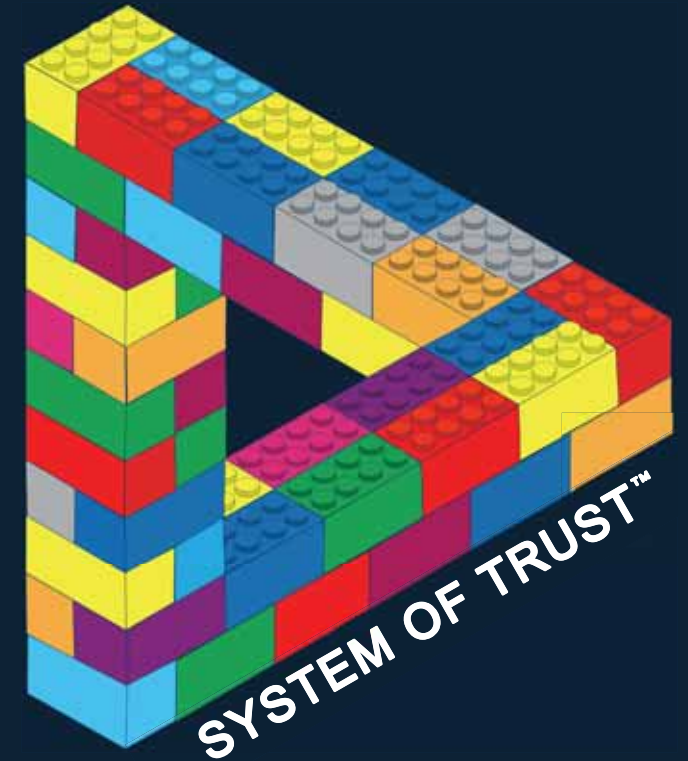


# MITRE System of Trust

**CORE TEAM.** *BOB MARTIN, BRIAN HALL, MIKE RIPLEY,  
SEAN BARNUM, PAUL GARVEY, MICHAEL  
AISENBERG, RON HODGE, KEITH HILL,  
JUSTIN YEAGER, CHUCK LEWIS*

**March 03, 2021**



**MITRE**

**SOLVING PROBLEMS  
FOR A SAFER WORLD™**

# Difficult Interactions for Supply Chain Participants Regarding Trust

(circa 2020)



Trustworthy  
SW/HW



High Value & High  
Unit cost COTS

Supplier



Outsourced  
Services

Data

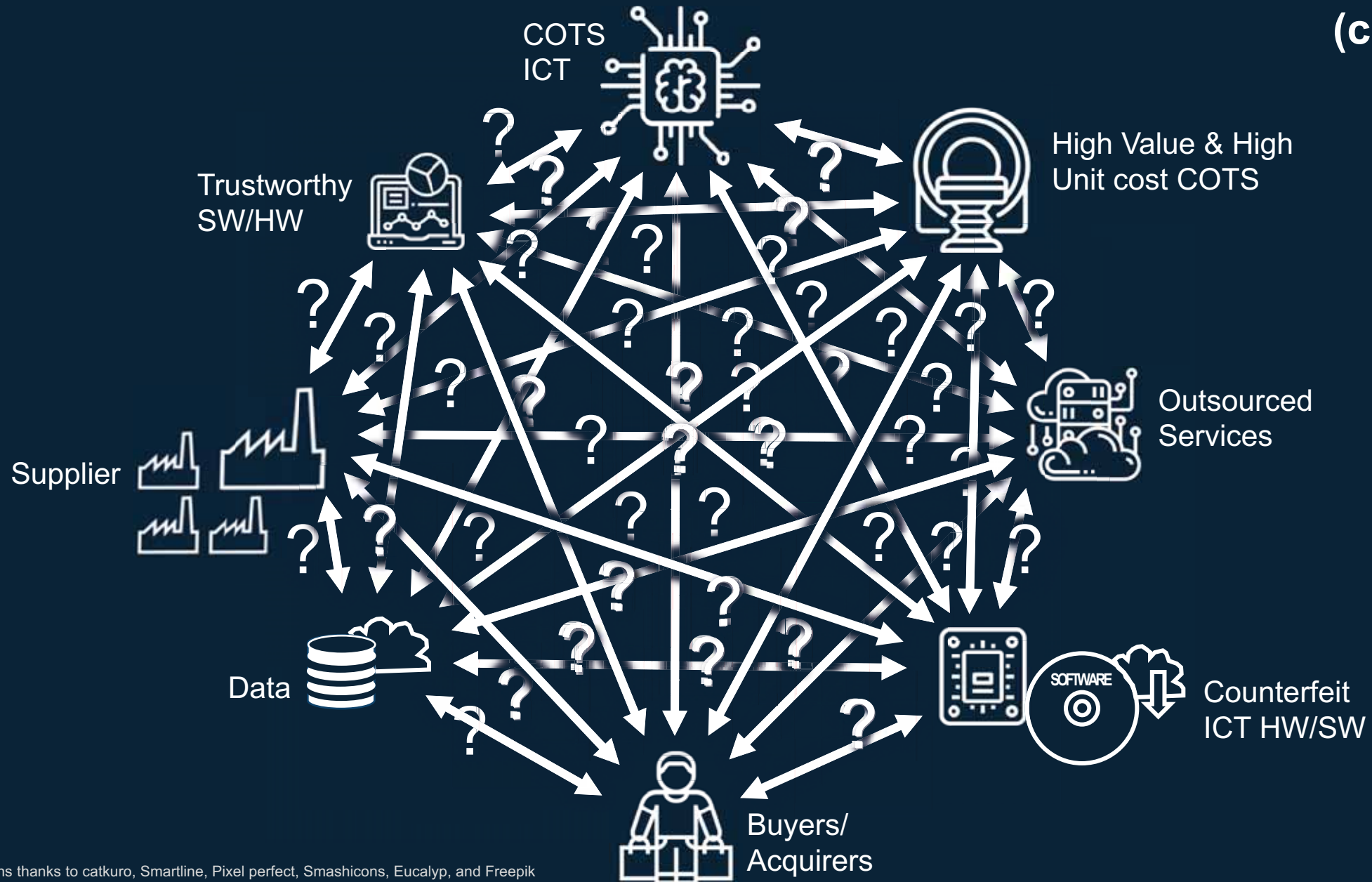


Counterfeit  
ICT HW/SW



Buyers/  
Acquirers

# Difficult Interactions for Supply Chain Participants Regarding Trust (circa 2020)



# The System of Trust Program's Main Two Aspects

## 30+ Publicly Available Items on Supply Chain Security Risk Areas

1. ANSI Homeland Security Standards Panel, "Final Workshop Report - Global Supply Chain Security Standards", November 2012.
2. The Software Alliance, "The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle", April 2019.
3. "Software Trustworthiness Best Practices - An Industrial Internet Consortium White Paper", March 2020.
4. Cohen, Brian, "A Framework for Understanding Trustworthy Suppliers", February 2015.
5. "The Evolution Path for Industrial Software Quality Evaluation Methods Applying ISO/IEC 9126:2001 Quality Model: Example of MITRE's SQA Method", March 2005.
6. "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", Proceedings of the IEEE, Vol. 102, No. 8, August 2014.
7. MITRE Corporation, "Deliver Uncompromised", August 2018.
8. MITRE Corporation, "Deliver Uncompromised - Tax and Insurance Roundtable Summary of Conclusions", March 2019.
9. MITRE Corporation, "Deliver Uncompromised - Legislative Protections and Contract Language Summary of Conclusions", March 2019.
10. "Hardware Intrusion Detection for Supply-Chain Threats to Critical Infrastructure Embedded Systems", 2012.
11. "Risk Management of Outsourced Technology Services", November 2000.
12. Government Accountability Office, "Report to Congressional Committees - Defense Procurement - Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership", November 2018.
13. "Constructive Disruption White Paper: Exploiting Publicly Available Information to Address Today's Security Challenges", February 2018.
14. "Hardware Security and Supply Chain Risk Management", September 2019, Public Release Case number: 19-2459.
15. "Novel Long-Line Supply Chain Campaign", August 2019.
16. "Providing a Framework for Effective Software Quality Assessment - A First Step in Automating Assessments", The First Annual Software Engineering & Economics Conference on Software Systems Modernization, April 1996.
17. "Supply Chain Attack Patterns: Framework and Catalog", 2013.
18. "The Growing Threat to Air Force Mission-Critical Electronics: Lethality at Risk: Unclassified Summary", 2019.
19. "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, April 2018.
20. NIST Draft NISTIR 8272, "Impact Analysis Tool for Interdependent Cyber Supply Chain Risks", March 2020.
21. "Automated Source Code Quality Measures (ASCOM)", Version 1.0, January 2020.
22. The Open Group, "Open Trusted Technology Provider Standard (OTTPS) - Mitigating Maliciously Tainted and Counterfeit Products - Parts 1 and 2 and ISO/IEC 20243-1:2018", Version 1.1.1, 2018.
23. The Open Group, "An Approach to Assessing Vendors to Lower Potential Risk of Outsourced Network Services", March 2020.
24. The Open Group, "Securing the Network and Supply Chain with Industry-Driven Standards", January 2020.
25. Open Web Application Security Project (2019) OWASP Application Security Verification Standard 4.0.
26. Open Web Application Security Project (2014) OWASP Testing Guide 4.0.
27. Payment Card Industry (PCI) Security Standards Council (2018) Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures Version 1.0.
28. SAFECODE (2012) Practical Security Stories and Security Tasks for Agile Development Environments.
29. SAFECODE (2018) Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program, Third Edition.
30. SAFECODE (2017) Managing Security Risks Inherent in the Use of Third-Party Components.
31. SAFECODE (2010) Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain. Software Assurance Forum for Excellence in Code (2017) Tactical Threat Modeling.
32. "Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security", Proceedings of the 11th International Conference on Cyber Warfare & Security, March 2016.
33. "Supply Chain Solutions for Smart Grid Security - Building on Business Best Practices", 2012.
34. NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations", April 2015.
35. "Assessing Risk Of Outsourcing the Crown Jewels", March 2017.
36. "State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation" Institute for Defense Analyses (IDA), Alexandria, VA, IDA Paper P-8005, 2016.
37. IT Sector Coordinating Council, "Managing ICT Supply Chain Risk: The Outsourcing Network Services Assessment Tool (ONSAT) downloadable Spreadsheet", July 2020.
38. IT Sector Coordinating Council, "Managing ICT Supply Chain Risk: The Outsourcing Network Services Assessment Tool (ONSAT) detailed User Manual", July 2020.

