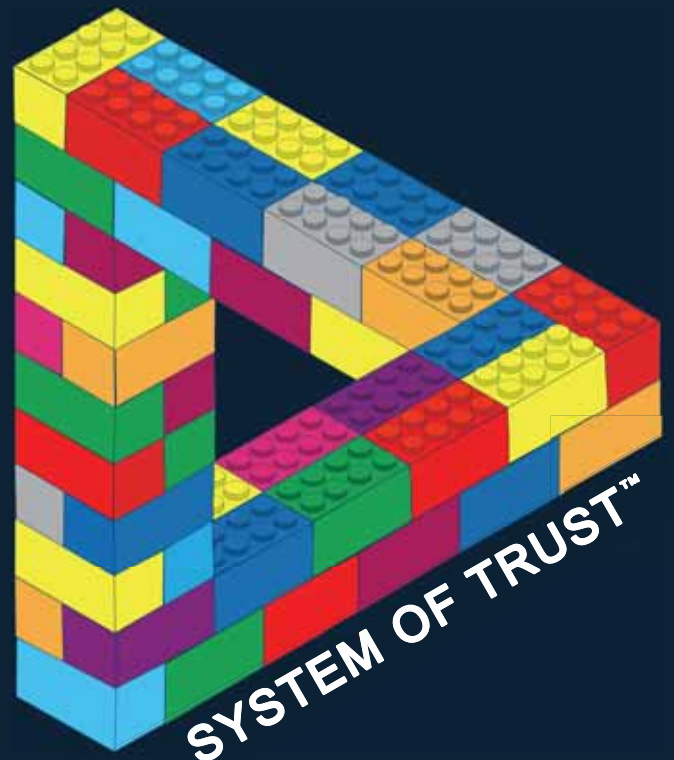
MITRE System of Trust

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)

COTS ICT

Trustworthy SW/HW

High Value & High Unit cost COTS

Supplier

Outsourced Services

Data

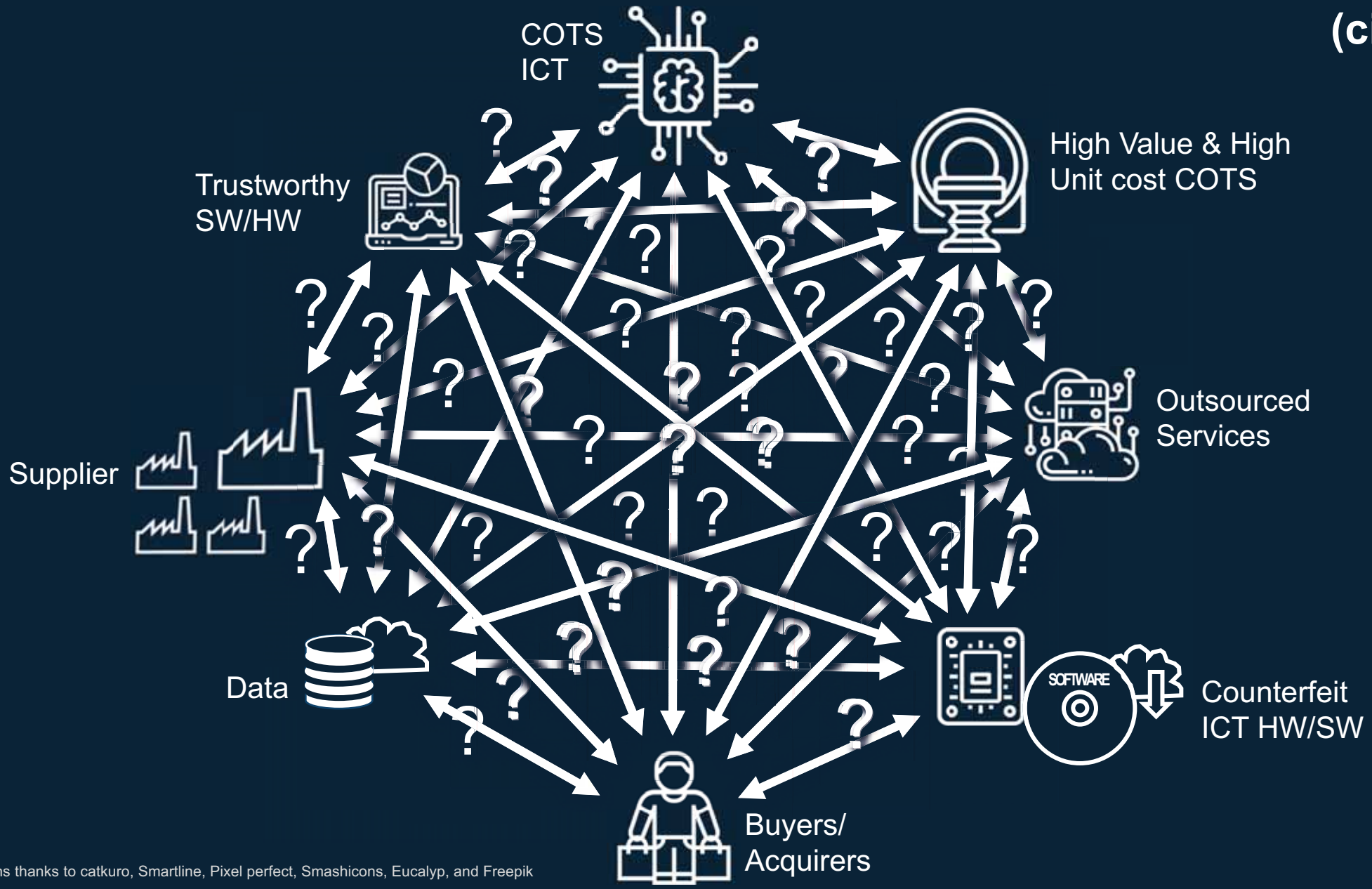
Counterfeit ICT HW/SW

Buyers/ Acquirers

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

MITRE

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



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

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 SQAE 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 2019.
13. "Constructive Disruption White Paper: Exploiting Publicly Available Information to Address Today's Security Challenges", February 2019.
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 (ASCQM)", Version 1.0, January 2020.
22. The Open Group, "Open Trusted Technology Provider Standard (O-TTPS) – 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 (2019) 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

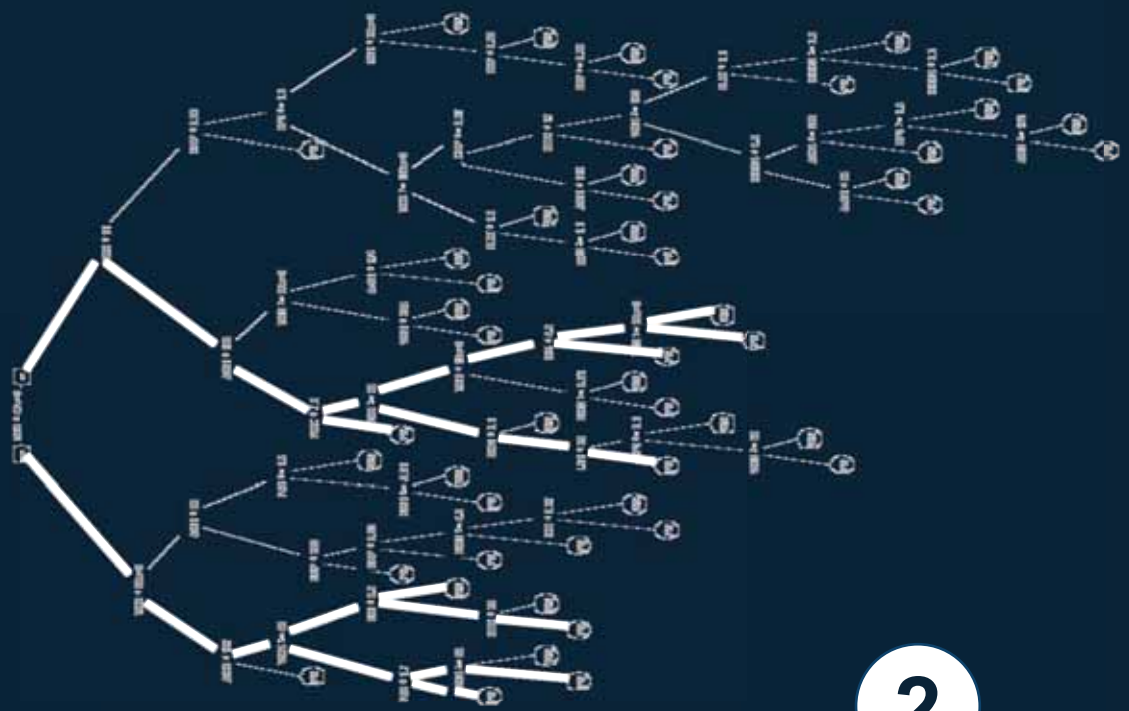
The System of Trust Program's Main Two Aspects

