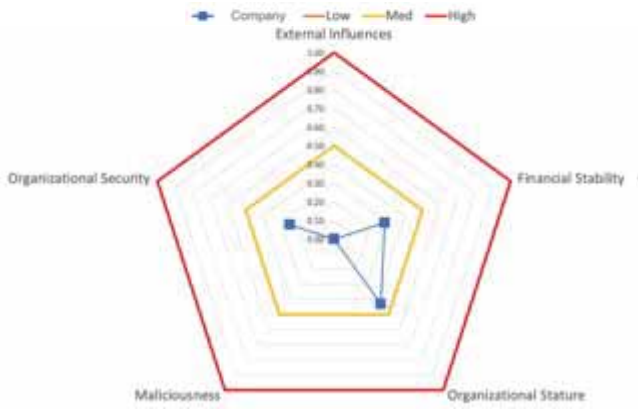




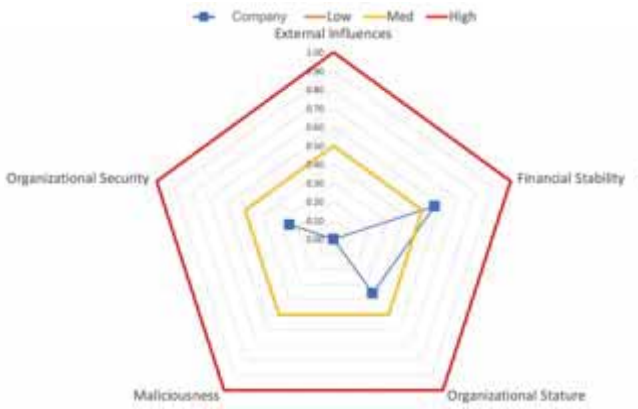
Company 1



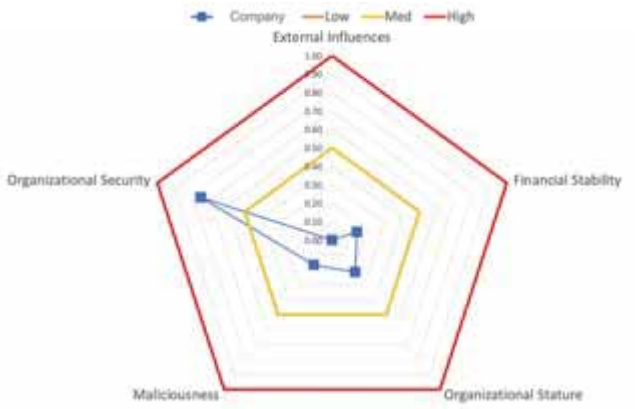
Company 2



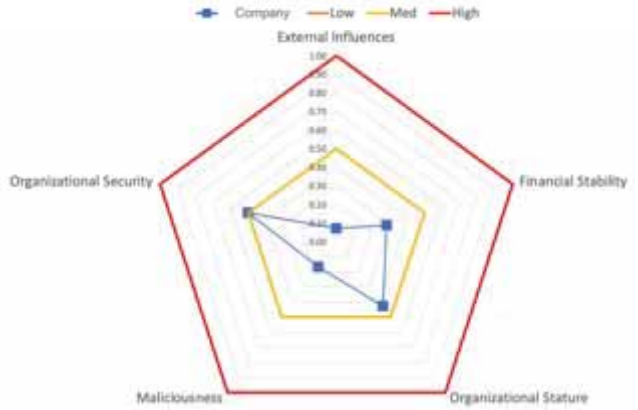
Company 3



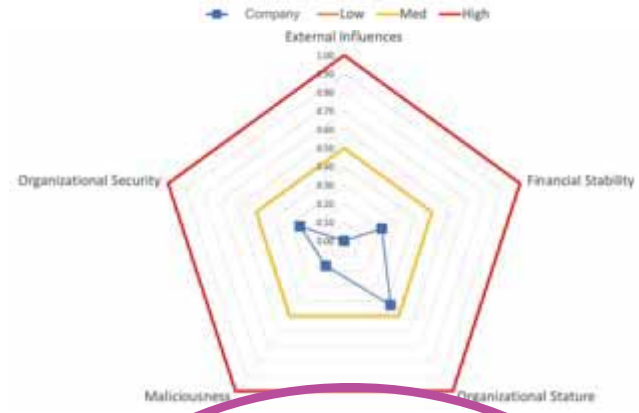
Company 4



Company 5

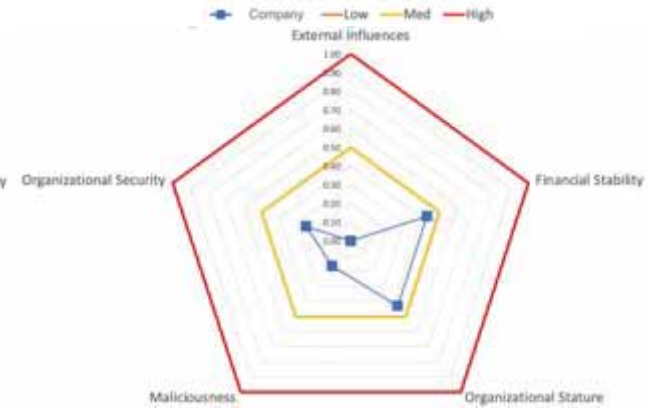


Company 6

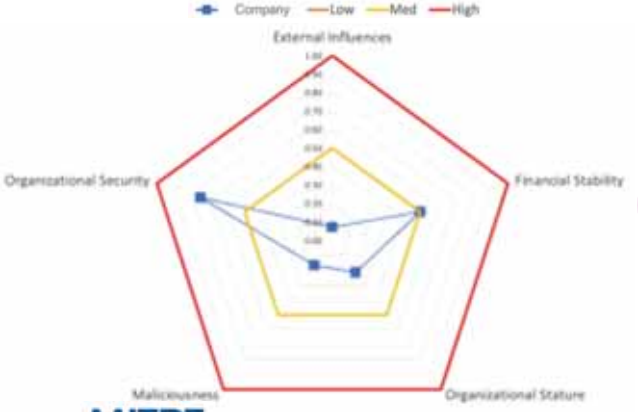


Company 7

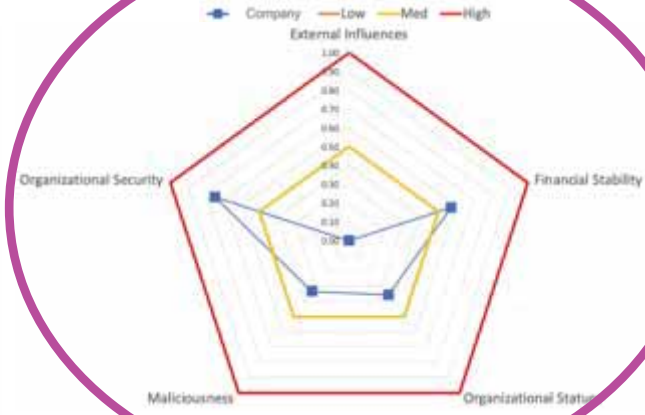
Company 8



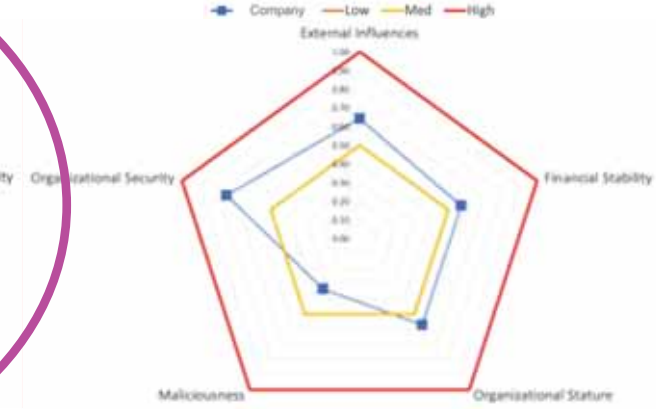
Company 9



Company 10



Company 11

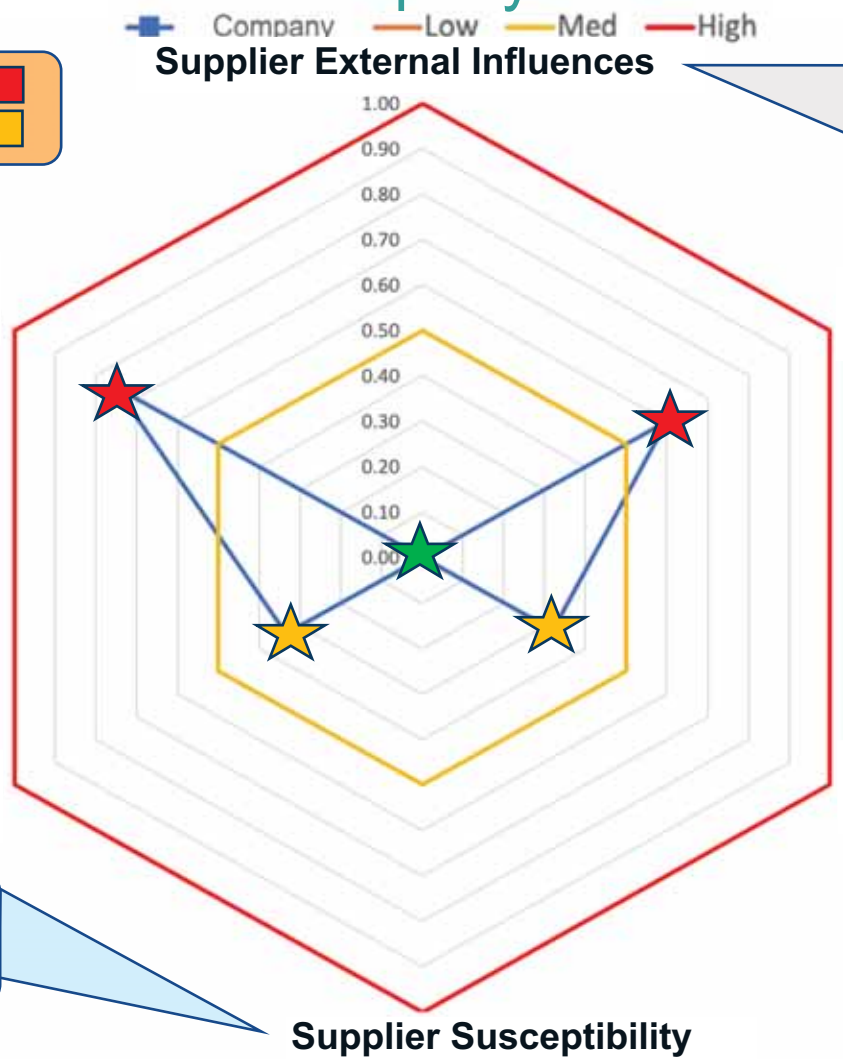


System of Trust Pilot 1: Companies of Interest

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

MITRE

Company 10



Supplier External Influences

13. Degree of foreign ownership
14. National Corruption
15. Political Vulnerability
16. National Governance Risks
17. Geopolitical Instability
18. PEP Members in Corporate Leadership

Supplier Organizational Security Risks

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

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

Supplier Ethics Risks

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

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

Supplier Susceptibility

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

Supplier and Public Data Profile

Using 6 Risk Categories With 25 Risk Factors

MITRE

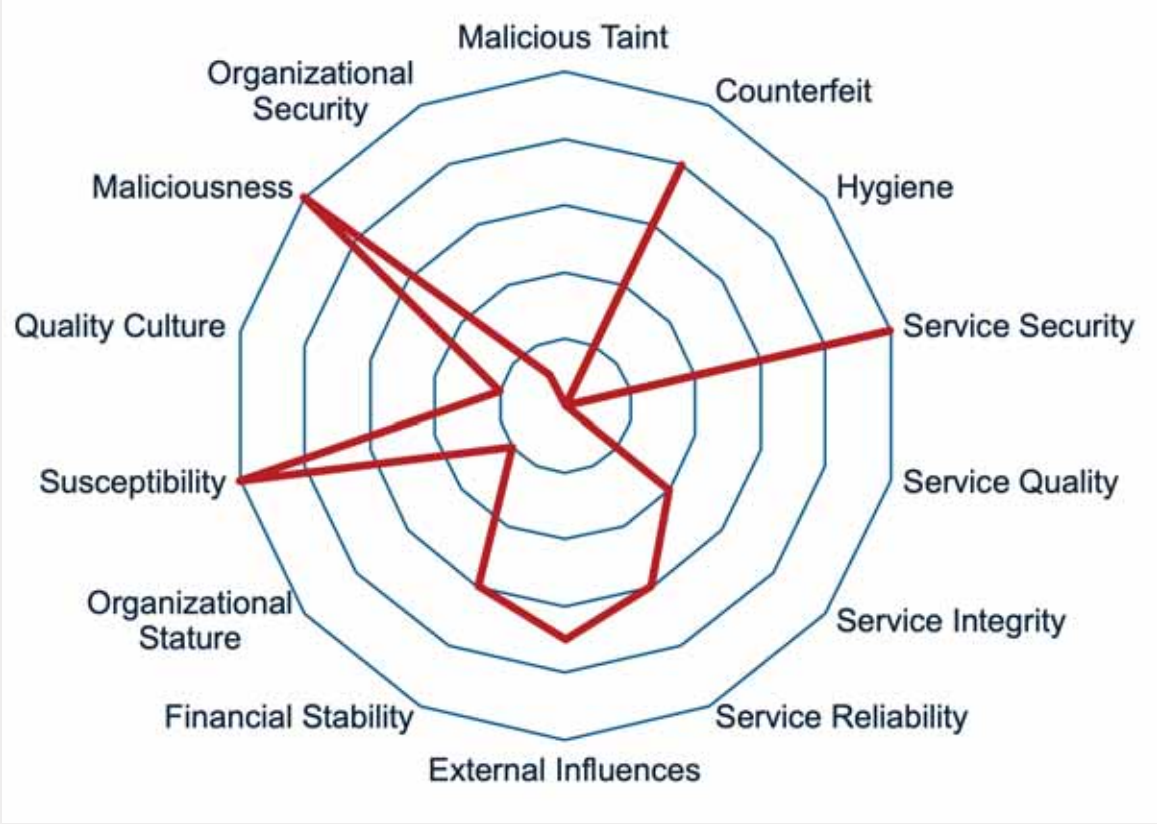
GOAL for use of SoT in Industry and Government…