# The System of Trust Program's Main Two Aspects

**40+ MITRE Supply Chain  
Related Efforts and Past  
Endeavors**

# The System of Trust Program's Main Two Aspects



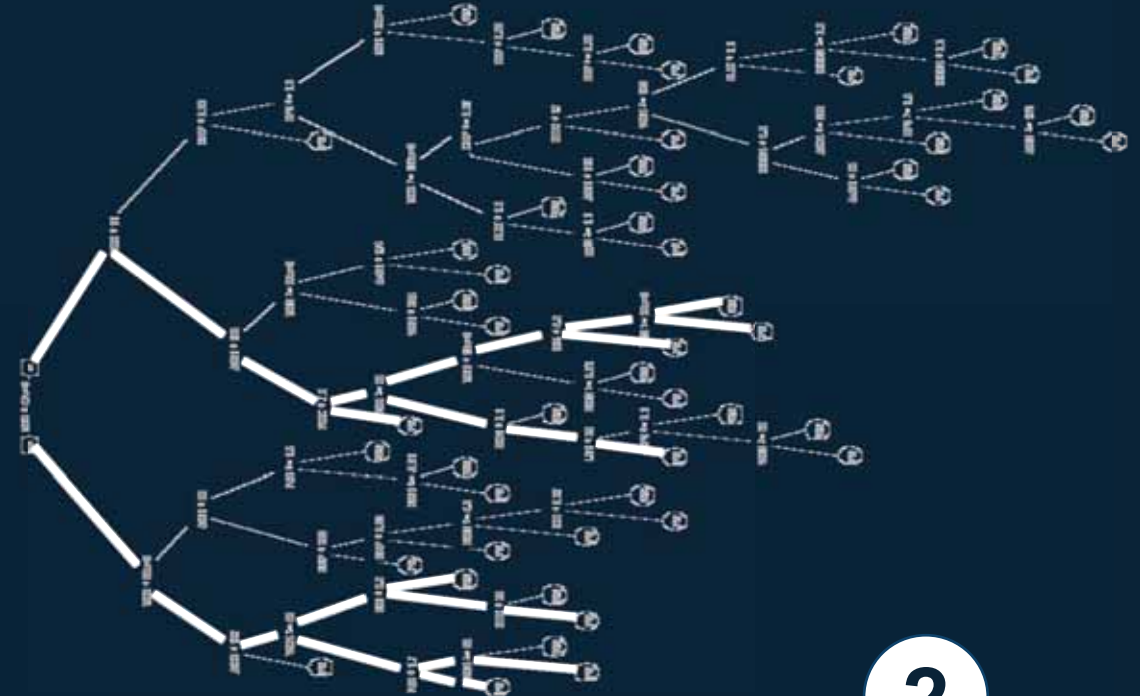
Address Chaos, Align & Organize



# The System of Trust Program's Main Two Aspects

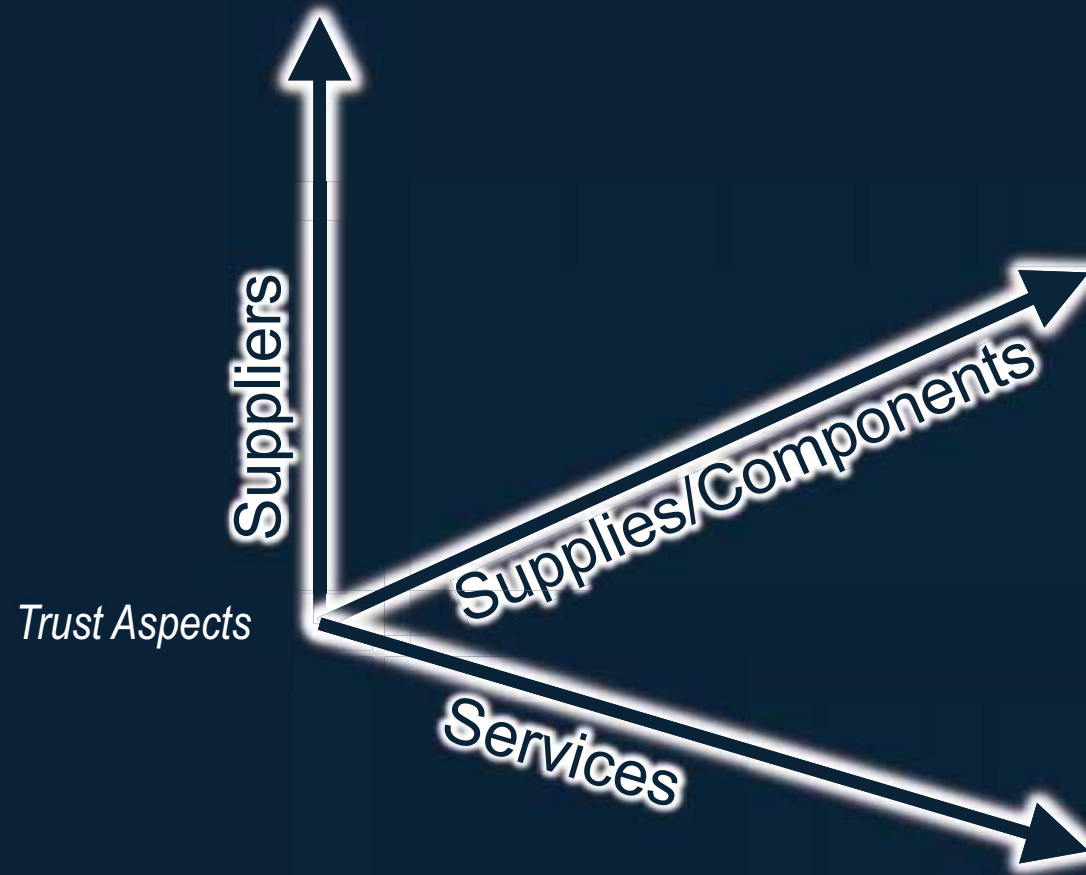


Address Chaos, Align & Organize



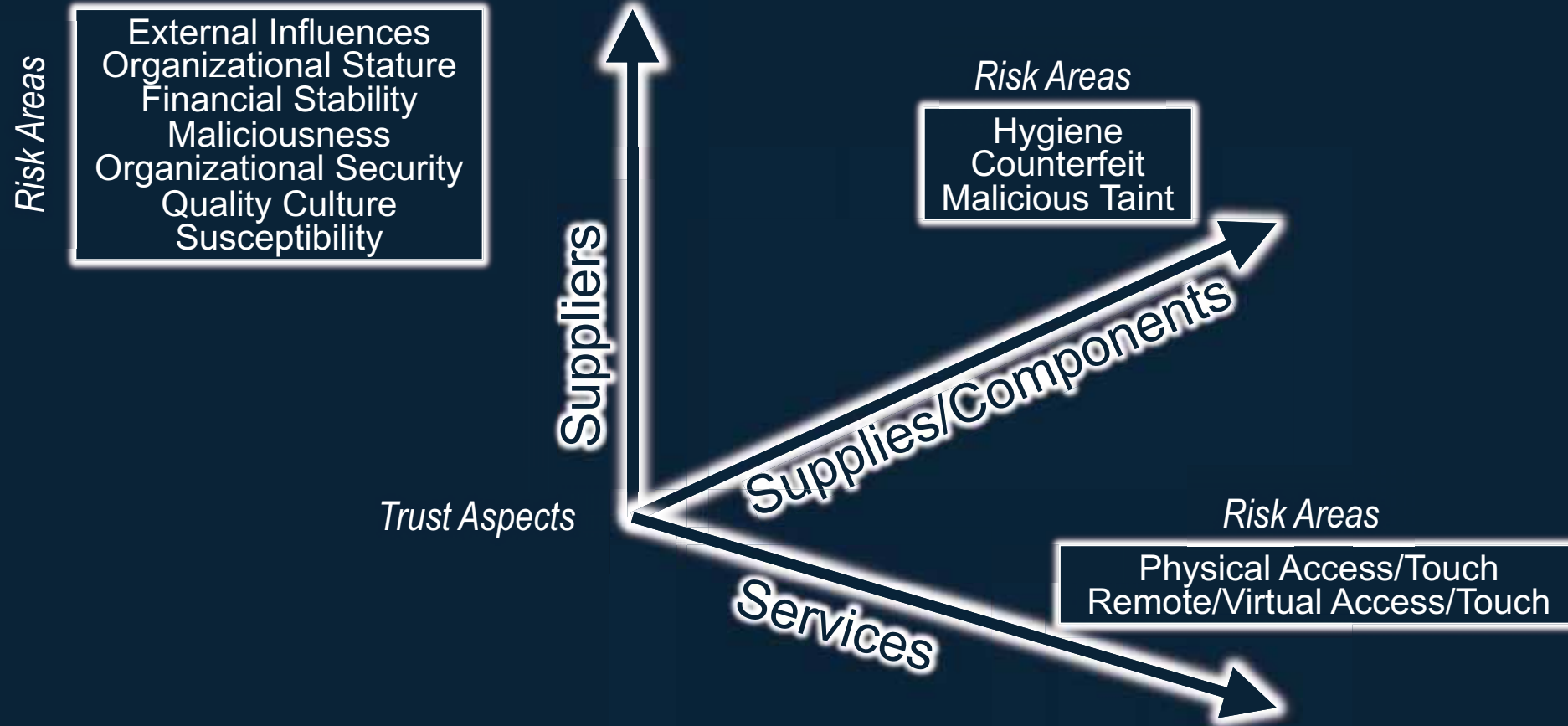
Simplify, Tailor & Make Usable

# Basis of Trust





# Basis of Trust



# Basis of Trust

*Risk Areas*

Financial Health  
Ownership  
Partners  
Leadership  
Personnel  
Training  
History  
Product Strategy

Reputation  
Agreements  
Legal/Law Issues  
Facilities Security  
Cyber Security  
Software Assurance  
Hardware Assurance  
Market position

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

*Suppliers*

*Trust Aspects*

*Risk Areas*

Hygiene  
Counterfeit  
Malicious Taint

Shipping Container  
Pallet  
Box  
Device  
Boards  
Chips (FPGA/ASIC)

Firmware/Bitstream  
Software Quality  
Software Composition  
Software Pedigree  
Software Provenance  
Updates

*Supplies/Components*

*Risk Areas*

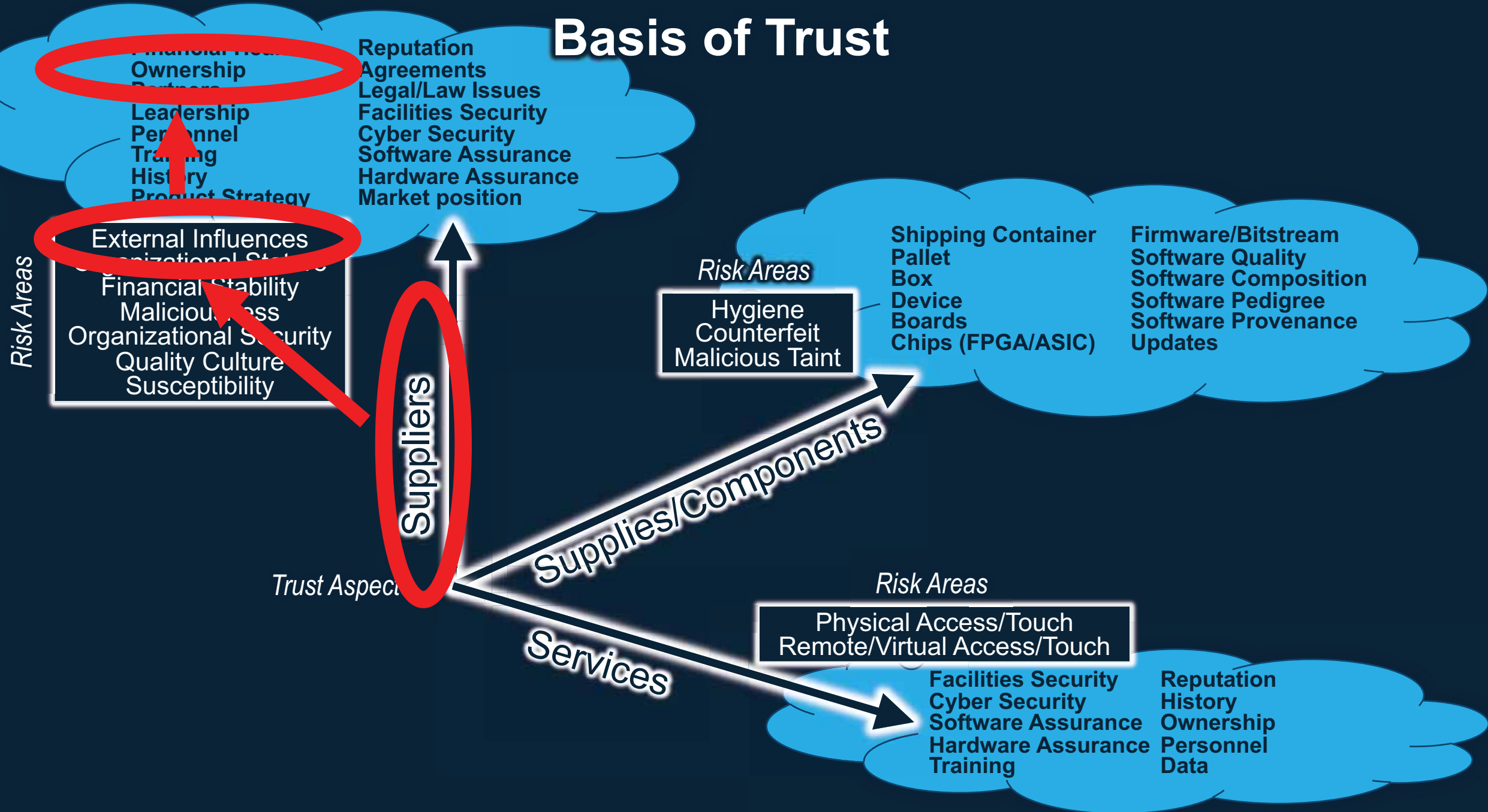
Physical Access/Touch  
Remote/Virtual Access/Touch