Address Chaos, Align & Organize

The System of Trust Program's Main Two Aspects

1

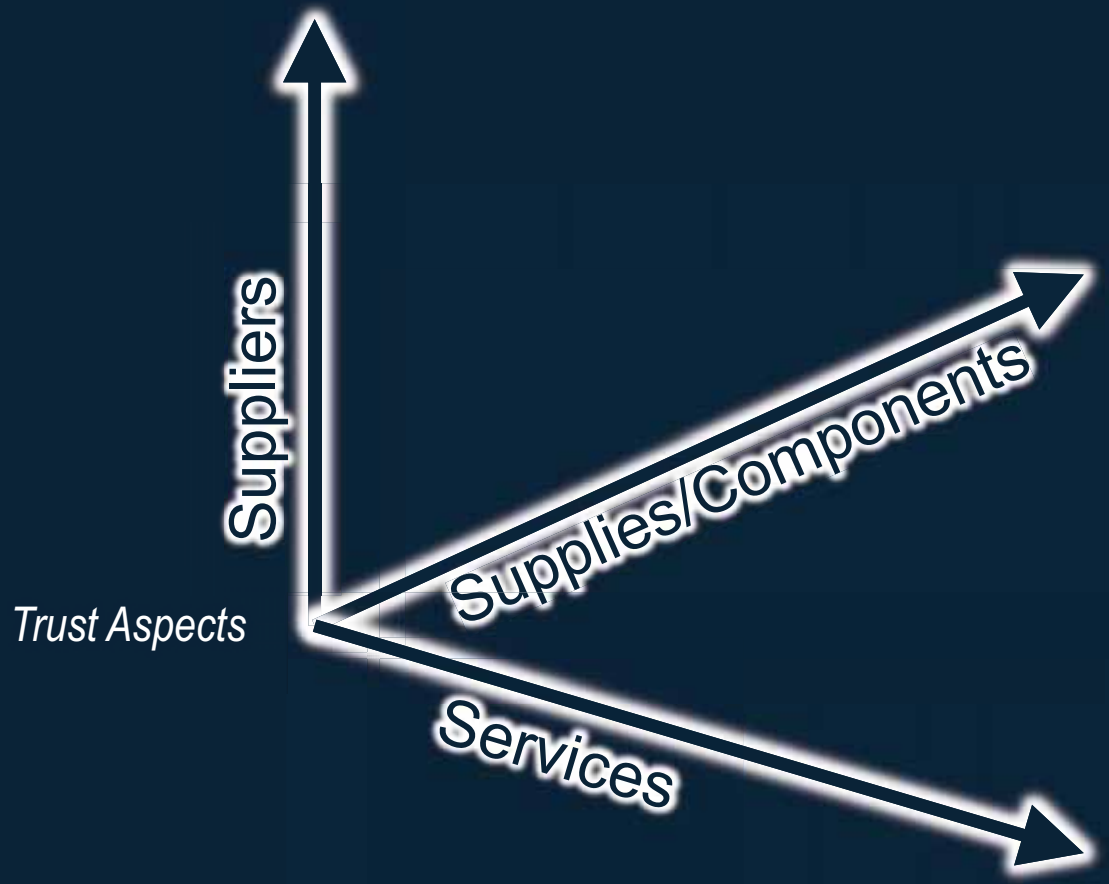
Address Chaos, Align & Organize



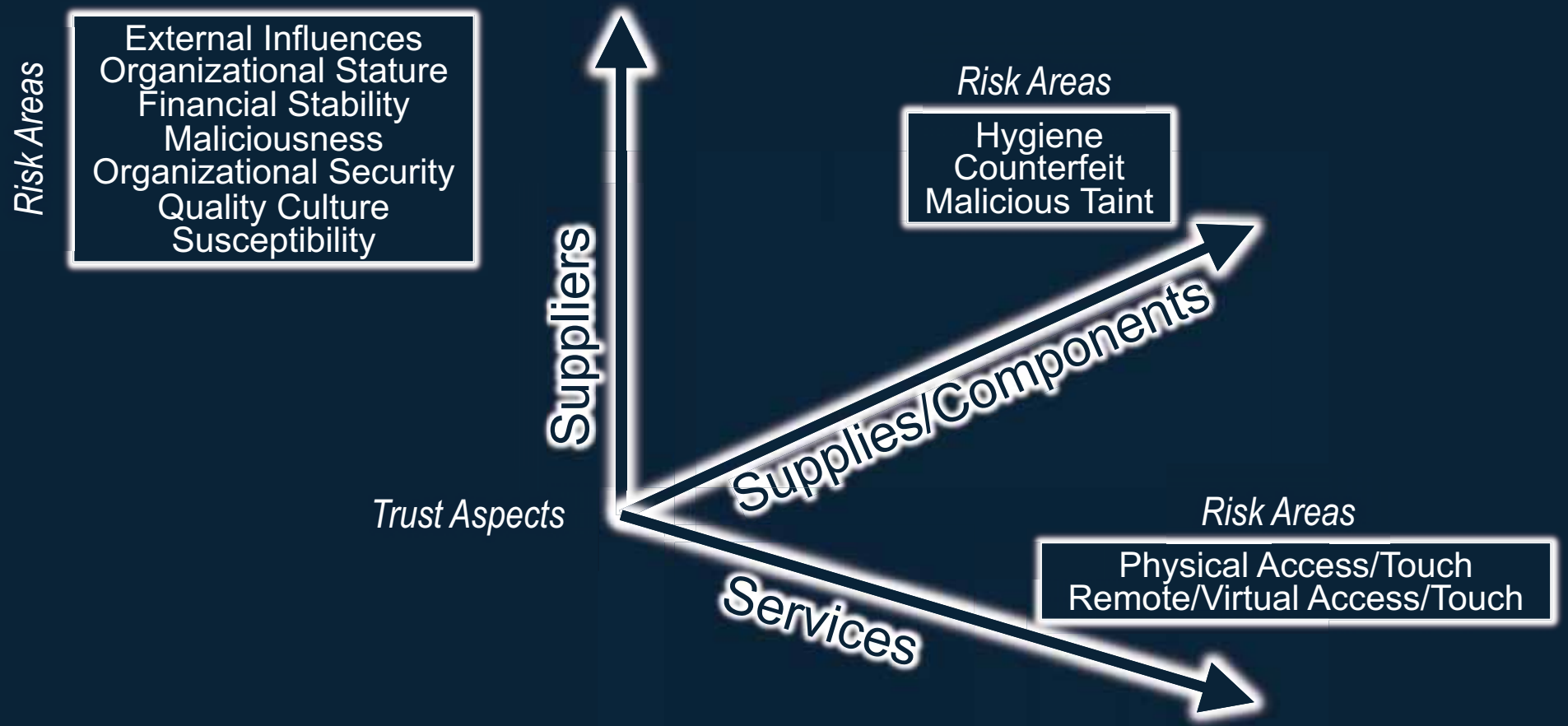
2

Simplify, Tailor & Make Usable

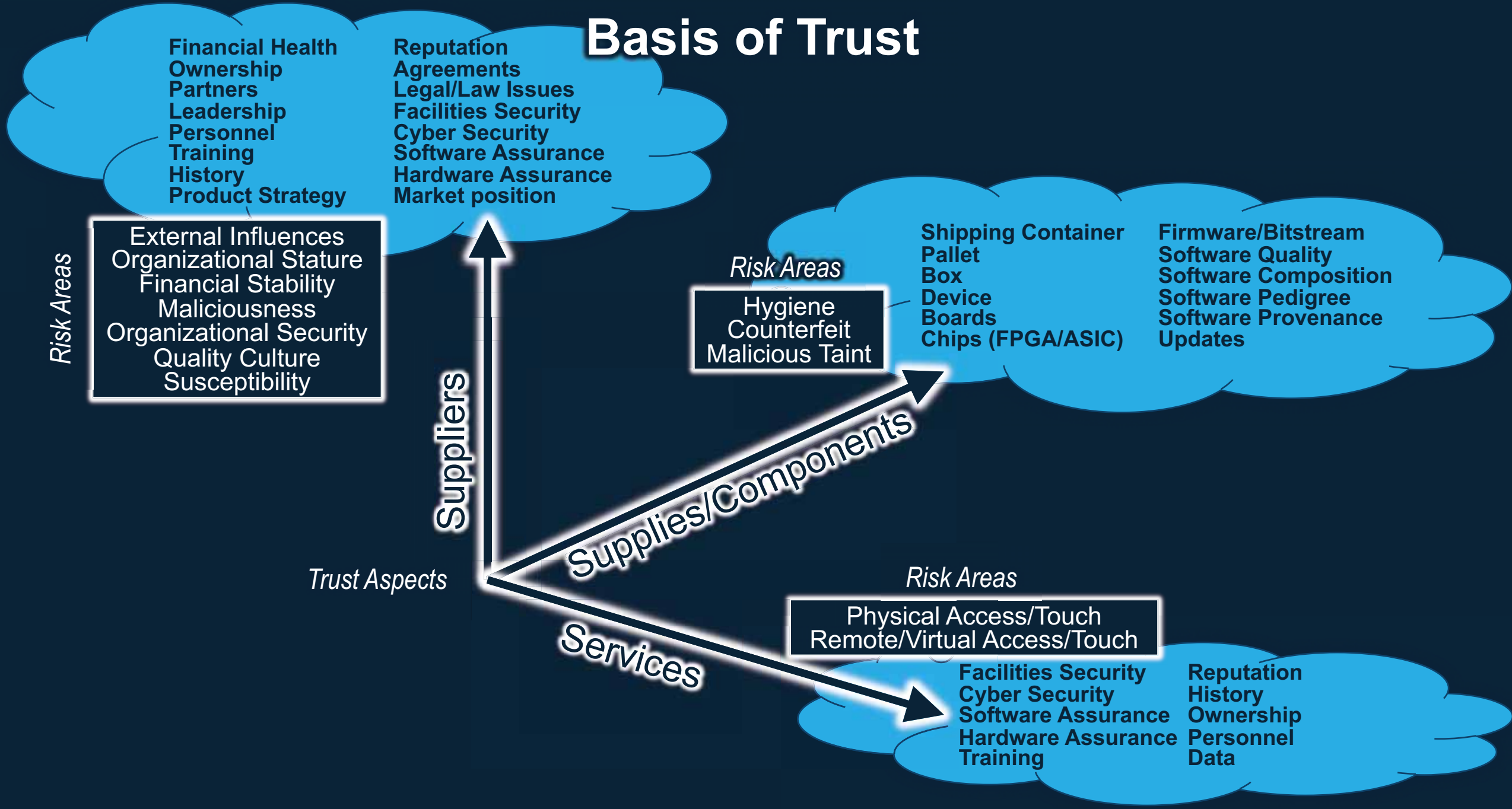
Basis of Trust



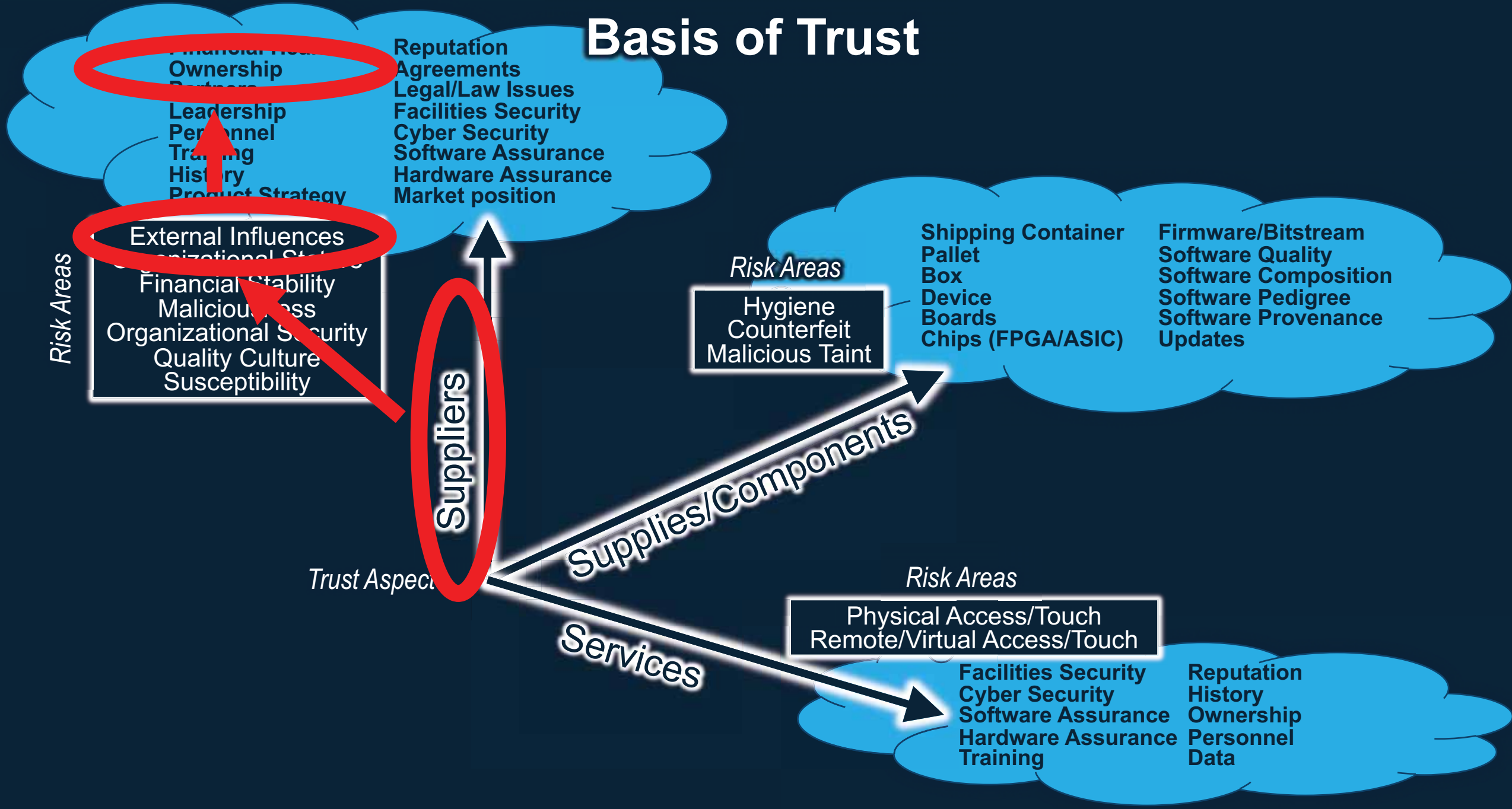
Basis of Trust

