

Visible by Design:

How Standards Are Closing the Gap Between Compliance Obligations and Supply Chain Visibility

Robert Martin

Sr. Software and Supply Chain Assurance Prin. Eng.

Cyber Integration and Innovation Cell Department

Cyber Engineering Division

Center for AI, Cyber, & Digital

MITRE Technology & Engineering



SCITT

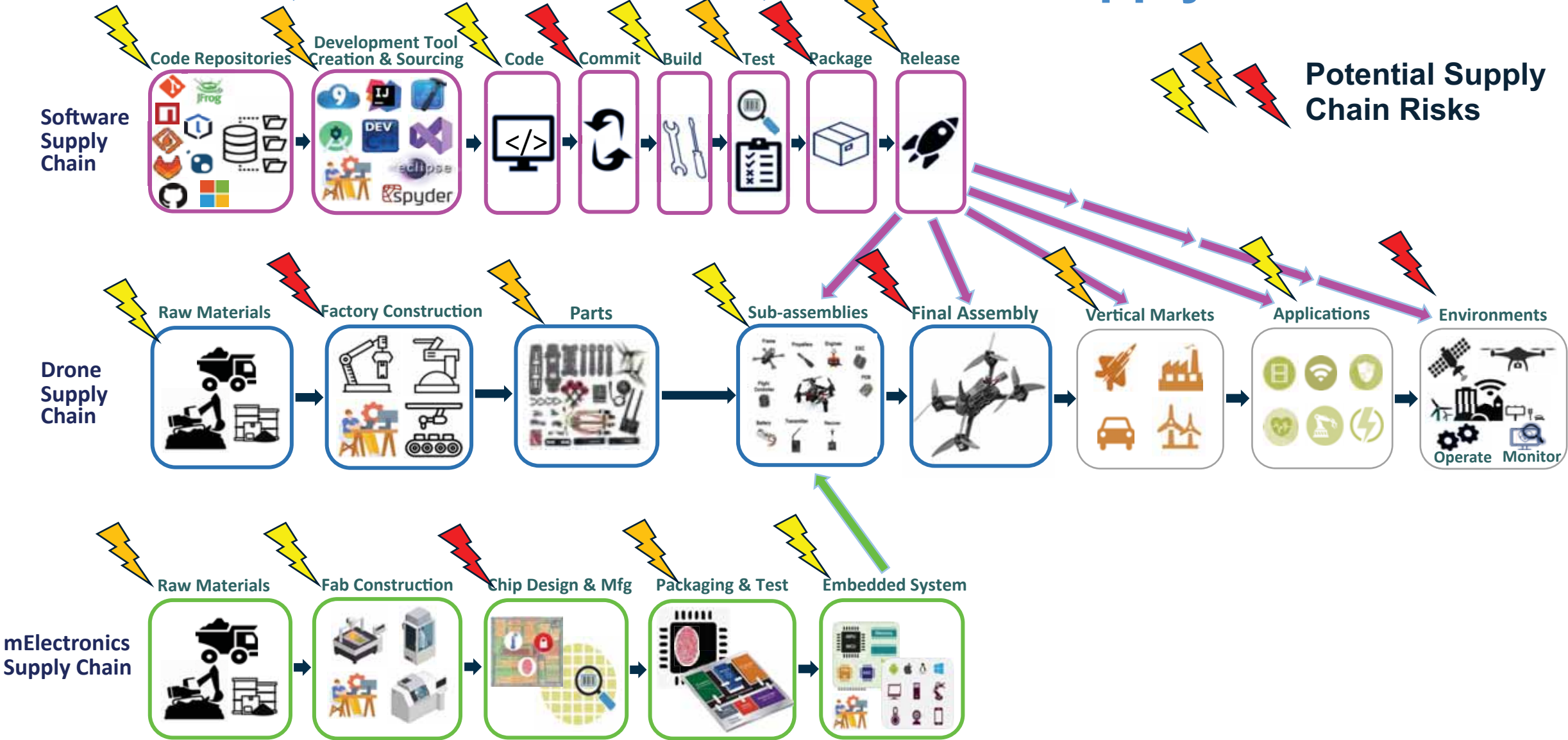


BOMs

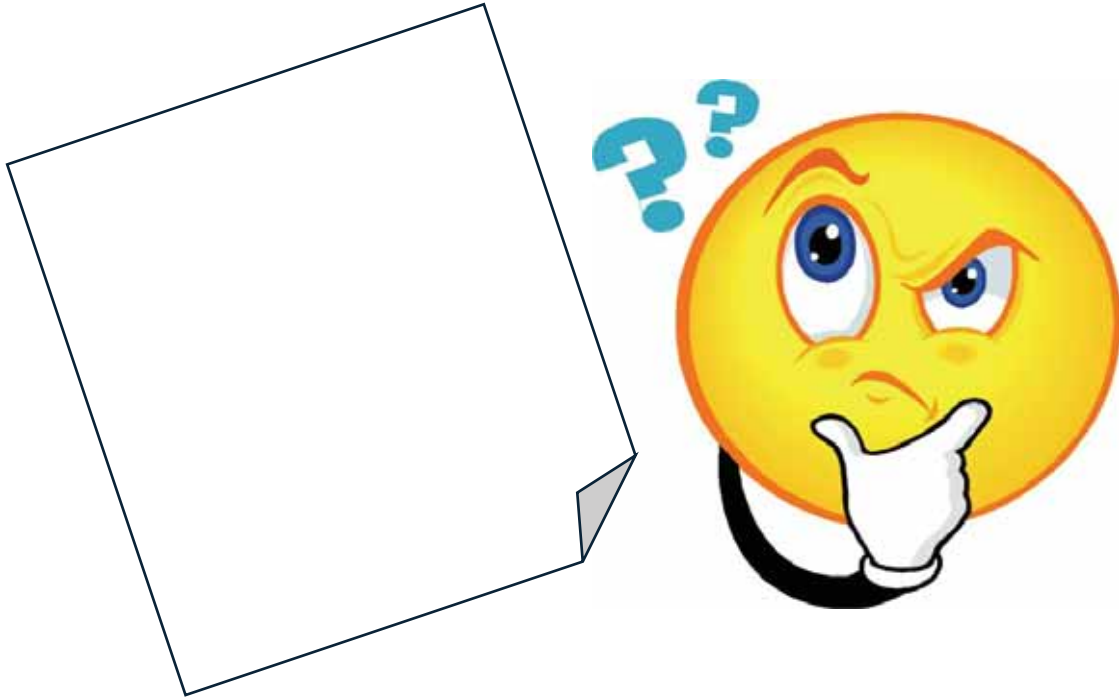
29 April 2026

MITRE

Software, MicroElectronics, and UAV Supply Chains



Open Question: What Supply Chain Risks to Manage?

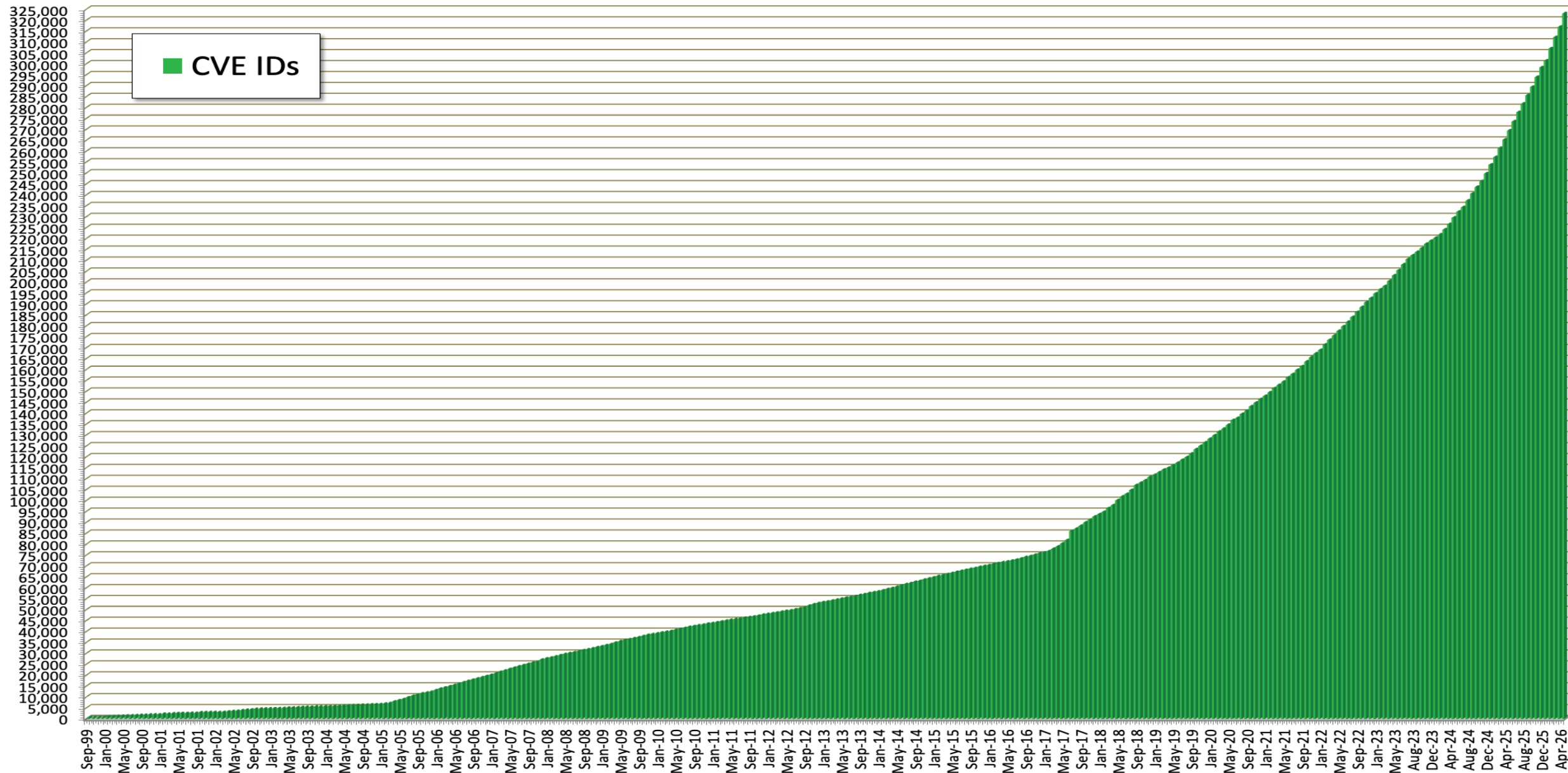


CVE 1999 to 2001

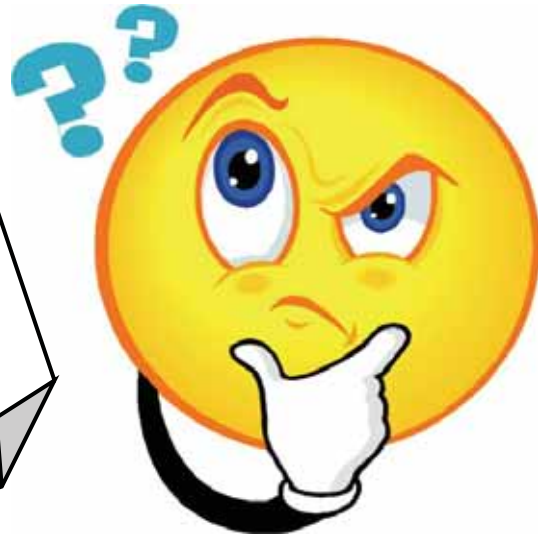


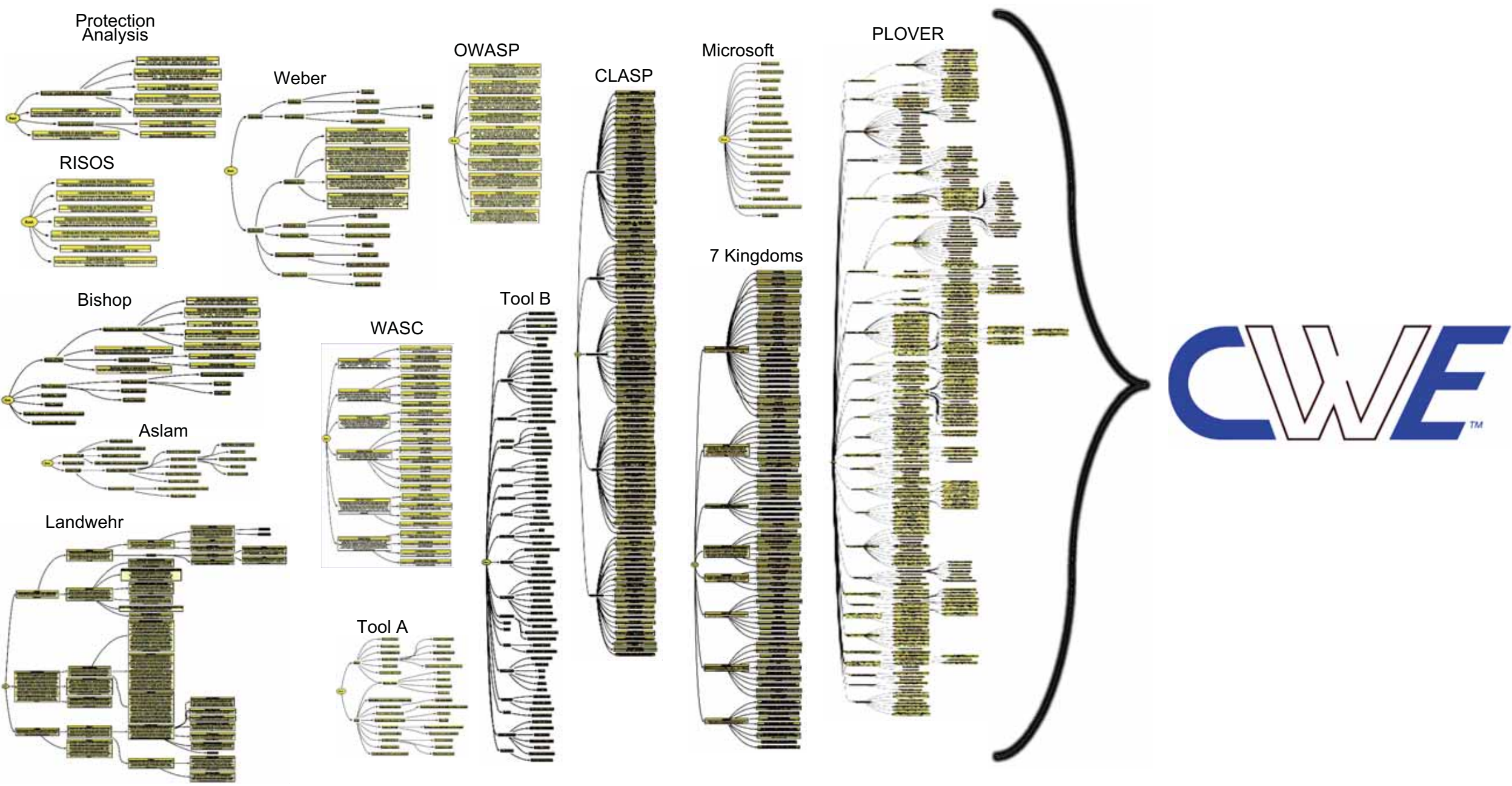


CVE 1999 to 2026

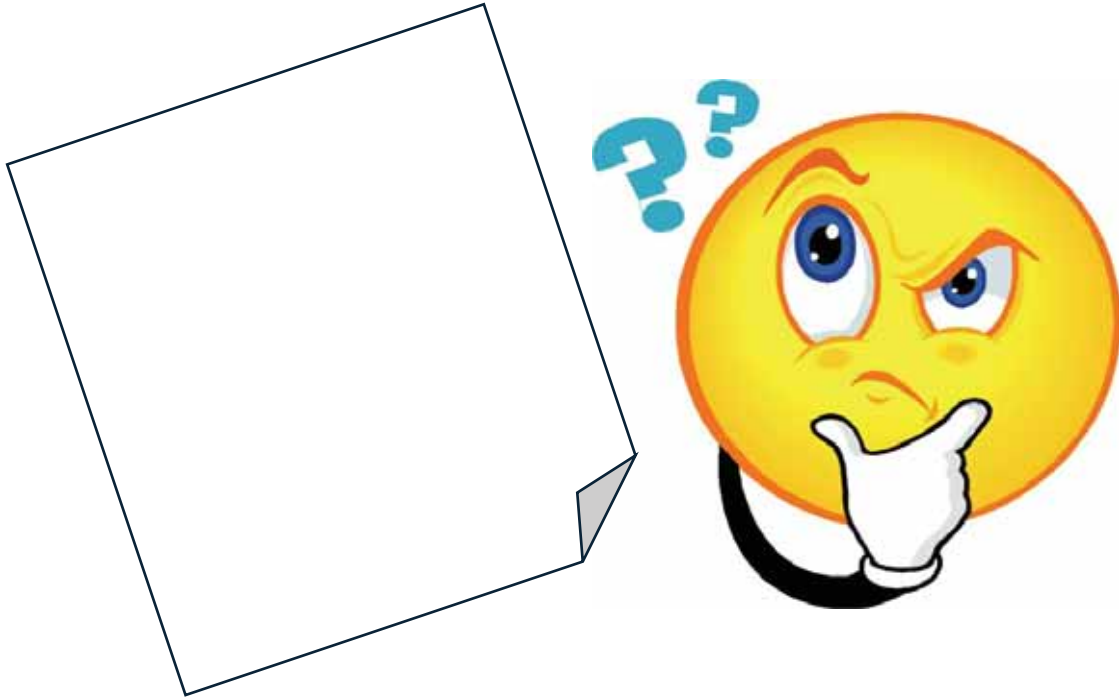


2003
What causes the
vulnerabilities we
tag with CVE Ids?





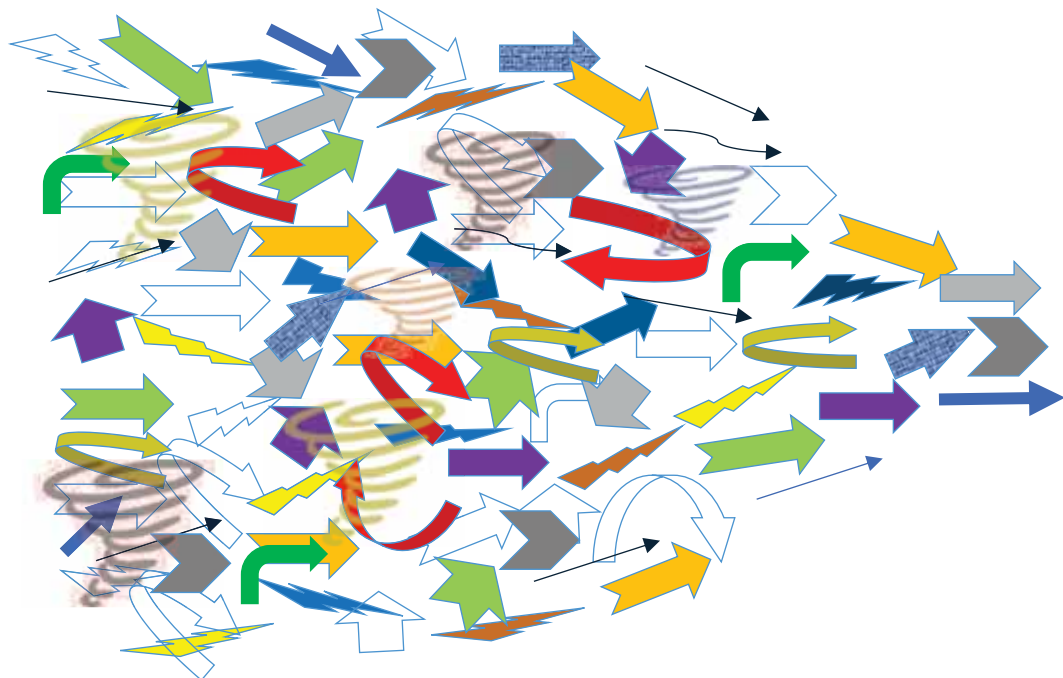
Open Question: What Supply Chain Risks to Manage?



