

“What do I do with an SBOM?”

SBOM Lifecycle Management and Use Cases

Developed by the SBOMOps Working Group
of the CISA SBOM Community

Anita D’Amico
anitacodedx@gmail.com

Tim Mackey
tmackey@blackduck.com

Ken Zalevsky
ken.zalevsky@vigilant-ops.com

Motivation of SBOMOps Working Group

- Answer the “now what” questions
 - *Once I generate or receive an SBOM, what do I do with it?*
 - *What additional insights or intelligence can I gain from the SBOM that will benefit my organization?”*
- Demonstrate benefits of SBOMs for both Producers and Consumers

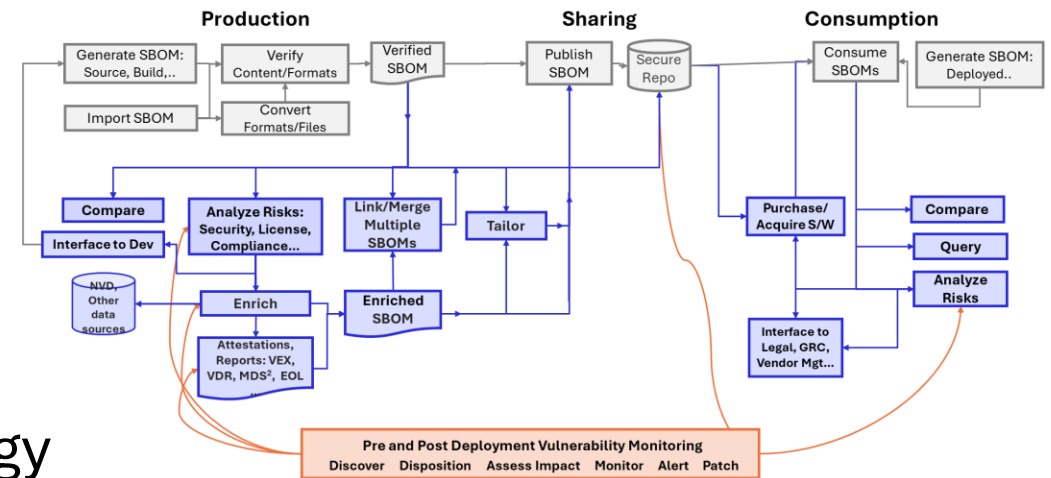
Goals of Document

Explain SBOM Lifecycle Management

- Graphical depiction of SBOM lifecycle
- Common reference workflow and terminology
 - Used by SBOM producers and consumers to express their needs
 - Used by solution providers to communicate what functions within the SBOM lifecycle they address

Provide practical use cases that exemplify how an organization can extract additional value from an SBOM after it has been generated

Improving Risk Management Decisions with SBOM Data (Draft April 4, 2025)



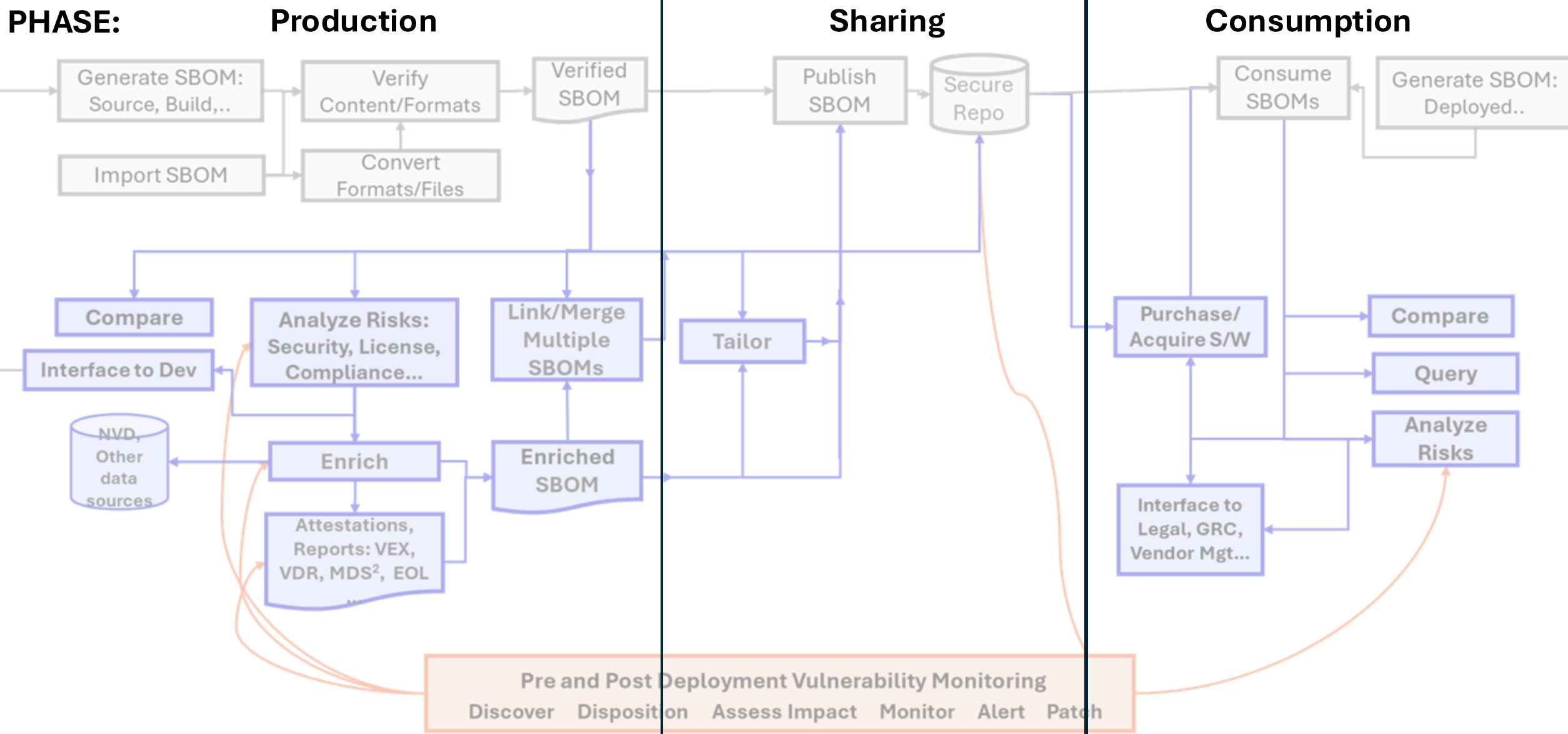
Major Sections of Document

- Explanation of SBOM Lifecycle with associated graphics
 - Analysis and synthesis of many sources: CISA, NTIA, NSA, SEI, CERT-In, academia, industry SBOM producers and consumers
- Thirteen Use Cases and where they fall in the SBOM Lifecycle
 - Narrative Description
 - Table of 7 Attributes:
 - Actors
 - Business Motivation
 - Functional Objectives
 - Steps to Achieve Objectives
 - NTIA Fields Used
 - Added or Cross-linked Data
 - Benefits Achieved
- Key Takeaways
 - Table of NTIA fields used for each use case
 - Table of other data sources cross-linked to SBOM data for each use case