Risk Model Manager

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

Top-Level Concerns Vendor/Product A

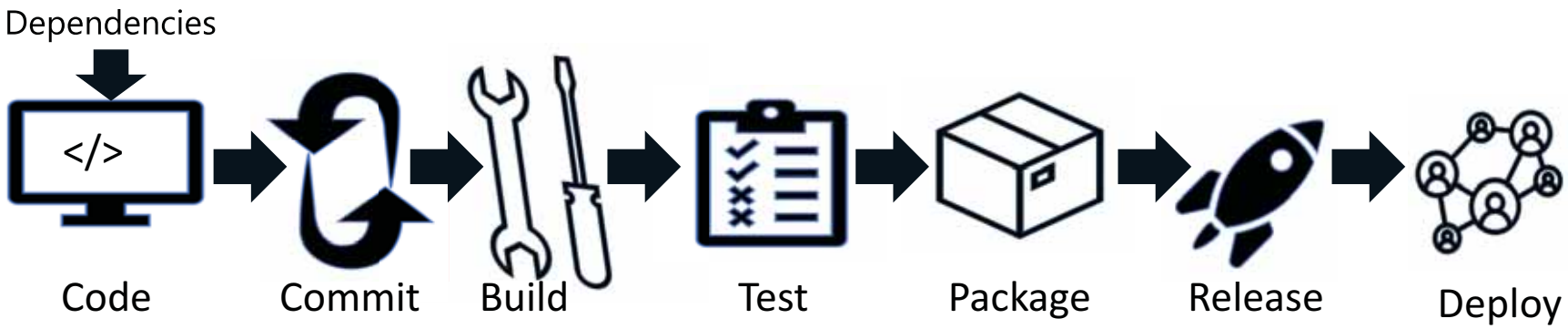
Top-Level Concerns Vendor/Product B



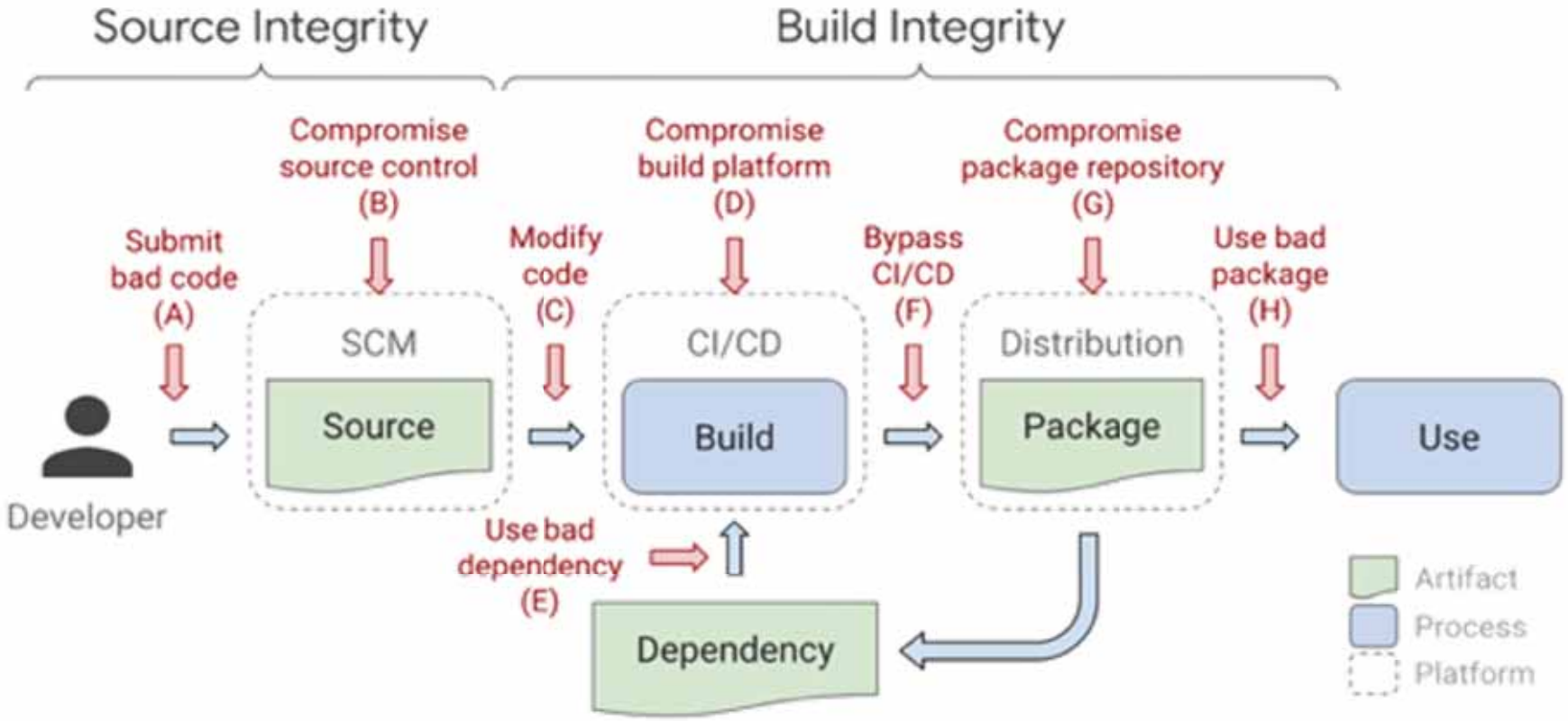
MITRE

Supply Chains

Software Supply Chain



Supply-chain Levels for Software Artifacts (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				O
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service Generated		✓	✓	✓
Provenance - Non-Falsifiable			✓	✓
Provenance - Dependencies Complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

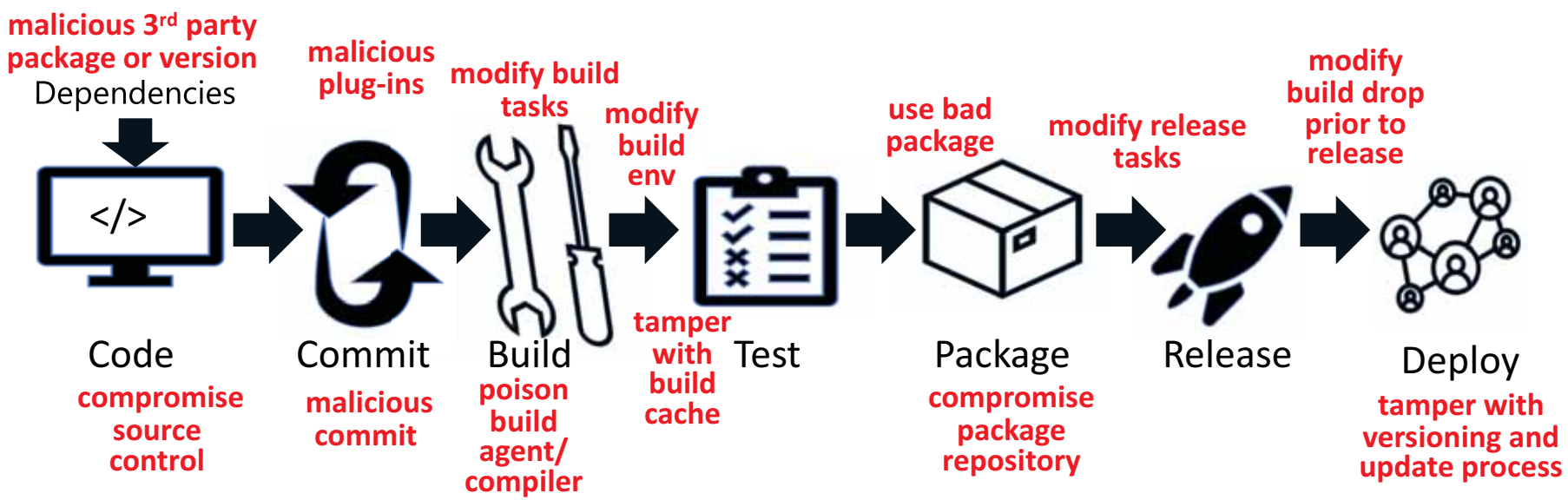
O = required unless there is a justification