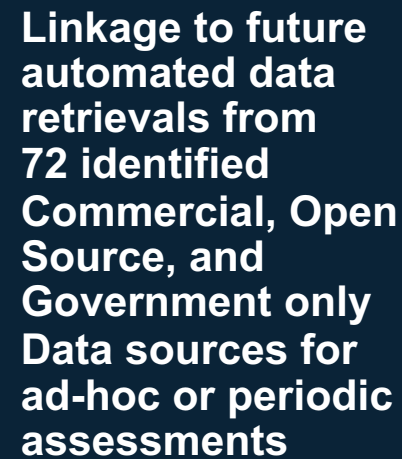
*Services*

Facilities Security  
Cyber Security  
Software Assurance  
Hardware Assurance  
Training

Reputation  
History  
Ownership  
Personnel  
Data

# Basis of Trust



[illegible][illegible]



# Risk Model Manager



## Type of Acquisition Issues

- ☐ COTS ICT
- ☐ Trustworthy SW/HW
- ☒ Supplier
- ☐ High Value & High Unit cost COTS
- ☐ Outsourced Services
- ☐ Counterfeit ICT HW/SW

## Assessment Scope, Skills & Means

- ☒ Open Source Information
- ☒ Purchased Data Sources
- ☐ Written Questions
- ☐ Oral Discussions
- ☐ Sampling of Components
- ☐ Software Analysis
- ☐ Intelligence Service Investigation

## Pilot 1 Supplier with Purchased & Public Data Profile [notional]

## Acquiring Organization

- ☒ US Federal Government
- ☐ US Military
- ☐ State/Local
- ☐ Tribal
- ☐ US Critical Infrastructure
- ☐ US DIB
- ☐ Commercial
- ☐ Small Business

## Assessment Constraints

- ☒ Time Period
  - ☐ Weeks
  - ☐ Days
  - ☒ Hours
- ☒ Monies for Data Purchase
- ☐ Investigative Staff Available



# Risk Model Manager

## Pilot 2 Supplier and Service with Purchased & Public Data Profile [notional]



### 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

## Pilot 3 Analysis of Software Supply Item Profile [notional]



### 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

## Pilot 4 Supplier with Purchased & Public Data Profile [notional]



### 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

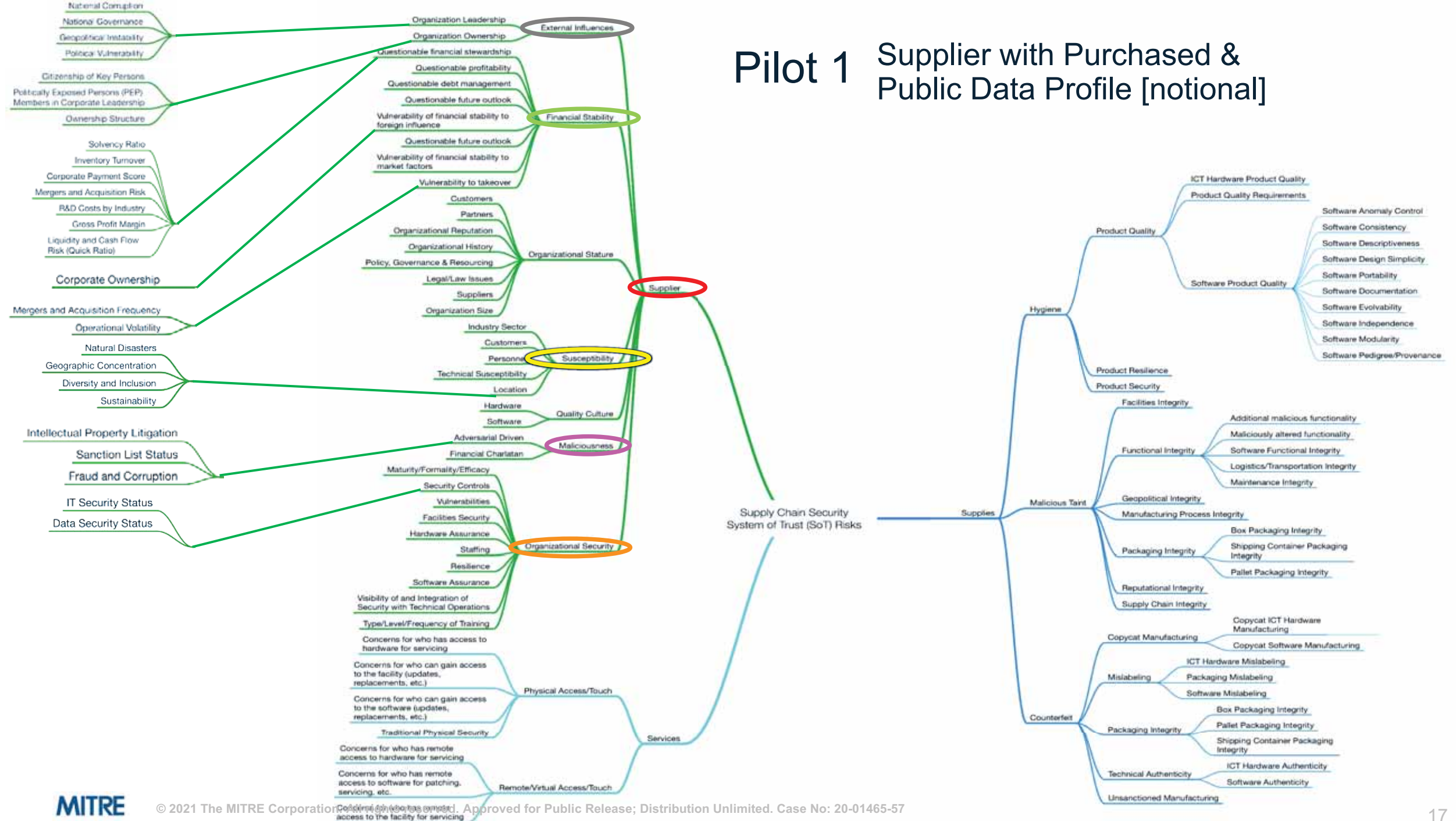
### Assessment Scope, Skills & Means

- ☒ Open Source Information
- ☒ Purchased Data Sources
- ☐ Written Questions
- ☐ Oral Discussions
- ☐ Sampling of Components
- ☐ Software Analysis
- ☐ Intelligence Service Investigation

### Assessment Constraints

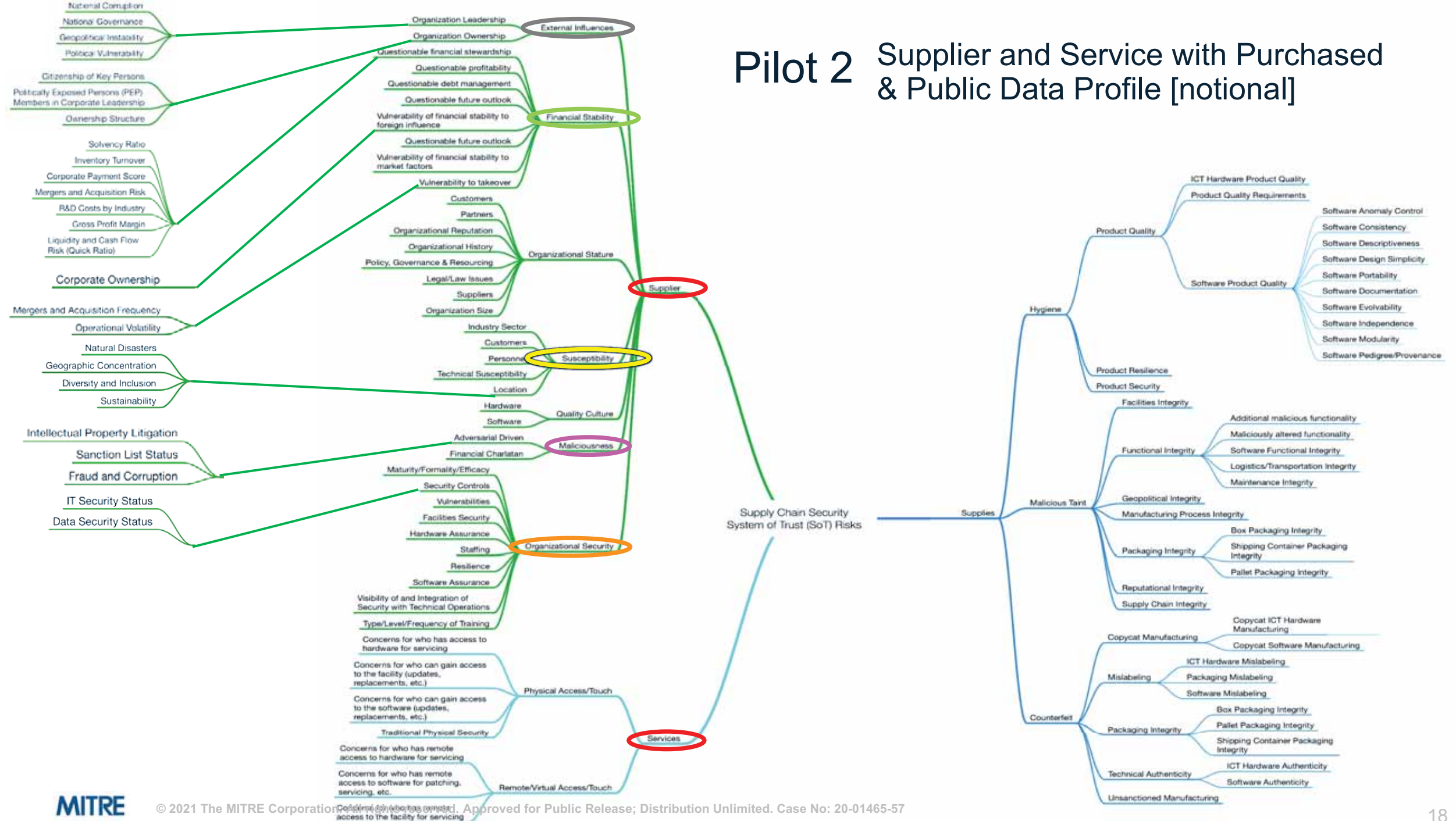
- ☒ Time Period
  - ☐ Weeks
  - ☐ Days
  - ☒ Hours
- ☒ Monies for Data Purchase
- ☐ Investigative Staff Available