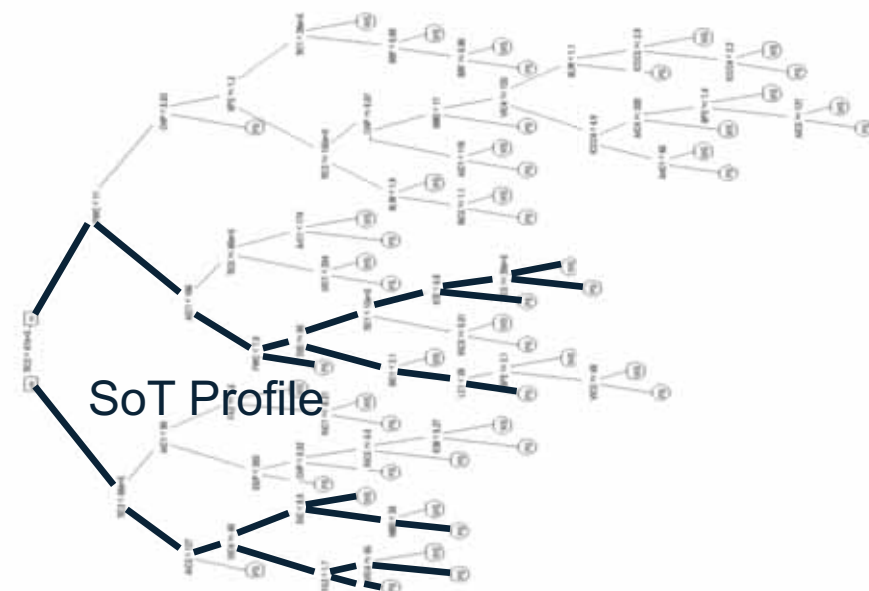
MITRE's System of Trust™ (SoT)

"What Supply Chain Risks to Manage?"

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



Address Chaos, Align & Organize



Simplify, Tailor & Use

System of Trust

Risk Categories

(RC-13)	Supplier Financial Stability Risks
(RC-76)	Supplier Organizational Security Risks
(RC-4)	Supplier Susceptibility
(RC-20)	Supplier Quality Culture Risks
(RC-105)	Supplier Organizational Effectiveness Risks
(RC-7)	Supplier Ethical Risks
(RC-6)	Supplier External Influences

(RC-13) Supplier Financial Stability Risks

- (RC-257) Short-term Financial Health Risks
- (RC-256) Financial Stewardship Risks
- (RC-260) Adverse Market Factors
- (RC-258) Long-term Financial Health Risks
- (RC-262) Foreign Financial Obligations

(RC-76) Supplier Organizational Security Risks

- (RC-403) Technical Operations Risks
- (RC-441) Cyber Threat Intelligence Risks
- (RC-16) Security Training Deficiencies
- (RC-346) Security Capabilities and Operations Risks
- (RC-434) Cyber Threat Activity Risks
- (RC-400) Security Governance and Compliance Risks

(RC-105) Supplier Organizational Effectiveness Risks

- (RC-538) Structural & Operational Instability
- (RC-537) Geographical/Geopolitical Instability

(RC-7) Supplier Ethical Risks

- (RC-15) Association with Foreign Intelligence Service or Foreign Military Entity
- (RC-26) Pattern of Criminal Behavior
- (RC-682) Pattern of Questionable Behavior

(RC-6) Supplier External Influences

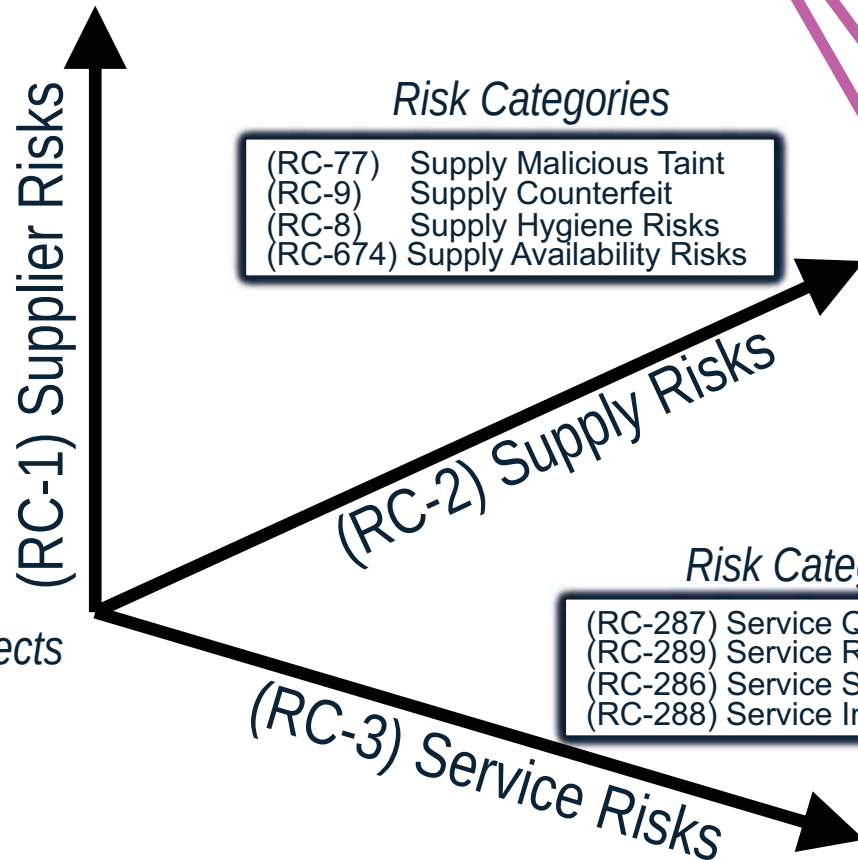
- (RC-5) Ownership and Control Risks
- (RC-534) Foreign Business Relationship Risks
- (RC-536) Adverse Corporate Influences
- (RC-683) Public or Reputational Association Risks

Risk Categories

(RC-77)	Supply Malicious Taint
(RC-9)	Supply Counterfeit
(RC-8)	Supply Hygiene Risks
(RC-674)	Supply Availability Risks

Risk Categories

(RC-287)	Service Quality Risks
(RC-289)	Service Resilience Risks
(RC-286)	Service Security Risks
(RC-288)	Service Integrity Risks



System of Trust Risk Areas* **

Supply Chain Risks							Supply Chain Risks							Supply Chain Risks			
Definition: Risks related to characteristics of a supply chain (products) or services, including their supply chain provenance and pedigree, that may potentially impact consumers of those supply chain products or services.							Definition: Risks related to characteristics of a supply (product), including their supply chain provenance and pedigree, that may potentially impact consumers of that supply (product).							Definition: Risks related to characteristics of a service, including their supply chain provenance and pedigree, that may potentially impact consumers of that service.			
(RC-13) Supplier Financial Stability Risks	(RC-76) Supplier Organizational Security Risks	(RC-4) Supplier Susceptibility	(RC-20) Supplier Quality Cultural Risks	(RC-5) Supplier Organizational Resilience Risks	(RC-7) Supplier Ethical Risks	(RC-6) Supplier External Influences	(RC-77) Supplier Malicious Taint	(RC-9) Supplier Counterfeit	(RC-8) Supplier Hygiene Risks	(RC-75) Supplier Reliability Risks	(RC-287) Service Quality Risks	(RC-289) Service Resilience Risks	(RC-288) Service Integrity Risks				
(RC-257) Short-term Financial Health Risks	(RC-403) Technical Operations Risks	(RC-22) Susceptibility due to Location	(RC-630) Subcontractor Supply Chain Hygiene Risks	(RC-538) Structural & Operational Instability	(RC-15) Association with Foreign Intelligence Service (FIS) or Foreign Military Entity	(RC-5) Ownership and Control Risks	(RC-155) Supply Chain Management Integrity Risks	(RC-54) Packaging Integrity Risks	(RC-214) Supply (product) Resilience Risks	(RC-678) Supply Material Sourcing Risks	(RC-563) Service Quality Infrastructure Pedigree Risks	(RC-598) Service Infrastructure Redundancy Risks	(RC-294) Service Specific Security Risks				
(RC-256) Financial Stewardship Risks	(RC-441) Cyber Threat Intelligence Risks	(RC-25) Susceptibility due to Industry Sector	(RC-631) Supplier has Past Performance Issues on Contracts with other Companies	(RC-537) Geographical/Geopolitical Instability	(RC-26) Pattern of Criminal Behavior	(RC-534) Foreign Business Relationship Risks	(RC-149) Manufacturing Process Integrity Risks	(RC-127) Unsanctioned Manufacturing	(RC-201) Supply (product) Security Risks	(RC-679) Supply Fragility Risks	(RC-562) Service Quality Infrastructure Provenance Risks	(RC-599) Service Infrastructure Diversity Risks	(RC-11) Remote/Virtual Access to Service Infrastructure Risks				
(RC-260) Adverse Market Factors	(RC-16) Security Training Deficiencies	(RC-21) Susceptibility due to Personnel	(RC-18) Subcontractor Supply Chain Security Risks		(RC-682) Pattern of Questionable Behavior	(RC-536) Adverse Corporate Influences	(RC-154) Geopolitical Integrity Risks	(RC-126) Mislabeling	(RC-201) Supply (product) Quality Risks	(RC-681) Supply Obsolescence/Diminishing Manufacturing Sources & Material Shortages (DMSMS)	(RC-300) Service Specific Quality Risks		(RC-296) Service Security Infrastructure Pedigree Risks				
(RC-258) Long-term Financial Health Risks	(RC-346) Security Capabilities and Operations Risks	(RC-448) Susceptibility due to Espionage	(RC-19) Internal Quality Control Risks			(RC-683) Public or Reputational Association Risks	(RC-153) Functional Integrity Risks	(RC-118) Technical Authenticity Risks		(RC-677) Supply Industrial Capacity Risks	(RC-302) Service Specific Reliability Risks		(RC-295) Service Security Infrastructure Provenance Risks				
(RC-262) Foreign Financial Obligations	(RC-434) Cyber Threat Activity Risks	(RC-24) Susceptibility due to Customers	(RC-632) Internal SCRM Policy and Practices Risks				(RC-151) Logistics/Transportation Integrity Risks	(RC-128) Copycat Manufacturing		(RC-676) Supply Industrial Capability Risks	(RC-587) Service Reliability Infrastructure Provenance Risks		(RC-10) Physical Access to Service Infrastructure Risks				
	(RC-400) Security Governance and Compliance Risks	(RC-23) Technical Susceptibility					(RC-152) Poor Reputation for Integrity			(RC-680) Supply Criticality	(RC-588) Service Reliability Infrastructure Pedigree Risks						
							(RC-150) Facilities Integrity Risks										
							(RC-54) Packaging Integrity Risks										
							(RC-156) Maintenance Integrity Risks										

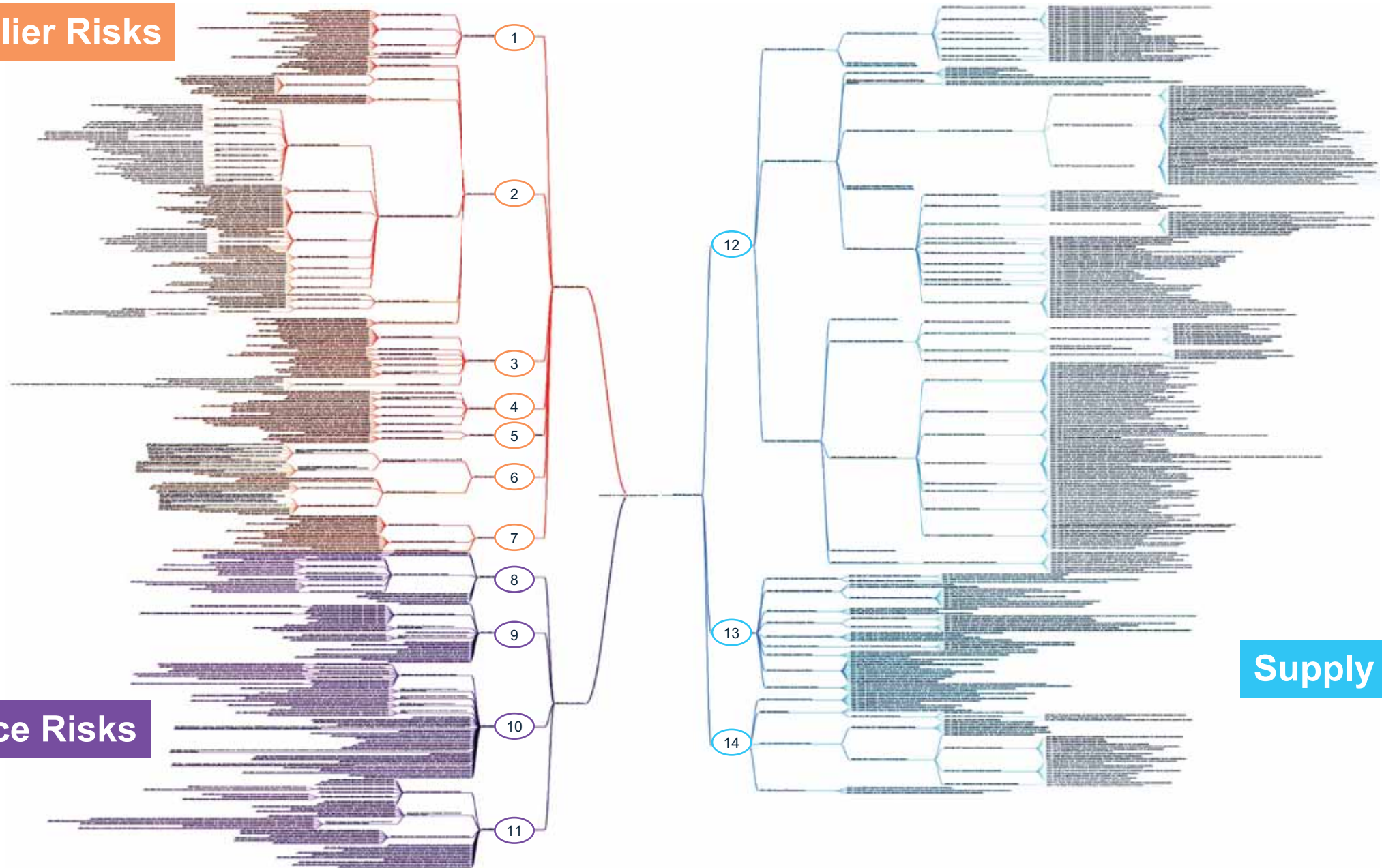


MITRE's Supply Chain Security System of Trust™ <https://sot.mitre.org/>

* Supply Chain Security Top 88 Risk Areas Levels 1-3
 ** System of Trust Expanding to Pharma, Food, and other types of Products

Supplier Risks

Service Risks



Supply Risks

Version 1.5 of SoT's Body of Knowledge

- Adding a group of risks about sustainability compliance risks from US and EU regulations
- Adding a group of risks about use of AI capabilities by the supplier, service provider, or in a product
- Revised and updated existing software supply risks to align with rest of SoT content
- Adding Risk Measures for all Risk Factors that had little or no coverage before.

<u>1.4.1</u>	<u>1.5</u>	
15	→ 15	top-level risk categories
243	→ 261	detailed risk categories
701	→ 733	specific measurable risks factors
1363	→ 2224	risk measures

International Society of Automation

Telecommunications Industry Association

bsi.

BATTELLE

THE Open GROUP

Micron

intel.

SIEMENS

SYNOPSYS

Onyx Spectrum TECHNOLOGY

gm

DELL Technologies

BOEING

SEAGATE

Microsoft

Schneider Electric

Hitachi, Ltd.

nasa SEWP V

CISCO

stryker

Raytheon Technologies

bakertilly INTERNATIONAL

V2X

TENCHI SECURITY

MITRE

opentext™

xylem
Let's Solve Water

LMI

EXIGER

KEARNEY

resilinc

interos

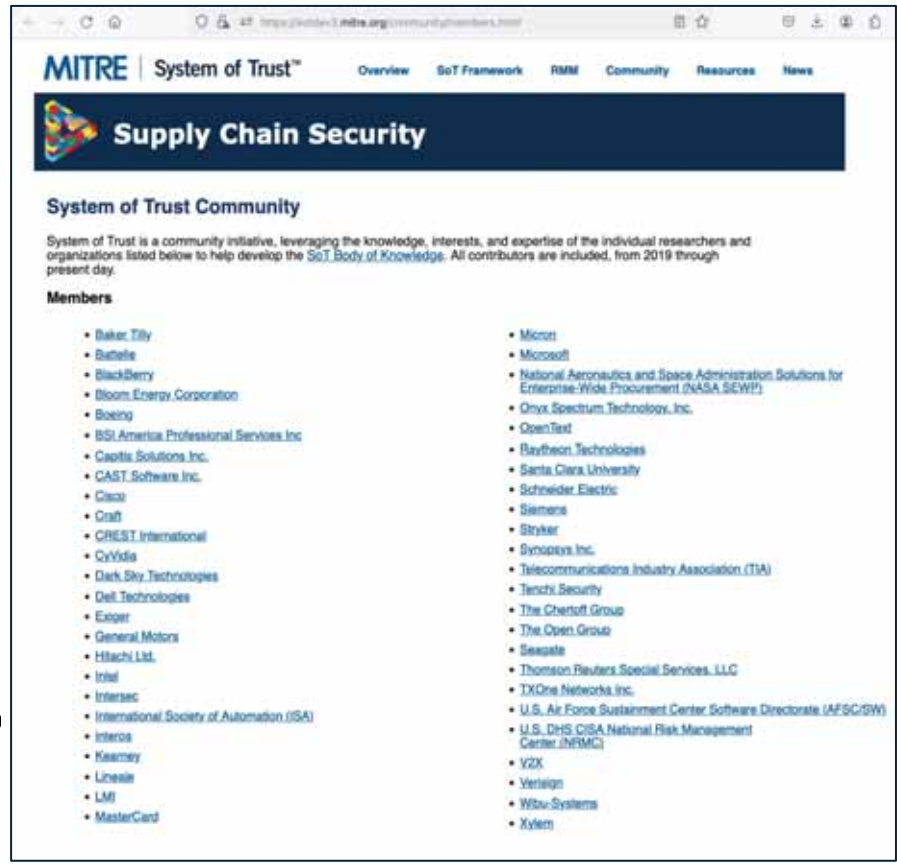
Craft

THOMSON REUTERS®

CAST
Software Intelligence for Digital Leaders

BlackBerry™

System of Trust™ Community



MITRE | System of Trust™

Supply Chain Security

System of Trust Community

System of Trust is a community initiative, leveraging the knowledge, interests, and expertise of the individual researchers and organizations listed below to help develop the SoT Body of Knowledge. All contributors are included, from 2019 through present day.

Members

- Baker, Tilly
- Battelle
- BlackBerry
- Bloom Energy Corporation
- Boeing
- BSI America Professional Services Inc.
- Capitis Solutions Inc.
- CAST Software Inc.
- Cisco
- Craft
- CREST International
- CyVidia
- Dark Sky Technologies
- Dell Technologies
- Exiger
- General Motors
- Hitachi Ltd.
- Intel
- Intersec
- International Society of Automation (ISA)
- Interos
- Kearney
- Lineale
- LMI
- MasterCard
- Micron
- Microsoft
- National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement (NASA SEWP)
- Onyx Spectrum Technology, Inc.
- OpenText
- Raytheon Technologies
- Santa Clara University
- Schneider Electric
- Siemens
- Stryker
- Synopsys Inc.
- Telecommunications Industry Association (TIA)
- Tenchi Security
- The Chertoff Group
- The Open Group
- Sesate
- Thomson Reuters Special Services, LLC
- TXOne Networks Inc.
- U.S. Air Force Sustainment Center Software Directorate (AFSC/SW)
- U.S. DHS CISA National Risk Management Center (NRMCC)
- V2X
- Verisign
- Wibu-Systems
- Xylem



CAPiTiS SOLUTIONS INC.

