RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: GRC-R05

SBOMs: Navigating the Evolving Landscape of Software Bill of Materials

#RSAC

Manoj Prasad

Security & Engineering, Predigle
Faculty, CS@Western Washington University

Disclaimer

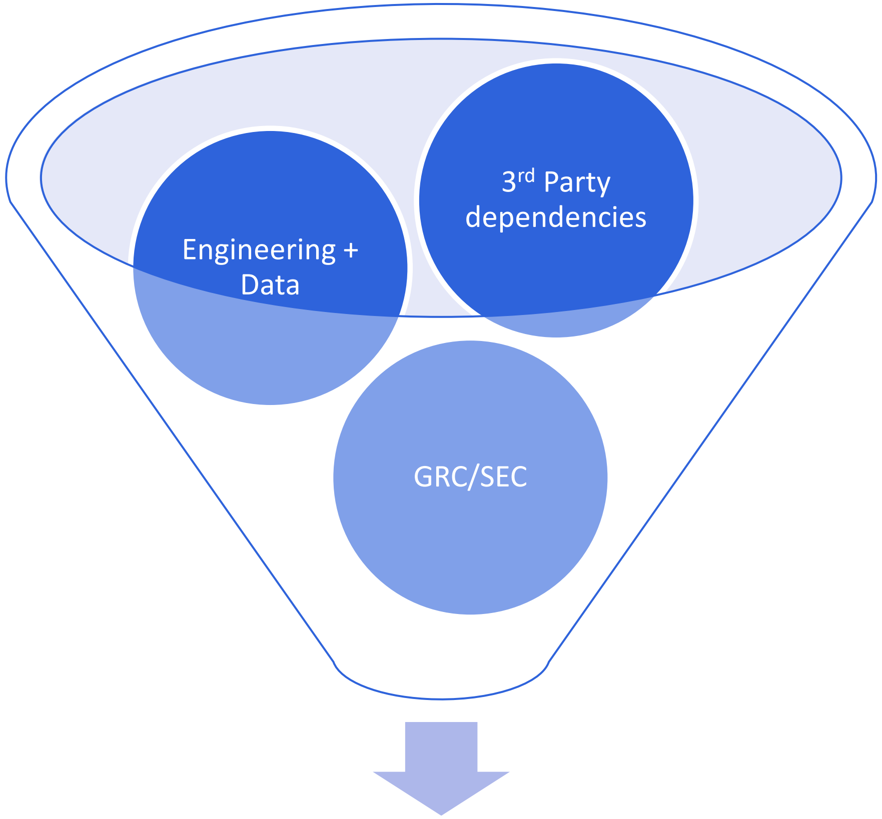
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Mental Model