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

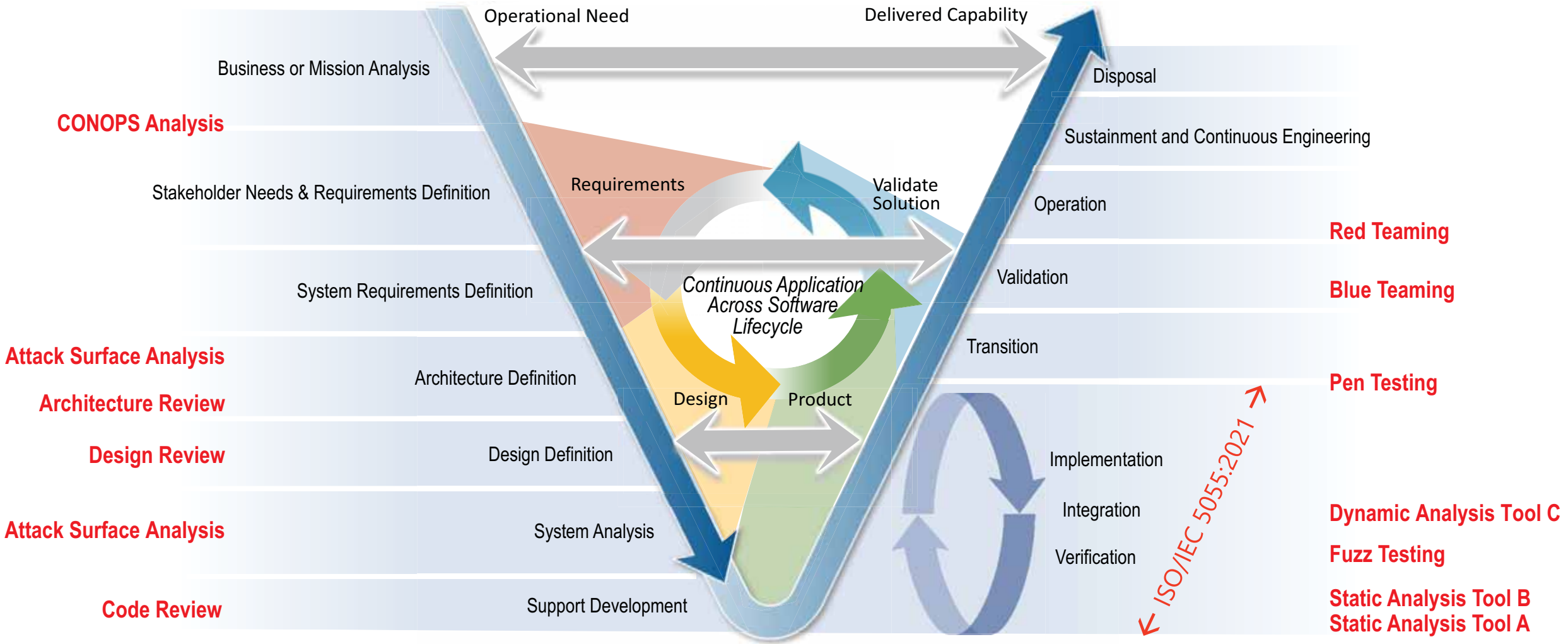
Supply Chains

Software Supply Chain



Hazards and Threats

Software Development and Assurance Lifecycle Phases

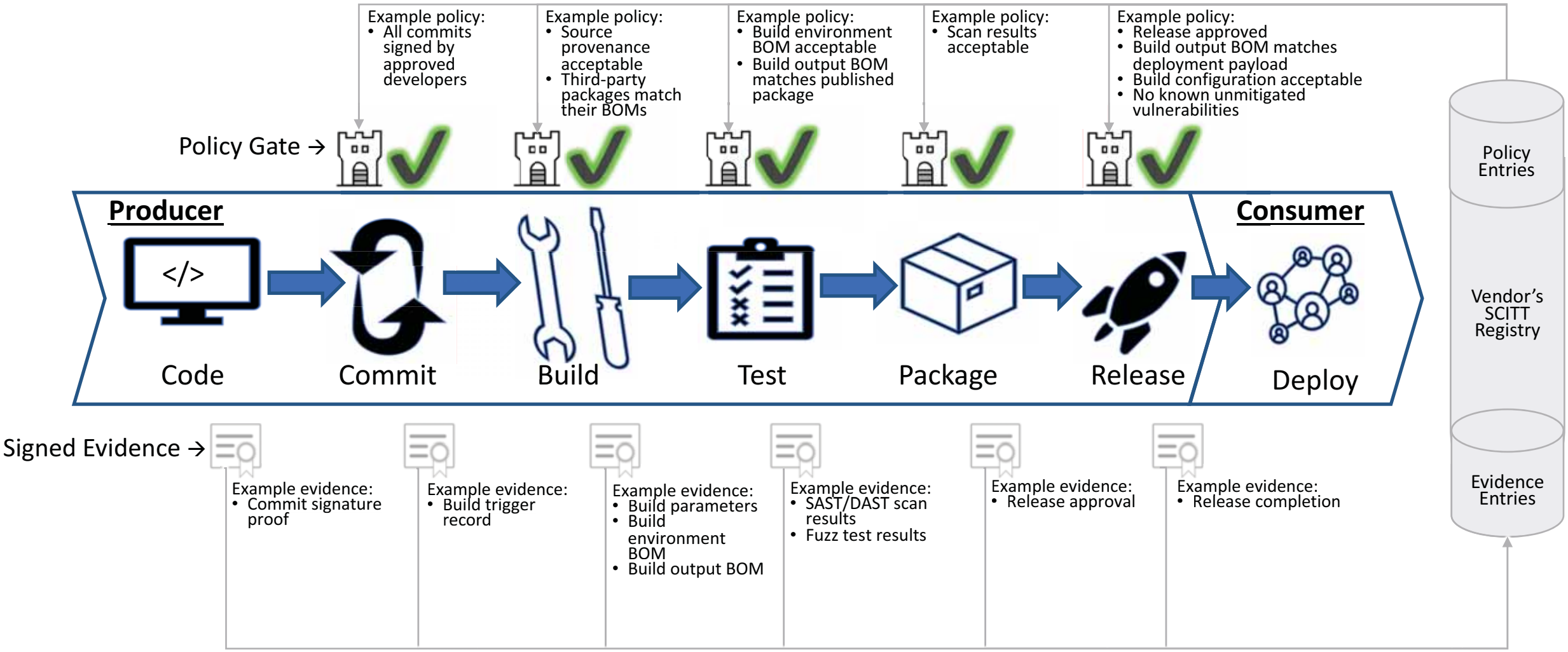


NOTE: *Lifecycle processes typically occur simultaneously, **not** in sequence; see ISO/IEC 15288 & 12207*

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

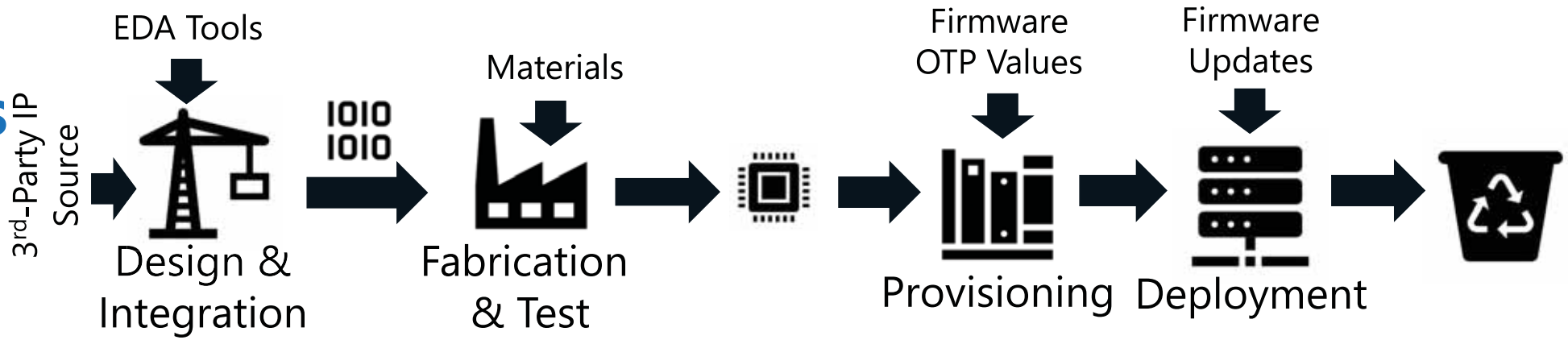
Deployment Example of SCITT in SW Development



MITRE

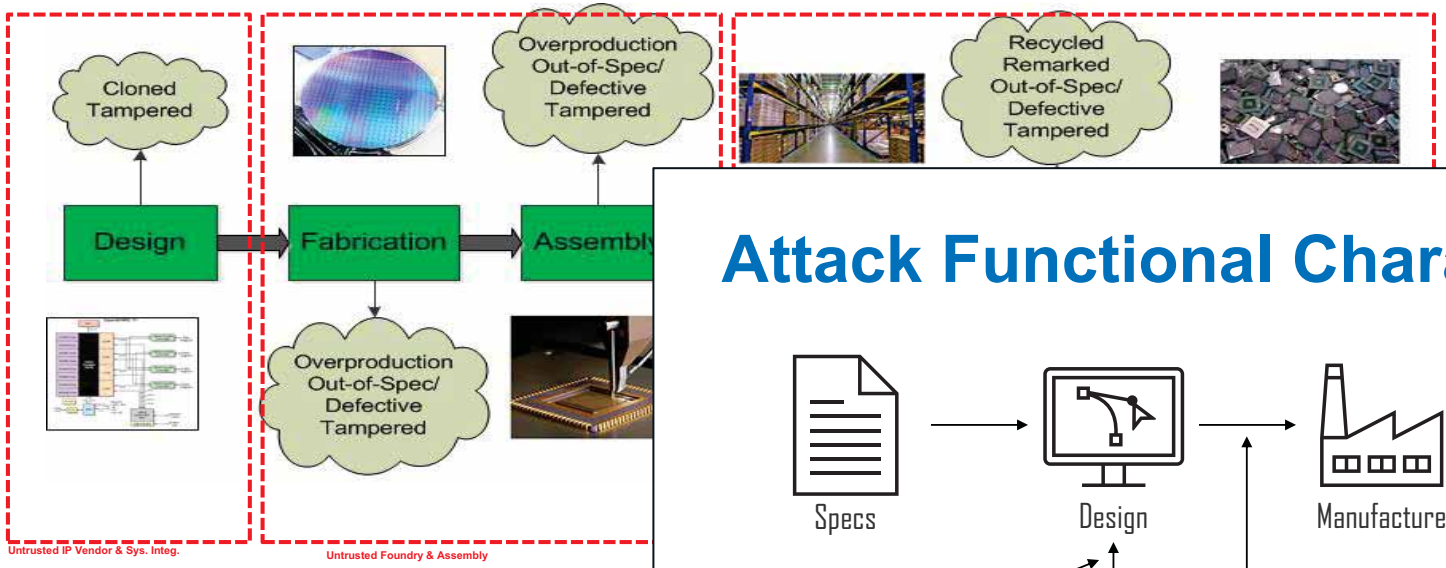
Supply Chains

Micro-electronics Supply Chain



CENTER FOR HARDWARE AND EMBEDDED SYSTEMS SECURITY AND TRUST

Electronics Supply Chain

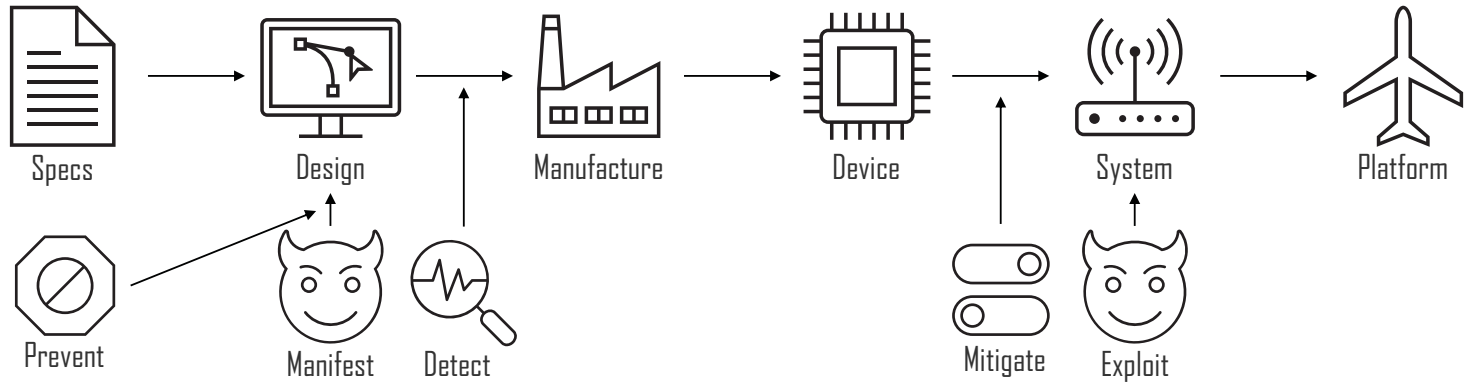


Maximum Flexibility

UCONN

5

Attack Functional Characterization



- How can an attack be decomposed into its functional ingredients?
- These ingredients may be how a countermeasure prevents/detects/mitigates the attack.
- Ingredients may be easier to simulate and generate data for