VERISIGN™

LINEAJE

The Chertoff Group

InterSec
Ignite. Inspire. Innovate.

Santa Clara University

WIBU SYSTEMS

Bloomenergy™

DARK SKY TECHNOLOGY

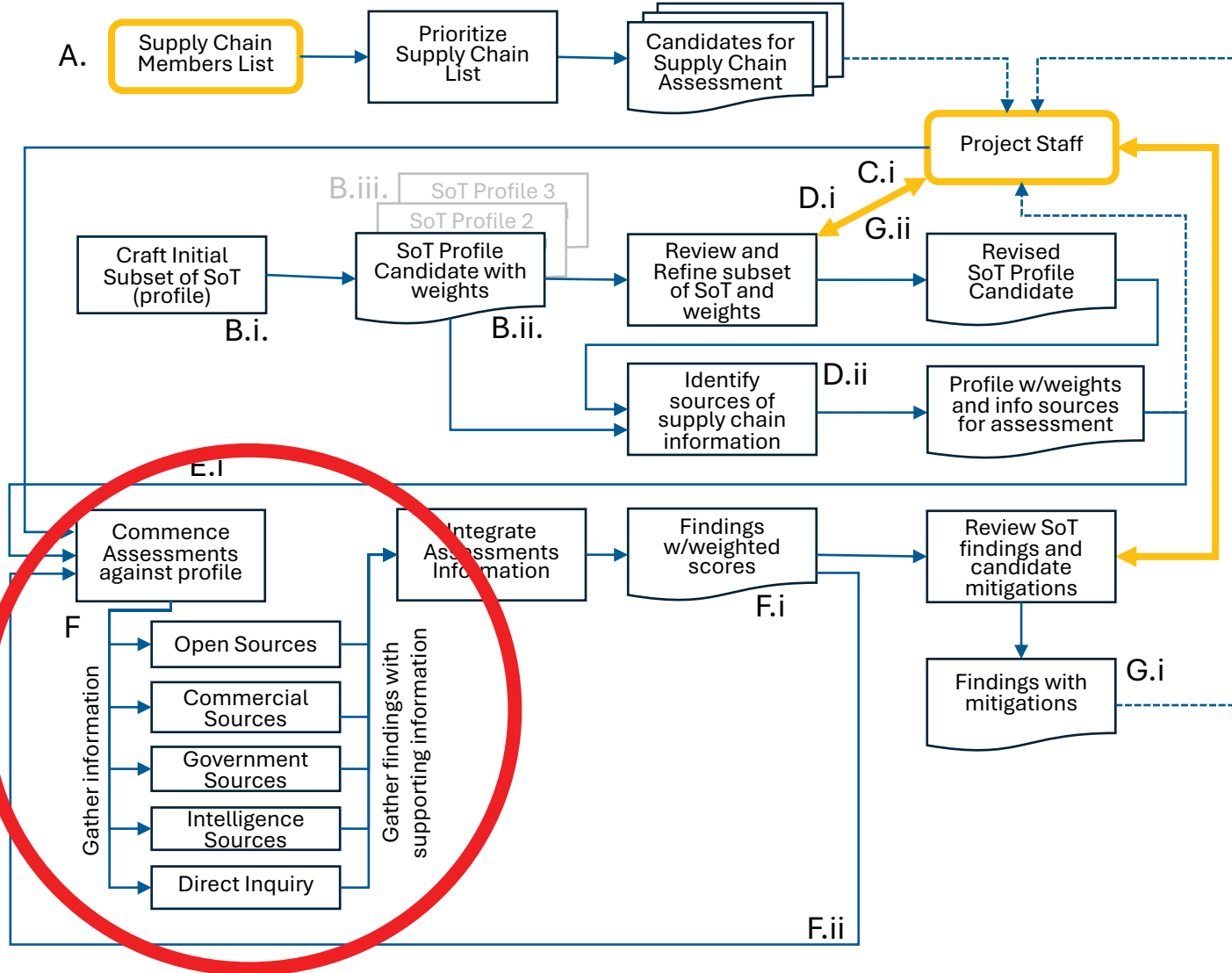
AF SUSTAINMENT CENTER
Software Directorate

txOne networks

CyVidia

CREST

Supply Chain Assessment Tasks



- A. Review supply chain(s) – Identify those to be assessed**
- B. Define initial scope of risks – based on areas of concern**
 - i. Review SoT's 600+ measurable risks factors and their 1300+ risk measures to determine the sub-set (profile) of risk factors/risk measures appropriate
 - ii. First cut – focused on supplier risks – identified ~100 RFs with 32 needing detailed risk measure crafting
 - iii. Can add additional profiles for product risks and for service risks
- C. Share resultant profile with stakeholders to validate the scope of risks**
 - i. Walk through with project personnel to trim or extend the profile details
- D. Prepare profile for assessment**
 - i. Review and assign profile specific weights with project personnel
 - ii. Identify potential information sources/methods for evaluating the risks
 - a. Public Sources (government, open source, company web site/publications, press, twitter, ect.)
 - b. Non-Public Sources (government, commercial, intelligence, law enforcement, classified sources, direct inquiry, testing of products)
- E. Finalize profile, sources, and whether to tier the evaluation**
 - i. Tiering: collect autonomously initially; collect from organization of interest next
- F. Evaluate risks where data is available for an initial set of suppliers**
 - i. Recognize un-evaluated risks due to lack of data as residual risks
 - ii. Expand to next tier of supply chains incrementally
- G. Review results incrementally**
 - i. Plan actions to mitigate evaluated and residual risks
 - ii. Refine profile(s) and process as appropriate

Current State of Supply Chain Visibility

- Details of supply flows are unavailable to the government and industry due to proprietary concerns.

"Limited supply chain visibility remains a challenge, meaning that companies still lack sufficient insight into the materials, components, goods and processes across their networks. Many have been investing in technologies to enhance real-time tracking, but more work is needed."

Page 27, para 1, 2021–2024 Quadrennial Supply Chain Review,
National Economic Council & National Security Council, December 2024.

- Open question – Can we leverage government and commercial efforts to gather trustworthy data on sustainability and forced labor provide a source of detailed anonymized trustable industry data on the flow of materials and finished goods?

Market forces motivating new supply chain data

- **Ecodesign for Sustainable Products Regulation (ESPR):**

- Focus on sustainability across product lifecycles.
- DPP data includes product identity, composition, provenance, and claims.
- Enforcement through EU Member States and customs authorities.

- **United Nations Transparency Protocol (UNTP):**

- Voluntary protocol for supply chain transparency.
- Decentralized, interoperable, and ESG-focused.
- Uses technologies like decentralized identifiers and verifiable credentials.

- **Uyghur Forced Labor Prevention Act (UFPLA):**

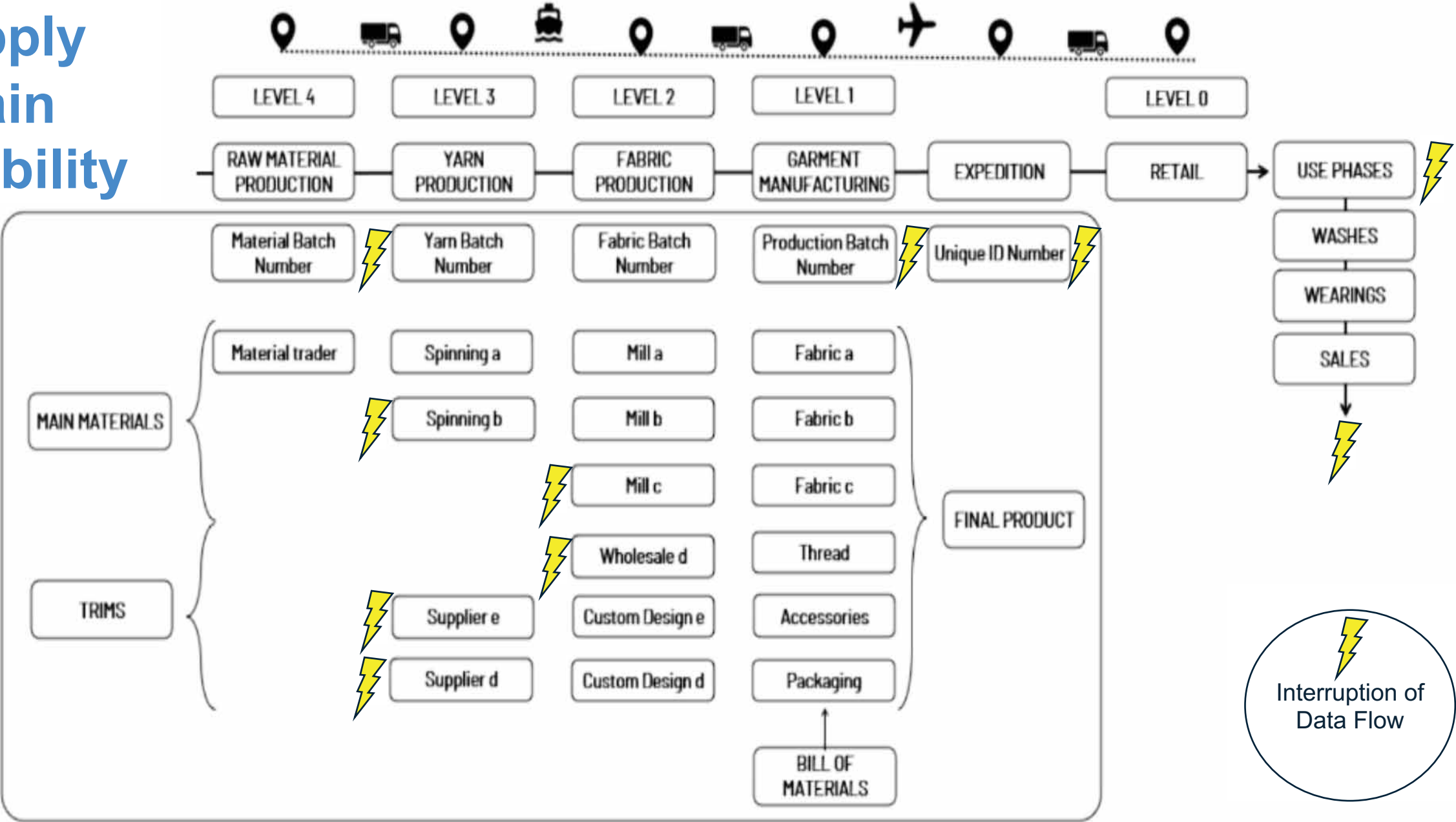
- Mandatory law with a rebuttable presumption against goods linked to Xinjiang
- Requires end-to-end traceability evidence to rebut.
- Enforced via detentions, exclusions, and seizures; guided by the UFLPA Entity List.

- **Bill of Materials (BOMs):**

- Structured product composition list detailing parts, materials, quantities, and assemblies.
- Provides composition, not provenance; must be linkable to supplier, lot/serial, and process data to support traceability and compliance claims.
- Used to feed mandatory reporting and documentation with component-level detail.

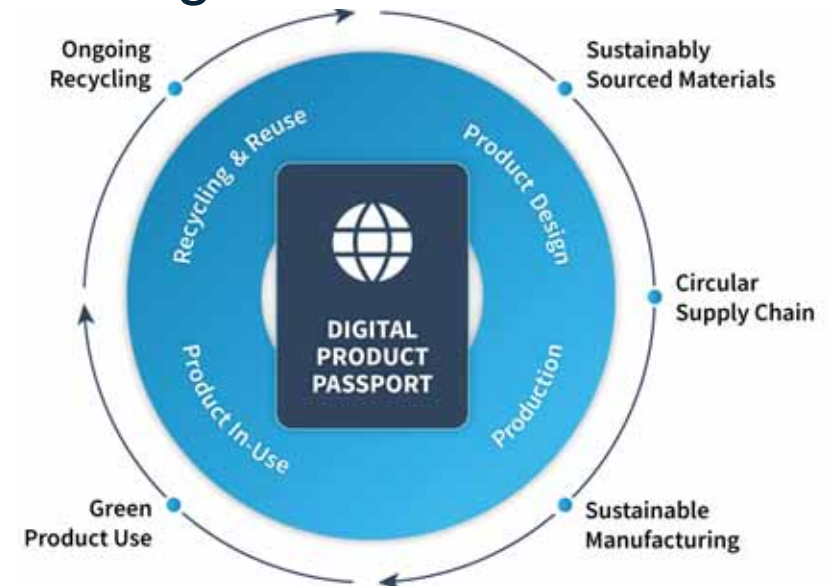


Supply Chain Visibility



What is a Digital Product Passport?

- The DPP is a powerful tool in the EU's push for sustainable, circular products, and it's now enshrined in law under two key pieces of legislation:
 - The [Ecodesign for Sustainable Products Regulation \(ESPR\)](#): *Regulation (EU) 2024/1781*, which sets the general framework for DPPs across the EU economy
 - The [Construction Products Regulation \(CPR\)](#): *Regulation (EU) 2024/1305*, which tailors sustainability and DPP requirements specifically for the construction sector
- The DPP is set to **redefine how product data is shared, verified, and used across Europe**. As part of the broader Circular Economy Action Plan under the European Green Deal, the DPP aims to enhance product sustainability by embedding transparency into the heart of product value chains.



END OF LIFE

COLLECTING/SORTING

REFERENCE	IDENTIFICATION TYPE	INPUT
TYPE OF PROCESSES	OUTPUT	COMPANY (COLLECTING)
LOCATION	DATE	

RECYCLING

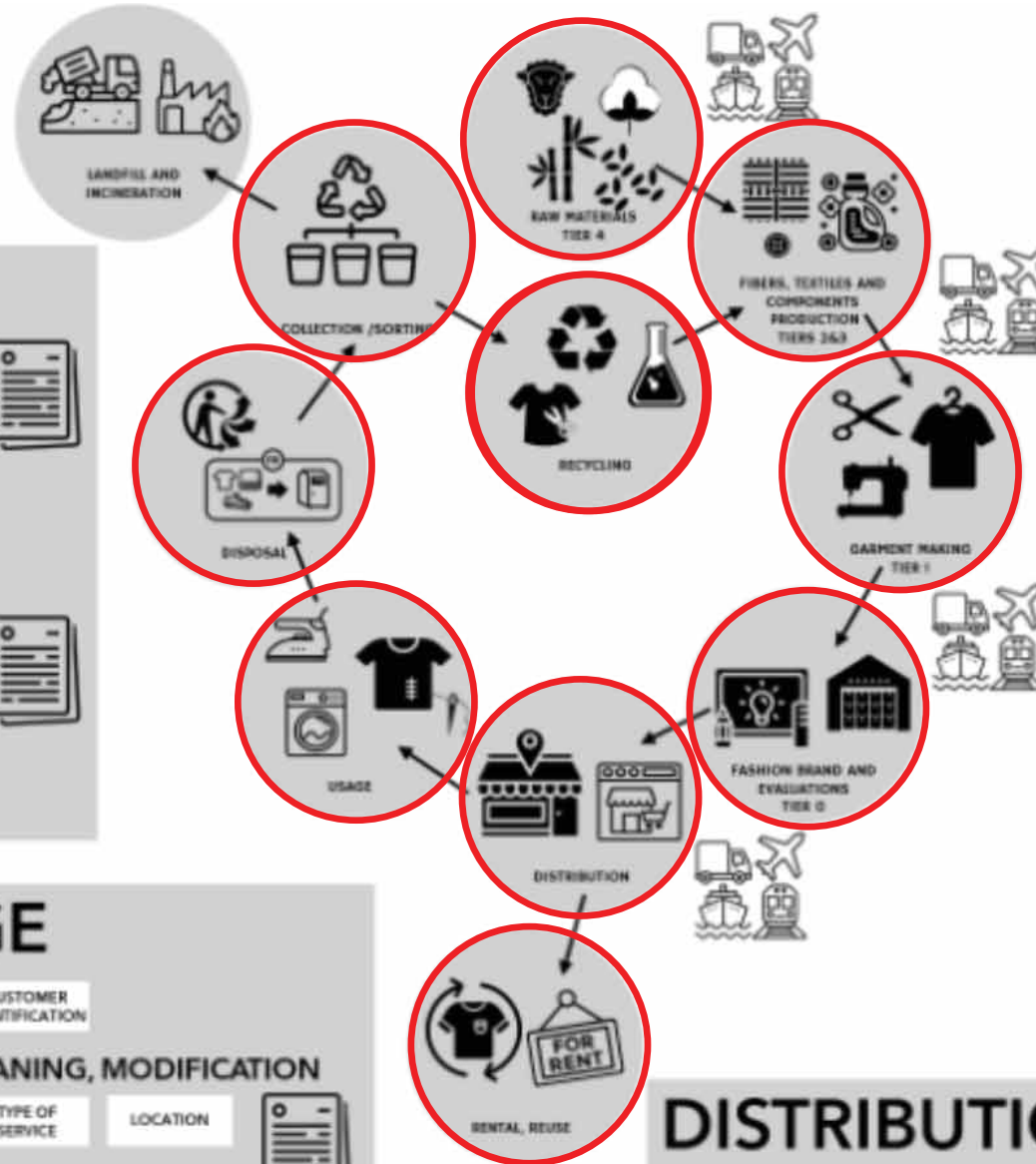
TYPE OF PROCESSES	COMPANY (RECYCLING)	LOCATION
RECYCLING STRATEGY	COMPOSITION	DATE

USAGE

USAGE TYPE	CUSTOMER IDENTIFICATION
------------	-------------------------

REPAIR, CLEANING, MODIFICATION

COMPANY (AFTERSALES)	TYPE OF SERVICE	LOCATION
DATE		



DISTRIBUTION

COMPANY (DISTRIBUTORS)	LOCATION	PURCHASE DATES
IN SHOP	ON LINE	SECOND HAND

SUPPLY CHAIN

PRODUCTION

REFERENCE	TRACEABLE ASSET	IDENTIFICATION TYPE
TYPE OF PROCESSES	COMPANY (TIER)	LOCATION
WEIGHT QUANTITY	COMPOSITION MATERIALS	DATE