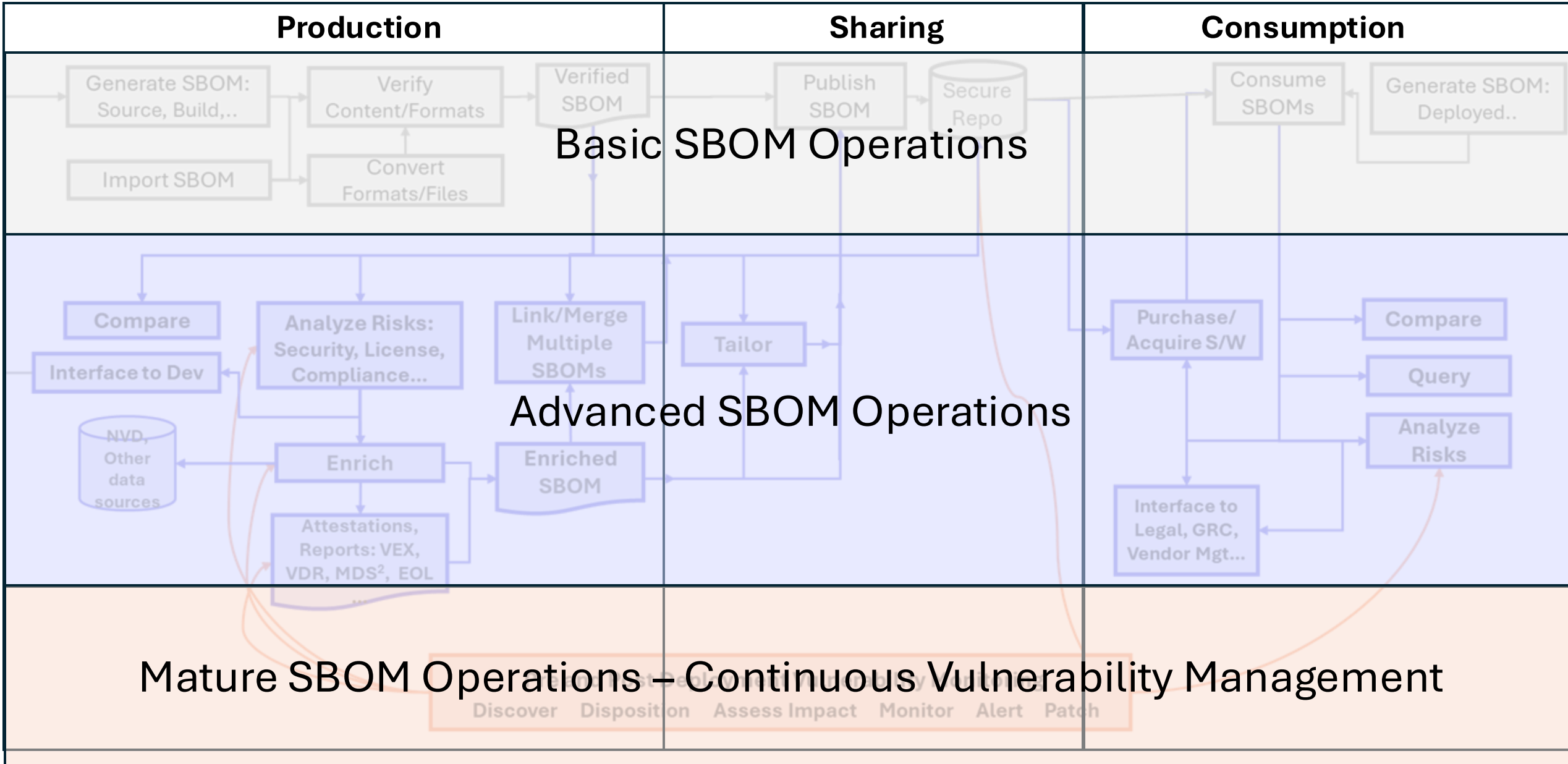
The SBOM Lifecycle and Operations Performed on an SBOM During Its Life

Organized into three lifecycle phases and three levels of maturity of SBOM operations