4

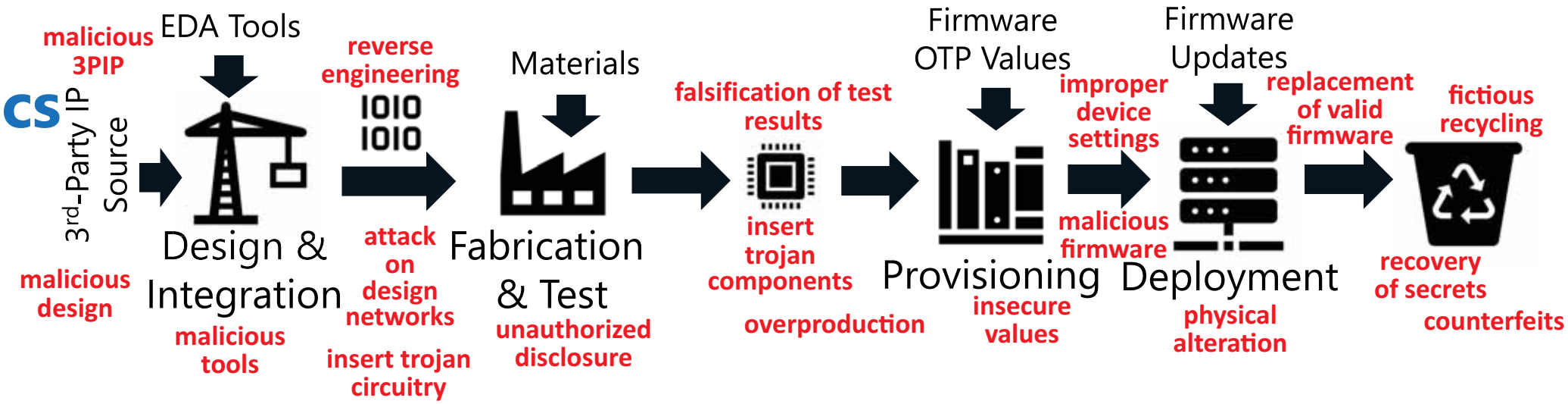
Battelle Proprietary

BATTELLE

MITRE

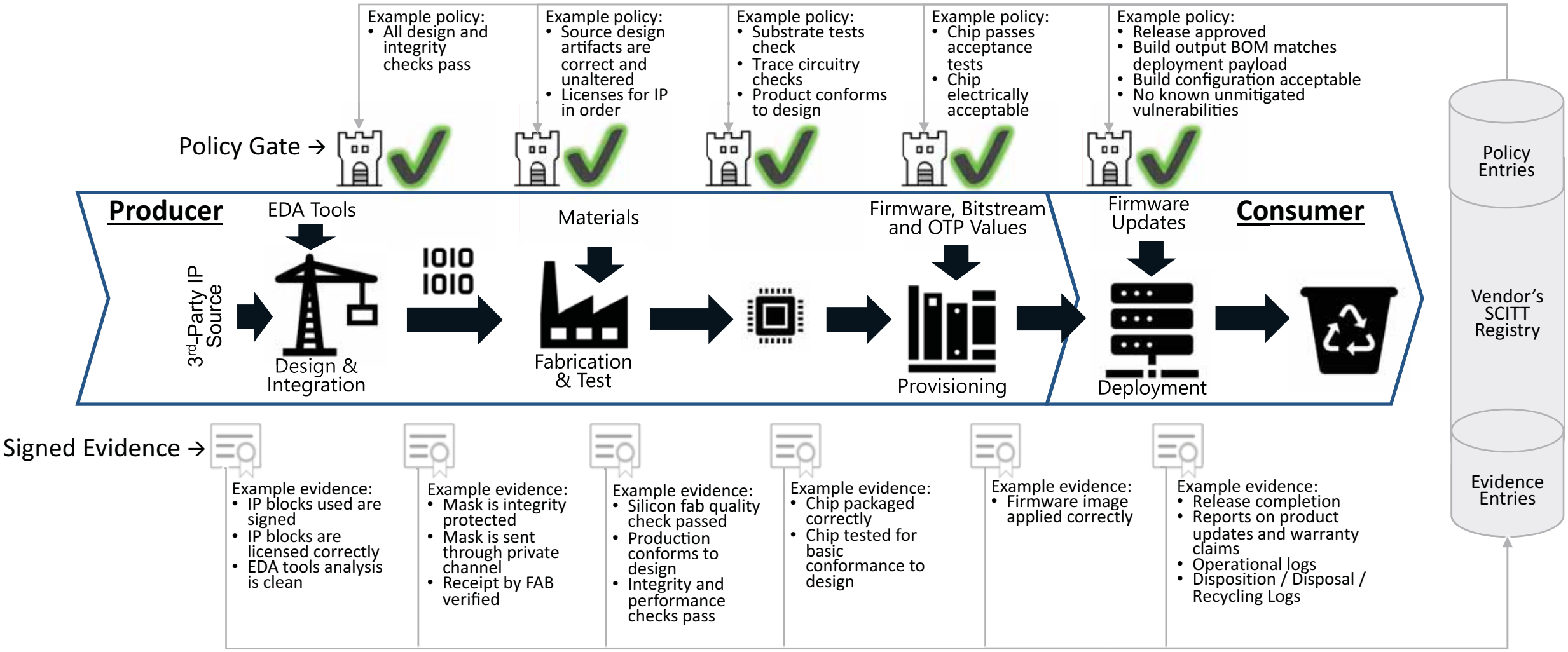
Supply Chains

Micro-electronics Supply Chain



Hazards and Threats

Deployment Example of SCITT in Chip Development

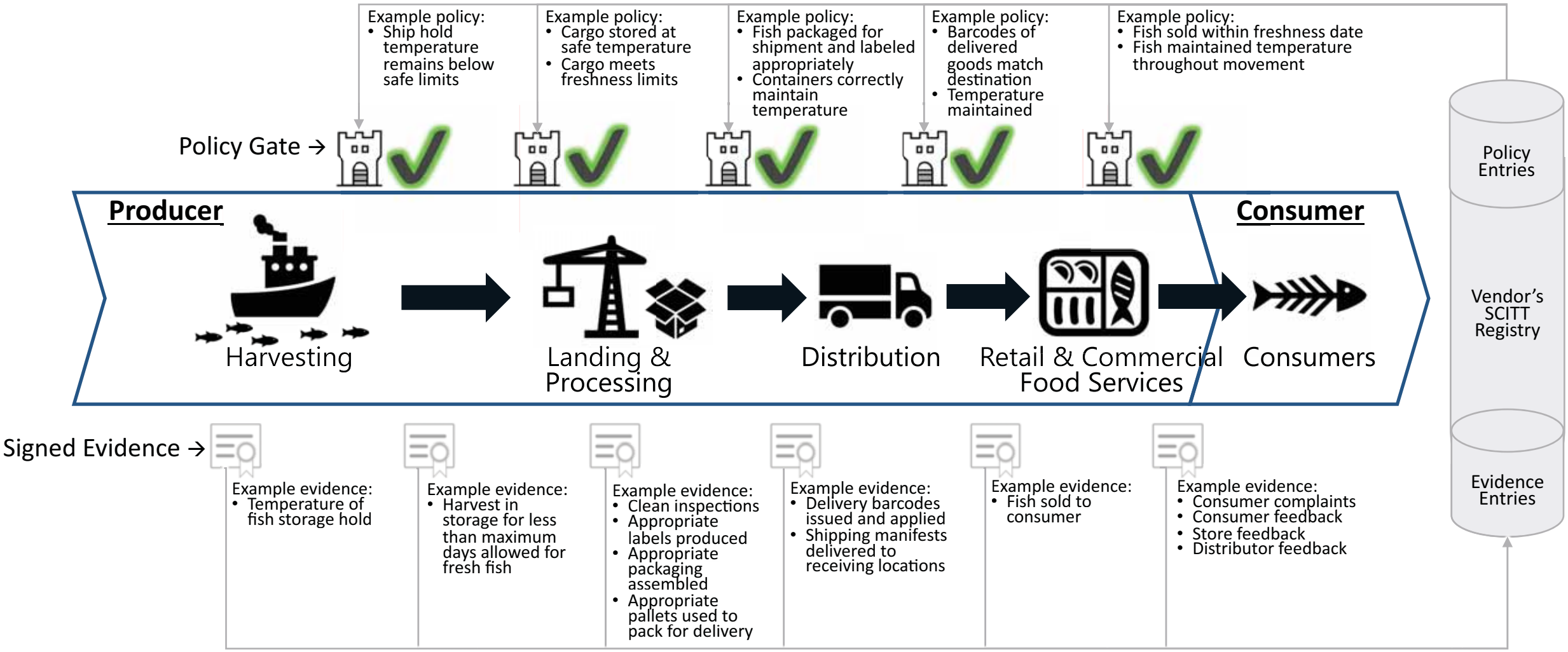


Supply Chains

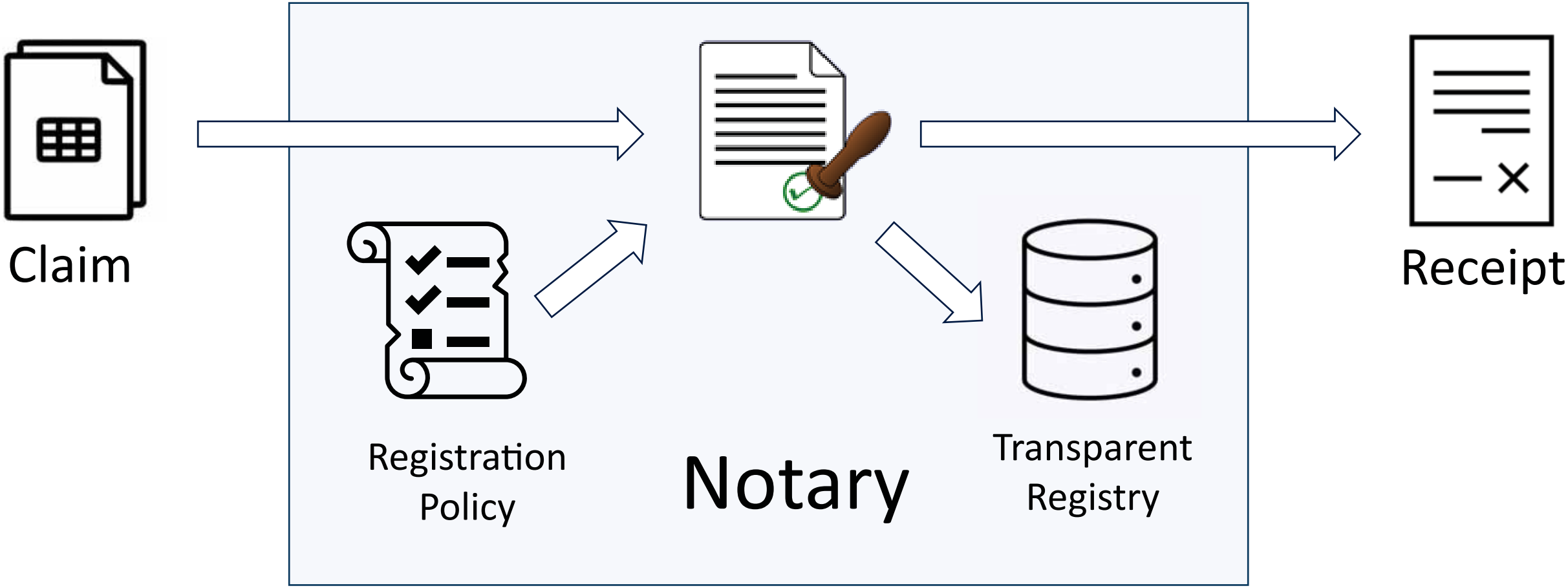
Seafood Supply Chain

Hazards and Threats

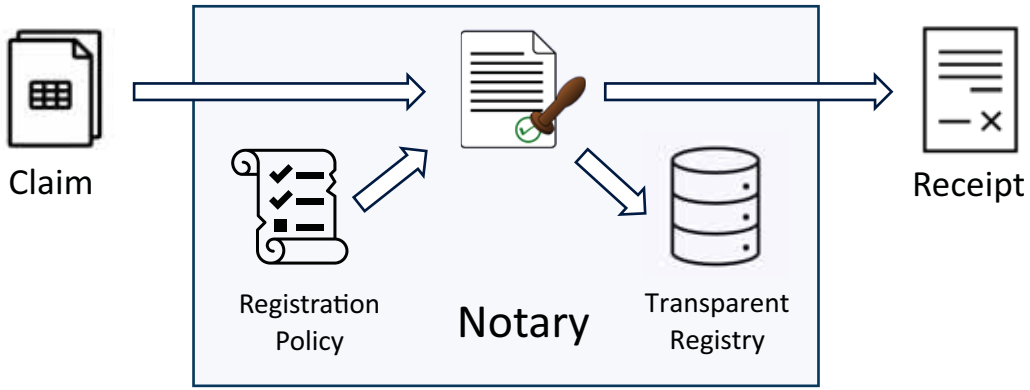
Deployment Example of SCITT in Harvesting Fish



SCITT Concepts



SCITT Definitions & Terms



Claim: Identifiable, non-repudiable statement about an **Artifact** made by an **Issuer.**

Registration Policy: Pre-condition for registering a claim.

This involves verifying the claim issuer, and may depend on other claim attributes and previously-registered claims.

Notary: **Transparency service** that receives claims; checks they pass its registration policy; registers them; and returns their receipts.

Registry: Verifiable data structure providing a consistent append-only log for all registered claims.

Transparency does not necessarily mean public access—the notary controls access.

Receipt: Offline, universally-verifiable proof that a claim is recorded in the registry.

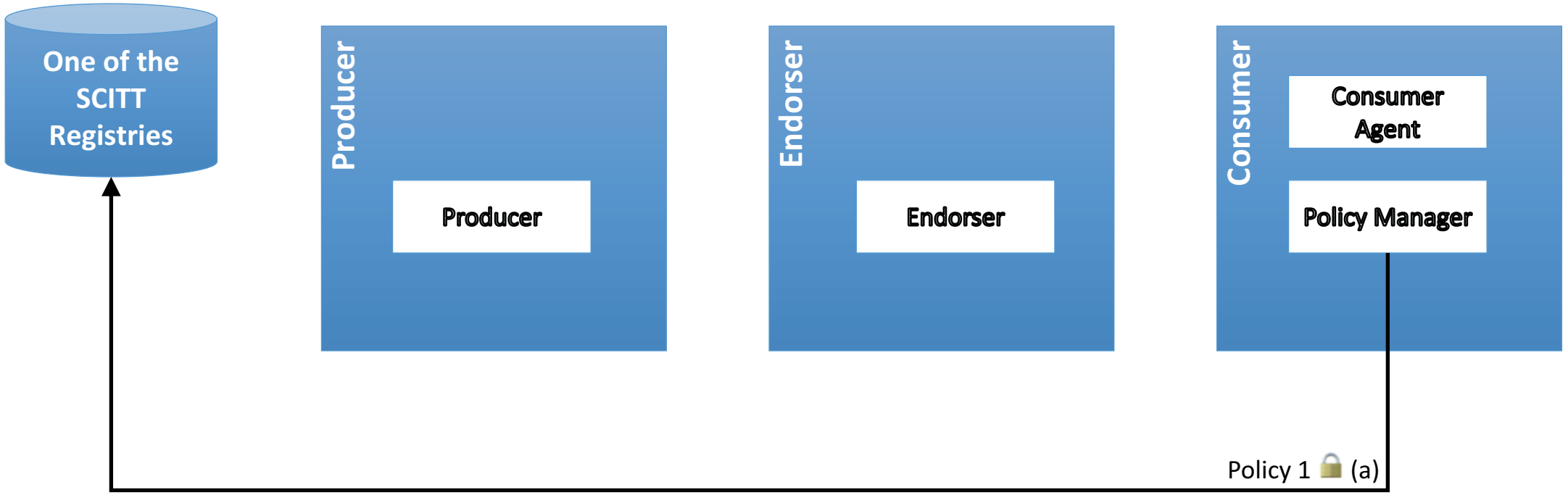
Claims and receipts do not expire, but newly registered claims may subsume older claims.