TRANSPORTS

COMPANY	MEANS	DISTANCE
DATE		

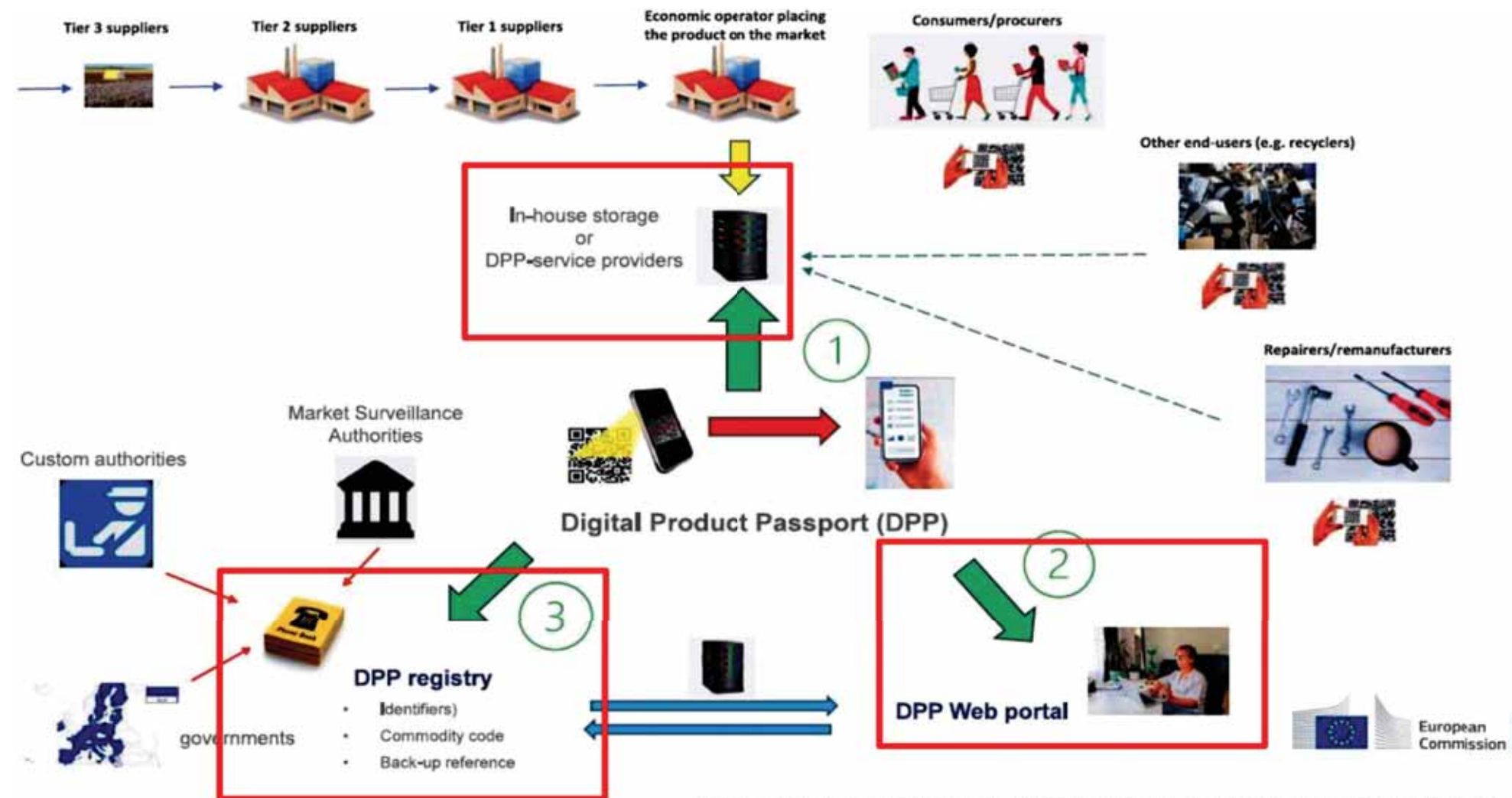
FINISHED PRODUCT

REFERENCE	IDENTIFICATION TYPE/ AUTHENTICATION	DESCRIPTION
COLOUR	COMPOSITION	SIZE
COSTS	PACKAGING	WEIGHT
CIRCULARITY STRATEGY	COMPANY (BRAND)	DATE
QUANTITY	PERFORMANCE	

EVALUATIONS

QUALITY TEST	ENVIRONMENTAL IMPACT	SOCIAL IMPACT
HEALTH IMPACT	ANIMAL IMPACT	CERTIFICATION
AUDITS	COMPANY (EVALUATION)	DATE

ESPR DPP in Governance, Consumption, and Production



Source: Michele Galatola/DG-GROW at BDI-Workshop DPP, Berlin, April 16, 2024

Where Did Digital Product Passports Come From? <https://dpp40.eu/>

"Digital Product Passport for Industry 4.0 builds on the Asset Administration Shell (IEC 63278) and the identification link (IEC 61406), which are already widely used in industry."

IDENTIFICATION LINK

1 Scope

This part of IEC 61406 specifies minimum requirements for a globally unique identifier for physical objects which also constitutes a link to its related digital information. This identifier is designated hereinafter as "Identification Link" (IL), with the encoded data designating the object. The IL string has the data-format of a link (URL). The IL is machine-readable and attached to the physical object in a 2D symbol or NFC tag.

The requirements in this document apply to physical objects

- that are provided by the manufacturer as an individual unit,
- and that have already been given a unique identity by the manufacturer.

This document does not specify any requirements on the content and the layout of nameplates/typeplates (e.g. spatial arrangement, content of the plain texts, approval symbols etc.).

ASSET ADMINISTRATION SHELL FOR INDUSTRIAL APPLICATIONS –

Asset Administration Shell structure

1 Scope

This part of IEC 63278 defines the structure and the content of the Asset Administration Shell (AAS) to information and services.

The purpose of the Asset Administration Shell is to enable the exchange of information and to mutualize resources in a secure way.

This document focuses on Asset Administration Shells for products and equipment. It defines the related structure and content.

The Asset Administration Shell applies to

- any type of industrial process (including hybrid production);
- any industrial sector applying industrial processes;
- the entire life cycle of assets from design to disposal;
- assets which are physical, digital or hybrid.

IEC 63278-1:2023 © IEC 2023

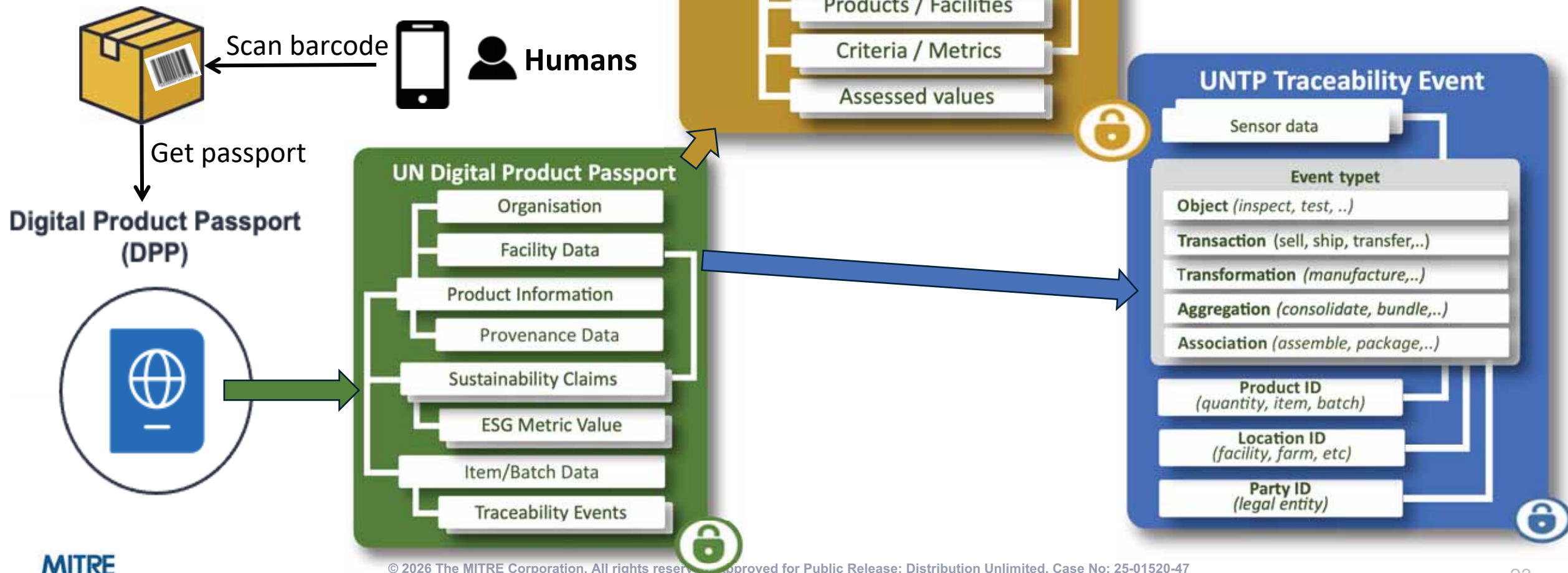
– 9 –

0.4 Key objectives of the Asset Administration Shell

The following statements summarize these discussions and formulate some aims for the Asset Administration Shell, helping to keep the focus:

- Asset Administration Shell aims at establishing cross-company interoperability. Assets within manufacturing are provided by many different enterprises. In order to fulfil the scenarios of today and tomorrow, information and services on assets should be interoperable.
- Asset Administration Shell is intended for non-intelligent and intelligent products. The concept of asset comprises many different entities, with or without the ability to communicate actively or being intelligent. To leverage benefits in engineering, maintenance or operation throughout all hierarchy levels, the idea of the Asset Administration Shell is suitable to be applied by all assets.
- Asset Administration Shell aims at covering the complete life cycle of products, devices, machines and facilities. Much useful information on assets is formed in the early phase of their life cycle, such as design, engineering and marketing. To maintain economic efficiency, digitized information from these early phases should be preserved and used in later phases, such as engineering higher level structures and operating and maintaining these structures.
- Asset Administration Shell aims at enabling integrated value chains. Assets for manufacturing lines and products are provided by many different value chain partners. To maintain economic efficiency, digitized information should be exchanged among value chain partners. This will also enable advanced production modes (see 0.1).
- Asset Administration Shell is intended to be a base for autonomous systems and artificial intelligence. In the future, many benefits are expected from approaches such as autonomous systems and artificial intelligence. These approaches require a sound basis of information and identifiers of elements. The Asset Administration Shell provides both.

UNTP includes the mechanisms for conformity credentials and traceability events



SBOM Regulatory Market Forces

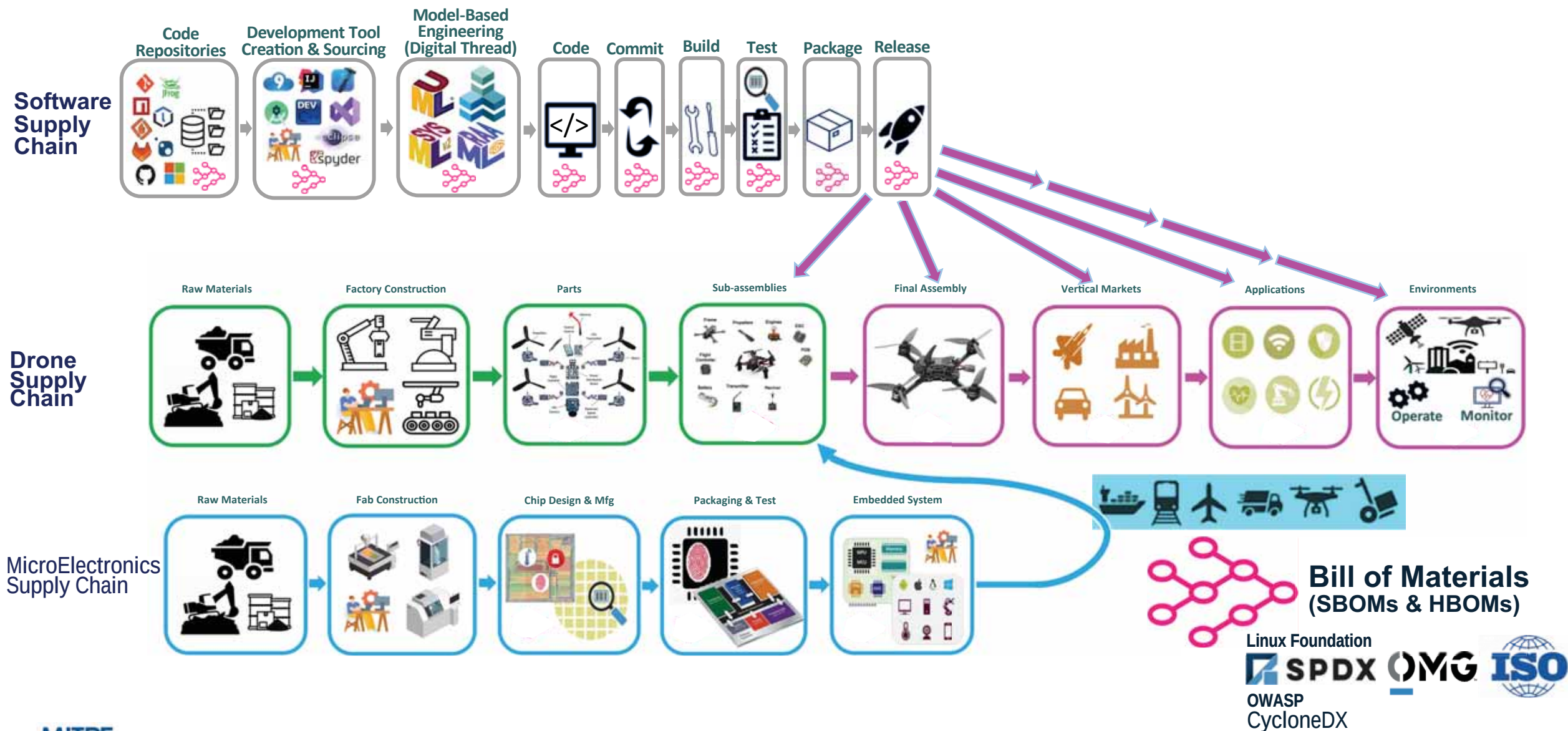
- **Motivating U.S. regulations**

- EO 14028, NIST SSDF, & memos (NSM, OSD, DoD CIO & OMB)
- FDA requires SBOMs for medical devices at the premarket stage, including lifecycle and vulnerability data,
- U.S. Army Directive mandates SBOMs for most software contracts starting in February 2025.
- PCI DSS v4.0 introduced controls that will require organizations to maintain living, searchable SBOMs by 2025.

- **Motivating global regulations**

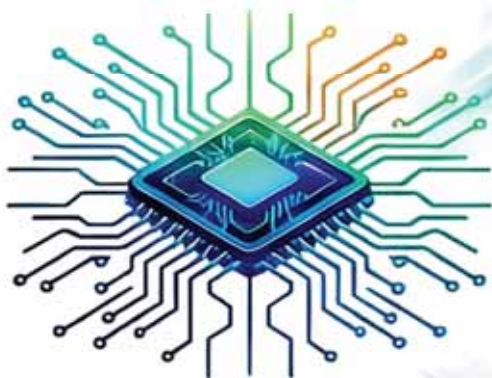
- EU Cyber Resilience Act (CRA) and Germany's BSI TR 03183 are setting SBOM requirements for digitally connected products
- Japan, the UK, and Australia are also advancing SBOM initiatives or offering strong guidance for adoption

Software, MicroElectronics & Drone Supply Chains



What's New in SPDX 3.1

New Profiles for Broader Coverage



Hardware Profile Introduced

Now describes both physical and virtual hardware components within the supply chain.



Supply Chain Lifecycle Tracking

Now documents the full product lifecycle and interlink design with risk management.



Curated Cryptography List

Includes a new list of over 130 curated cryptographic algorithms.



Advanced AI Use Case Support

Manages Agentic AI, including Prompts and Retrieval-Augmented Generation (RAG) context.

Enhanced Profiles for AI & Security



Improved Relationship Types

New types describe prompt chaining and the specific tools used in a process.



Demonstrates Regulatory Readiness

Helps organizations meet compliance standards like CRA and ISO 42001.

The SPDX Metamorphosis: From Static SBOM to Live Knowledge Graph

THE PAST: The File-Based SBOM

A Static Snapshot



Limited Scope: Primarily a list of software components.

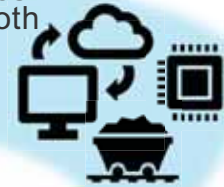
Point-in-Time: Captures a single state, like a build or release.

Simple Connections: Describes basic "contains" or "depends on" relationships.

THE FUTURE: The Live Knowledge Graph

A Dynamic System Model

Hardware Profiles: Now describes both physical and virtual hardware components.



Supply Chain Lifecycle Tracking: Documents the full product lifecycle for harvesting, making, transporting, and storing goods, and linking design to risk management.



Improved Relationship Types: Introduces new relationship types like "usesTool" and "follows" to describe complex processes like prompt chaining.



New AI Component Definitions: Defines crucial elements like AI Agents, Prompts, and Retrieval Augmented Generation (RAG).



Regulatory Readiness: Helps align with emerging standards like the EU Cyber Resilience Act (CRA) and ISO 42001.



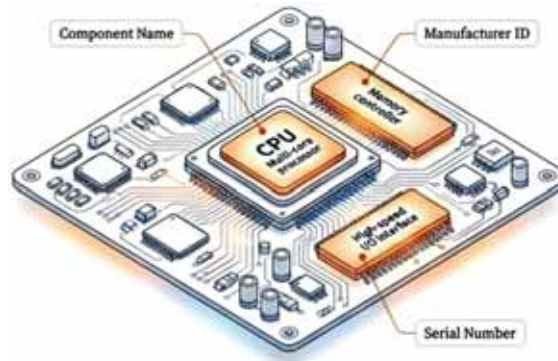
System-Wide Context: Models software, hardware, AI, and data.

Supply Chain Lifecycle: Tracks components and their interactions over time.

Rich Relationships: Defines the "how" and "why" of system interactions.