# Pilot 1 Supplier with Purchased & Public Data Profile [notional]



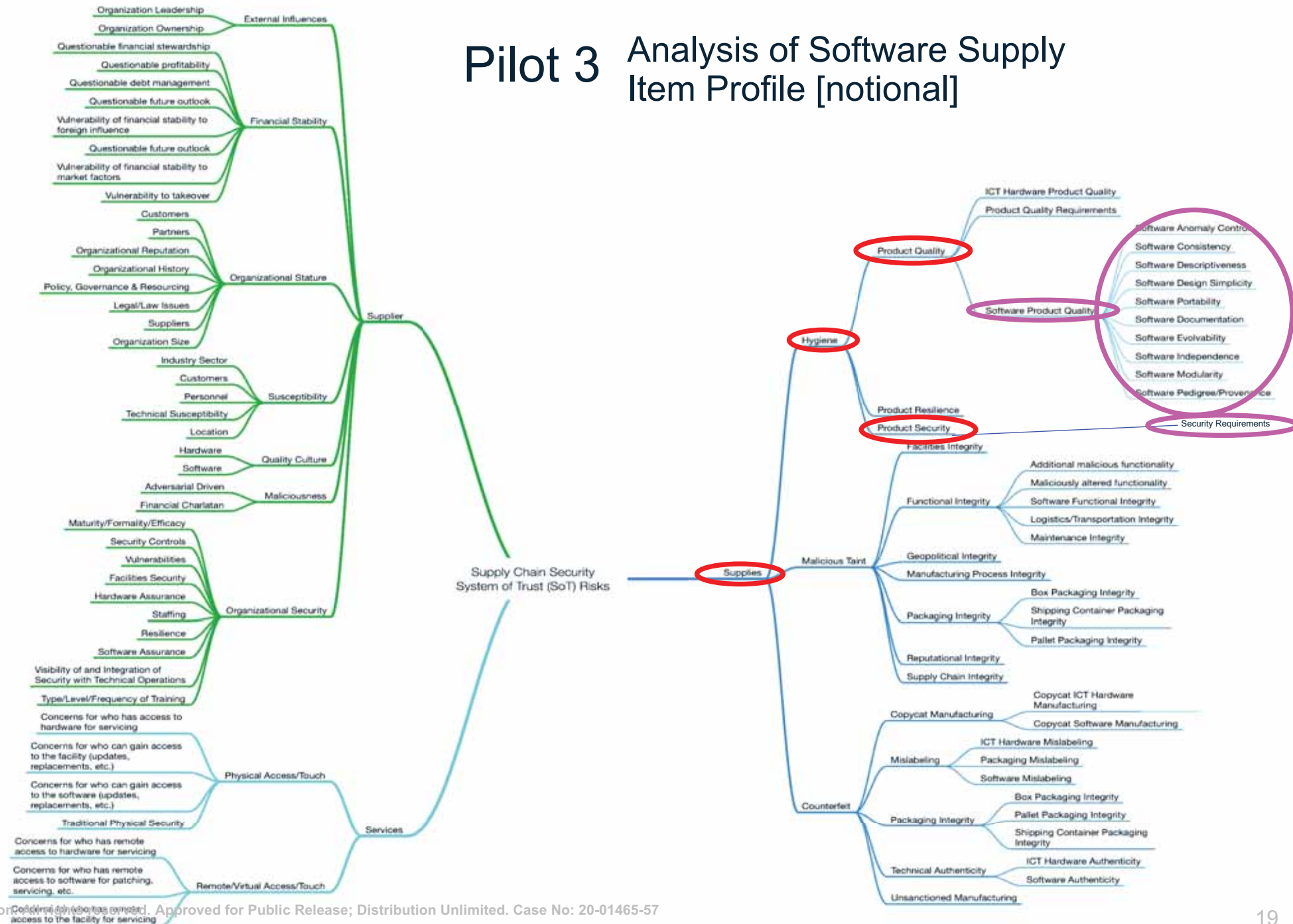


# Pilot 2 Supplier and Service with Purchased & Public Data Profile [notional]

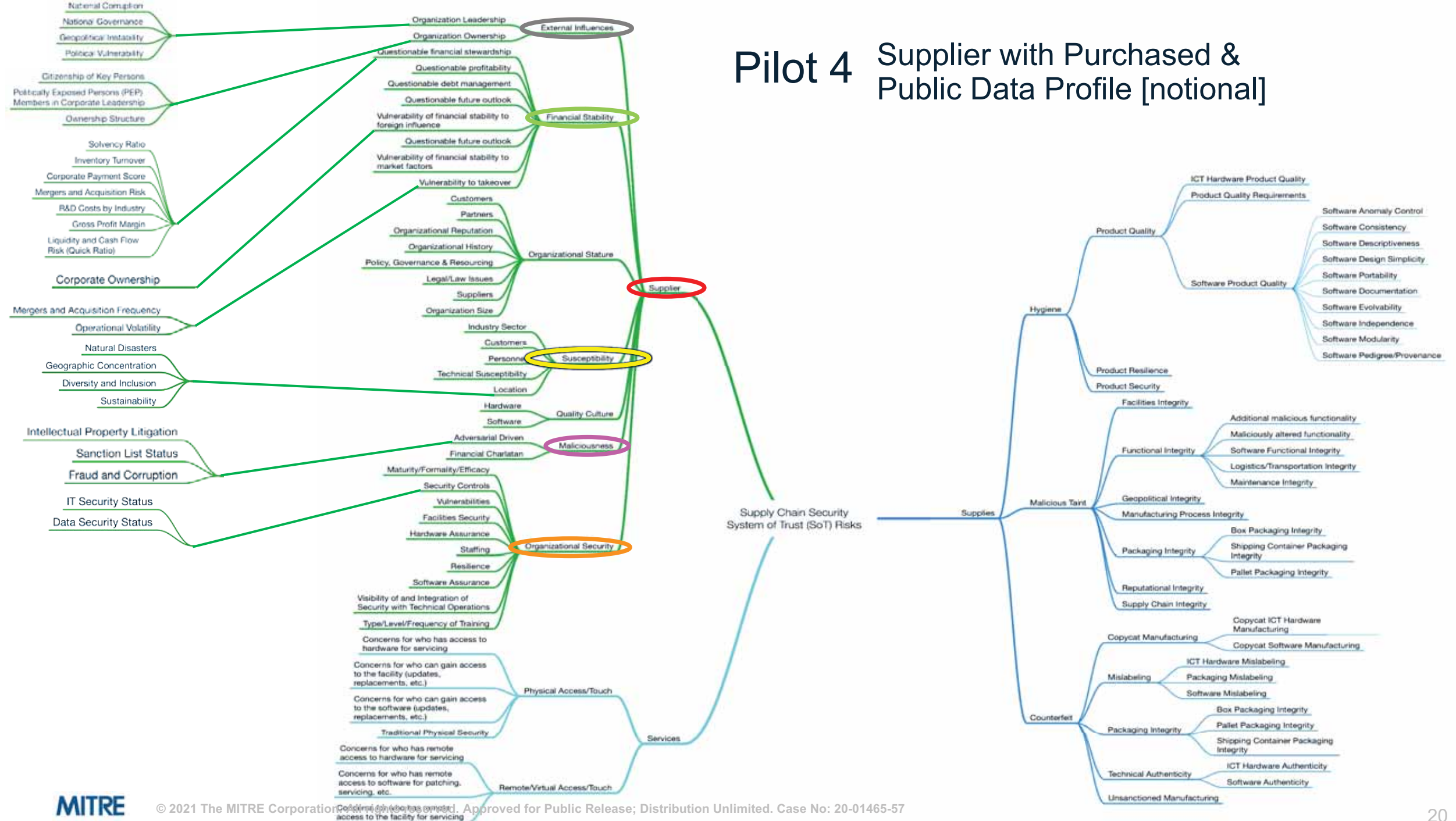




# Pilot 3 Analysis of Software Supply Item Profile [notional]

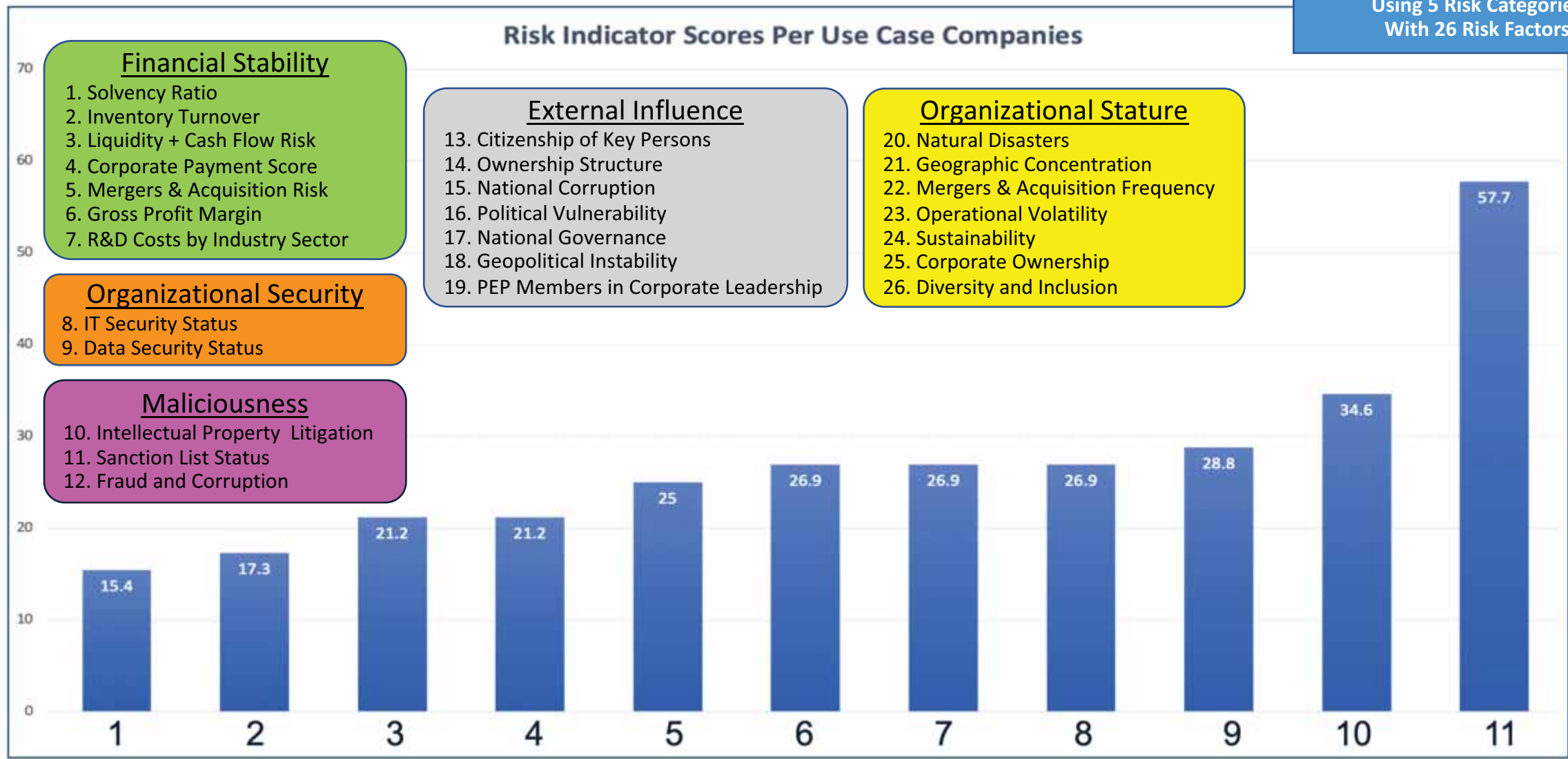


# Pilot 4 Supplier with Purchased & Public Data Profile [notional]



# SoT Pilot 1: Companies of Interest

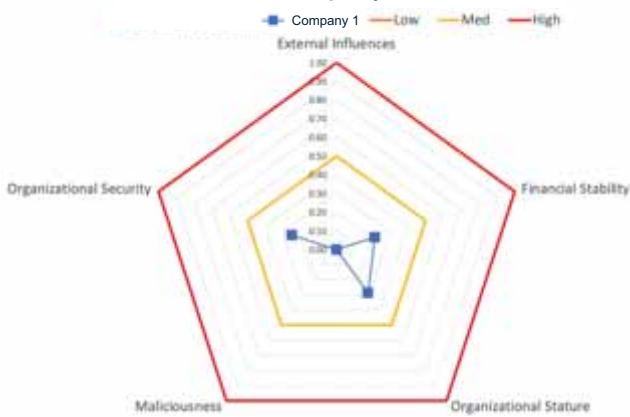
Supplier and Public Data Profile of the System of Trust Using 5 Risk Categories With 26 Risk Factors



\* Risk scorecard based on the preliminary System of Trust scoring methodology for 5 top-level concern areas and 52 risk measure questions for 26 risk factors.



