MITRE's System of Trust:

Supply Chain Assessment Synergy Consistency and Evidence-Based

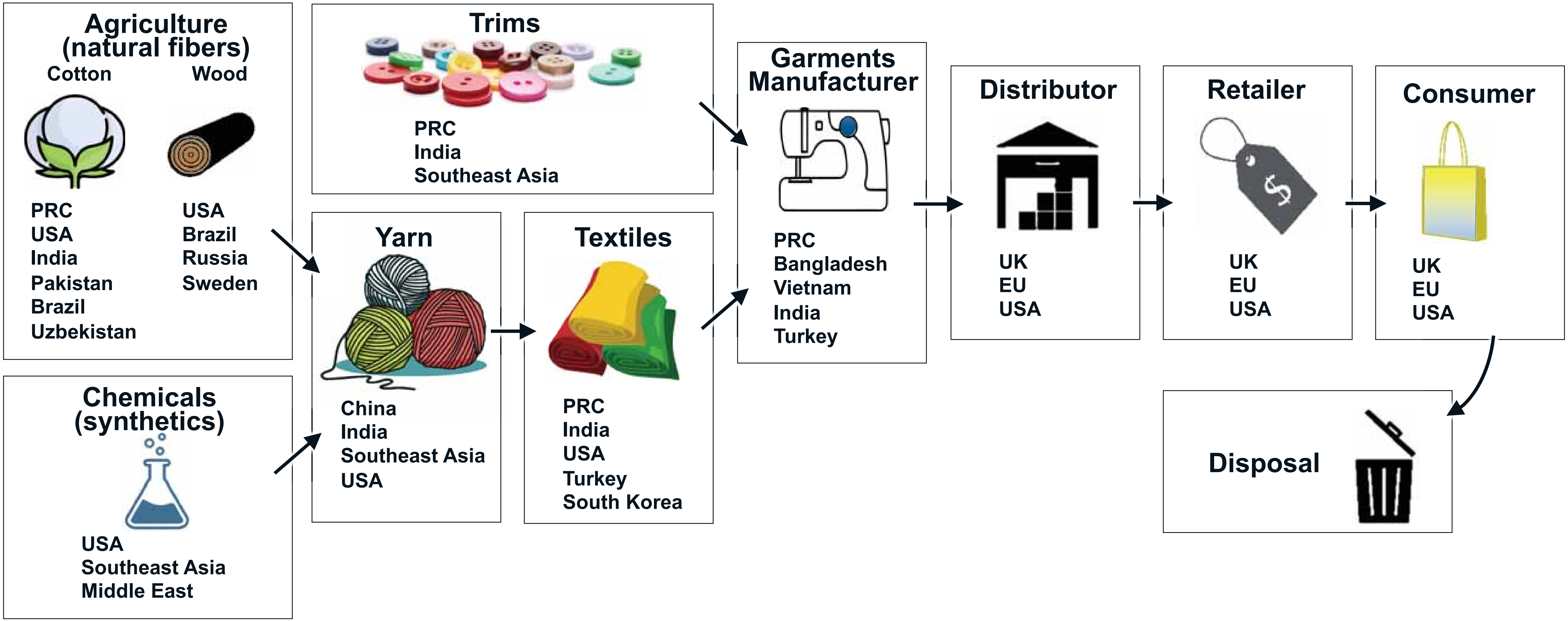
MITRE | System of Trust™

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

MITRE Labs

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

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

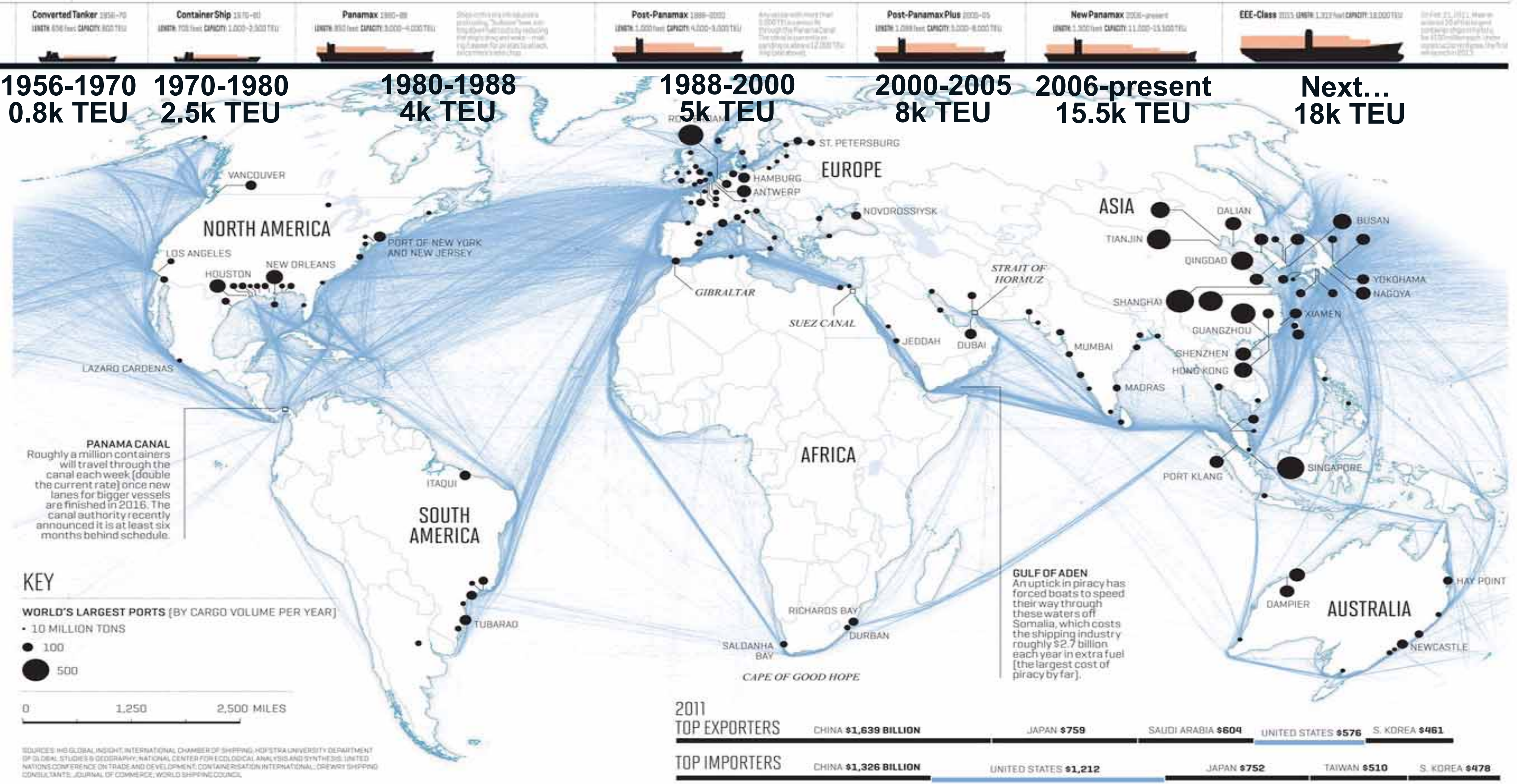
Consumer

UK, EU, USA

Disposal

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

MITRE



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).

2011

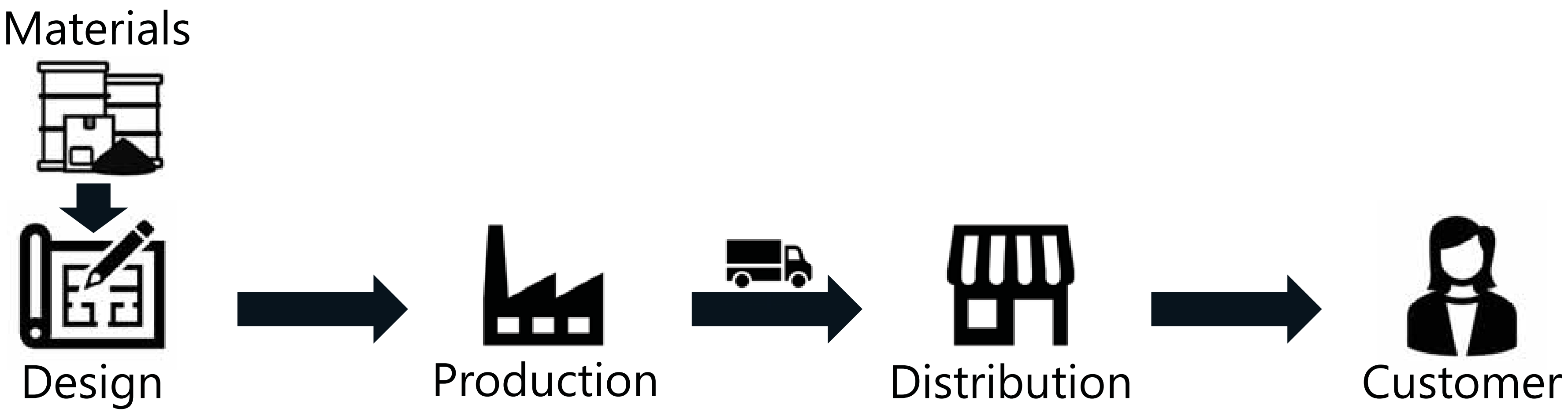
TOP EXPORTERS: CHINA $1,639 BILLION; JAPAN $759; SAUDI ARABIA $604; UNITED STATES $576; S. KOREA $461

TOP IMPORTERS: CHINA $1,326 BILLION; UNITED STATES $1,212; JAPAN $752; TAIWAN $510; S. KOREA $478

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

Supply Chains

Generic Supply Chain



Materials

Design

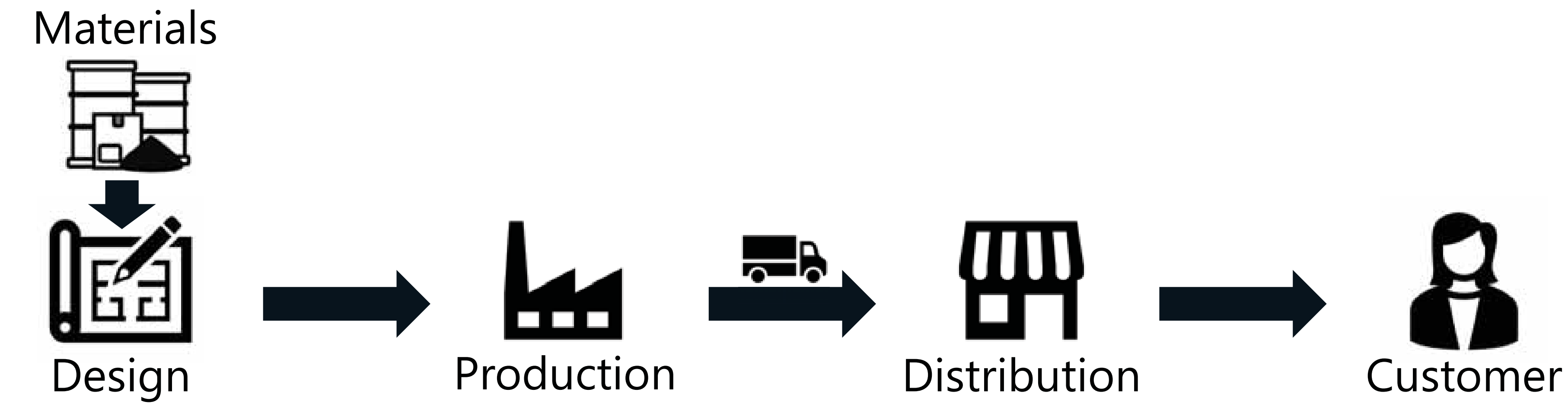
Production

Distribution

Customer

Supply Chains

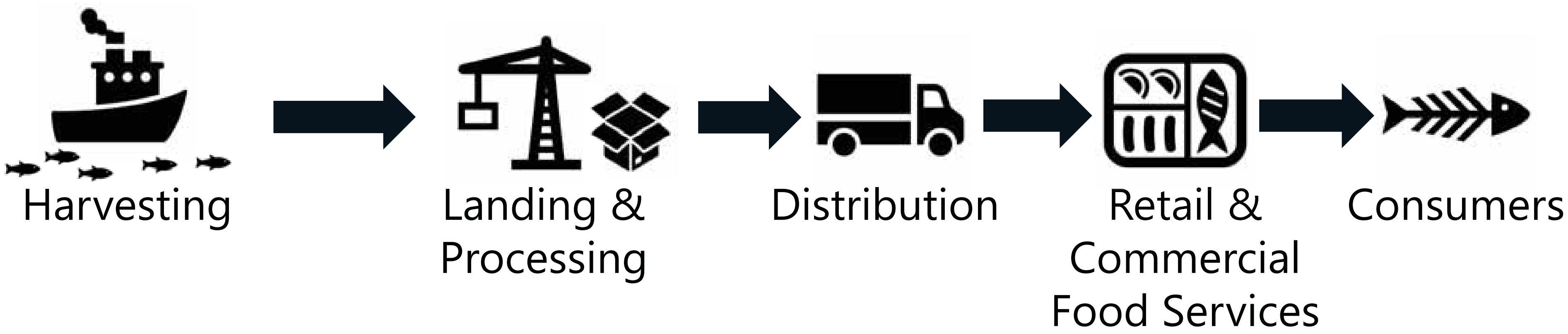
Generic Supply Chain



Materials

Design → Production → Distribution → Customer

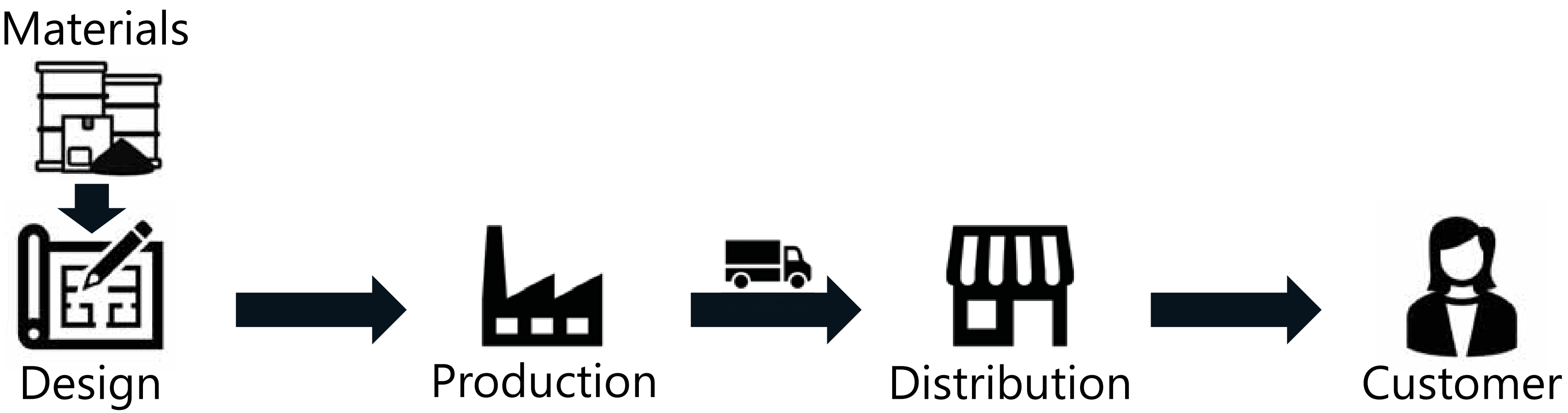
Seafood Supply Chain



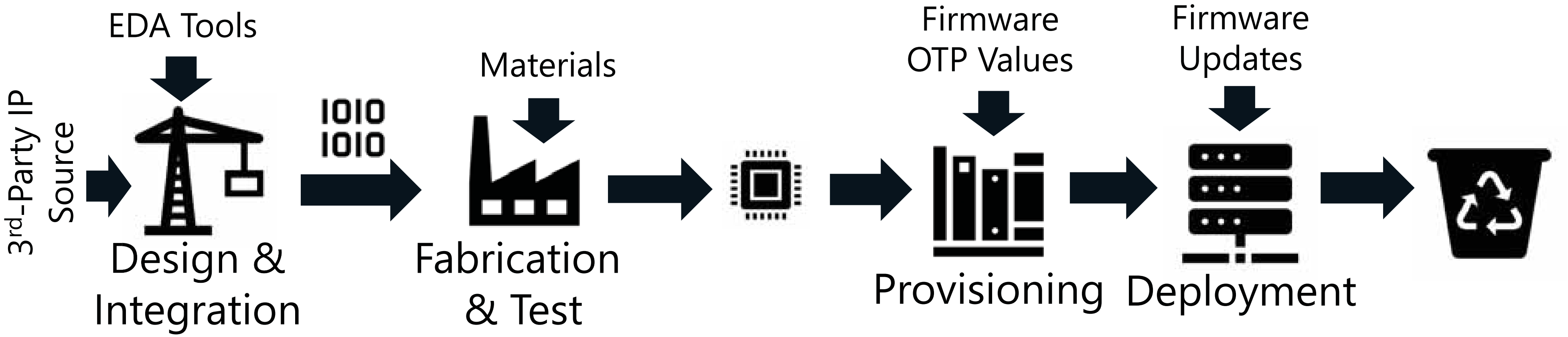
Harvesting → Landing & Processing → Distribution → Retail & Commercial Food Services → Consumers

