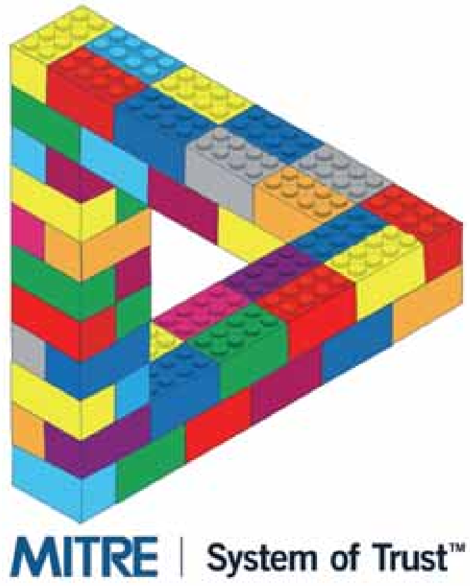
Taming the Chaos of Supply Chain Security Risks with MITRE's System of Trust™

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

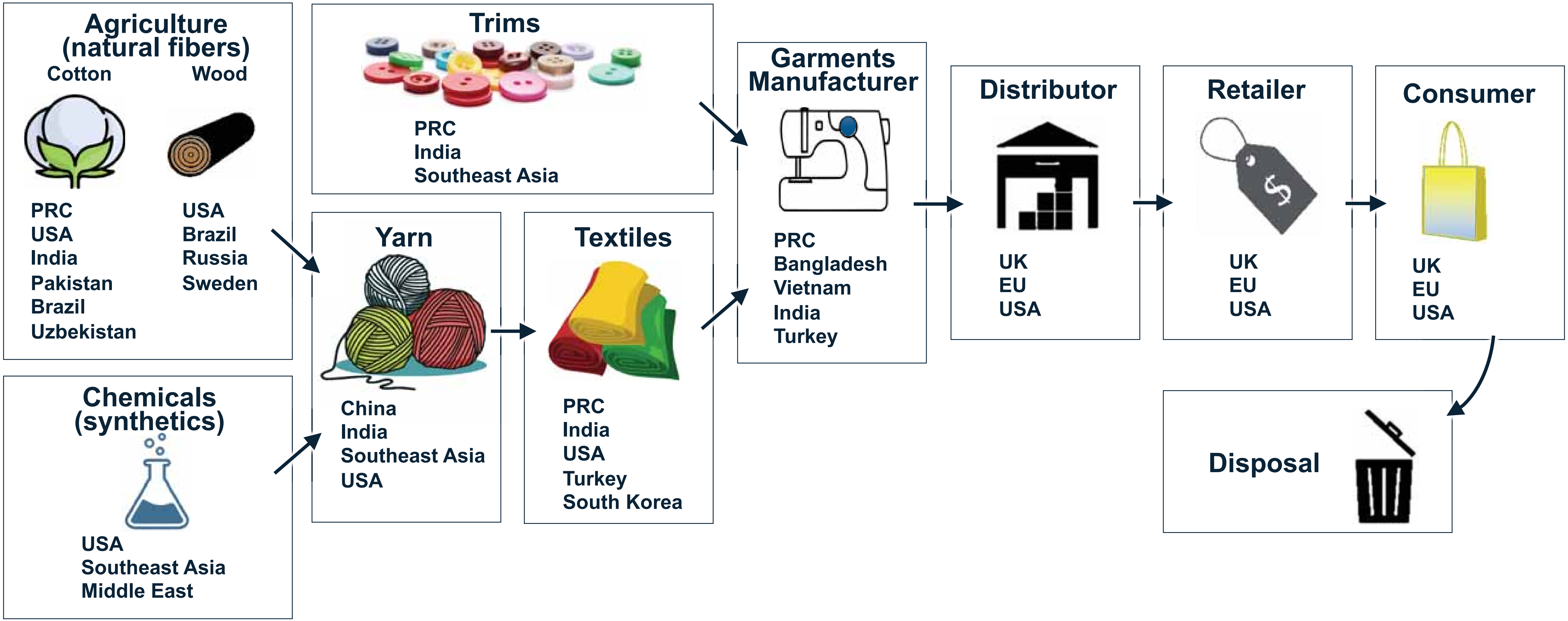
MITRE Labs



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chain Example – Consumer Clothing



Agriculture (natural fibers)

Cotton
PRC
USA
India
Pakistan
Brazil
Uzbekistan

Wood
USA
Brazil
Russia
Sweden

Chemicals (synthetics)

USA
Southeast Asia
Middle East

Trims

PRC
India
Southeast Asia

Yarn

China
India
Southeast Asia
USA

Textiles

PRC
India
USA
Turkey
South Korea

Garments Manufacturer

PRC
Bangladesh
Vietnam
India
Turkey

Distributor

UK
EU
USA

Retailer

UK
EU
USA

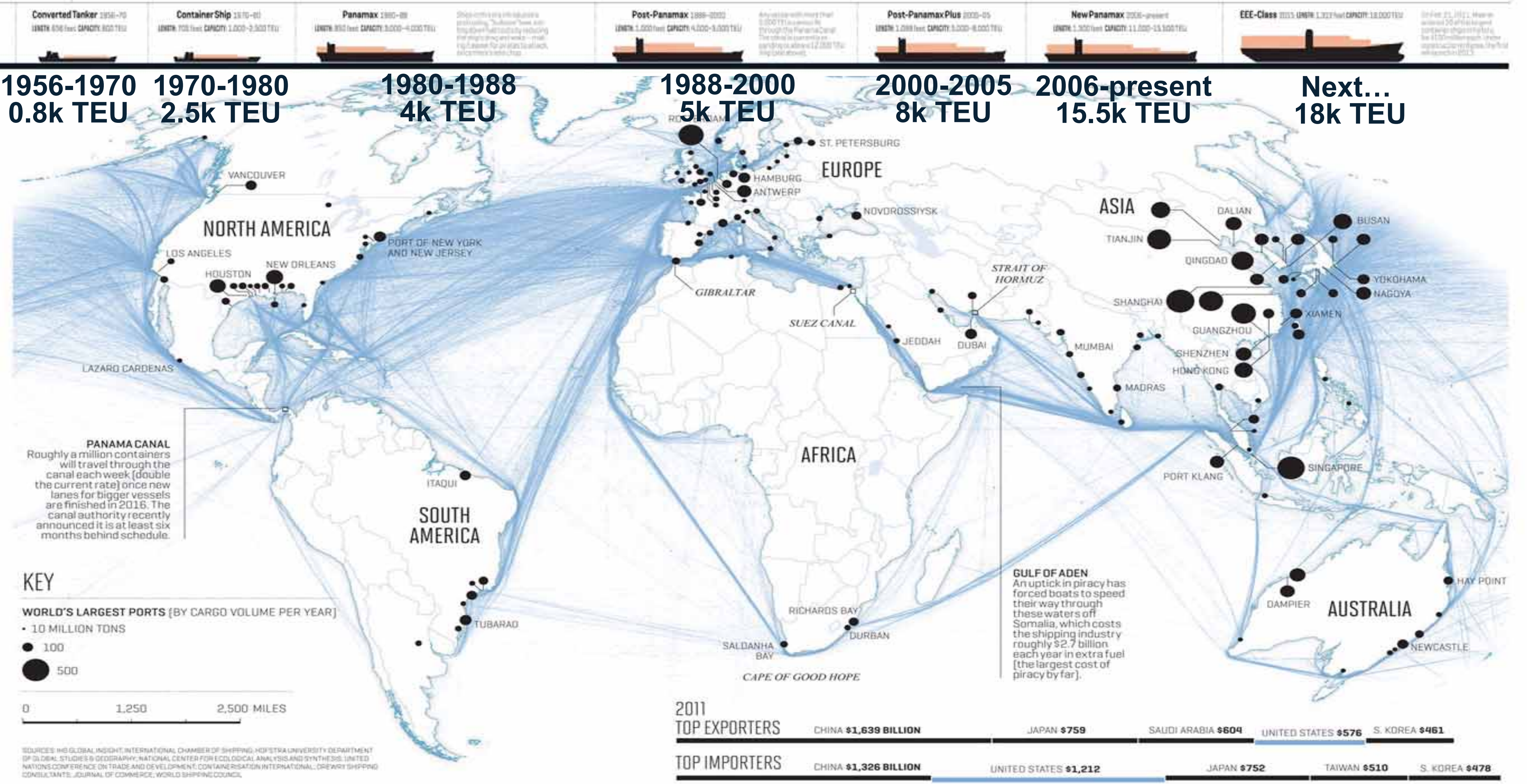
Consumer

UK
EU
USA

Disposal

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: 22-01488-10



1956-1970
0.8k TEU

1970-1980
2.5k TEU

1980-1988
4k TEU

1988-2000
5k TEU

2000-2005
8k TEU

2006-present
15.5k TEU

Next…
18k TEU

PANAMA CANAL
Roughly a million containers will travel through the canal each week (double the current rate) once new lanes for bigger vessels are finished in 2016. The canal authority recently announced it is at least six months behind schedule.

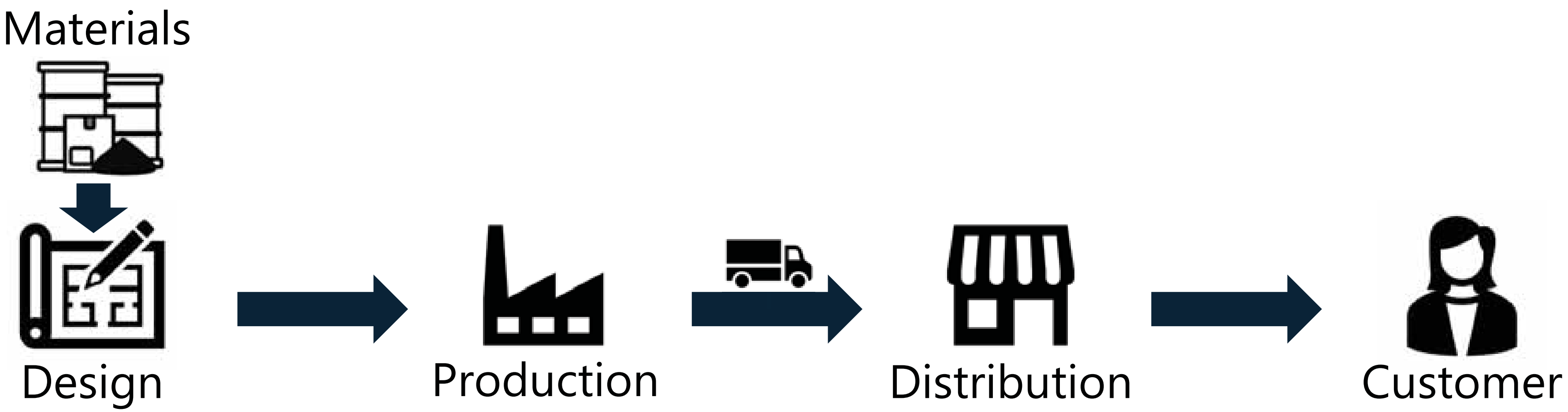
GULF OF ADEN
An uptick in piracy has forced boats to speed their way through these waters off Somalia, which costs the shipping industry roughly $2.7 billion each year in extra fuel (the largest cost of piracy by far).

SOURCES: IHS GLOBAL INSIGHT; INTERNATIONAL CHAMBER OF SHIPPING; HOFSTRA UNIVERSITY DEPARTMENT OF GLOBAL STUDIES & GEOGRAPHY; NATIONAL CENTER FOR ECOLOGICAL ANALYSIS AND SYNTHESIS; UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT; CONTAINERISATION INTERNATIONAL; DREWRY SHIPPING CONSULTANTS; JOURNAL OF COMMERCE; WORLD SHIPPING COUNCIL

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chains

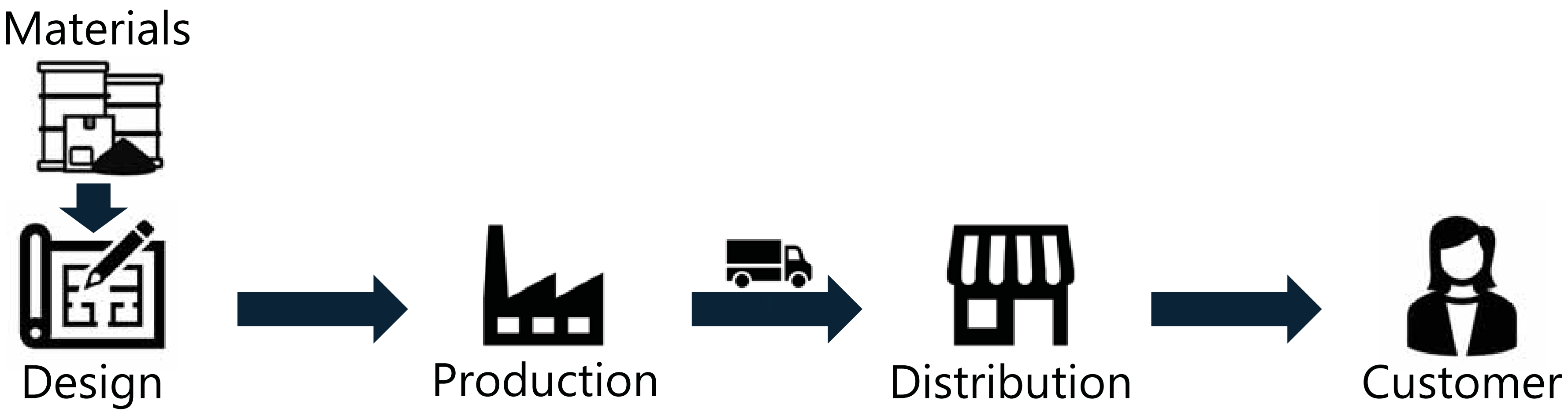
Generic Supply Chain



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chains

Generic Supply Chain



Materials

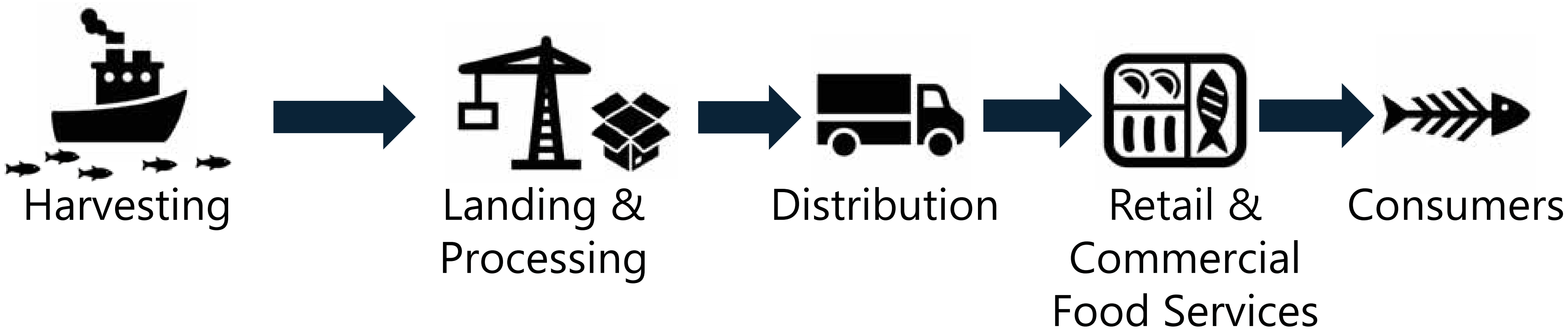
Design

Production

Distribution

Customer

Seafood Supply Chain



Harvesting

Landing & Processing

Distribution

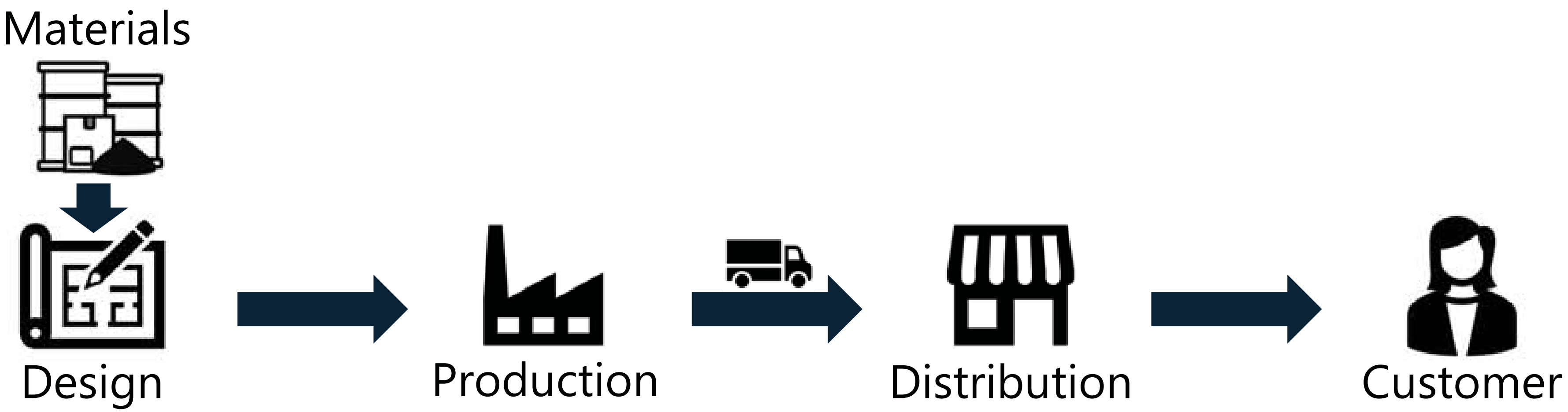
Retail & Commercial Food Services

Consumers

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chains

Generic Supply Chain



Materials

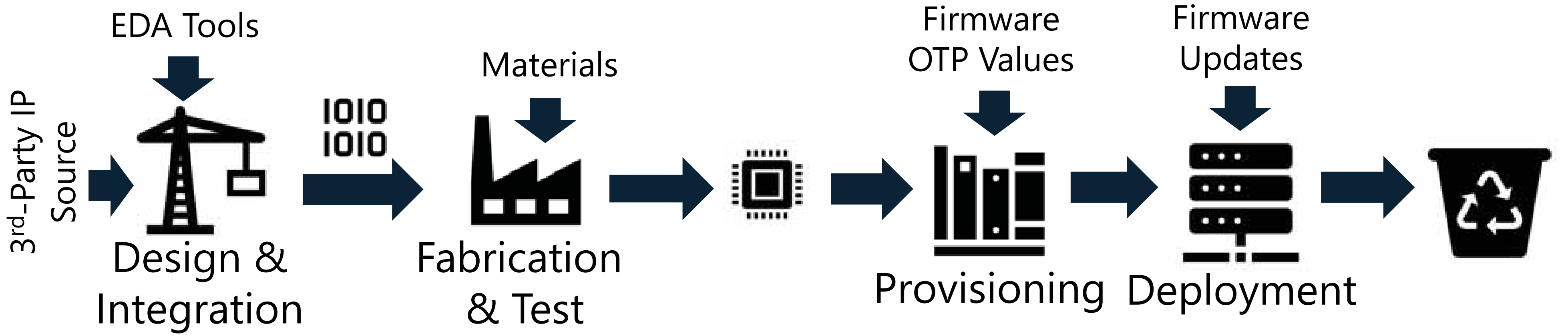
Design

Production

Distribution

Customer

Micro-electronics Supply Chain



3^{rd}-Party IP Source

EDA Tools

Design & Integration

1010
1010

Materials

Fabrication & Test

Firmware OTP Values

Provisioning

Firmware Updates

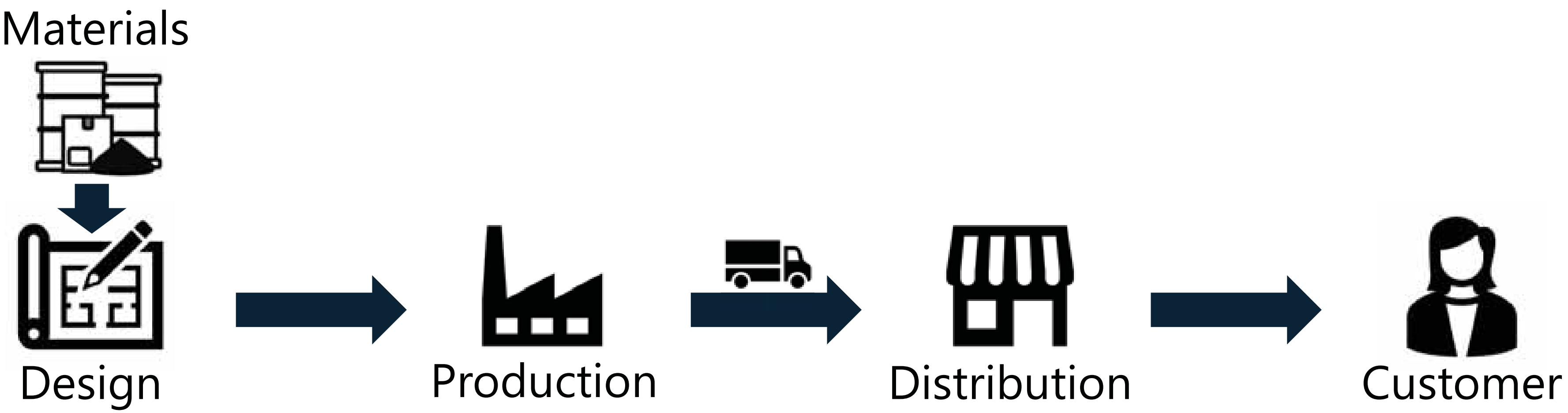
Deployment

MITRE

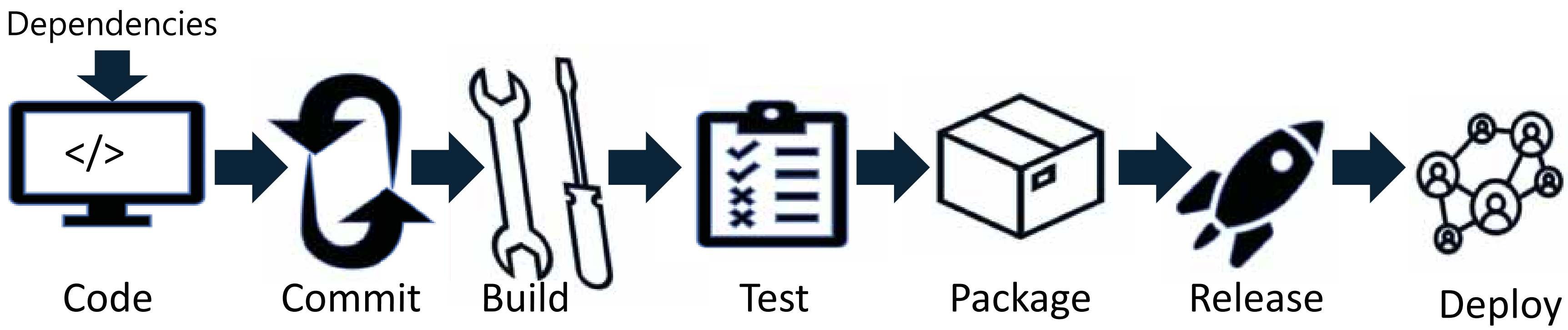
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chains