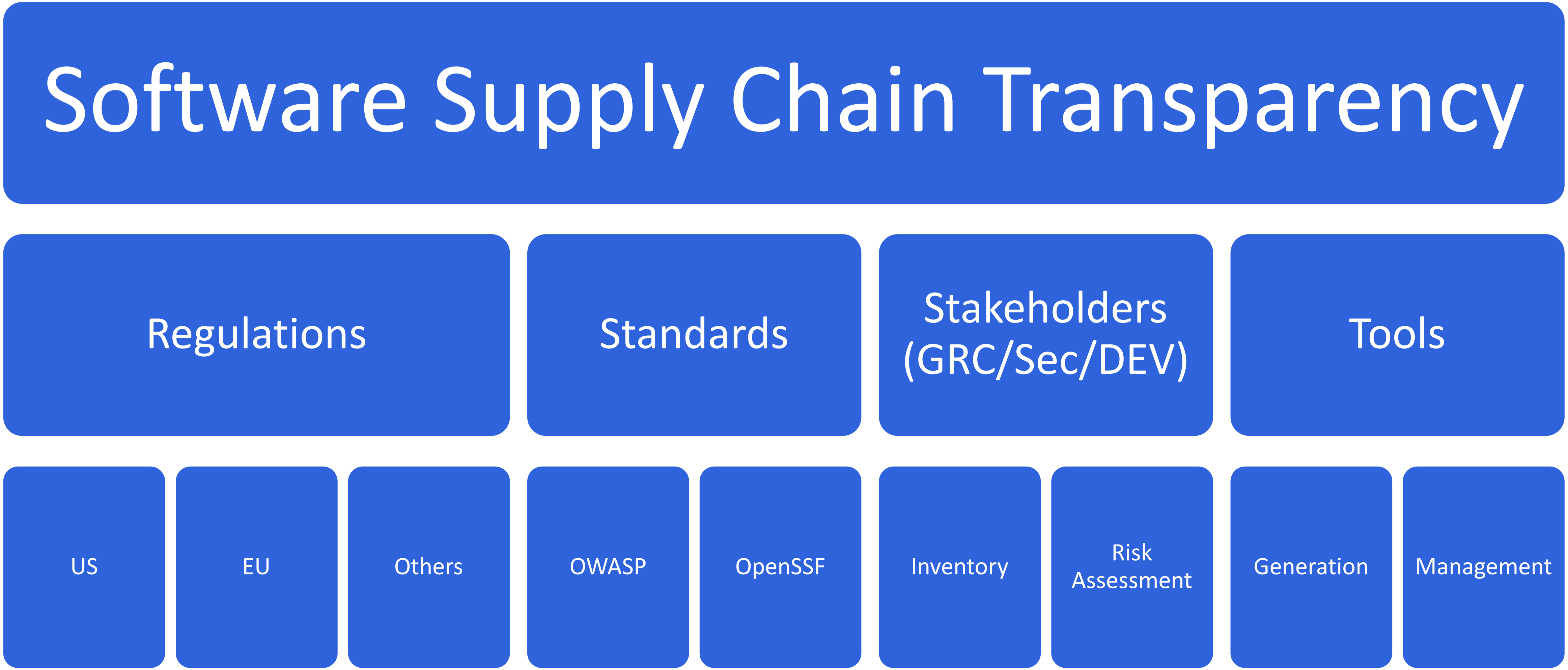
HOW TO ORGANIZE OUR THOUGHTS ON SOFTWARE SUPPLY CHAIN TRANSPARENCY

Supply Chain Transparency



Software

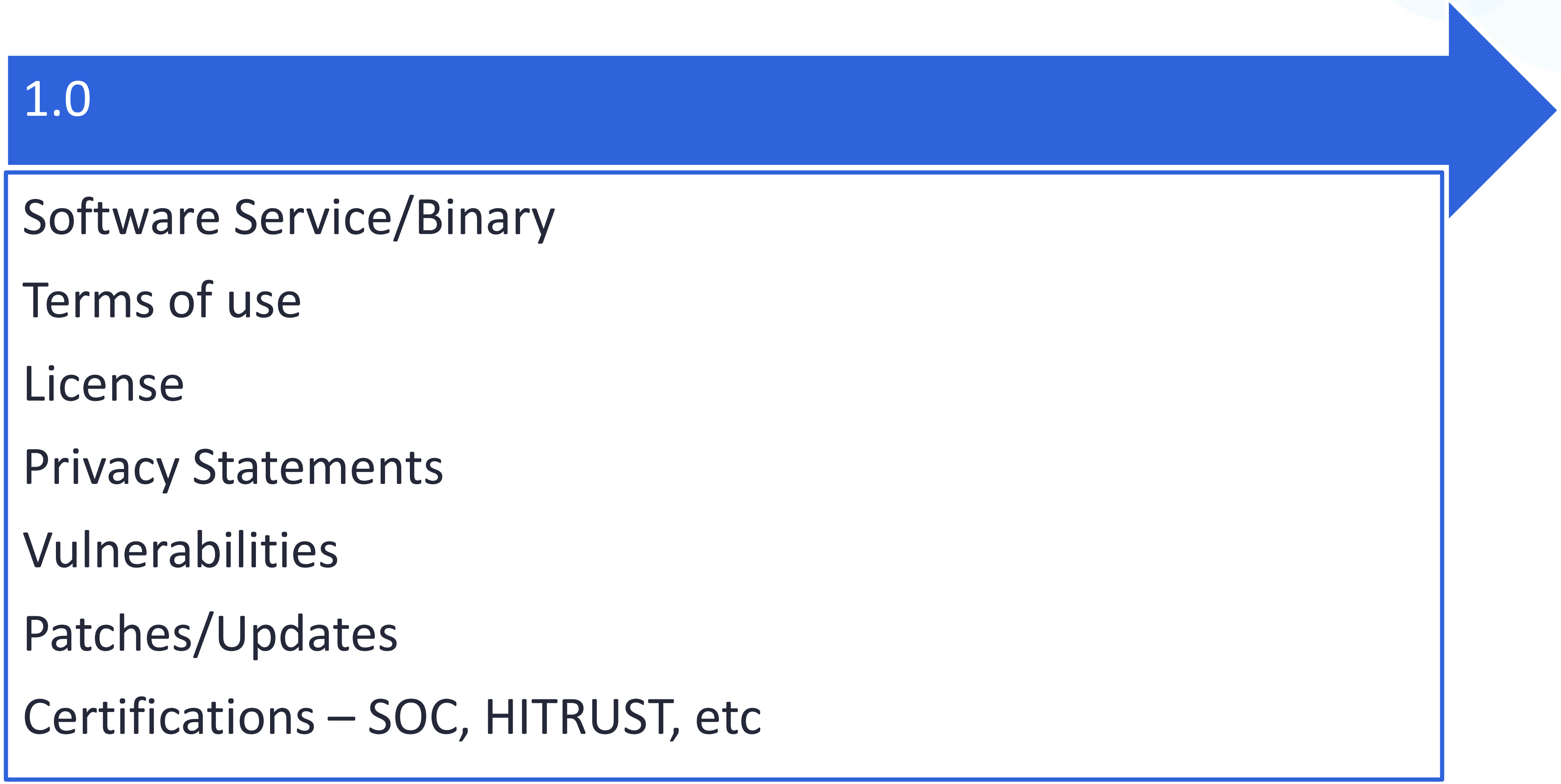
Agenda



Software Supply Chain Transparency

- Regulations
  - US
  - EU
  - Others
- Standards
  - OWASP
  - OpenSSF
- Stakeholders (GRC/Sec/DEV)
  - Inventory
  - Risk Assessment
- Tools
  - Generation
  - Management