Supply Chains

Generic Supply Chain

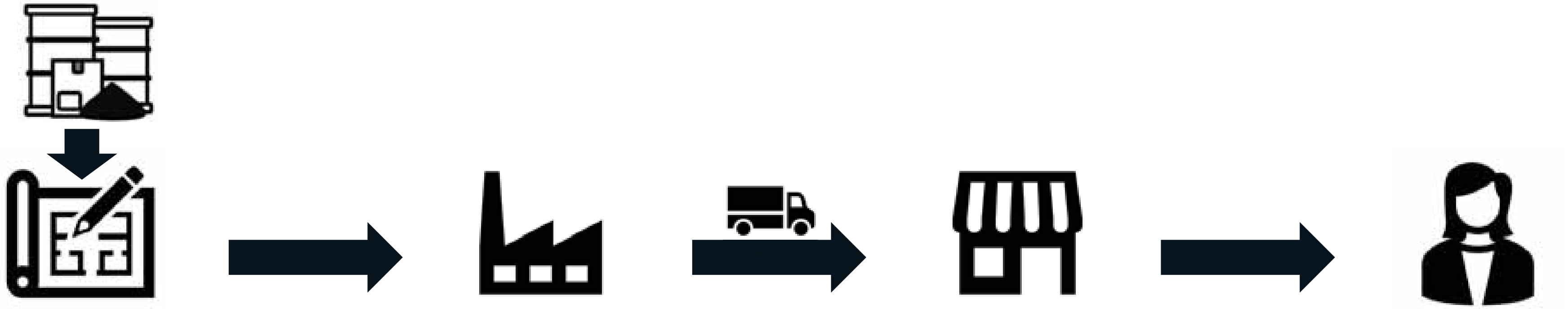


Micro-electronics Supply Chain



Supply Chains

Generic Supply Chain



Materials

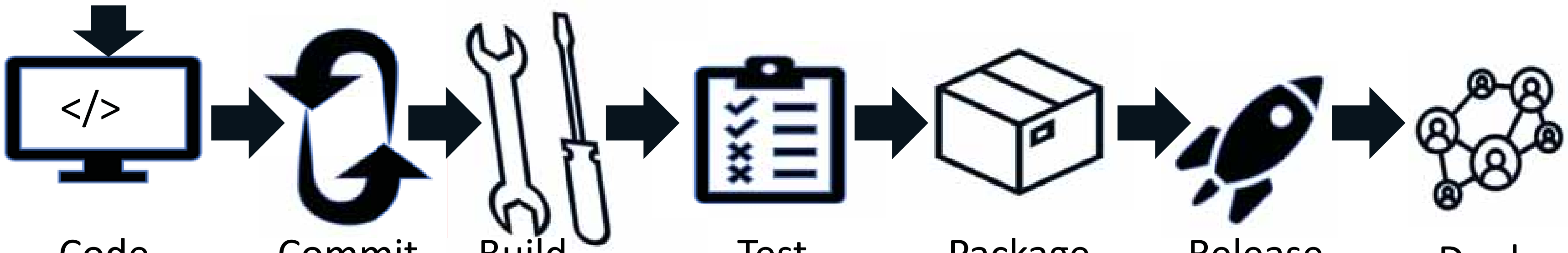
Design

Production

Distribution

Customer

Software Supply Chain



Dependencies

Code

Commit

Build

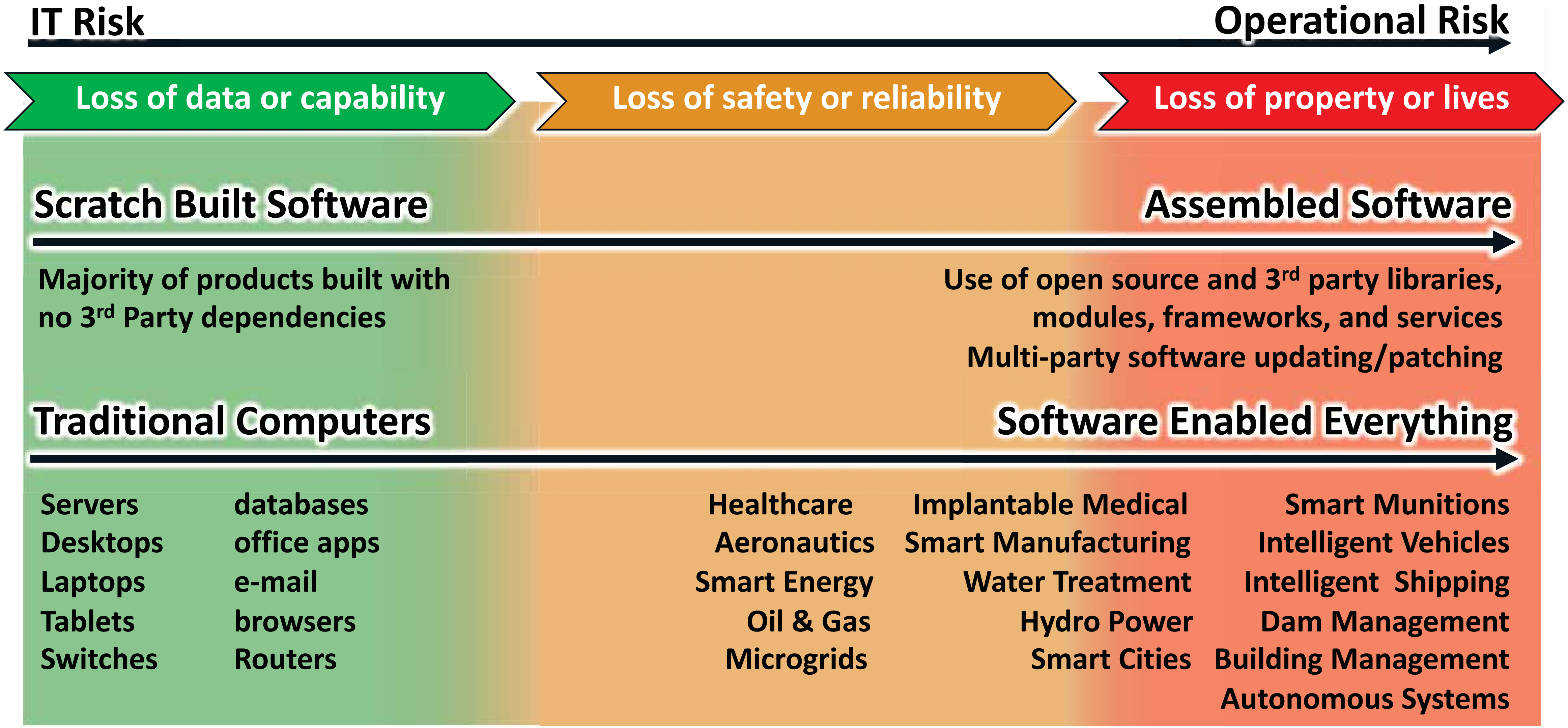
Test

Package

Release

Deploy

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

Software Enabled Critical Infrastructure and Mission Capabilities…

Medical

Vehicles

Buildings

Temperature, Humidity,CO2

Motion Sensor

AC,Chiller

Electric power

Elevator

Entrance gate

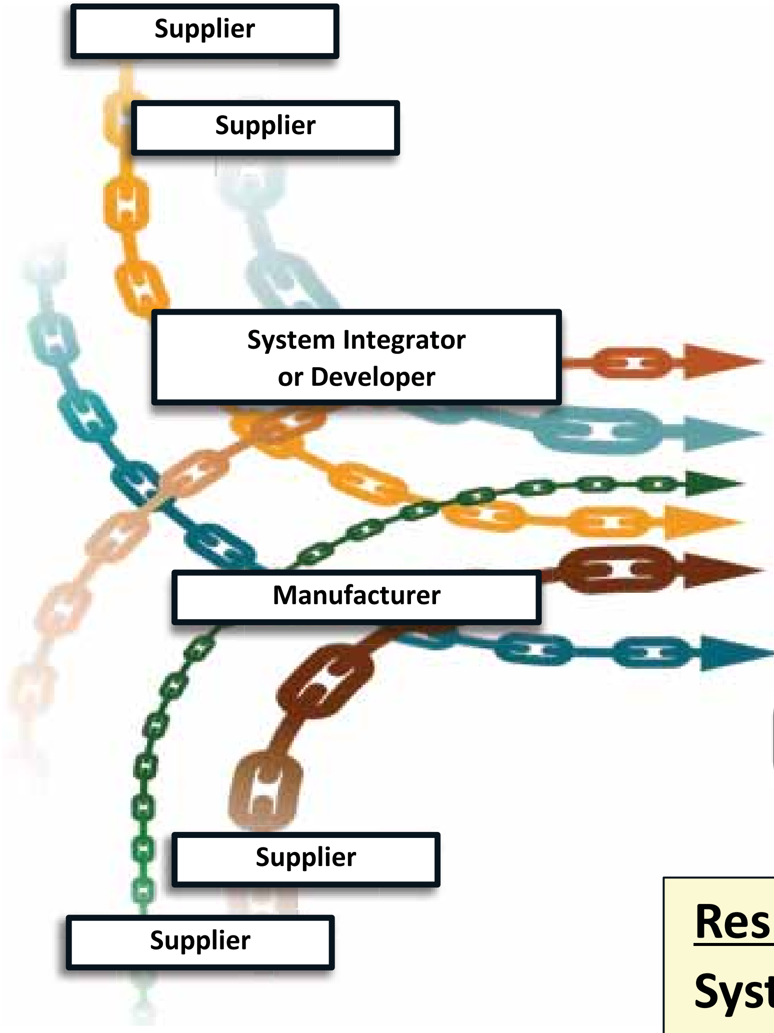
Aeronautics

Manufacturing

Energy

Shipping

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



Based on SEI/CMU materials

Intentional acts

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

Unintentional acts

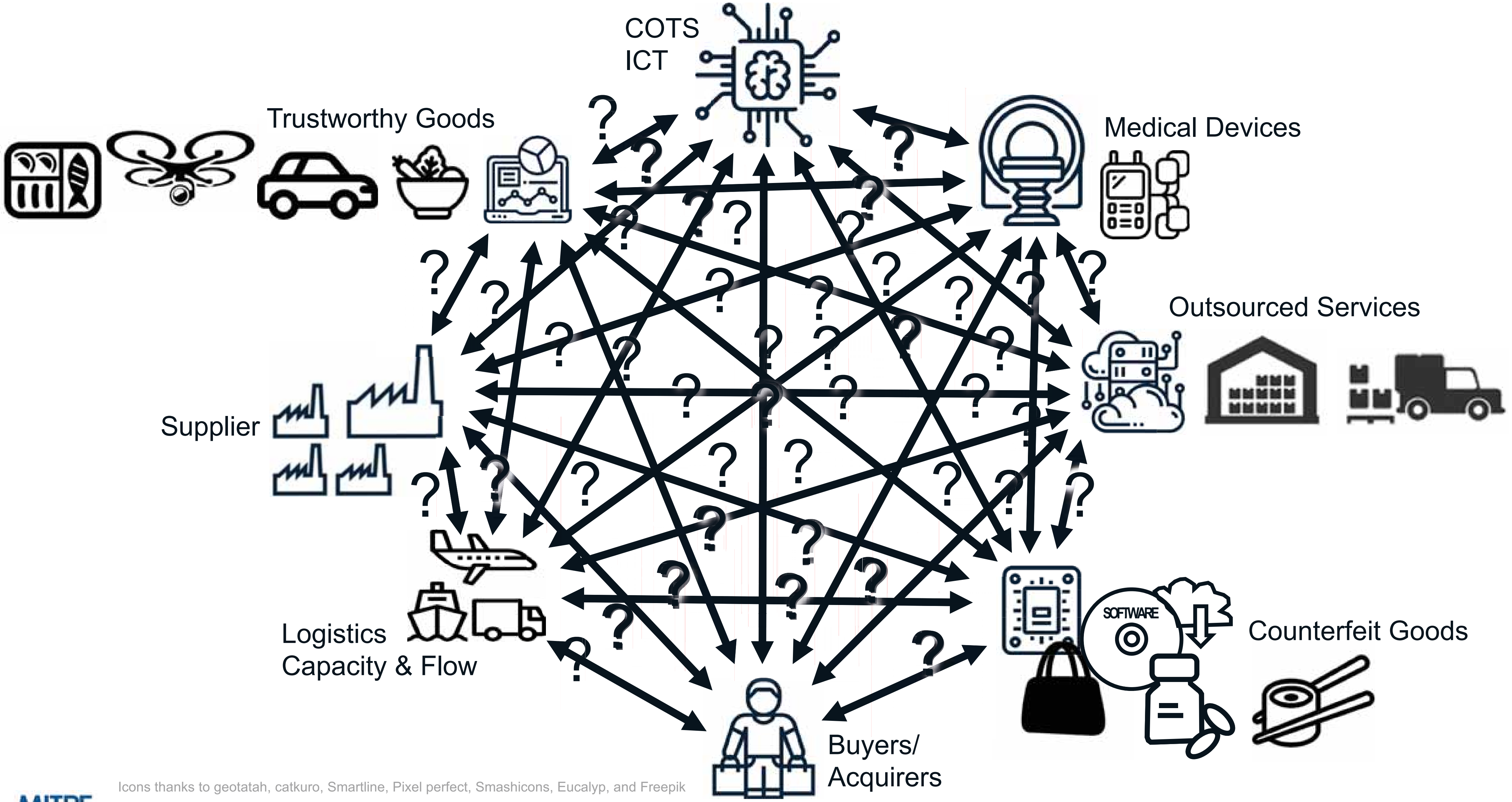
- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/weaknesses and/or known vulnerabilities)

Result of Supply Chain Attacks:

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

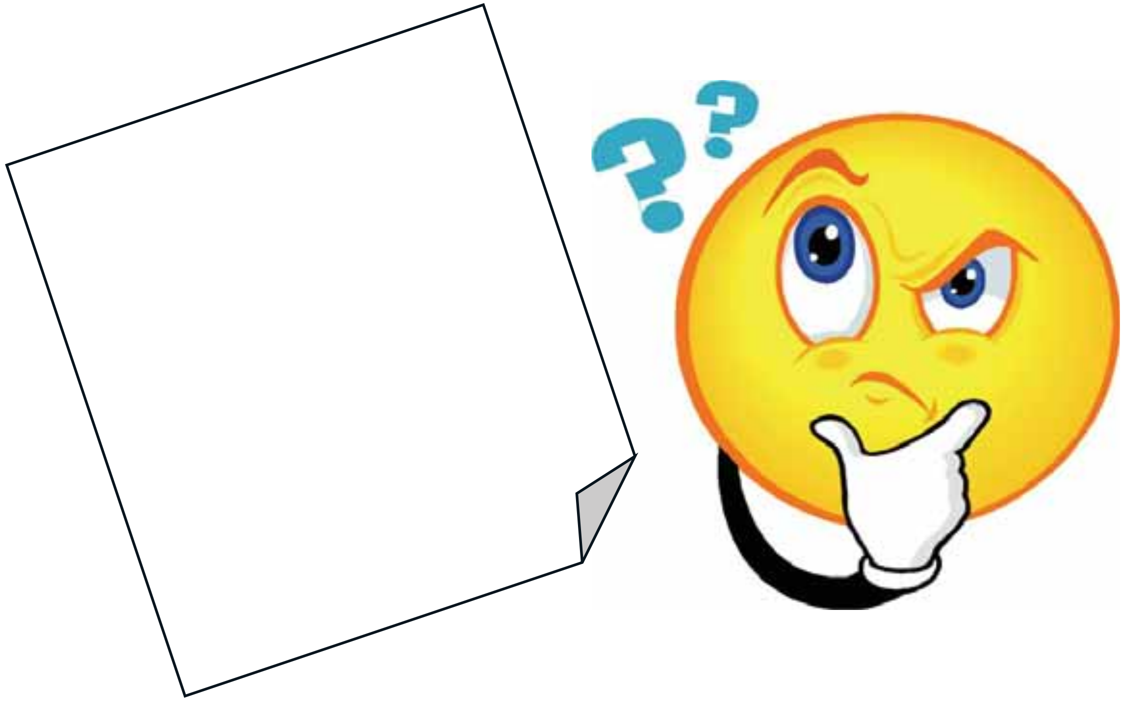
MITRE

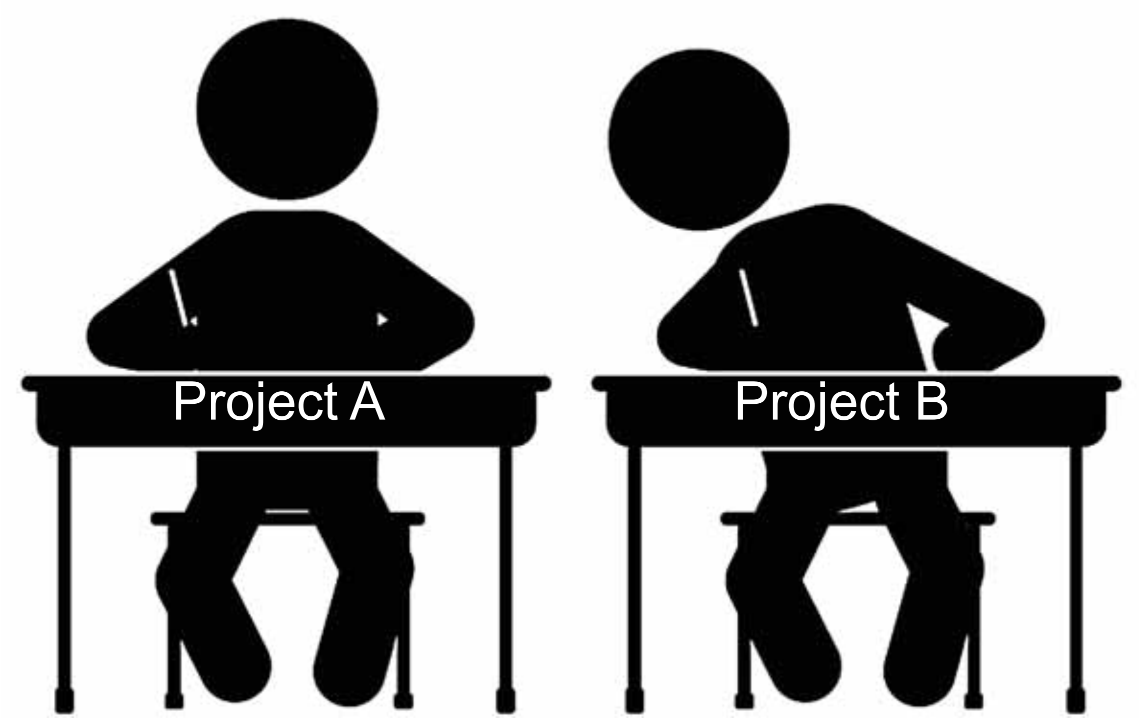
Open Question: What Supply Chain Risks to Manage?



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

Open Question: What Supply Chain Risks to Manage?