The SBOM Lifecycle: 3 Phases



The SBOM Lifecycle: 3 Phases, 3 Levels of Maturity

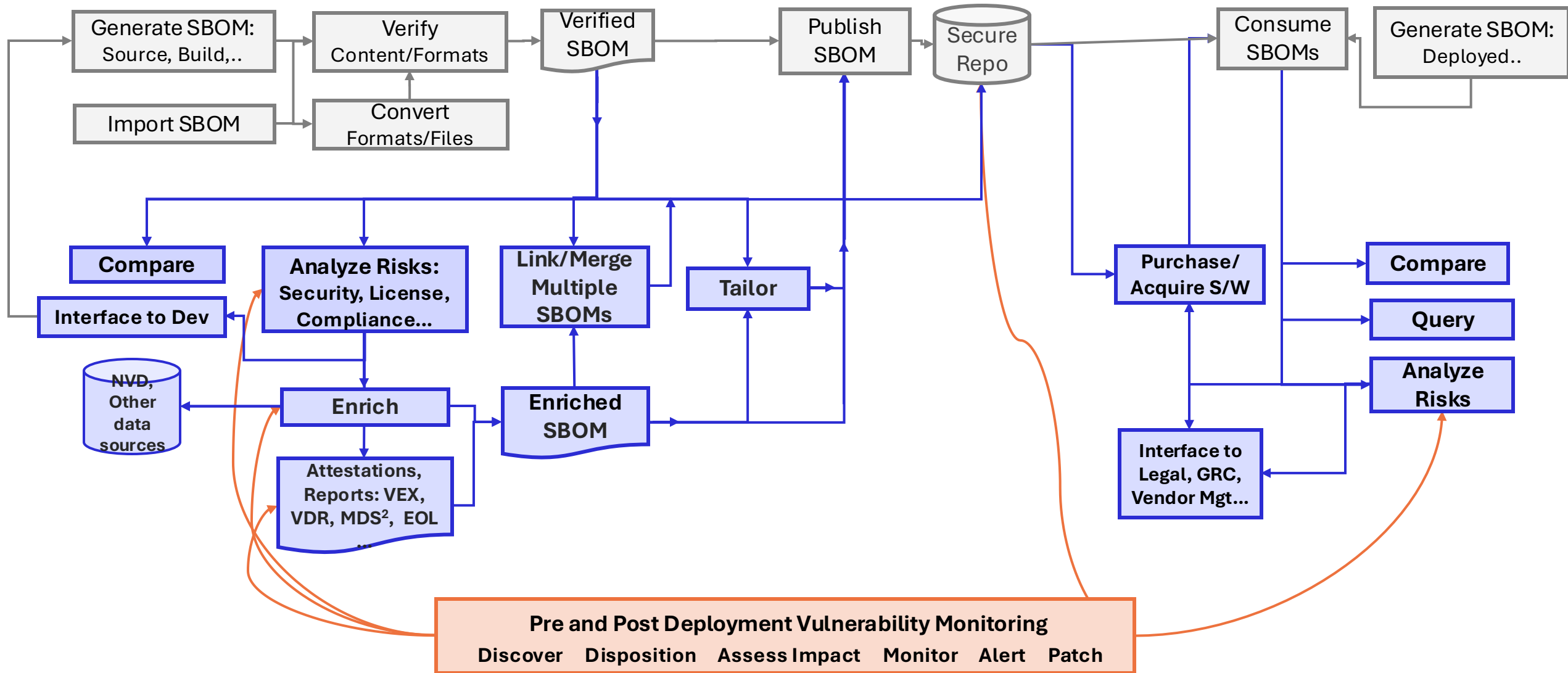


The SBOM Lifecycle

Production

Sharing

Consumption



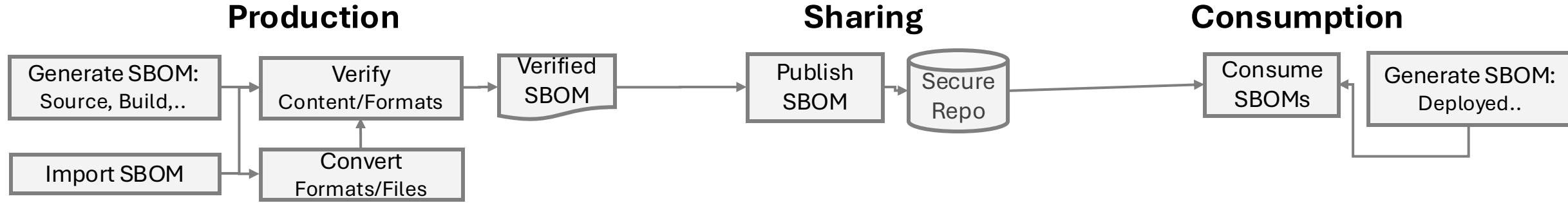
Color Legend

Basic SBOM Operations

Advanced SBOM Operations

Continuous Vulnerability Monitoring

Basic SBOM Operations

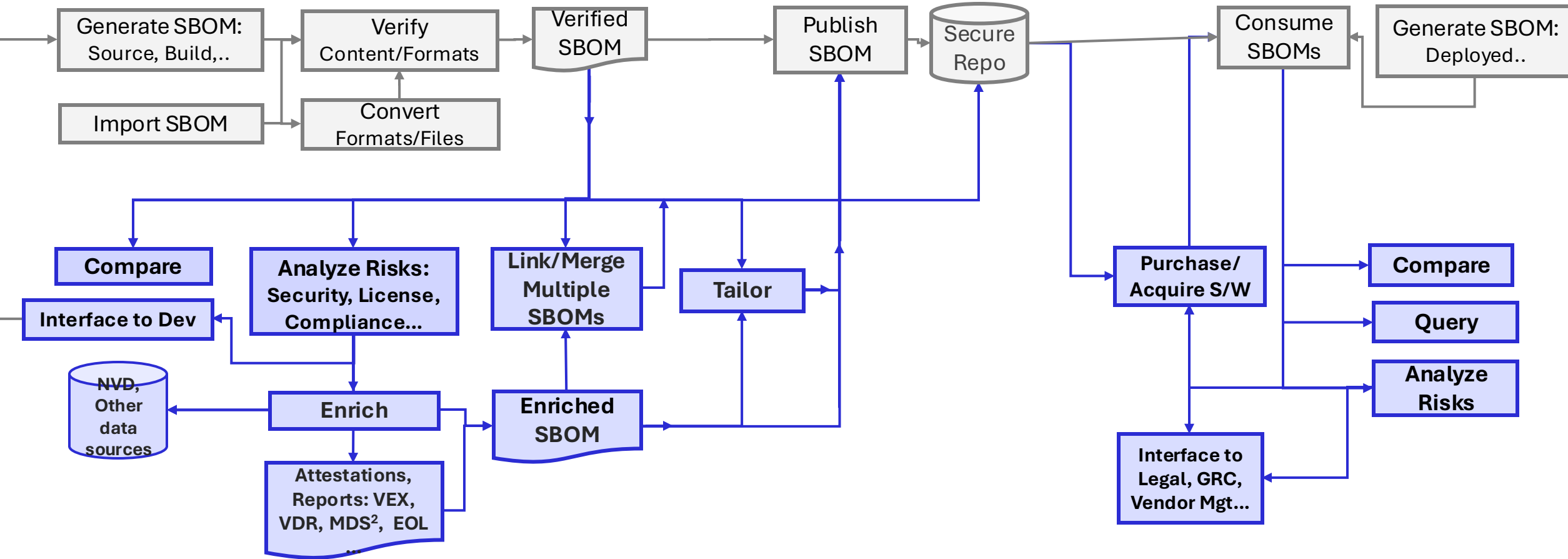