Supply Chain Transparency Artifacts



1.0

Software Service/Binary

Terms of use

License

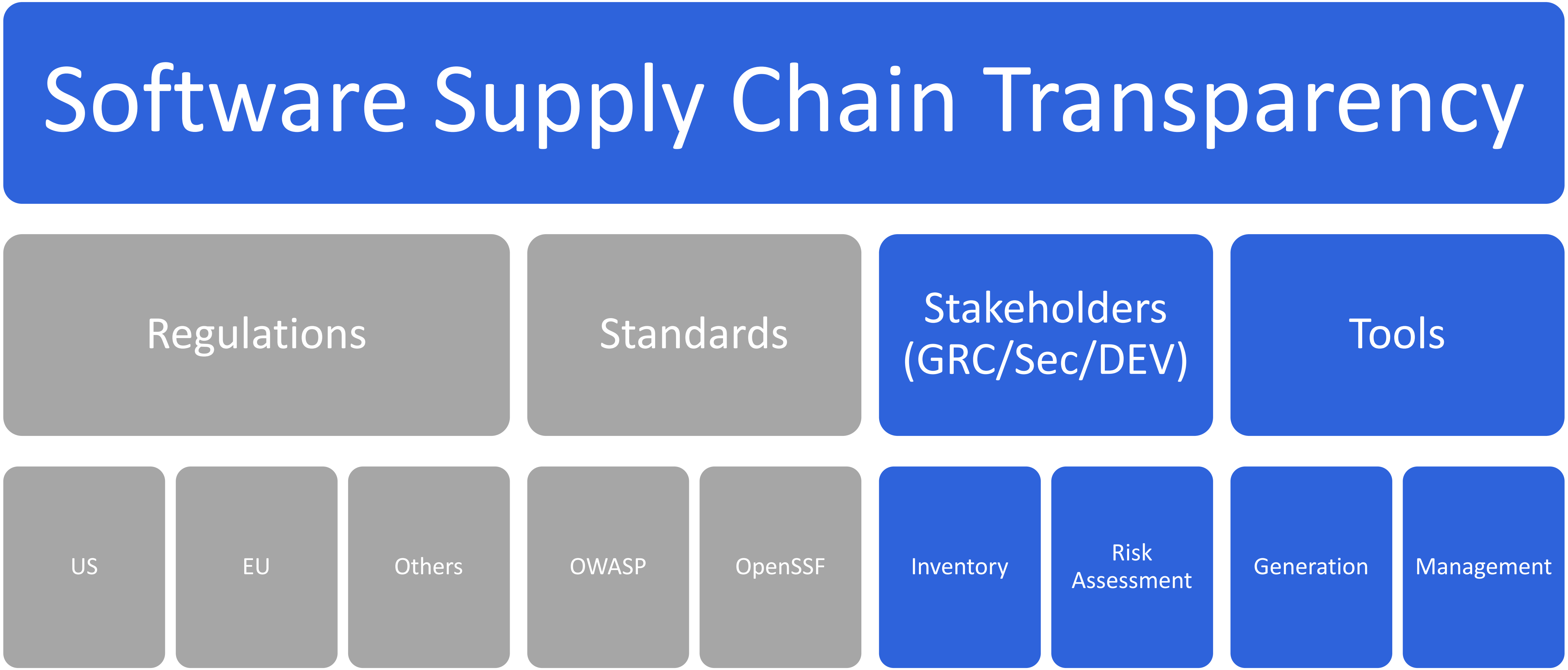
Privacy Statements

Vulnerabilities

Patches/Updates

Certifications – SOC, HITRUST, etc

Agenda



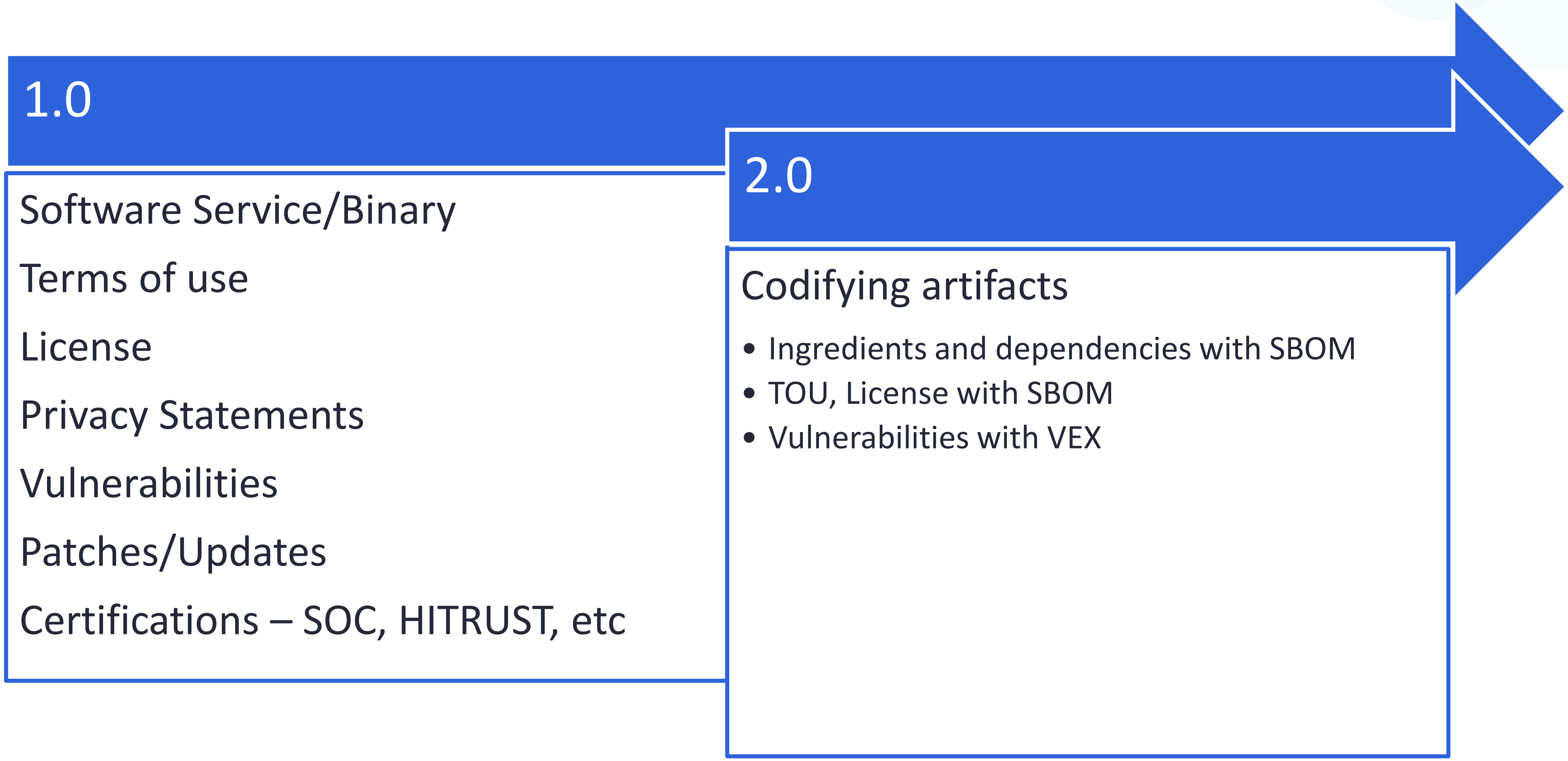
Software Supply Chain Transparency

- Regulations
  - US
  - EU
  - Others
- Standards
  - OWASP
  - OpenSSF
- Stakeholders (GRC/Sec/DEV)
  - Inventory
  - Risk Assessment
- Tools
  - Generation
  - Management

Accountability/Trust/Liability

- Accountability
  - TOU
  - License
  - Privacy Policy
- Trust
  - Certifications
  - FDA – Medical Device software
- Liability
  - Private contract controlled by License