Supply Chain Risk Areas

Natural Disasters and Hazards

Icons thanks to freepik

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

Quality Culture of the Supplier

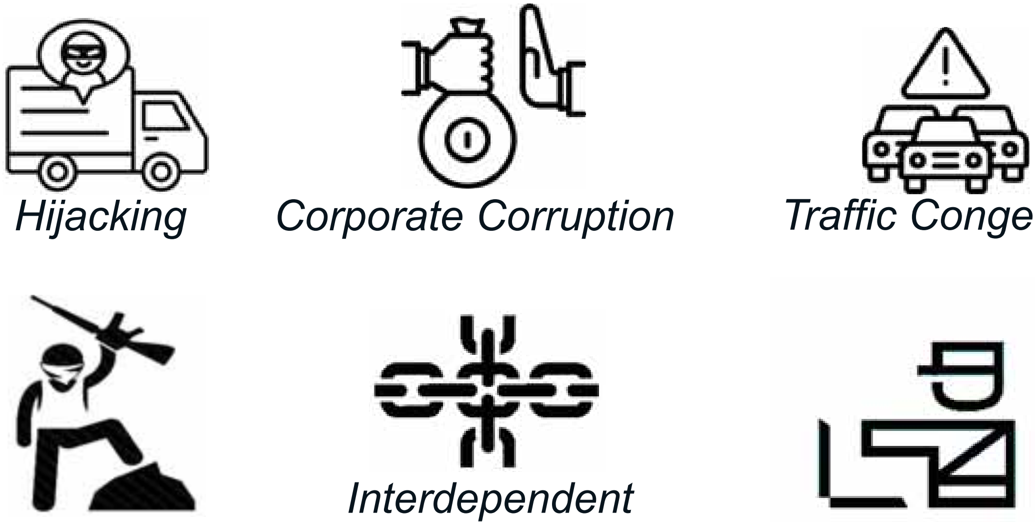
External Influences of the Supplier

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

Maliciousness of the Supplier
Organizational Security

Attackers & Counterfeits

Human Hazards



Hijacking

Corporate Corruption

Traffic Congestion

Civil Disruption

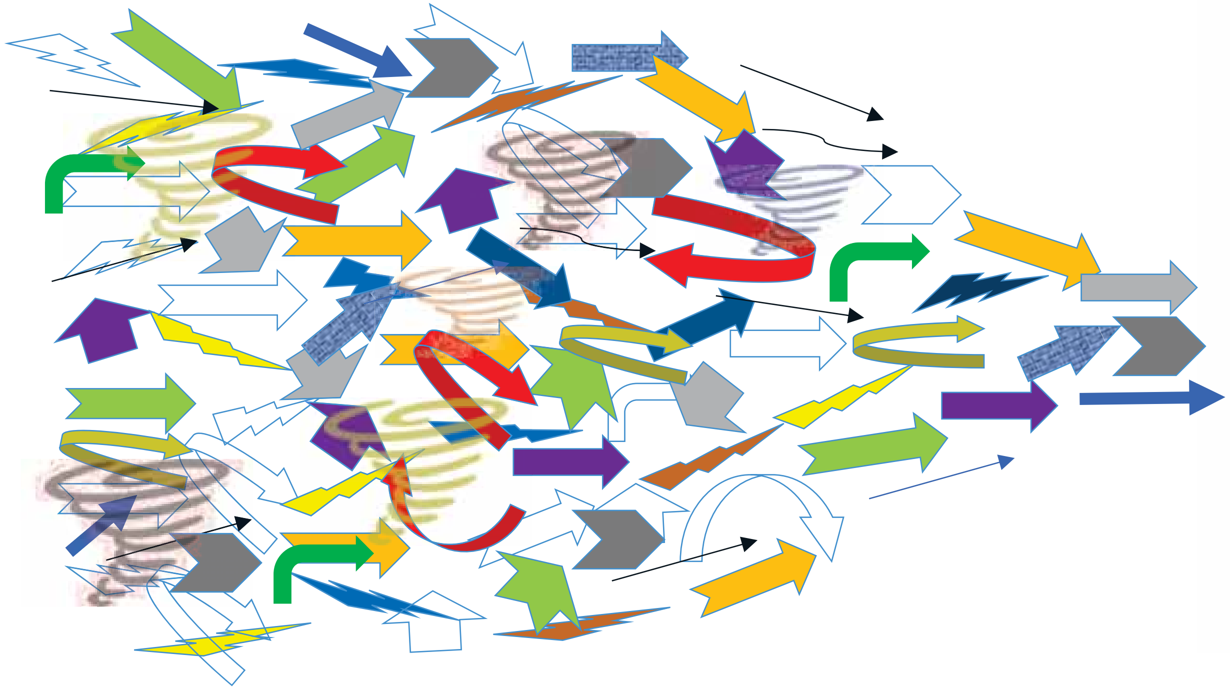
Interdependent Supply Chains

National Corruption

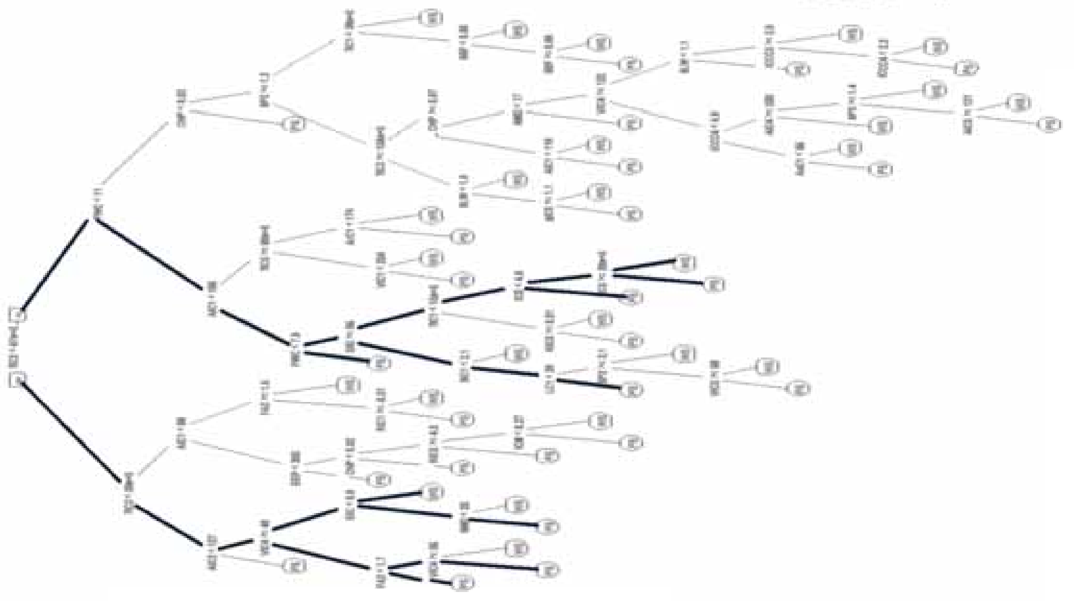
Supply Chain Security (SCS) System of Trust (SoT)

“What Supply Chain Risks to Manage?”

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

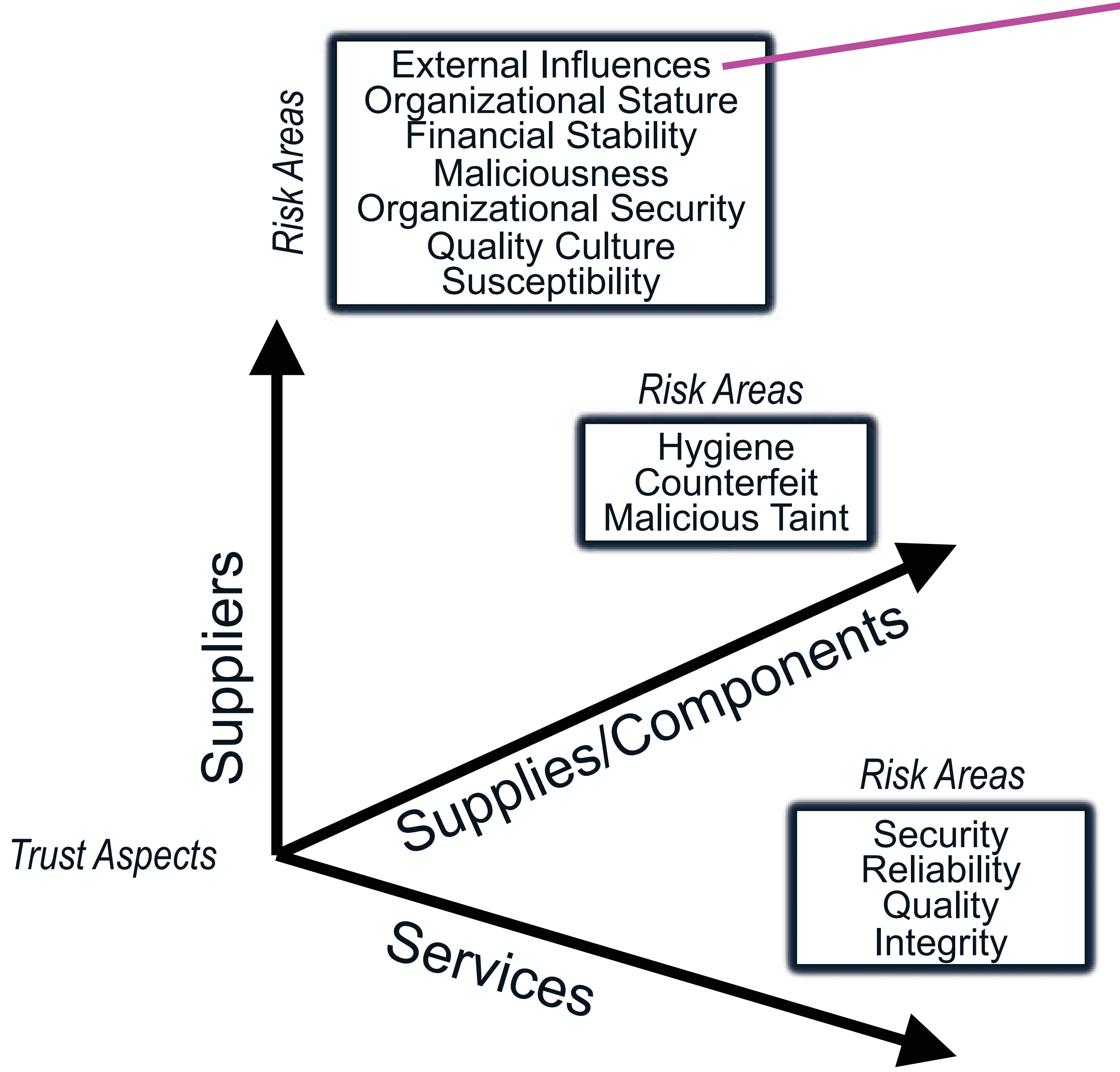


Address Chaos, Align & Organize



Simplify, Tailor & Use

Basis of Trust



Trust Aspects

Suppliers

Risk Areas

External Influences
Organizational Stature
Financial Stability
Maliciousness
Organizational Security
Quality Culture
Susceptibility

Supplies/Components

Risk Areas

Hygiene
Counterfeit
Malicious Taint

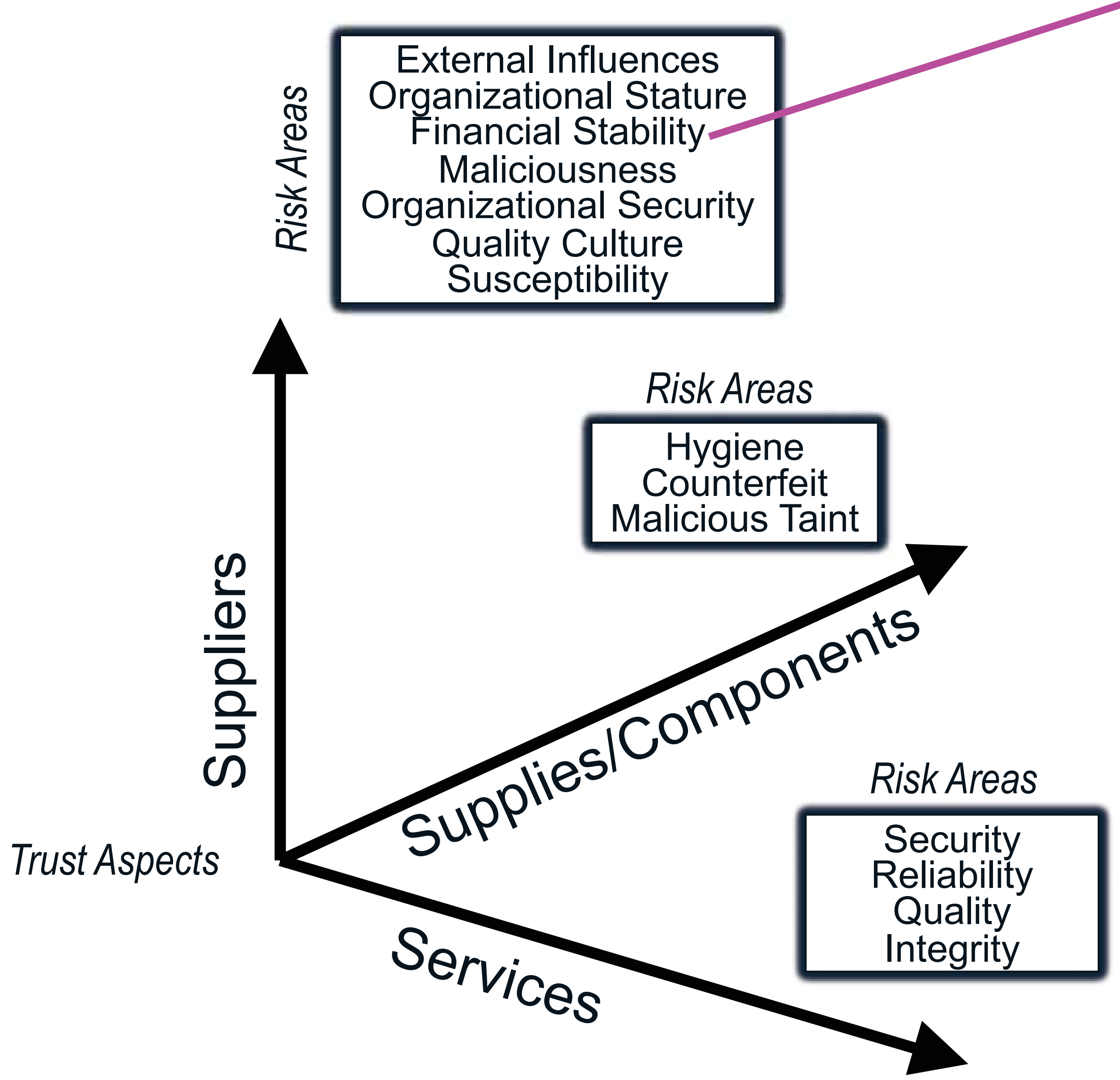
Services

Risk Areas

Security
Reliability
Quality
Integrity

- **Company foreign relationships with countries of concern**
- **Company operational locations in countries of concern**
- **Foreign registration/incorporation**
- **Geopolitical instability**
- **Key Management Personnel (KMP) and non-person entity relationships of concern**
- **National corruption**
- **National governance**
- **Organization ownership and control**
- **Politically Exposed Persons (PEPs) in corporate leadership**
- **Political vulnerability**
  Transparency of organization control

Basis of Trust



Risk Areas

External Influences
Organizational Stature
Financial Stability
Maliciousness
Organizational Security
Quality Culture
Susceptibility

Suppliers

Risk Areas

Hygiene
Counterfeit
Malicious Taint

Supplies/Components

Risk Areas

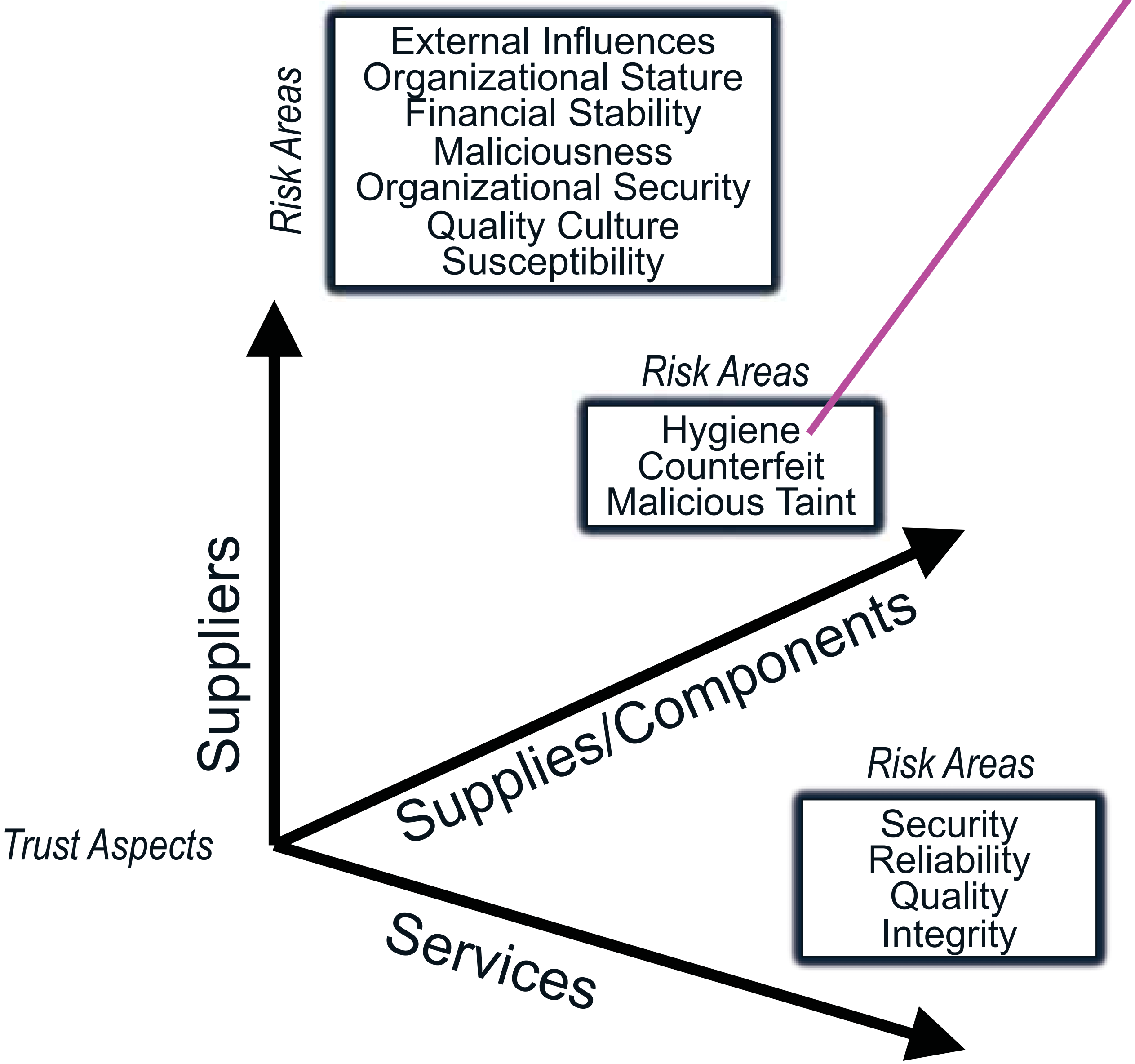
Security
Reliability
Quality
Integrity

Trust Aspects

Services

- **Questionable debt management**
  - 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
- **Questionable financial stewardship**
  - 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
- **Questionable future outlook**
  - Company has concerning R&D investment level
  - Organization has concerning inventory turnover rate
- **Questionable profitability**
  - Gross profit margin is of concern
  - Organization is not showing a profit
- **Vulnerability of financial stability to foreign influence**
  - …
- **Vulnerability of financial stability to market factors**
  - …
- **Vulnerability to takeover**
  - …