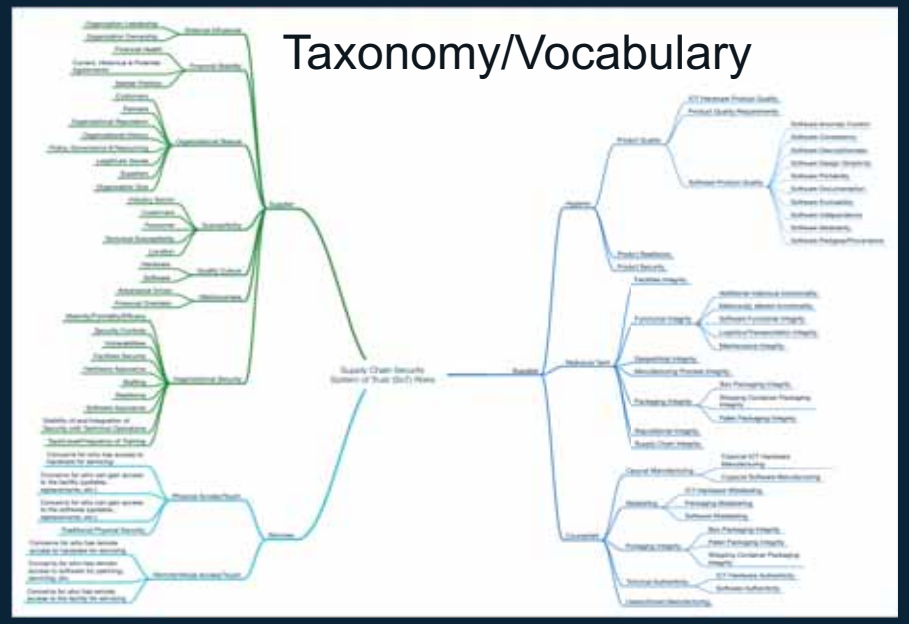


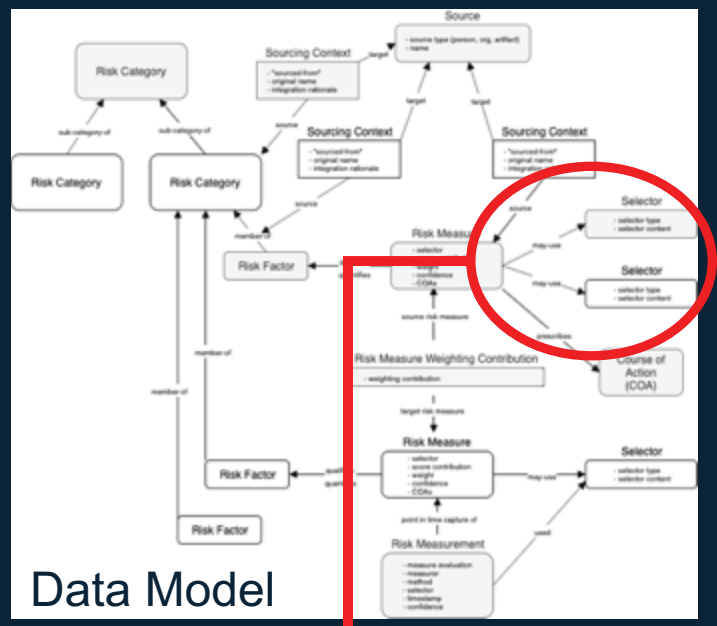
Basis of Trust



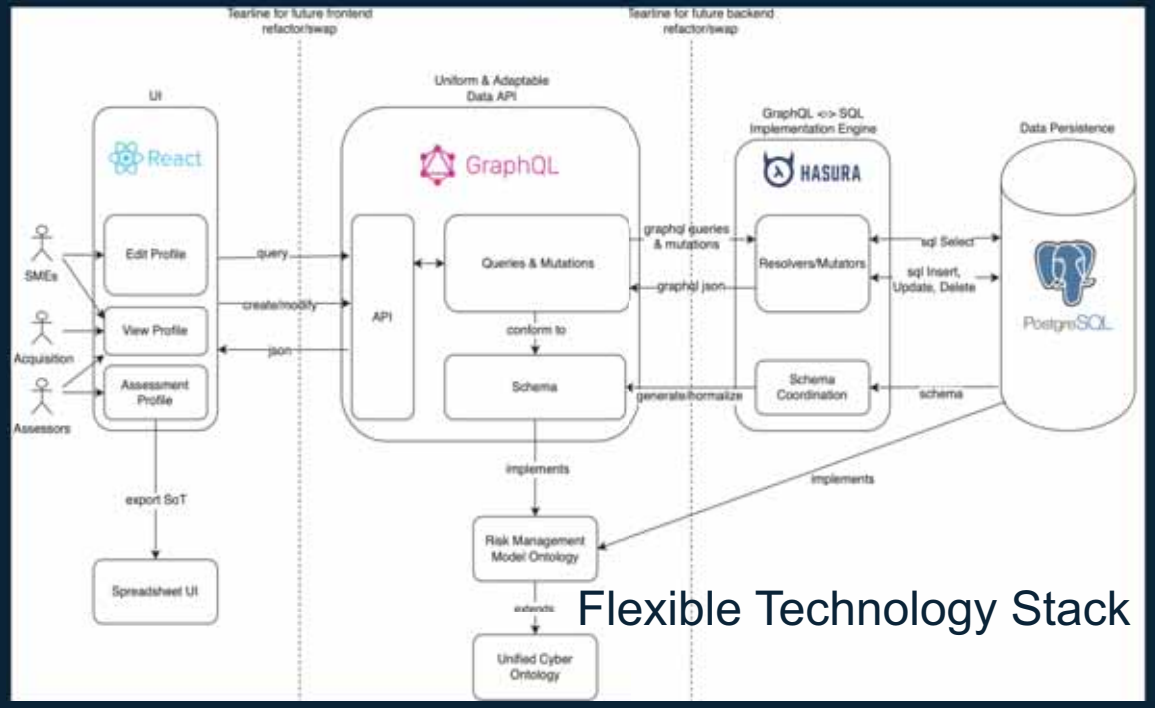
Basis of Trust







Analytic Methods



Linkage to future automated data retrievals from 72 identified Commercial, Open Source, and Government only Data sources for ad-hoc or periodic assessments