Verifier: Entity that receives claims + receipts and verifies them before using their contents

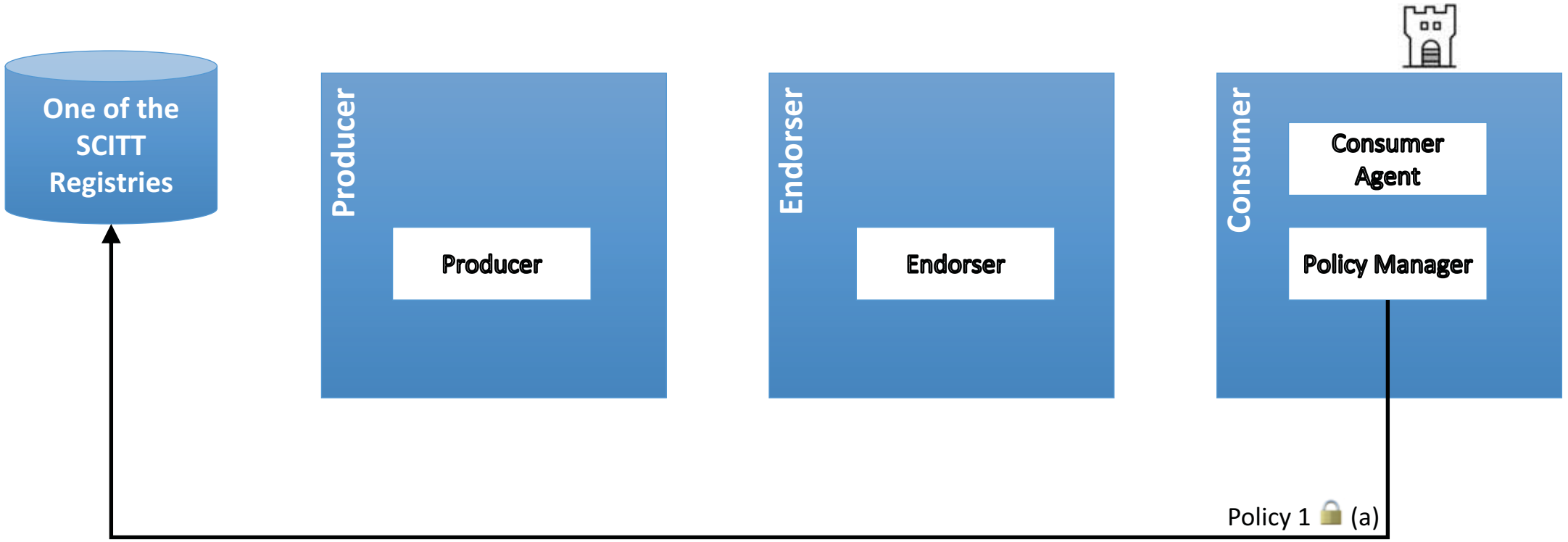
Auditor: Entity that checks the correctness and consistency if all claims in the registry.

https://ietf-scitt.github.io/draft-birkholz-scitt-architecture/draft-birkholz-scitt-architecture.html#name-definition-of-transparency

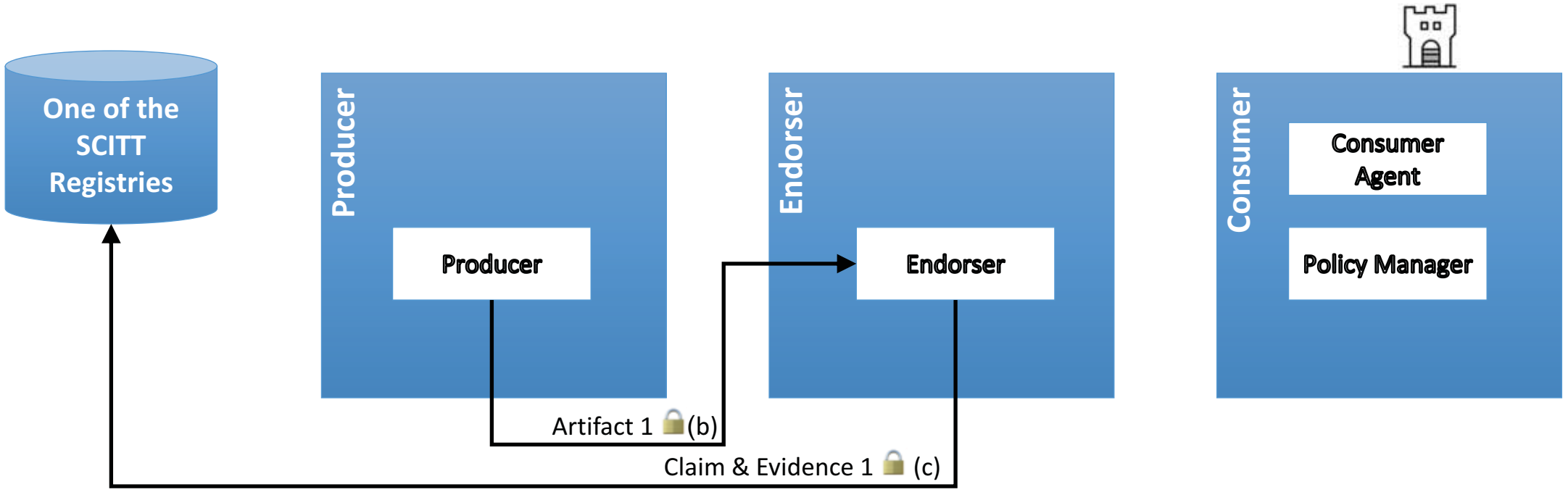
Deployment Example of SCITT in the Marketplace



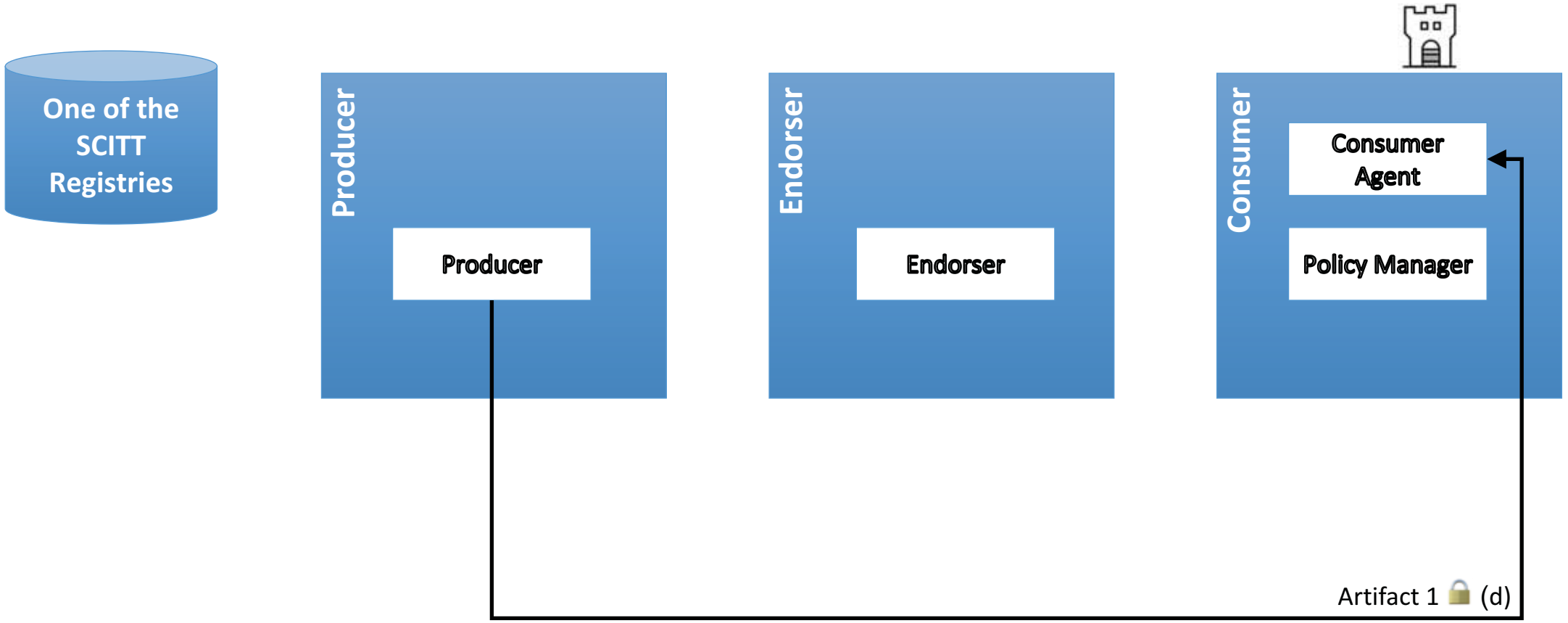
Deployment Example of SCITT in the Marketplace



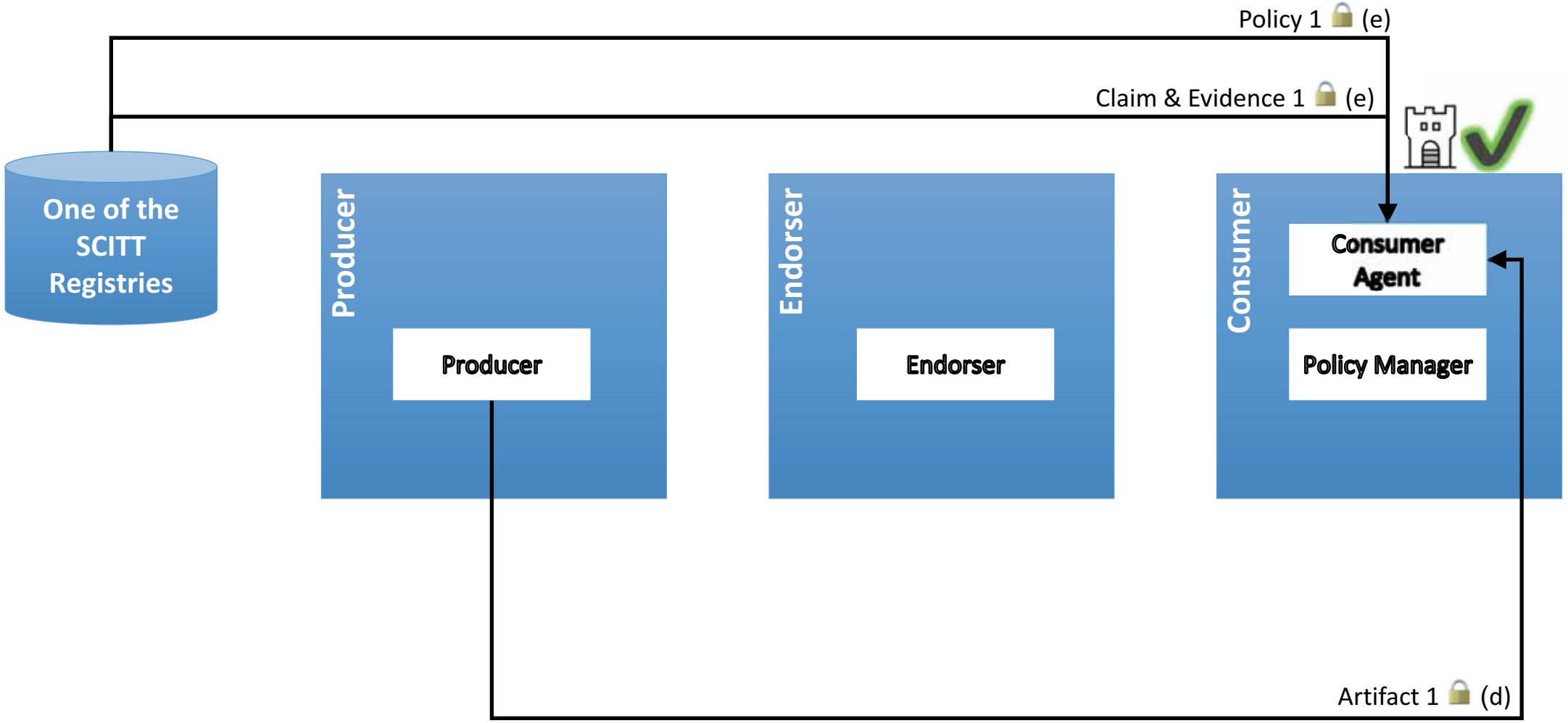
Deployment Example of SCITT in the Marketplace