Hardware

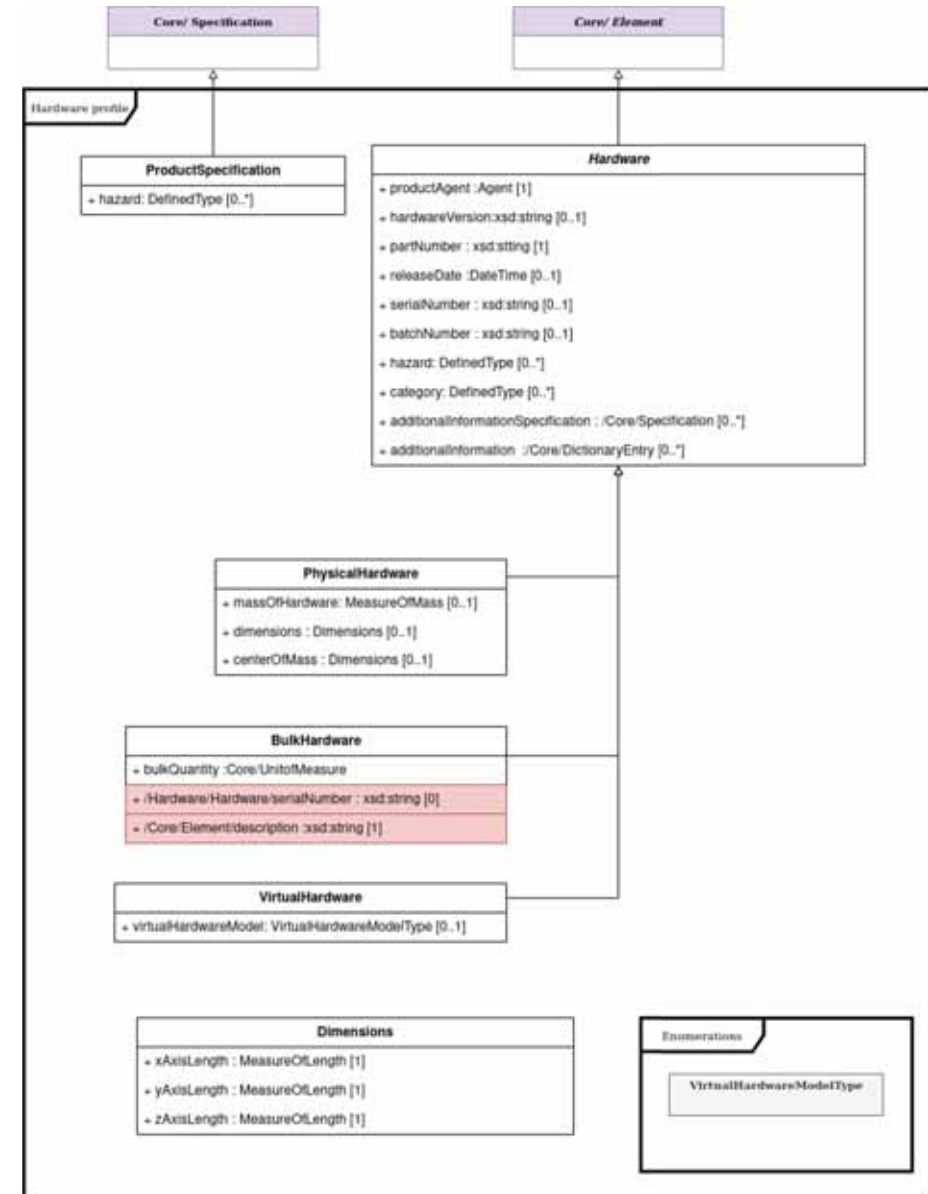
- Physical
- **Virtual**
- Bulk



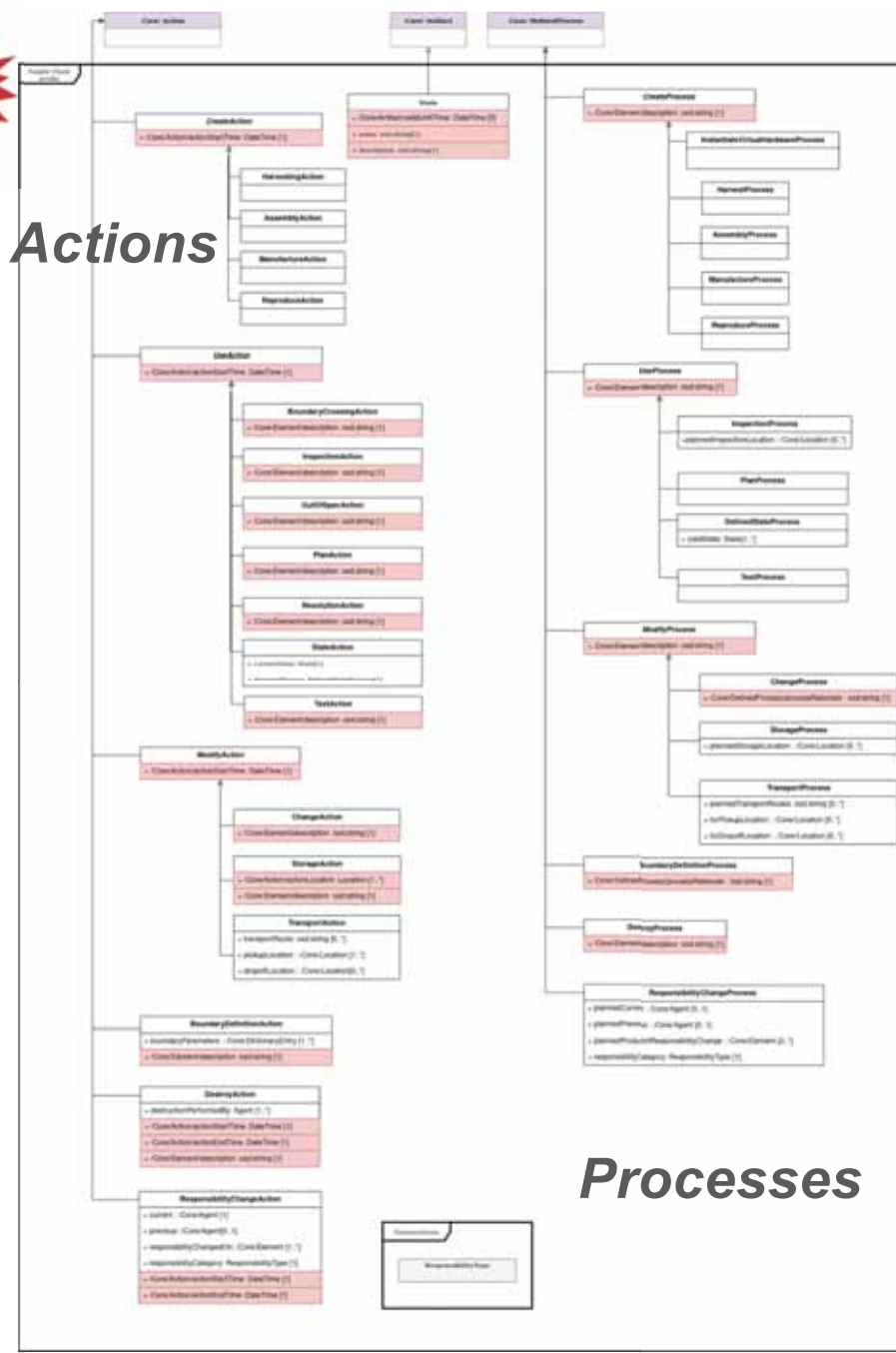
Hardware Description

The Hardware namespace defines metadata related to physical and virtual hardware properties. Hardware is any product, real or virtual. A product is tangible and is the result of labor, or of a natural or artificial process.

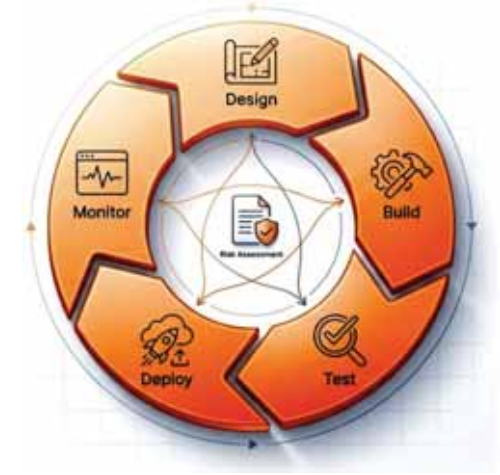
<https://github.com/spdx/spdx-3-model/blob/develop/images/model-Hardware.png>



Actions



Processes



Responsibility

- Owner
- Custody

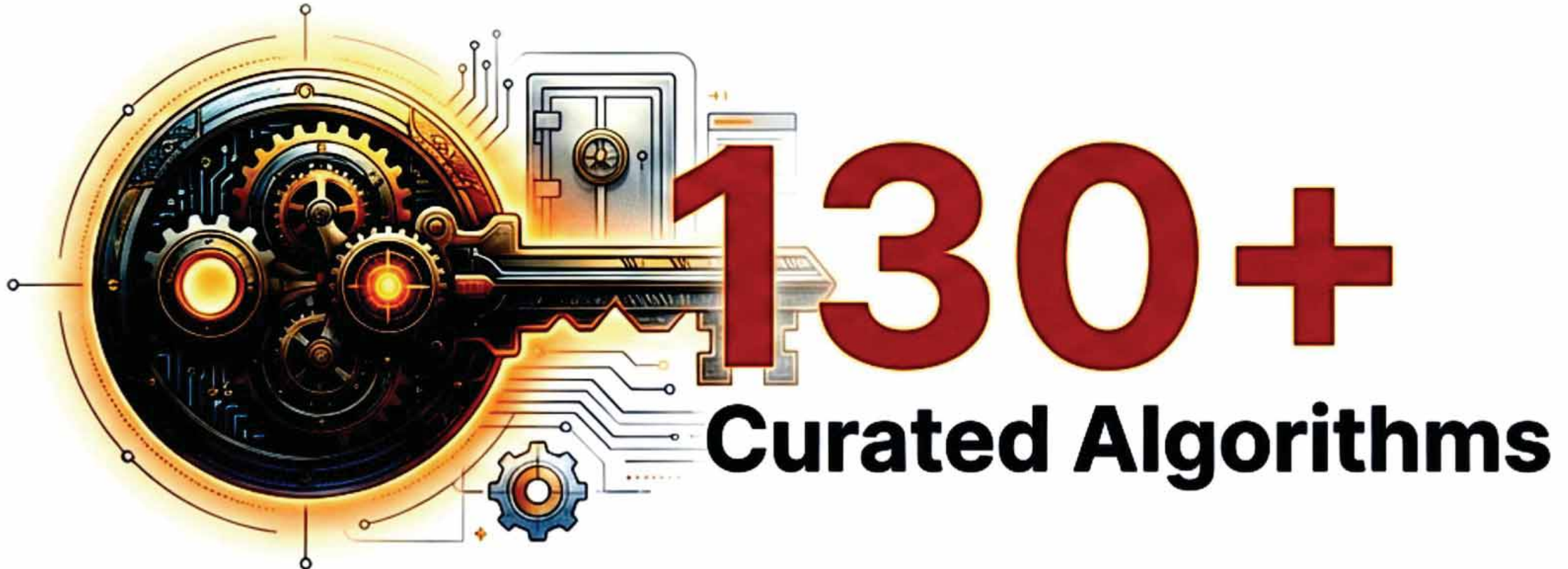
Use:

- Inspection
- Plan
- Resolution
- Boundary
- Out of Spec

The Supply Chain profile documents events and processes associated with the lifecycle of a product, including its creation, transportation, usage, and decommissioning.

<https://github.com/spdx/spdx-3-model/blob/develop/images/model-SupplyChain.png>

SPDX 3.1 includes a new, vetted list of cryptographic algorithms to standardize how security mechanisms are documented in the same way it offers the SPDX License List.



This provides an unambiguous way to declare the specific cryptographic tools used in a component, aiding in security audits, export licensing, and compliance checks.

SPDX 3.1 extends the standard SBOM to include crucial components of modern AI systems, providing a structured way to document AI agents, prompts, and RAG setups for enhanced transparency.



AI Prompt

Defined as a type of "Software Artifact", allowing it to be documented with key metadata.

Key Attributes:

modality

isContextAugmented

inLanguage



AI Agent

Represents an autonomous entity that can perform tasks, with its capabilities clearly defined.

Key Attributes:

autonomyType

collaborationMechanism

framework



RAG (Retrieval-Augmented Generation)

Provides a standard way to describe the components of a RAG system.

Key Attributes:

dataSourcePackage

embeddingModel

retrieveMethod

EU CRA Manufacturer Guidance



Work in progress:

[SPDX-examples/conformance](https://github.com/spdx/spdx-examples/tree/master/conformance)

<https://github.com/spdx/spdx-examples/tree/master/conformance>

(SEBoK for Consumer Electronics)
includes Stakeholder Needs and
Stakeholder Requirements)

EU CRA Regulatory Knowledge Graph

Work in progress: Mapping of SPDX fields to CRA clauses/appendix are captured in a spreadsheet

<https://docs.google.com/spreadsheets/d/10KdQTkXH3K-kp1zD7wIhuSUc91U8ttm7gVZ0BEVC004/edit?gid=0#gid=0%20%20%09https://owasp.org/www-project-application-security-verification-standard>



Source: <https://openssf.org/blog/2025/10/22/sboms-in-the-era-of-the-cra-toward-a-unified-and-actionable-framework/>

SPDX Tools: Example 1 – SPDX Knowledge Graph Explorer



From Hugging Face to GitHub: Tracing License Drift in the Open-Source AI Ecosystem

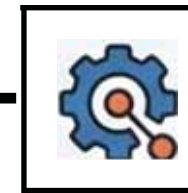
James Jewitt, Hao Li, Bram Adams, Gopi Krishnan Rajbahadur, Ahmed E. Hassan

School of Computing, Queen's University, Kingston, ON, Canada
{james.jewitt, hao.li, bram.adams}@queensu.ca, grajbahadur@acm.org, ahmed@cs.queensu.ca

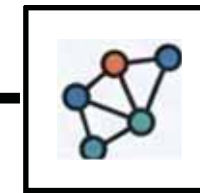
Source: <https://arxiv.org/pdf/2509.09873>



Whitepaper/Doc/Code



SPDX Knowledge
Graph Tool



Graph Output

IMPLEMENTING AI BILL OF MATERIALS (AI BOM) WITH SPDX 3.0

More than **60% of models**
& **70% of datasets** on
platforms like Hugging Face
are undocumented
[Oreamuno et al., 2023],
rendering **effective**
auditing of these assets
impossible.



SPDX Knowledge Graph Explorer

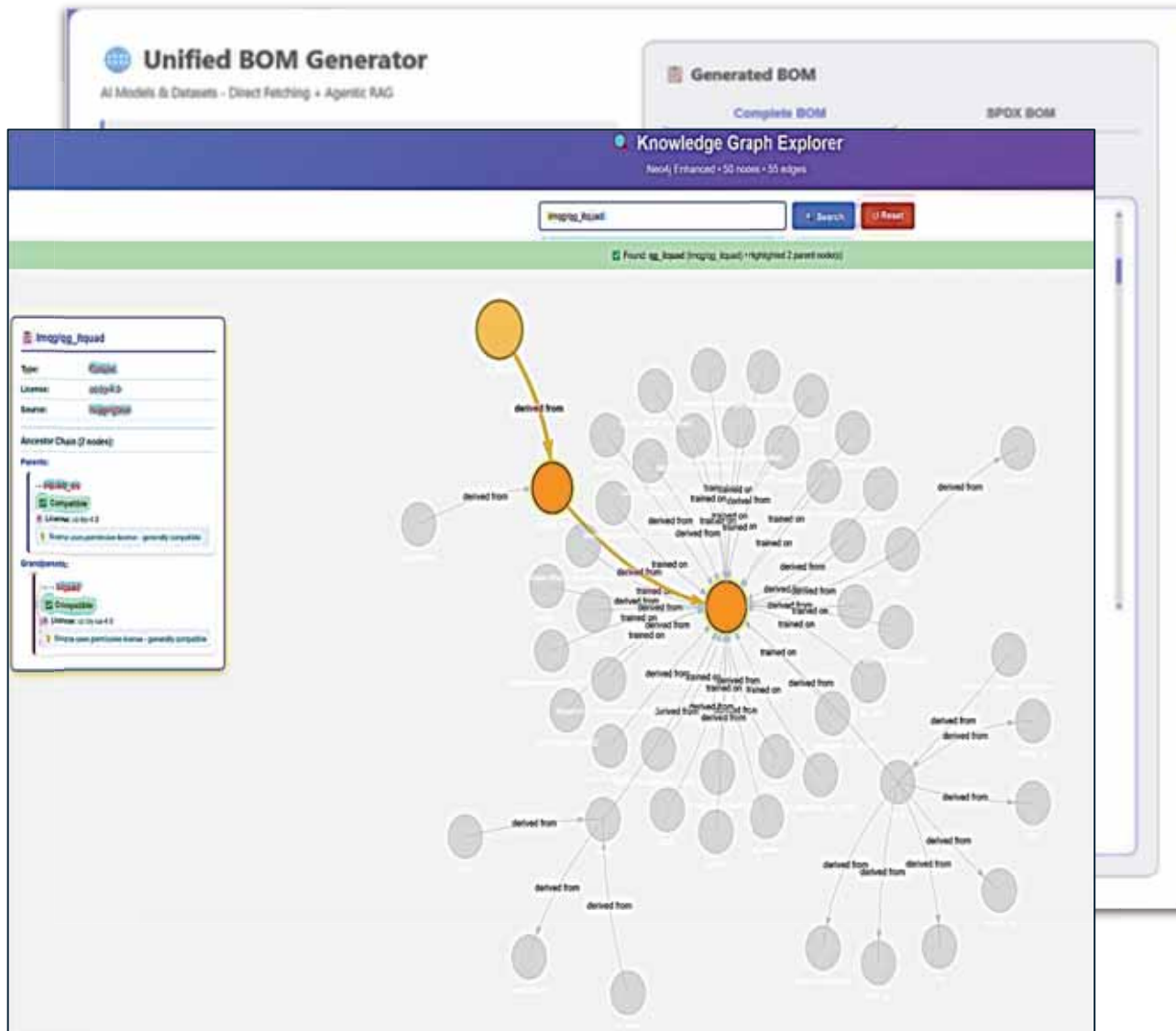


Information Rich Knowledge Graph from multiple sources (source, user guides, hugging face, github, etc).

Generates AI and Dataset BOM that be integrated into Supply Chain Graph

Conflict Resolution / Confidence Checker - checks metadata across multiple sources, identifies conflicts like licensing

Demo version available upon request



SPDX Tools: Example 2 – The KernelSbom tool



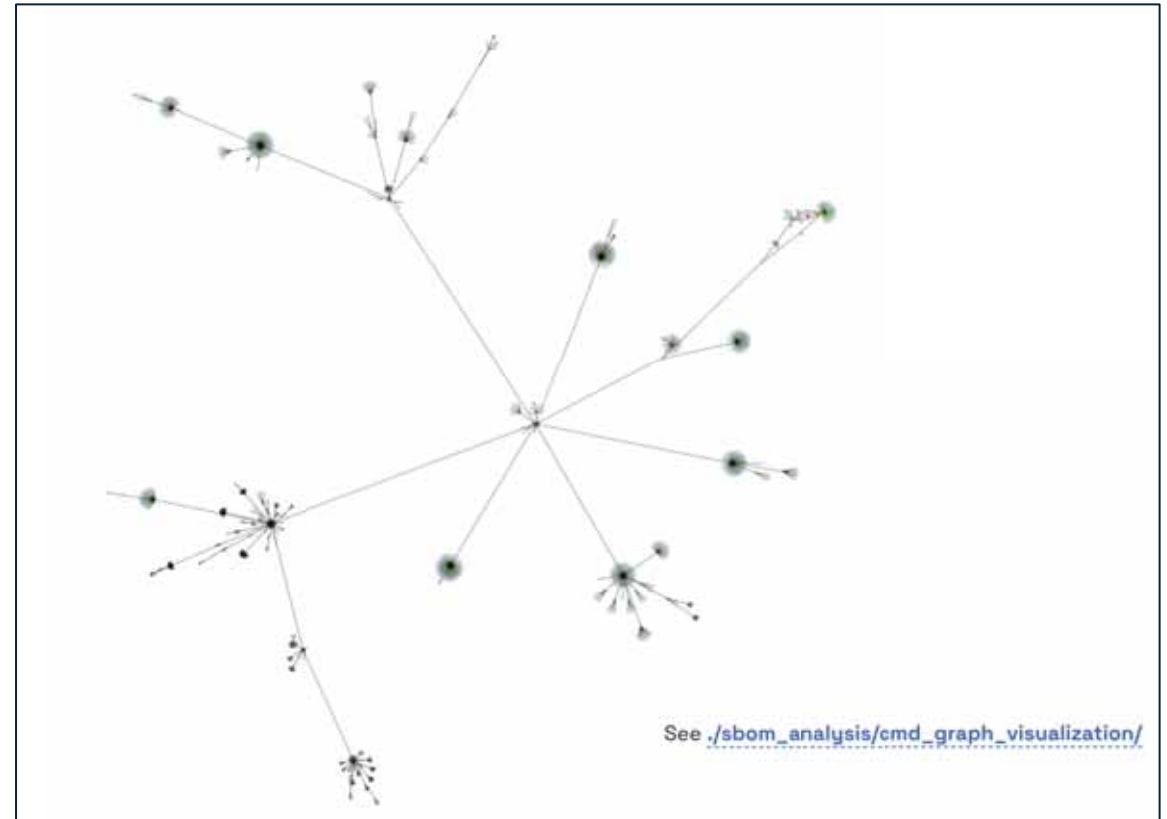
- A tool that analyzes a kernel build and produces SBOM documents in SPDX 3.0
 - <https://github.com/TNG/KernelSbom> (The name and home might change)

Example Call:

```
$ export SRCARCH=x86
$ python3 sbom/sbom.py \
- src-tree path/to/Linux \
-obj-tree path/to/kernel_build \
xroots arch/x86/boot/bzImage \
generate-spdx
```