Export to Spreadsheet for ”Offline” Assessment

Risk Model Manager

Pilot 1 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

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

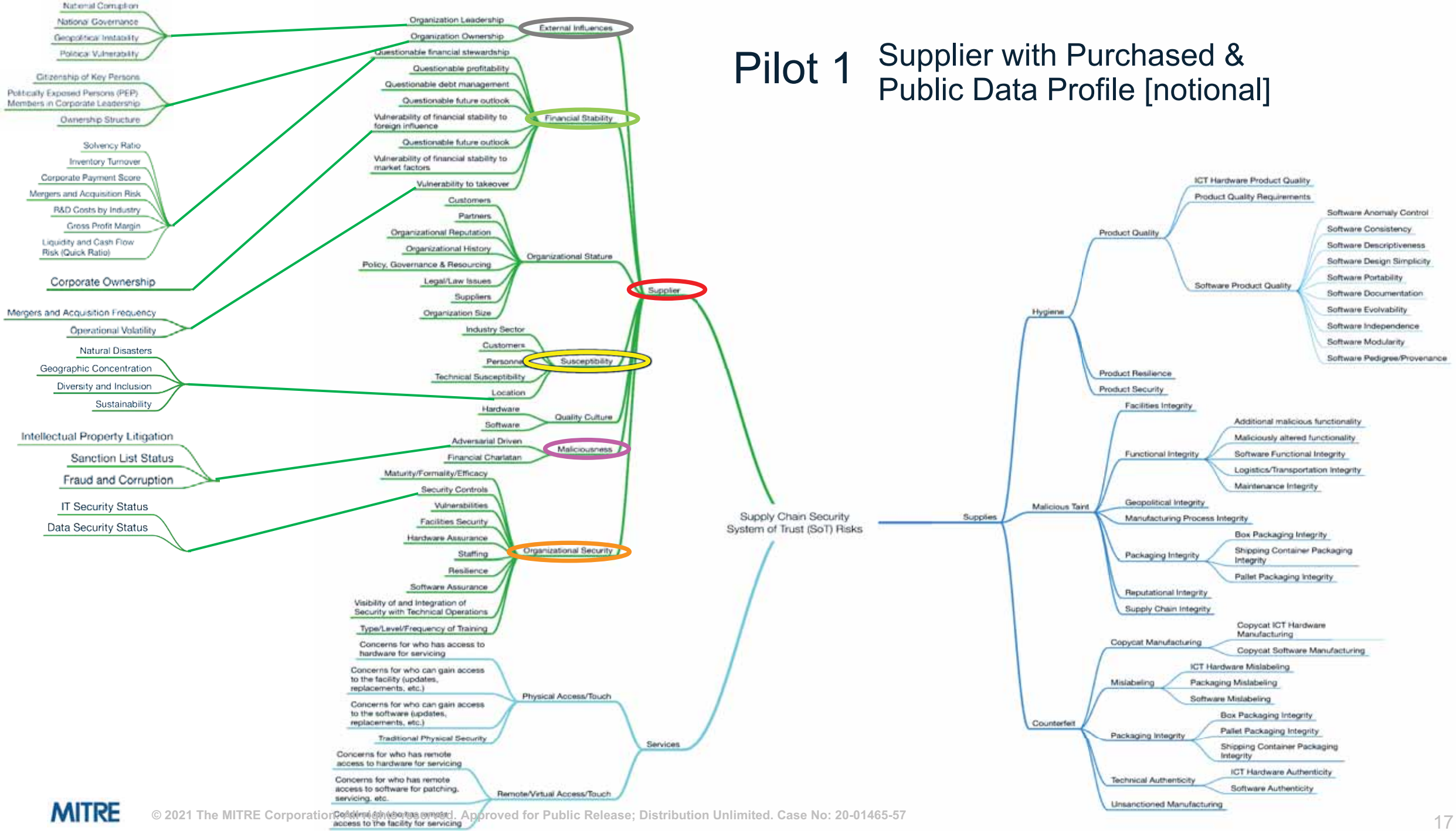
Assessment Scope, Skills & Means

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

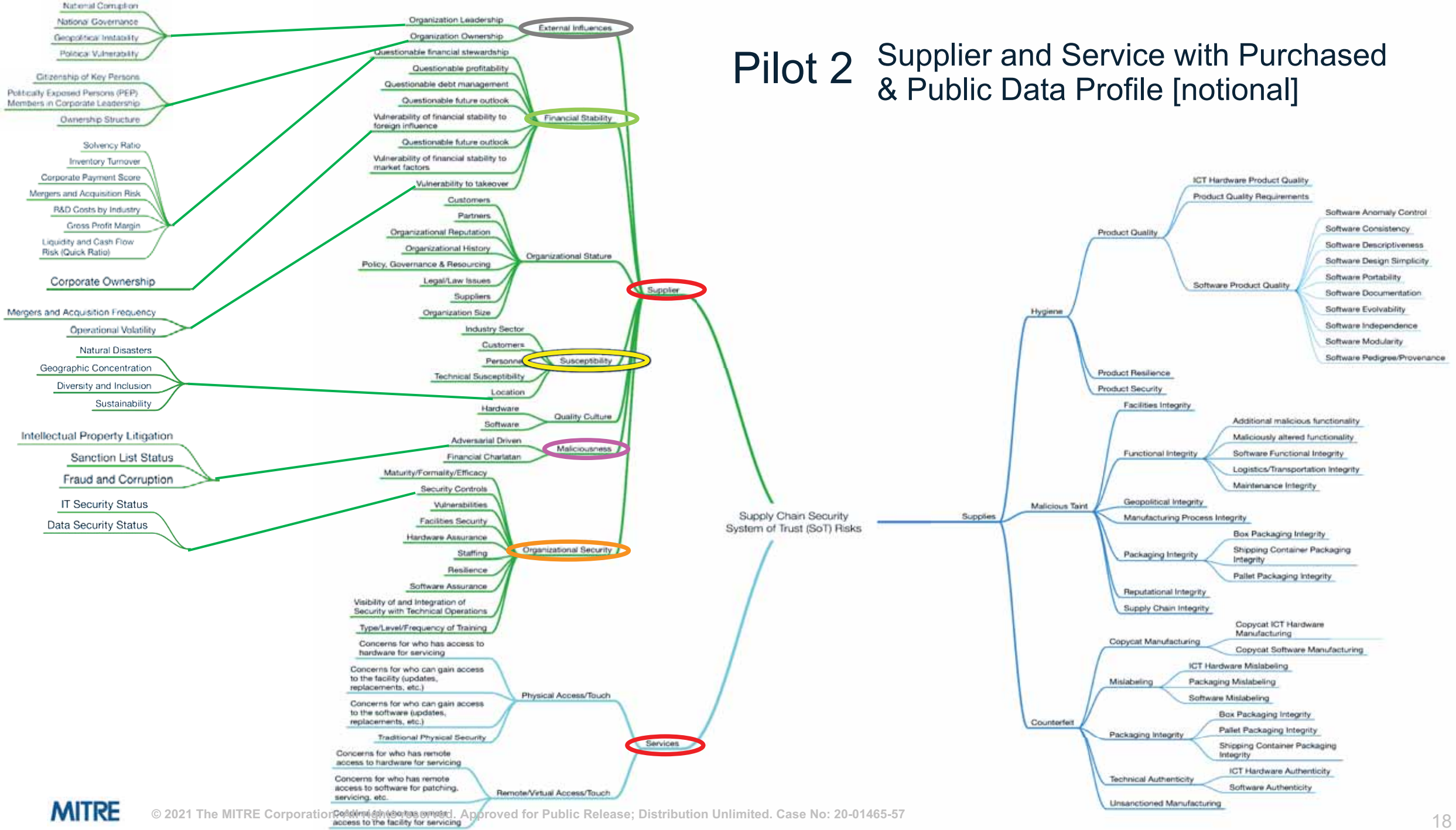
Assessment Constraints

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

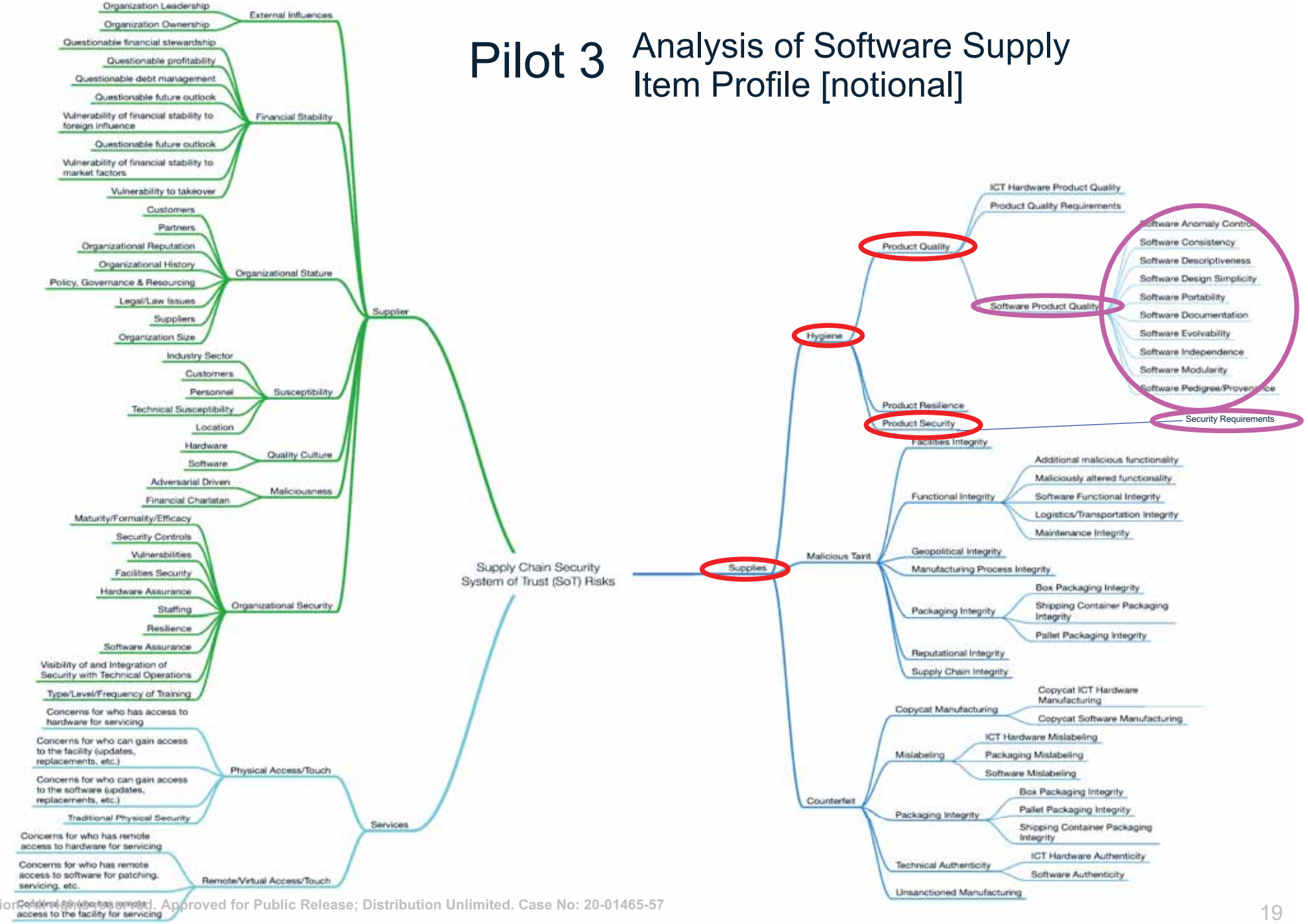
Pilot 1 Supplier with Purchased & Public Data Profile [notional]



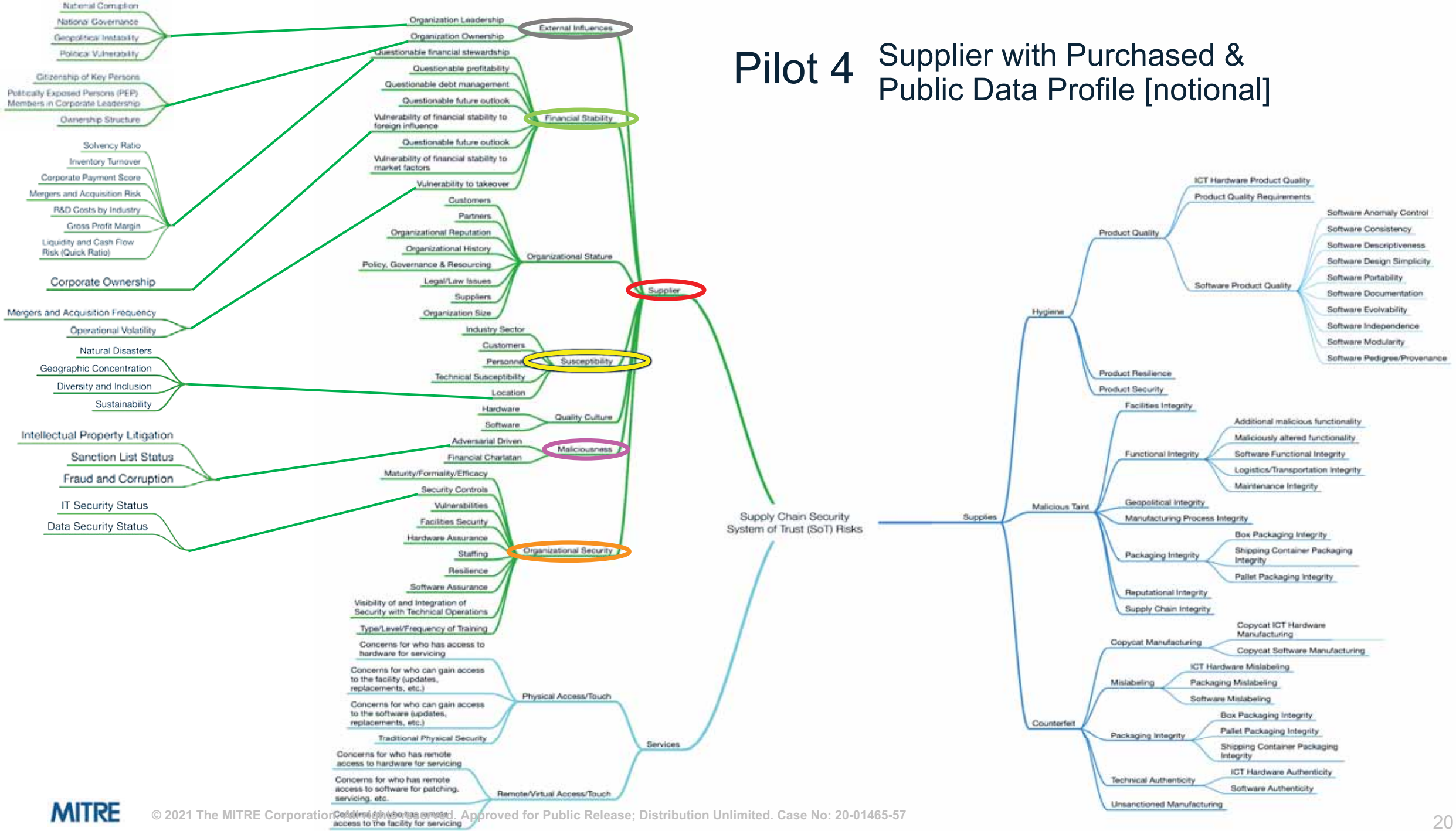
Pilot 2 Supplier and Service with Purchased & Public Data Profile [notional]



Pilot 3 Analysis of Software Supply Item Profile [notional]

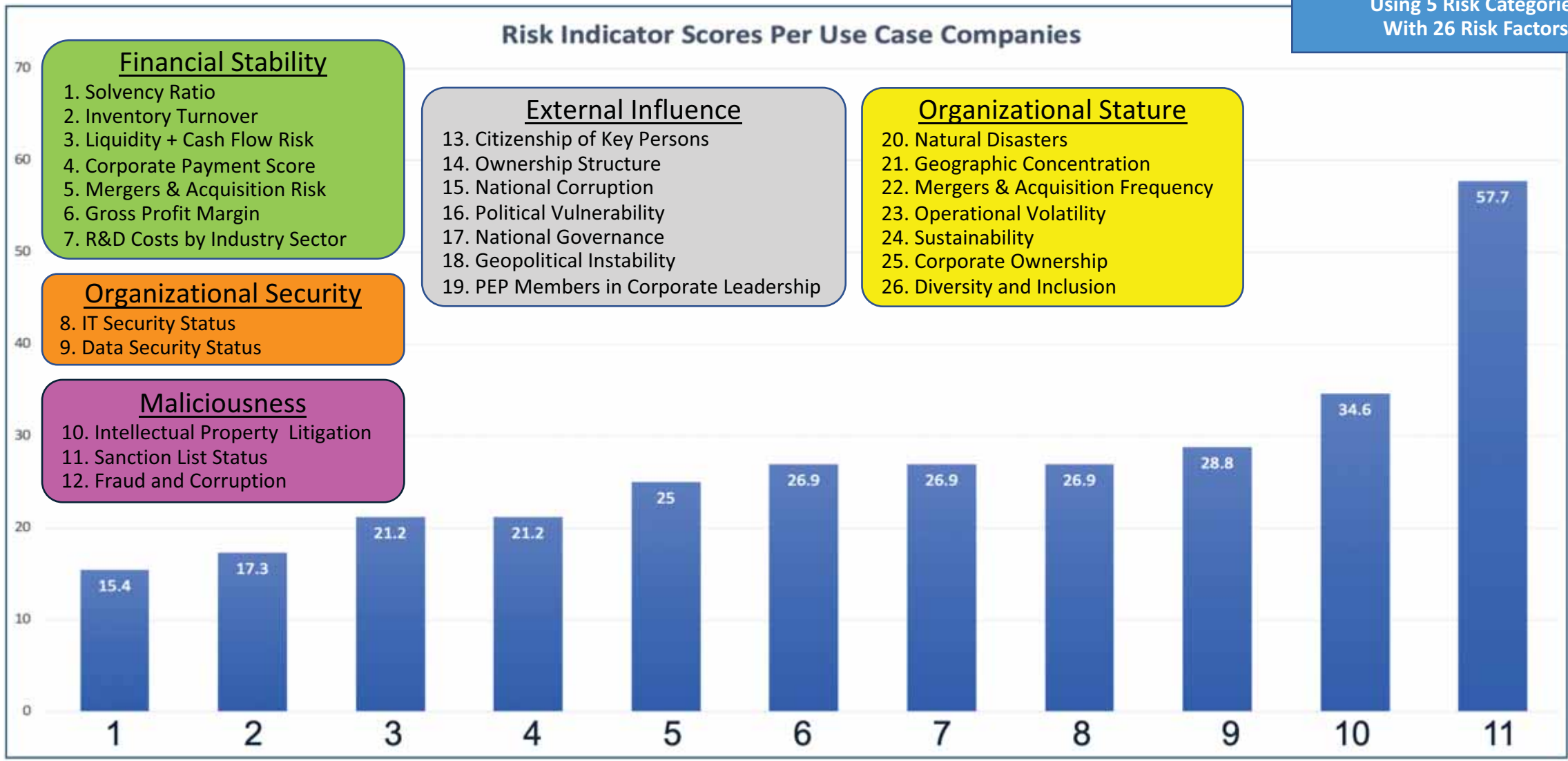


Pilot 4 Supplier with Purchased & Public Data Profile [notional]