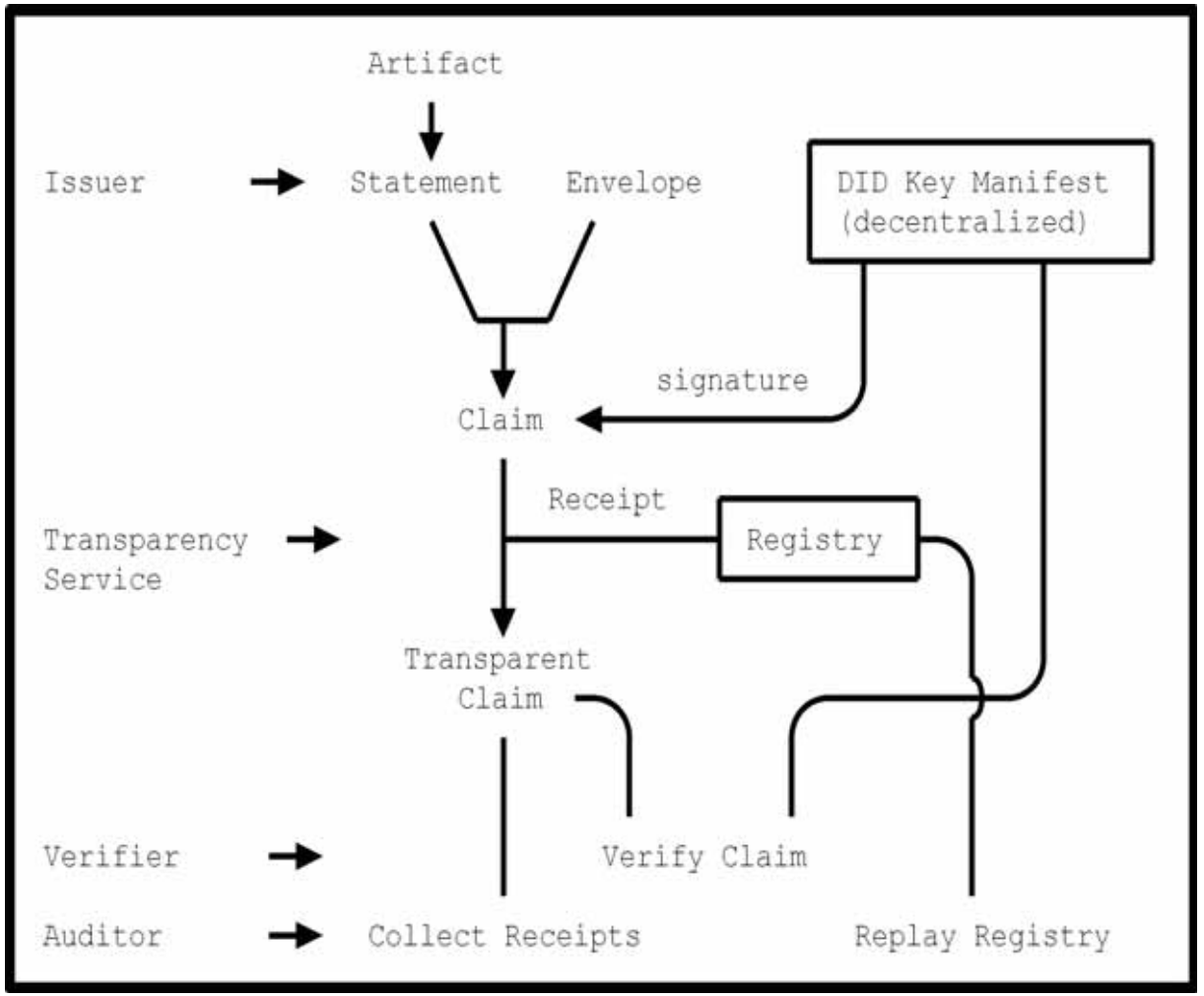
Deployment Example of SCITT in the Marketplace



Deployment Example of SCITT in the Marketplace



SCITT Architecture Model

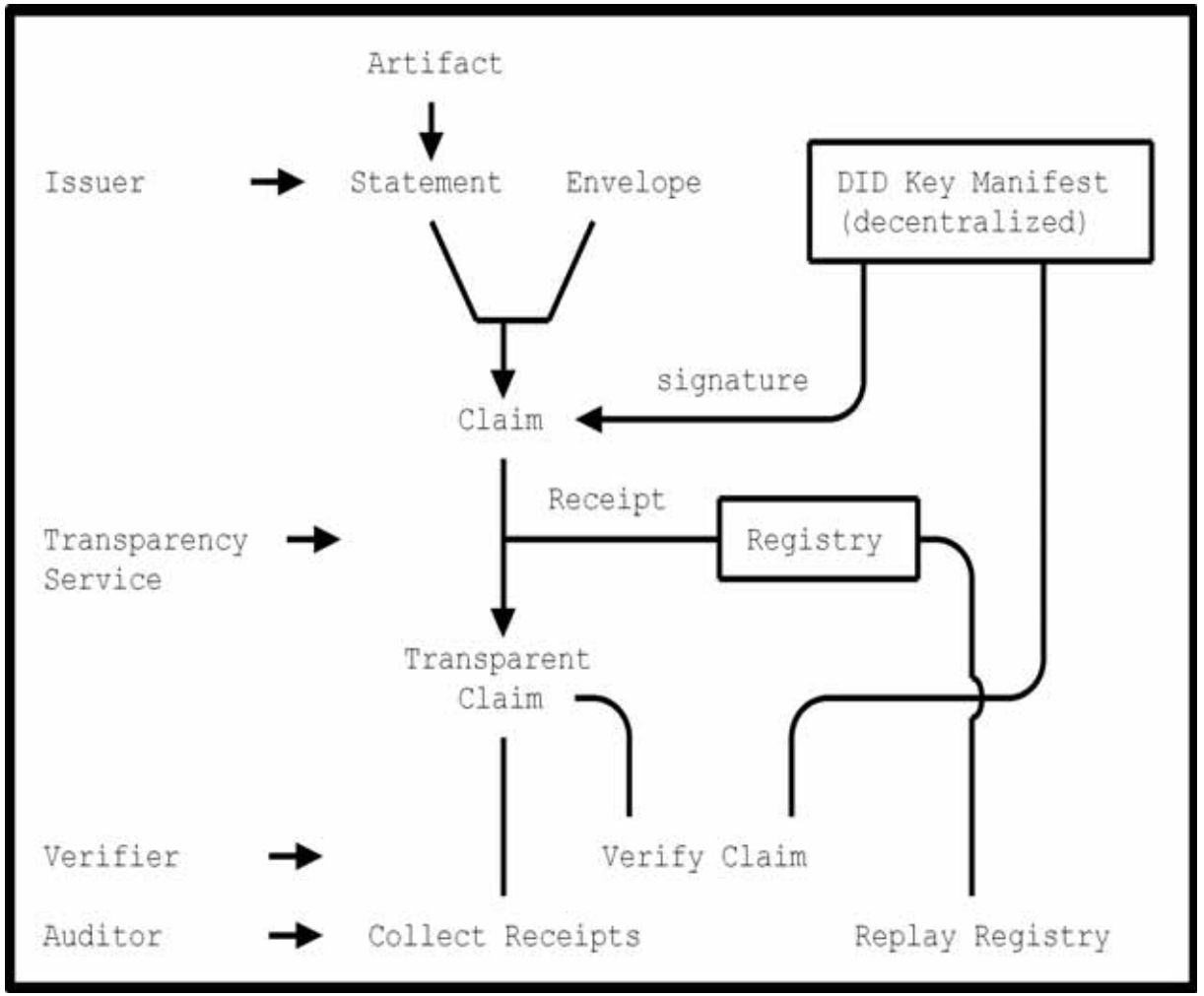


SCITT Standard Components

Issuer Identification (re-using DID)

Formats for Signed Claims (using CBOR and COSE)

Claim Endorsements



Registration Policies

Algorithms for Transparent Registry (Merkle trees)

Formats for Receipts

Auditing

Goal of SCITT is to simplify and standardize these interactions

SCITT Roadmap

Industry Standards

- Internet Engineering Task Force (IETF) Working Group
  - SCITT Charter https://datatracker.ietf.org/wg/scitt/about/
- Current tasks: gathering use cases and working draft documents
  - IETF-SCITT GitHub Repository https://github.com/ietf-scitt/
  - IETF-SCITT Use Cases https://github.com/ietf-scitt/use-cases/
  - SCITT architecture draft:
    - An Architecture for Trustworthy and Transparent Digital Supply Chains
  - SCITT countersigning draft:
    - Countersigning COSE Envelopes in Transparency Services
  - IETF-SCITT Mailing List https://www.ietf.org/mailman/listinfo/scitt

- IETF 116 (Yokohama) SCITT Session is planned for Thursday 30 March from 9:30-11:30am

MITRE

Software related policy

EO 14028 part 4

THE WHITE HOUSE

MAY 12, 2021

Executive Order on Improving t
Nation's Cybersecurity

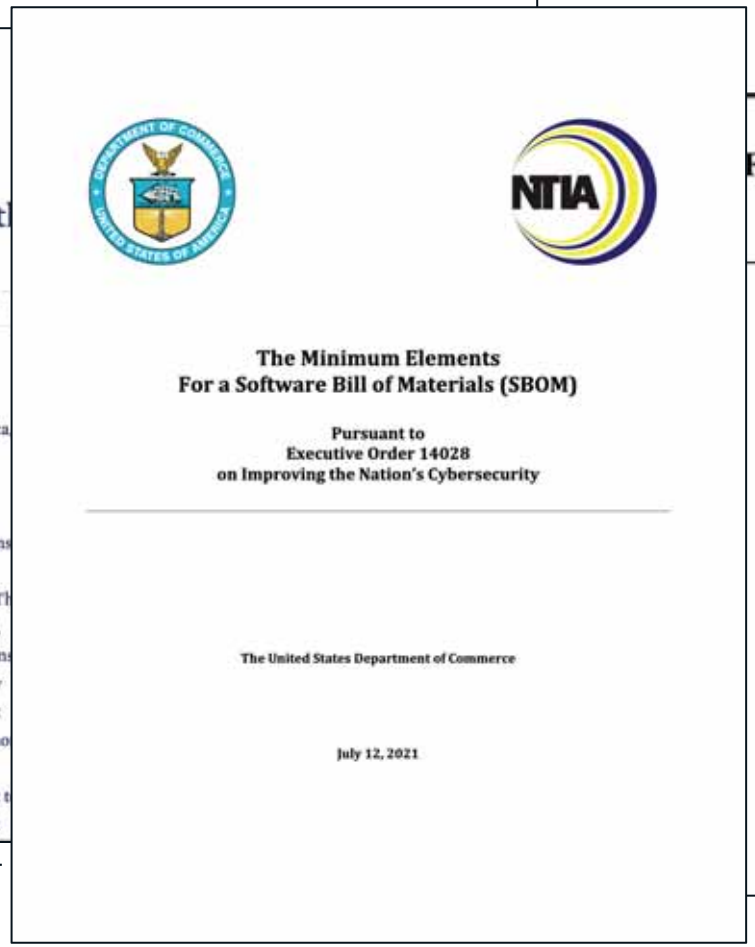
BRIEFING ROOM • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. Th Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires mo than government action. Protecting our Nation from malicious cyber actors requires the Federal Government t partner with the private sector. The private sector must

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

DoC / NTIA Minimal Elements of an SBOM



NTIA

The Minimum Elements
For a Software Bill of Materials (SBOM)

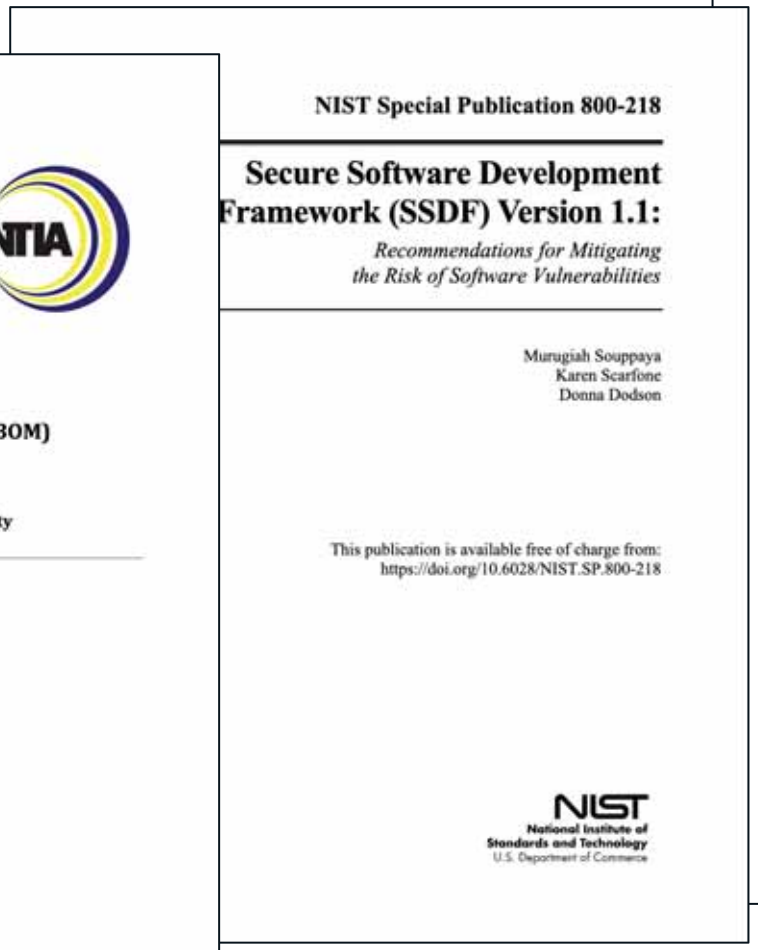
Pursuant to
Executive Order 14028
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