Advanced SBOM Operations

Production

Sharing

Consumption



Color Legend

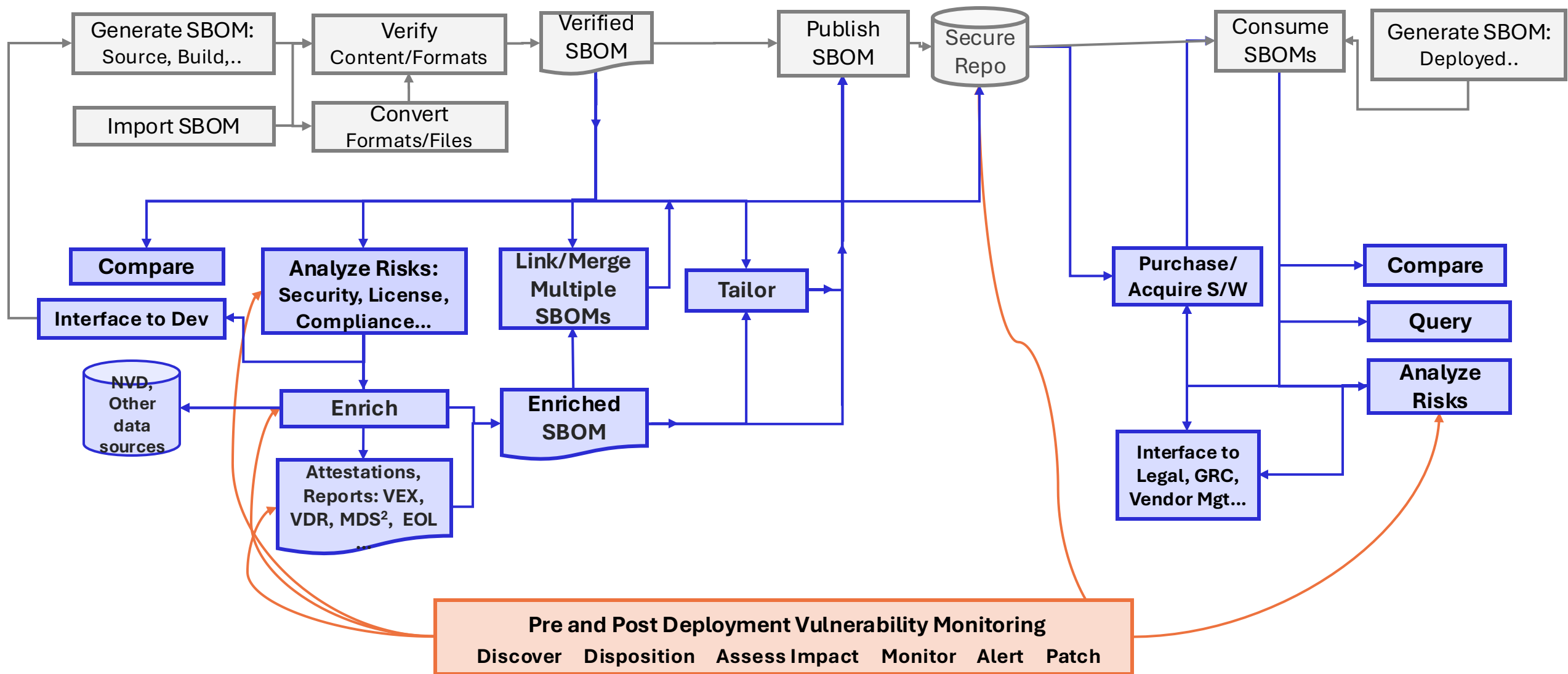
Basic SBOM Operations	Advanced SBOM Operations
-----------------------	--------------------------

Mature Operations - Continuous Vulnerability Monitoring

Production

Sharing

Consumption



Color Legend

- Basic SBOM Operations
- Advanced SBOM Operations
- Continuous Vulnerability Monitoring