Basis of Trust



Risk Areas

External Influences
Organizational Stature
Financial Stability
Maliciousness
Organizational Security
Quality Culture
Susceptibility

Risk Areas

Hygiene
Counterfeit
Malicious Taint

Risk Areas

Security
Reliability
Quality
Integrity

Trust Aspects

Suppliers

Supplies/Components

Services

- **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
  - …

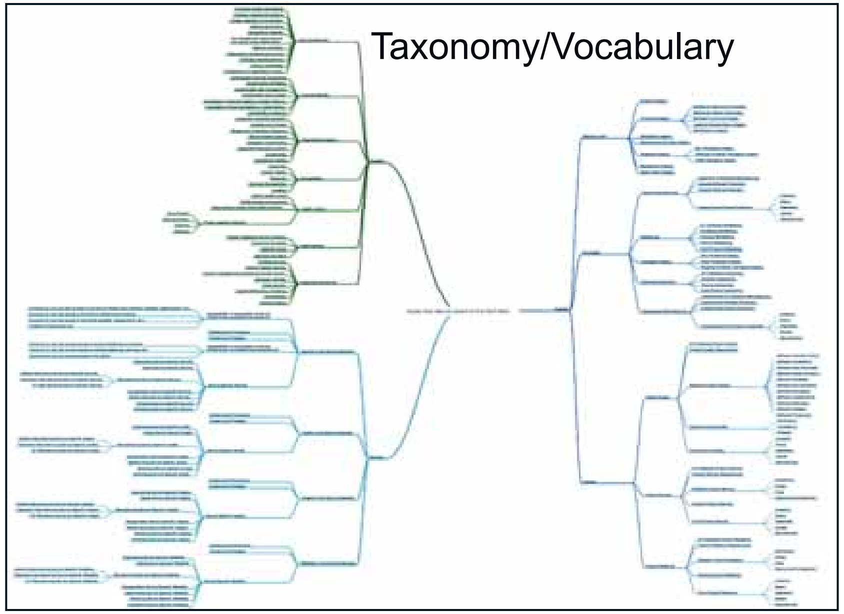
MITRE Supply Chain Security System of Trust Risk Areas* **

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 facilit 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													

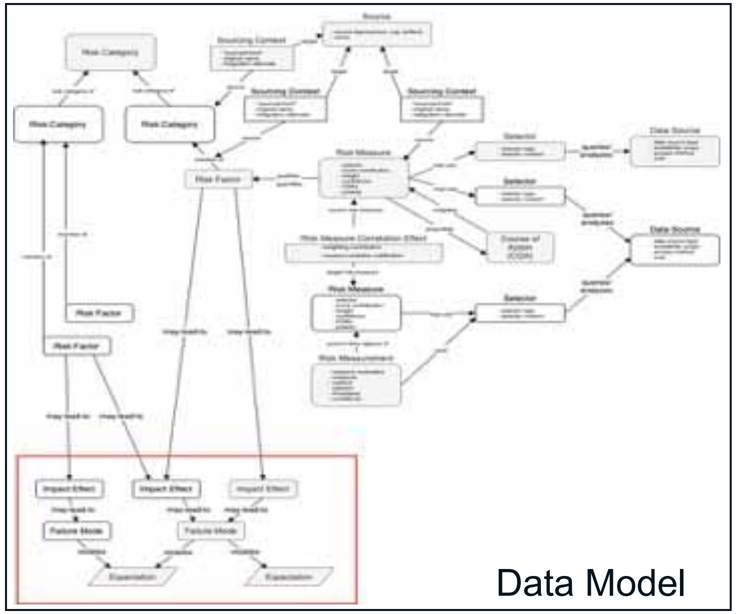
MITRE's Supply Chain Security System of Trust™
https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach

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

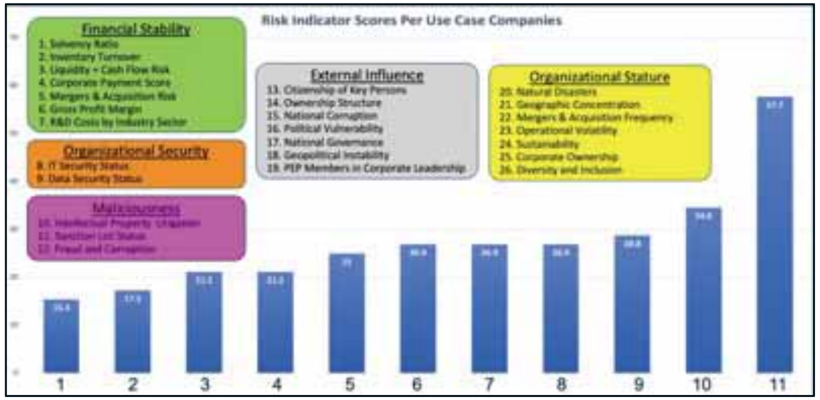
Taxonomy/Vocabulary

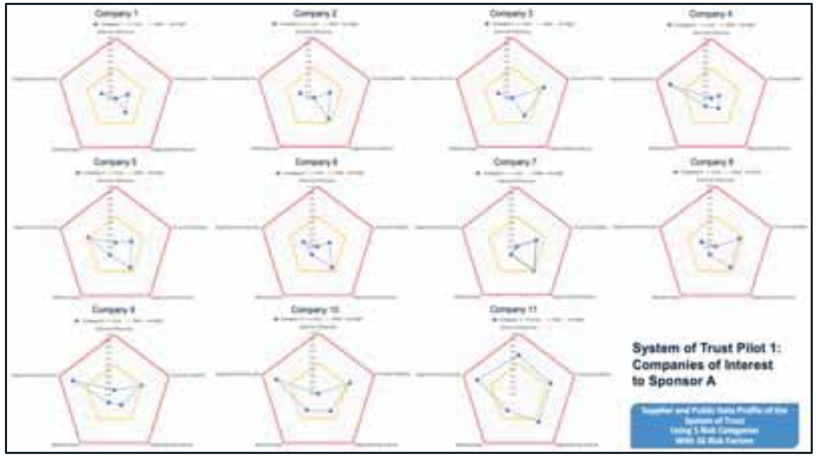


Data Model

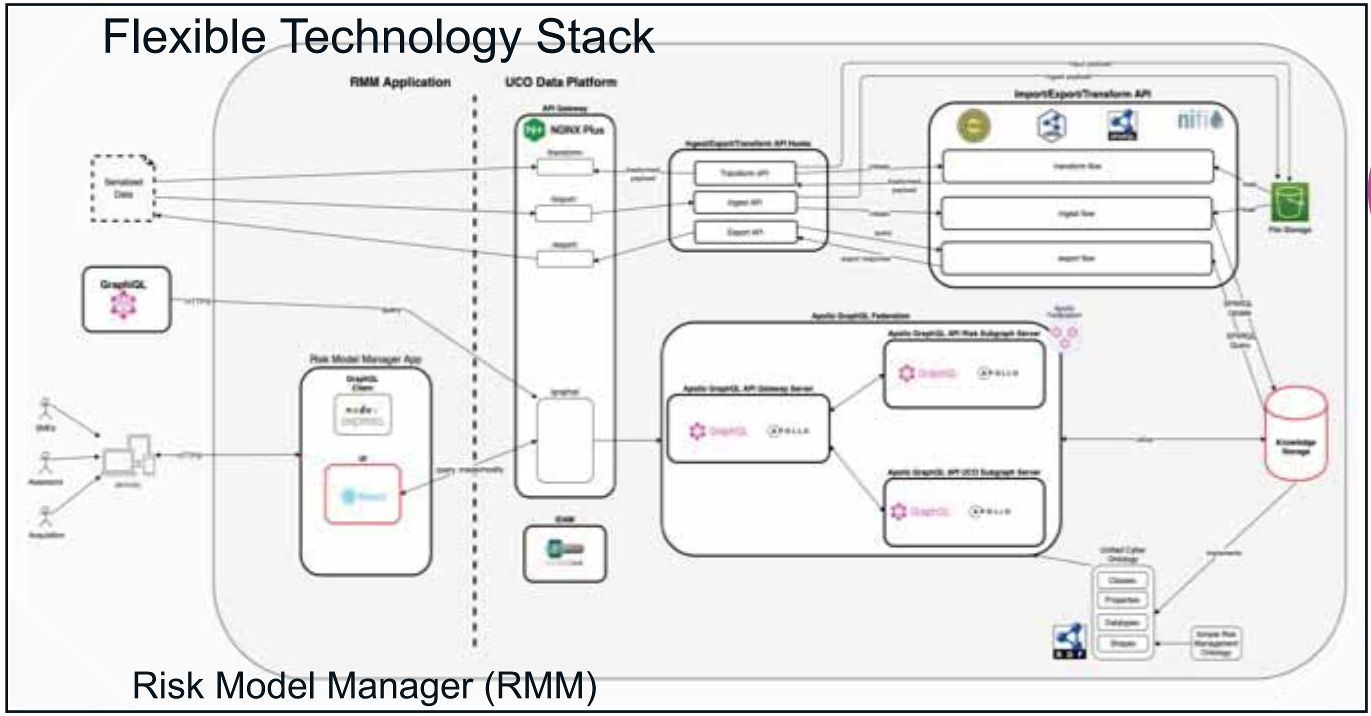


Analytic Methods


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



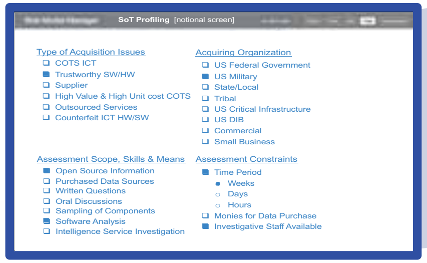
Risk Model Manager (RMM)

Piloting

11, 3, 1, 6, 22, 12, …

Export to Spreadsheet for “Offline” Assessment

Tying together SoT and RMM



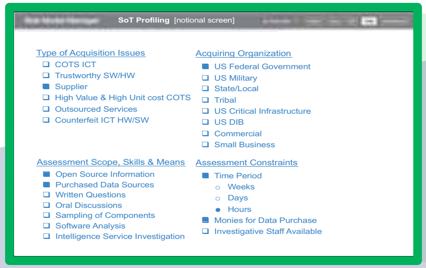
SoT Profiling [notional screen]

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



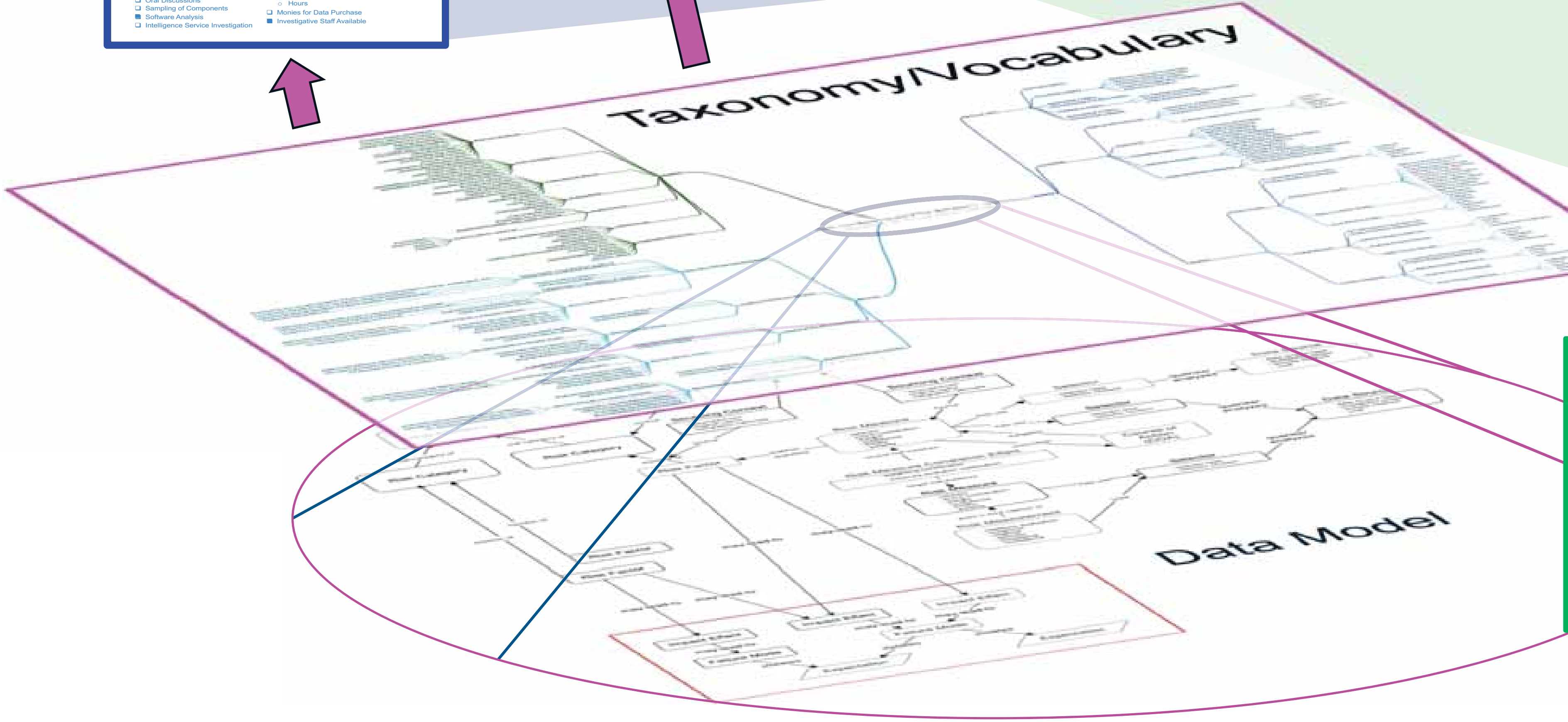
SoT Profiling [notional screen]

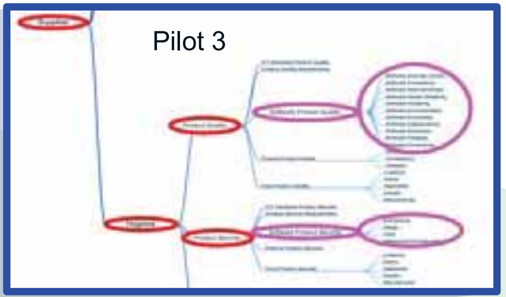
Type of Acquisition Issues
- ❑ COTS ICT
- ❑ Trustworthy SW/HW
- ■ Supplier
- ❑ High Value & High Unit cost COTS
- ❑ Outsourced Services
- ❑ Counterfeit ICT HW/SW

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

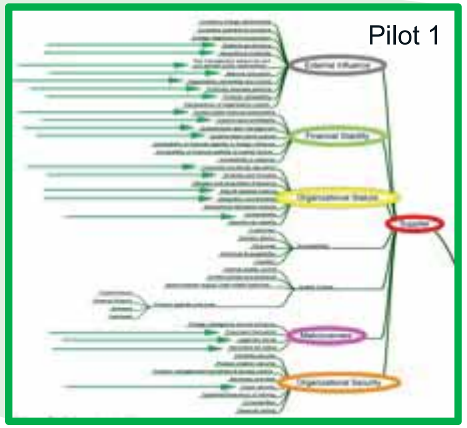
Assessment Scope, Skills & Means
- ■ Open Source Information
- ■ Purchased Data Sources
- ❑ Written Questions
- ❑ Oral Discussions
- ❑ Sampling of Components
- ❑ Software Analysis
- ❑ Intelligence Service Investigation

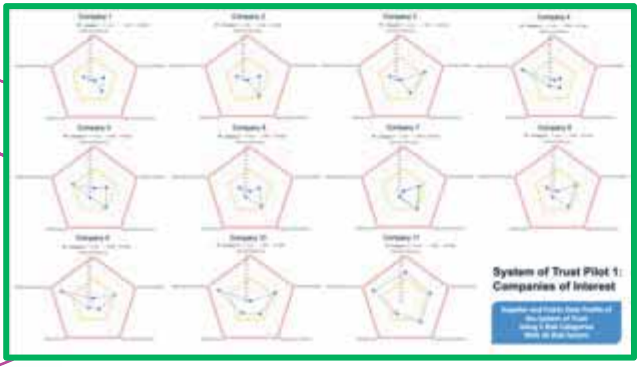
Assessment Constraints
- ■ Time Period
  - ○ Weeks
  - ○ Days
  - ● Hours
- ■ Monies for Data Purchase
- ❑ Investigative Staff Available