Generic Supply Chain

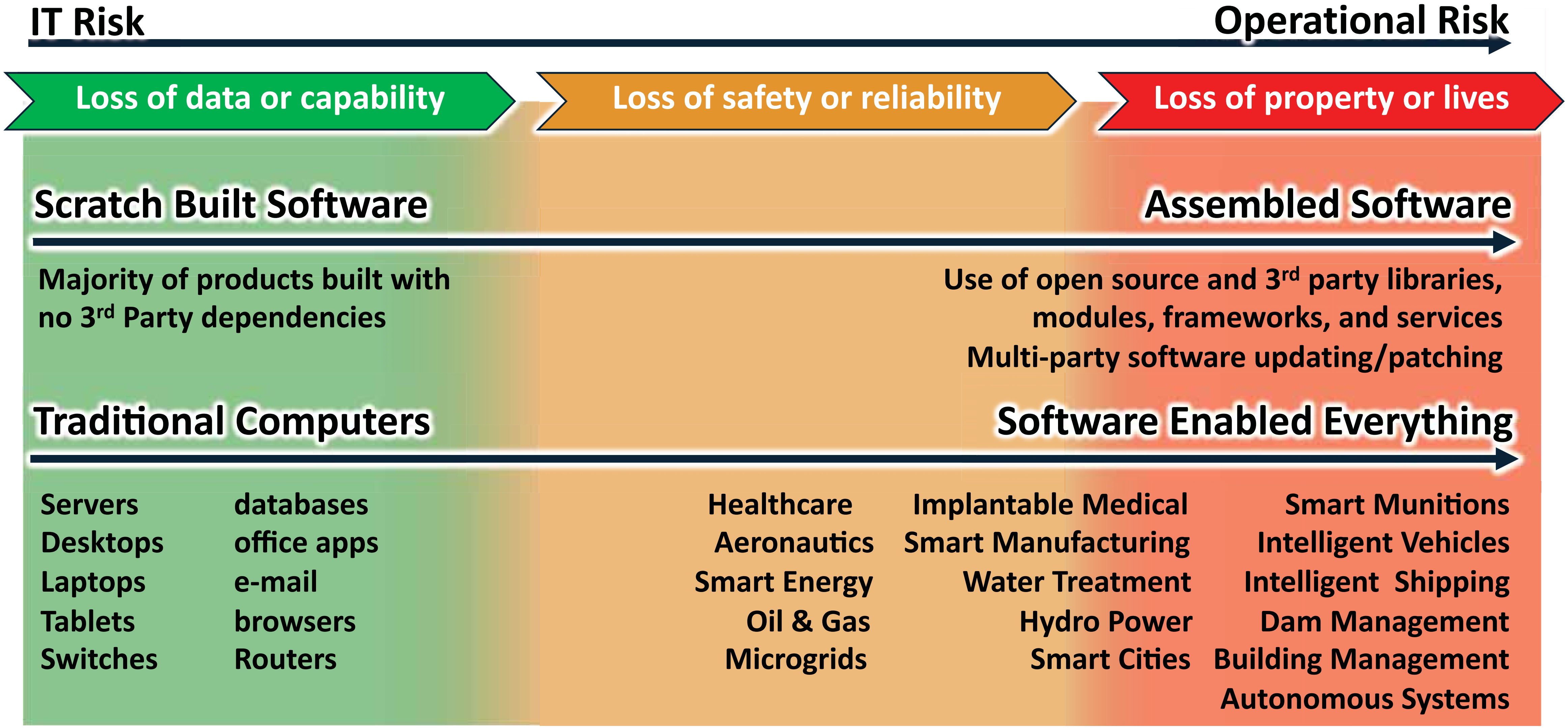


Software Supply Chain



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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
Desktops
Laptops
Tablets
Switches

databases
office apps
e-mail
browsers
Routers

Healthcare
Aeronautics
Smart Energy
Oil & Gas
Microgrids

Implantable Medical
Smart Manufacturing
Water Treatment
Hydro Power
Smart Cities

Smart Munitions
Intelligent Vehicles
Intelligent Shipping
Dam Management
Building Management
Autonomous Systems

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Software Enabled Critical Infrastructure and Mission Capabilities…

Medical

Vehicles

Buildings

Temperature, Humidity,CO2

Motion Sensor

AC,Chiller

Electric power

Elevator

Entrance gate

Aeronautics

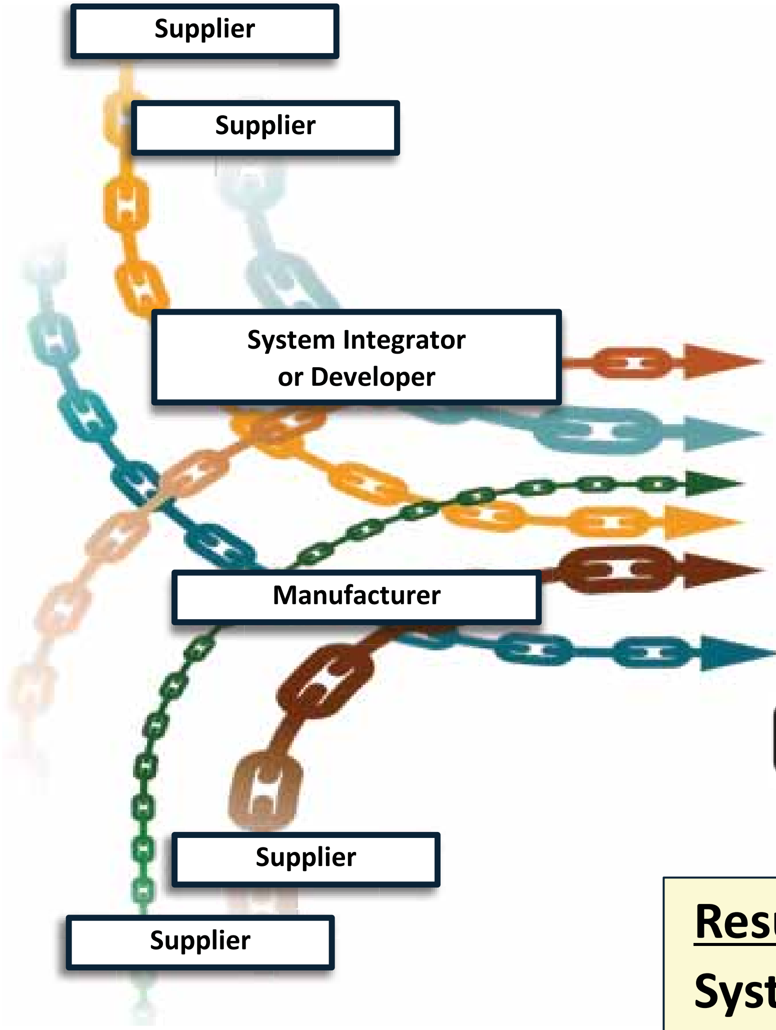
Energy

Manufacturing

Shipping

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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



Supplier

Supplier

System Integrator or Developer

Manufacturer

Supplier

Supplier

Based on SEI/CMU materials

Acquirer

Intentional acts

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

Unintentional acts

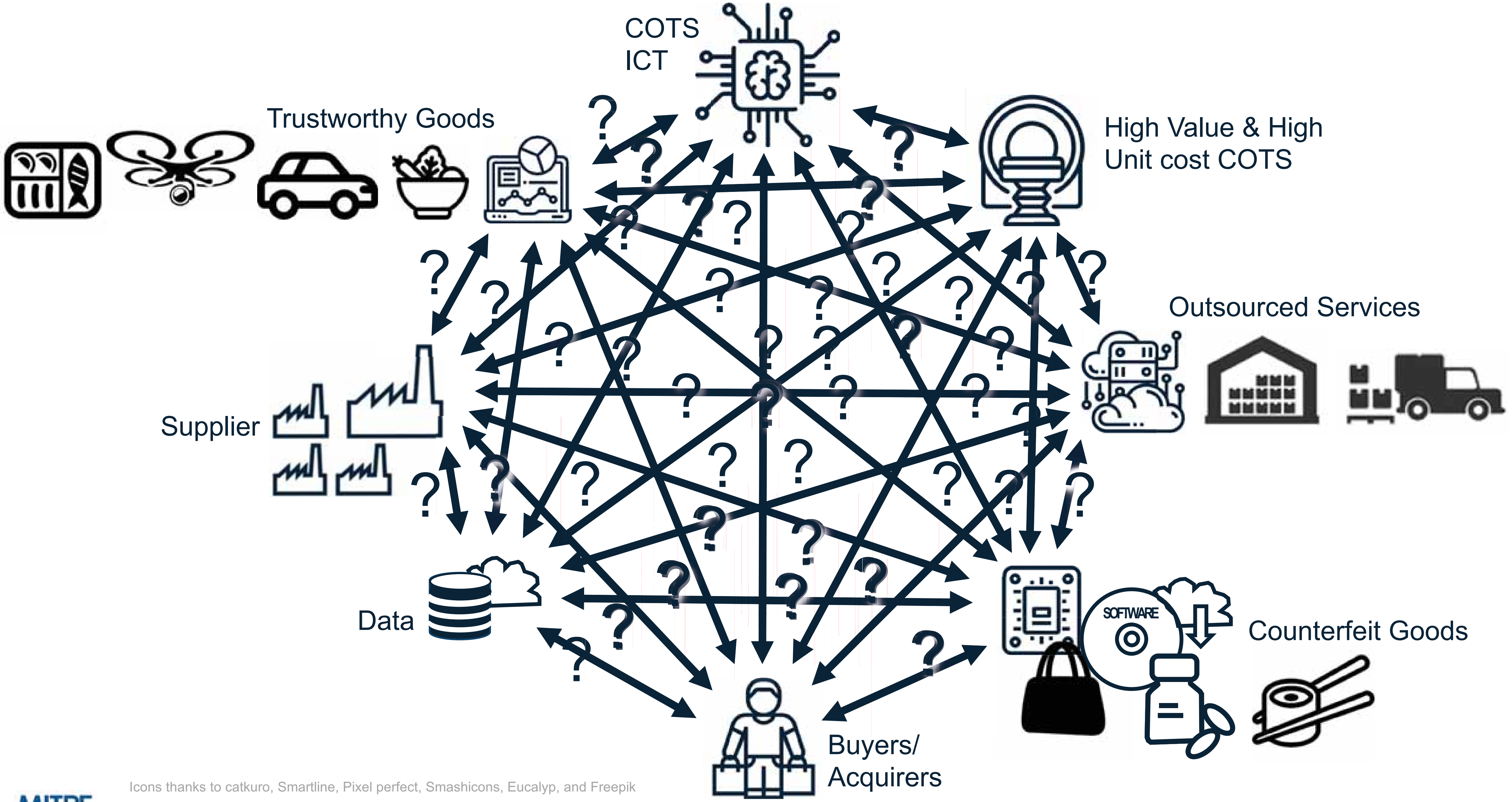
- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/weaknesses and/or known vulnerabilities)

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: 22-01488-10

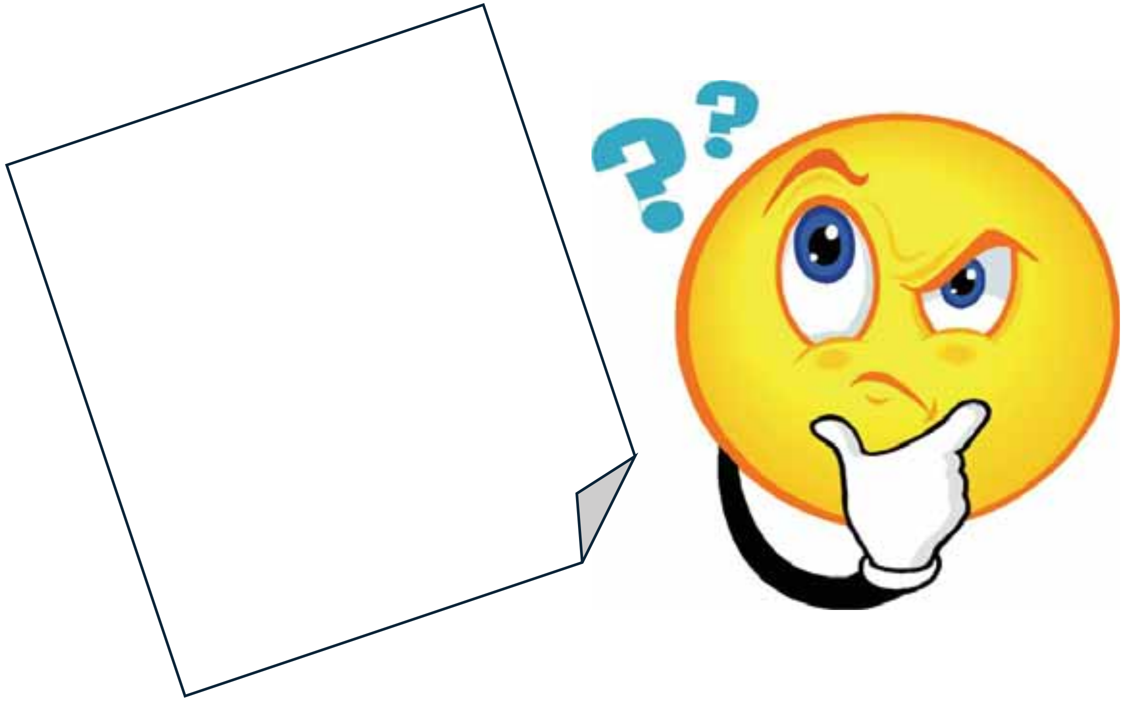
Open Question: What Supply Chain Risks to Manage?

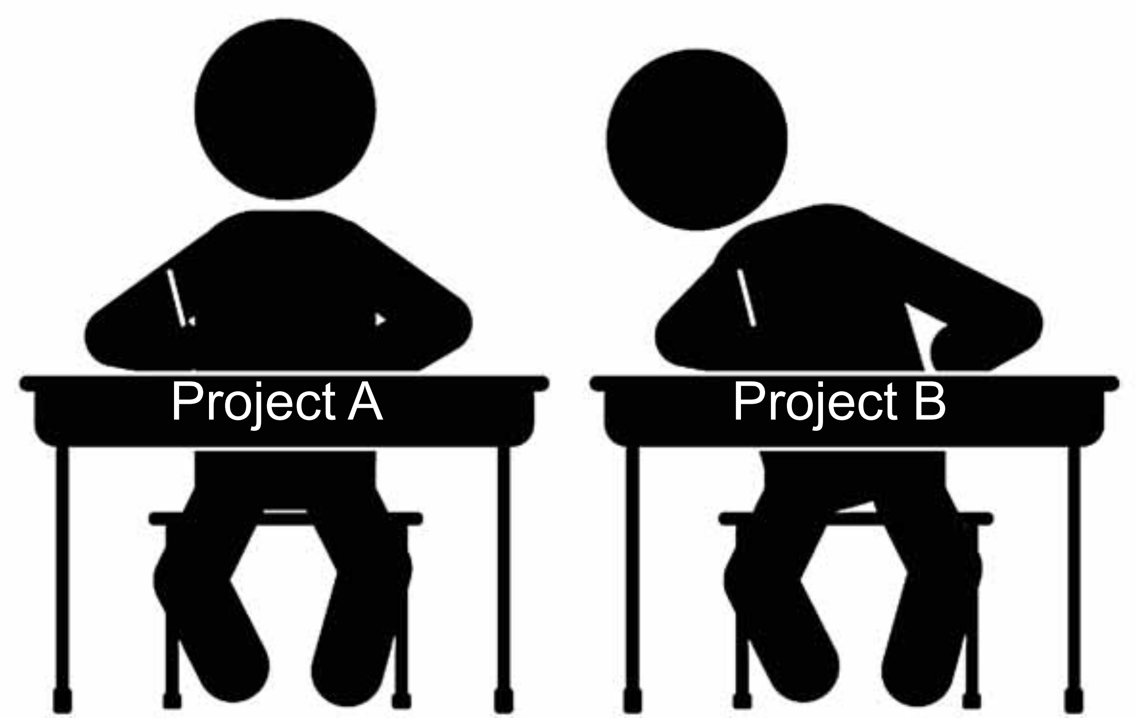


Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Open Question: What Supply Chain Risks to Manage?





© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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

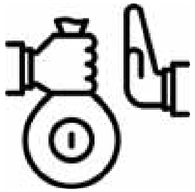
Financial Stability of the Supplier
Organizational Stature of the Supplier
Susceptibility of the Supplier

Maliciousness of the Supplier
Organizational Security

Attackers & Counterfeits

Human Hazards

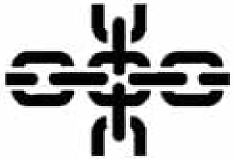
Hijacking



Corporate Corruption

Traffic Congestion

Civil Disruption



Interdependent Supply Chains

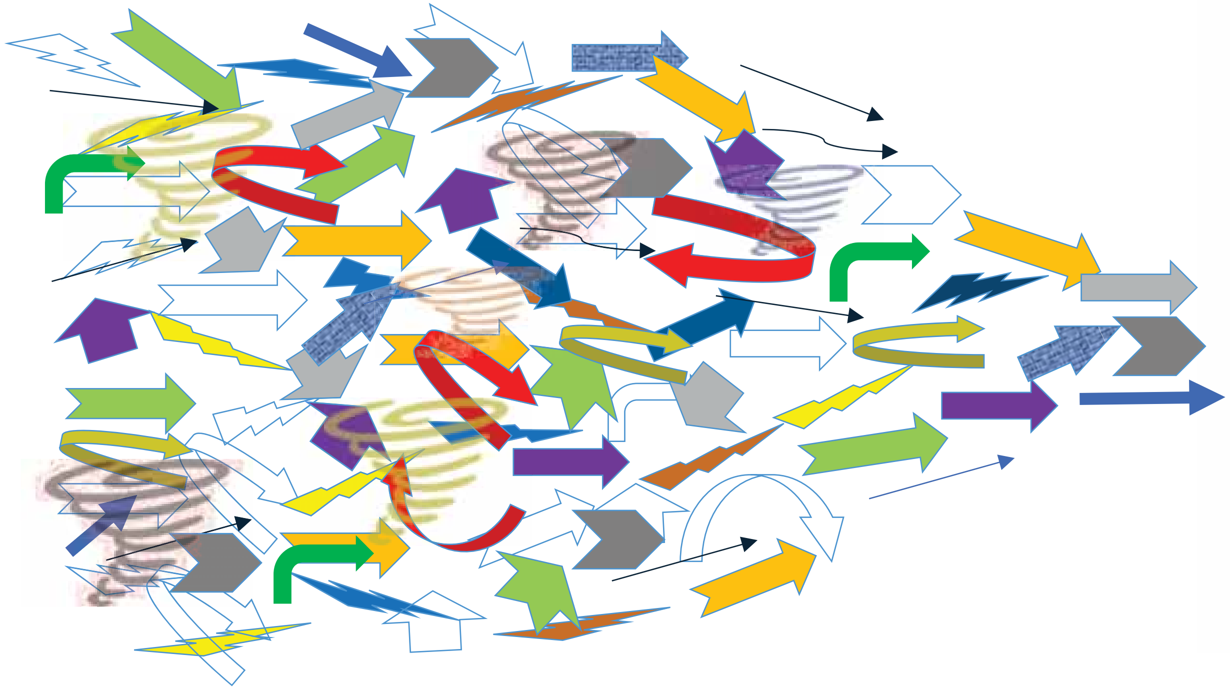
National Corruption

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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

"What Supply Chain Risks to Manage?"

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

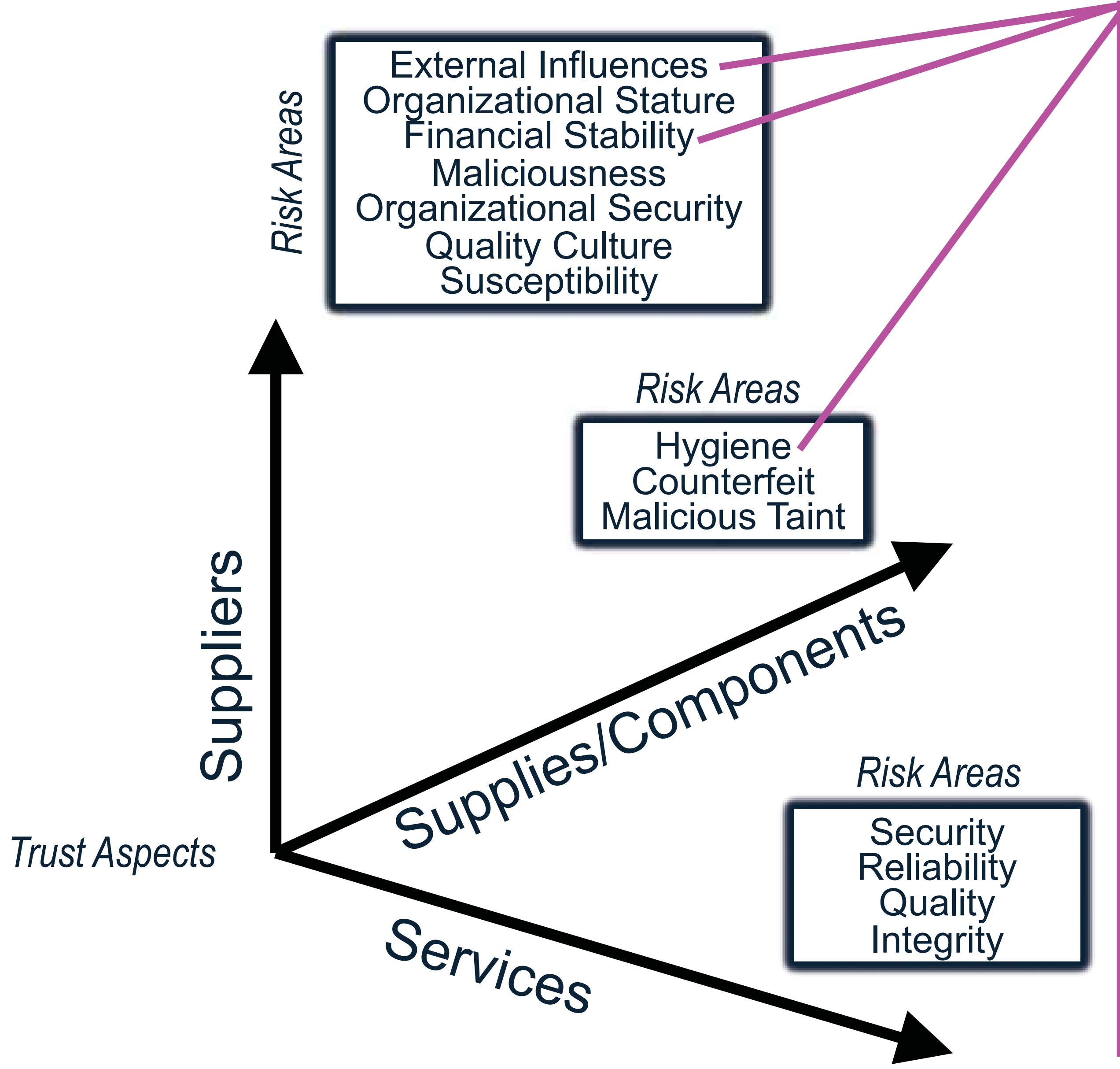


Address Chaos, Align & Organize

Simplify, Tailor & Use

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Basis of Trust

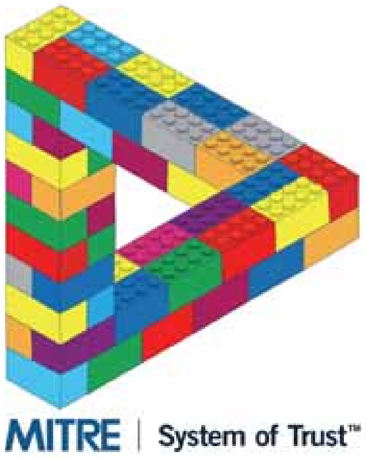


- **Product Quality**
  - ICT Hardware Product Quality
  - Product Quality Requirements
  - Software Product Quality
    - ○ Software Anomaly Control
    - ○ Software Consistency
    - ○ Software Design Simplicity
    - ○ Software Provenance & Pedigree
    - ○ …
- **Product Resilience**
  - ICT Hardware 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: 22-01488-10

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

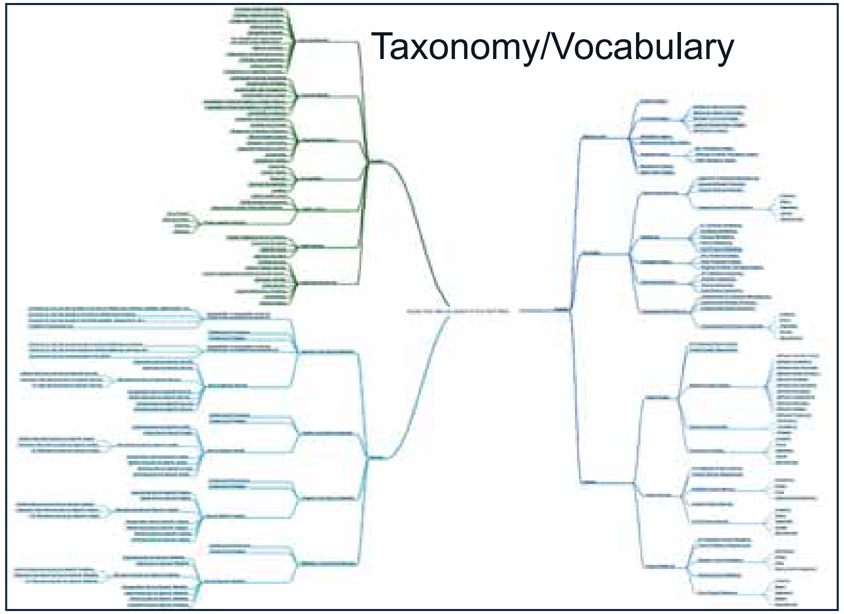
Supply Chain Risks													
Supplier Risks							Supply Risks			Services Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service 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 Person (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													