Use Cases that Illustrate Insights and Value Gained from SBOM Analysis

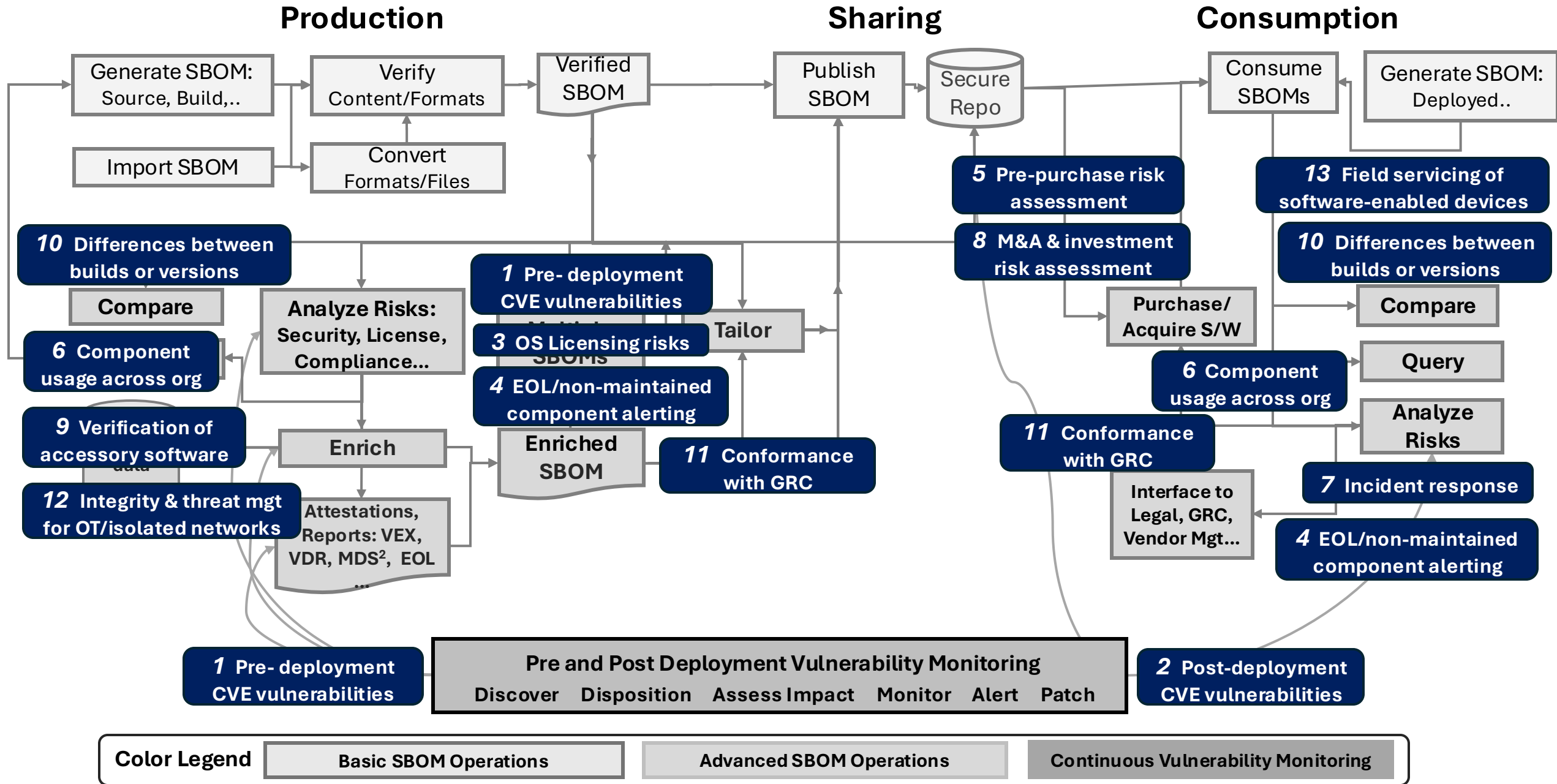
After initial SBOM generation

When linked with other data sources

13 Use Cases Covering Entire SBOM Lifecycle

Use Case #	Maturity / Applicability	Lifecycle Phase	
Most Mature / Broadest Applicability		Produce	Consume
1	Pre-Deployment CVE Risks	x	
2	Post-Deployment CVE Risks		x
3	Open Source Licensing Risks	x	x
4	EOL and Non-maintained Component Alerting	x	x
5	Pre-purchase Risk Assessment		x
6	Component Usage Across an Organization	x	x
Moderately Mature / Moderate Applicability			
7	Incident Response		x
8	M&A and Investment Risk Assessment		x
9	Verification of Accessory Software		x
10	Differences in Components Between Builds or Versions	x	x
Least Mature / Focused Applicability			
11	Conformance with Disparate GRC Specifications	x	x
12	Integrity and Threat Management for OT and isolated networks	x	
13	Field Servicing of Software-enabled Devices	x	x

Use Cases Cover the Entire SBOM Lifecycle



Deeper Dive into Four Use Cases

Use Case #1 - Pre-deployment Common Vulnerabilities and Exposures (CVE)

vulnerabilities: Discover vulnerabilities in software products before release. (Ken Z)

Use Case #5 - Pre-purchase risk assessment: Assess software for risks prior to purchase or acquisition. (Tim M)

Use Case # 7 - Incident response: Identify all applications that depend on a component involved in a security incident. (Tim M)

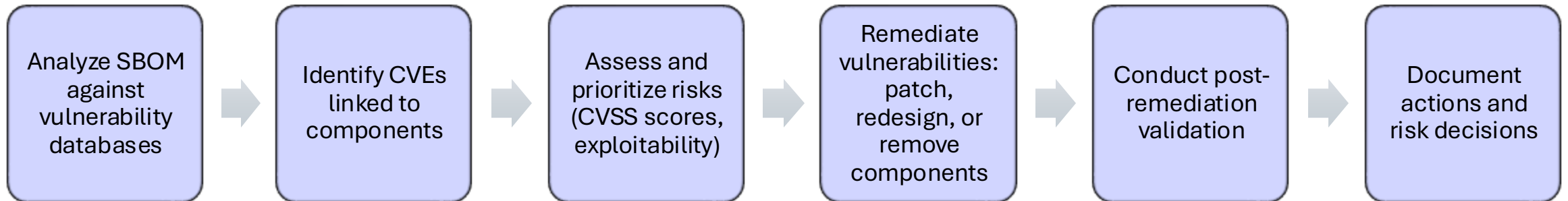
Use Case # 13 - Field servicing of software-enabled devices. To assist maintenance and troubleshooting, field service representatives compare a previously- generated SBOM of a device to data collected from an operationally deployed device. (Ken Z)

Use Case 1 – Pre-deployment vulnerabilities and exposures

Overview ♦ Identify and mitigate vulnerabilities in software components *before* product release to minimize risk, support compliance, and enhance trust.