Company 1



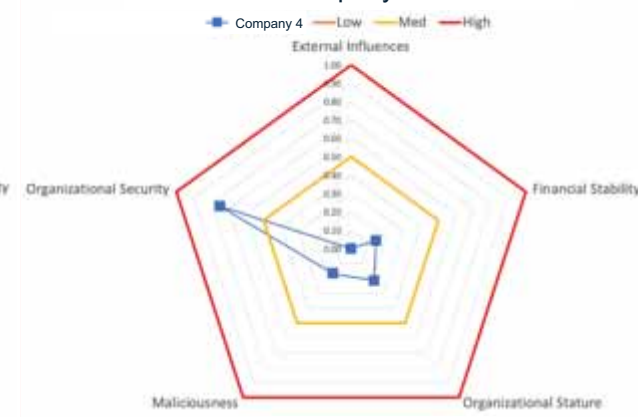
Company 2



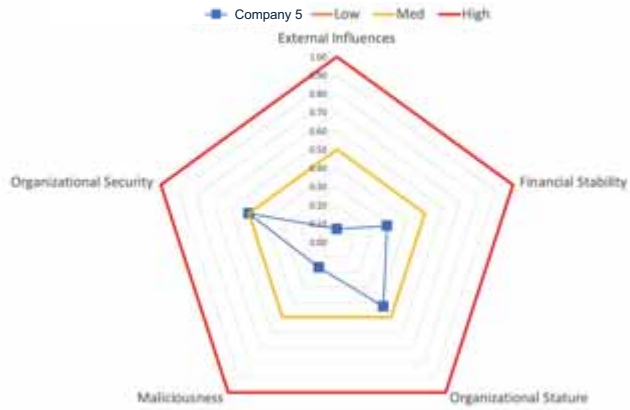
Company 3



Company 4



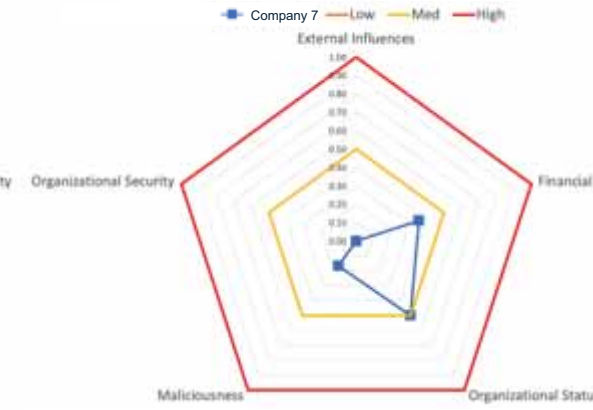
Company 5



Company 6



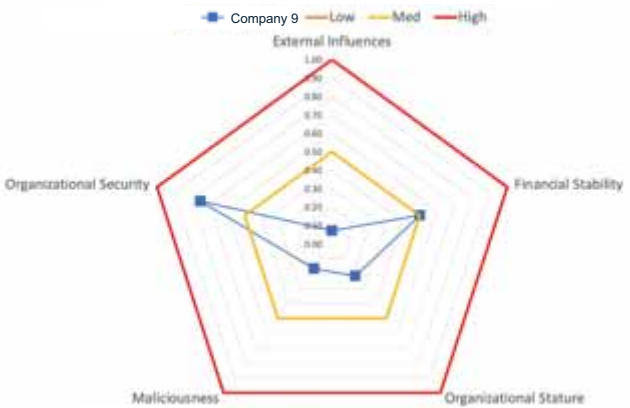
Company 7



Company 8



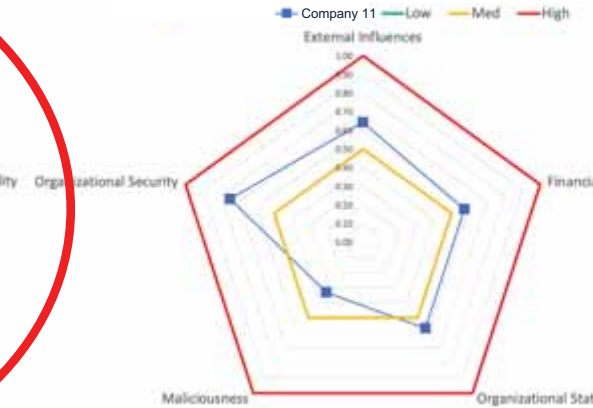
Company 9



Company 10



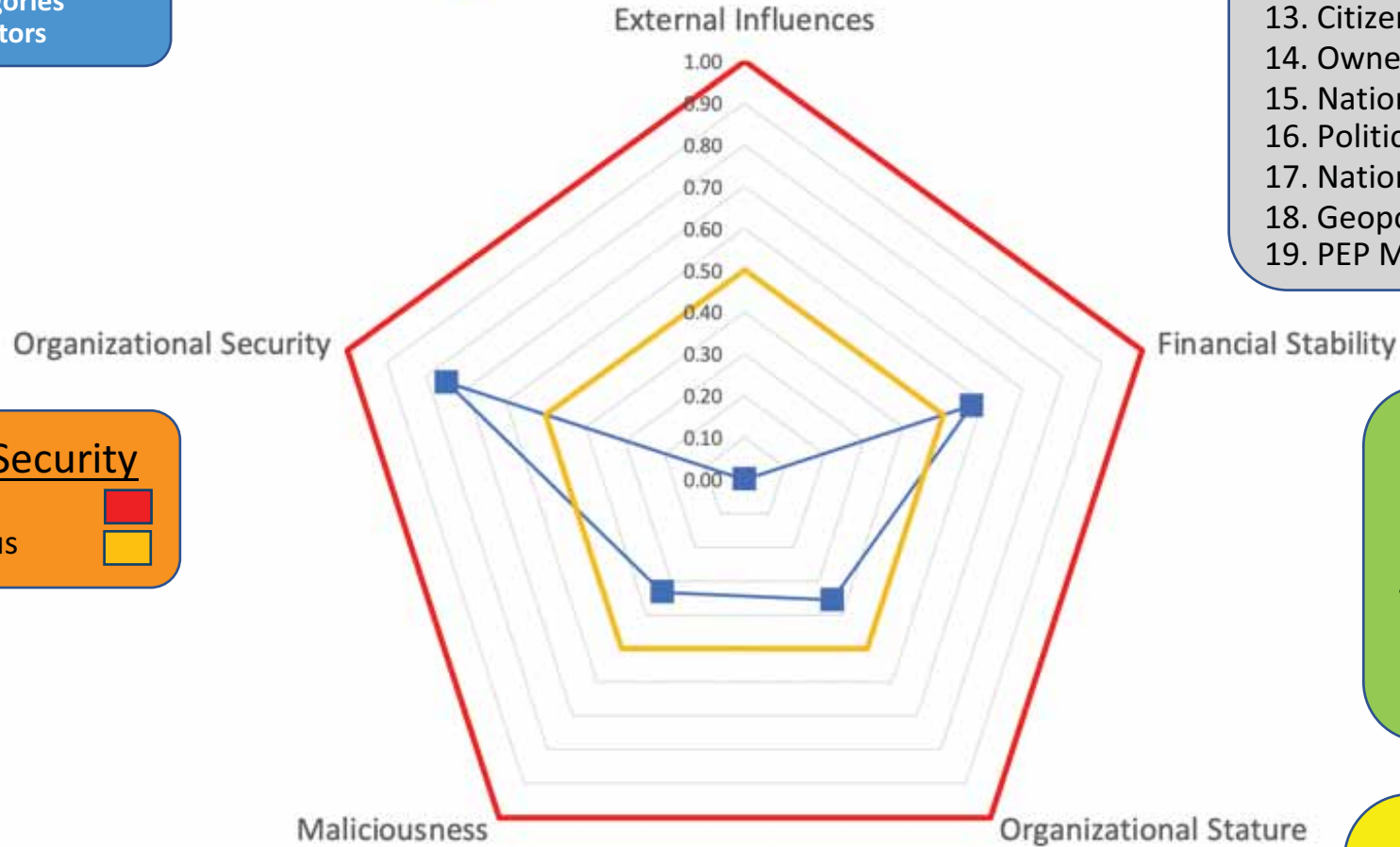
Company 11



## System of Trust Pilot 1: Companies of Interest

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

# Company 10



## 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 Security

- 8. IT Security Status
- 9. Data Security Status



## 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



## Maliciousness

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



## Organizational Stature

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





| Data Sources   | Concern Areas | External Influences | Financial Stability | Organizational Stature | Susceptibility | Quality Culture | Maliciousness | Organizational Security | Hygiene | Counterfeit | Malicious Taint | Physical Access/Touch | Remote/Virtual Access/Touch |
|--|---------------|---------------------|---------------------|------------------------|----------------|-----------------|---------------|-------------------------|---------|-------------|-----------------|-----------------------|-----------------------------|
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Regulatory DataCorp, Inc. (RDC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Dunn and Bradstreet  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Pitchbook  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau van Dijk (BvD) - Orbis & Zephyr   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Electronic Resellers Association International (ERAi)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Government Industry Data Exchange Program (GIDEP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Independent Distributors of Electronics Association (IDEA)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Securities and Exchange Commission (SEC) Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| USASpending  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of Labor, Employment and Training Administration, Office of Foreign Labor Certification    |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Global Legal Entity Identifier Foundation (GLEIF)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Thompson Reuters   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Yahoo! Finance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| System for Award Management (SAM)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Foreign Assets Control (OFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| World Bank Listing of Ineligible Firms   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Five Eyes Alliance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| United Nations Security Council Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canada Terrorists List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Better Business Bureau   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) website                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| NIST National Vulnerability Database   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Small Business Innovation Research (SBIR) & Small Business Technology Transfer                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau of Industry and Security (BIS), U.S. Department of Commerce denied entities                         |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Company Check (Europe)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Companies House (UK)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Australian Department of Foreign Affairs and Trade   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Federal Risk and Authorization Management Program (FedRAMP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| International Criminal Police Organization (INTERPOL)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Myvisajobs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Financial Sanctions Implementation; HM Treasury  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canadian Office of the Superintendent of Financial Institutions (OSFI)                                     |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Global Research Centre for Research on Globalization   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| GuruFocus  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Macrotrends  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RevenuesAndProfits   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Statista   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Securities and Exchange Commission Trading Suspensions  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wikipedia "List of data breaches."   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wisconsin Dept of Agriculture, Trade and Consumer Protection Data Breaches                                 |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| State of California Department of Justice  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Privacy Rights Clearinghouse   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Trade Representative Priority Watch List  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of the Treasury Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of Justice   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Software Quality Assurance Evaluation (SQAE)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Naval Surface Warfare Center, Crane Division (NSWC Crane)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Intelligence Agency SCRM Threat Assessment Center (DIA TAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Sandia National Labs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Joint Federated Assurance Center (JFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/A4 (Logistics)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/IN (Acquisition Intelligence)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Deloitte   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Electronic Resellers Association International (ERAi)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Interos  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBM  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Virtual Knowledge  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Semantic AI  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Expanse  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Fortress   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBAT (Industrial Base Analysis Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| SERA (Sustainment Engineering Risk Assessment)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RMC / SOLAS  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBIDS (Industrial Base Integrated Data System)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| BDP (Big Data Picture)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| DIBnow (Defense Industrial Base-Now)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| CIBAT (Critical Industrial Base Assessment Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AWARE (Alerts, Warnings, Advice, Resolutions, and Experience)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |