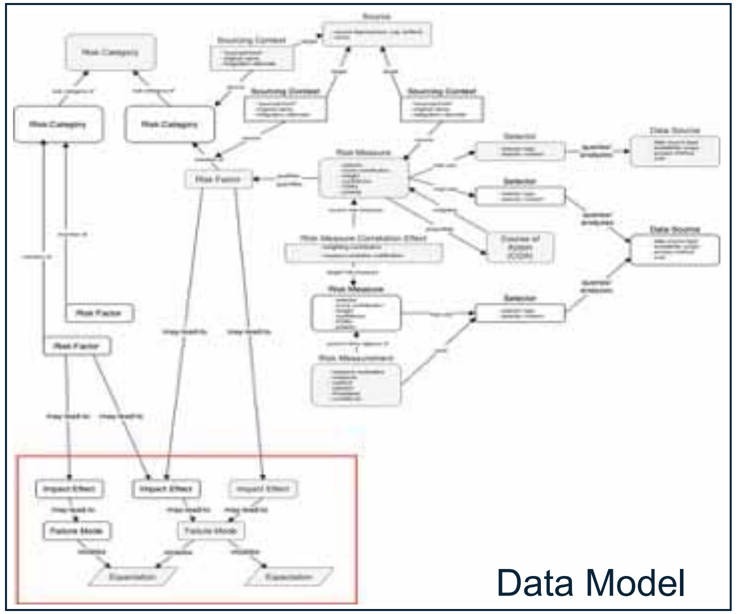
MITRE's Supply Chain Security System of Trust™
https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach

* 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: 22-01488-10

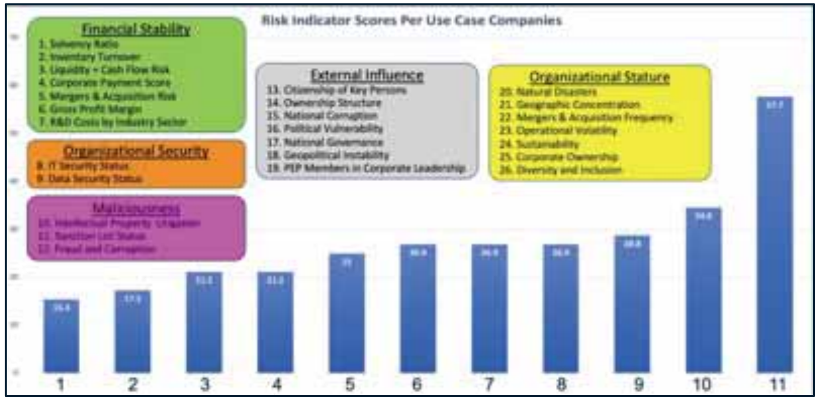


Taxonomy/Vocabulary

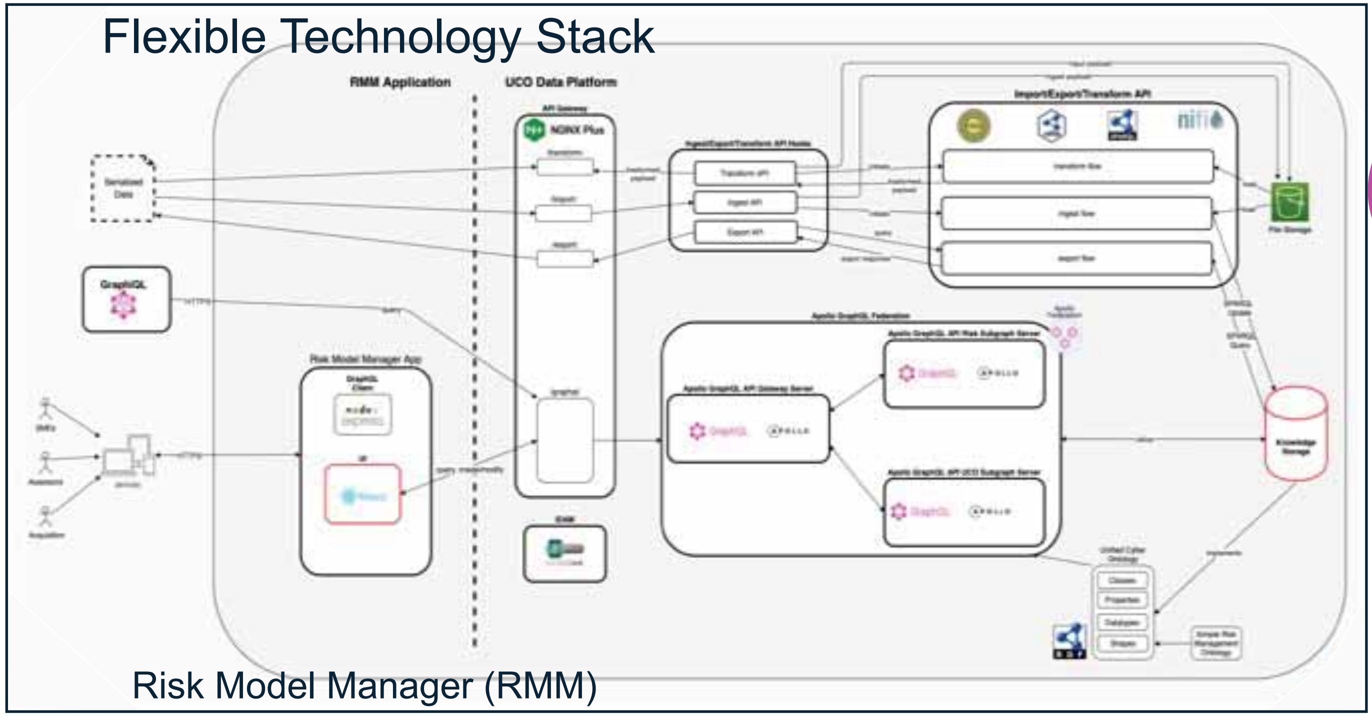


Data Model

Analytic Methods



Risk Indicator Scores Per Use Case Companies
Financial Stability
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
Organizational Security
8. IT Security Status
9. Data Security Status
Maliciousness
10. Intellectual Property Litigation
11. Sanction List Status
12. Fraud and Corruption
External Influence
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
Organizational Stature
20. Natural Disasters
21. Geographic Concentration
22. Mergers & Acquisition Frequency
23. Operational Volatility
24. Sustainability
25. Corporate Ownership
26. Diversity and Inclusion
1
2
3
4
5
6
7
8
9
10
11

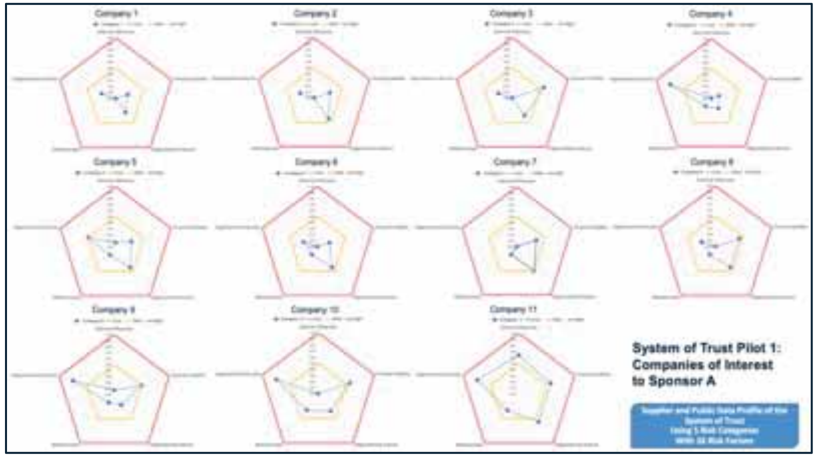


Flexible Technology Stack

Risk Model Manager (RMM)

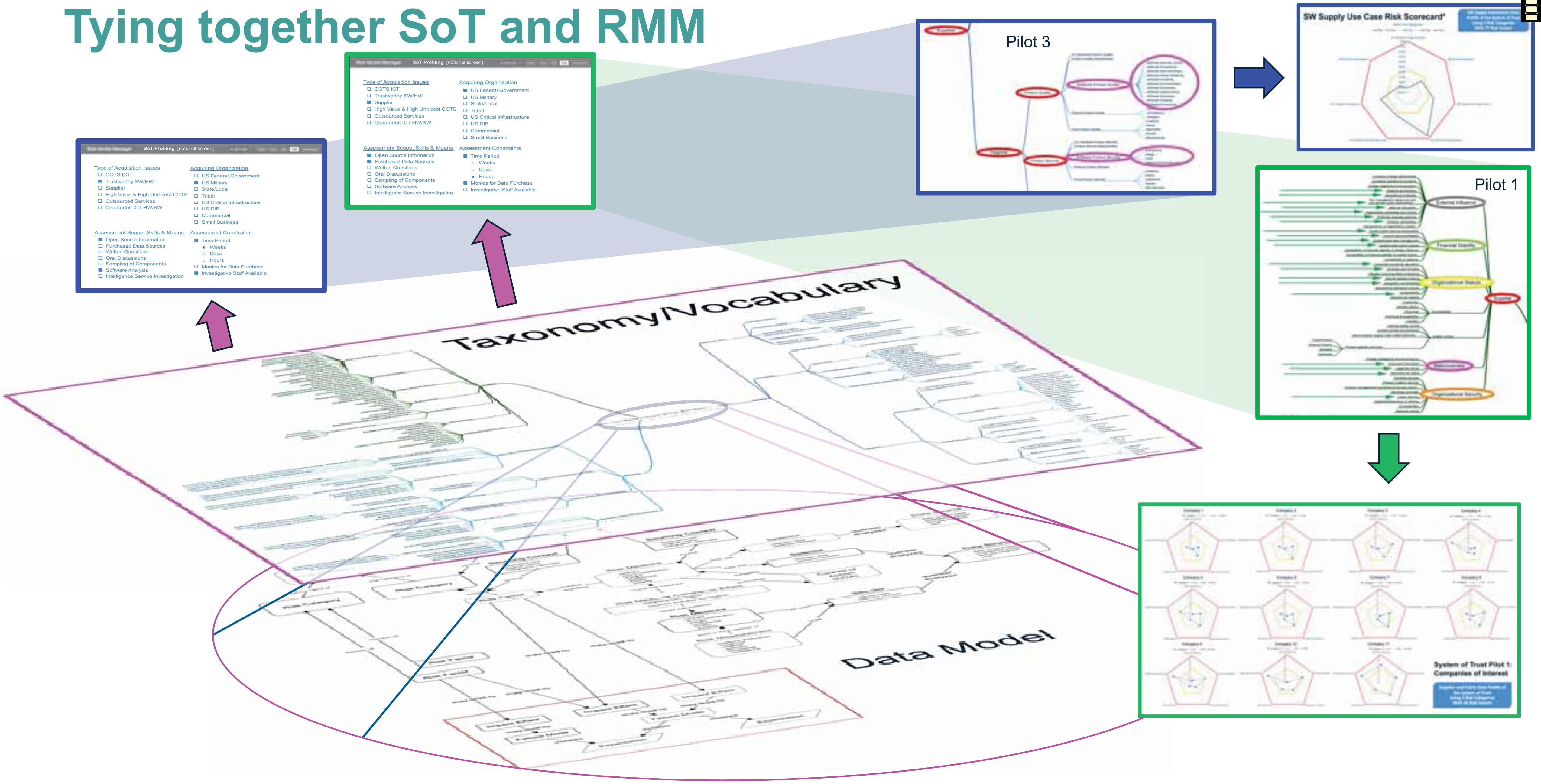
Piloting
11, 3, 1, 6,
22, 12, …

Export to Spreadsheet for "Offline" Assessment



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Tying together SoT and RMM



Risk Model Manager SoT Profiling [notional screen]

Type of Acquisition Issues
□ COTS ICT
■ Trustworthy SW/HW
□ Supplier
□ High Value & High Unit cost COTS
□ Outsourced Services
□ Counterfeit ICT HW/SW

Acquiring Organization
□ US Federal Government
■ US Military
□ State/Local
□ Tribal
□ US Critical Infrastructure
□ US DIB
□ Commercial
□ Small Business

Assessment Scope, Skills & Means
■ Open Source Information
□ Purchased Data Sources
□ Written Questions
□ Oral Discussions
□ Sampling of Components
■ Software Analysis
□ Intelligence Service Investigation

Assessment Constraints
■ Time Period
● Weeks
○ Days
○ Hours
□ Monies for Data Purchase
■ Investigative Staff Available

Risk Model Manager SoT Profiling [notional screen]

Type of Acquisition Issues
□ COTS ICT
□ Trustworthy SW/HW
■ Supplier
□ High Value & High Unit cost COTS
□ Outsourced Services
□ Counterfeit ICT HW/SW

Acquiring Organization
■ US Federal Government
□ US Military
□ State/Local
□ Tribal
□ US Critical Infrastructure
□ US DIB
□ Commercial
□ Small Business

Assessment Scope, Skills & Means
■ Open Source Information
■ Purchased Data Sources
□ Written Questions
□ Oral Discussions
□ Sampling of Components
□ Software Analysis
□ Intelligence Service Investigation

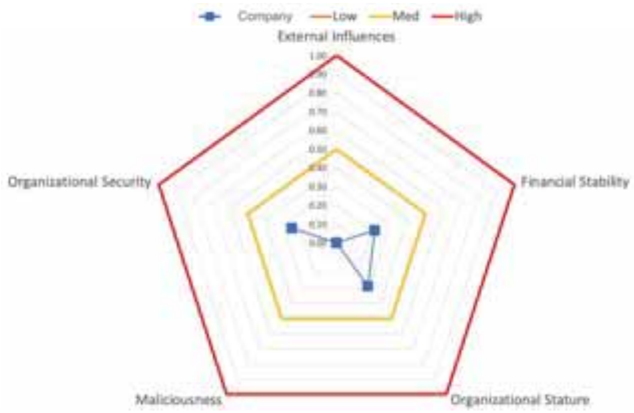
Assessment Constraints
■ Time Period
○ Weeks
○ Days
● Hours
■ Monies for Data Purchase
□ Investigative Staff Available

Pilot 3
SW Supply Use Case Risk Scorecard*
Pilot 1
Taxonomy/Vocabulary
Data Model
System of Trust Pilot 1: Companies of Interest