Supply Chain Transparency Artifacts



1.0

Software Service/Binary

Terms of use

License

Privacy Statements

Vulnerabilities

Patches/Updates

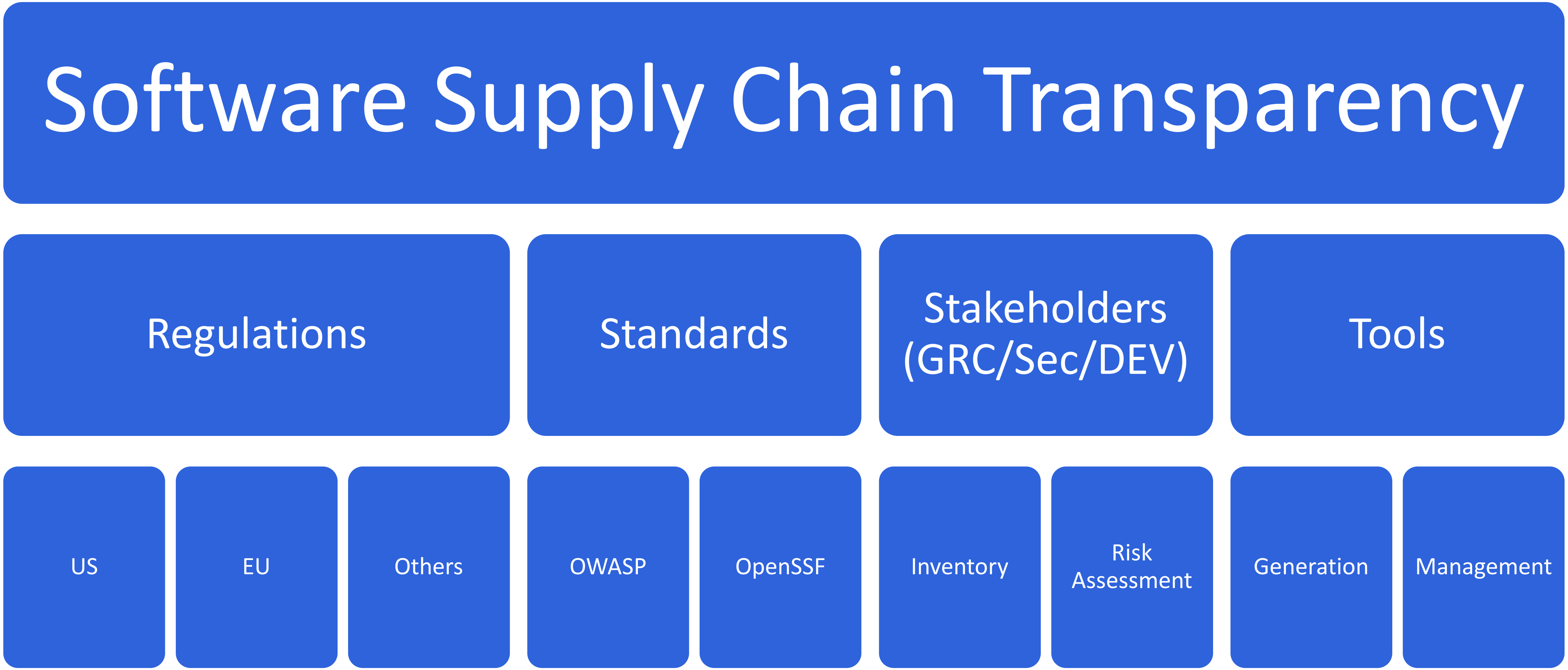
Certifications – SOC, HITRUST, etc

2.0

Codifying artifacts

- Ingredients and dependencies with SBOM
- TOU, License with SBOM
- Vulnerabilities with VEX