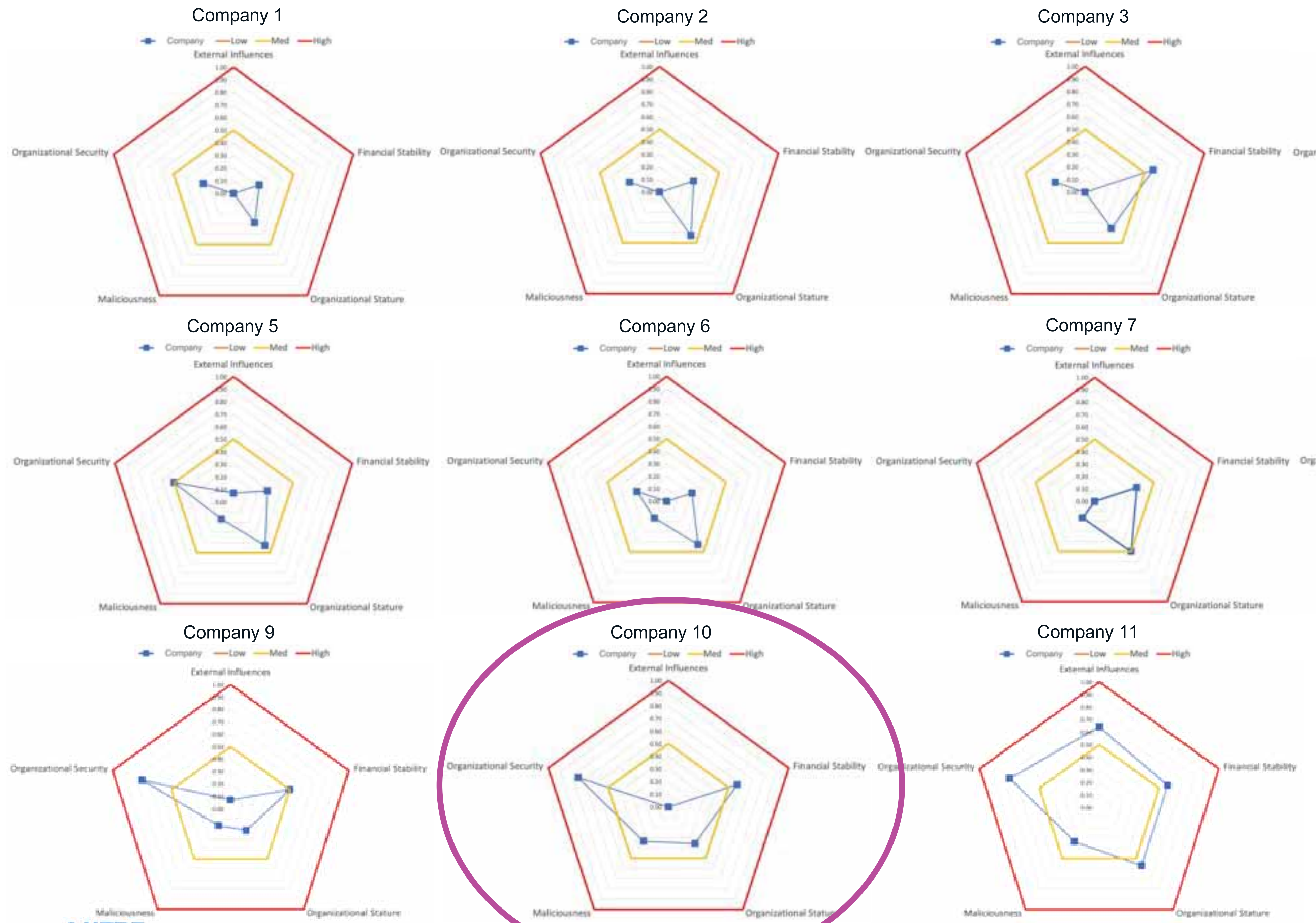




SW Supply Use Case Risk Scorecard*





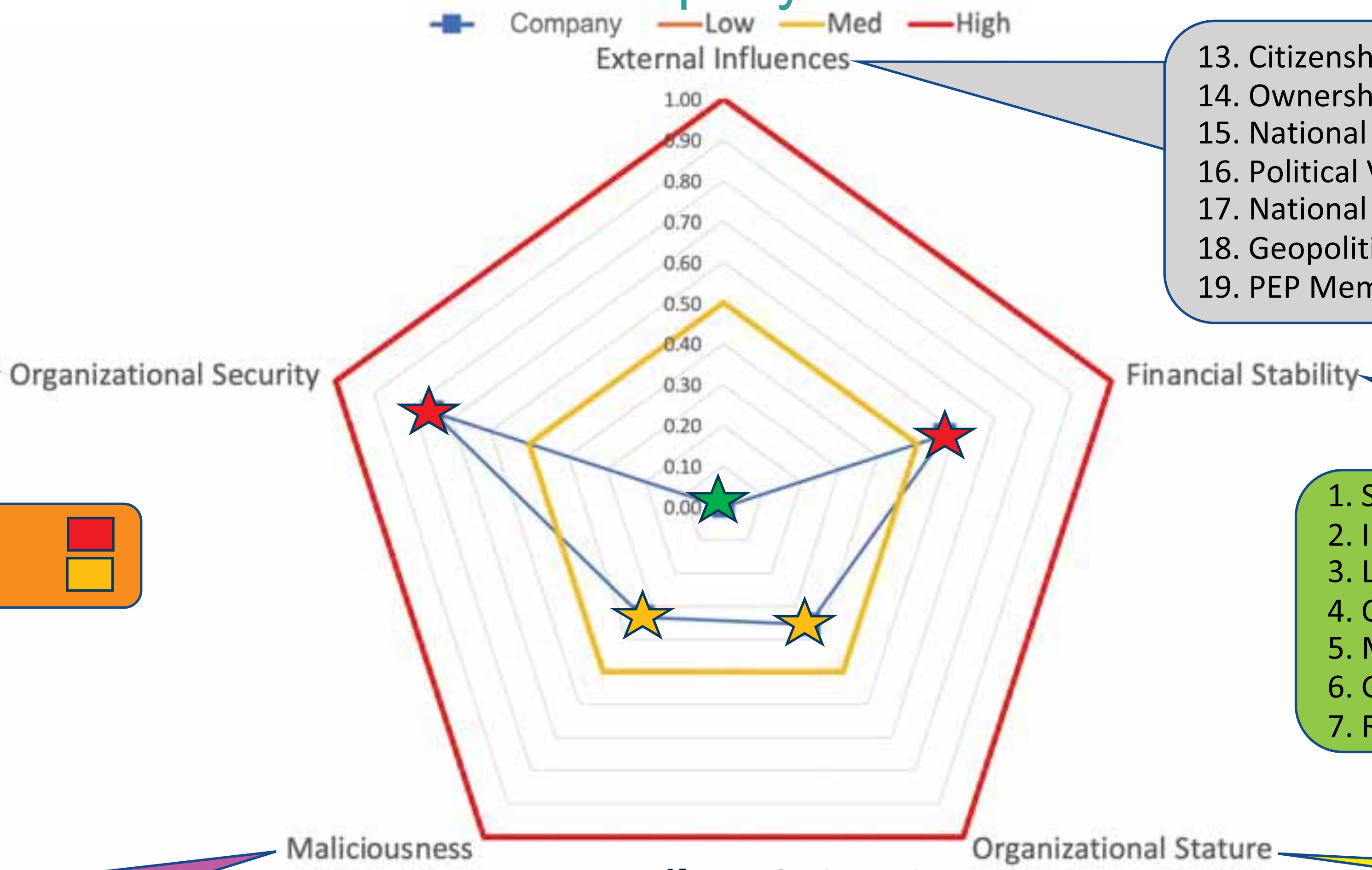


Applying

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

Company 10



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

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

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

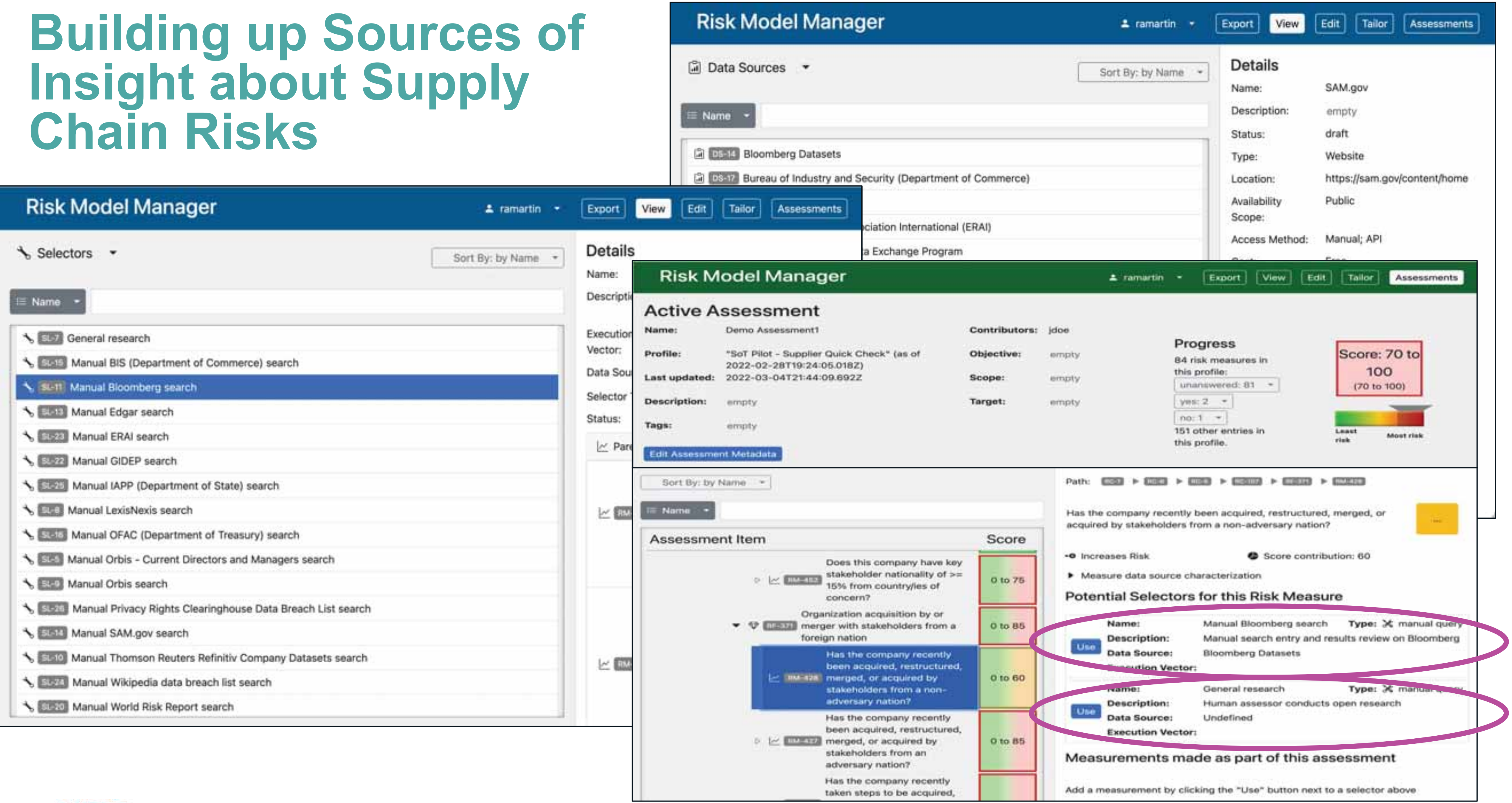
10. Intellectual Property Litigation 🟩
11. Sanction List Status 🟩
12. Fraud and Corruption 🟥

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

Pilots 1, 2, 4 & 5

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

Building up Sources of Insight about Supply Chain Risks



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

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

Active Assessment

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

Edit Assessment Metadata

Progress

84 risk measures in this profile:
unanswered: 81
yes: 2
no: 1
151 other entries in this profile.

Score: 70 to 100 (70 to 100)

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

Path: RC-1 ▶ RC-4 ▶ RC-5 ▶ RC-107 ▶ RF-371 ▶ RM-428

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

Increases Risk
Score contribution: 60
▶ Measure data source characterization

Potential Selectors for this Risk Measure

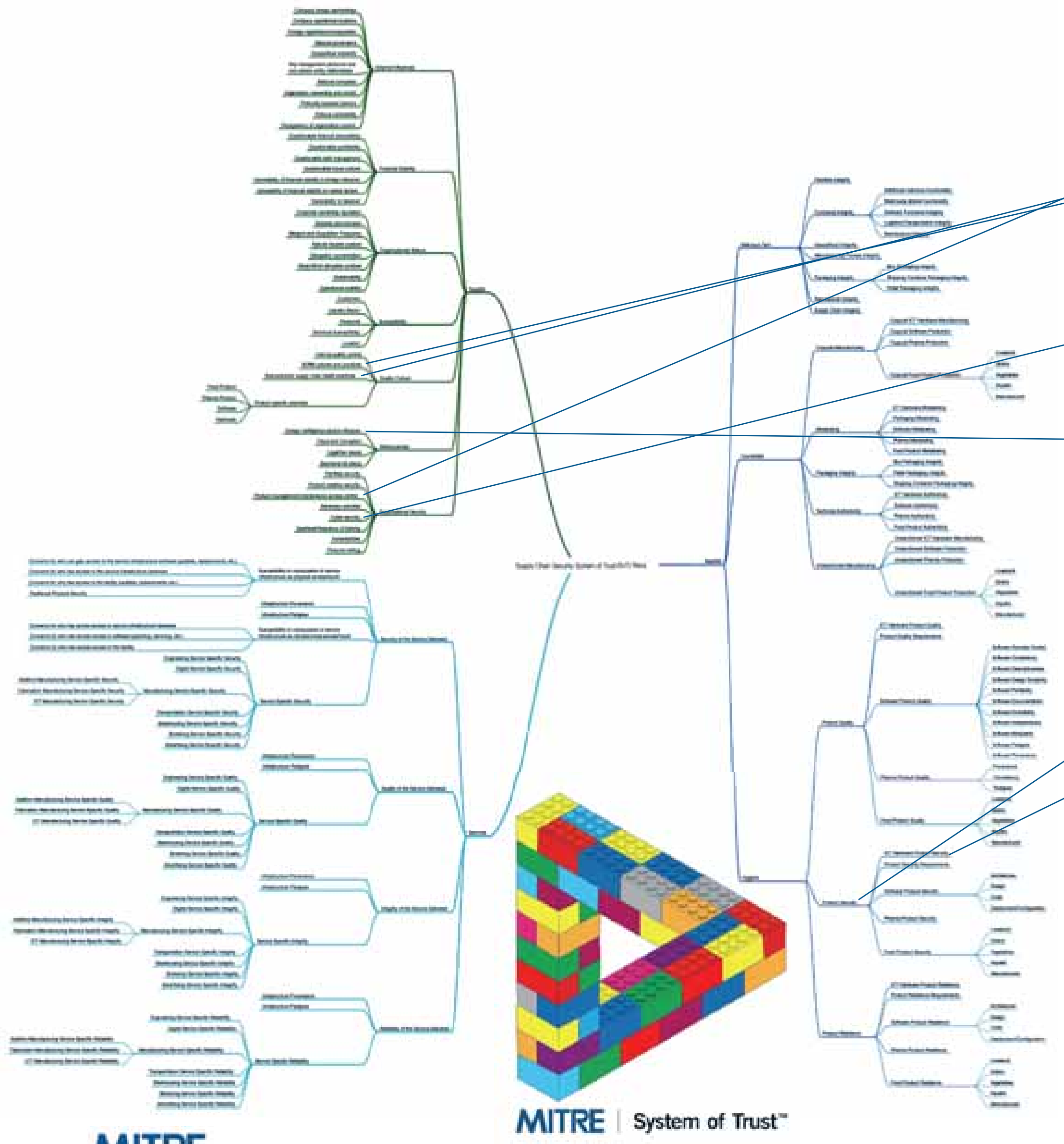
Use
Name: Manual Bloomberg search
Type: manual query
Description: Manual search entry and results review on Bloomberg
Data Source: Bloomberg Datasets
Execution Vector:

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

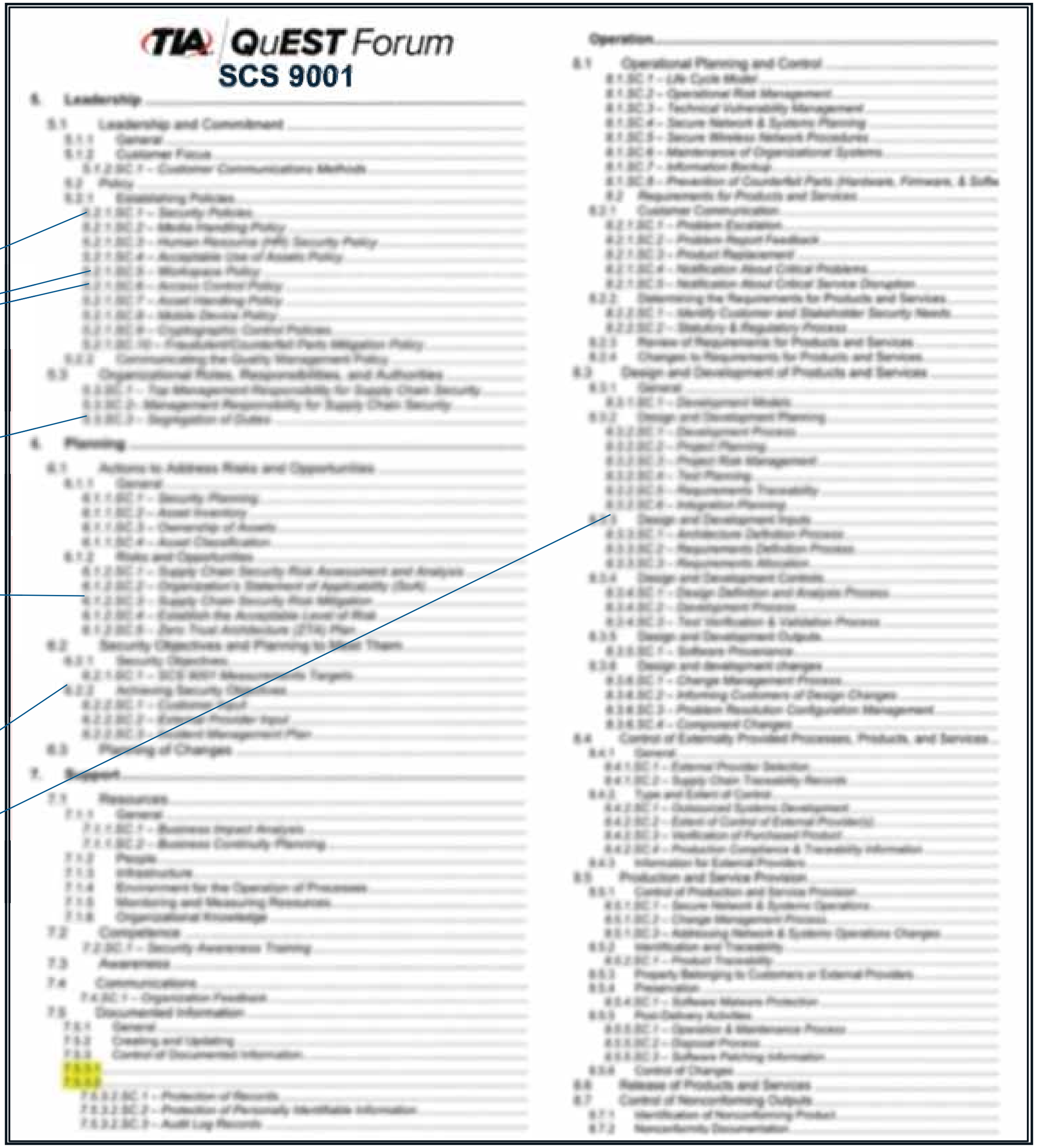
Measurements made as part of this assessment