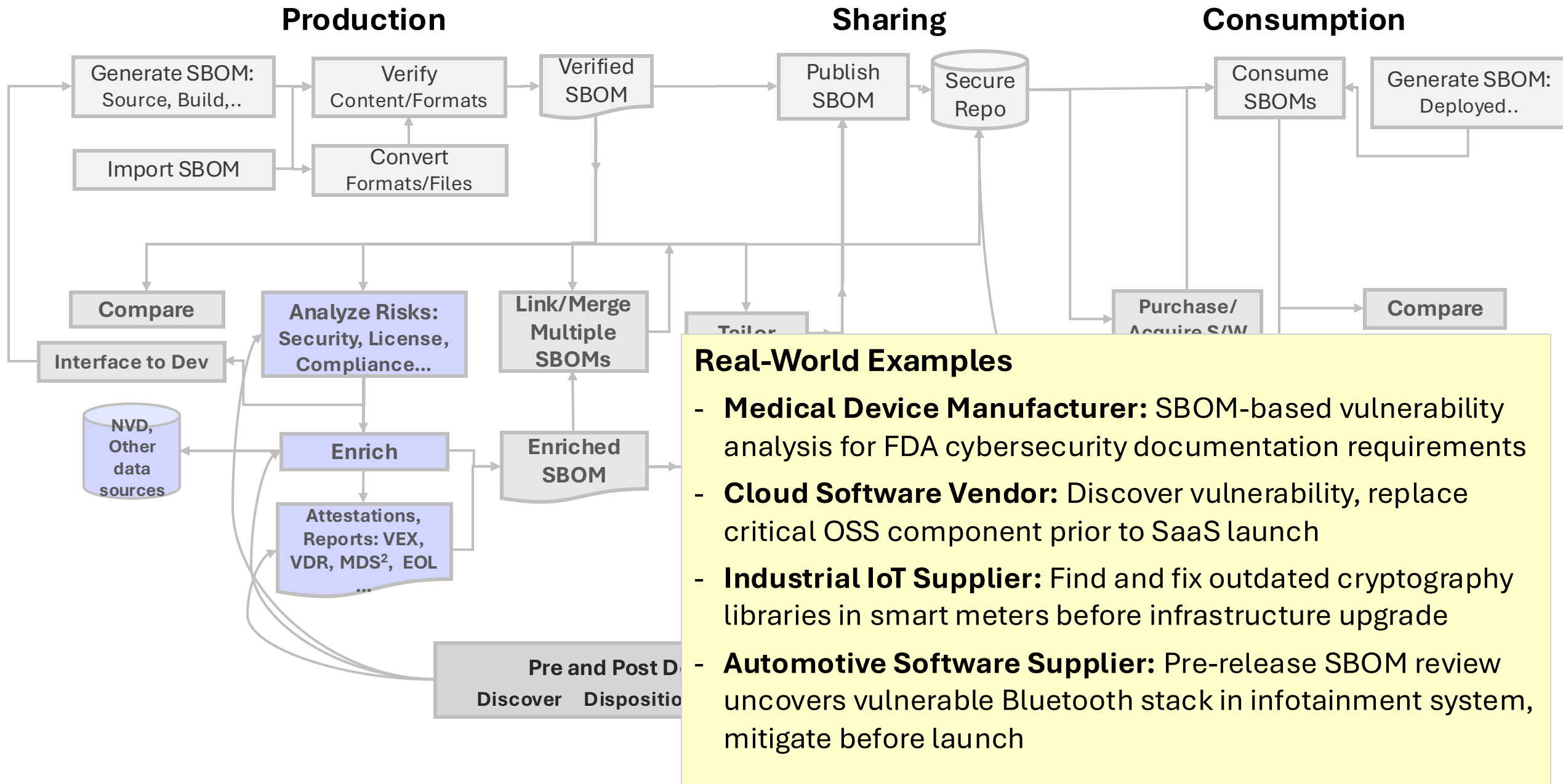
Key Actors ♦ Procurement ♦ Regulatory ♦ Engineering ♦ Product Security (PSIRT)

Process Steps



Benefits ♦ Proactively secure products before release ♦ Strengthen regulatory and customer confidence ♦ Reduce costly post-release patches and liability

Use Case 1 – Pre-deployment vulnerabilities and exposures

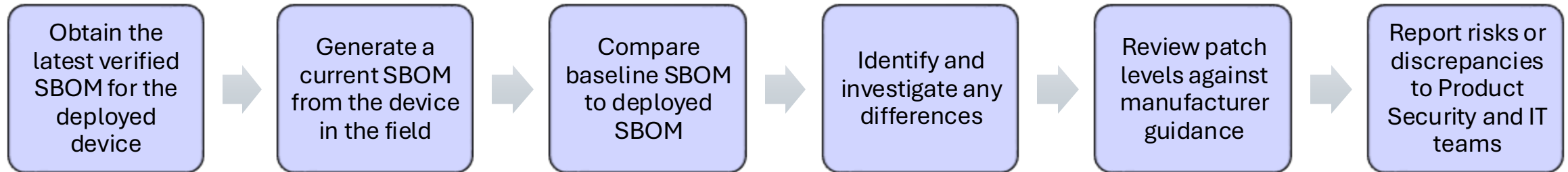


Use Case 13 – Field servicing of software-enabled devices

Overview ♦ Use SBOMs to maintain, troubleshoot, and verify deployed devices over operational life. ♦ By comparing original authorized software inventory against live environment, field teams detect unauthorized changes, assess patch status, and ensure devices remain compliant over lifetime.

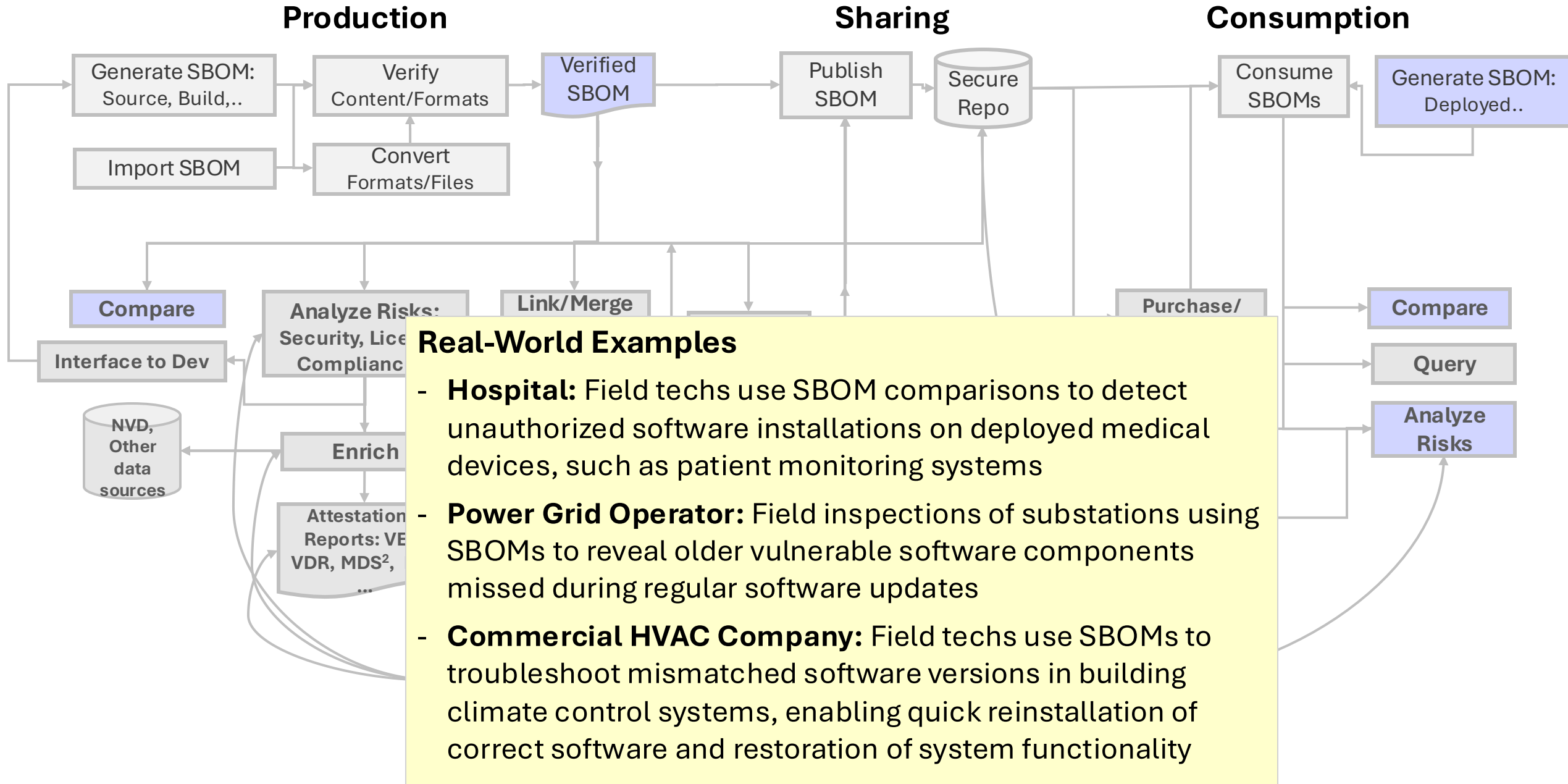
Key Actors ♦ Product Security ♦ Field Service ♦ Consumer IT ♦ Consumer Security