Agenda



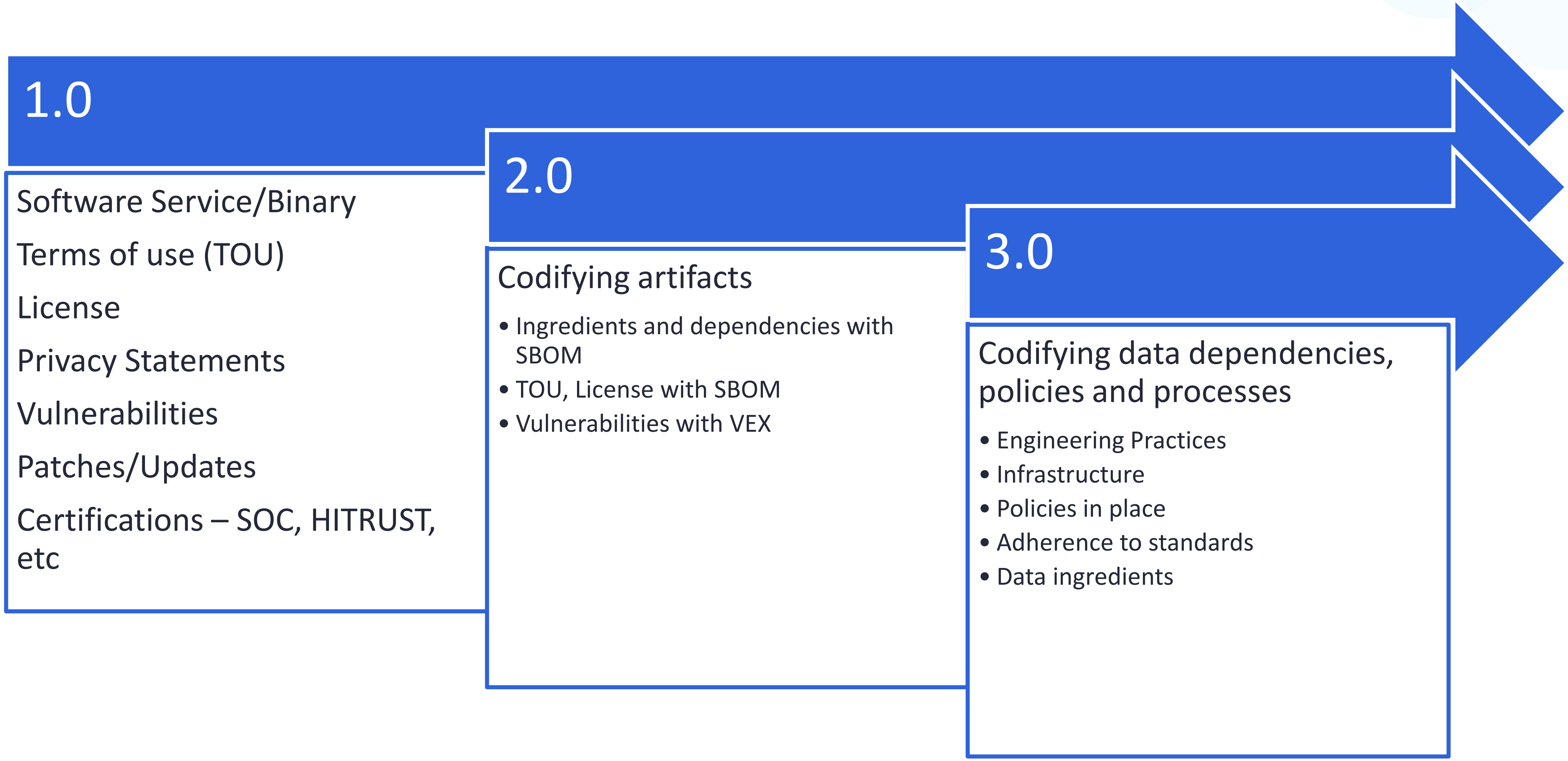
Software Supply Chain Transparency

- Regulations
  - US
  - EU
  - Others
- Standards
  - OWASP
  - OpenSSF
- Stakeholders (GRC/Sec/DEV)
  - Inventory
  - Risk Assessment
- Tools
  - Generation
  - Management

Accountability/Trust/Liability

- Accountability
  - TOU
  - License
  - Privacy Policy
  - SBOM/VEX – Transparency into the ingredients and process
- Trust
  - Certifications
  - FDA – Medical Device software
  - Attestations – Transparency into compliance
- Liability
  - Private contract controlled by License
  - Legal framework to incentivize compliance

Supply Chain Transparency Artifacts



1.0

Software Service/Binary

Terms of use (TOU)

License

Privacy Statements

Vulnerabilities

Patches/Updates

Certifications – SOC, HITRUST, etc

2.0

Codifying artifacts

- Ingredients and dependencies with SBOM
- TOU, License with SBOM
- Vulnerabilities with VEX

3.0

Codifying data dependencies, policies and processes

- Engineering Practices
- Infrastructure
- Policies in place
- Adherence to standards
- Data ingredients

Regulations

Regulations - Accelerating Evolution

- EO 14028 - Improving the Nation’s Cybersecurity
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-218: Secure Software Development Framework (SSDF)
  - NTIA minimum requirements
  - Office of Management and Budget (OMB) Memorandum M-23-16
  - Dept of Homeland Security, Department of Energy, HH
  - FDA / Medical Devices - Consolidated Appropriations Act and Patch Act 2022 (Protecting and Transforming Healthcare Act)

Regulations - Accelerating Evolution

- EU
  - BSI - The German IT Security Act 2.0
  - National Cyber Security Centre Finland SBOM Guidelines
  - Cyber Resilience Act 2024

    Manufacturers of the products with digital elements shall: (1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product.
  - Digital Operational Resilience for the Financial Sector 2024

Regulations - Accelerating Evolution

- Australia
  - Australian Cyber Security Centre - ISM-1730: Software bill of materials

Evolution of Incentives to secure SDLC

- * Software provider accountability
  - Moved from private domain to public domain
  - Provided legal framework
  - Deterministic liability