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

Mapping SoT Risks to Assessment Information Sources / Standards



NOTIONAL



TIA | QuEST Forum
SCS 9001

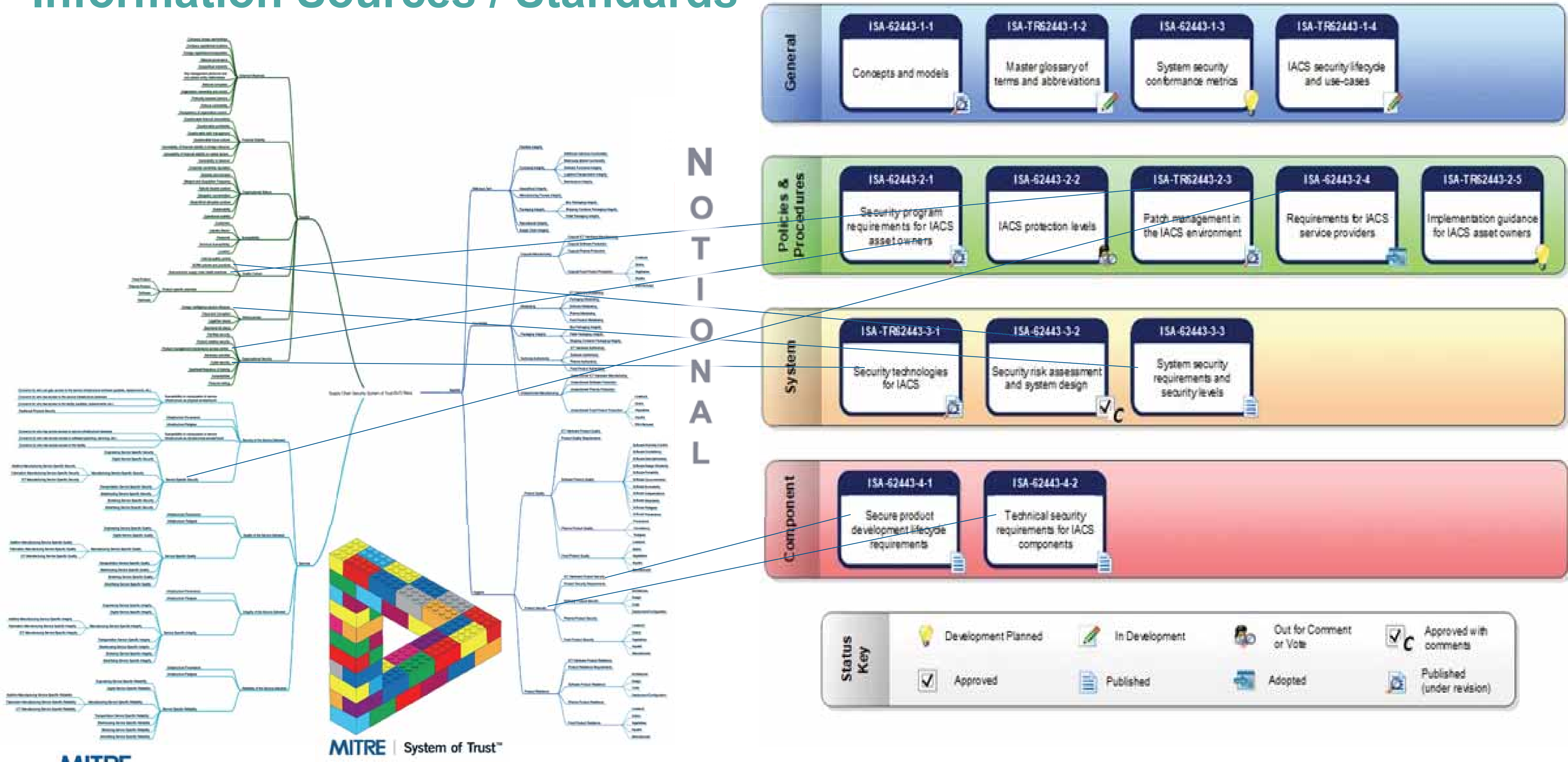
5. Leadership
- 5.1 Leadership and Commitment
  - 5.1.1 General
  - 5.1.2 Customer Focus
    - 5.1.2.SC.1 – Customer Communications Methods
- 5.2 Policy
  - 5.2.1 Establishing Policies
    - 5.2.1.SC.1 – Security Policies
    - 5.2.1.SC.2 – Media Handling Policy
    - 5.2.1.SC.3 – Human Resource (HR) Security Policy
    - 5.2.1.SC.4 – Acceptable Use of Assets Policy
    - 5.2.1.SC.5 – Workspace Policy
    - 5.2.1.SC.6 – Access Control Policy
    - 5.2.1.SC.7 – Asset Handling Policy
    - 5.2.1.SC.8 – Mobile Device Policy
    - 5.2.1.SC.9 – Cryptographic Control Policies
    - 5.2.1.SC.10 – Fraudulent/Counterfeit Parts Mitigation Policy
  - 5.2.2 Communicating the Quality Management Policy
- 5.3 Organizational Roles, Responsibilities, and Authorities
  - 5.3.SC.1 – Top Management Responsibility for Supply Chain Security
  - 5.3.SC.2 – Management Responsibility for Supply Chain Security
  - 5.3.SC.3 – Segregation of Duties

6. Planning
- 6.1 Actions to Address Risks and Opportunities
  - 6.1.1 General
    - 6.1.1.SC.1 – Security Planning
    - 6.1.1.SC.2 – Asset Inventory
    - 6.1.1.SC.3 – Ownership of Assets
    - 6.1.1.SC.4 – Asset Classification
  - 6.1.2 Risks and Opportunities
    - 6.1.2.SC.1 – Supply Chain Security Risk Assessment and Analysis
    - 6.1.2.SC.2 – Organization's Statement of Applicability (SoA)
    - 6.1.2.SC.3 – Supply Chain Security Risk Mitigation
    - 6.1.2.SC.4 – Establish the Acceptable Level of Risk
    - 6.1.2.SC.5 – Zero Trust Architecture (ZTA) Plan
- 6.2 Security Objectives and Planning to Meet Them
  - 6.2.1 Security Objectives
    - 6.2.1.SC.1 – SCS 9001 Measurements Targets
  - 6.2.2 Achieving Security Objectives
    - 6.2.2.SC.1 – Customer Input
    - 6.2.2.SC.2 – External Provider Input
    - 6.2.2.SC.3 – Incident Management Plan
- 6.3 Planning of Changes

7. Support
- 7.1 Resources
  - 7.1.1 General
    - 7.1.1.SC.1 – Business Impact Analysis
    - 7.1.1.SC.2 – Business Continuity Planning
  - 7.1.2 People
  - 7.1.3 Infrastructure
  - 7.1.4 Environment for the Operation of Processes
  - 7.1.5 Monitoring and Measuring Resources
  - 7.1.6 Organizational Knowledge
- 7.2 Competence
  - 7.2.SC.1 – Security Awareness Training
- 7.3 Awareness
- 7.4 Communications
  - 7.4.SC.1 – Organization Feedback
- 7.5 Documented Information
  - 7.5.1 General
  - 7.5.2 Creating and Updating
  - 7.5.3 Control of Documented Information
  - 7.5.3.1
  - 7.5.3.2
    - 7.5.3.2.SC.1 – Protection of Records
    - 7.5.3.2.SC.2 – Protection of Personally Identifiable Information
    - 7.5.3.2.SC.3 – Audit Log Records

Operation
- 8.1 Operational Planning and Control
  - 8.1.SC.1 – Life Cycle Model
  - 8.1.SC.2 – Operational Risk Management
  - 8.1.SC.3 – Technical Vulnerability Management
  - 8.1.SC.4 – Secure Network & Systems Planning
  - 8.1.SC.5 – Secure Wireless Network Procedures
  - 8.1.SC.6 – Maintenance of Organizational Systems
  - 8.1.SC.7 – Information Backup
  - 8.1.SC.8 – Prevention of Counterfeit Parts (Hardware, Firmware, & Softw
- 8.2 Requirements for Products and Services
  - 8.2.1 Customer Communication
    - 8.2.1.SC.1 – Problem Escalation
    - 8.2.1.SC.2 – Problem Report Feedback
    - 8.2.1.SC.3 – Product Replacement
    - 8.2.1.SC.4 – Notification About Critical Problems
    - 8.2.1.SC.5 – Notification About Critical Service Disruption
  - 8.2.2 Determining the Requirements for Products and Services
    - 8.2.2.SC.1 – Identify Customer and Stakeholder Security Needs
    - 8.2.2.SC.2 – Statutory & Regulatory Process
  - 8.2.3 Review of Requirements for Products and Services
  - 8.2.4 Changes to Requirements for Products and Services
- 8.3 Design and Development of Products and Services
  - 8.3.1 General
    - 8.3.1.SC.1 – Development Models
  - 8.3.2 Design and Development Planning
    - 8.3.2.SC.1 – Development Process
    - 8.3.2.SC.2 – Project Planning
    - 8.3.2.SC.3 – Project Risk Management
    - 8.3.2.SC.4 – Test Planning
    - 8.3.2.SC.5 – Requirements Traceability
    - 8.3.2.SC.6 – Integration Planning
  - 8.3.3 Design and Development Inputs
    - 8.3.3.SC.1 – Architecture Definition Process
    - 8.3.3.SC.2 – Requirements Definition Process
    - 8.3.3.SC.3 – Requirements Allocation
  - 8.3.4 Design and Development Controls
    - 8.3.4.SC.1 – Design Definition and Analysis Process
    - 8.3.4.SC.2 – Development Process
    - 8.3.4.SC.3 – Test Verification & Validation Process
  - 8.3.5 Design and Development Outputs
    - 8.3.5.SC.1 – Software Provenance
  - 8.3.6 Design and development changes
    - 8.3.6.SC.1 – Change Management Process
    - 8.3.6.SC.2 – Informing Customers of Design Changes
    - 8.3.6.SC.3 – Problem Resolution Configuration Management
    - 8.3.6.SC.4 – Component Changes
- 8.4 Control of Externally Provided Processes, Products, and Services
  - 8.4.1 General
    - 8.4.1.SC.1 – External Provider Selection
    - 8.4.1.SC.2 – Supply Chain Traceability Records
  - 8.4.2 Type and Extent of Control
    - 8.4.2.SC.1 – Outsourced Systems Development
    - 8.4.2.SC.2 – Extent of Control of External Provider(s)
    - 8.4.2.SC.3 – Verification of Purchased Product
    - 8.4.2.SC.4 – Production Compliance & Traceability Information
  - 8.4.3 Information for External Providers
- 8.5 Production and Service Provision
  - 8.5.1 Control of Production and Service Provision
    - 8.5.1.SC.1 – Secure Network & Systems Operations
    - 8.5.1.SC.2 – Change Management Process
    - 8.5.1.SC.3 – Addressing Network & Systems Operations Changes
  - 8.5.2 Identification and Traceability
    - 8.5.2.SC.1 – Product Traceability
  - 8.5.3 Property Belonging to Customers or External Providers
  - 8.5.4 Preservation
    - 8.5.4.SC.1 – Software Malware Protection
  - 8.5.5 Post-Delivery Activities
    - 8.5.5.SC.1 – Operation & Maintenance Process
    - 8.5.5.SC.2 – Disposal Process
    - 8.5.5.SC.3 – Software Patching Information
  - 8.5.6 Control of Changes
- 8.6 Release of Products and Services
- 8.7 Control of Nonconforming Outputs
  - 8.7.1 Identification of Nonconforming Product
  - 8.7.2 Nonconformity Documentation