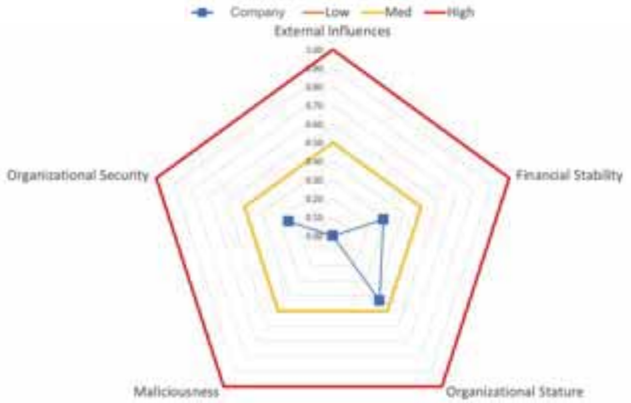
MITRE

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

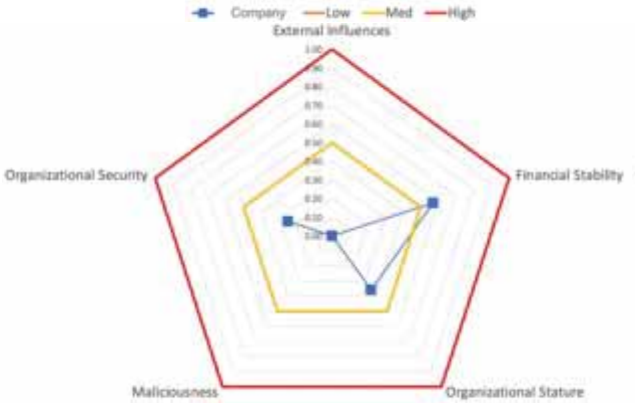
Company 1



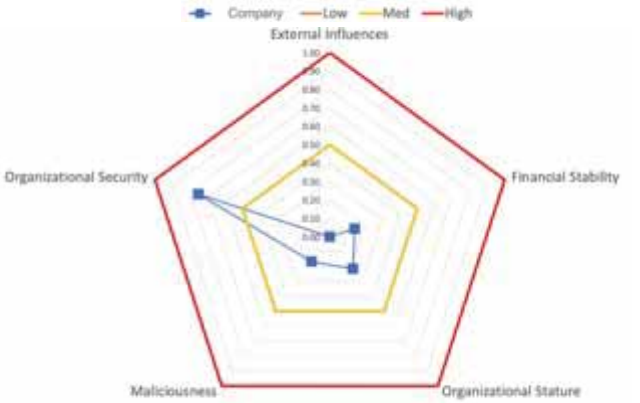
Company 2



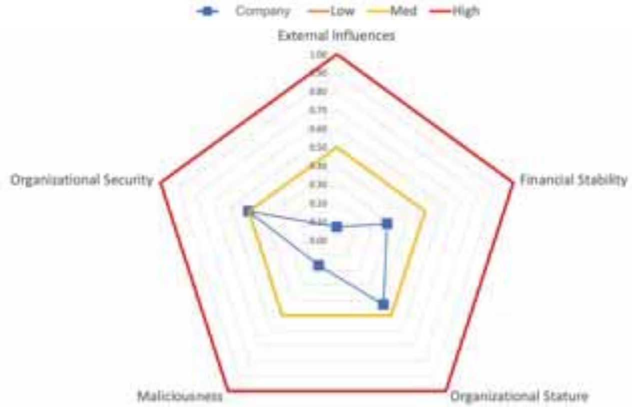
Company 3



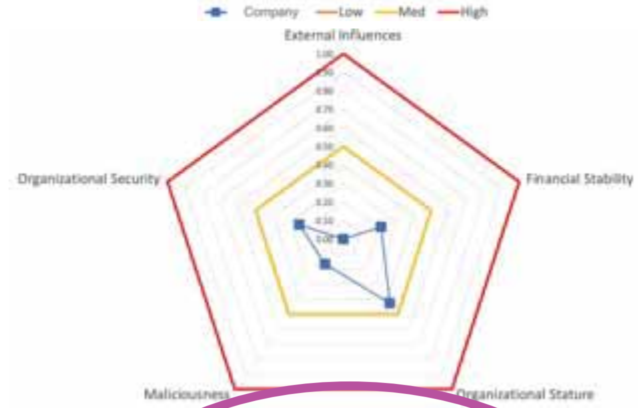
Company 4



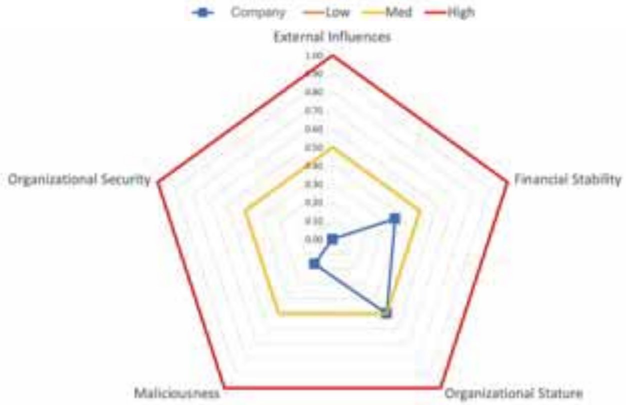
Company 5



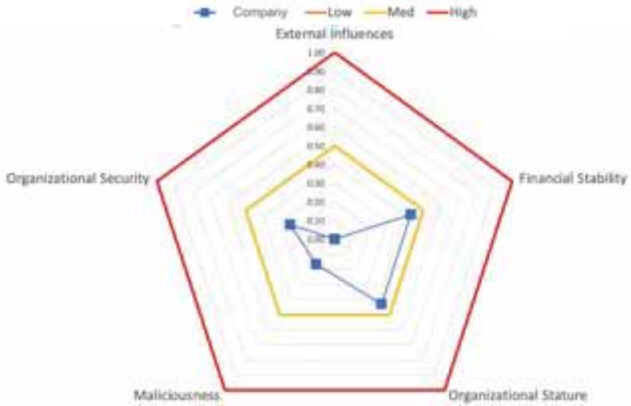
Company 6



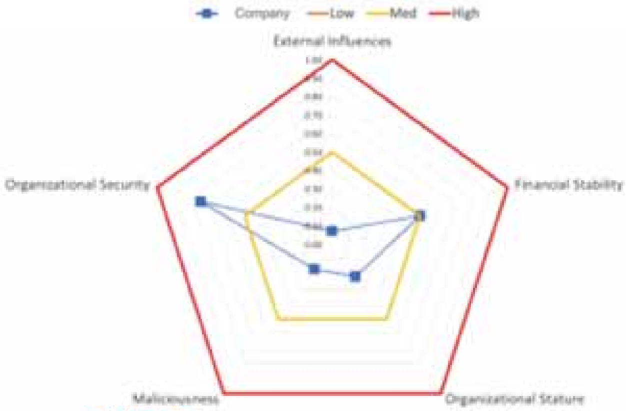
Company 7



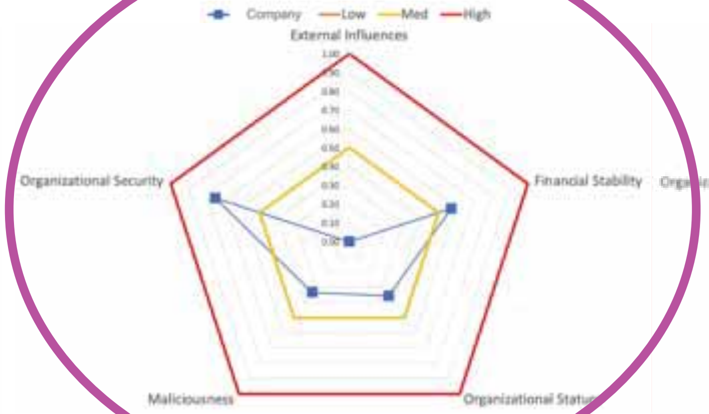
Company 8



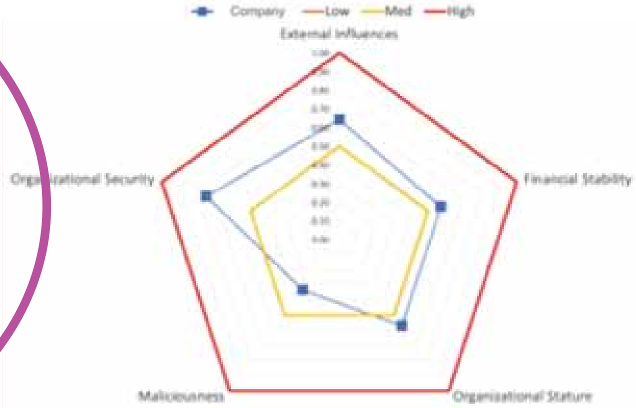
Company 9



Company 10



Company 11



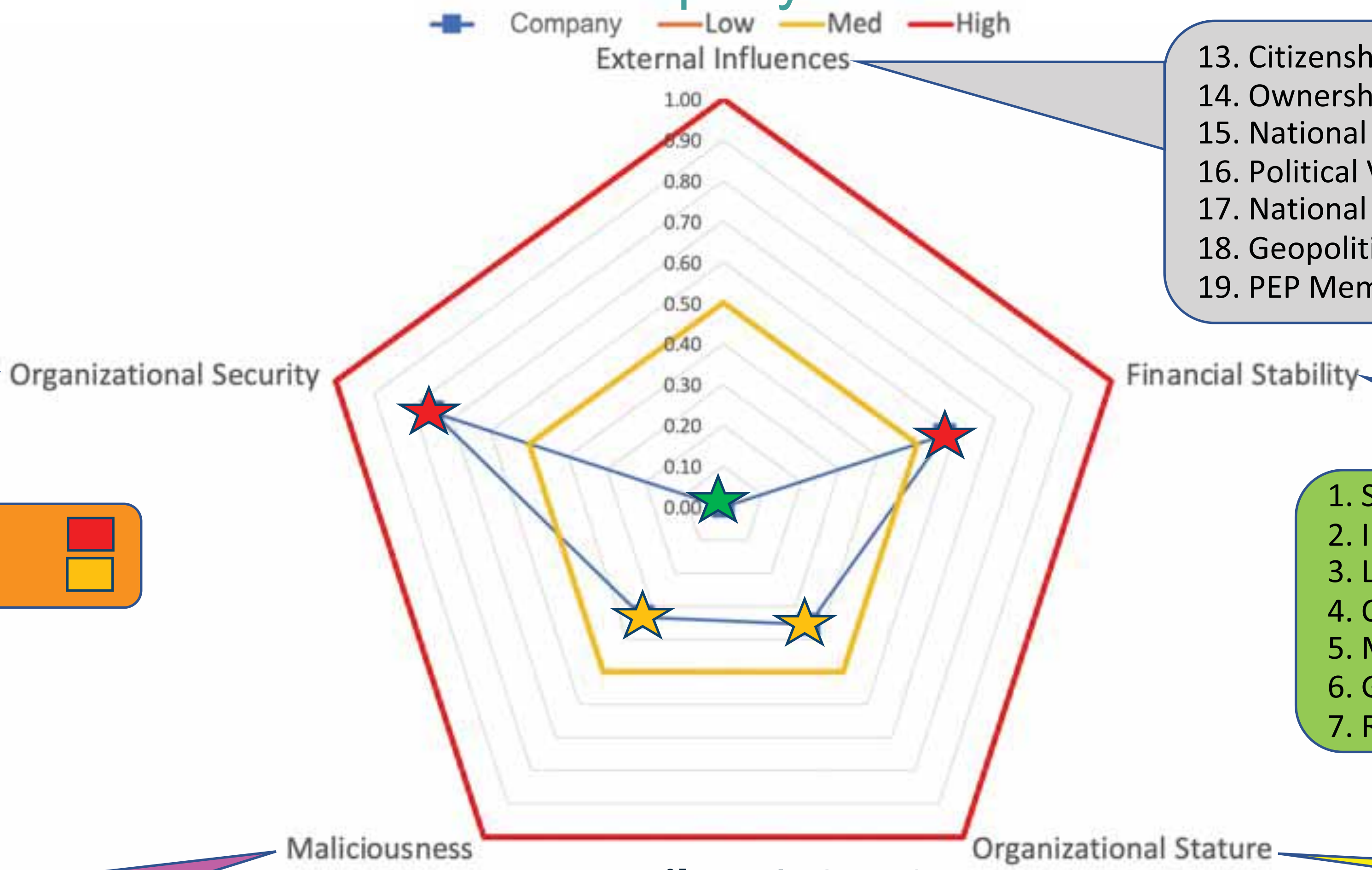
Applying

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: 22-01488-10

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	🟩

8. IT Security Status	🟥
9. Data Security Status	🟨

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	🟩

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

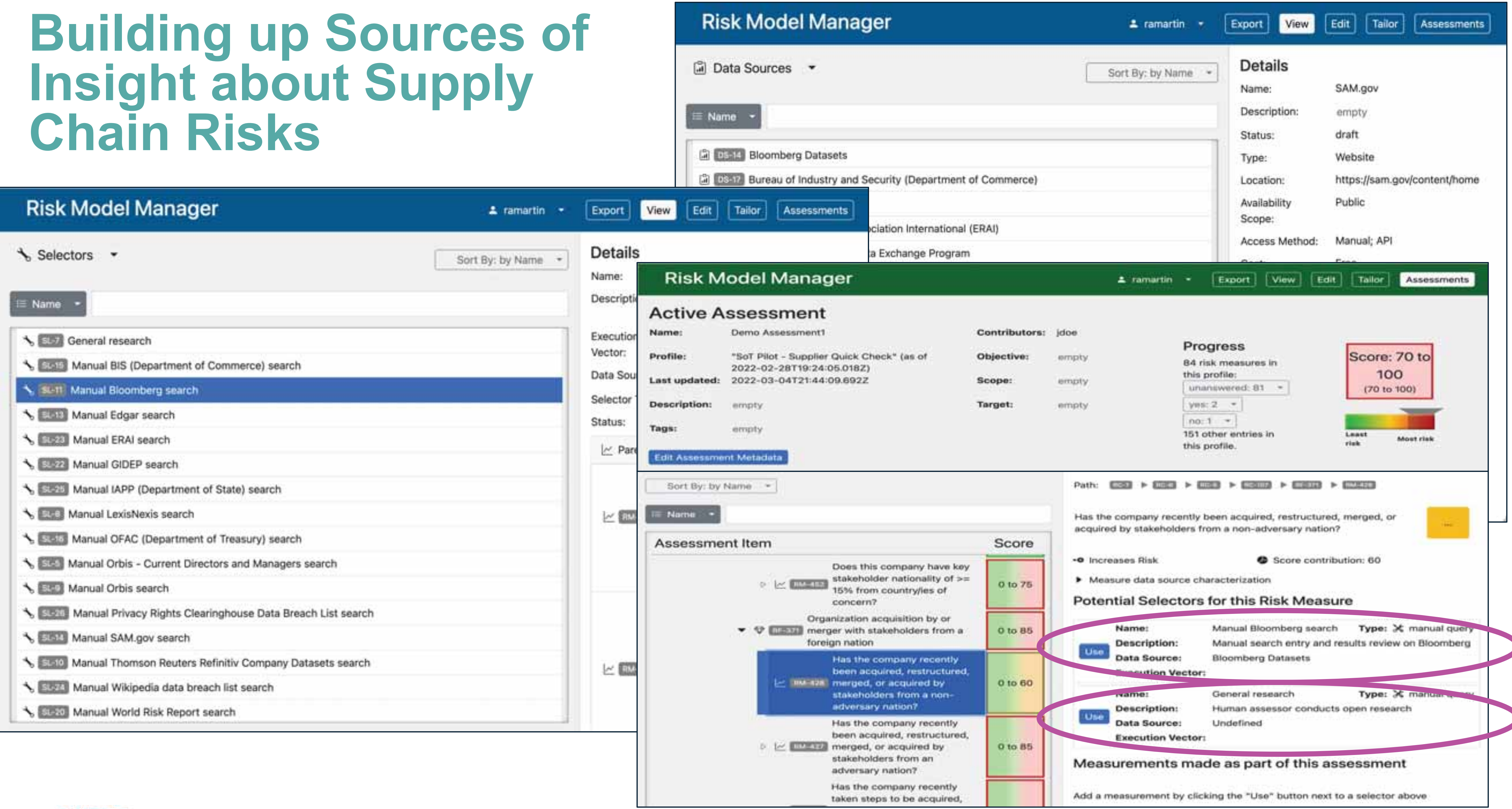
Pilots 1, 2, 4 & 5

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: 22-01488-10

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…

Risk Model Manager — ramartin — Export | View | Edit | Tailor | Assessments

Active Assessment

Name:	Demo Assessment1	Contributors:	jdoe
Profile:	"SoT Pilot - Supplier Quick Check" (as of 2022-02-28T19:24:05.018Z)	Objective:	empty
Last updated:	2022-03-04T21:44:09.692Z	Scope:	empty
Description:	empty	Target:	empty
Tags:	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)

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: [illegible] ▶ [illegible] ▶ [illegible] ▶ [illegible] ▶ [illegible] ▶ [illegible]

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:

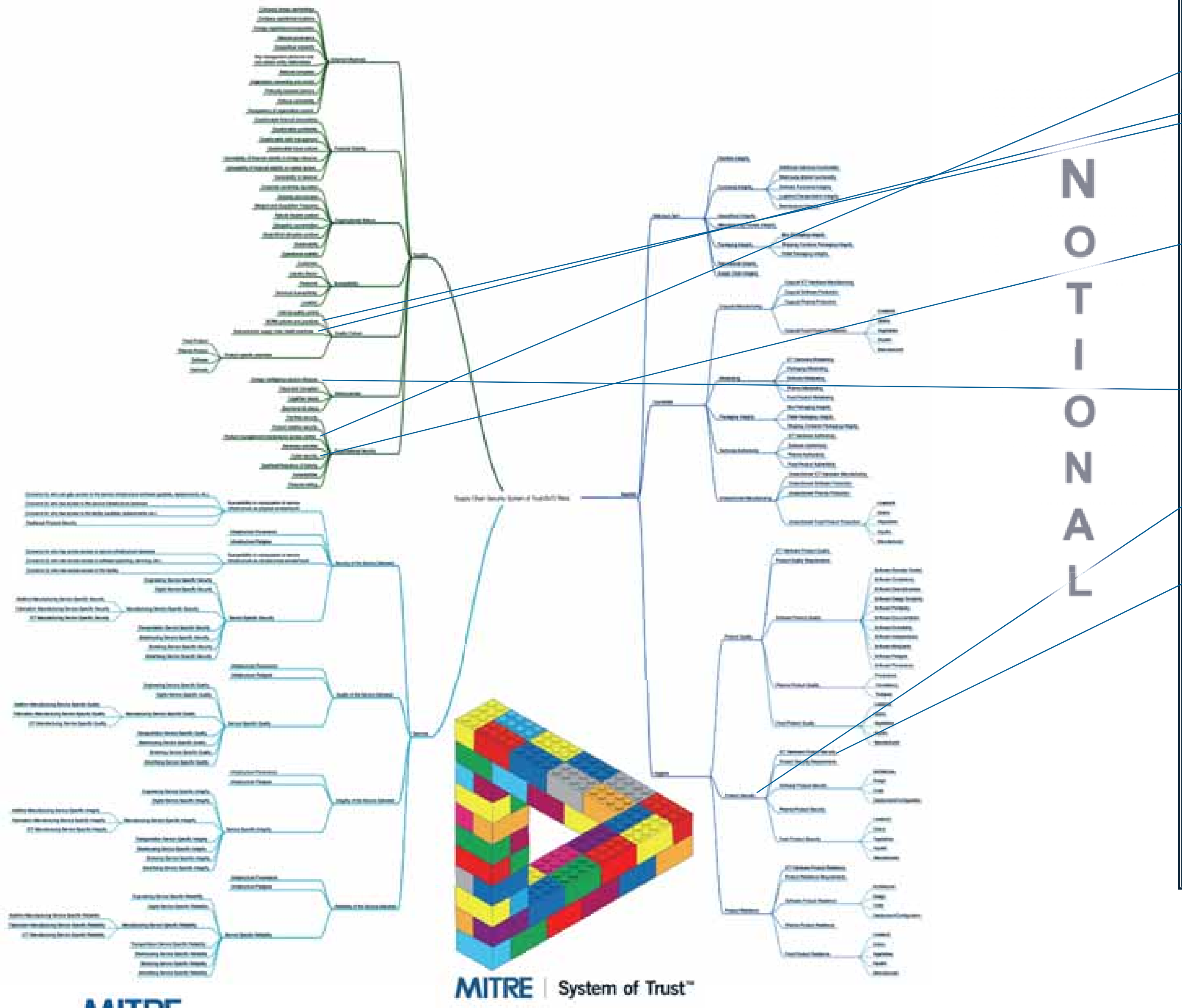
Use — Name: General research — Type: manual query
Description: Human assessor conducts open research
Data Source: Undefined
Execution Vector:

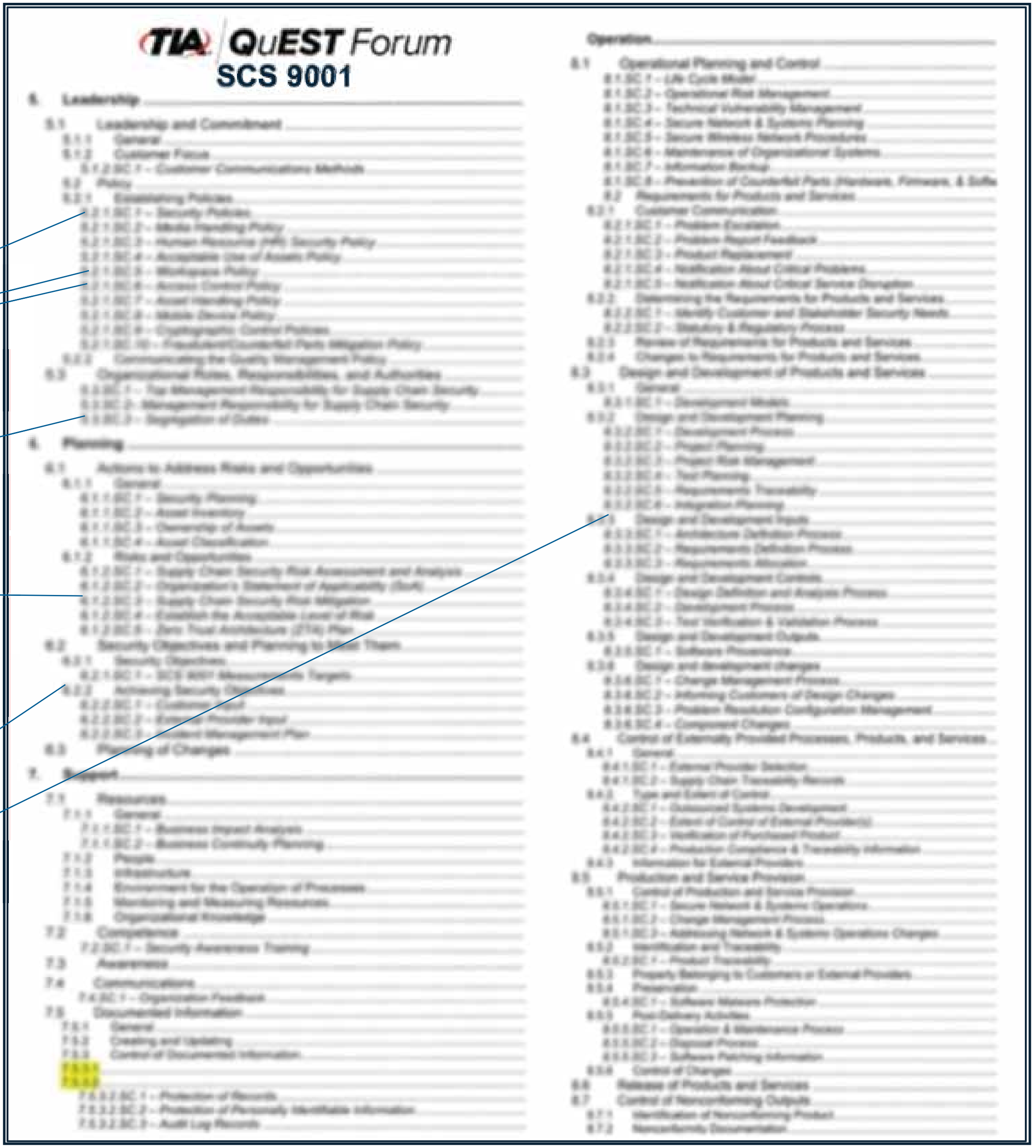
Measurements made as part of this assessment

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

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Mapping SoT Risks to Assessment Information Sources / Standards



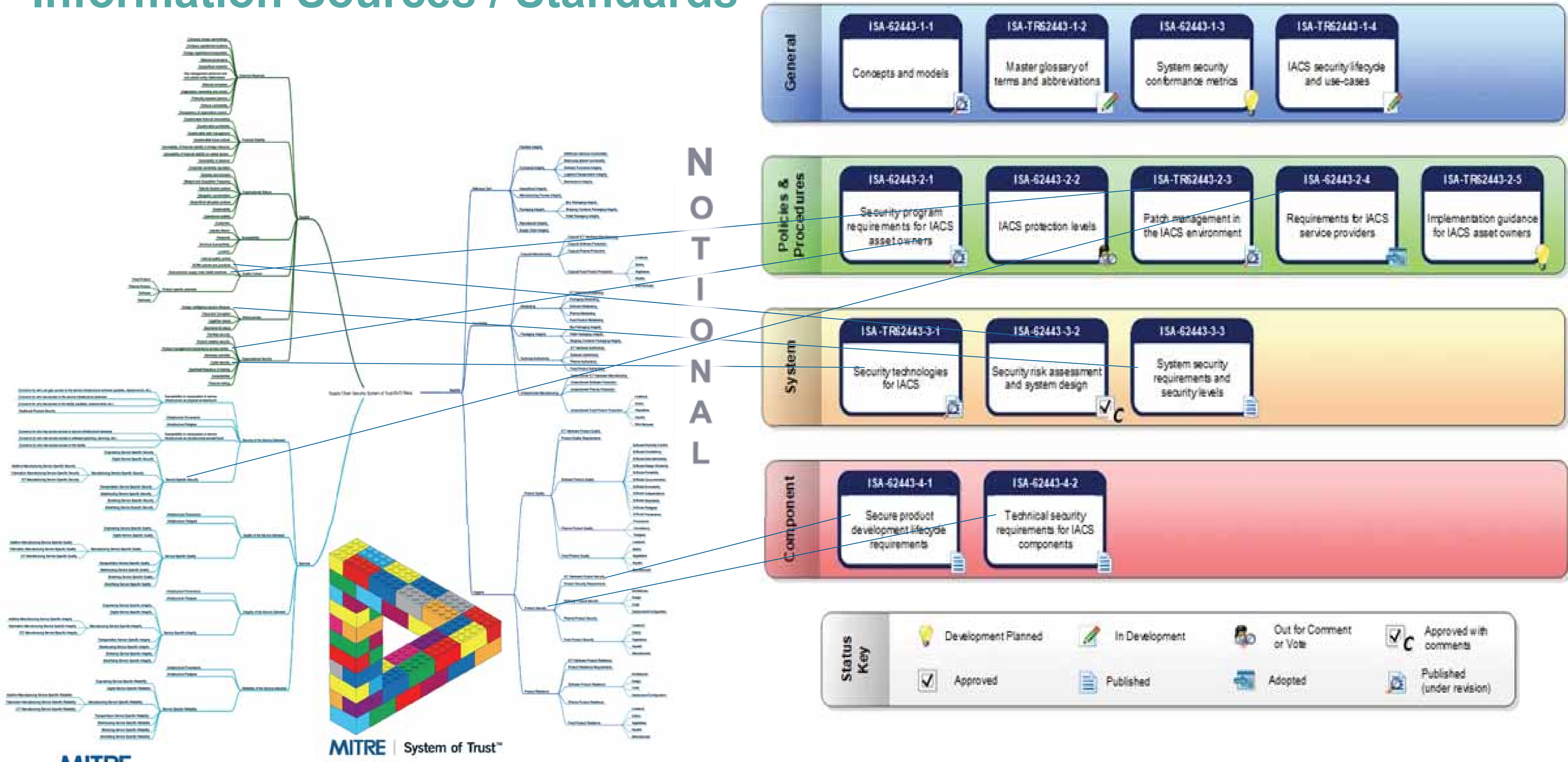


Along with DHS ICT SCRM Task Force Vendor Template, and others, …

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Mapping SoT Risks to Assessment Information Sources / Standards

ISA/IEC 62443



General	ISA-62443-1-1 Concepts and models	ISA-TR62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	ISA-62443-2-1 Security program requirements for IACS asset owners	ISA-62443-2-2 IACS protection levels	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Requirements for IACS service providers	ISA-TR62443-2-5 Implementation guidance for IACS asset owners
System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment and system design	ISA-62443-3-3 System security requirements and security levels		
Component	ISA-62443-4-1 Secure product development lifecycle requirements	ISA-62443-4-2 Technical security requirements for IACS components			

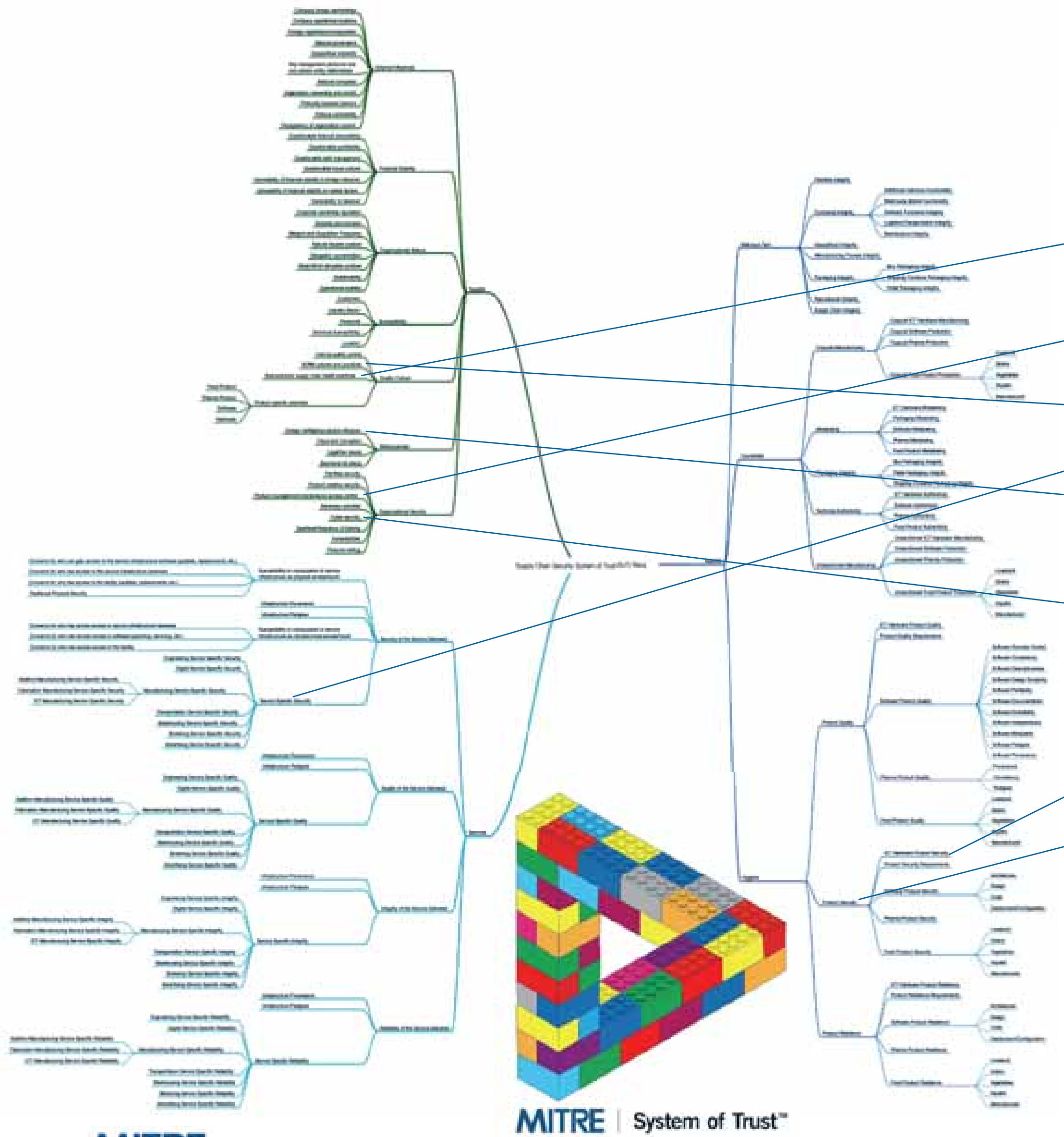
Status Key

- Development Planned
- In Development
- Out for Comment or Vote
- Approved with comments
- Approved
- Published
- Adopted
- Published (under revision)

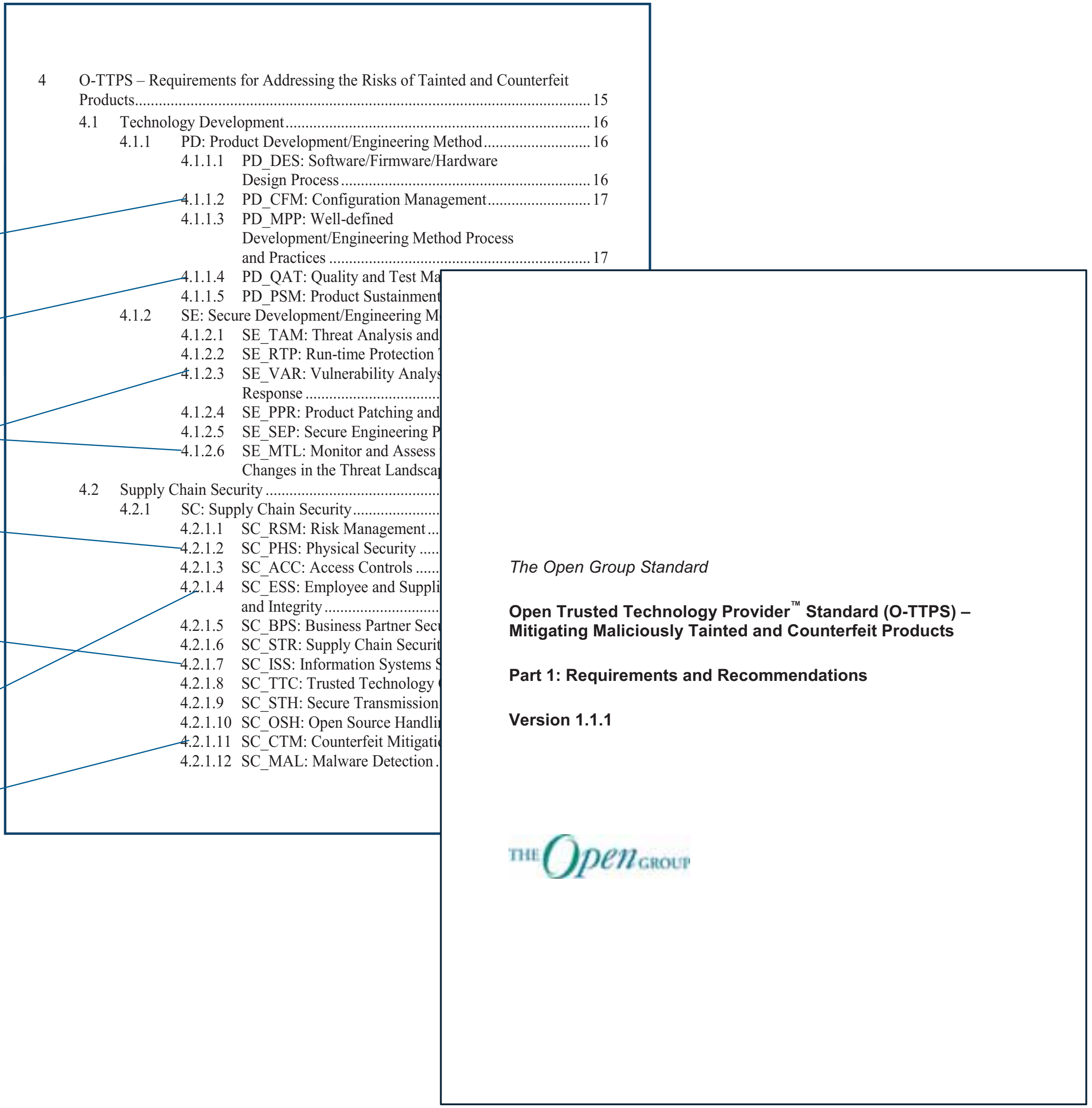
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Mapping SoT Risks to Assessment Information Sources / Standards