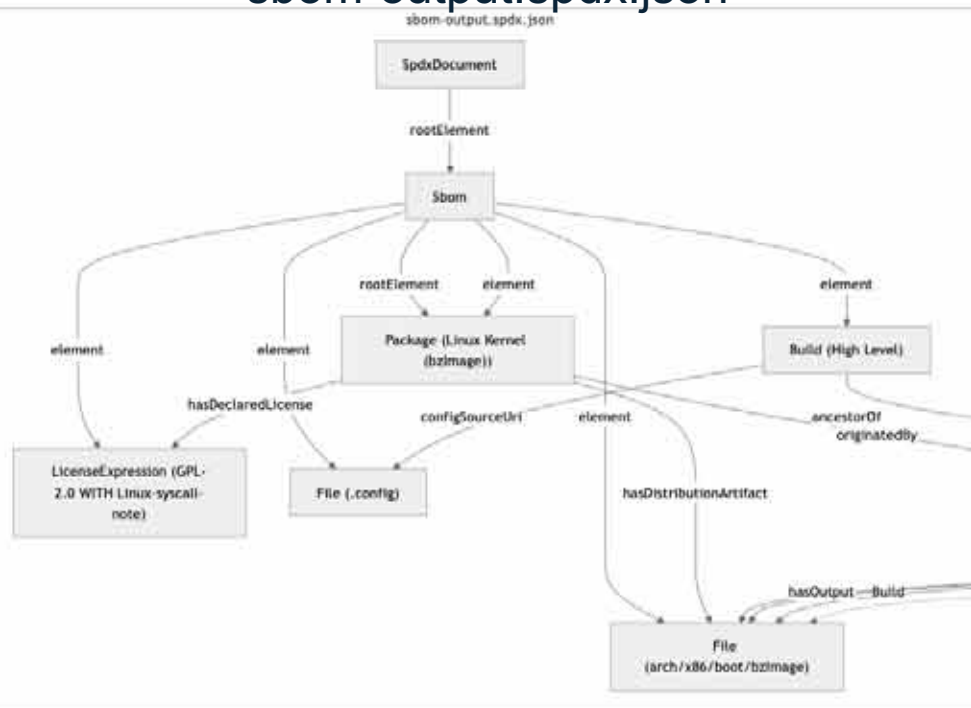
After merge:

```
$ make sbom
```

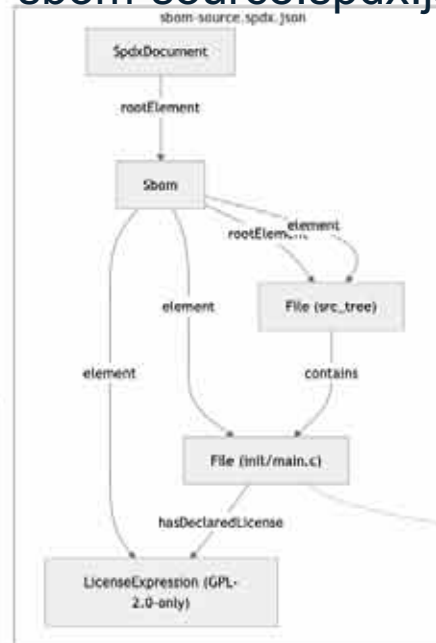


The KernelSbom tool: structures for sbom- output, sbom-source, and sbom-build

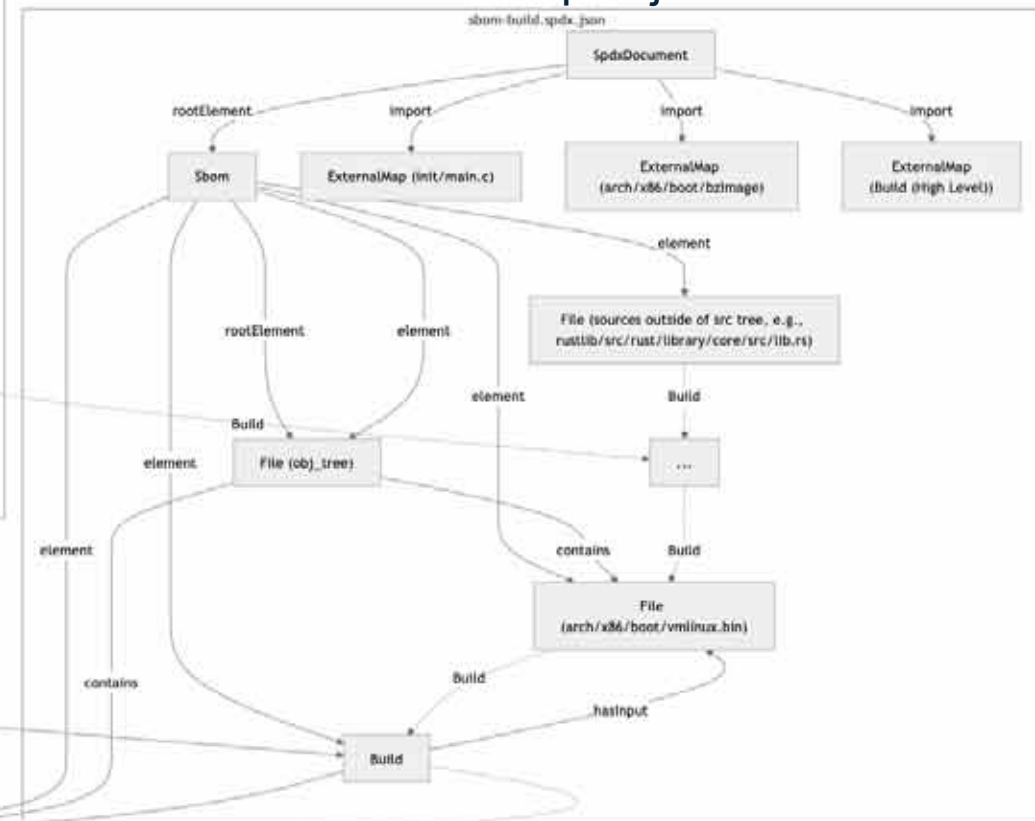
sbom-output.spdx.json



sbom-source.spdx.json



sbom-build.spdx.json



FOSDEM talk about the tool: https://fosdem.org/2026/schedule/event/938CKB-how_to_create_the_sbom_for_the_linux_kernel/

SPDX Tools: Example 3 – Zephyr Project

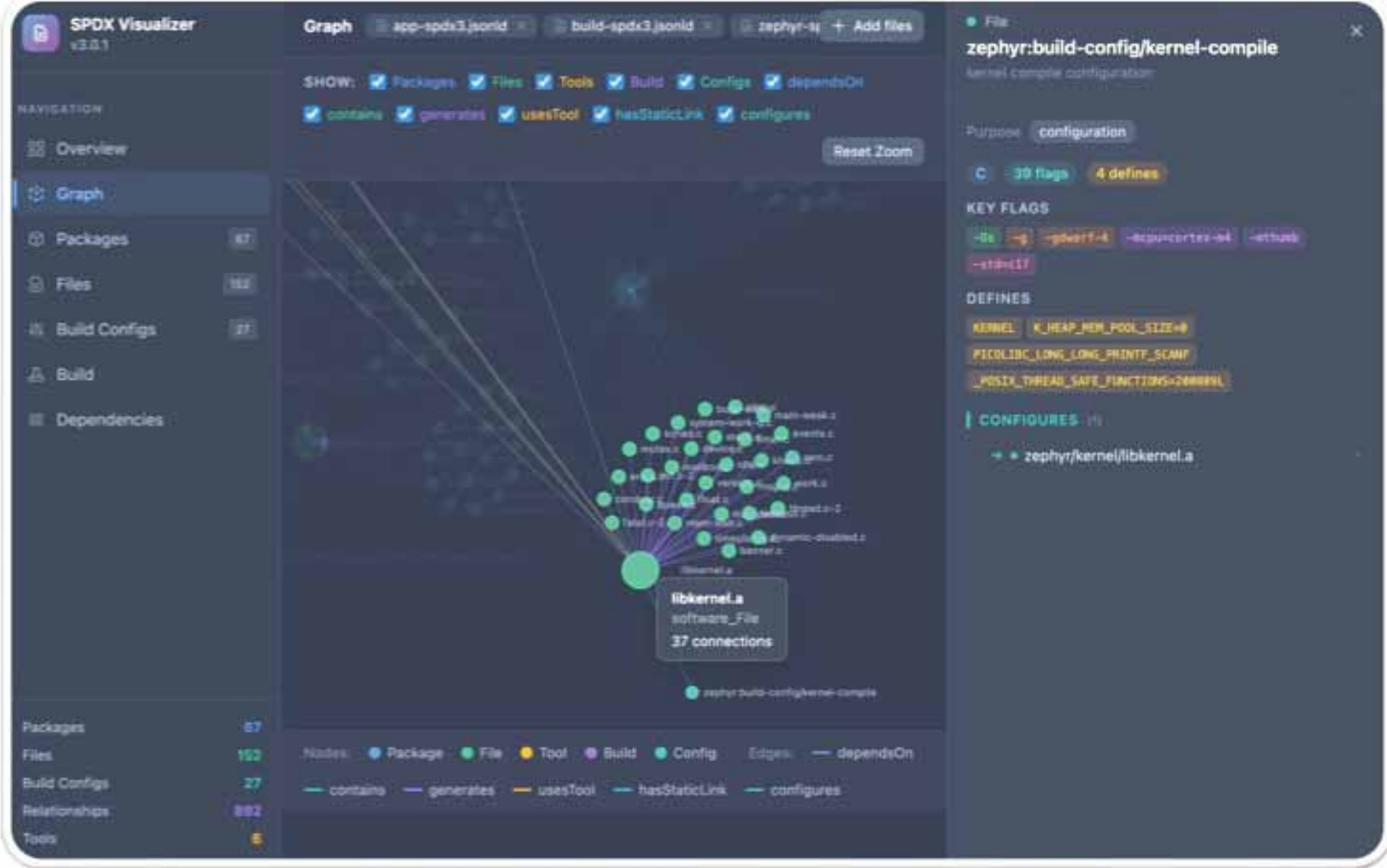


- ×SPDX 3.0 profiles (Software, Security, Licensing, Build, AI/ML, ...) are very relevant for embedded
- ×Much easier to bake more "Zephyr-specific" intelligence without being constrained by document-oriented serialization
- ×Graph-oriented (JSON-LD)
- Richer semantics
- ×e.g. LifecycleScopedRelationship detailed information regarding the compilation process



A widely deployed, industrial-grade, real-time operating system

SPDX Visualizer



BLACK DUCK

Products & Services

Solutions

Resources

Company

Contact sales

Table of Contents

Why AI models matter

Black Duck's AI model scanning

The Black Duck difference

Why it matters to you

Subscribe to the blog newsletter

Required Fields *

* Email Address:

* Country:

Select...

Get Newsletter

Get answers from the Community

Join discussions →

Why AI models matter

AI models are transforming how we build software, from autogenerating code to powering intelligent features. But they're also a new frontier of risk. Hidden in your apps, these models can carry licensing issues, murky origins, or modifications that don't align with your security policies. Without visibility, you can't navigate regulations like the [EU AI Act](#) and the stakeholders demanding accountability. That's not just a compliance headache—it's a business risk.

Black Duck's answer: AI model scanning

October 2025

AI model scanning, which rolled out in October 2025, is built to tackle these challenges head-on. Here's the rundown.

- **Spot models anywhere:** Our signature-based scanning detects AI/ML models even if they're deliberately obscured or not listed in your build manifest. No more guessing what's in your codebase.
- **License clarity:** Black Duck SCA identifies model licenses to keep you compliant, whether it's open source or commercial, saving you from costly legal surprises.
- **Deep insights made simple:** A dedicated UI screen serves up model-specific metadata showing what the model is good at (e.g., code completion) and details on datasets. This helps teams build usage policies like "no retrained foundational models" with ease.
- **Seamless integration:** AI model scanning plugs right into your existing Black Duck workflows, leveraging our [SBOM](#) engine for a unified SCA experience.
- **Supply chain transparency:** Any model identified or manually added to a project can be included in an SBOM to satisfy customer and industry requirements.

This is our MVP, focused on identification and licensing, but it's built to scale. Future updates will bring deeper insights into security and operational risks introduced by models, and more customized policy configuration.

<https://www.blackduck.com/blog/black-duck-ai-model-scanning.html#1>

MITRE

© 2026 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 25-01520-47

Black Duck AI model scanning

documentation.blackduck.com/bundle/bd-hub/page/ReleaseNotes/2025.10.x/newAndChangedFeatures_2025_10_0

ed features

<

AI Model Support in Bill of Materials

Black Duck now supports the addition of AI models to your Bill of Materials (BOM) as part of the Black Duck Supply Chain Edition, enabling comprehensive tracking and management of artificial intelligence components within your projects. This new feature allows organizations to maintain visibility into their AI model usage alongside traditional software components.

Key capabilities include:

- Manual addition and editing of AI models to your BOM with detailed metadata
- Filtering and search options to quickly identify AI models within large BOMs

Note: This feature is currently available only for hosted customers, as it requires signature scans to be processed through the SCA Scan Service (SCASS).

To use this feature, ensure your product registration has the AI Model Scanning feature enabled and run Detect scans with the parameter `--detect.blackduck.signature.scanner.individual.file.matching=ALL`.

This enhancement helps organizations address the growing need to track AI components as part of their software supply chain management and compliance processes.

Binary scanner information

https://documentation.blackduck.com/bundle/bd-hub/page/ReleaseNotes/2025.10.x/newAndChangedFeatures_2025_10_0.html

39

Other Tools to Analyze AI systems and produce BOMs

Open source:

- OWASP aibom-generator (CycloneDX, SPDX 3.0 support in development)

<https://github.com/GenAI-Security-Project/aibom-generator>

- AlkaBoOM (beta) aibom generation (SPDX 3.0 & CycloneDX)

<https://github.com/rgopikrishnan91/aibom>

https://github.com/rgopikrishnan91/aikaboom/blob/main/docs/PIPELINE_WALKTHROUGH.md



- PITLOOM (beta) sbom/aibom generation (SPDX 3.0)

<https://github.com/bact/pitloom>



PITLOOM

Commercial

- Black Duck - produces an SPDX file with AI data from the model or from the development environment for AI code creation.

Other SPDX 3.0 Analysis and Production Capabilities ^(1of2)



BASIL – The Functional Safety (FuSa) Spice BASIL is a tool designed to support companies working on safety-critical applications, where establishing traceability between software requirements, test specifications, test cases, software design, source code, and test results and exports a SBOM in the SPDX 3.0 format. <<https://github.com/elisa-tech/BASIL/releases/tag/v1.8.9>> BASIL is open source and maintained by ELISA <<https://elisa.tech/>>, a Linux Foundation project. It is available at <<https://github.com/elisa-tech>

SPDX Java Tools

SPDX Java Tools – SPDX Java Tools is a command-line utility for creating, converting, comparing, and validating SPDX documents across multiple formats including SPDX 3.0 for communicating the components, licenses and copyrights associated with a software and systems. <<https://github.com/spdx/tools-java>>, <<https://github.com/spdx/Spdx-Java-Library>>, <<https://github.com/spdx/spdx-maven-plugin>>, and <<https://github.com/spdx/spdx-to-osv>>.



SysAuditor Suite – The SysAuditor <<https://www.sysauditor.com>> is an operational set of tools designed to capture and utilize metadata related to systems, processes, and operations to build a comprehensive picture of IT organizations, applications, and systems environments. SysAuditor Suite uses the SPDX 3.1 structure to capture and store metadata to create an inventory, such as hardware, software, relationships, and licenses on a device. SysAuditor Suite is designed for operation on Linux-based environments. <<https://www.smarttalkbeacon.com>>



Threatrix – Snippet level copy/paste & AI Code detection with 99.9% accuracy create dynamic, hyper-accurate SBOMs. CLI deploys in build server. <<https://threatrix.io>>



Yocto Project – The Yocto Project is an open source collaboration project that helps developers create custom Linux-based systems regardless of the hardware architecture. The project provides a flexible set of tools and a space where embedded developers worldwide can share technologies, software stacks, configurations, and best practices that can be used to create tailored Linux images for embedded and IOT devices, or anywhere a customized Linux OS is needed. The Yocto Project's Bitbake tooling produces SPDX 3.0 <<https://patchwork.yoctoproject.org/project/oe-core/patch/20240703140059.4096394-4-JPEWhacker@gmail.com/>>



Anchore Enterprise – Anchore Enterprise 5.20 introduces support for SPDX 3 SBOM storage, enabling organizations to upload, manage, and retrieve next-generation software bill of materials documents while maintaining existing workflows. The update helps enterprises prepare for evolving software supply chain security and compliance requirements, especially for distributed and AI-native systems. <<https://anchore.com/blog/anchore-enterprise-is-now-spdx-3-ready/>>

Other SPDX 3.0 Analysis and Production Capabilities (2of2)

SBOM-CVE-check

sbom-cve-check – sbom-cve-check is a lightweight, standalone and easy-to-use tool that parses Software Bill Of Materials (SBOM) files and using publicly available databases of security vulnerabilities (CVEs), provides a report detailing which software components are affected by known security vulnerabilities. <<https://github.com/bootlin/sbom-cve-check>>



Black Duck SCA – Black Duck® software composition analysis (SCA) and make software bills of materials (SBOMs) part of the entire app lifecycle. Import SBOMs, automatically map dependencies, and document new components from custom or commercial dependencies. Export SPDX 3.0 and monitor SBOM dependencies for emergent risks. <<https://www.blackduck.com/software-composition-analysis-tools/black-duck-sca.html>> for more information.



FOSSology – FOSSology <<https://www.fossology.org/>> is an open source license compliance software system and toolkit allowing users to run license, copyright and export control scans from a REST API. As part of the toolkit multiple license scanners, copyright and export scanners are tools available to help with compliance activities. Supports SPDX 3.0. <<https://github.com/fossology>>



Interlynk – Interlynk <<https://docs.interlynk.io/>> provides a comprehensive, automated platform for creating, managing, and securing Software Bill of Materials (SBOMs) and AI BOMs. It helps organizations manage open-source components, ensure licensing compliance, monitor vulnerabilities using VEX, and enforce security policies across the software supply chain.



Microsoft's Open Source SBOM Tool – The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 and SPDX 3.0 compatible SBOMs for any variety of artifacts. The tool uses the Component Detection libraries to detect components and the Clearly Defined API to populate license information for these components. <<https://github.com/microsoft/sbom-tool>>



Sbomify – <<https://app.sbomify.com/>> sbomify is a SBOM and document management platform that can be self-hosted or accessed at sbomify.com. The platform provides a centralized location to upload and manage your SBOMs and related documentation, allowing you to share them with stakeholders or make them publicly accessible. The sbomify backend integrates with their github actions module to automatically generate SBOMs from lock files and docker files. Support for CycloneDX and SPDX SBOM formats (including SPDX 3.0).

sbom-cve-check

sbom-cve-check is implemented in Python, takes a few command line arguments and gets the job done.