NIST SP 800-218 SSDF



NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

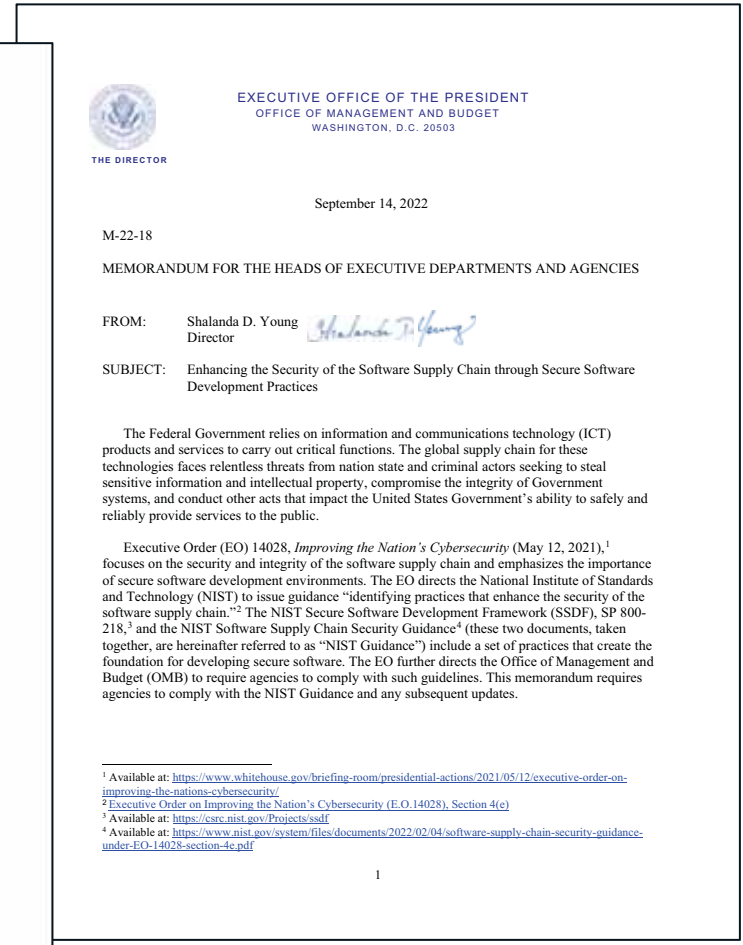
Murugiah Souppaya
Karen Scarfone
Donna Dodson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-218

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

OMB memo M-22-18



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government's ability to safely and reliably provide services to the public.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain."[2] The NIST Secure Software Development Framework (SSDF), SP 800-218,[3] and the NIST Software Supply Chain Security Guidance[4] (these two documents, taken together, are hereinafter referred to as "NIST Guidance") include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] Executive Order on Improving the Nation's Cybersecurity (E.O.14028), Section 4(e)
[3] Available at: https://csrc.nist.gov/Projects/ssdf
[4] Available at: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

1

https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

SBOM Definition

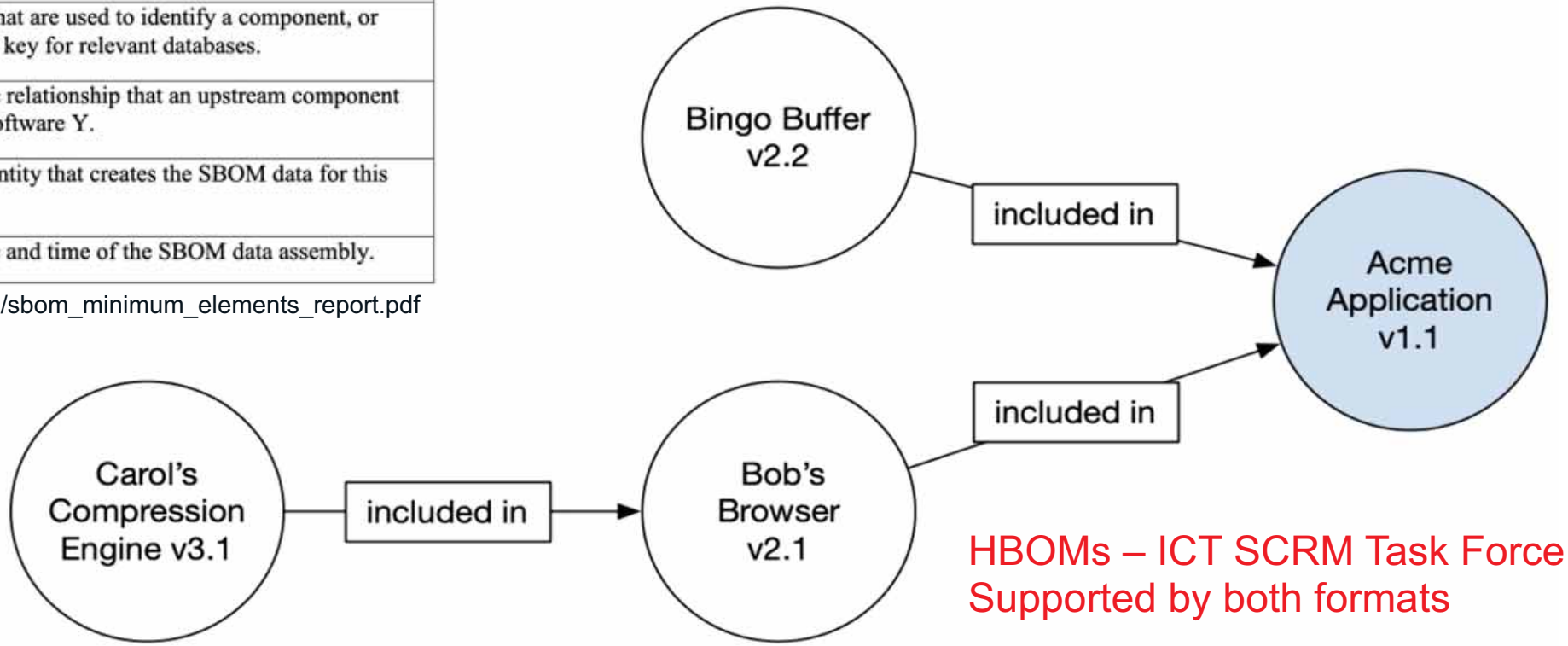
Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

SPDX
CycloneDX
SWID



HBOMs – ICT SCRM Task Force
Supported by both formats

Source: https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

MITRE

SBOM Communications Channels and Use Cases

Acquisitions
(Pre & Post Acquisition)

Acquisitions
(Pre & Post Acquisition)

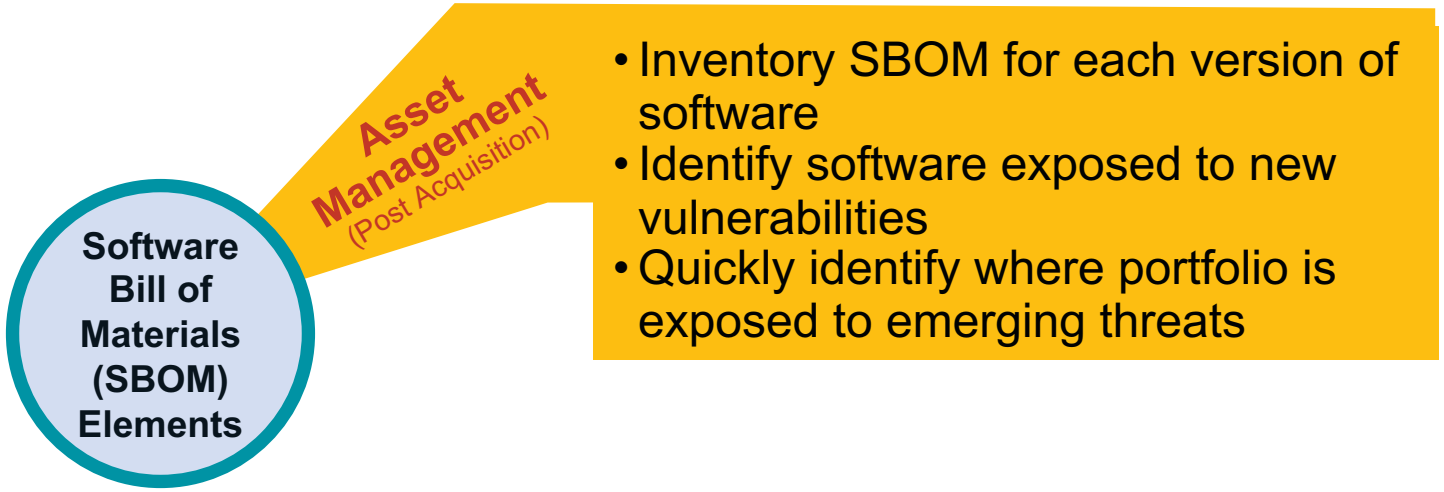
Software Bill of Materials (SBOM) Elements

Acquisition Software Assurance Assessment

- Validate software meets requirements for acquisition
- Flag issues for remediation before deployment

SBOM Communications Channels and Use Cases

Asset Management
(Post Acquisition)



SBOM Communications Channels and Use Cases

Policy
(SBOM Standard & Risk Threshold)

Software Bill of Materials (SBOM) Elements

Policy
(SBOM Standard & Risk Threshold)

- Define reporting and scanning requirements
- Define and maintain blocklist/allowlist of SBOM components
- Define risk thresholds for emerging threats (e.g. new CVEs for existing software)
- Define mitigation and remediation protocol

SBOM Communications Channels and Use Cases

Vulnerability Management
(Patching, Updates & Versioning)

Software Bill of Materials (SBOM) Elements

Vulnerability Management
(Patching, Updates & Versioning)

- Verify upgrade / patch/version meets blocklist / allowlist component requirements
- Verify software and SBOM components free of policy-violating vulnerabilities

MITRE

SBOM Communications Channels and Use Cases

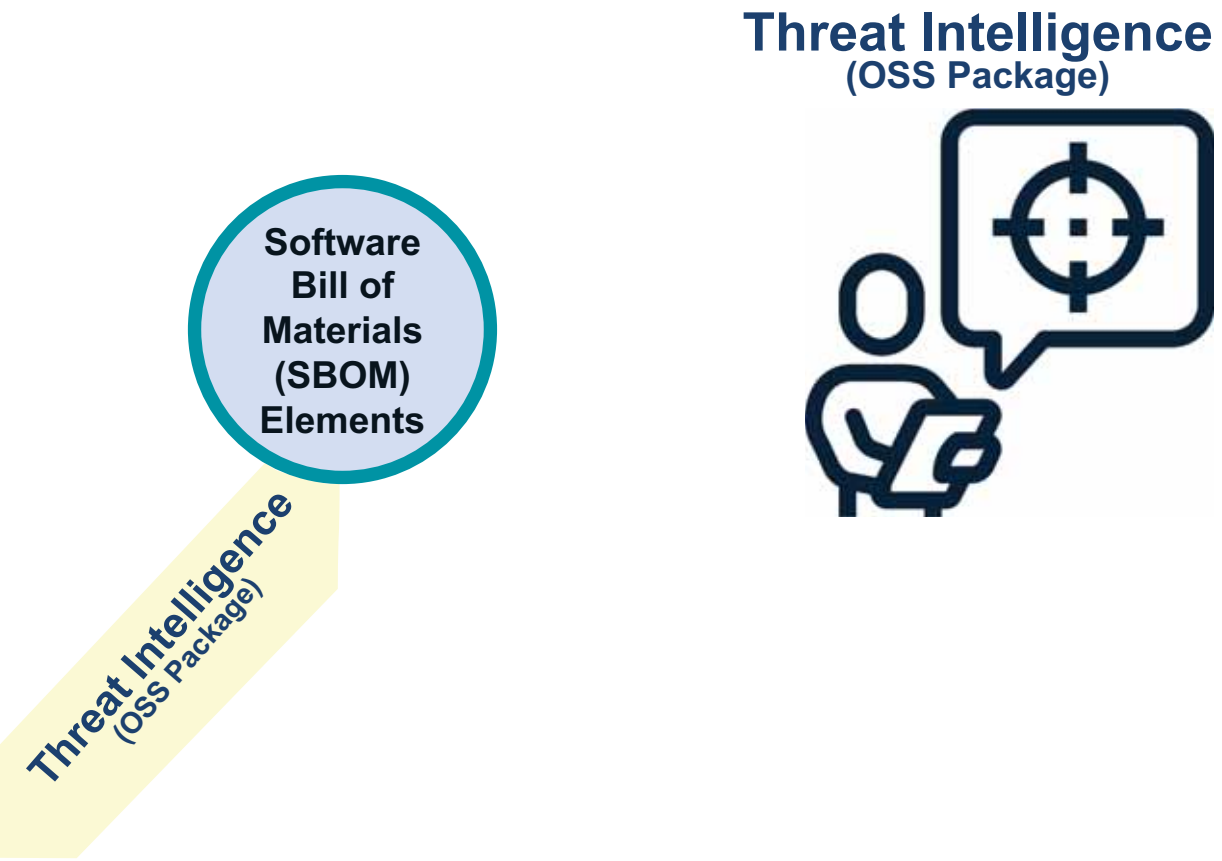
Incident Response

Software Bill of Materials (SBOM) Elements

Incident Response

- Use SBOM to quickly identify emerging threat exposure
- Target mitigation for compensating controls
- Target patching across software portfolio

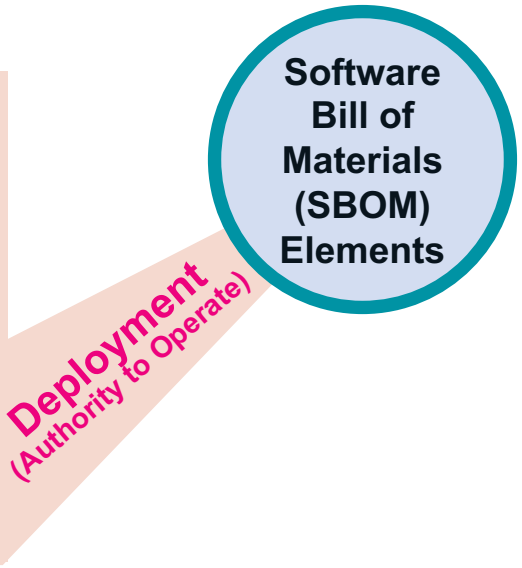
SBOM Communications Channels and Use Cases