ISO/IEC 20243



NOTIONAL



The Open Group Standard

Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products

Part 1: Requirements and Recommendations

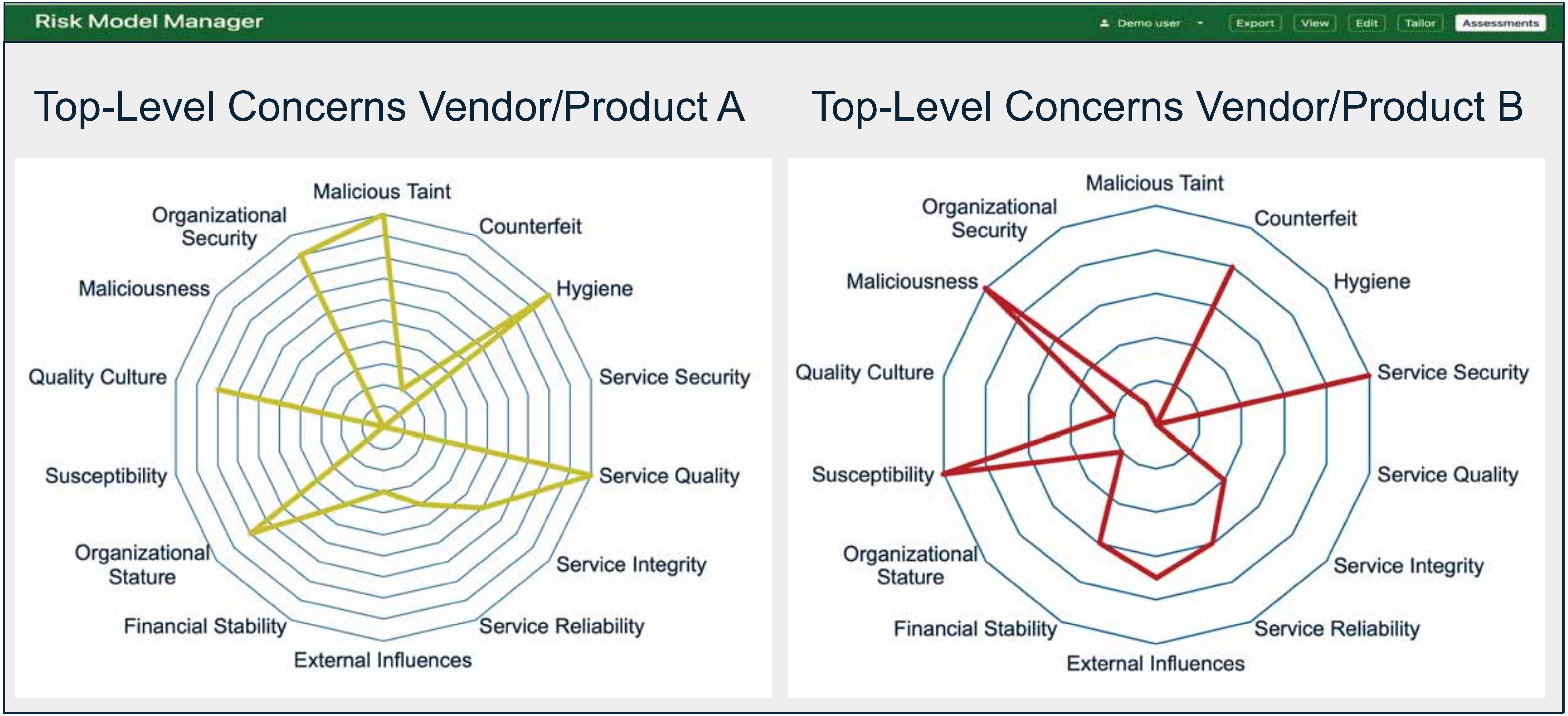
Version 1.1.1

THE Open GROUP

MITRE

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

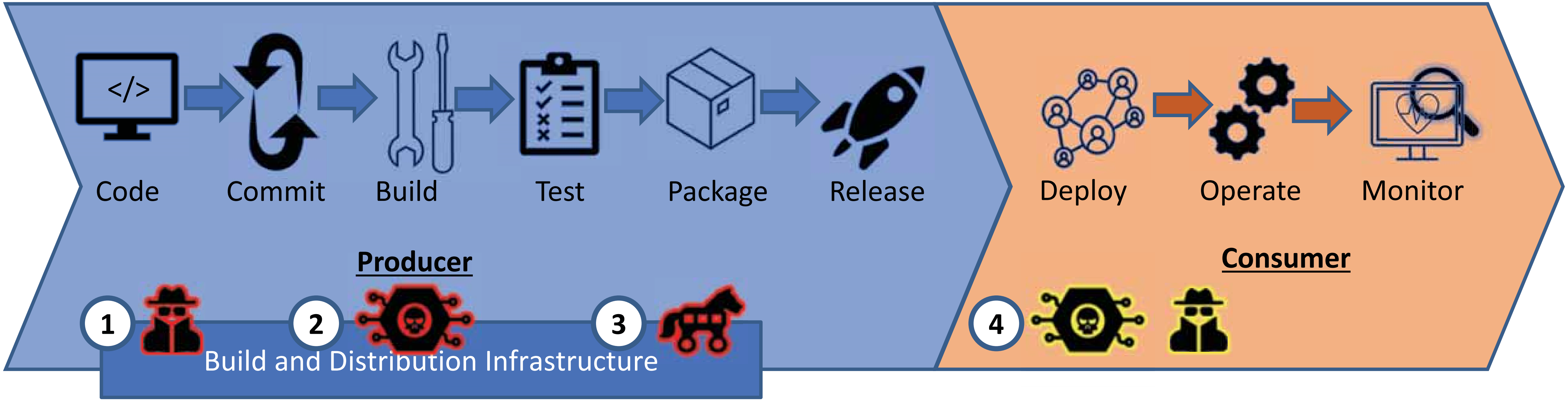
GOAL for use of SoT in Industry and Government…



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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: 22-01488-10

MITRE

DELIVER UNCOMPROMISED:
SECURING CRITICAL SOFTWARE
SUPPLY CHAINS

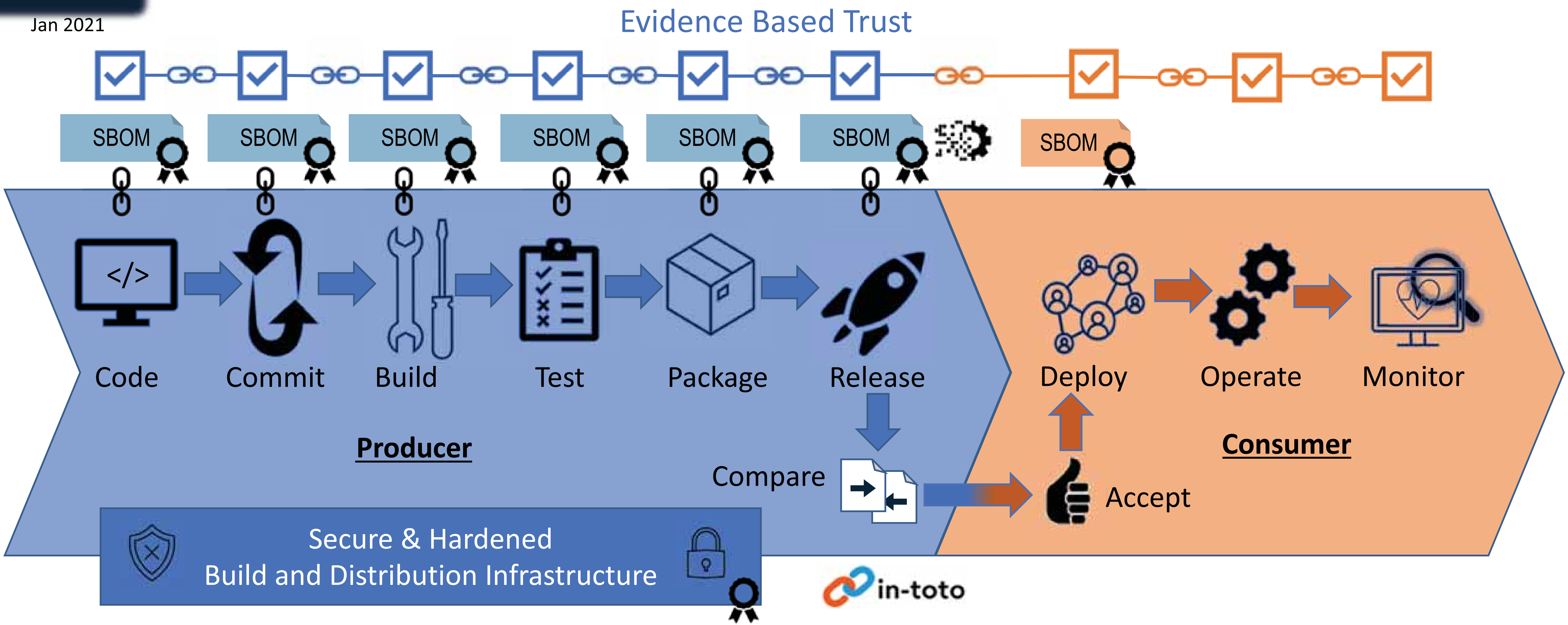
PROPOSAL TO ESTABLISH AN END-TO-END FRAMEWORK FOR SOFTWARE SUPPLY CHAIN INTEGRITY

by Charles Clancy, Joseph Ferraro, Robert Martin, Adam Pennington, Christopher Sledjeski, and Craig Wiener

© 2021 MITRE #21-XXXX 1-28-2021

Jan 2021

Software Supply Chain Integrity



Evidence Based Trust

SBOM

SBOM

SBOM

SBOM

SBOM

SBOM

SBOM

Code → Commit → Build → Test → Package → Release

Deploy → Operate → Monitor

Producer

Compare

Accept

Consumer

Secure & Hardened
Build and Distribution Infrastructure

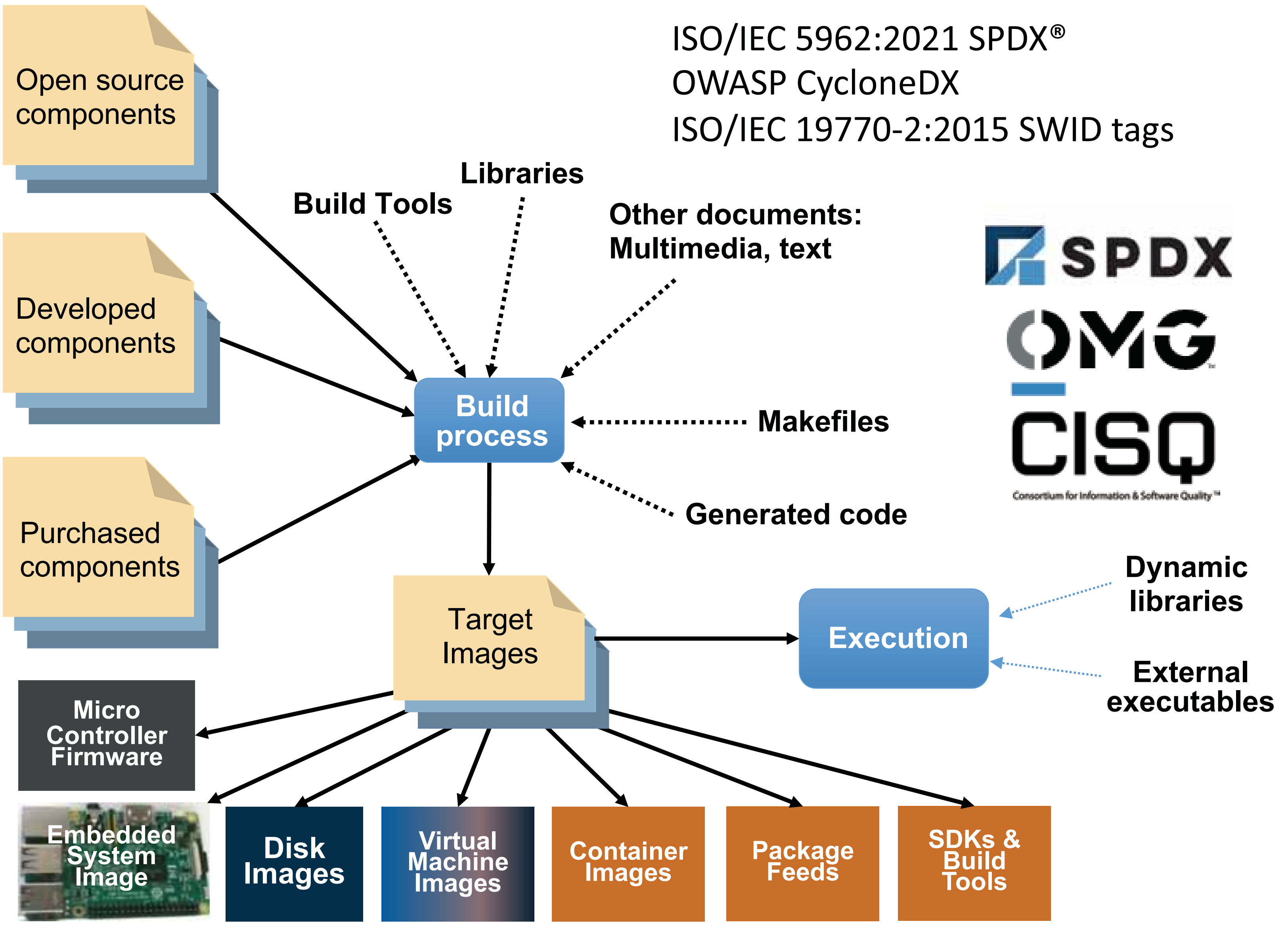
in-toto

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: 22-01488-10

Software Bill of Materials Standardization

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



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)

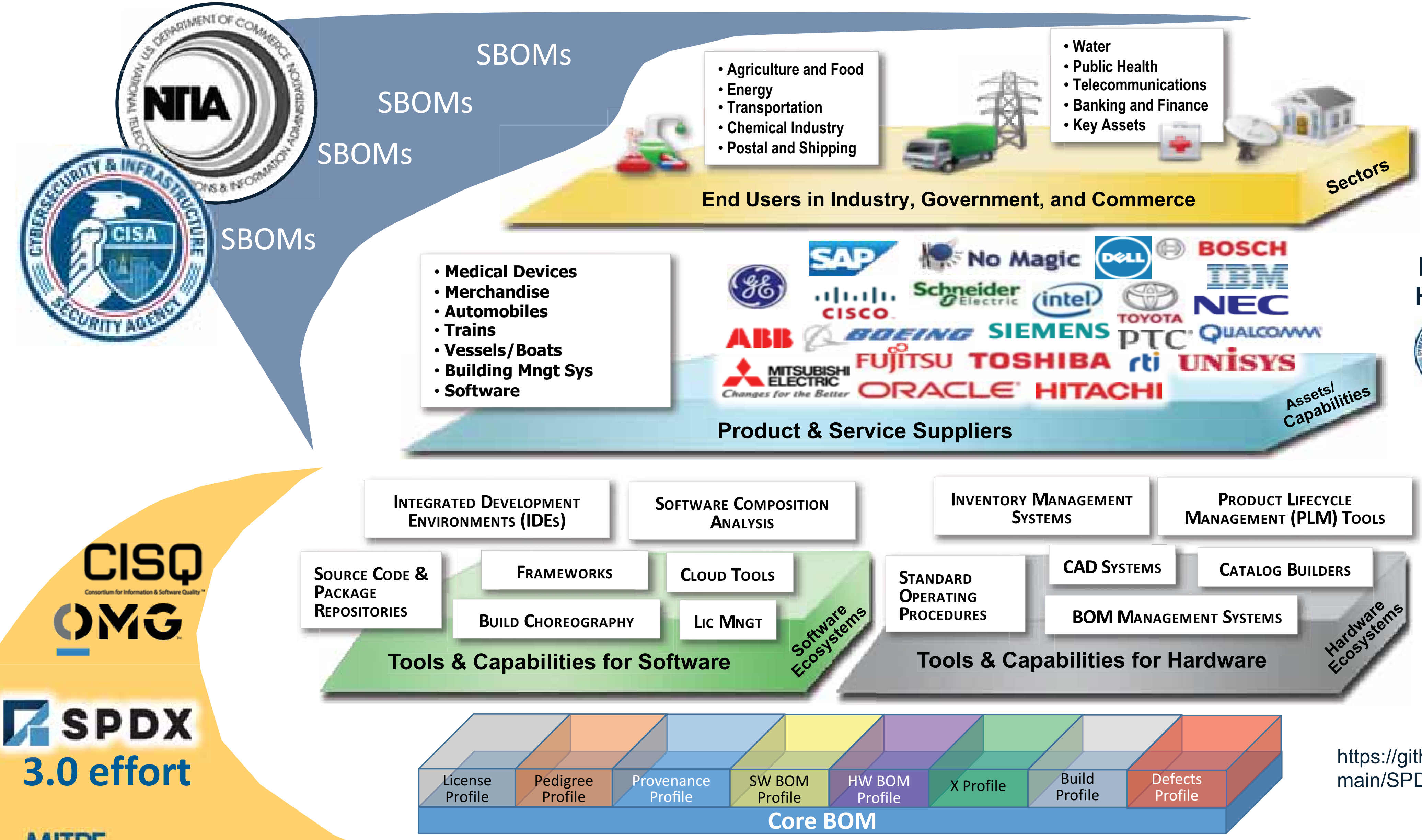
SBoM of a SW Service
(SBoM of sw delivering service)

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: 22-01488-10

Lowering Adoption Hurdles for SBOMs and more



- 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

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

Product & Service Suppliers

Integrated Development Environments (IDEs)

Software Composition Analysis

Source Code & Package Repositories

Frameworks

Cloud Tools

Build Choreography

Lic Mngt

Tools & Capabilities for Software

Inventory Management Systems

Product Lifecycle Management (PLM) Tools

Standard Operating Procedures

CAD Systems

Catalog Builders

BOM Management Systems

Tools & Capabilities for Hardware

License Profile | Pedigree Profile | Provenance Profile | SW BOM Profile | HW BOM Profile | X Profile | Build Profile | Defects Profile

Core BOM

3.0 effort

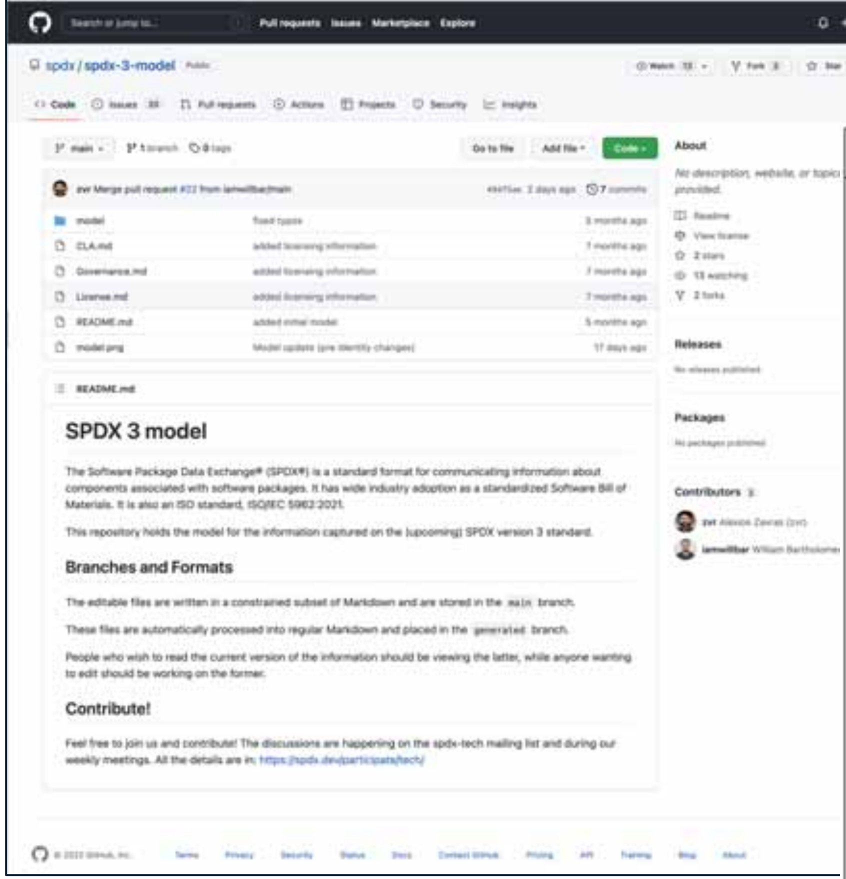
ICT SCRM Task Force HBOM Working Group

THE LINUX FOUNDATION

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: 22-01488-10

SPDX 3.0 effort



model	fixed typos	3 months ago
CLA.md	added licensing information	7 months ago
Governance.md	added licensing information	7 months ago
License.md	added licensing information	7 months ago
README.md	added initial model	5 months ago
model.png	Model update (pre identity changes)	17 days ago

README.md

SPDX 3 model

The Software Package Data Exchange® (SPDX®) is a standard format for communicating information about components associated with software packages. It has wide industry adoption as a standardized Software Bill of Materials. It is also an ISO standard, ISO/IEC 5962:2021.

This repository holds the model for the information captured on the (upcoming) SPDX version 3 standard.

Branches and Formats

The editable files are written in a constrained subset of Markdown and are stored in the `main` branch.

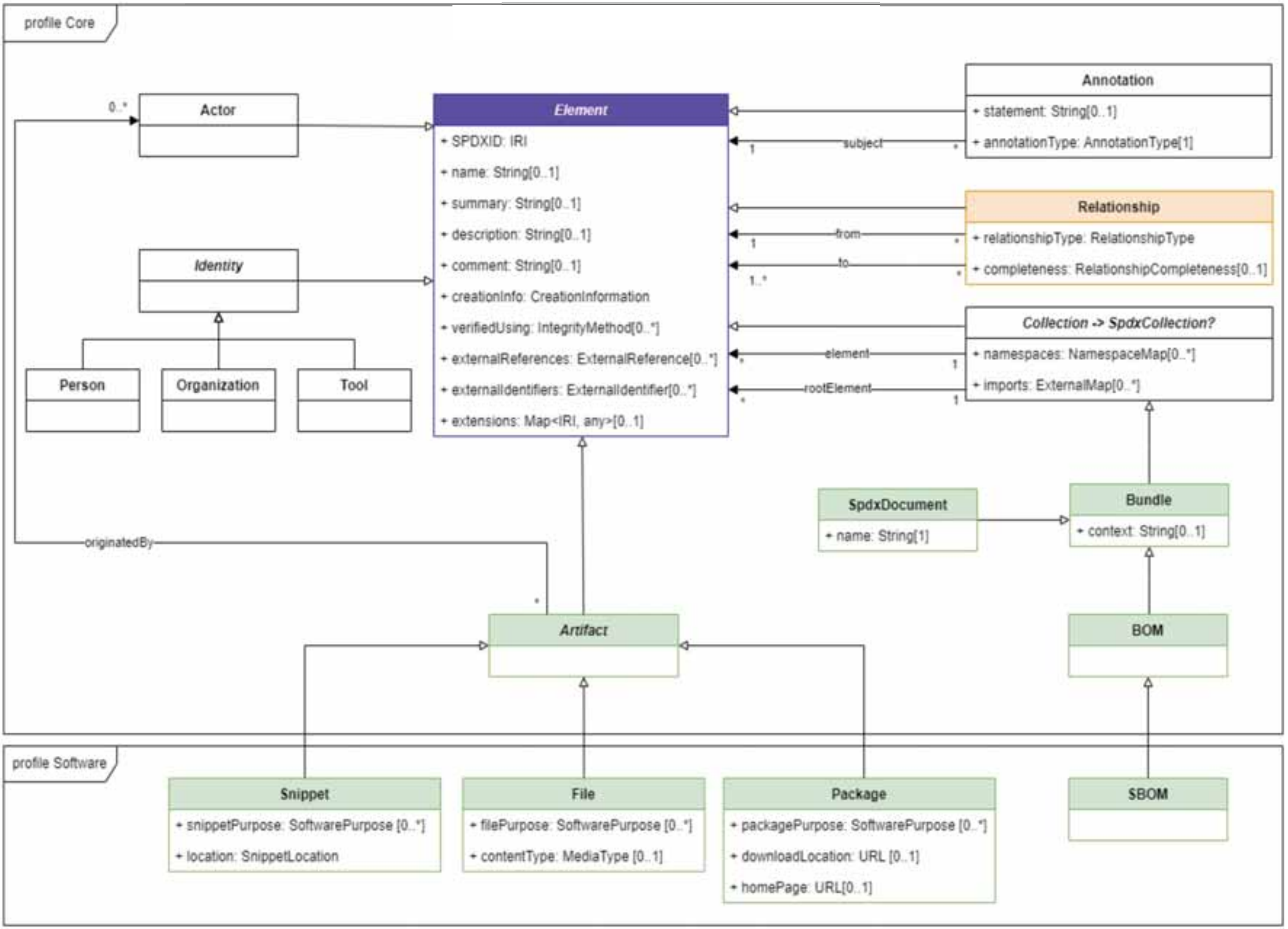
These files are automatically processed into regular Markdown and placed in the `generated` branch.