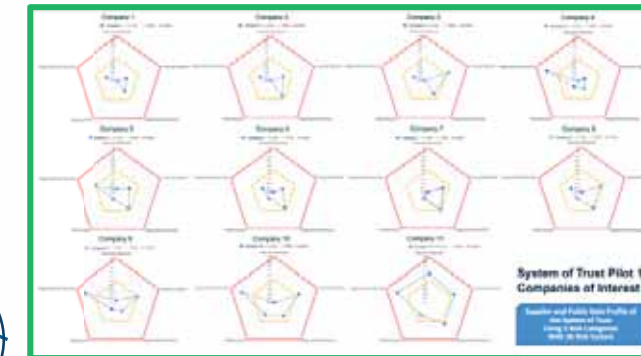
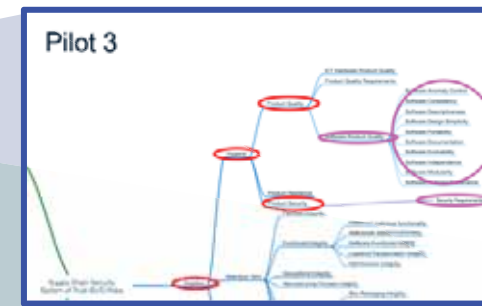
# Risk Categories and Data Sources for Supplier Profile Assessment (Pilots 1, 2, & 4)

| Data Sources   | Concern Areas | External Influences | Financial Stability | Organizational Stature | Susceptibility | Quality Culture | Maliciousness | Organizational Security | Hygiene | Counterfeit | Malicious Taint | Physical Access/Touch | Remote/Virtual Access/Touch |
|--|---------------|---------------------|---------------------|------------------------|----------------|-----------------|---------------|-------------------------|---------|-------------|-----------------|-----------------------|-----------------------------|
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Regulatory DataCorp, Inc. (RDC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Dunn and Bradstreet  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau van Dijk (BvD) - Orbis & Zephyr   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Government-Industry Data Exchange Program (GIDEP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Securities and Exchange Commission (SEC) Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Spending  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of Labor, Employment and Training Administration, Office of Foreign Labor Certification    |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Global Legal Entity Identifier Foundation (GLEIF)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Thompson Reuters   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Yahoo! Finance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| System for Award Management (SAM)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Foreign Assets Control (OFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| World Bank Listing of Ineligible Firms   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Five Eyes Alliance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| United Nations Security Council Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canada Terrorists List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Better Business Bureau   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) website                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| NIST National Vulnerability Database   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Small Business Innovation Research (SBIR) & Small Business Technology Transfer                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau of Industry and Security (BIS), U.S. Department of Commerce denied entities                         |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Company Check (Europe)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Companies House (UK)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Australian Department of Foreign Affairs and Trade   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Federal Risk and Authorization Management Program (FedRAMP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| International Criminal Police Organization (INTERPOL)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Myvisajobs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Financial Sanctions Implementation; HM Treasury  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canadian Office of the Superintendent of Financial Institutions (OSFI)                                     |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| GuruFocus  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Macrotrends  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RevenuesAndProfits   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Statista   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Securities and Exchange Commission Trading Suspensions  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wikipedia "List of data breaches."   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wisconsin Dept of Agriculture, Trade and Consumer Protection Data Breaches                                 |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| State of California Department of Justice  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Privacy Rights Clearinghouse   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Trade Representative Priority Watch List  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of the Treasury Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of Justice   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Software Quality Assurance Evaluation (SQAE)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Naval Surface Warfare Center, Crane Division (NSWC Crane)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Intelligence Agency SCRM Threat Assessment Center (DIA TAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Sandia National Labs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Joint Federated Assurance Center (JFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/A4 (Logistics)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/IN (Acquisition Intelligence)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Deloitte   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Electronic Resellers Association International (ERAi)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Interos  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBM  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Virtual Knowledge  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Semantic AI  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Expanse  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Fortress   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBAT (Industrial Base Analysis Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| SERA (Sustainment Engineering Risk Assessment)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RMC / SOLAS  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBIDS (Industrial Base Integrated Data System)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| BDP (Big Data Picture)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| DIBnow (Defense Industrial Base-Now)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| CIBAT (Critical Industrial Base Assessment Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AWARE (Alerts, Warnings, Advice, Resolutions, and Experience)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |

# Analysis of Software Supply Item Profile Assessment (Pilot 3)

| Data Sources   | Concern Areas | External Influences | Financial Stability | Organizational Stature | Susceptibility | Quality Culture | Maliciousness | Organizational Security | Hygiene | Counterfeit | Malicious Taint | Physical Access/Touch | Remote/Virtual Access/Touch |
|--|---------------|---------------------|---------------------|------------------------|----------------|-----------------|---------------|-------------------------|---------|-------------|-----------------|-----------------------|-----------------------------|
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Regulatory DataCorp, Inc. (RDC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Dunn and Bradstreet  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Pitchbook  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau van Dijk (BvD) - Orbis & Zephyr   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Electronic Resellers Association International (ERA)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Government Industry Data Exchange Program (GIDEP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Independent Distributors of Electronics Association (IDEA)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Securities and Exchange Commission (SEC) Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| USASpending  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of Labor, Employment and Training Administration, Office of Foreign Labor Certification    |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Global Legal Entity Identifier Foundation (GLEIF)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Thompson Reuters   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Yahoo! Finance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| System for Award Management (SAM)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Foreign Assets Control (OFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| World Bank Listing of Ineligible Firms   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Five Eyes Alliance   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| United Nations Security Council Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canada Terrorists List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Better Business Bureau   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) website                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| NIST National Vulnerability Database   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Small Business Innovation Research (SBIR) & Small Business Technology Transfer                             |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bureau of Industry and Security (BIS), U.S. Department of Commerce denied entities                         |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Company Check (Europe)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Companies House (UK)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Australian Department of Foreign Affairs and Trade   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Federal Risk and Authorization Management Program (FedRAMP)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| International Criminal Police Organization (INTERPOL)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Myvisajobs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Office of Financial Sanctions Implementation; HM Treasury  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Canadian Office of the Superintendent of Financial Institutions (OSFI)                                     |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Global Research Centre for Research on Globalization   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| GuruFocus  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Macrotrends  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RevenuesAndProfits   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Statista   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Securities and Exchange Commission Trading Suspensions  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wikipedia "List of data breaches."   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Wisconsin Dept of Agriculture, Trade and Consumer Protection Data Breaches                                 |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| State of California Department of Justice  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Privacy Rights Clearinghouse   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Trade Representative Priority Watch List  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| U.S. Department of the Treasury Sanctions List   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Software Quality Assurance Evaluation (SQAE)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Naval Surface Warfare Center, Crane Division (NSWC Crane)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Defense Intelligence Agency SCRM Threat Assessment Center (DIA TAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Sandia National Labs   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Joint Federated Assurance Center (JFAC)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/A4 (Logistics)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AFLCMC/IN (Acquisition Intelligence)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Deloitte   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Electronic Resellers Association International (ERA)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Bloomberg  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Interos  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Govini   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBM  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Virtual Knowledge  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Semantic AI  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Expanse  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| Fortress   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBAT (Industrial Base Analysis Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| SERA (Sustainment Engineering Risk Assessment)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| RMC / SOLAS  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| IBIDS (Industrial Base Integrated Data System)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| BDP (Big Data Picture)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| DIBnow (Defense Industrial Base-Now)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| CIBAT (Critical Industrial Base Assessment Tool)   |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |
| AWARE (Alerts, Warnings, Advice, Resolutions, and Experience)  |               |                     |                     |                        |                |                 |               |                         |         |             |                 |                       |                             |

# Tying together the System of Trust

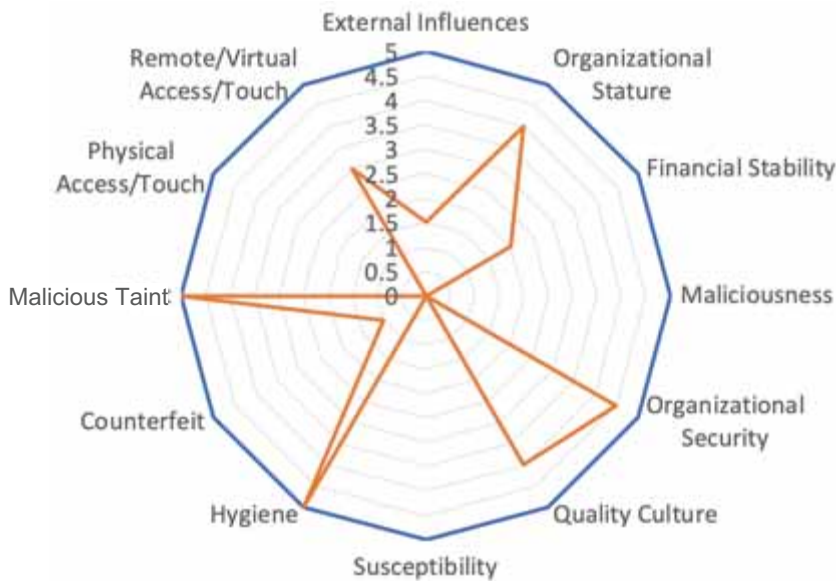


- View
- Edit
- Tailor
- Assess

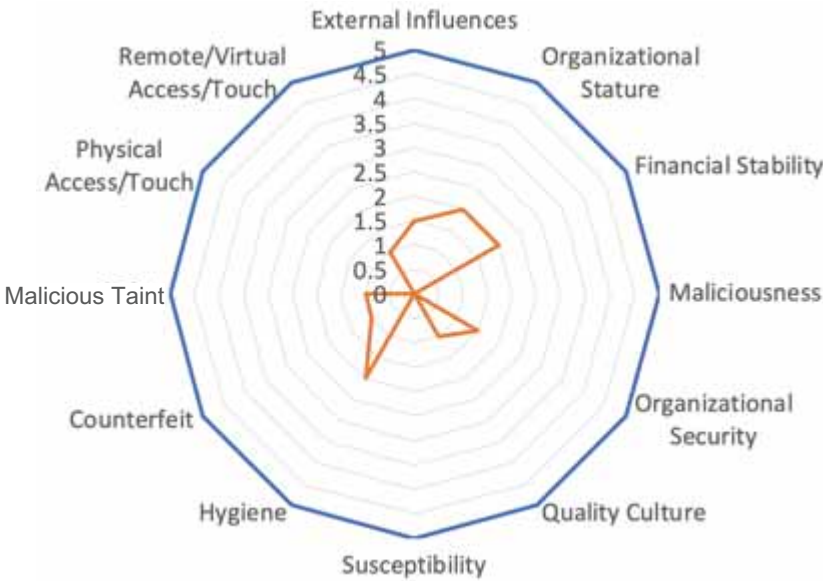
Risk Scoring [notional]