Process Steps



Benefits ♦ Assure device security and reliability ♦ Enable faster and more accurate field maintenance ♦ Reduce risk of unauthorized software changes

Use Case 13 – Field servicing of software-enabled devices

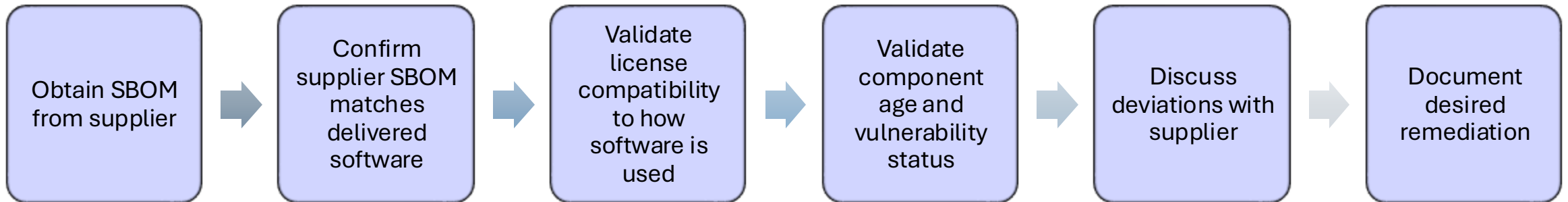


Use Case 5 – Pre-acquisition/purchase risk assessment

Overview ♦ Avoid introduction of new security, compliance, or supportability risks from software that is being considered for purchase or acquisition

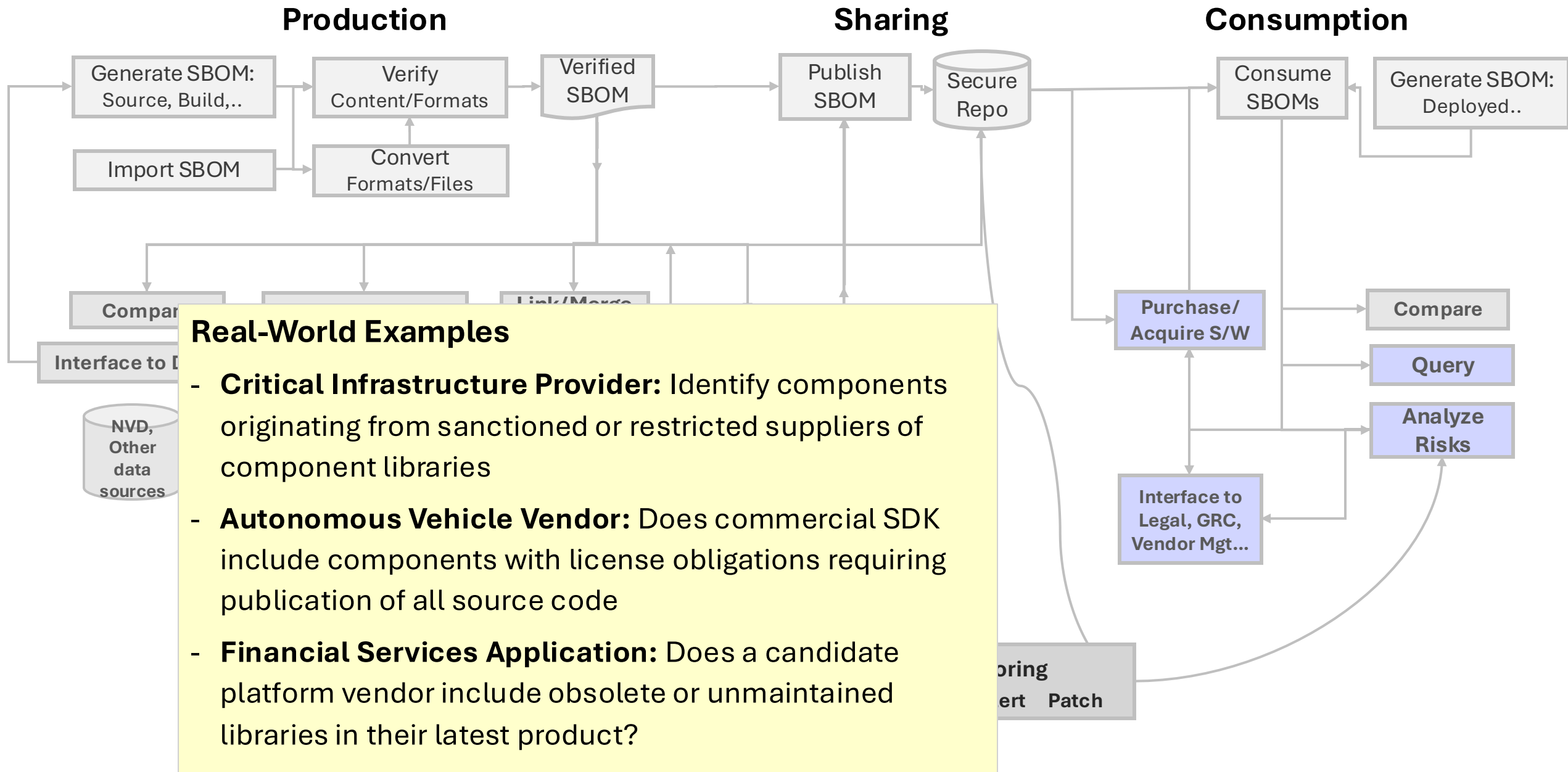
Key Actors ♦ Procurement ♦ Risk and Compliance ♦ Legal ♦ Security Teams