Key features

- Accepts an SBOM file as input: currently supports SPDX v2.2 and SPDX v3 (CycloneDX support planned)
- Supports multiple sources of vulnerability information: currently NVD and CVE List
- Can consume various annotation formats, like OpenVEX
- Generates exports in multiple formats, including SPDX v3 (CycloneDX support planned)
- Supports plugins to add additional features
- Filters affected CVEs based on compiled sources: if the source file affected by a CVE is not compiled in, this CVE is considered not applicable. Mostly useful to filter Linux kernel CVEs
- Very few dependencies, lightweight, easy to setup/use
- Fully open-source, under GPLv2

sbom-cve-check documentation

Introduction

User Guide

- Dependencies & installation
- Usage
- Compatibility with Yocto Project
- Examples of invocation
- Overview of command-line options
- Overview of environment variables

Databases

- Common database options
- Git database options
- Database types
- Database Configuration

SBOM

- Supported formats
- Annotations
- Yocto Project SBOM

Export

- Export formats
- Export options
- Reproducible output

Plugins

- Search locations
- Plugin namespace
- Python package as plugin
- Minimal examples

Configuration

- Configurable elements
- Configuration generation

<https://sbom-cve-check.readthedocs.io/>

Tool design

- Concepts
- Find applicable CVE
- Compute VEX assessment
- Developer Guide
- Download Git sources
- Python virtual environment
- Documentation generation
- Tool installation for development
- Linter and static analysis
- pylint
- Tests
- Release process
- Roadmap & planned developments

Terminology

Index

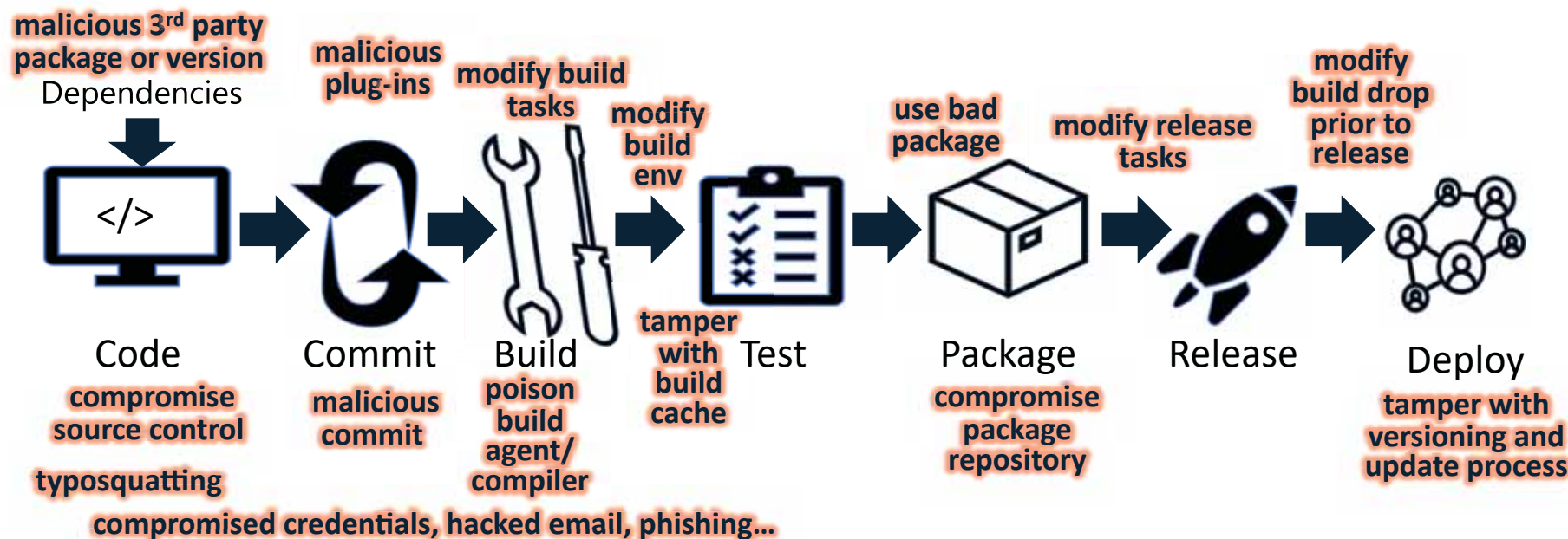


<https://github.com/bootlin/sbom-cve-check>

Supply Chain Attestation Targets

What do we need evidence about?

Software Supply Chain

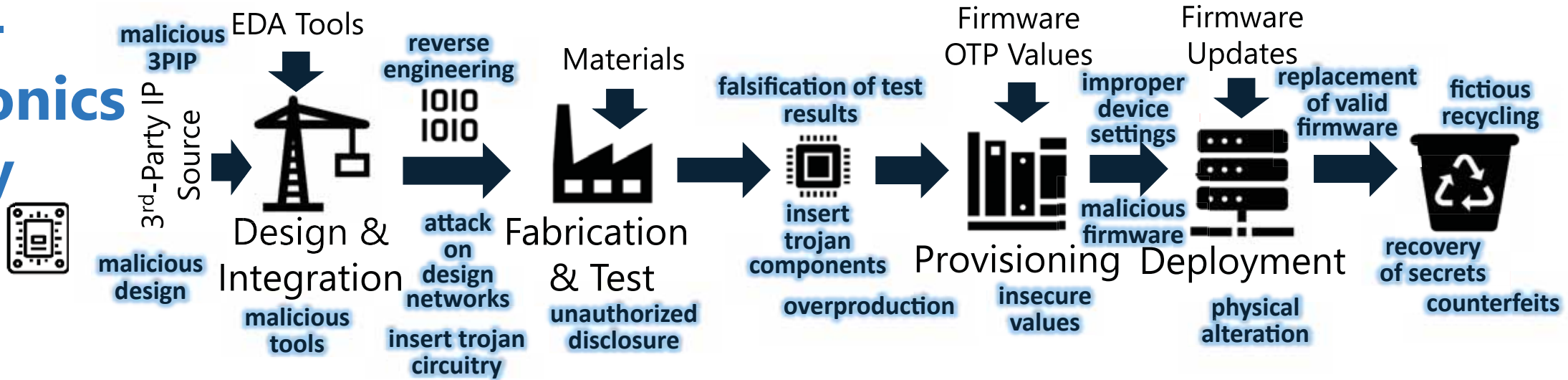


Hazards and Threats

Supply Chain Attestation Targets

What do we need evidence about?

Micro-electronics Supply Chain

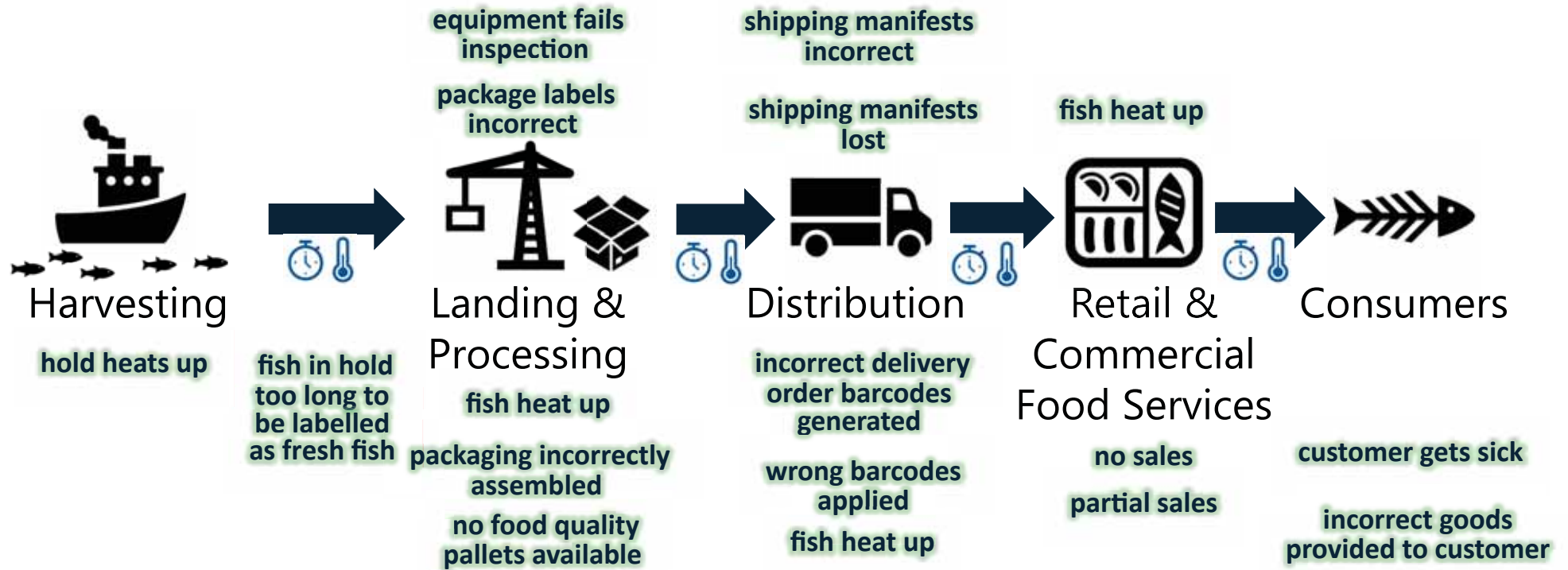


Hazards and Threats

Supply Chain Attestation Targets

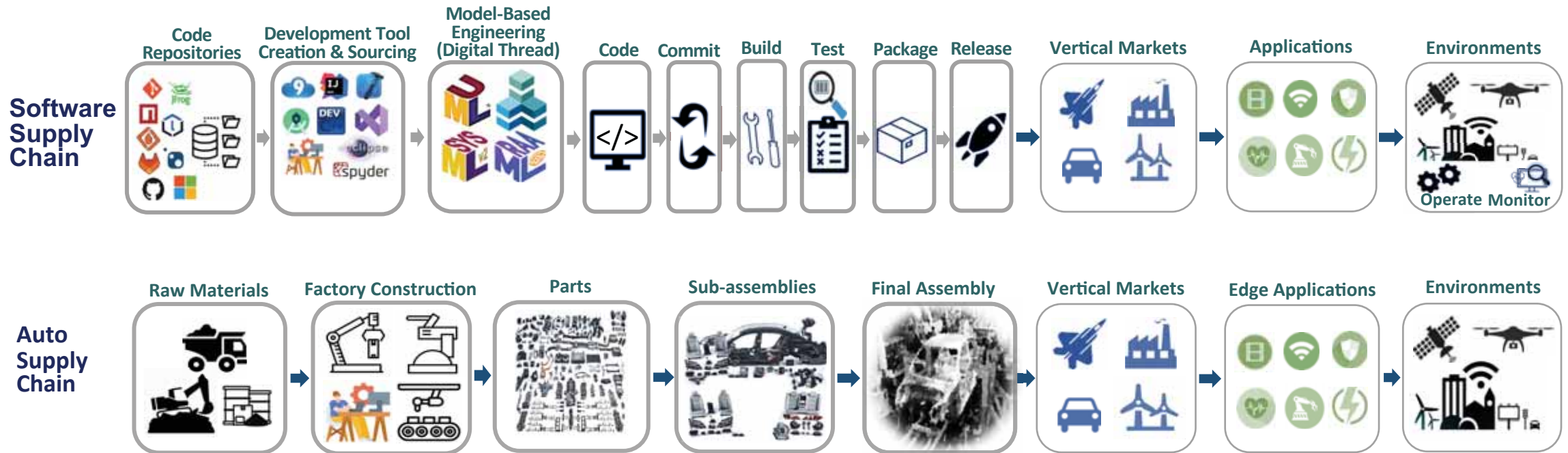
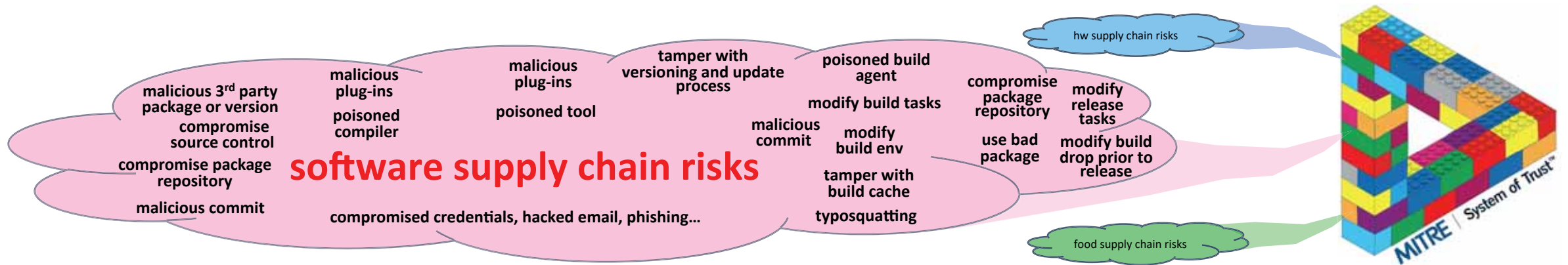
What do we need evidence about?

Seafood Supply Chain



Hazards and Threats

SCITT and MITRE's SoT™

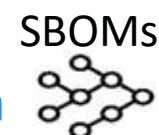
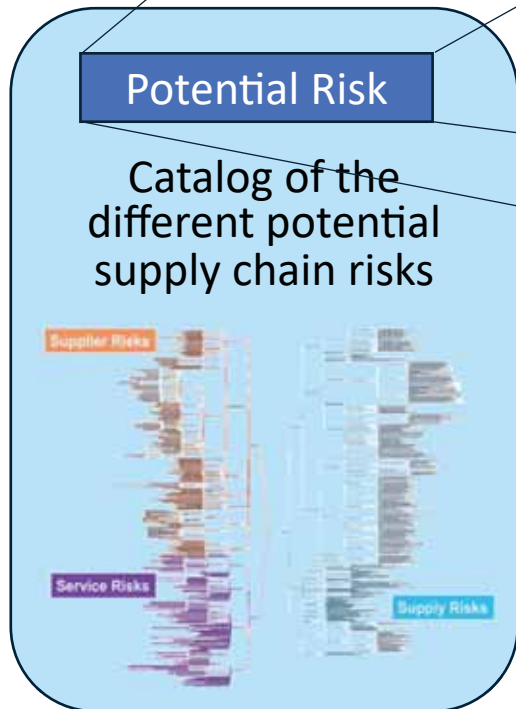


System of Trust™

Assessing Risks with Data/Information



SoT consists of 733 measurable risk factors (RFs) with 2,224 risk measures (RMs)



Binary



Claims from supplier about supplies and the supplier



Vulnerability Assessment



Site visit



Direct measurement



Direct questioning

NIST

TIA

SAE INTERNATIONAL

ISA

THE Open GROUP

Lexus Nexis

BVD

Exiger

interos

Classified Sources

State Dept

Treasury Dept

web



Data / information

Data / information

Data / information

Data / information

Data / information

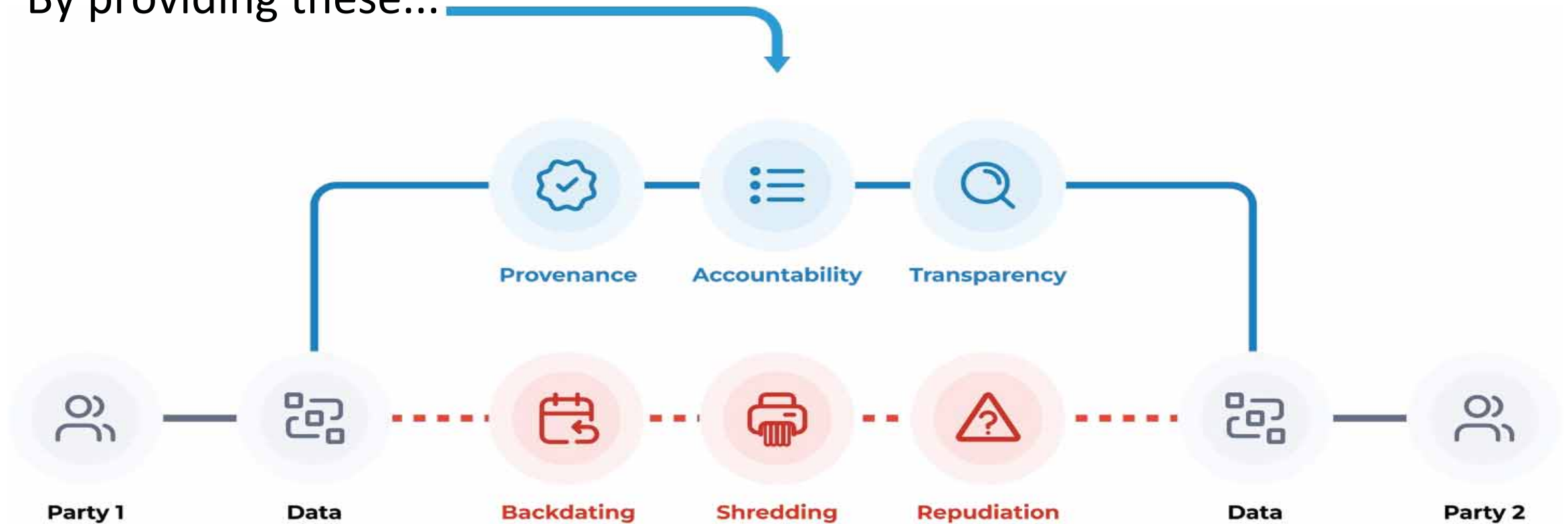
Data / information

Data / information

Data / information

Bringing Integrity into the Digital Supply Chain

By providing these...



...we mitigate these

Publish attestations and statements

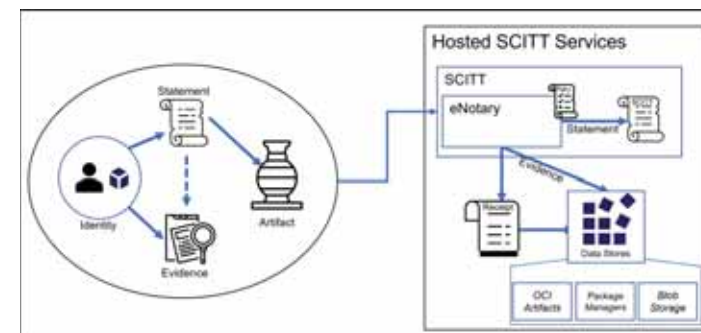


Alongside binaries published in a source repository



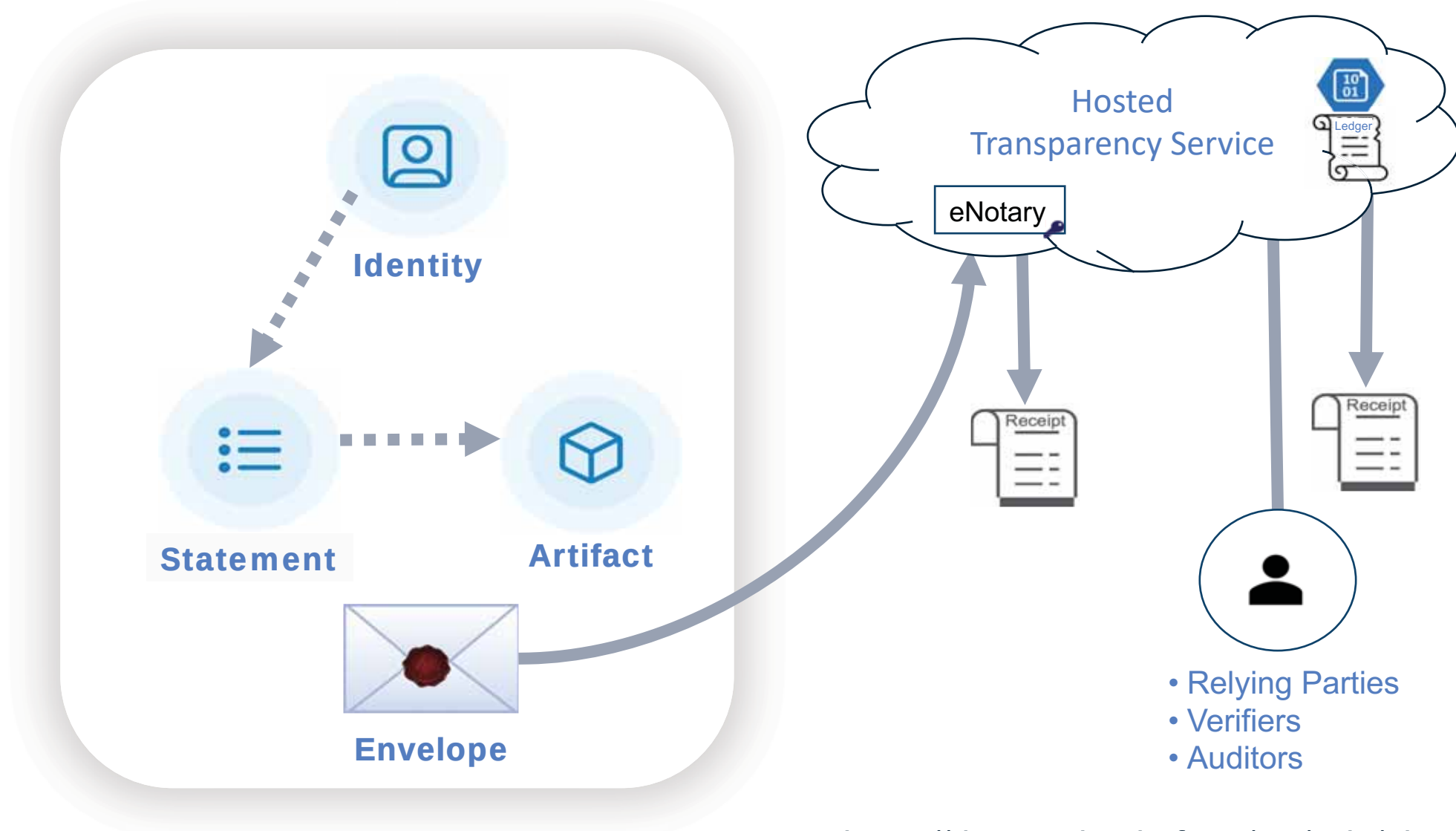
Alongside an artifact in a package registry (e.g. PyPI)