# Goal

Top-Level Concerns Vendor/Product A



Top-Level Concerns Vendor/Product B





# Risk Manager Modeler Data Model

Confluence Spaces Terms Create Search Log in

Supply Chain Security System of Trust

Dashboard / Supply Chain Security System of Trust Home / Risk Assessment & Scoring Knowledge Model

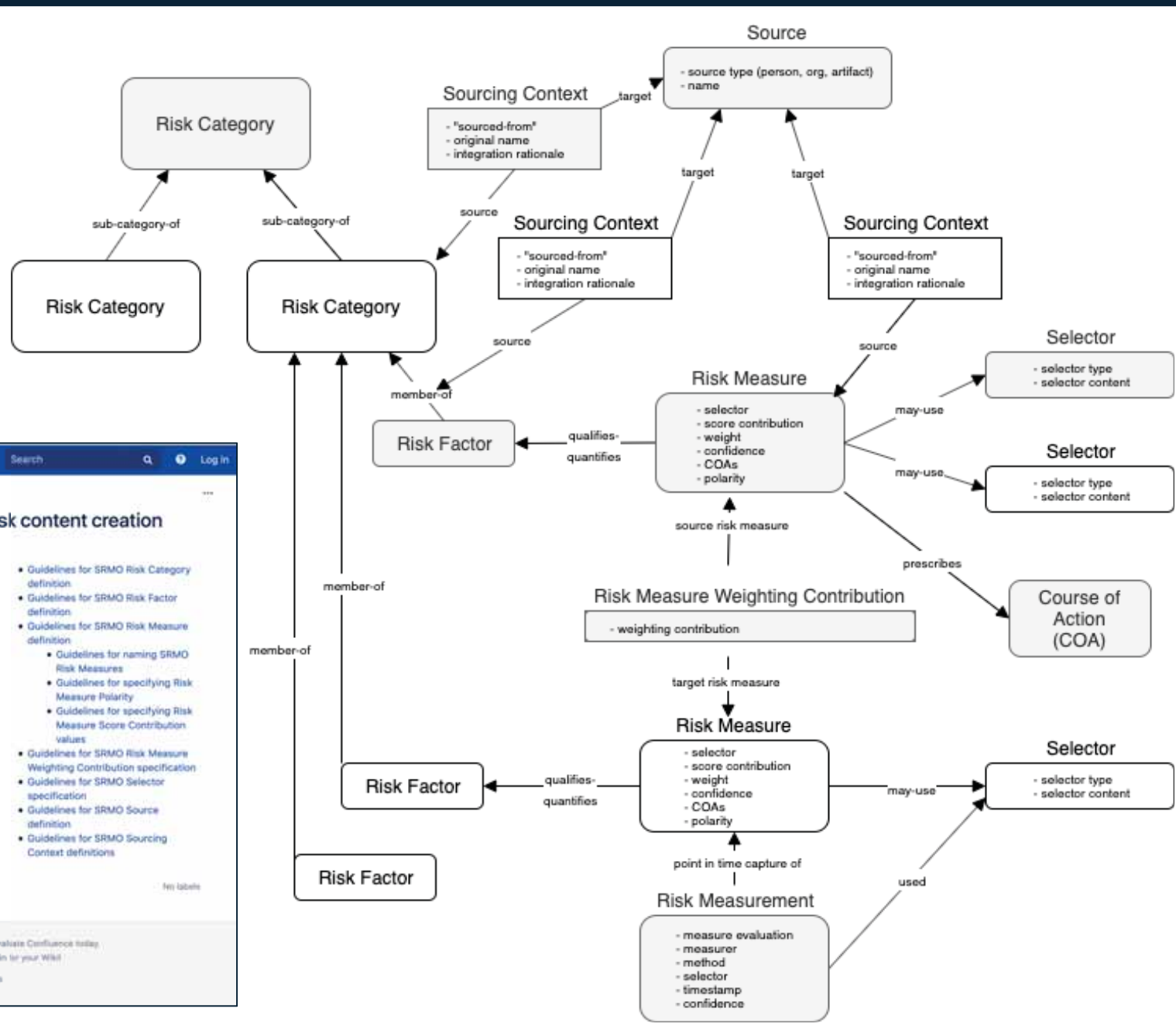
## Guidelines for Simple Risk Management Ontology (SRMO) risk content creation

Created by Sean Barnum, last modified on Jul 02, 2020

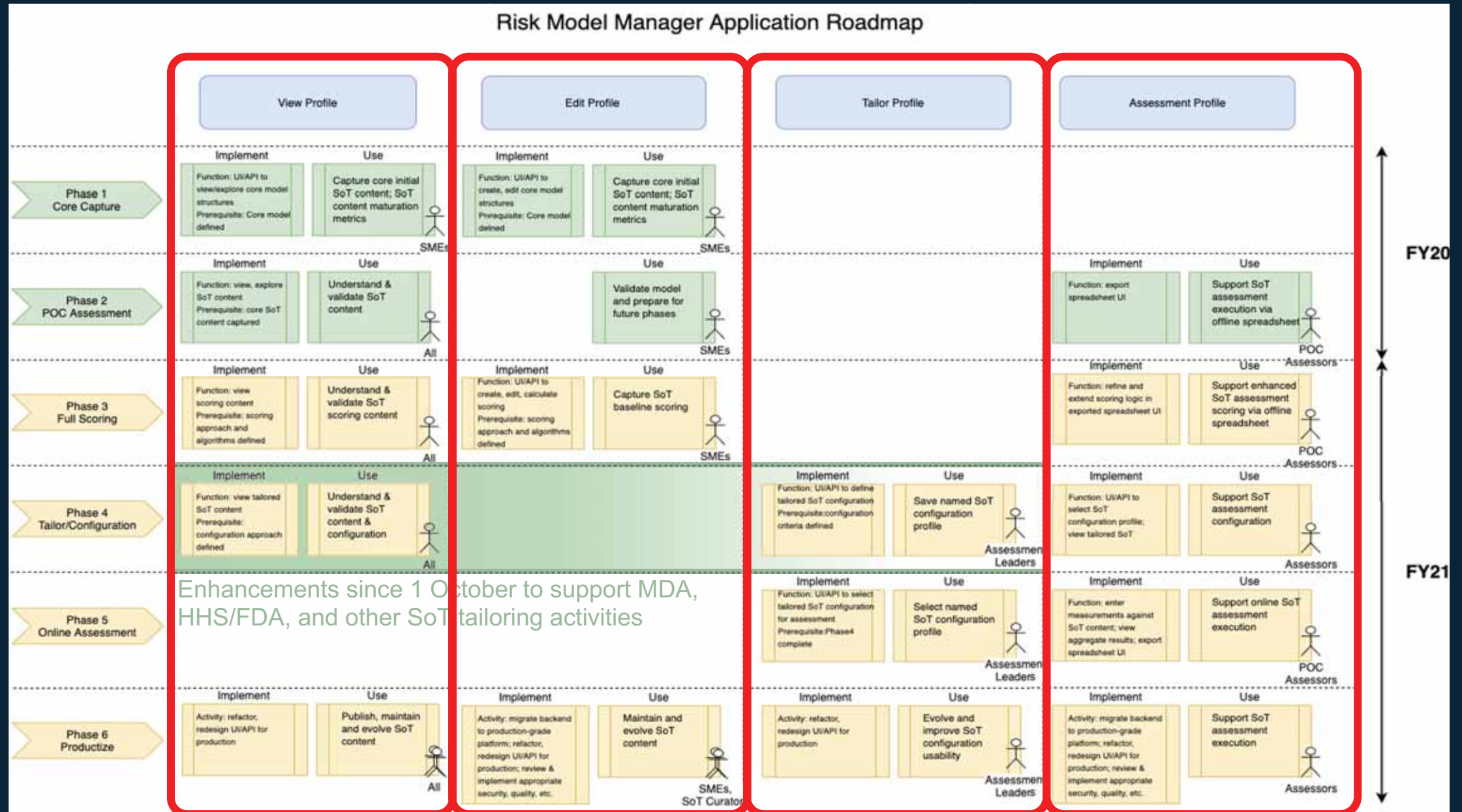
- Guidelines for SRMO Risk Category definition
- Guidelines for SRMO Risk Factor definition
- Guidelines for SRMO Risk Measure definition
  - Guidelines for naming SRMO Risk Measures
  - Guidelines for specifying Risk Measure Polarity
  - Guidelines for specifying Risk Measure Score Contribution values
- Guidelines for SRMO Risk Measure Weighting Contribution specification
- Guidelines for SRMO Selector specification
- Guidelines for SRMO Source definition
- Guidelines for SRMO Sourcing Context definitions

Powered by a free Atlassian Confluence Community License granted to The MITRE Corporation. Evaluate Confluence today. This Confluence installation runs a Free Giphy License - Evaluate the Giphy Confluence Plugin for your Wiki.

Powered by Atlassian Confluence 6.13.10 Report a bug Atlassian News

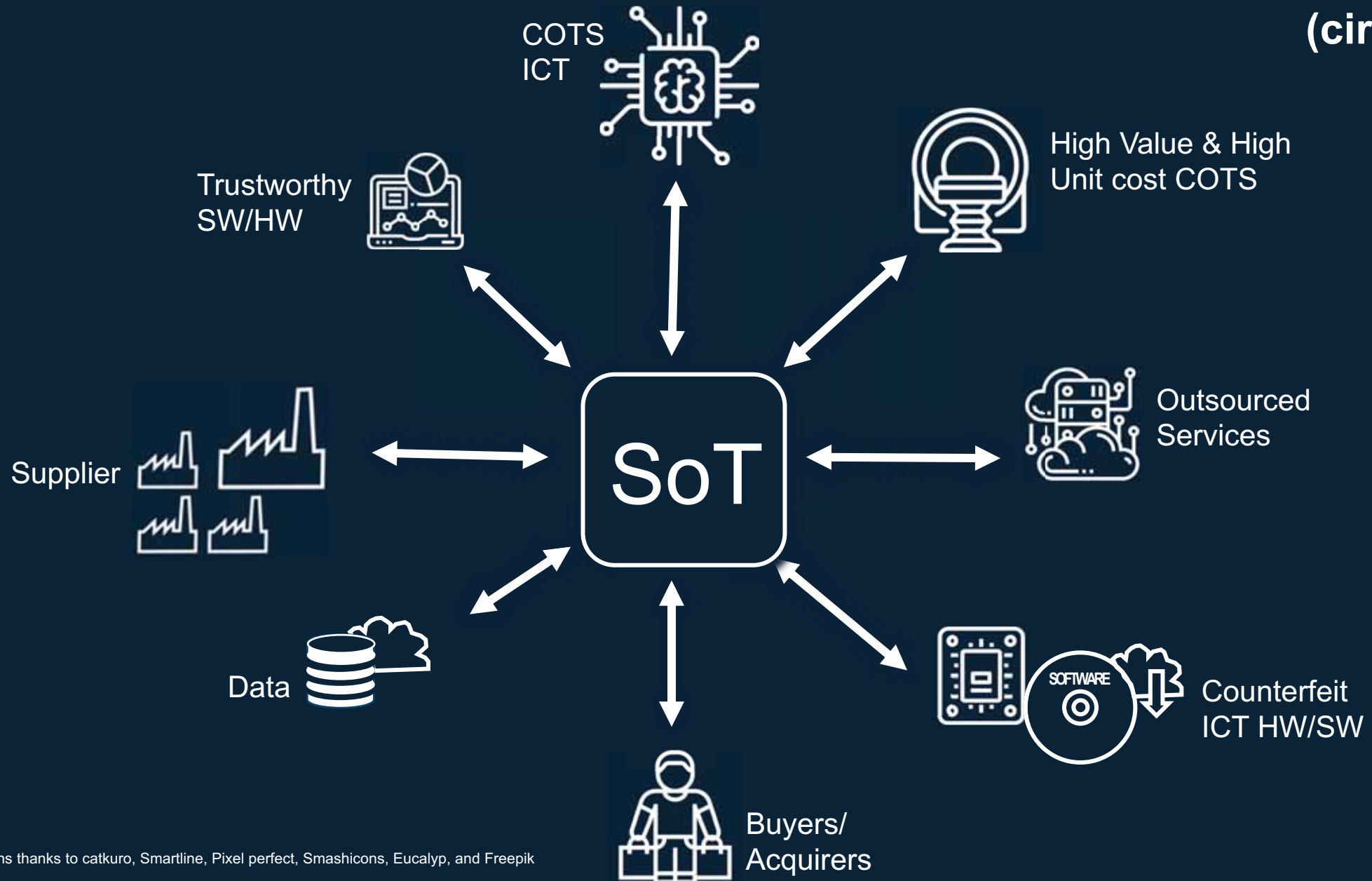


# System of Trust Risk Model Manager\* Application Roadmap



# Effective Supply Chain Trust Interactions

(circa 2021+)