Mapping SoT Risks to Assessment Information Sources / Standards



ISA/IEC 62443

NOTIONAL

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

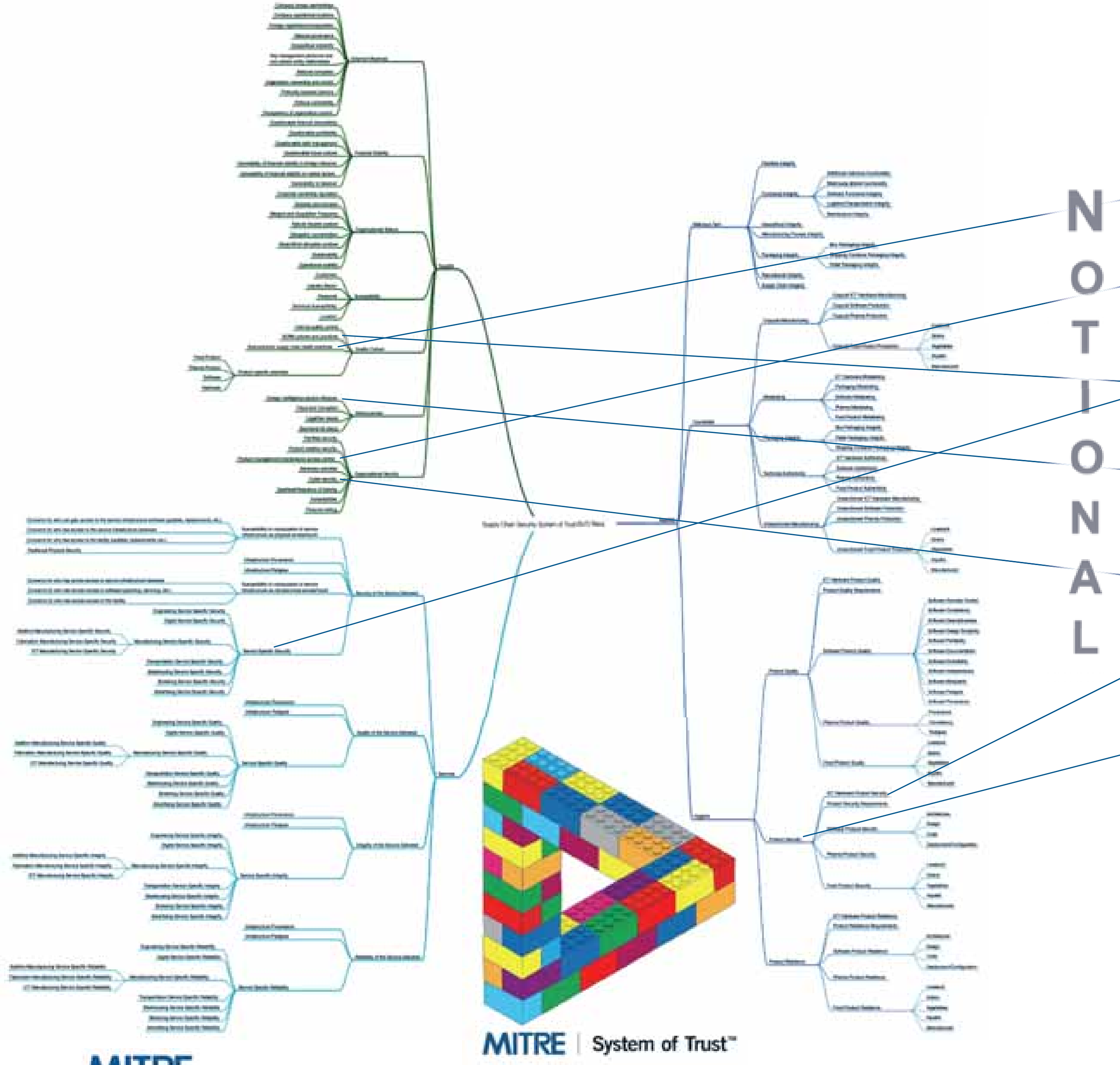
Status Key

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

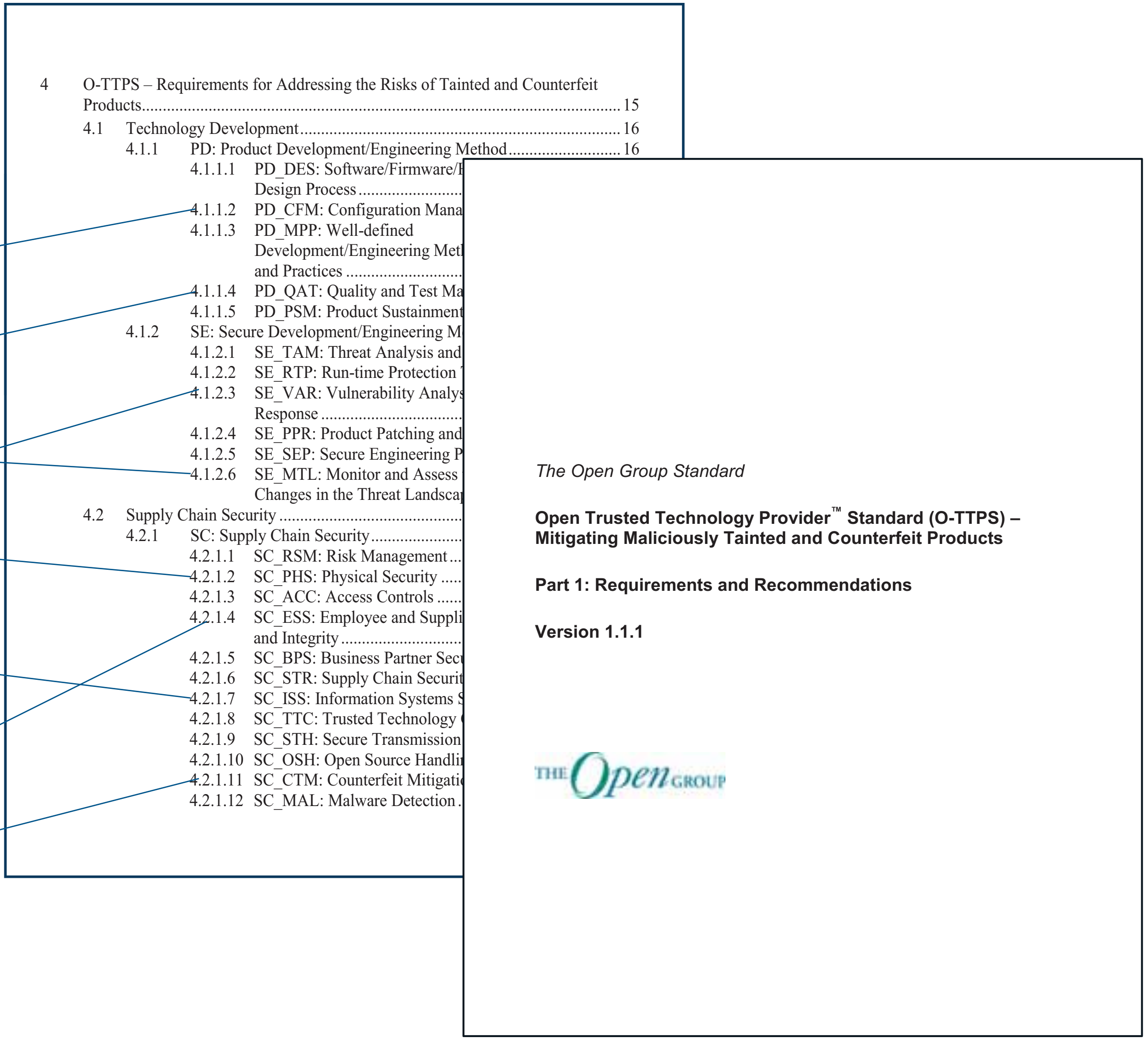
MITRE | System of Trust™

MITRE

Mapping SoT Risks to Assessment Information Sources / Standards



ISO/IEC 20243



The Open Group Standard

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

Part 1: Requirements and Recommendations

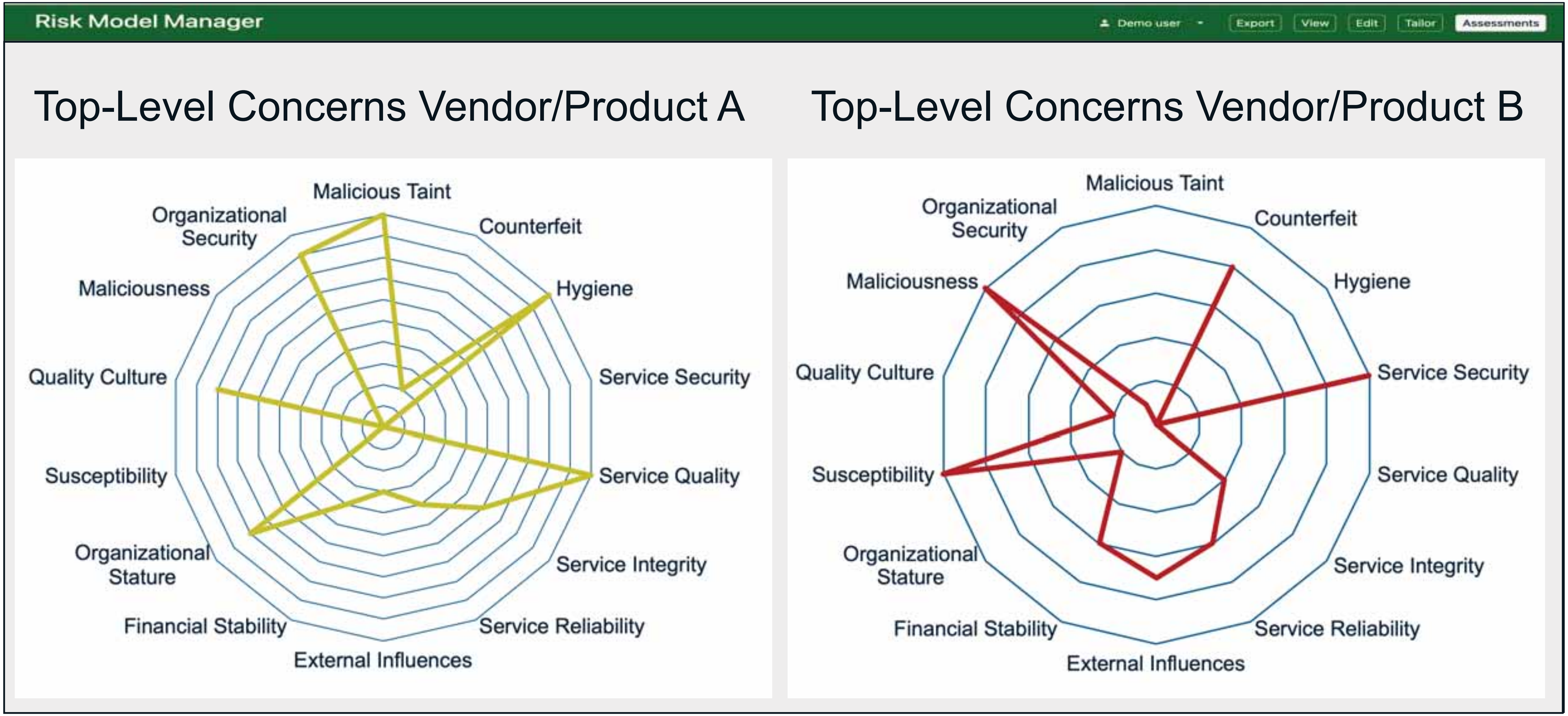
Version 1.1.1

THE Open GROUP

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

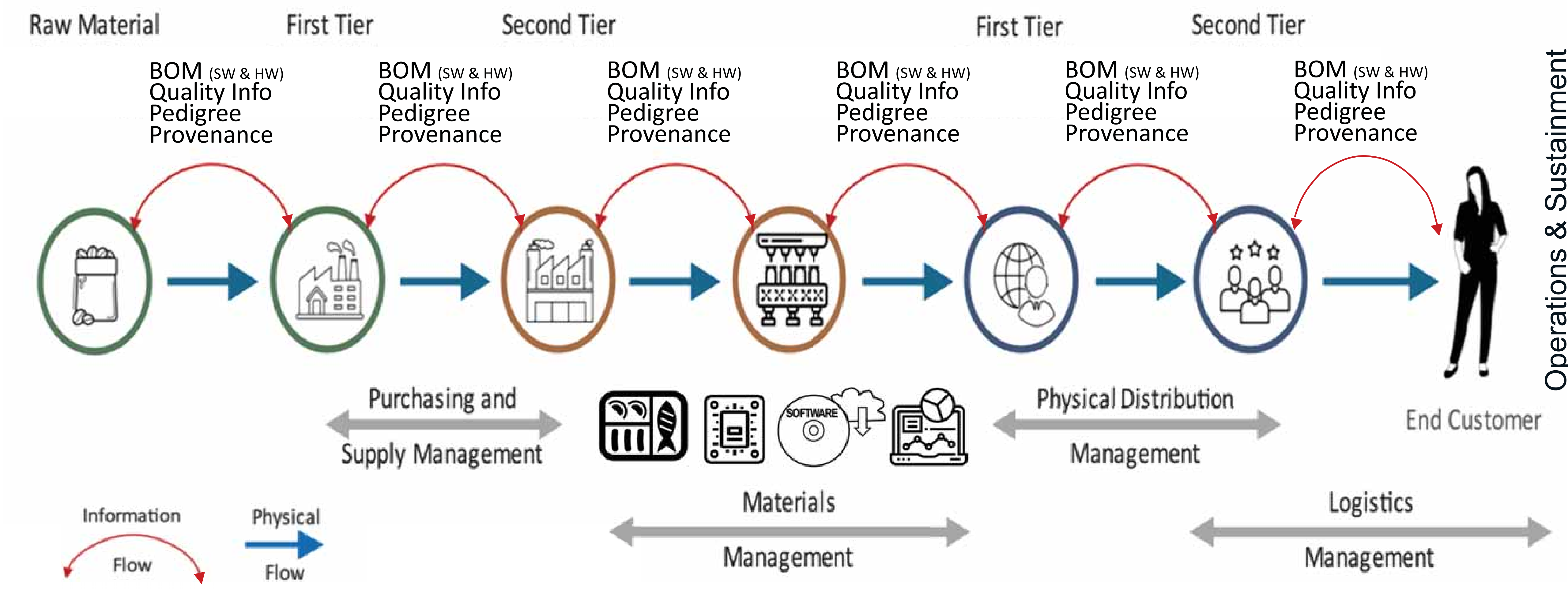
MITRE

GOAL for use of SoT in Industry and Government…



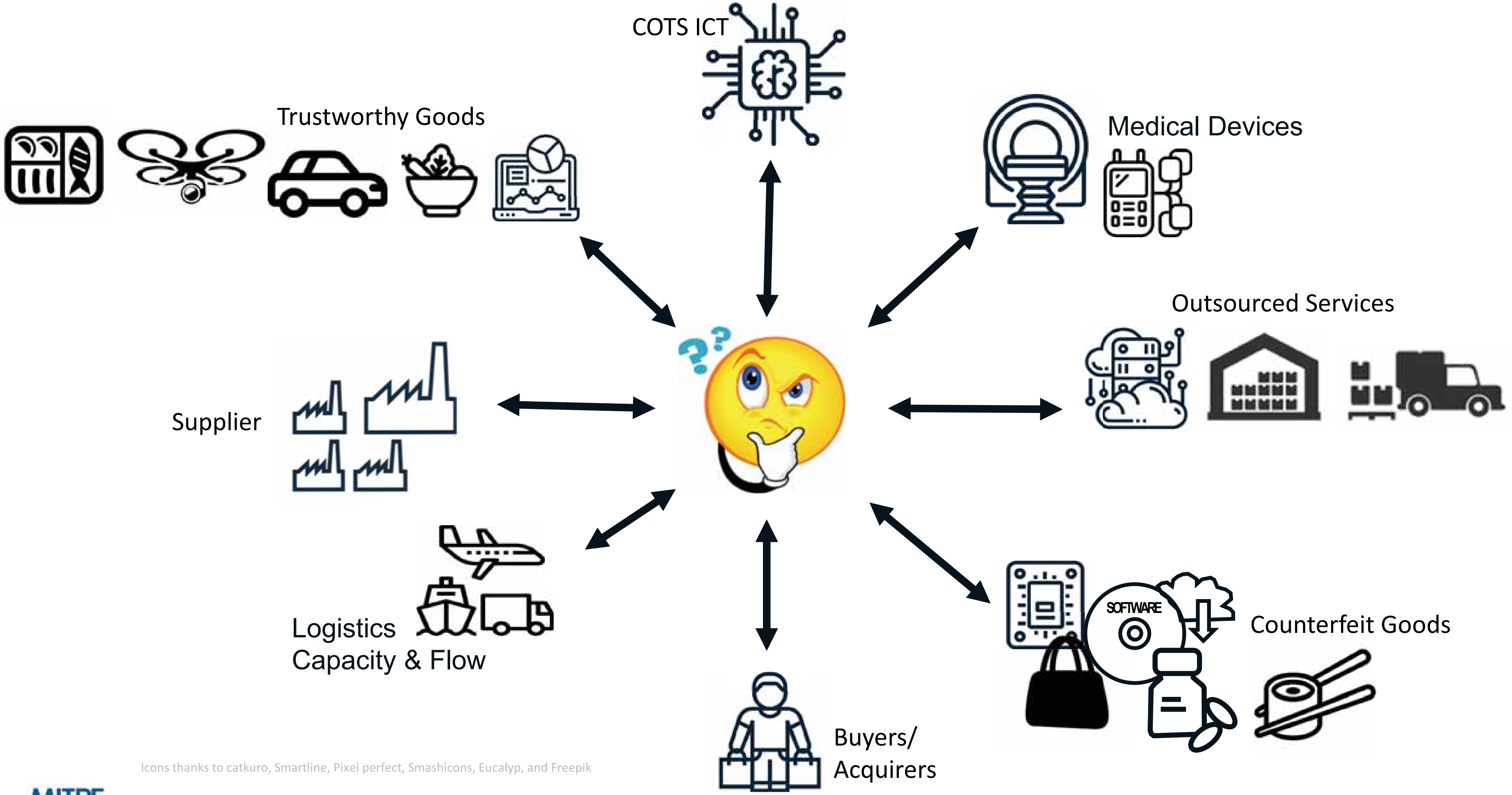
MITRE

Supply Chains – As multi-Stakeholder Network



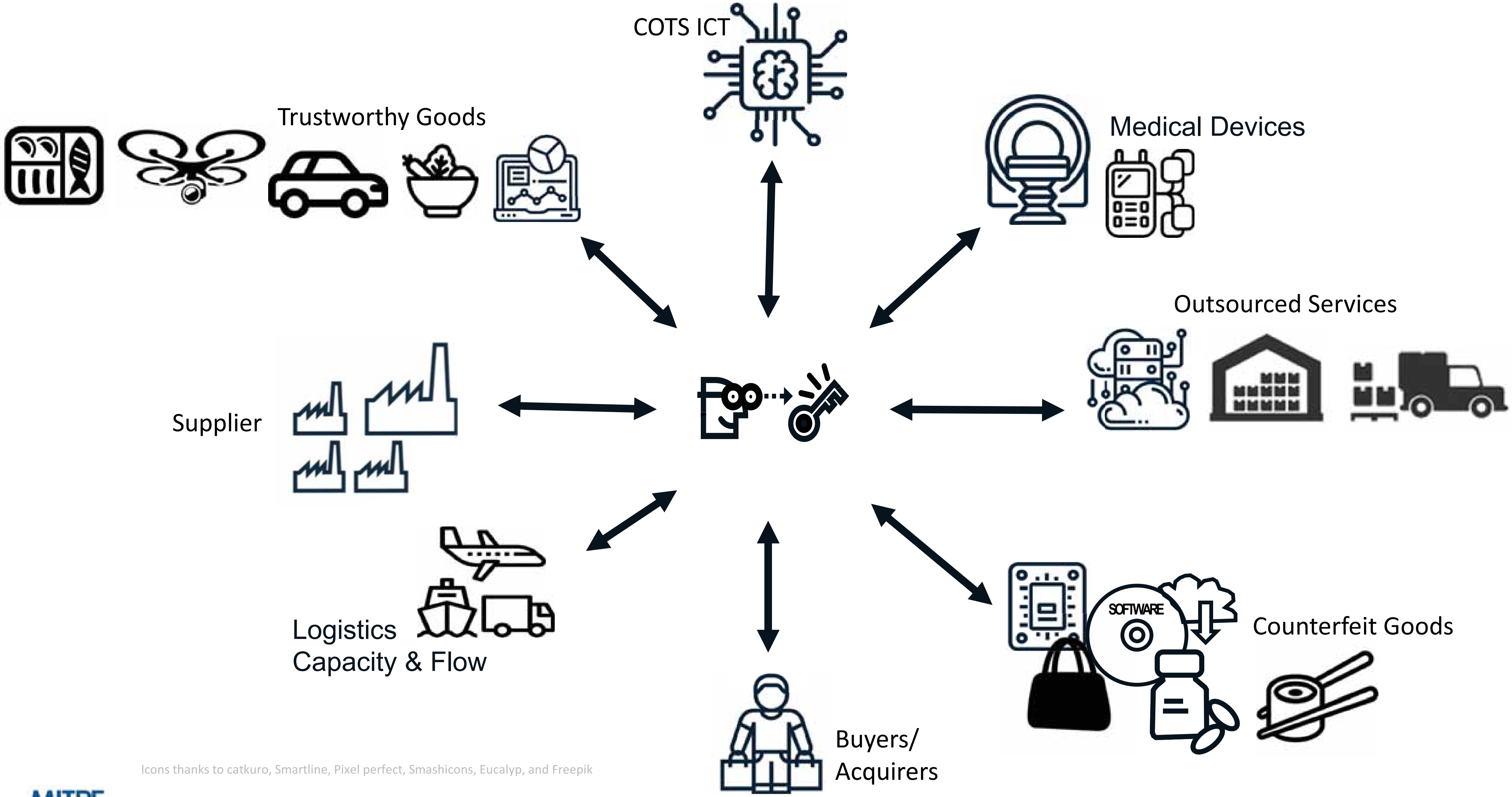
https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

Effective Supply Chain Trust Interactions



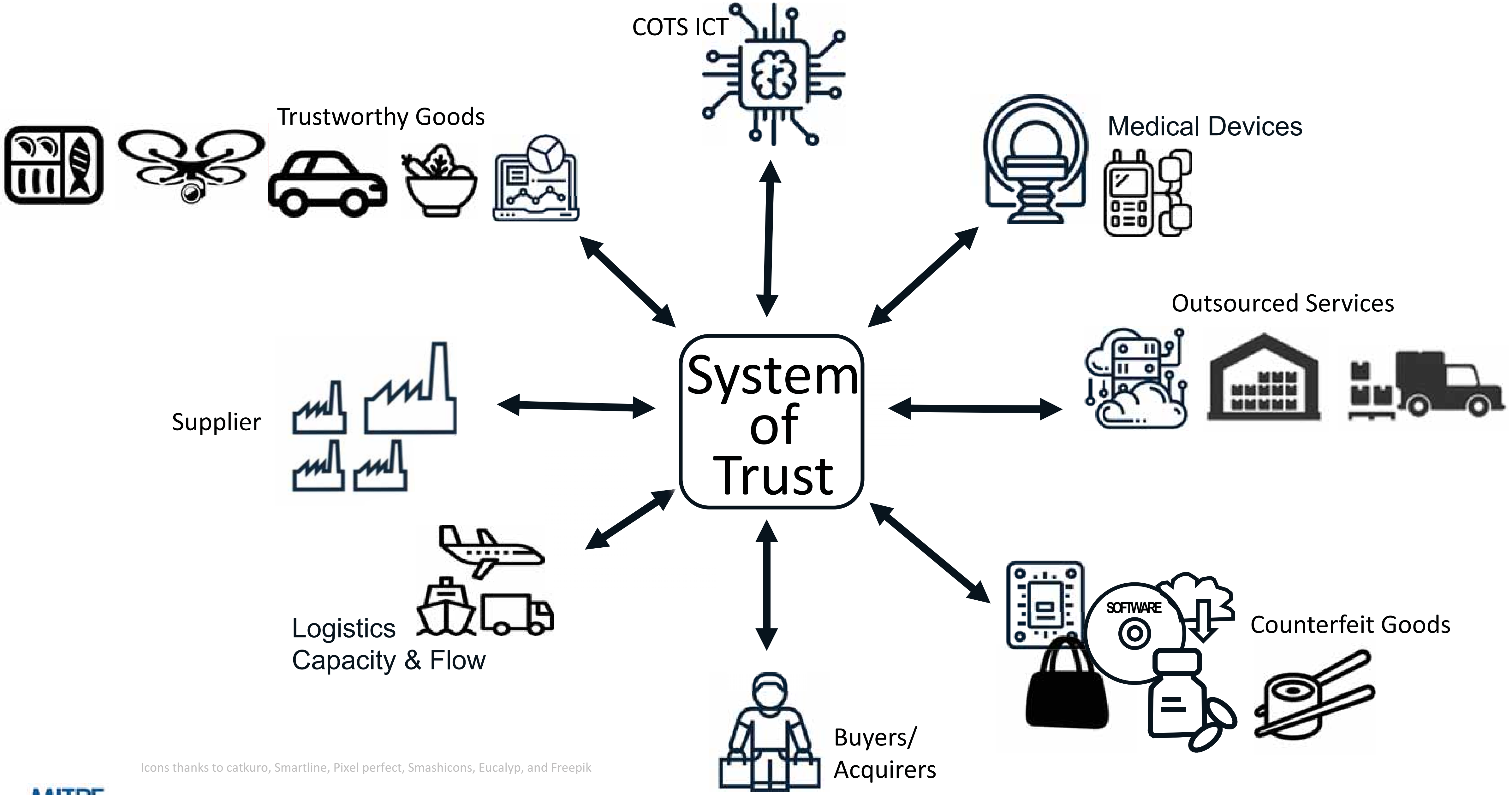
Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