People who wish to read the current version of the information should be viewing the latter, while anyone wanting to edit should be working on the former.

Contribute!

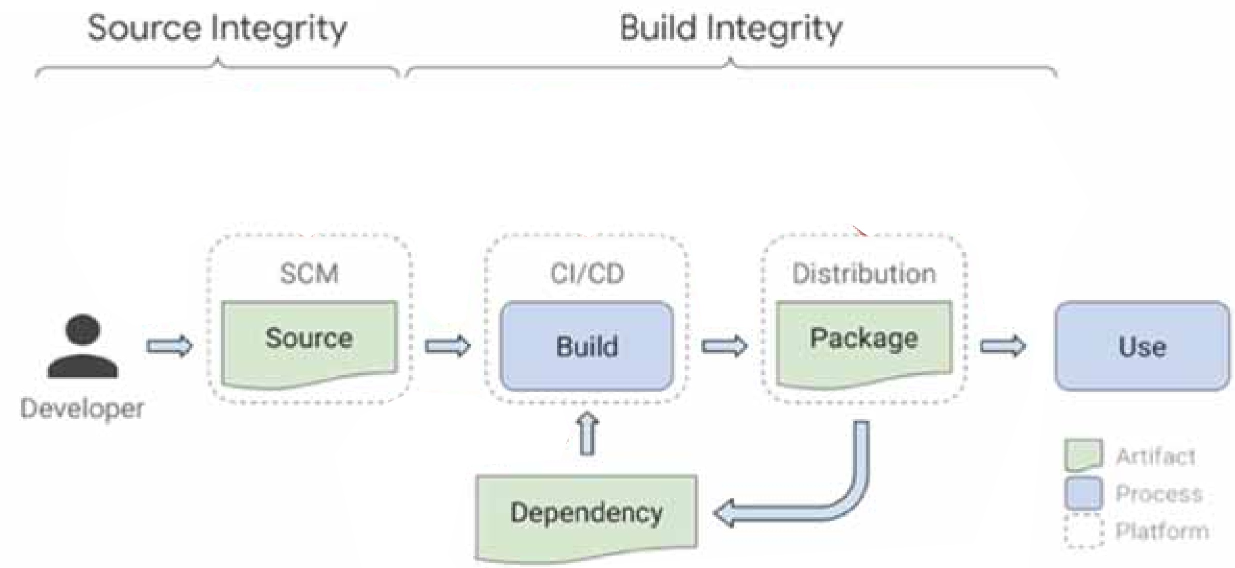
Feel free to join us and contribute! The discussions are happening on the spdx-tech mailing list and during our weekly meetings. All the details are in: https://spdx.dev/participate/tech/

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


profile Core
Actor
0..*
Identity
Person
Organization
Tool
Element
+ SPDXID: IRI
+ name: String[0..1]
+ summary: String[0..1]
+ description: String[0..1]
+ comment: String[0..1]
+ creationInfo: CreationInformation
+ verifiedUsing: IntegrityMethod[0..*]
+ externalReferences: ExternalReference[0..*]
+ externalIdentifiers: ExternalIdentifier[0..*]
+ extensions: Map<IRI, any>[0..1]
Annotation
+ statement: String[0..1]
+ annotationType: AnnotationType[1]
subject
1
*
Relationship
+ relationshipType: RelationshipType
+ completeness: RelationshipCompleteness[0..1]
from
to
1
1..*
*
Collection -> SpdxCollection?
+ namespaces: NamespaceMap[0..*]
+ imports: ExternalMap[0..*]
element
rootElement
SpdxDocument
+ name: String[1]
Bundle
+ context: String[0..1]
BOM
originatedBy
Artifact
profile Software
Snippet
+ snippetPurpose: SoftwarePurpose [0..*]
+ location: SnippetLocation
File
+ filePurpose: SoftwarePurpose [0..*]
+ contentType: MediaType [0..1]
Package
+ packagePurpose: SoftwarePurpose [0..*]
+ downloadLocation: URL [0..1]
+ homePage: URL[0..1]
SBOM

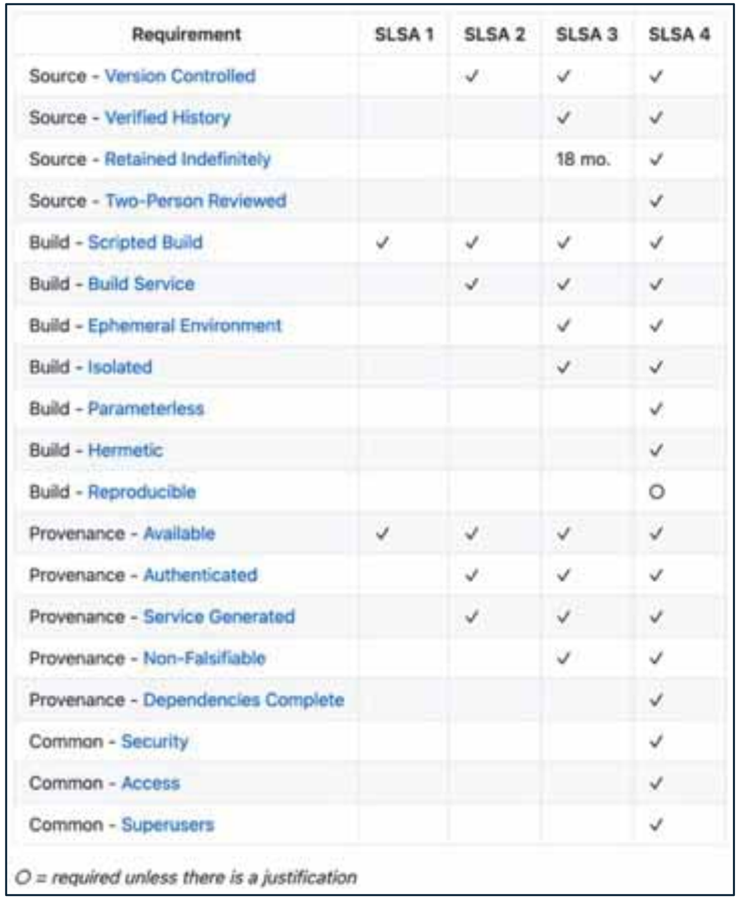
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply-chain Levels for Software Artifacts (SLSA)



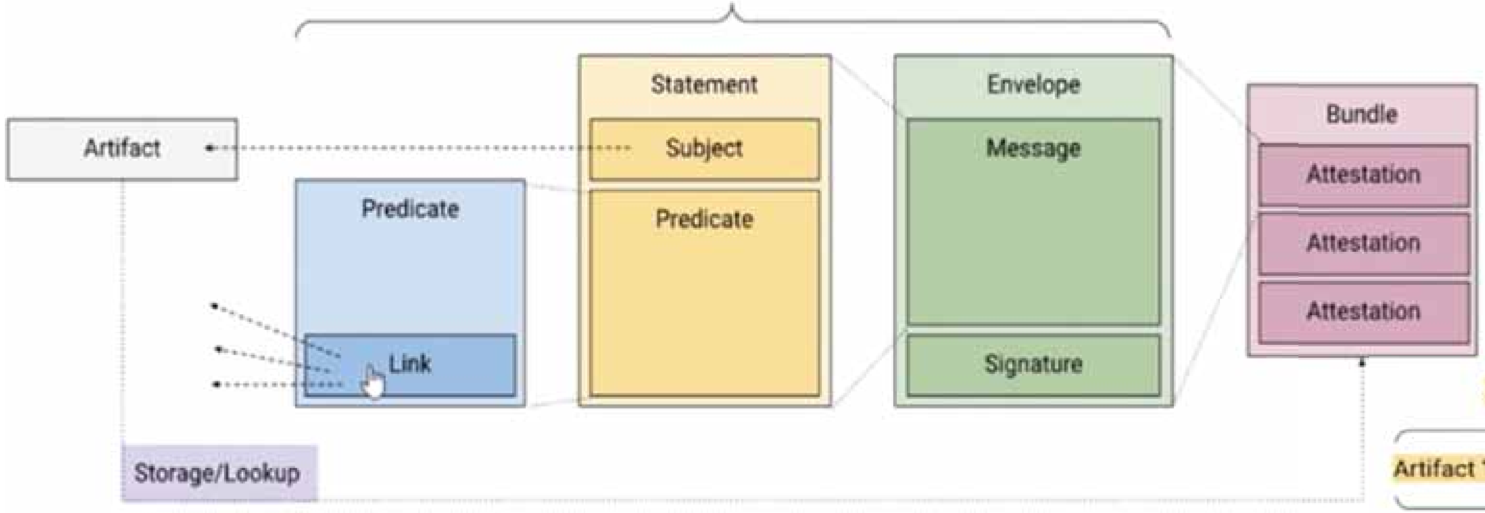
SLSA guidelines have 4 levels of incremental and actionable things that software producers can claim to do to protect against specific integrity attacks

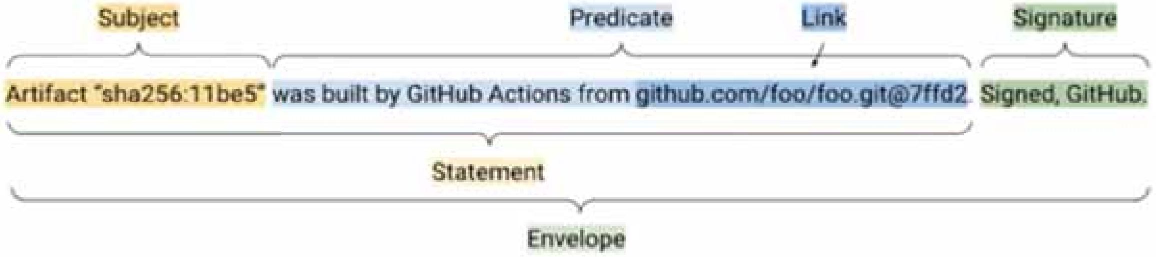
https://github.com/slsa-framework/slsa



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				✓

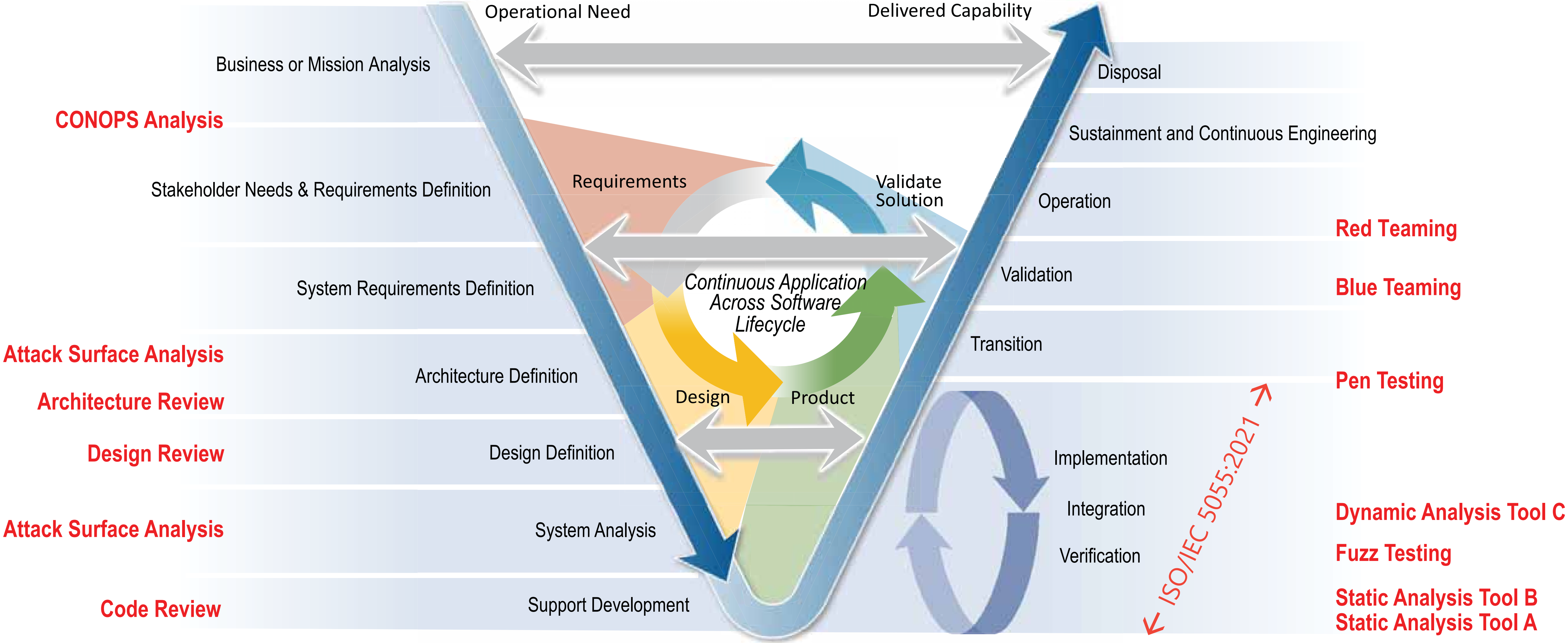
○ = required unless there is a justification




Subject
Predicate
Link
Signature
Artifact "sha256:11be5" was built by GitHub Actions from github.com/foo/foo.git@7ffd2. Signed, GitHub.
Statement
Envelope

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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: 22-01488-10

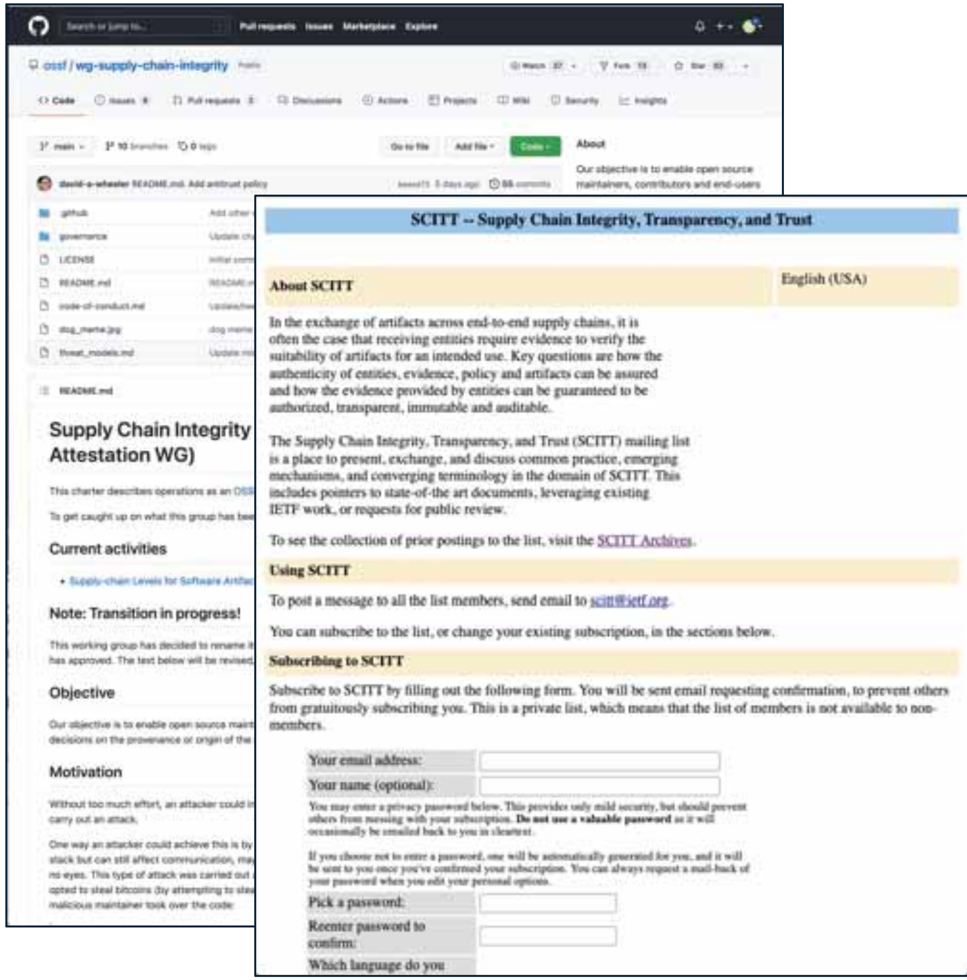
Supply Chain Integrity Transparency and Trust (SCITT) IETF Working Group Formed (July 2022)

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.



About

Our objective is to enable open source maintainers, contributors and end-users

david-a-wheeler README.md: Add antitrust policy

Supply Chain Integrity Attestation WG)

This charter describes operations as an OSS

To get caught up on what this group has bee

Current activities

- Supply-chain Levels for Software Artifac

Note: Transition in progress!

This working group has decided to rename it has approved. The text below will be revised,

Objective

Our objective is to enable open source maint decisions on the provenance or origin of the

Motivation

Without too much effort, an attacker could in carry out an attack.

One way an attacker could achieve this is by stack but can still affect communication, may no eyes. This type of attack was carried out opted to steal bitcoins (by attempting to stea malicious maintainer took over the code:

SCITT -- Supply Chain Integrity, Transparency, and Trust

About SCITT

In the exchange of artifacts across end-to-end supply chains, it is often the case that receiving entities require evidence to verify the suitability of artifacts for an intended use. Key questions are how the authenticity of entities, evidence, policy and artifacts can be assured and how the evidence provided by entities can be guaranteed to be authorized, transparent, immutable and auditable.

The Supply Chain Integrity, Transparency, and Trust (SCITT) mailing list is a place to present, exchange, and discuss common practice, emerging mechanisms, and converging terminology in the domain of SCITT. This includes pointers to state-of-the art documents, leveraging existing IETF work, or requests for public review.

To see the collection of prior postings to the list, visit the SCITT Archives.

Using SCITT

To post a message to all the list members, send email to scitt@ietf.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to SCITT

Subscribe to SCITT by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a private list, which means that the list of members is not available to non-members.

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

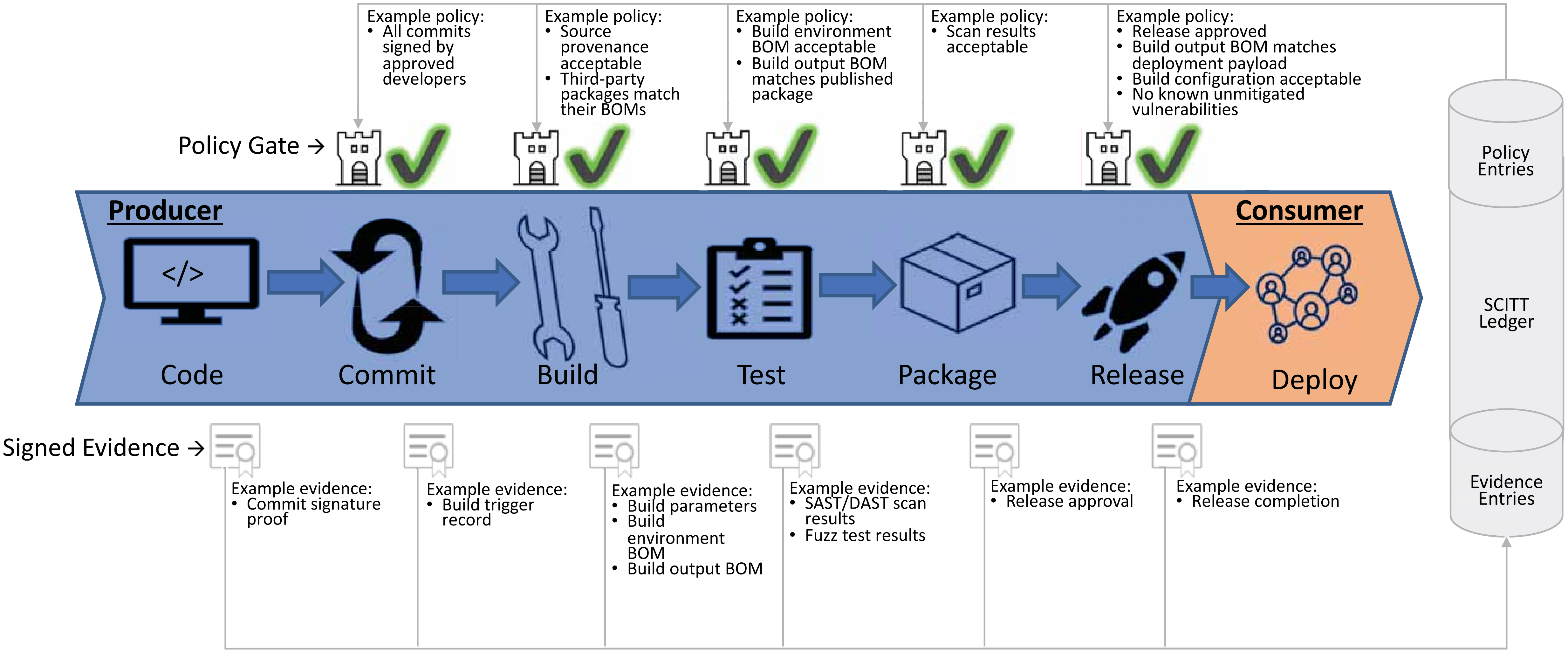
If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options.