Supply Chain Integrity, Transparency and Trust (SCITT)



In a durable tamper-proof transparency log

Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency and Trust (SCITT) Working Group Efforts

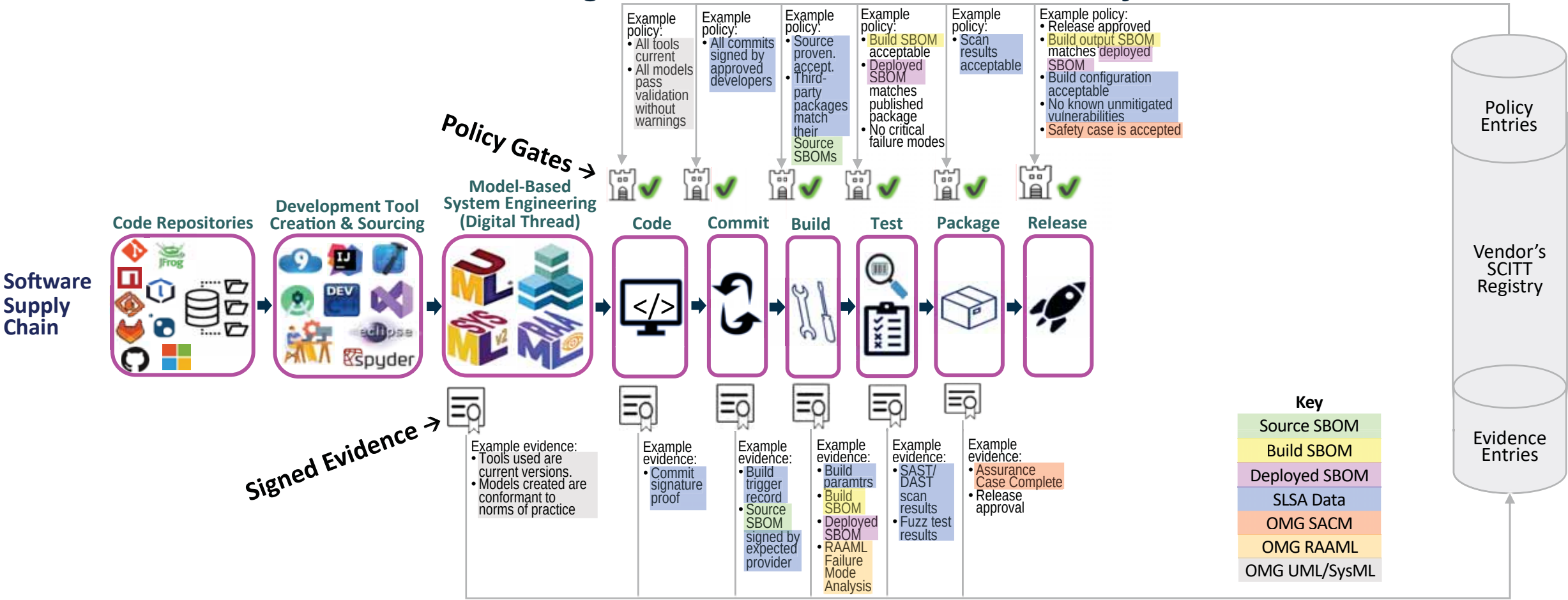


Identities make Statements about Artifacts

<https://datatracker.ietf.org/wg/scitt/about/>

IETF's Supply Chain Integrity, Transparency, and Trust (SCITT) standards in Software Supply Chain Security

Policies looking for evidence about the risks from System of Trust

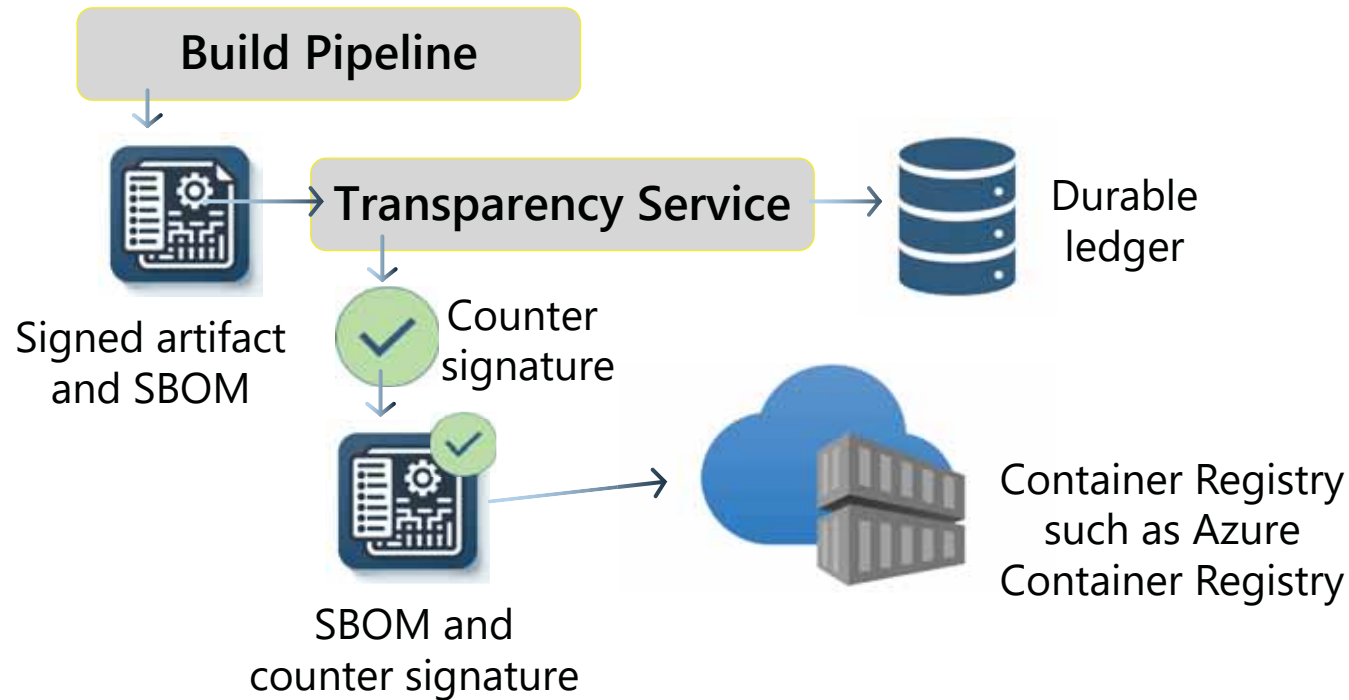


Example of IETF SCITT in SW Development

Microsoft's use of SCITT

SCITT can be used to sign a variety of statements and attestations. In this case we'll look at a simple case, counter signing an SBOM with SCITT.

Counter Signing an SBOM with SCITT



Implementers of SCITT can use their preferred durable ledger, container registry, and graph databases as part of their implementation.

Verifiable AI Provenance (VAP) Framework and Legal AI Profile (LAP)

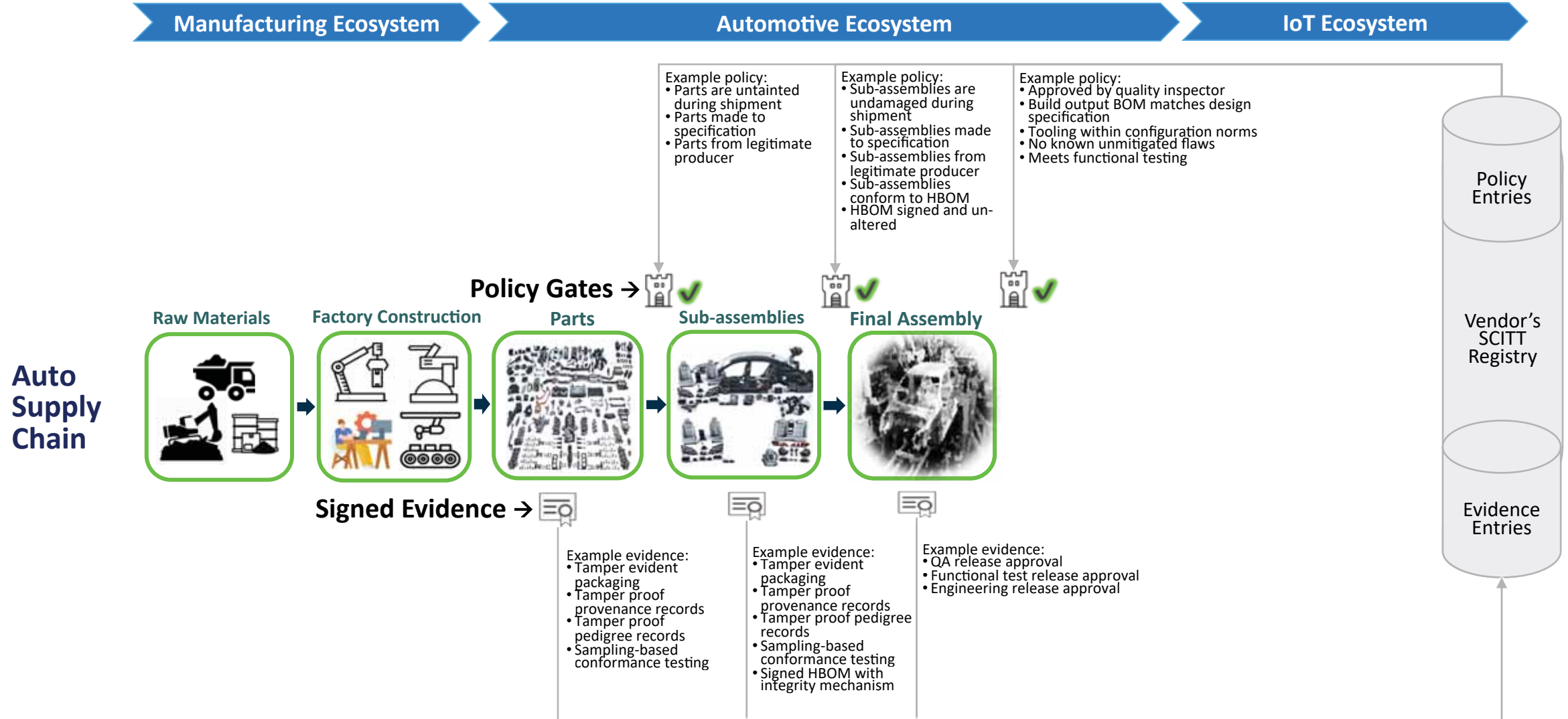
Intended status: Experimental

- Datatracker: <https://datatracker.ietf.org/doc/draft-ailex-vap-legal-ai-provenance/>

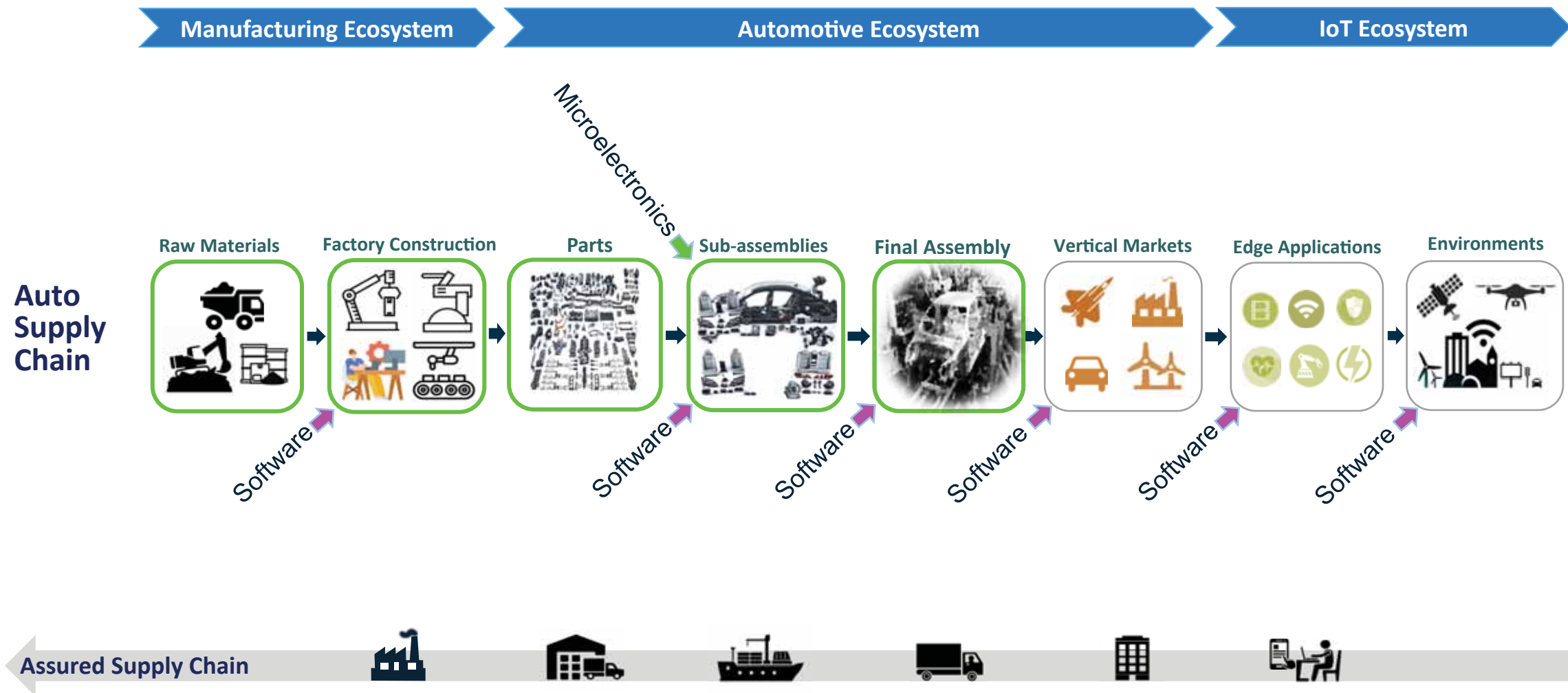
A cross-domain upper framework for cryptographically verifiable decision audit trails in high-risk AI systems, along with the Legal AI Profile (LAP), a domain-specific instantiation for legal AI and LegalTech systems.

- VAP defines common infrastructure including hash chain integrity, digital signatures, unified conformance levels via RFC 3161 Time-Stamp Protocol and compatible transparency services (including IETF SCITT), a Completeness Invariant pattern guaranteeing no selective logging, standardized Evidence Pack format for regulatory submission, and privacy-preserving verification protocols.
- LAP extends VAP for the judicial AI domain, addressing unique requirements including attorney oversight verification (Human Override Coverage), three-pipeline completeness invariants for legal consultation, document generation, and fact-checking, tiered content retention with legal hold protocols for judicial discovery compliance, graduated override enforcement mechanisms, and privacy-preserving fields designed to maintain attorney-client privilege while enabling third-party auditability.

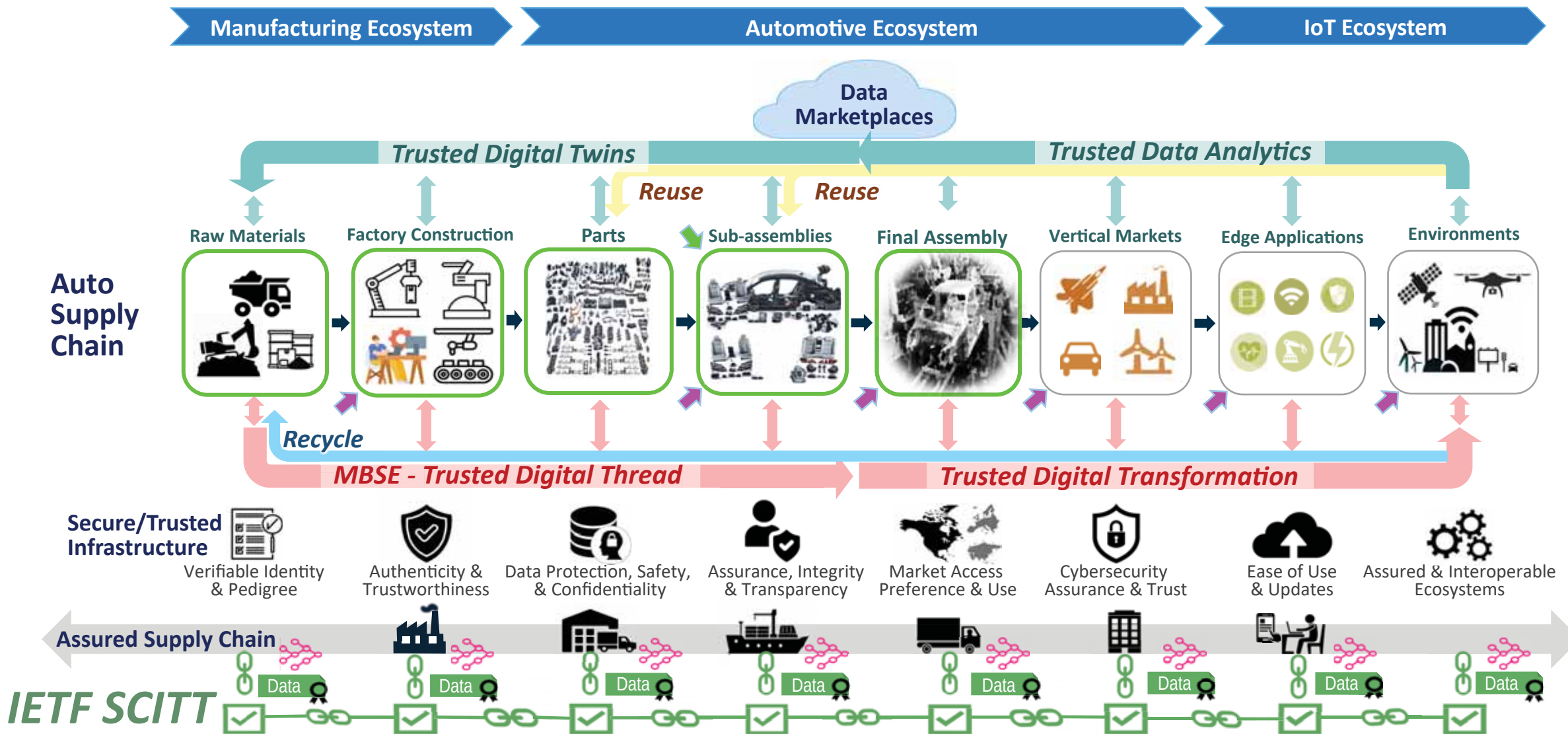
Example of the IETF SCITT in Auto Supply Chain



A Fuller Auto Supply Chain



A Fuller Auto Supply Chain



Putting things together for Visible by Design

- **What risks should I assess and manage?**
 - Leverage MITRE's System of Trust™
- **What data/information do I need to do that?**
 - Make use of BOMs, DDPs, and other attestations
- **How can I trust the data without collecting it myself?**
 - Investigate IETF's Supply Chain Integrity, Transparency, and Trust (SCITT)
- **How can I address all the different requirements about supply chains?**
 - Help explore SoT mappings

**Need to
harmonize and
make available**

Standards like SPDX, DPPs, UNTP, SCITT, and SoT are providing the tools for closing the gap between compliance obligations and supply chain visibility.



Questions?

ramartin@mitre.org