SoT Pilot 1: Companies of Interest

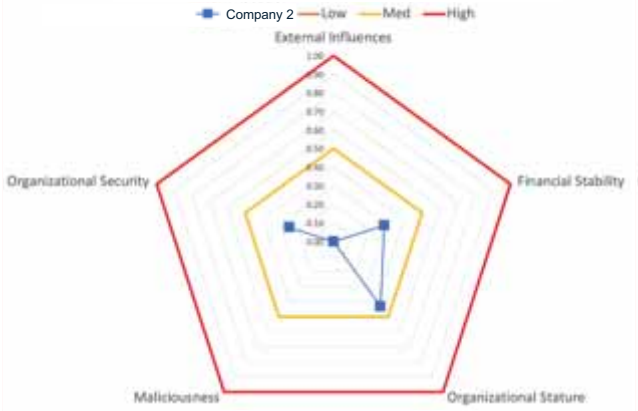
Supplier and Public Data Profile of the System of Trust Using 5 Risk Categories With 26 Risk Factors



* 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

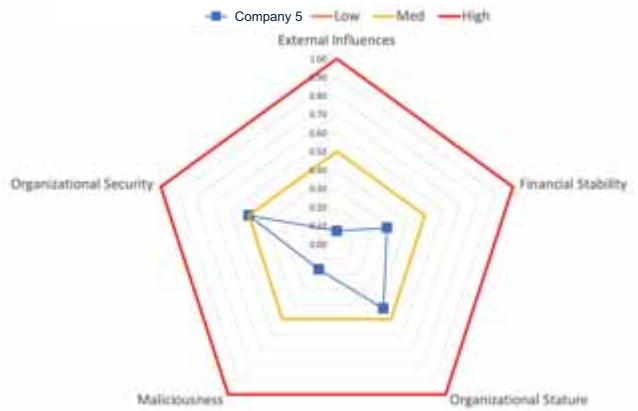
Company 2



Company 3

Company 4

Company 5



Company 6

Company 7

Company 8

Company 9

Company 10

Company 11

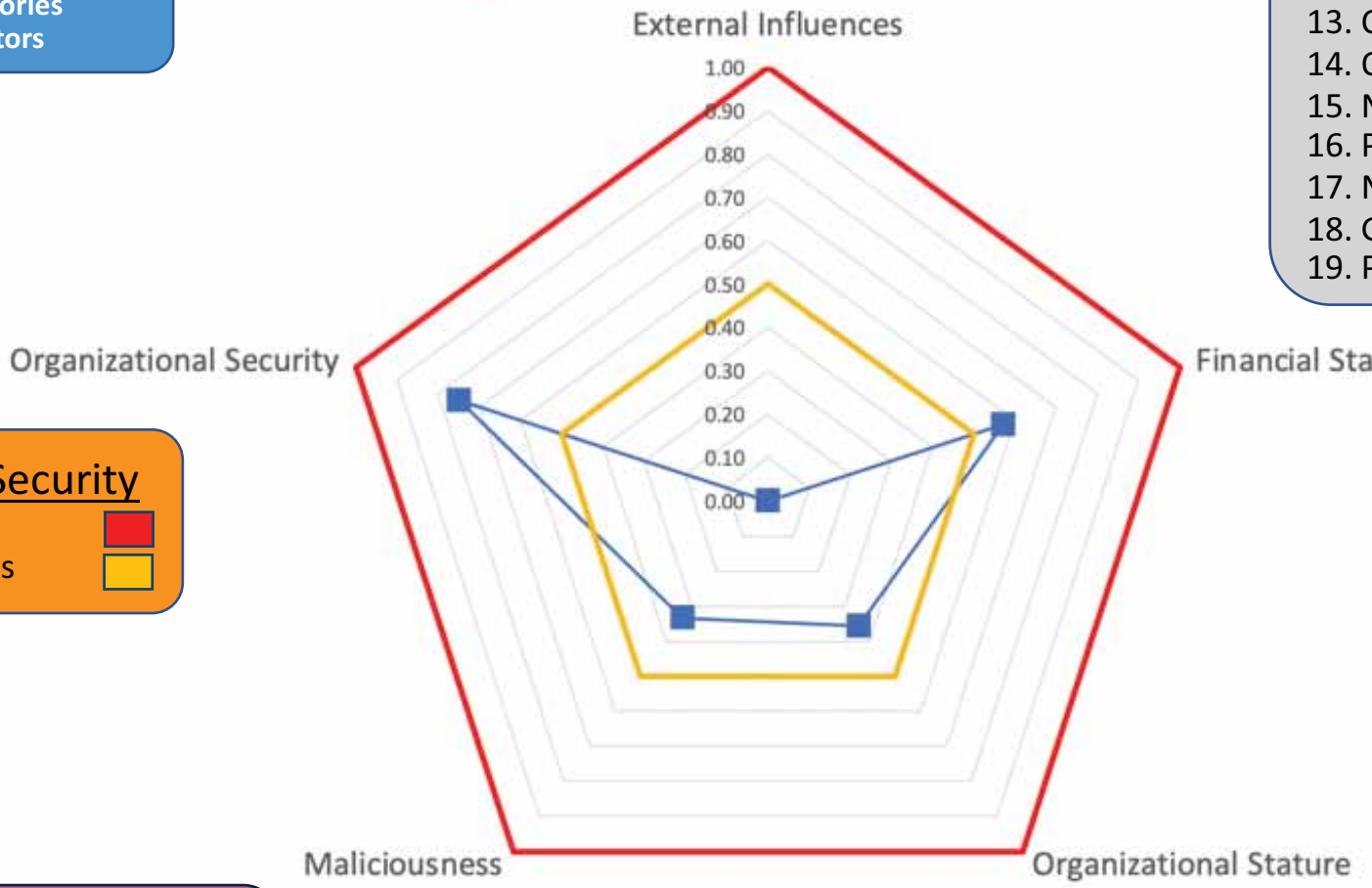
System of Trust Pilot 1: Companies of Interest

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

MITRE

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

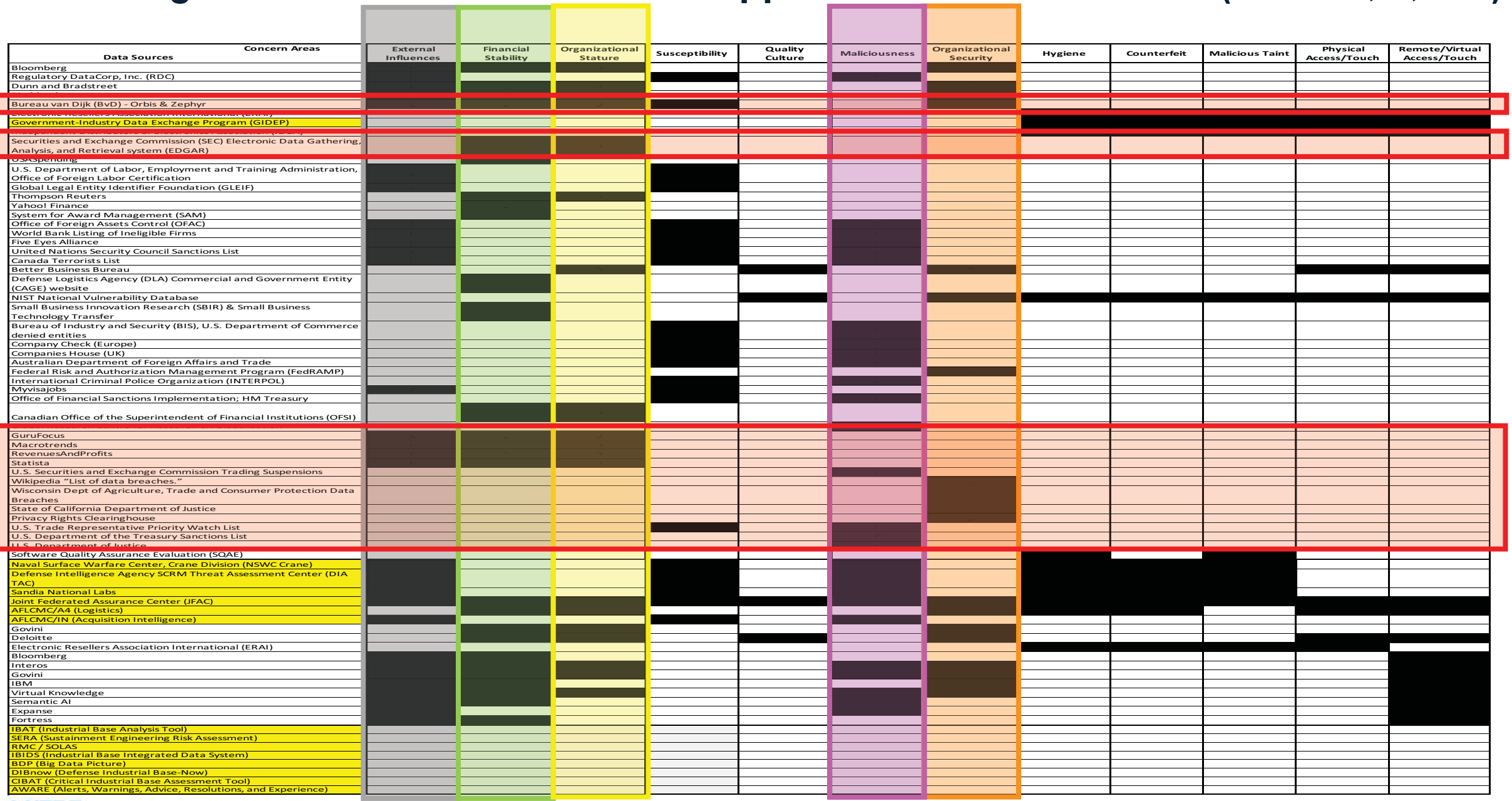
Financial Stability
1. Solvency Ratio
2. Inventory Turnover
3. Liquidity + Cash Flow Risk
4. Corporate Payment Score
5. Mergers & Acquisition Risk
6. Gross Profit Margin
7. R&D Costs by Industry Sector

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 (OFSI)												
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)												