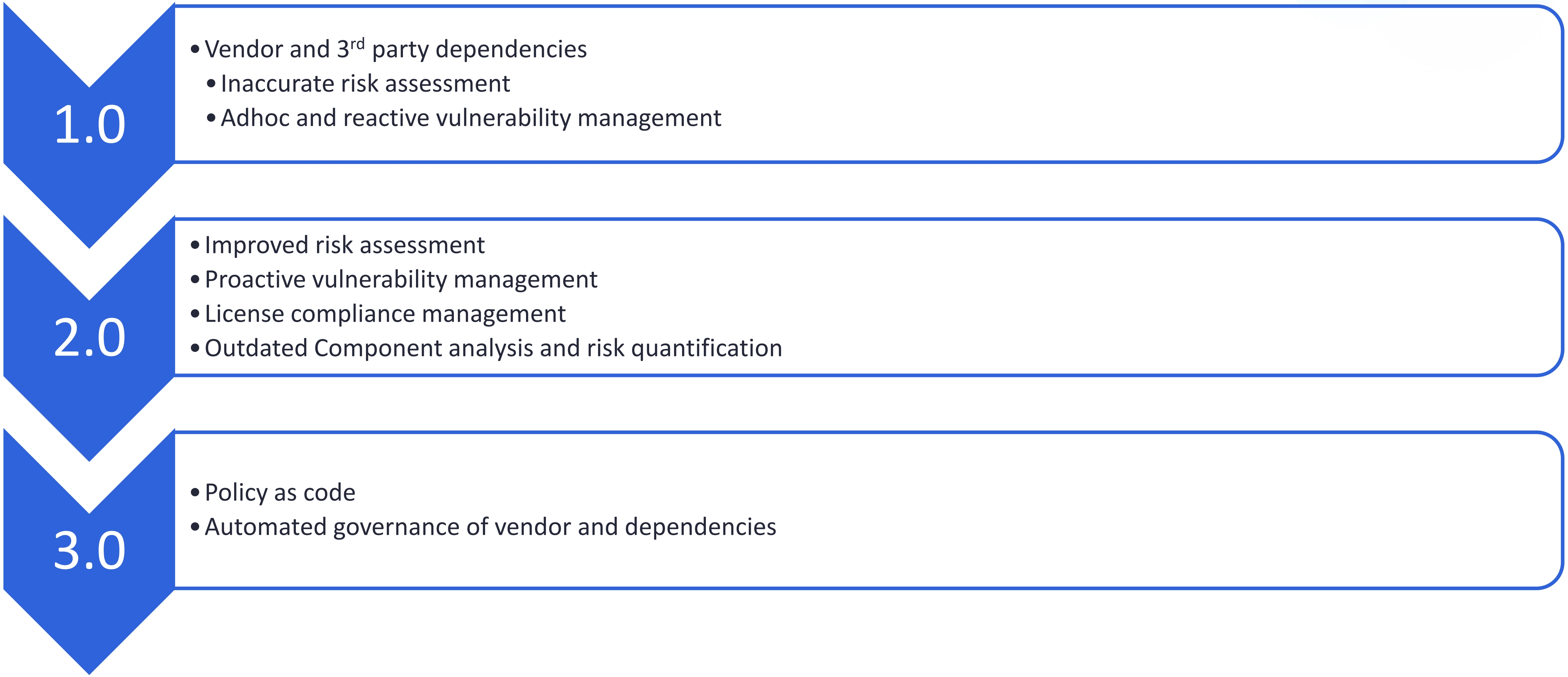
Evolving Standards

- Ingredients, License
  - Cyclone DX - OWASP
  - SPDX – OpenSSF
  - SWID - NIST
    - *NTIA minimum elements for SBOM*
- Vulnerability Exchange
  - Cyclone DX (VEX) - OWASP
  - OpenVEX - OpenSSF

Evolving Standards

- Software Supply chain maturity
  - Attesting to SDLC and compliance to standards
  - Maturity Model
    - NIST SSDF
    - SLSA – OpenSSF/Google
    - S2c2f – OpenSSF/Microsoft
  - Machine readable representation
    - In-TOTO
    - Cyclone DX

GRC



1.0

- Vendor and 3rd party dependencies
  - Inaccurate risk assessment
  - Adhoc and reactive vulnerability management