Effective Supply Chain Trust Interactions



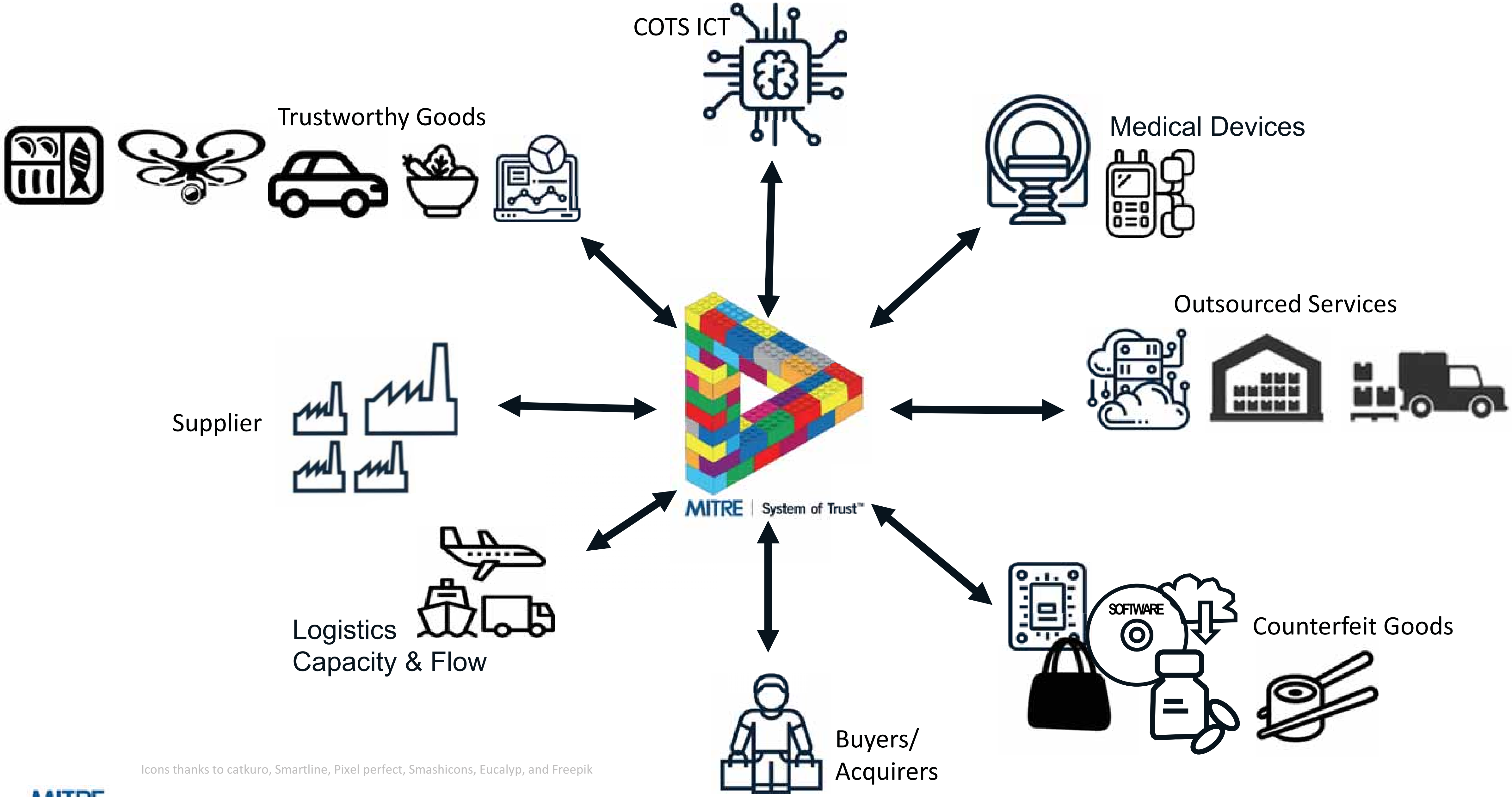
Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

Effective Supply Chain Trust Interactions



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

Effective Supply Chain Trust Interactions



COTS ICT

Trustworthy Goods

Medical Devices

Outsourced Services

Supplier

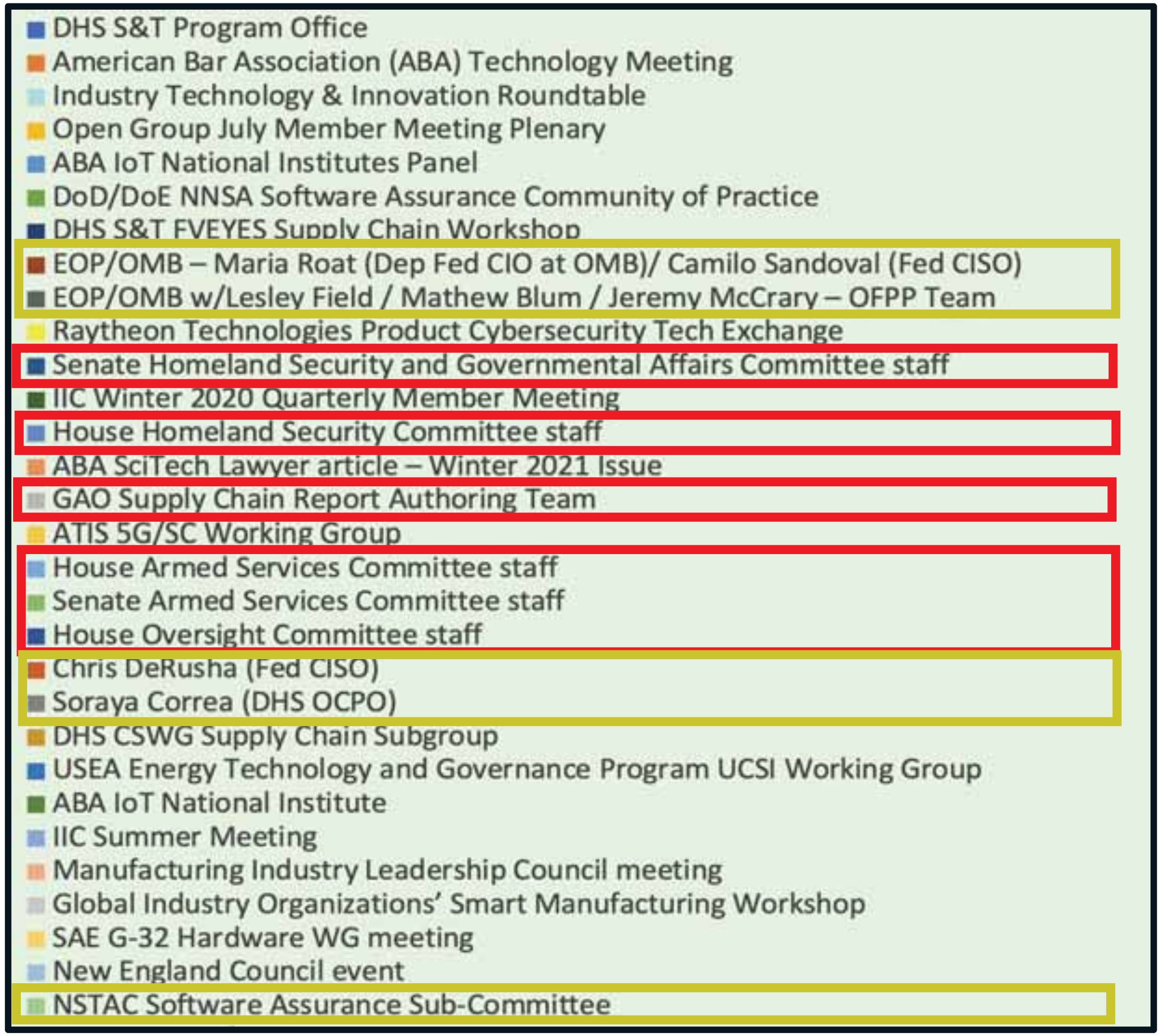
Logistics
Capacity & Flow

Counterfeit Goods

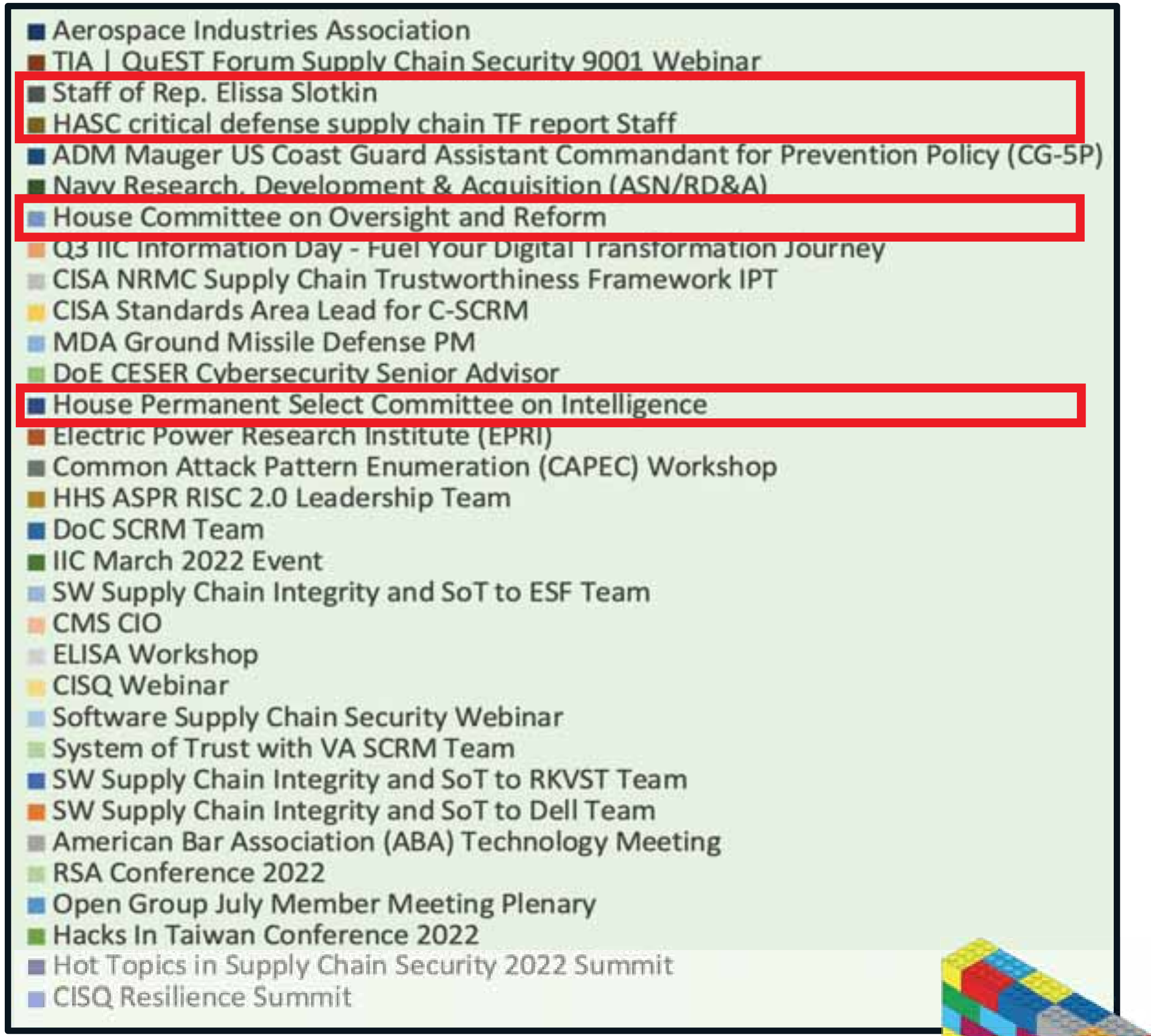
Buyers/
Acquirers

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

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

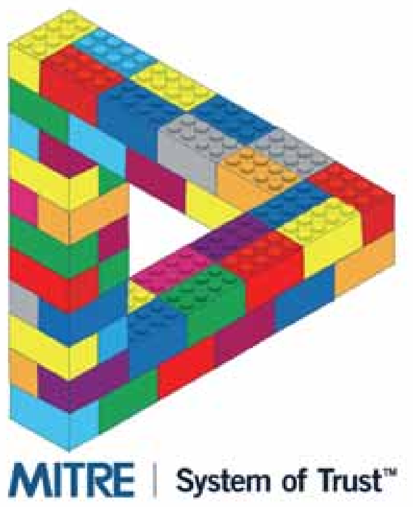
🟨 Executive Acquisition

🟥 Congressional Committees

MITRE

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…

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 disruptive 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.

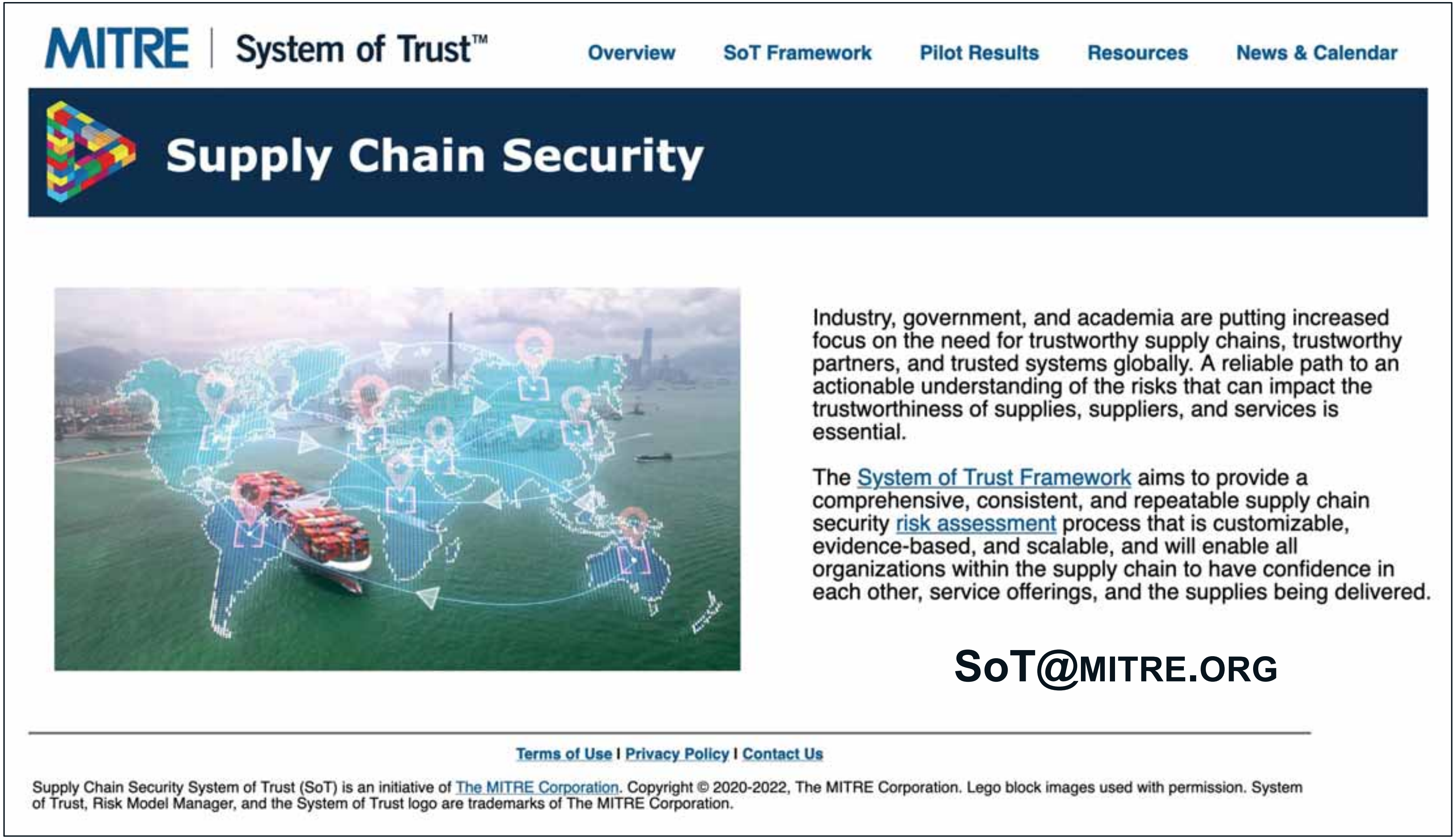
Supply chain security is at the center of many of today's national security challenges.[1] Few things illustrate this reality as well as the recent SolarWinds software supply chain hack where it was discovered that the U.S. has been the target of a massive Russian espionage campaign,[2] exploiting trust 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

MITRE

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.

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