- Map emerging Open Source threats embedded in software supply-chain

SBOM Communications Channels and Use Cases

- Identify disallowed SBOM components
- Drive remediations requirements to supplier
- Identify vulnerabilities and other OSS policy violations
- Verify software standards
- Applies to patches/updates/upgrades



SBOM Communications Channels and Use Cases

- Monitor that software complies with standards across software life cycle
- Pre-installation scan of patches / updates / upgrades

Continuous Monitoring
(Post Acquisition, Requirements & Remediation)

Software Bill of Materials (SBOM) Elements

Continuous Monitoring
(Post Acquisition, Requirements & Remediation)

SBOM Communications Channels and Use Cases

Contract requirements:
- 3rd party scanning chosen by agency required
- Vendor provides software for SBOM Validation
- On-going scanning req't across software life-cycle

Legal (Licensing)

Software Bill of Materials (SBOM) Elements

Legal
(Licensing)

SBOM Communications Channels and Use Cases

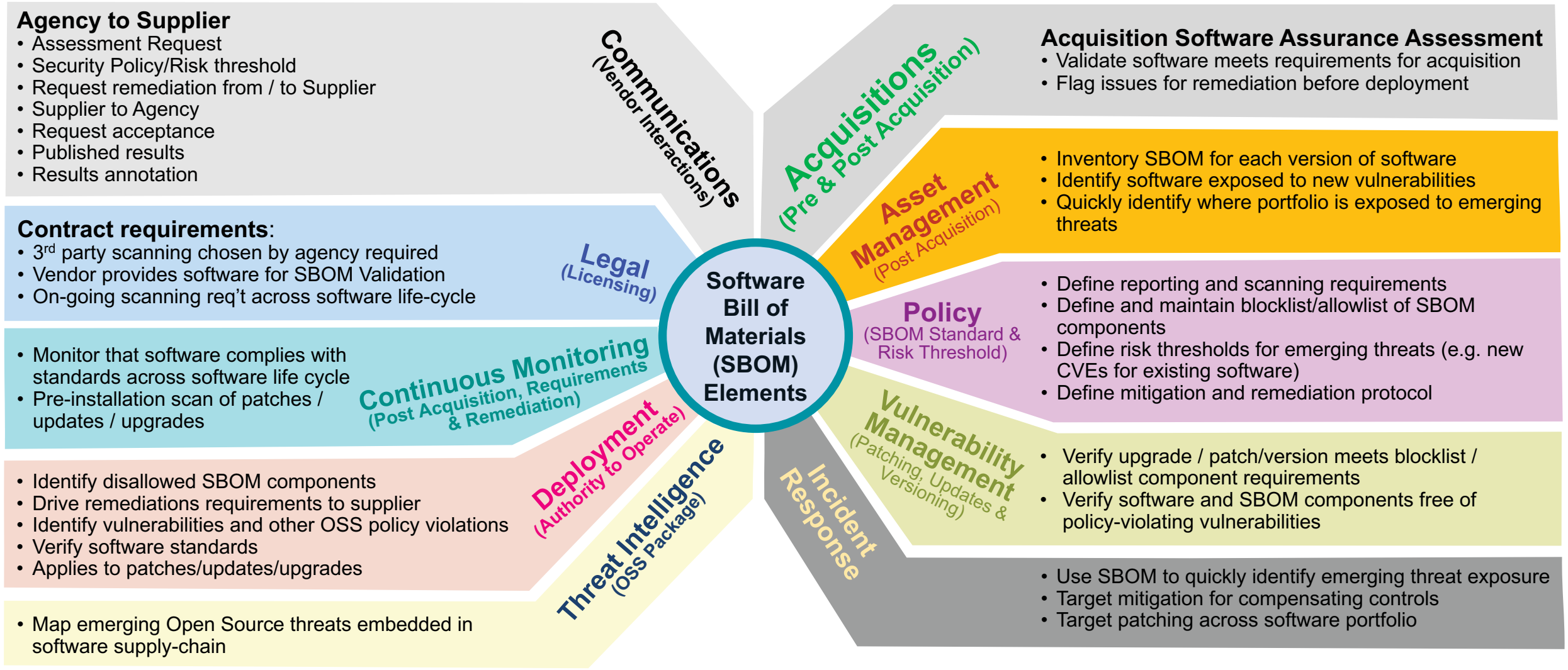
Agency to Supplier
- Assessment Request
- Security Policy/Risk threshold
- Request remediation from / to Supplier
- Supplier to Agency
- Request acceptance
- Published results
- Results annotation

Communications (Vendor Interactions)

Software Bill of Materials (SBOM) Elements

Communications
(Vendor Interactions)

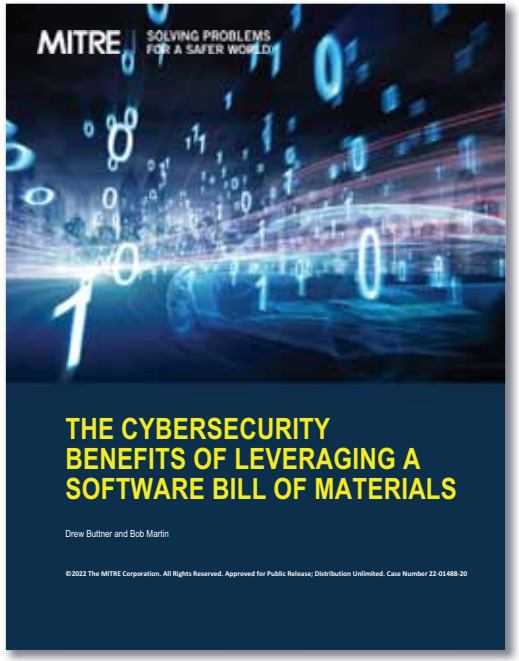
SBOM Communications Channels and Use Cases



Three MITRE and one Atlantic Council SBOM papers

https://www.mitre.org/sites/default/files/2021-10/pr-19-01876-16-standardizing-sbom-within-the-sw-development-tooling-ecosystem.pdf

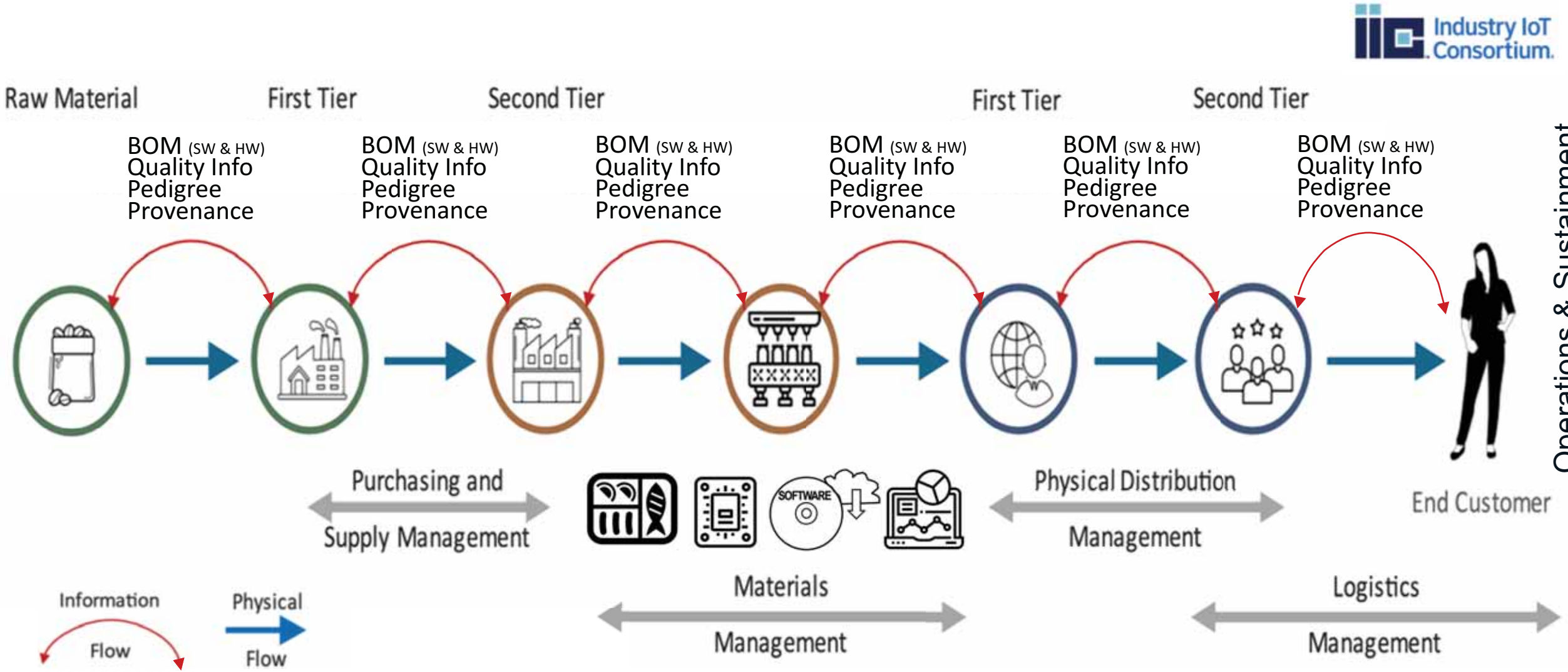
https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf



https://www.mitre.org/sites/default/files/2022-10/cybersecurity benefits_of_sbom_september_2022.pdf

https://www.atlanticcouncil.org/wp-content/uploads/2022/11/AC_SBOM_IB_v2-002.pdf

Supply Chains – As multi-Stakeholder Network



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

MITRE

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
- 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
- Cyber Physical Systems Symposium in Tokyo Japan
- others…

Executive Acquisition

Congressional Committees

MITRE

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

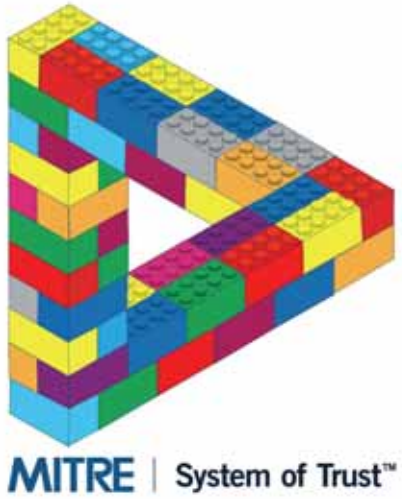
Standards and best practices oriented around SoT

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

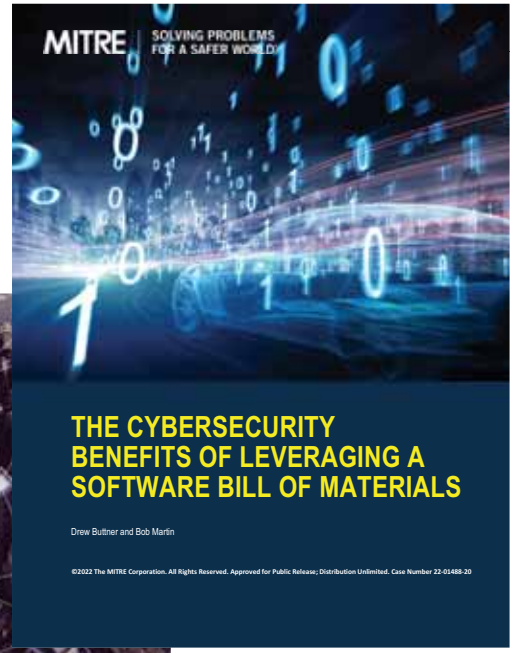
No-Cost* Licensing RMM tool & SoT content to Industry for integration in their own assessment practices and offerings



Publications to date…

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

SoT.MITRE.ORG

MITRE | System of Trust™

Overview | SoT Framework | Pilot Results | Resources | News & Calendar

Supply Chain Security

Hot Topics in Supply Chain Security Summit 2022 speaker bios, session videos, SoT video, and SoT slides now available! Click here

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 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

Growing Engagement about System of Trust

	Organization	Role
Signed NDA	Company 1	Microelectronics SMEs
	Company 2	Supply Chain Illumination SMEs
	Company 3	Critical Infrastructure SMEs
	Company 4	Supply Chain Illumination SMEs
	Company 5	Organization with Supply Chains
	Company 6	Organization with Supply Chains
	Company 7	Cybersecurity Illumination SMEs
	Company 8	Cybersecurity Illumination SMEs
	Company 9	Supply Chain Illumination SMEs
	Company 10	Organization with Supply Chains
	Company 11	Community Engagement SMEs
Drafting NDA	Company 12	Organization with Supply Chains
	Company 13	Organization with Supply Chains
	Company 14	Organization with Supply Chains
Discussing SoT	Company 15	Supply Chain Illumination SMEs
	Company 16	Organization with Supply Chains
	Company 17	Retail Banking SMEs
	Company 18	Third Party Risk Management SMEs
	Company 19	Sustainability SMEs
	(plus 20 more)	

Working on mechanisms to scale our engagements beyond NDAs