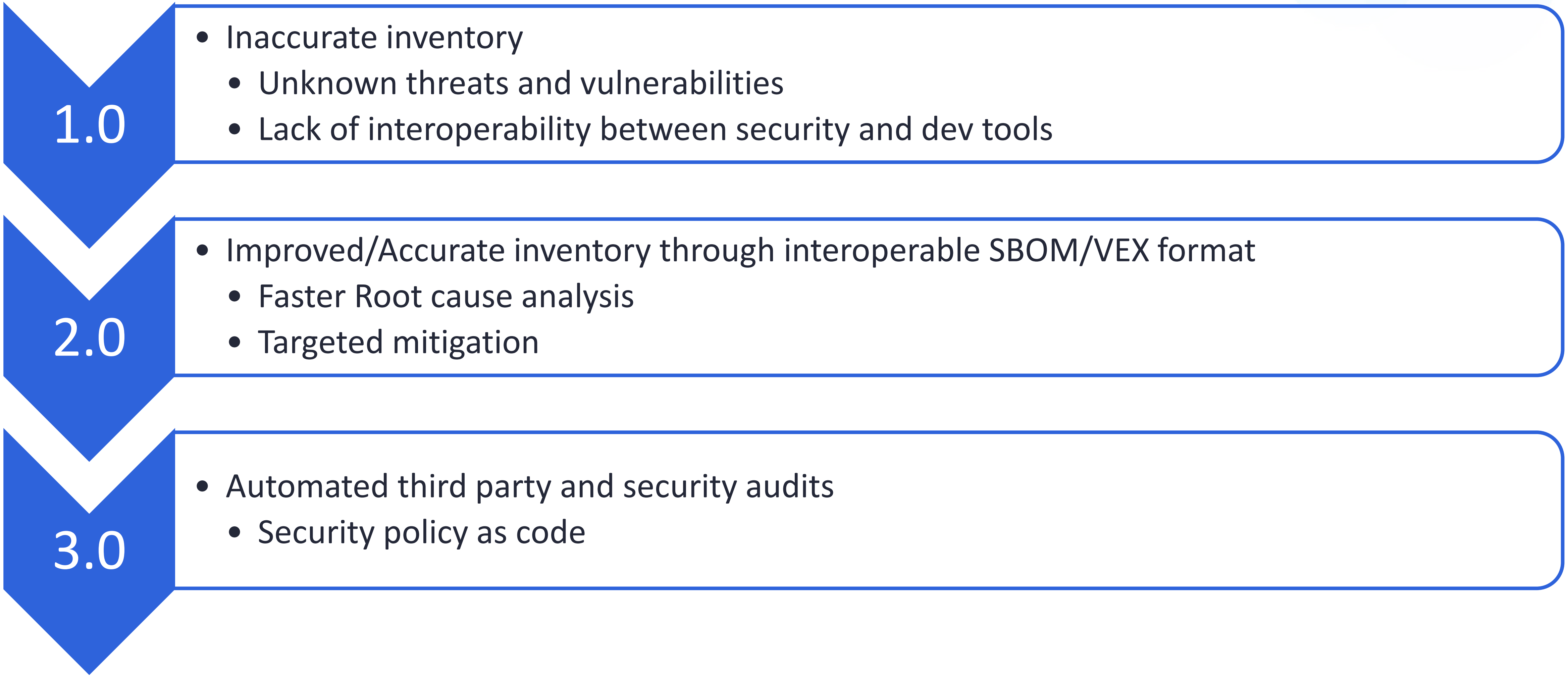
2.0

- Improved risk assessment
- Proactive vulnerability management
- License compliance management
- Outdated Component analysis and risk quantification

3.0

- Policy as code
- Automated governance of vendor and dependencies

Security



1.0

- Inaccurate inventory
  - Unknown threats and vulnerabilities
  - Lack of interoperability between security and dev tools

2.0

- Improved/Accurate inventory through interoperable SBOM/VEX format
  - Faster Root cause analysis
  - Targeted mitigation

3.0

- Automated third party and security audits
  - Security policy as code

Tools for 2.0 & beyond

- Generate / Validate
- Attestations
- Sign
- Distribute
- Consume / Manage

Tools for 2.0 & beyond – Generation / Validation

OSS Community driven

- OWASP Cyclone DX Generator - CDXGen (Apache 2.0)
  - CDX tool center
- OpenSSF SPDX SBOM Generator (Apache 2.0)

Industry driven

- Anchore Syft (Apache 2.0)
- Microsoft SBOM tool (MIT)
- Lockheed Martin Hoppr (MIT)
- ZARF (Apache 2.0)
  - Bundler

Tools for 2.0 & beyond – Attestations

- OWASP Cyclone DX Generator - CDXGen (Apache 2.0)

- Anchore Syft (Apache 2.0)
  - In-TOTO attestations
- Aqua Security Trivy (Apache 2.0)
  - In-TOTO attestations for scanners

Tools for 2.0 & beyond – Signing

- OWASP Cyclone DX Generator - CDXGen (Apache 2.0)

- OpenSSF Sigstore (Apache 2.0)

Tools for 2.0 & beyond – Distribution/Release Management

- Same as artifact distribution services
  - Docker registries
  - Package managers

Tools for 2.0 & beyond – Assured Package Service

Services offering security assurance over OSS through SBOM and provenance validation

- Sonatype Maven Central
- Google Assured OSS

Tools for 2.0 & beyond – SBOM management

OSS Community driven

- Dependency Track (Apache 2.0)

Industry driven

- FOSSA

Opportunities for OSS Community + Entrepreneurs

Providers

Tooling for distribution

- VEX data
- SBOM & Attestation Release management

Consumers

Tooling for GRC and Security

- Tools to enforce GRC policy in SDLC - using SBOM, VEX & Attestation to filter consumption of trusted
  - Container images
  - Packages
  - Runtime architectures

Opportunities for GRC/Security Practitioners

Next Week

- Identify critical components for SBOM generation
- Research and select tools for SBOM generation

3 Months

- Implement a process for SBOM generation for critical components
- Establish a process to include dependencies in SBOM.
- Develop a strategy to integrate vulnerability management with available SBOMs.
  - Identify tools to support vulnerability management with VEX and SBOMS

6 Months

- Identify tools to support generating attestations on critical component SDLC
- Establish a process of release management based on attestations generated during the SDLC

Questions ?