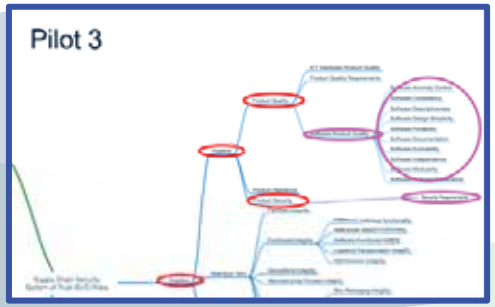
Risk Categories and Data Sources for Supplier Profile Assessment (Pilots 1, 2, & 4)

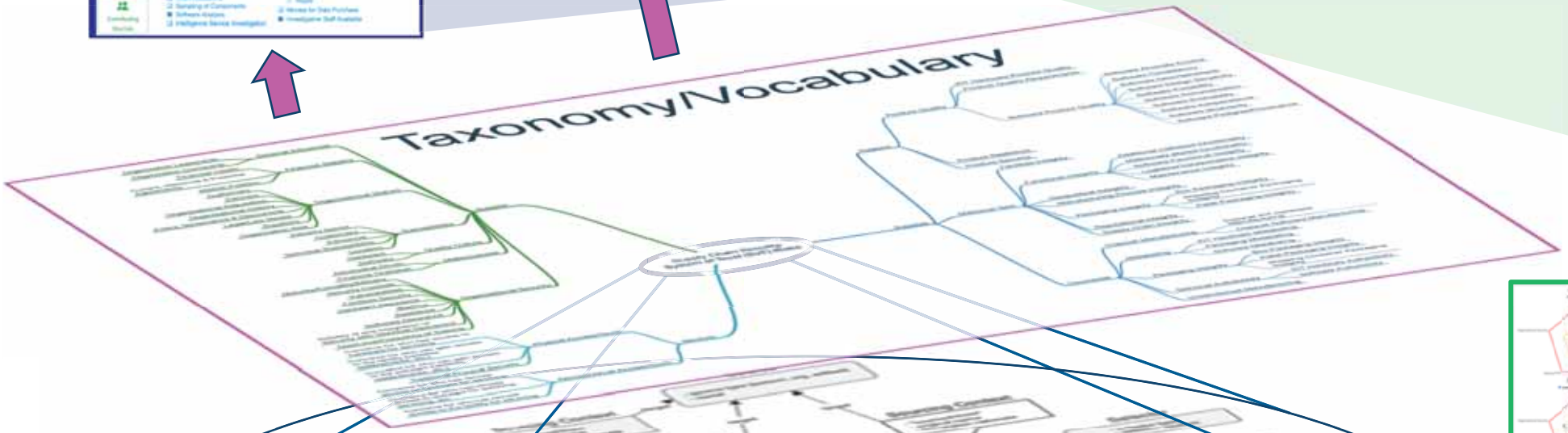


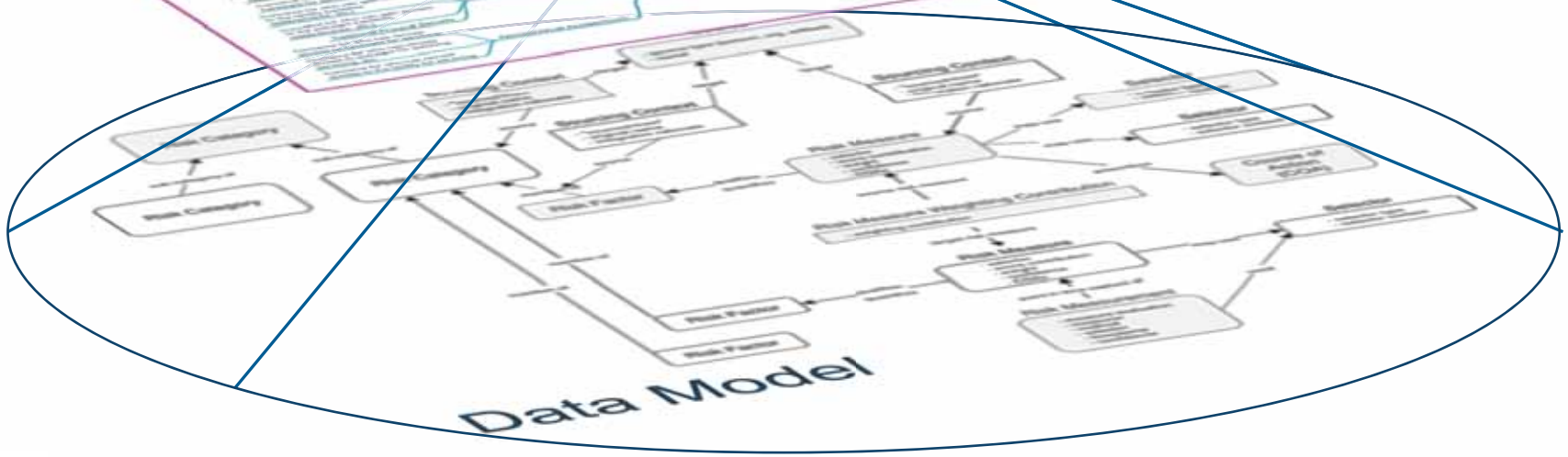
Analysis of Software Supply Item Profile Assessment (Pilot 3)

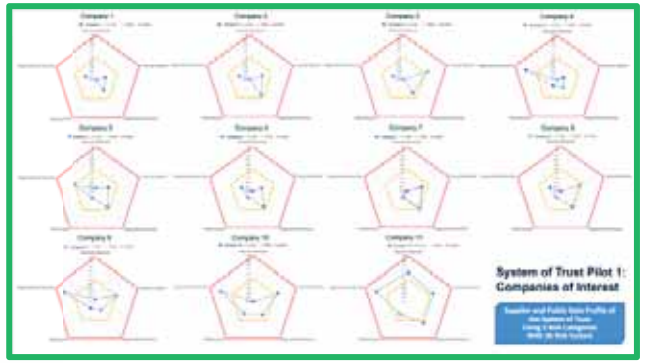
Data Sources / Concern Areas	External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Counterfeit	Malicious Taint	Physical Access/Touch	Remote/Virtual Access/Touch
Bloomberg												
Regulatory DataCorp, Inc. (RDC)												
Dunn and Bradstreet												
Pitchbook												
Bureau van Dijk (BvD) - Orbis & Zephyr												
Electronic Resellers Association International (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 (OFSI)												
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 (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)												

Tying together the System of Trust









Risk Model Manager

Export to CSV

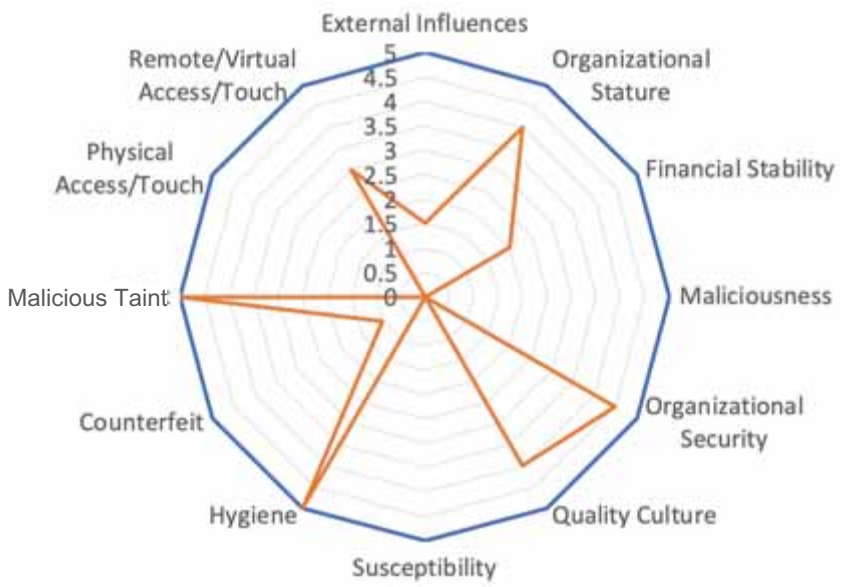
View

- View
- Edit
- Tailor
- Assess

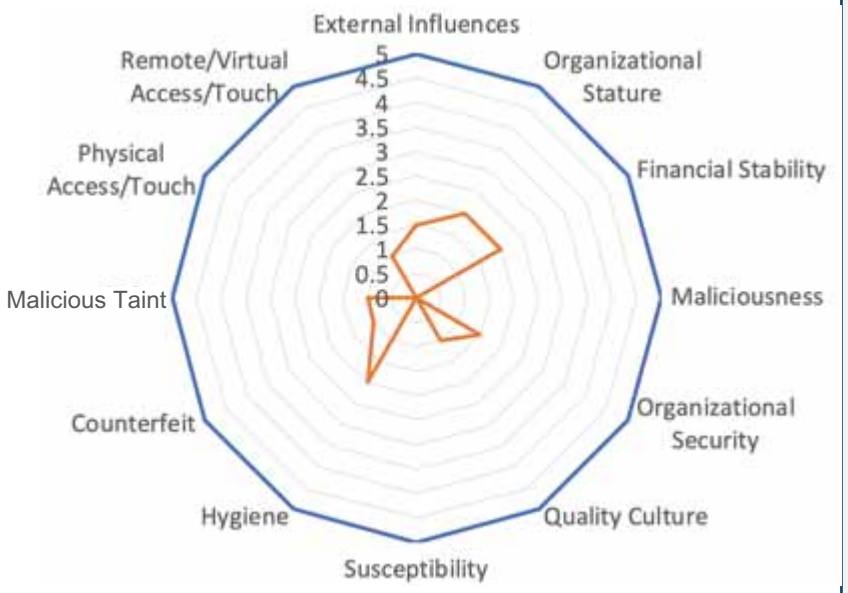
Risk Scoring [notional]