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

# Next Steps – SoT Opportunities with Sponsors and Industry

---



Assessments for Sponsors and Industry by MITRE SoT teams



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



Standards and best practices



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

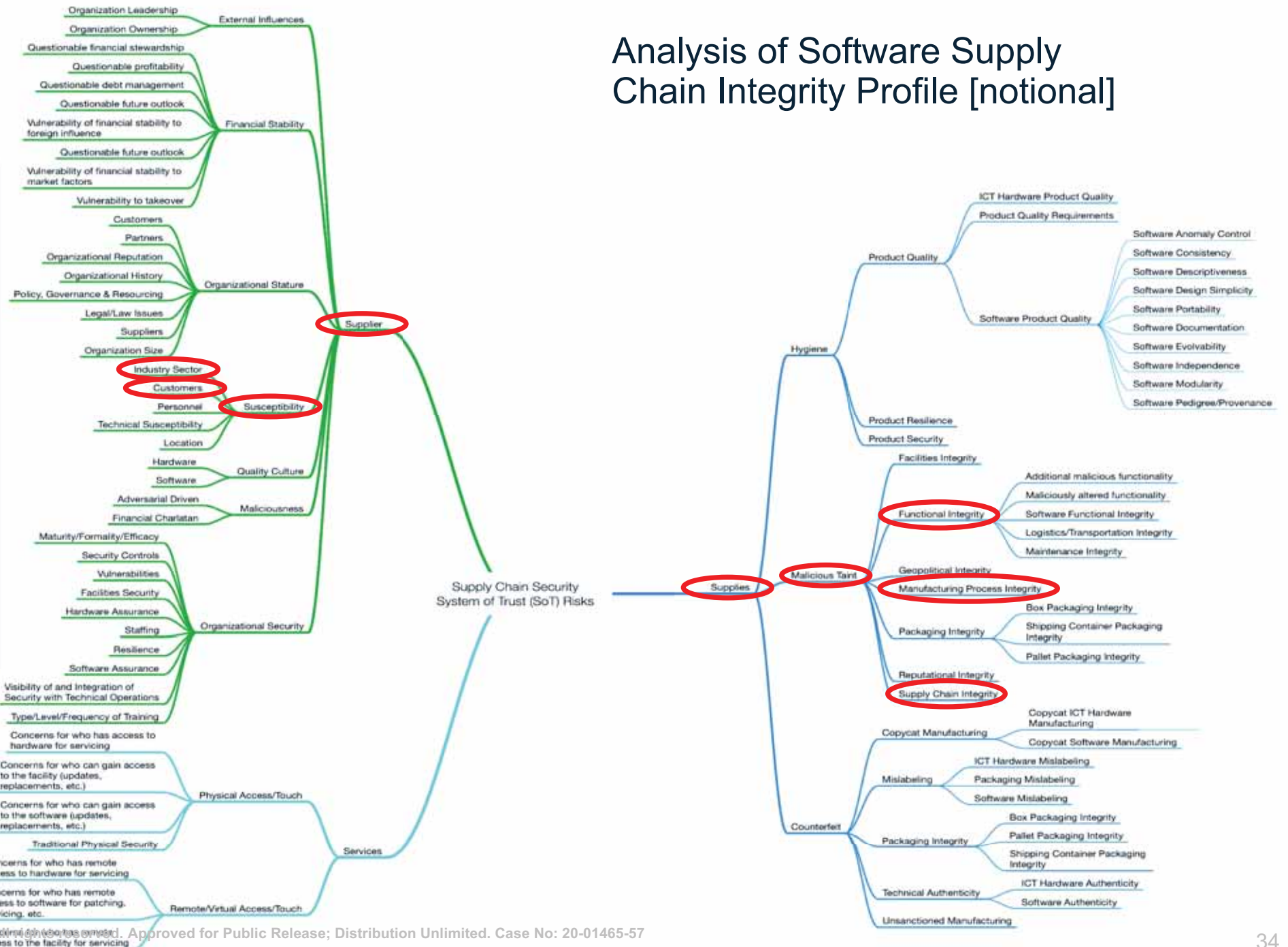


# Outreach and Engagement

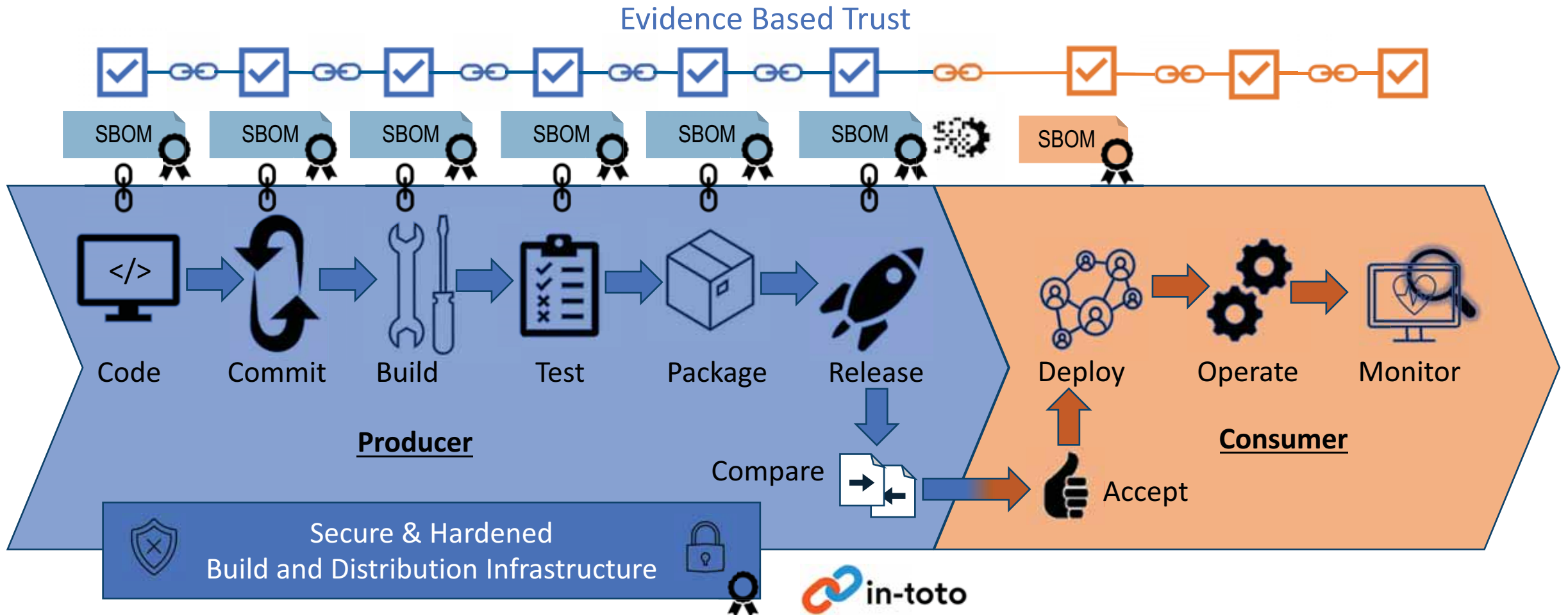
- American Bar Association (ABA) Technology Meeting
- Industry Technology & Innovation Roundtable
- MITRE Technical Centers Engineering Council
- DHS CISA NRMCM & SNL "Company/ICT Element Scorecard" Team
- MITRE CyberSecurity Days
- Open Group July Member Meeting Plenary
- DHS OPO Director and Team
- DHS CISA NRMCM Risk Analysis Branch & SNL Team Members
- MITRE Supply Chain Security Summit II
- ABA IoT National Institutes Panel
- DoD/DoE NNSA Software Assurance Community of Practice
- DHS S&T FVEYES Supply Chain Workshop
- System of Trust - Biomed Deeper Dive
- SoT Methodology for Industrial Base Reviews
- EOP/OMB – Maria Roat (Dep Fed CIO at OMB)/ Camilo Sandoval (Fed CISO)
- SoT Methodology for Military Industrial Base Review
- System of Trust as the 3rd Party Supply Chain Risk Framework for Boards/Officers
- 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
- ODNI SCRM Leadership
- SoT to VA C-SCRM Lead
- IIC Winter 2020 Quarterly Member Meeting
- House Homeland Security Committee staff
- ABA SciTech Lawyer article on System of Trust and the Pandemic – Winter 2021 Issue
- DHS CISA NRMCM on SoT progress and plans
- Treasury OCIO Team
- GAO Supply Chain Report Authoring Team
- ATIS 5G/SC Working Group
- House Armed Services Committee staff
- CISA NRMCM Team
- MDA Supply Chain Team
- Senate Armed Services Committee staff
- DHS CISO
- House Oversight Committee staff



# Analysis of Software Supply Chain Integrity Profile [notional]



# Software Supply Chain Integrity



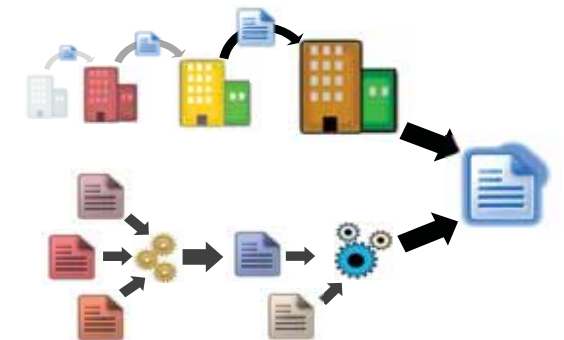


MITRE

## Provenance and Pedigree

\*Definitions (from Merriam-Webster)

## Separating Provenance and Pedigree



**Pedigree**  
Captures the **history** of how an Artifact or Document *was produced or derived*





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.

By Robert A. Martin,  
Vivian Barbaoui,  
J. Brian Hall, PhD, and  
Michael A. Anandberg

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

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 2013, 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. 115-382), signed into law on December 21, 2018, established the Federal Acquisition Security Council (FASCC). The FASCC 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

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

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

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

# Questions?

MITRE

© 2021 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 20-01465-57

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