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: 22-01488-10

Example of Applying SCITT in SW Development



Policy Gate →

Example policy:
- All commits signed by approved developers

Example policy:
- Source provenance acceptable
- Third-party packages match their BOMs

Example policy:
- Build environment BOM acceptable
- Build output BOM matches published package

Example policy:
- Scan results acceptable

Example policy:
- Release approved
- Build output BOM matches deployment payload
- Build configuration acceptable
- No known unmitigated vulnerabilities

Producer

Code

Commit

Build

Test

Package

Release

Consumer

Deploy

Signed Evidence →

Example evidence:
- Commit signature proof

Example evidence:
- Build trigger record

Example evidence:
- Build parameters
- Build environment BOM
- Build output BOM

Example evidence:
- SAST/DAST scan results
- Fuzz test results

Example evidence:
- Release approval

Example evidence:
- Release completion

Policy Entries

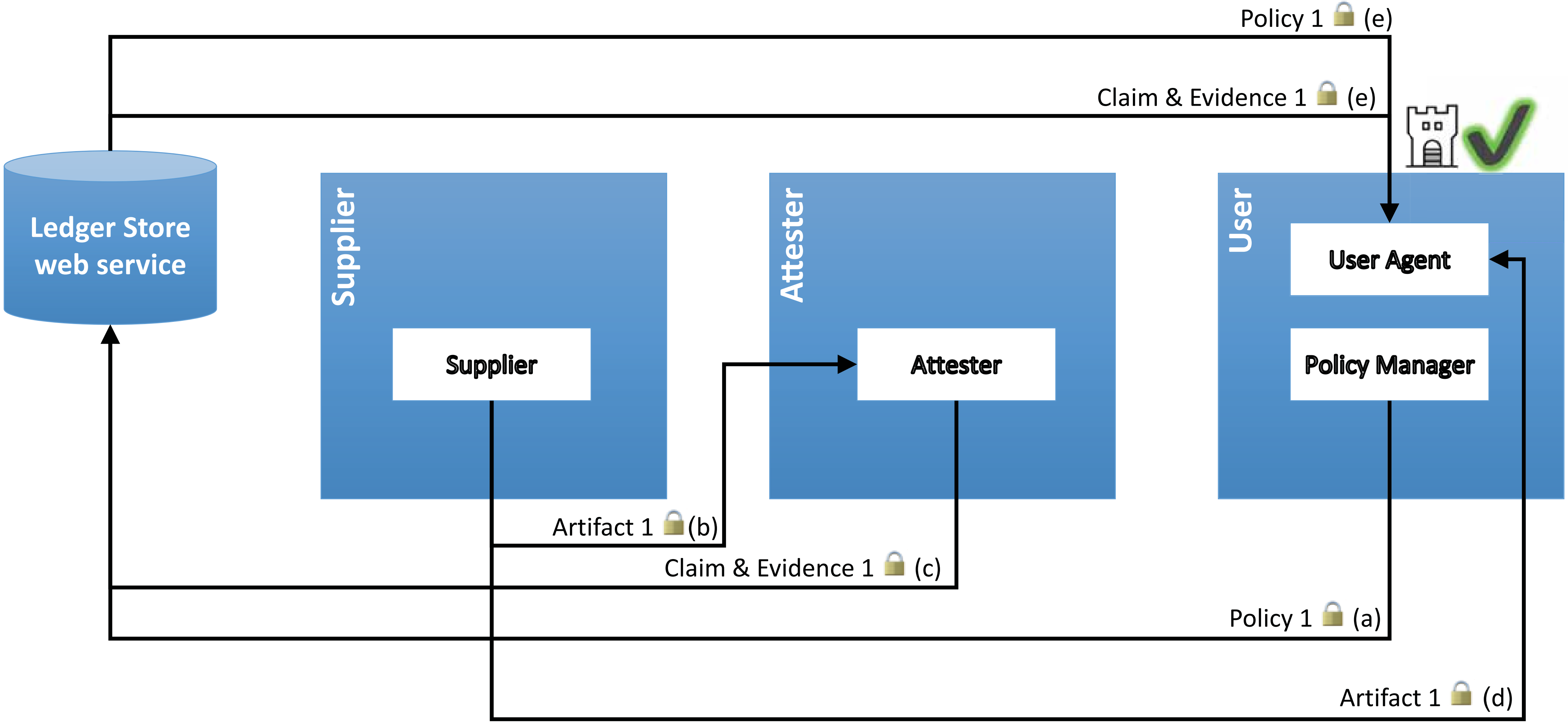
SCITT Ledger

Evidence Entries

MITRE

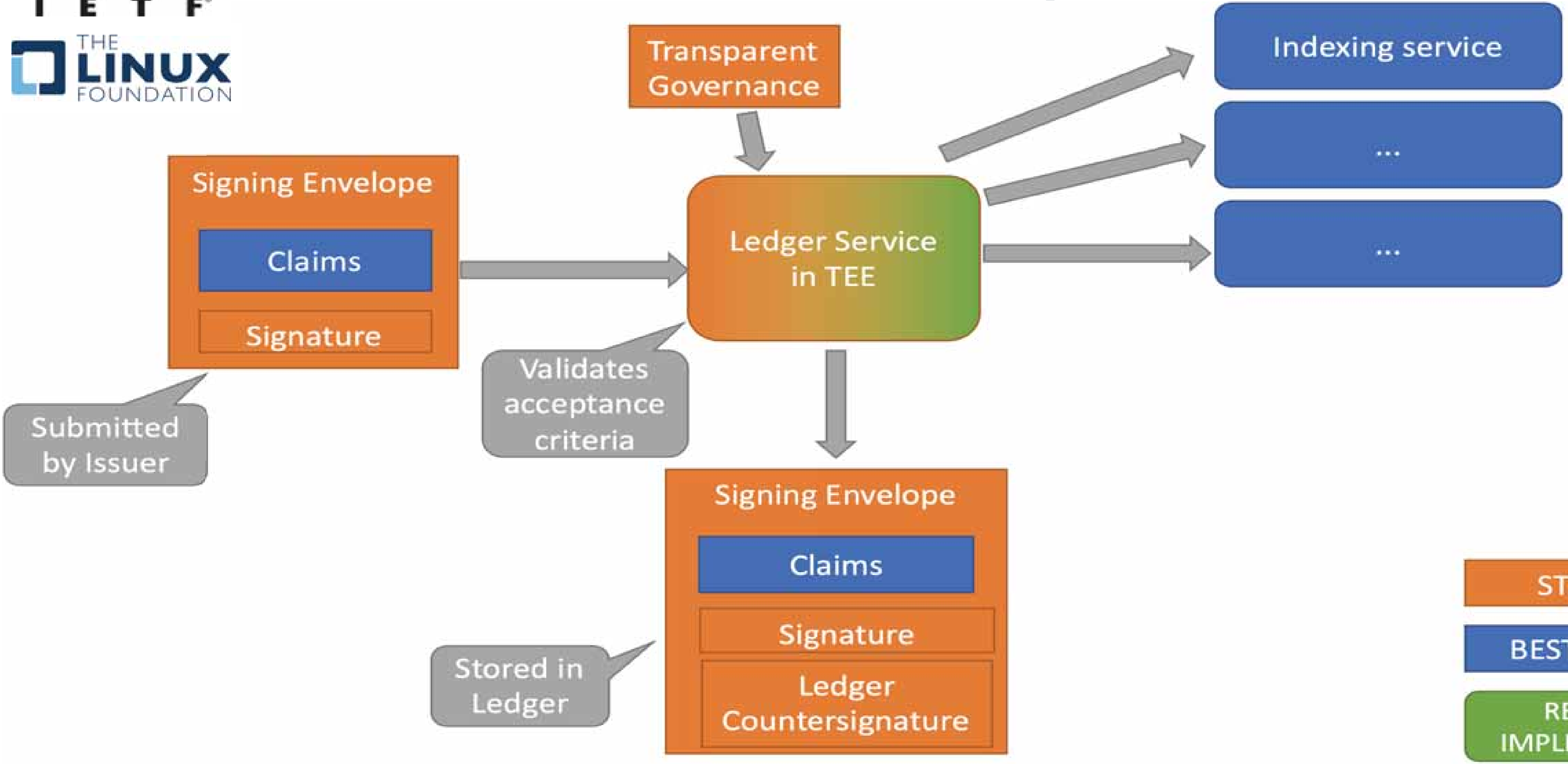
© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Example of SCITT in the Marketplace



© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

SCITT Concepts



STANDARD

BEST PRACTICE

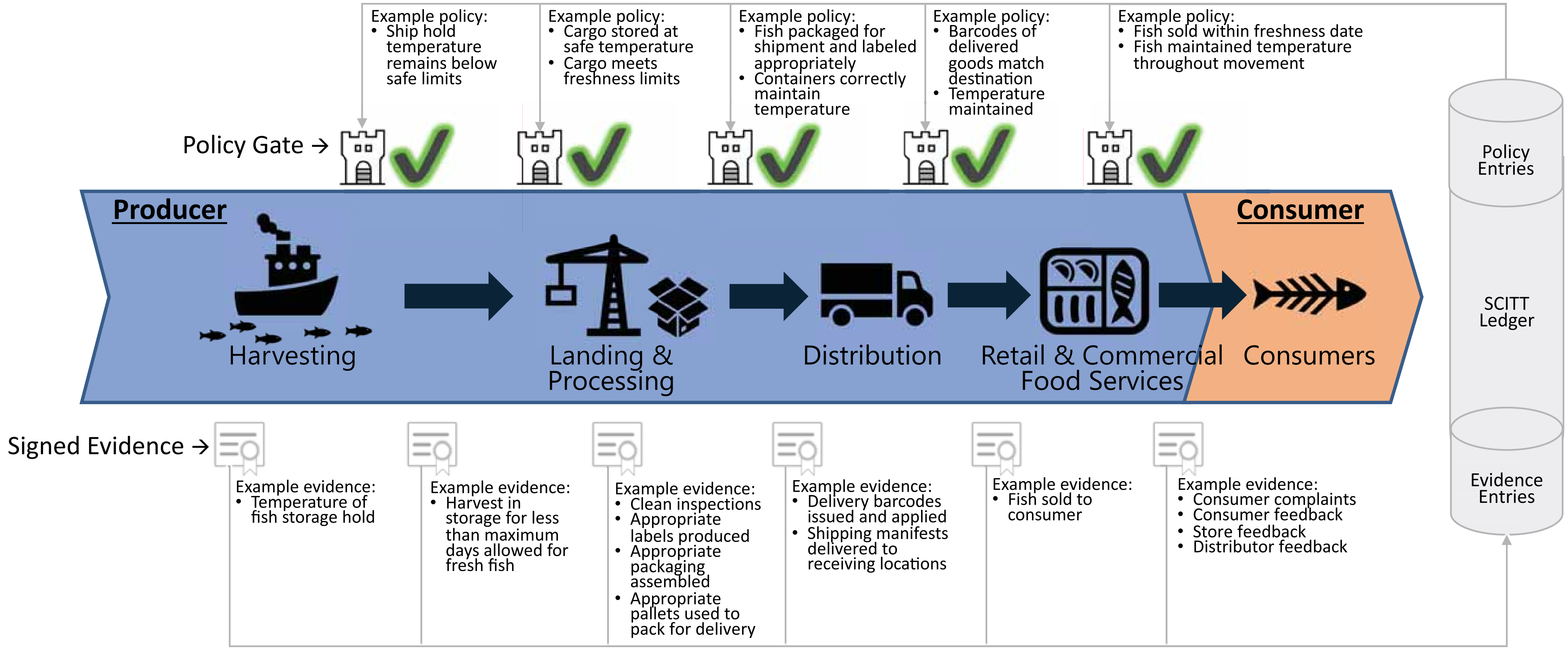
REFERENCE IMPLEMENTATION

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: 22-01488-10

Example of Applying SCITT in Harvesting Fish



Example policy:
- Ship hold temperature remains below safe limits

Example policy:
- Cargo stored at safe temperature
- Cargo meets freshness limits

Example policy:
- Fish packaged for shipment and labeled appropriately
- Containers correctly maintain temperature

Example policy:
- Barcodes of delivered goods match destination
- Temperature maintained

Example policy:
- Fish sold within freshness date
- Fish maintained temperature throughout movement

Example evidence:
- Temperature of fish storage hold

Example evidence:
- Harvest in storage for less than maximum days allowed for fresh fish

Example evidence:
- Clean inspections
- Appropriate labels produced
- Appropriate packaging assembled
- Appropriate pallets used to pack for delivery

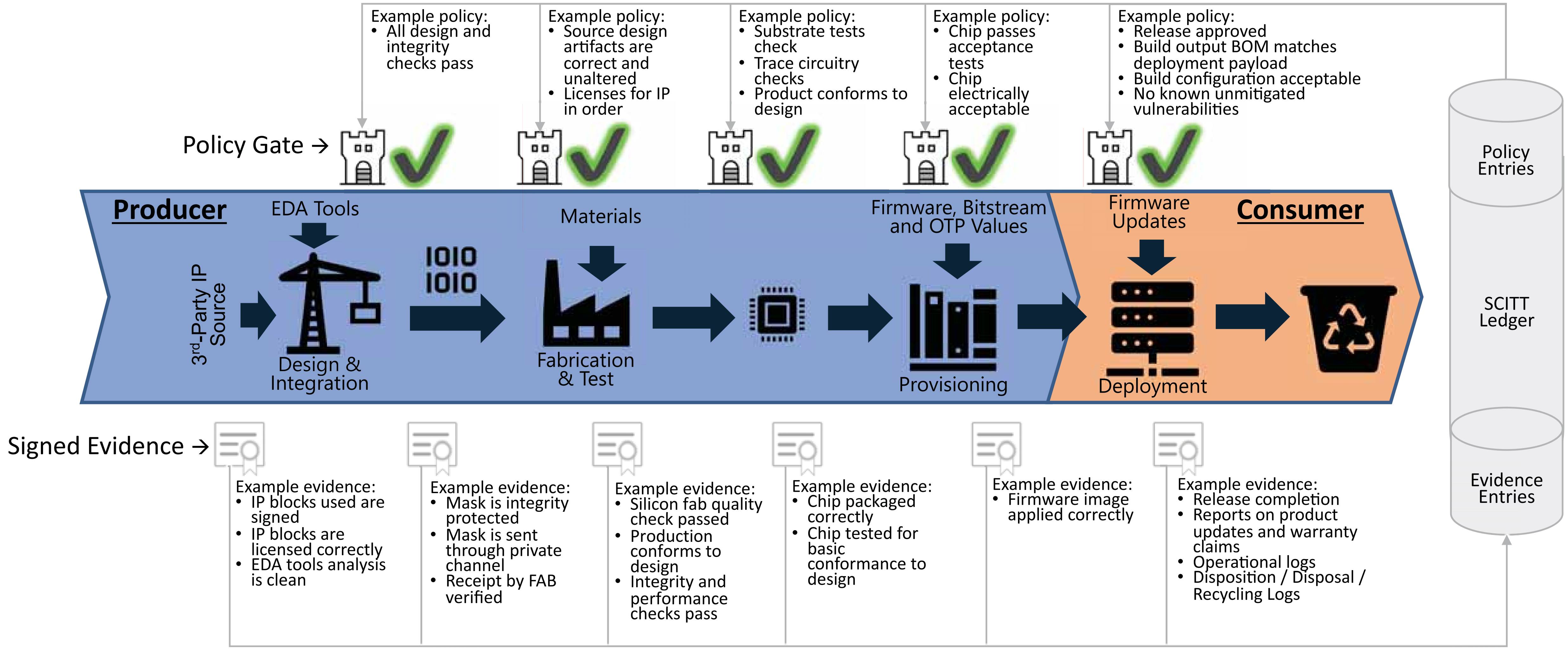
Example evidence:
- Delivery barcodes issued and applied
- Shipping manifests delivered to receiving locations

Example evidence:
- Fish sold to consumer

Example evidence:
- Consumer complaints
- Consumer feedback
- Store feedback
- Distributor feedback

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Example of Applying SCITT in Chip Development



Example policy:
- All design and integrity checks pass

Example policy:
- Source design artifacts are correct and unaltered
- Licenses for IP in order

Example policy:
- Substrate tests check
- Trace circuitry checks
- Product conforms to design

Example policy:
- Chip passes acceptance tests
- Chip electrically acceptable

Example policy:
- Release approved
- Build output BOM matches deployment payload
- Build configuration acceptable
- No known unmitigated vulnerabilities

Policy Gate →

Producer

3rd-Party IP Source

EDA Tools

Design & Integration

Materials

Fabrication & Test

Firmware, Bitstream and OTP Values

Provisioning

Firmware Updates

Consumer

Deployment

Policy Entries

SCITT Ledger

Evidence Entries

Signed Evidence →

Example evidence:
- IP blocks used are signed
- IP blocks are licensed correctly
- EDA tools analysis is clean

Example evidence:
- Mask is integrity protected
- Mask is sent through private channel
- Receipt by FAB verified

Example evidence:
- Silicon fab quality check passed
- Production conforms to design
- Integrity and performance checks pass

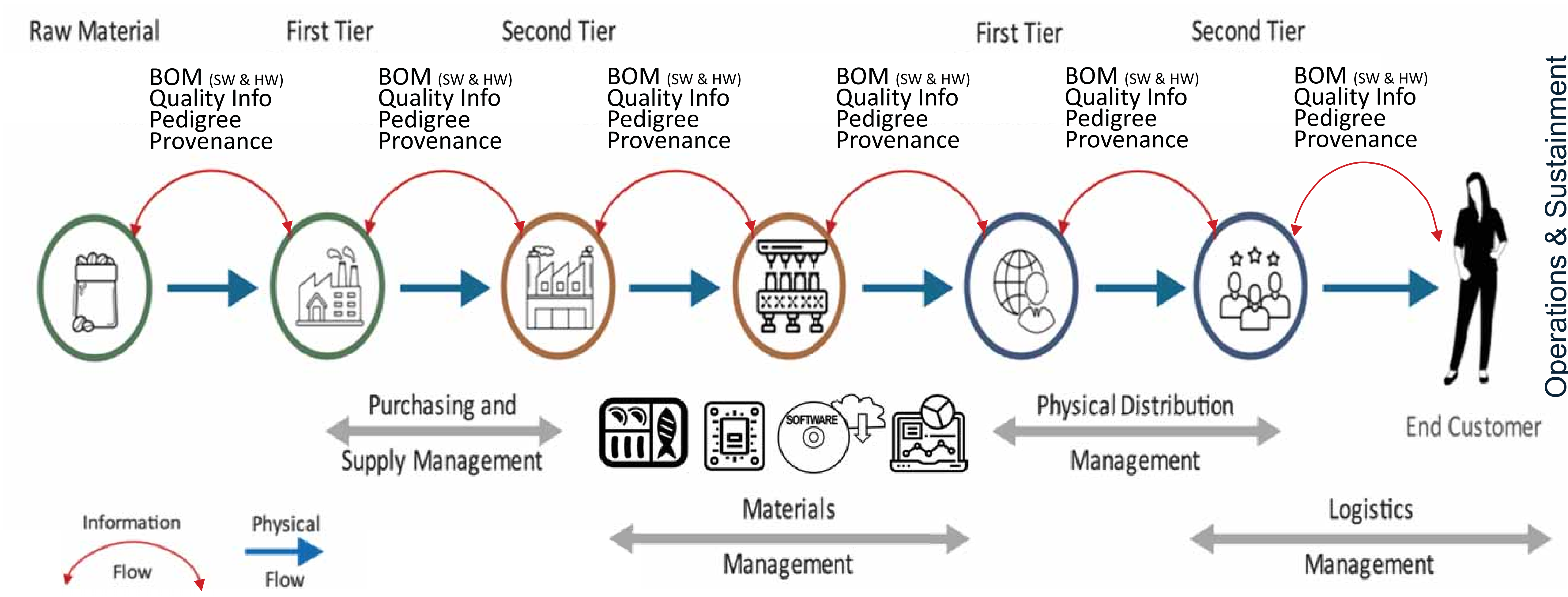
Example evidence:
- Chip packaged correctly
- Chip tested for basic conformance to design

Example evidence:
- Firmware image applied correctly

Example evidence:
- Release completion
- Reports on product updates and warranty claims
- Operational logs
- Disposition / Disposal / Recycling Logs

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Supply Chains – As multi-Stakeholder Network

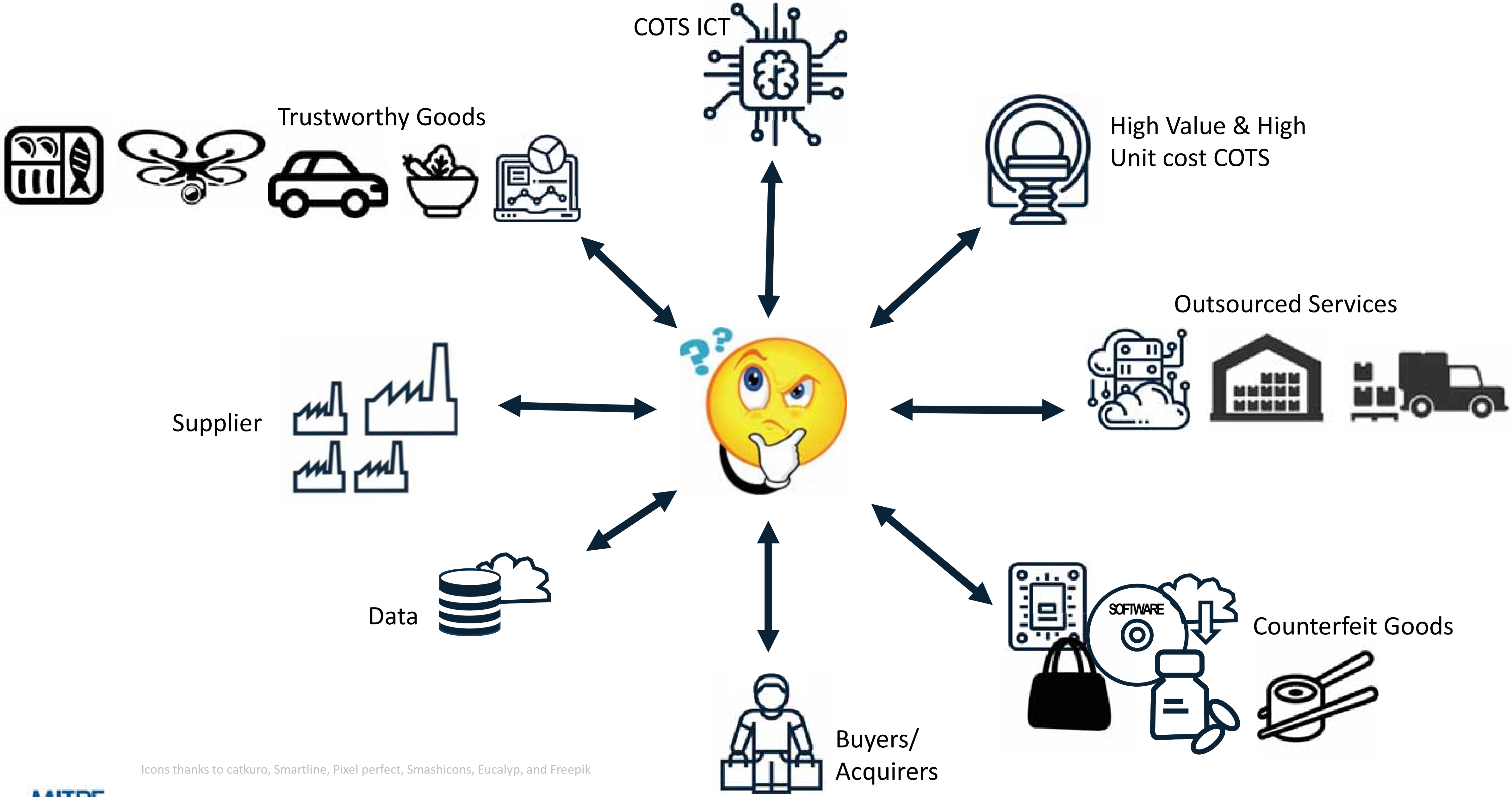


Operations & Sustainment

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

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

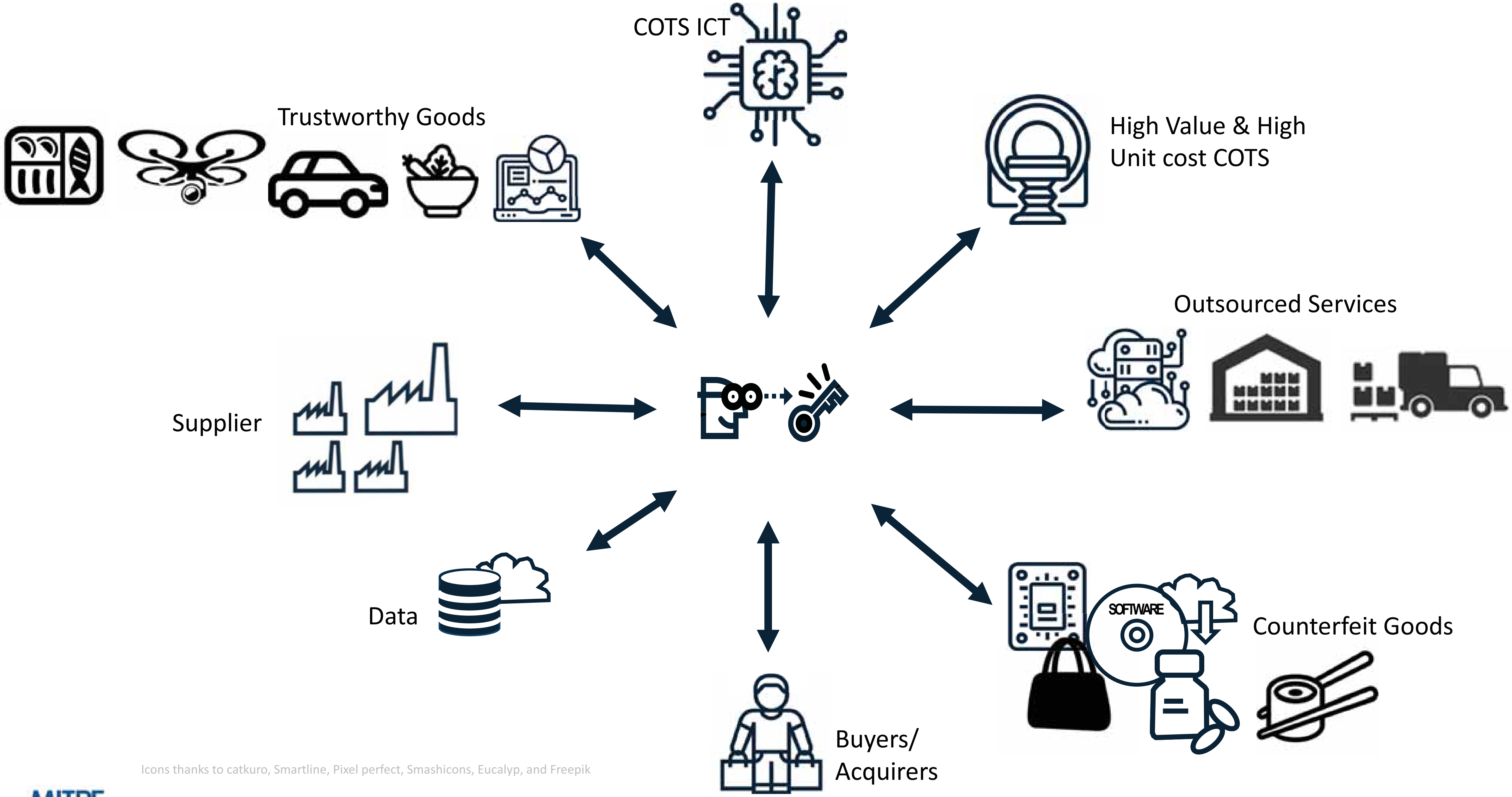
Effective Supply Chain Trust Interactions