Goal

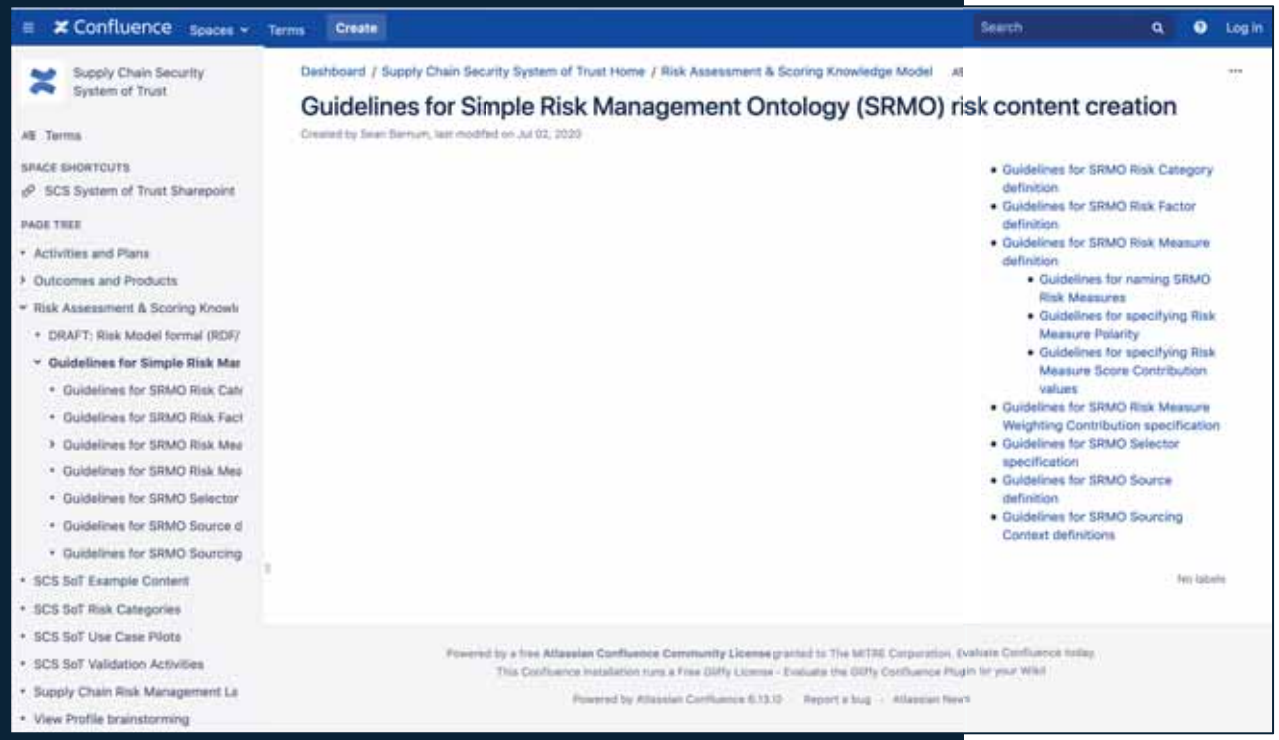
Top-Level Concerns Vendor/Product A

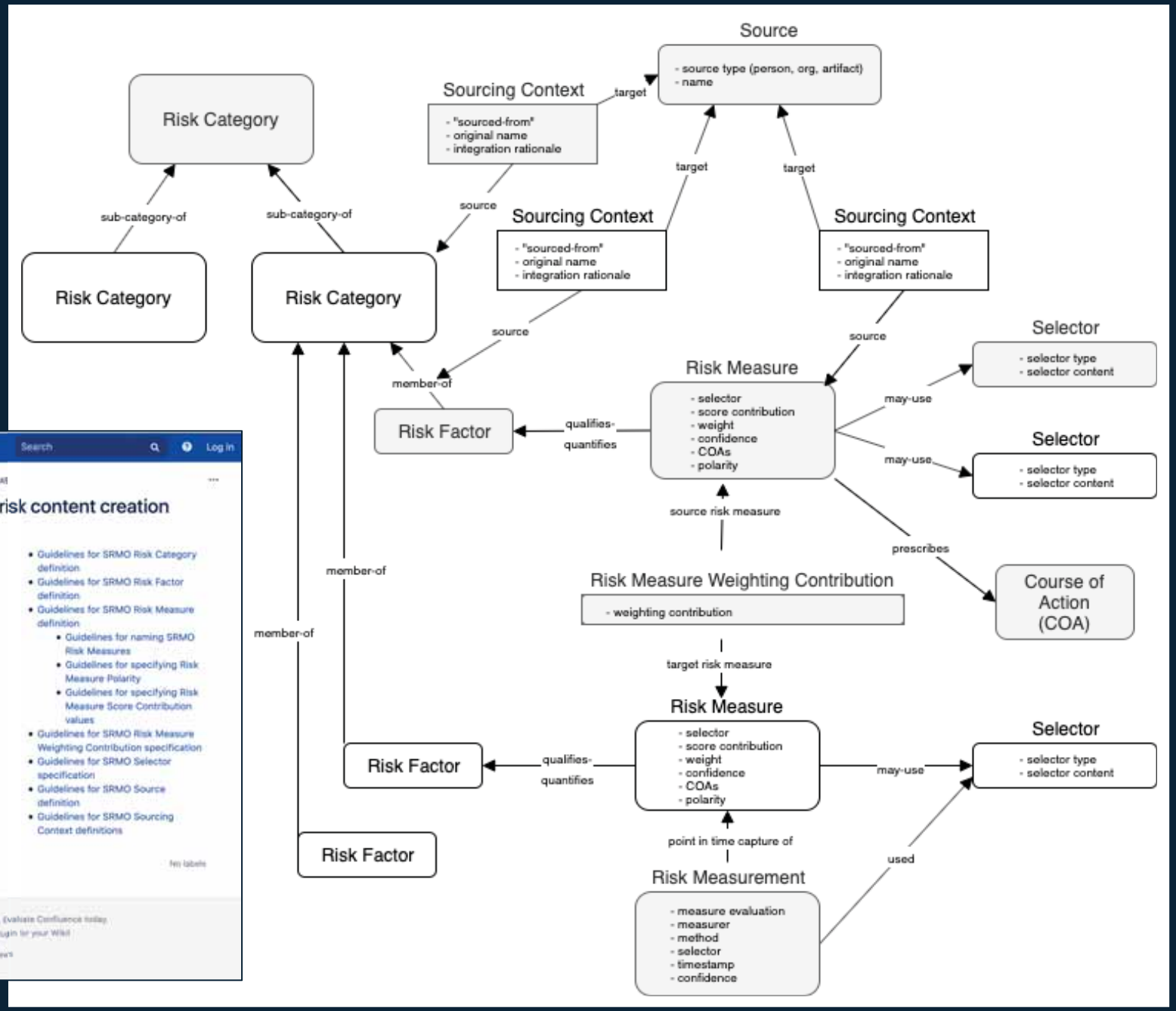


Top-Level Concerns Vendor/Product B

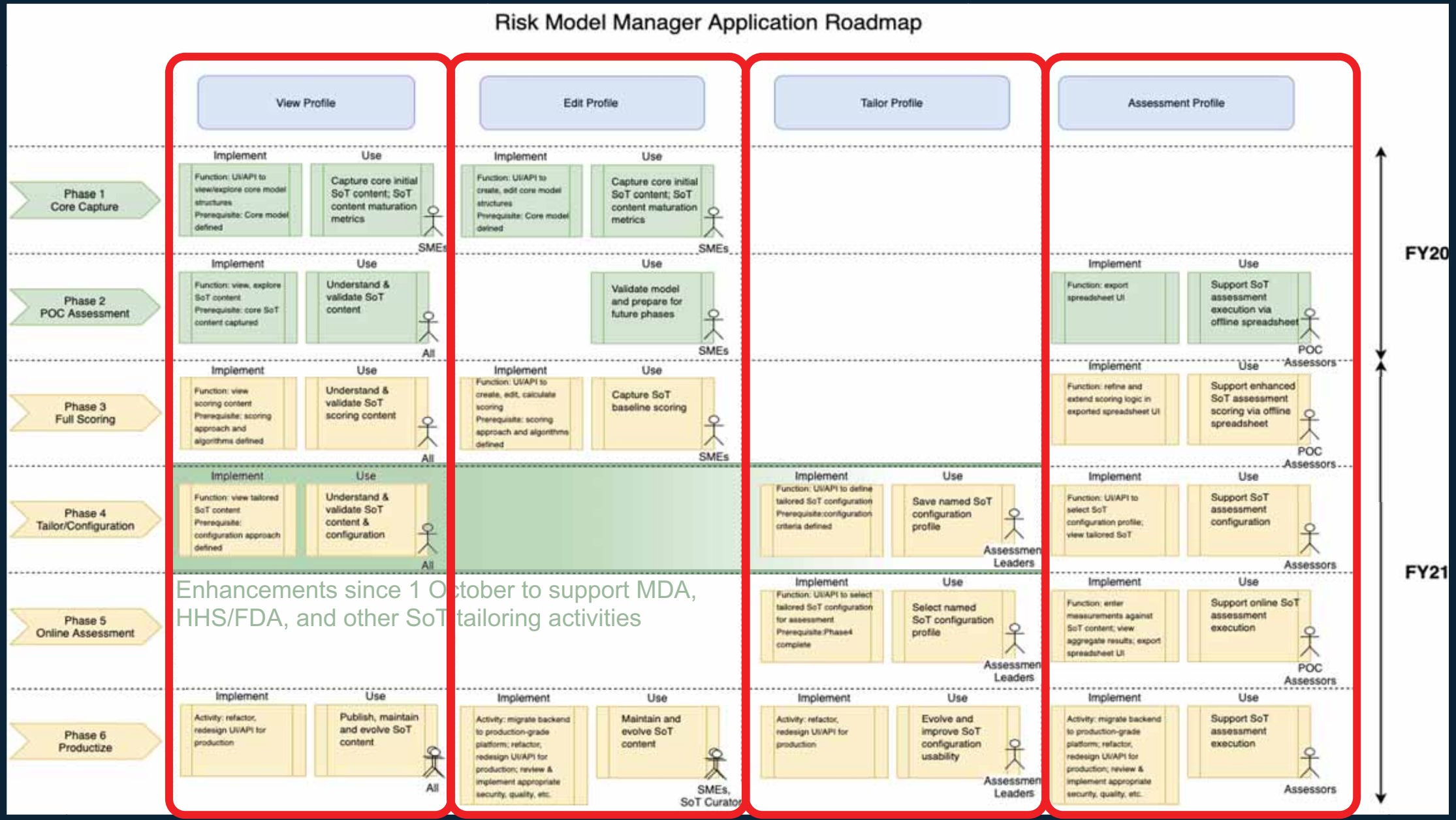


Risk Manager Modeler Data Model





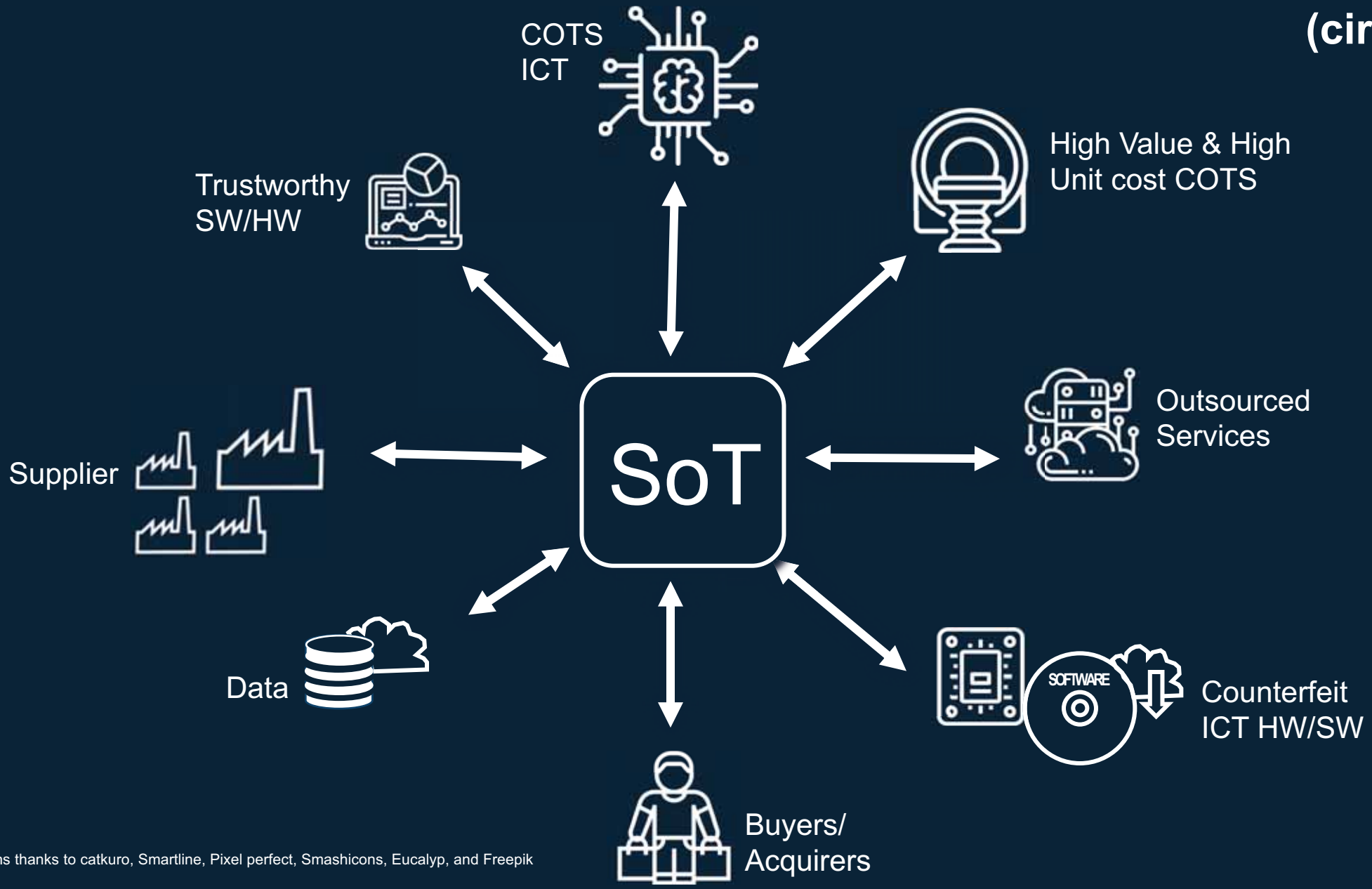
System of Trust Risk Model Manager* Application Roadmap