Process Steps



Benefits ♦ Have risk-mitigating discussions with suppliers ♦ Cross functional sharing of risk assessments ♦ Empower procurement in cyber risk mitigation

Use Case 5 – Pre-acquisition/purchase risk assessment

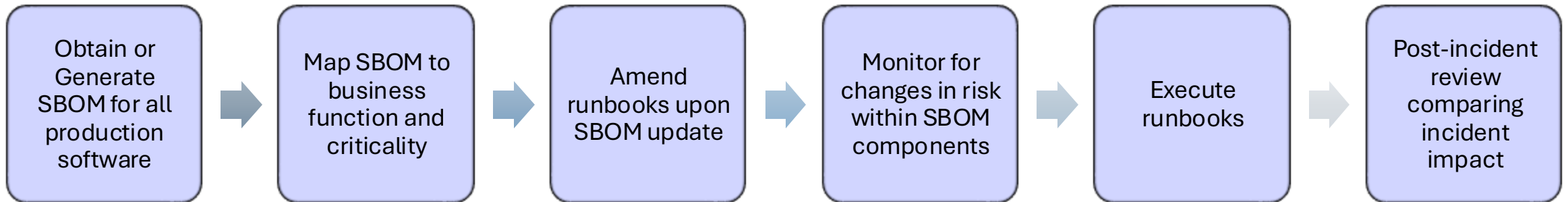


Use Case 7 – Incident response

Overview ♦ Enhance incident response processes by enabling faster identification, containment, and remediation of incidents (e.g. Log4J)

Key Actors ♦ IT/DevSecOps ♦ Risk and Compliance ♦ Legal ♦ Engineering

Process Steps



Benefits ♦ Reduce MTTI/MTTR ♦ Reduce blind spots ♦ Enable strategic remediation planning

NTIA Minimum Fields Needed for Use Cases

NTIA Minimum Fields Used

Use Case	Supplier	Component	Version	Other Unique IDs	Dependency Relationship	Author	Timestamp
1. Pre-deployments CVE vulnerabilities	✓	✓	✓	✓	✓		
5. Pre-purchase risk assessment	✓	✓	✓	✓	✓	✓	✓
7. Incident response	✓	✓	✓	✓		✓	✓
13. Field servicing of software devices	✓	✓	✓	✓	✓	✓	✓

Key Take-aways

- **Many different stakeholders** analyze SBOMs across the lifecycle
 - Software Producers, Distributors and Consumers
 - Engineering, Security, Regulatory, Procurement, Legal, IT, Vendor Management
- Because SBOM data is re-used across the lifecycle, operational efficiencies can be gained with a **centralized SBOM inventory**
- Use cases correlate **additional data** with SBOMs to meet objectives
 - Most common data: **Vulnerabilities, Licenses, Sanctioned Entities, EOL/EOS**
 - SBOM-drive workflows reduce **security, licensing, compliance and maintainability** risks
- SBOM lifecycle management is becoming a specialized practice
 - Many opportunities for automation and expansion

Acknowledgements

Authors

Bunny Hernández Banowsky (SHE BASH)
Anita D'Amico (Cotopaxi Consulting,
Vigilant Ops)
Ian Dunbar-Hall (Lockheed Martin)
Bill Hansen (Hansen Enterprises LLC)
JC Herz (Exiger)
Nisha Kumar (Oracle)
Tim Mackey (Black Duck)
Mike Lieberman (Kusari)
Victoria Ontiveros (CISA)
Anusha Penumacha (Splunk)
Ricardo Reyes (Chainguard)
Ken Zalevsky (Vigilant Ops)

Designated Technical Reviewers

Bunny Hernández Banowsky (SHE BASH)
Cassie Crossley (Schneider Electric)
Anita D'Amico (Cotopaxi Consulting,
Vigilant Ops)
JC Herz (Exiger)
Nisha Kumar (Oracle)
Tim Mackey (Black Duck)
Mike Lieberman (Kusari)
Bob Martin (MITRE)
John Nuckles (ODNI)
Victoria Ontiveros (CISA)
Kayra Otaner (Roche)
Animesh Pattanayak (PNNL)
Vijaya Ramamurthi (Accenture Federal
Services)
Ricardo Reyes (Chainguard)
Ria Schalnat (HPE)
Anant Shrivastava (Cyfinoid Research)
Gaurav Srivastava (Siemens)
Ken Zalevsky (Vigilant Ops)

Other Contributors

Ralph Bean (Red Hat)
John Cavanaugh (ProCap360)
Brindusa Curcaneanu
(NeuroPace)
Anthony Harrison (APH10)
Charlie Hart (Hitachi America,
Ltd.)
Syed Zaeem Hosain (Aeris
Communications, Inc.)
Philippe Ombredanne
(AboutCode.org, Package-URL,
and nexB Inc.)
Melissa Rhodes (Medtronic)
Duncan Sparrell (sFractal)

PRESENTERS



Anita D'Amico, Ph.D.
President, Cotopaxi Consulting
Board Member, Vigilant Ops
anitacodedx@gmail.com
[linkedin.com/in/anita-damico/](https://www.linkedin.com/in/anita-damico/)
www.cotopaxiconsulting.com



Tim Mackey
Head of Software Supply Chain Strategy
Black Duck, Inc.
tmackey@blackduck.com
[linkedin.com/in/mackeytim/](https://www.linkedin.com/in/mackeytim/)
www.blackduck.com



Ken Zalevsky
CEO
Vigilant Ops, Inc.
ken.zalevsky@vigilant-ops.com
[linkedin.com/in/ken-zalevsky/](https://www.linkedin.com/in/ken-zalevsky/)
www.vigilant-ops.com