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: 22-01488-10

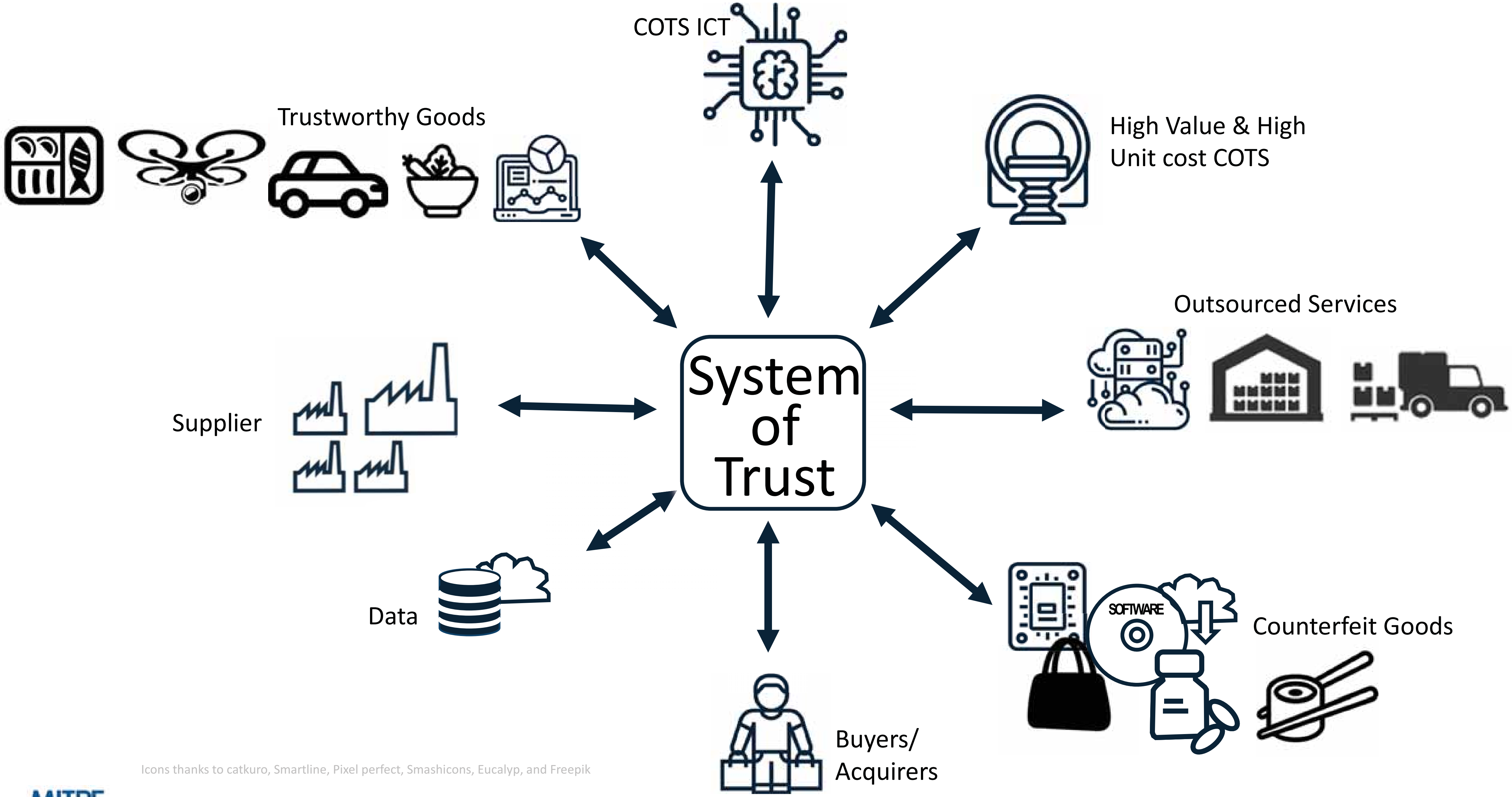
Effective Supply Chain Trust Interactions



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: 22-01488-10

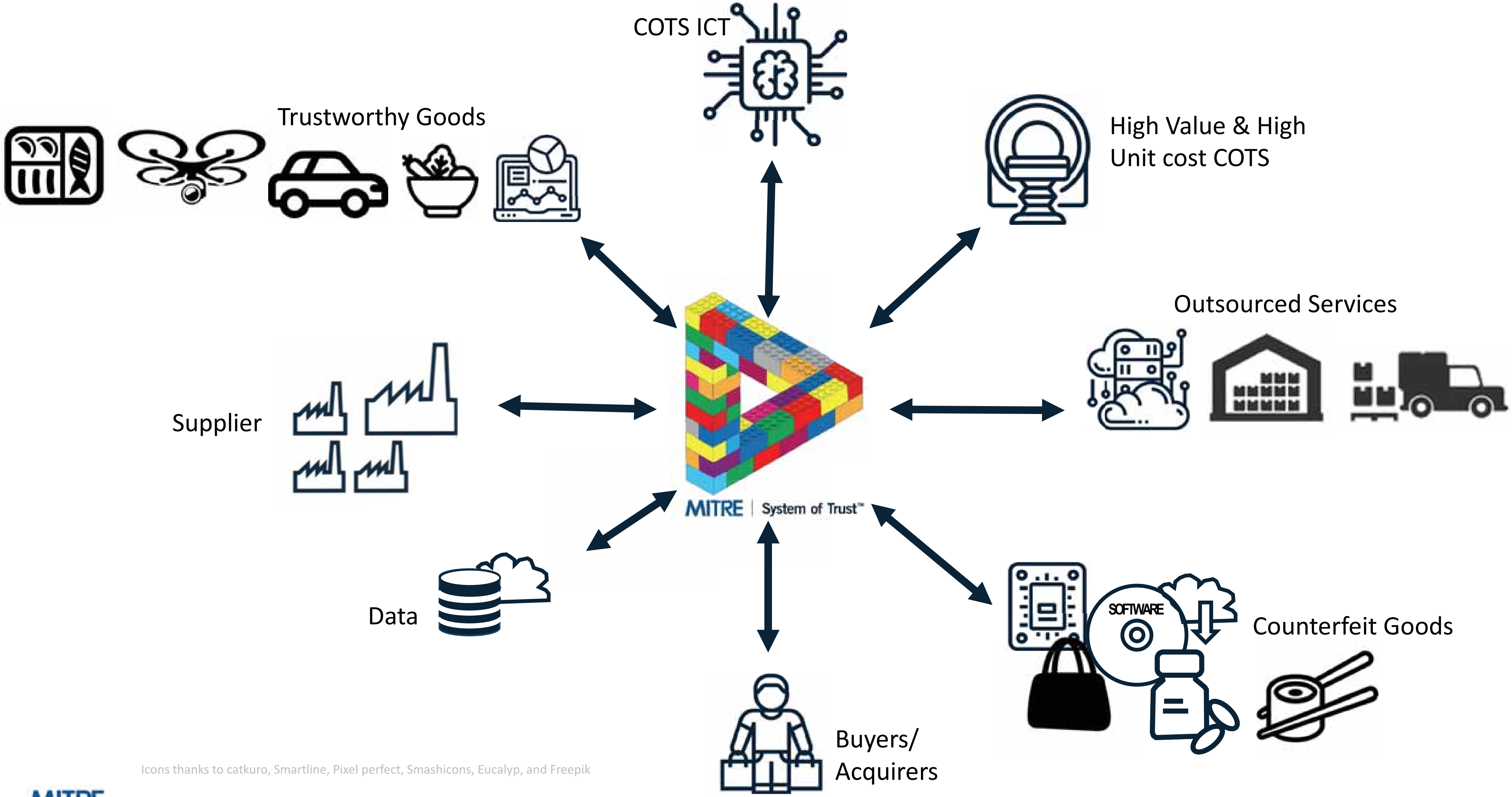
Effective Supply Chain Trust Interactions



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: 22-01488-10

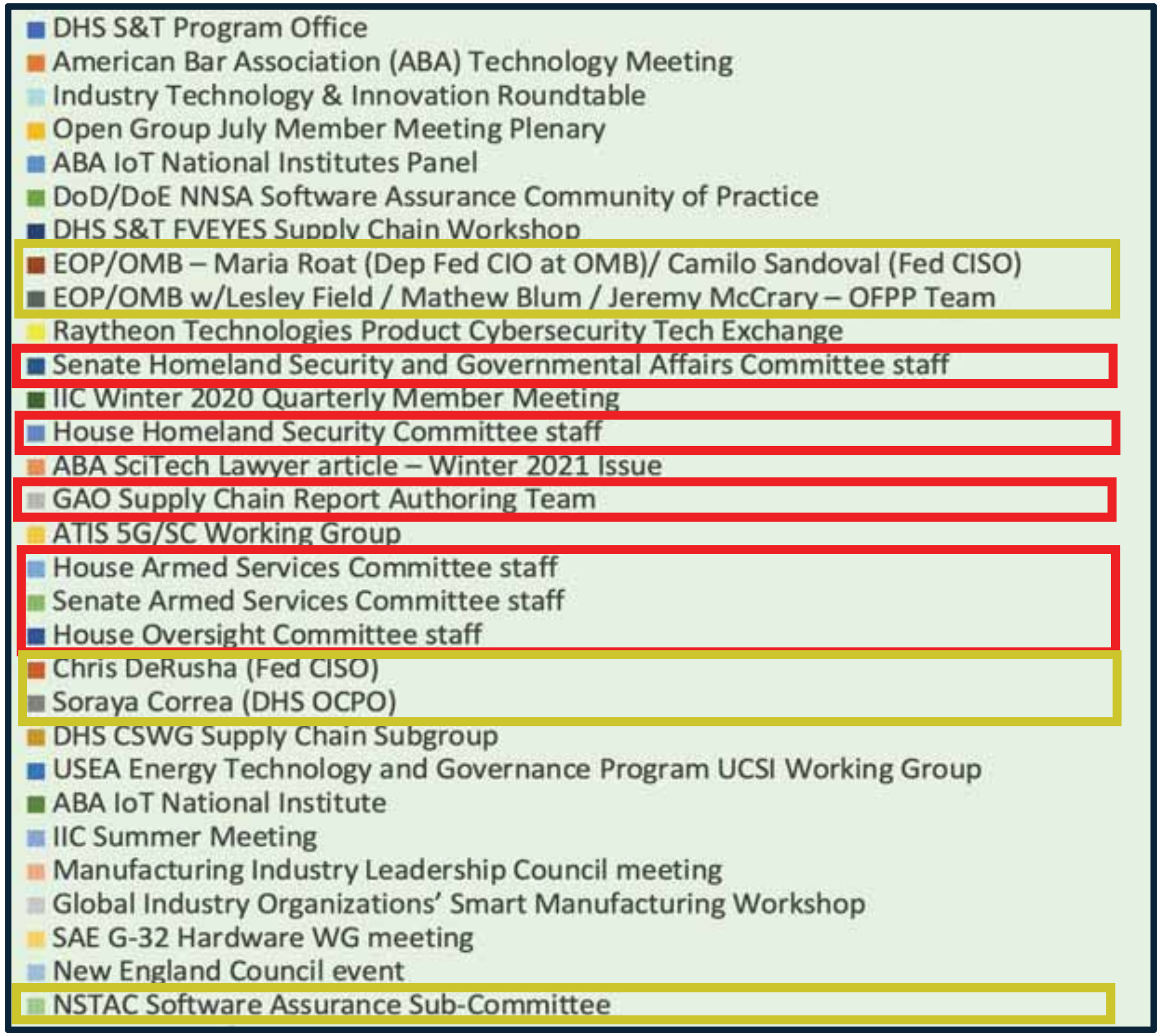
Effective Supply Chain Trust Interactions



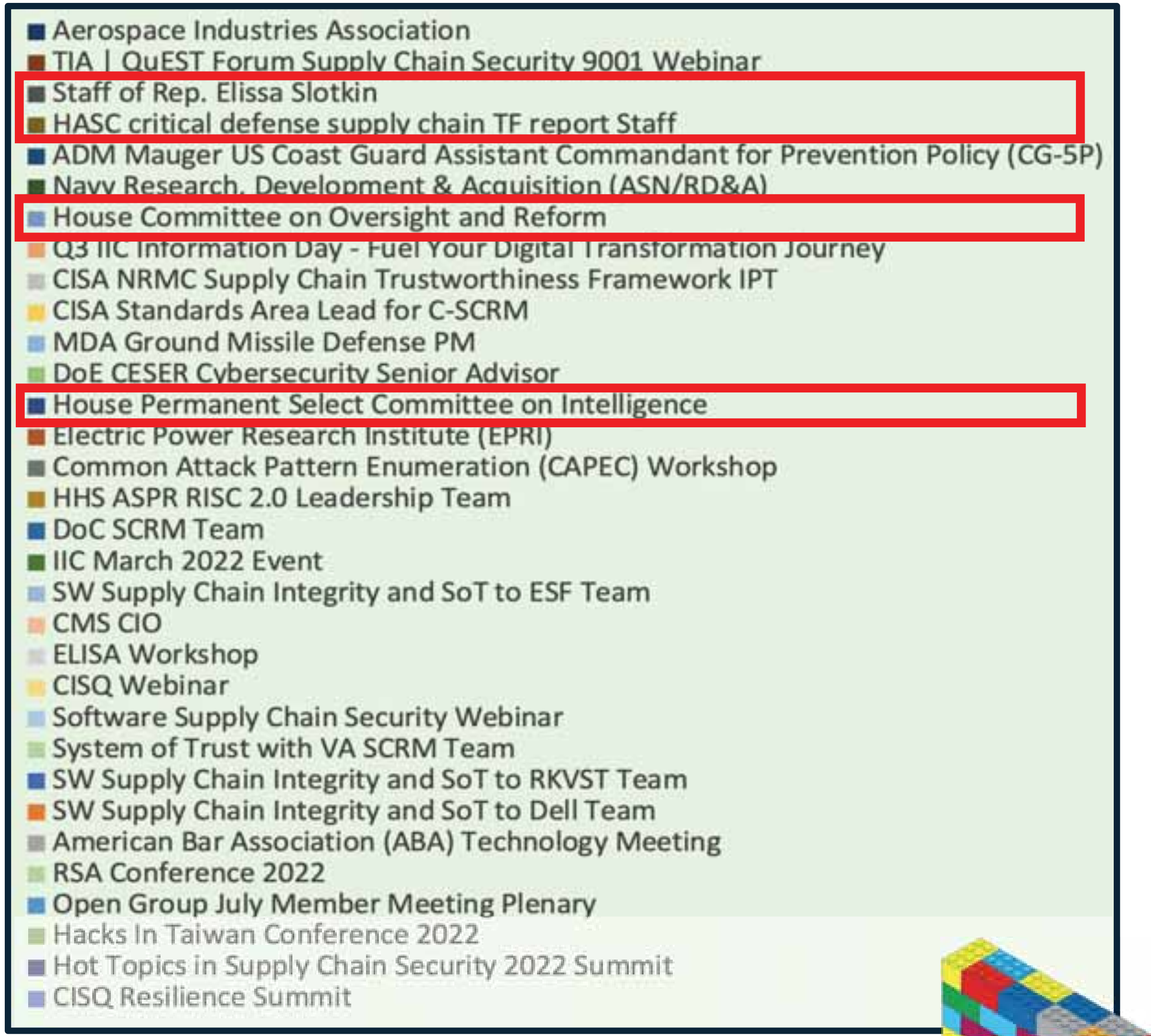
Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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
- CISQ Resilience Summit

🟨	Executive Acquisition
🟥	Congressional Committees

SYSTEM OF TRUST™

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

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: 22-01488-10

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
Drafting NDA	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
Discussing SoT	Company 10	Organization with Supply Chains
	Company 11	Community Engagement SMEs
	Company 12	Organization with Supply Chains
	Company 13	Organization with Supply Chains
	Company 14	Organization with Supply Chains
	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

Working on mechanisms to scale our engagements beyond NDAs

© 2022 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 22-01488-10

Publications to date…

TheSciTechLawyer WINTER 2021

CUTTER Business Technology Journal

Management, Innovation, Transformation

Vol. 33, No. 5 2020 ● REPRINT

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

The Supply Chain Security System of Trust:

A Framework for the Concerns Blocking Trust in Supplies, Suppliers, and Services

by Robert A. Martin

In this article, Robert A. Martin addresses the complete ecosystem involved in the procurement of products and services. What does it mean to trust that what you buy, and the organizations that sell to you, meet all the conditions required to merit your trust? Martin describes the elements of a system of trust for supply chain security that is currently under development and is based on collecting information from a wide community of procurement departments and standards organizations.

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

By Robert A. Martin, [illegible], J. Brian Hall, PhD, and Michael A. Aisenberg

DEFINING A SYSTEM OF TRUST (SoT) AS A KEYSTONE TOOL FOR SUPPLY CHAIN SECURITY

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

DELIVER UNCOMPROMISED: SECURING CRITICAL SOFTWARE SUPPLY CHAINS

PROPOSAL TO ESTABLISH AN END-TO-END FRAMEWORK FOR SOFTWARE SUPPLY CHAIN INTEGRITY

by Charles Clancy, Joseph Ferraro, Robert Martin, Adam Pennington, Christopher Sledjeski, and Craig Wiener

© 2021 MITRE # 21-XXXX 1-28-2021

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

MITRE'S CENTER FOR DATA-DRIVEN POLICY

TRUSTING OUR SUPPLY CHAINS: A COMPREHENSIVE DATA-DRIVEN APPROACH

By Robert A. Martin

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

The COVID-19 pandemic has brought supply chain security (SCS) into sharpened focus, and many inadequacies have surfaced regarding timely access to reliable stocks of personal protective equipment, medical devices, and food supplies, to name a few.

This is not a new challenge. In the 2000s, many U.S. government practices related to supply chain logistics management, dating from the Cold War era, were extended into the broader commercial information and communications technology (ICT) marketplace as those technologies and the efficiencies they brought to business and government became key enablers of the information economy.

For many suppliers providing the Department of Defense with commercial goods, the concept of a "cleared industry partner" became part of their way of life.

At the same time, the computerization of everything gave rise to pervasive cyber threats – including those stemming from vulnerabilities inherent in repurposed software of often dubious provenance. Further complicating this picture is the increasingly globalized nature of service support for ICT systems. Our adversaries seek to inject themselves into every conceivable stage of technology development, for both disruption and intelligence objectives.

Congressional Actions

Since 2011, Congress has passed several National Defense Authorization Acts and laws that contain more than 100 references to supply chain security. Many of these still remain to be implemented by their target agencies. More recently, in 2018, the executive branch and Congress worked to pass new legislation to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks. The Federal Acquisition Supply Chain Security Act of 2018 (Title II of Pub. L. 115-390), signed into law on December 21, 2018, established the Federal Acquisition Security Council (FASC). The FASC is an executive branch interagency council, chaired by a senior-level official from the Office of Management and Budget (OMB), and includes representatives from the General Services Administration, Department of Homeland Security, Office of the Director of National Intelligence, Department of Justice, Department of Defense, and Department of Commerce. This new interagency council, with its multiagency leadership and broad mandate for both cyber and SCS policy, could become the much-needed coordinating mechanism for federal agencies seeking to answer questions about vendor and product trustworthiness.

MITRE 1

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

MITRE Center for Data-Driven Policy

SUPPLY CHAIN SECURITY – IT'S EVERYONE'S BUSINESS

by Ron Hodge, Robert A. Martin, and Michael Aisenberg

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

But when it comes to supply chain security, the United States continues to relearn painful lessons from the past without taking the necessary steps to prevent or mitigate these mistakes before they occur again. This is true even while the nature of many goods has evolved to a point where much of their functionality includes a software element. The DIB can no longer afford to continue making the same mistakes, repeatedly, with regard to safeguarding the nation's critical supply chains. Rather, the U.S. must create a comprehensively scoped approach to supply chain security tailored to the mission and technologies of concern that mitigates the potential impacts of a successful attack on a supply chain. Additionally, the defense industry must address the compromises in its supply chains regardless of whether they come from purposeful, accidental, or negligent conduct or sources. This requires the DIB and the national security community to determine what negative operational impacts stakeholders should try to avoid and use that to drive supply chain focus. And for the industrial base specifically, it must be made clear that failures to effectively address the various aspects of supply chain security will affect not only our national security posture but industry's own ability to conduct business with the U.S. government.

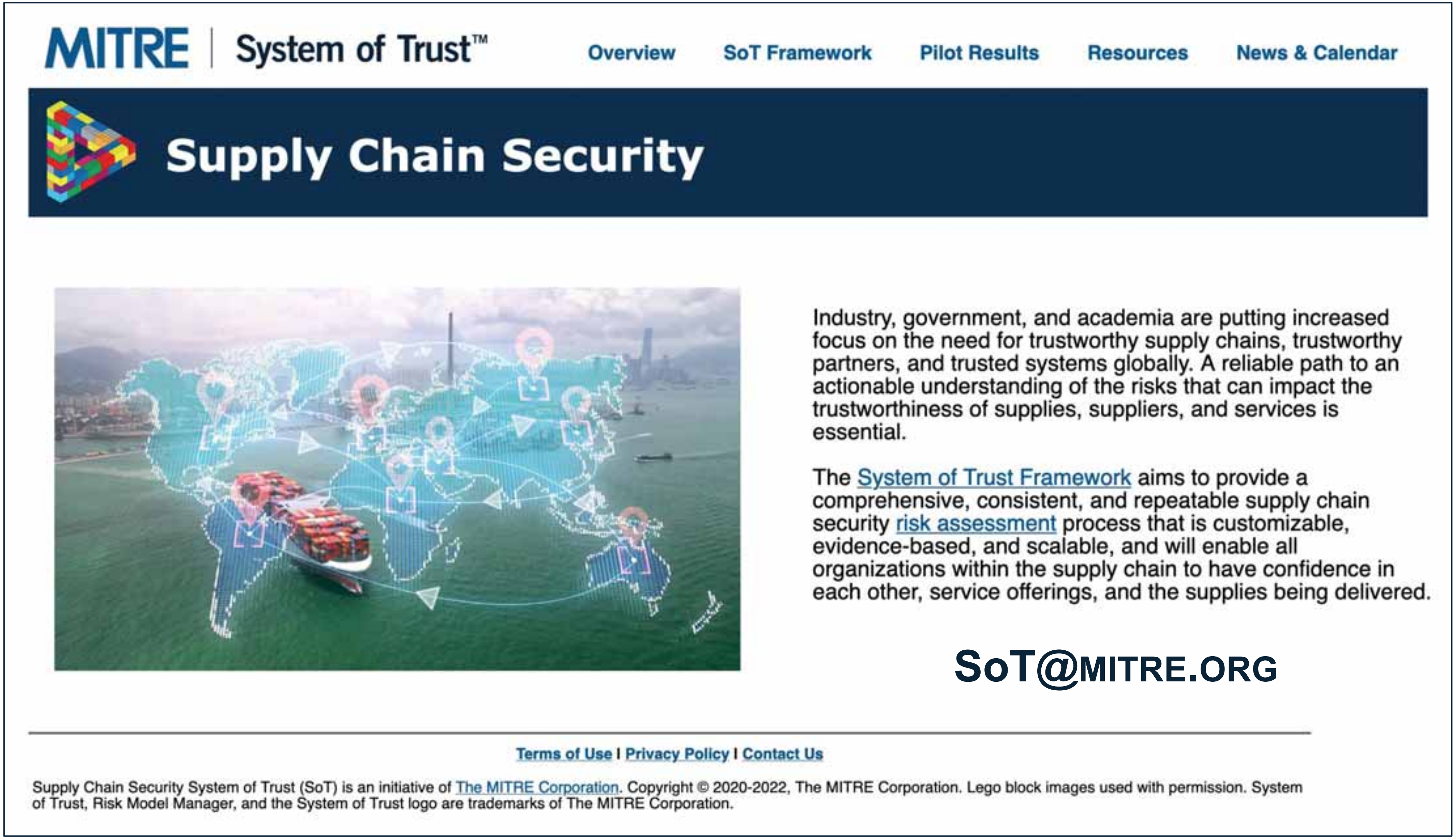
Supply chain security is at the center of many of today's national security challenges.[1] Few things illustrate this reality as well as the recent SolarWinds software supply chain hack where it was discovered that the U.S. has been the target of a massive Russian espionage campaign,[2] exploiting trust in information and communications technology supply chains. In spring 2020, the SolarWinds company networks were penetrated by a state-sponsored attack. While on the SolarWinds systems and networks, the adversary learned how SolarWinds crafted and created its software. With this understanding the adversary developed a piece of malware that it implanted into the SolarWinds software build system, which, during the building of SolarWinds' Orion Network Management

JULY 2021

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: 22-01488-10

SoT.MITRE.ORG



MITRE | System of Trust™

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

Supply Chain Security

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

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: 22-01488-10