*Defining, viewing and evaluating the System of Trust

Effective Supply Chain Trust Interactions

(circa 2021+)



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

MITRE

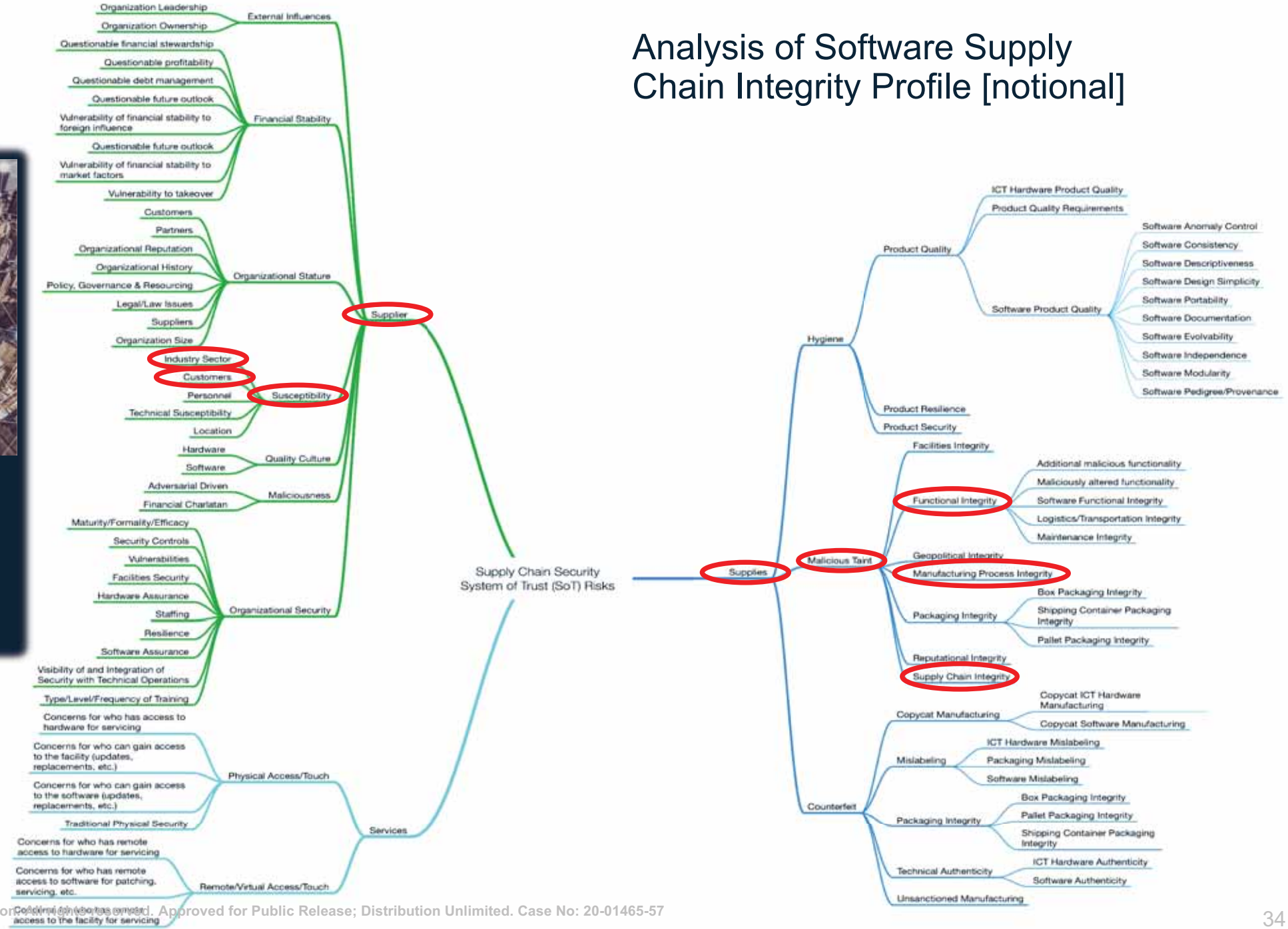
Next Steps – SoT Opportunities with Sponsors and Industry

- 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

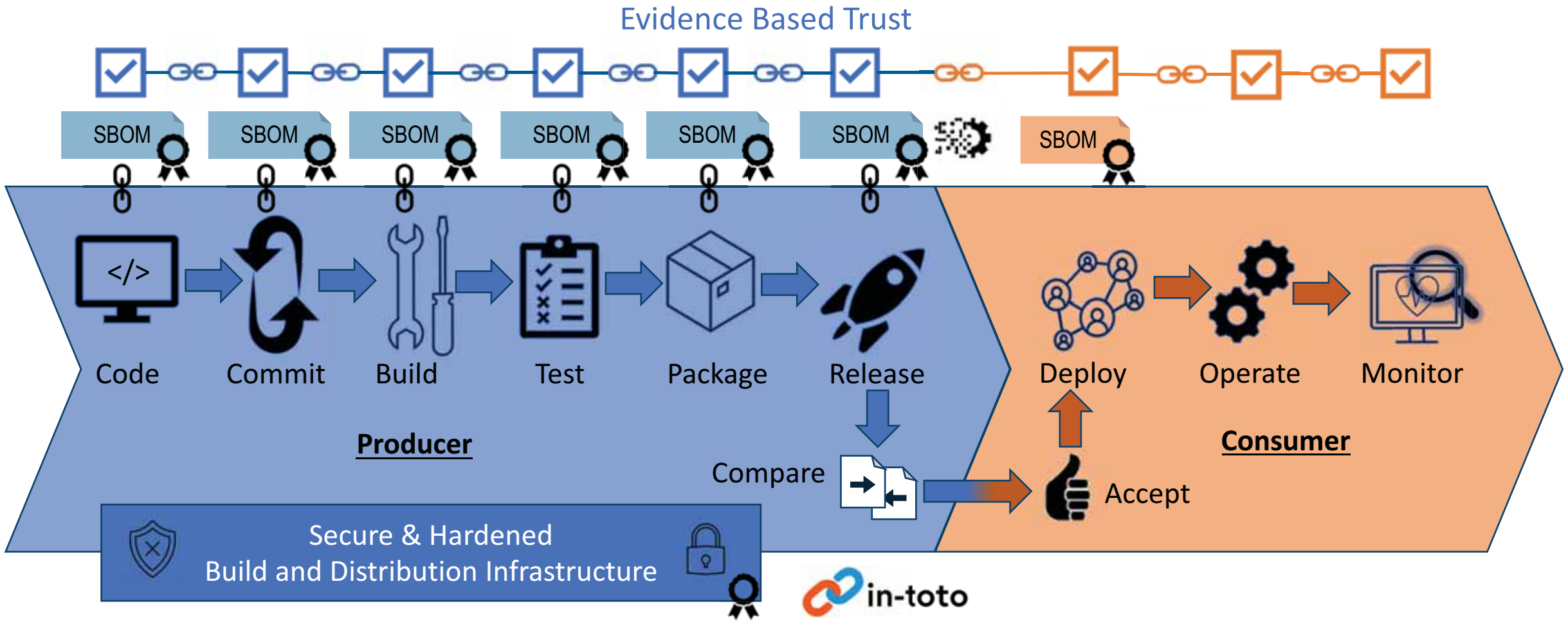
Outreach and Engagement

- American Bar Association (ABA) Technology Meeting
- Industry Technology & Innovation Roundtable
- MITRE Technical Centers Engineering Council
- DHS CISA NRMC & SNL "Company/ICT Element Scorecard" Team
- MITRE CyberSecurity Days
- Open Group July Member Meeting Plenary
- DHS OPO Director and Team
- DHS CISA NRMC 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 NRMC 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 NRMC 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



CISQ

WORKING GROUP

TOOL-TO-TOOL SOFTWARE BILL OF MATERIALS EXCHANGE

THE LINUX FOUNDATION

SPDX

About

The Software Package Data Ex
(SPDX®)

An open standard for communicating software bill of
information, including components, licenses, copyri
references. SPDX reduces redundant work by providi
format for companies and communities to share imp
thereby streamlining and improving compliance.

LEARN MORE

in-toto

About

Community

Get started

Learn more

GitHub

in-toto

A framework to secure the integrity of software supply chains

Provenance and Pedigree

DEFINITIONS

- *Provenance**
  1. The origin, or source of something
  2. The history of ownership of a valued ob
     literature
- *Pedigree**
  1. A register recording a line of ancestors
  2. An ancestral line : lineage
     The origin and the history of something
     history

CONFUSION

- *Many use "Provenance" for both mea*

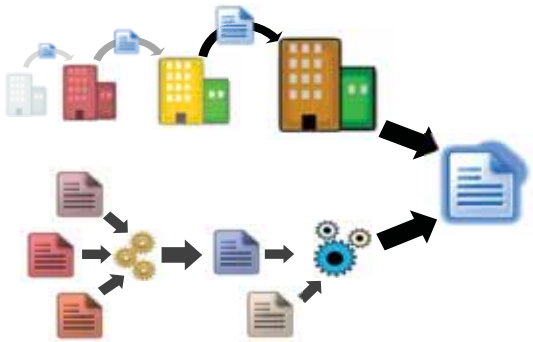
*The provenance of a piece of data is both the cu
lineage of processing and/or derivation that led*

**Definitions (from Merriam-Webs*

Separating Provenance and Pedigree

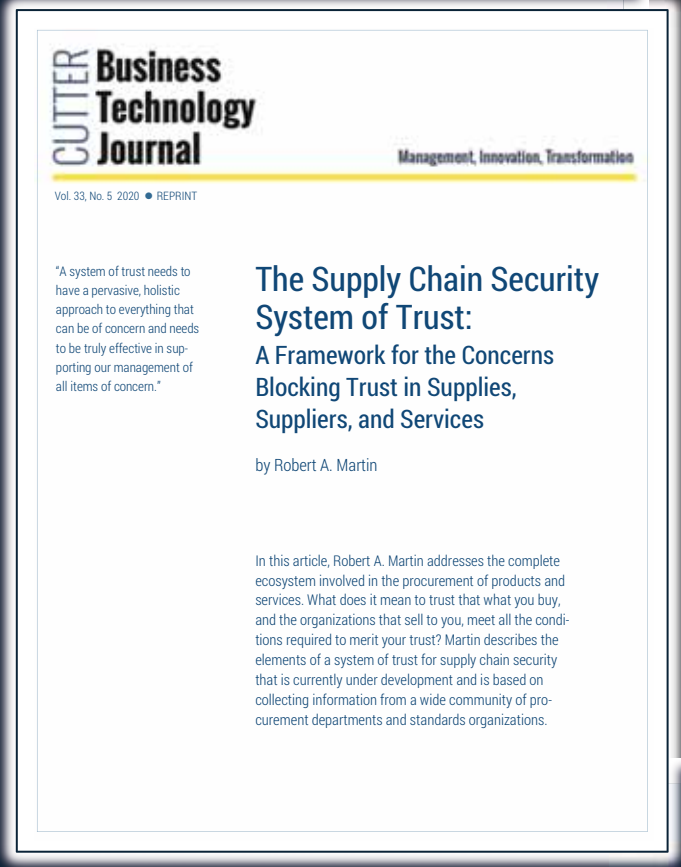
Provenance
Captures ***chain of custody*** of an Artifact, Document or Record

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



OMG
OBJECT MANAGEMENT GROUP

MITRE



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

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

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

Questions?