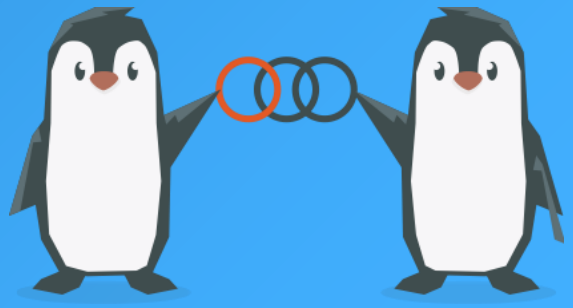
Overview of various regulations and guidelines, and What is needed for future discussion

SBOM Study Group, OpenChain Project
2024-10-23

THE LINUX FOUNDATION

OPENCHAIN



Laws, Regulations, Standards, Guidelines

Official Document

- E.O. 14028
- CRA
- NTIA Minimum Elements for SBOM
- BSI TR-03183-2 v2.0.0
- Medical Device (FDA)
- CISA Framing Third Edition
- METI Guide v2.0

Process Management

- ISO/IEC 5230
- ISO/IEC 18974

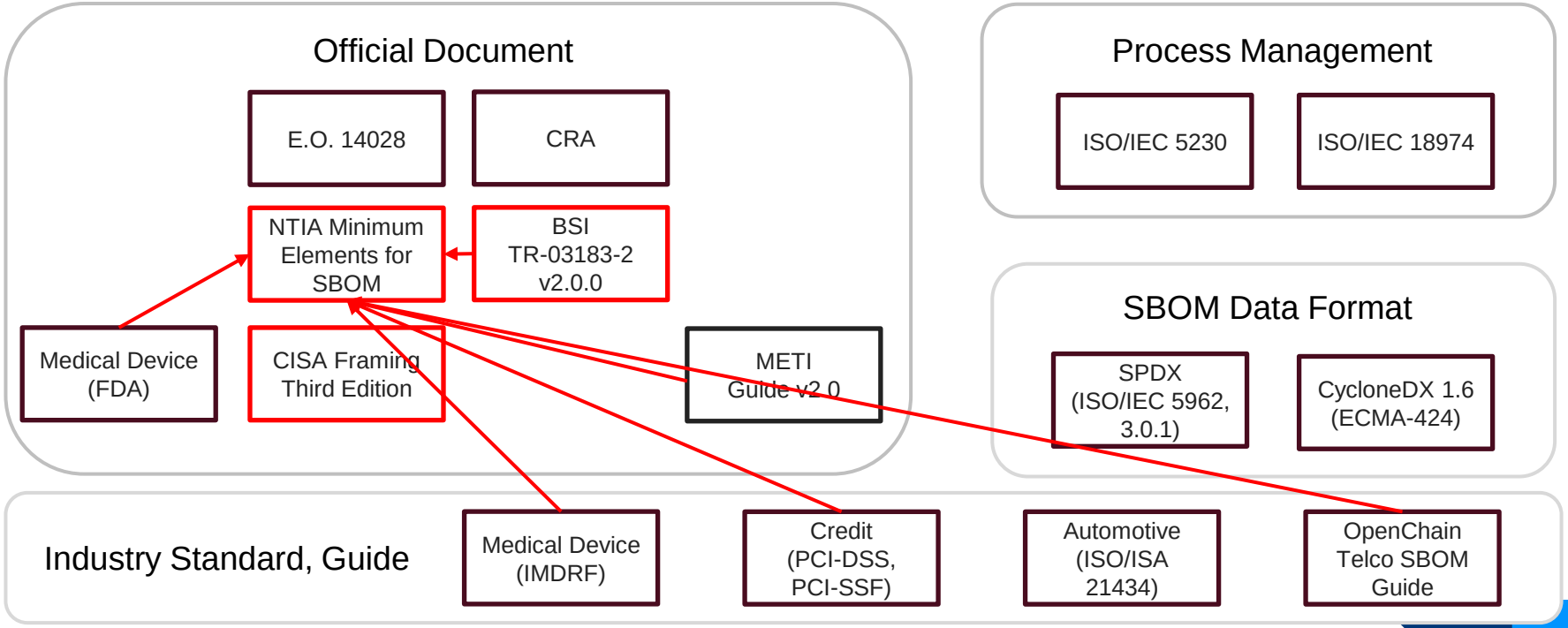
SBOM Data Format

- SPDX (ISO/IEC 5962, 3.0.1)
- CycloneDX 1.6 (ECMA-424)

Industry Standard, Guide

- Medical Device (IMDRF)
- Credit (PCI-DSS, PCI-SSF)
- Automotive (ISO/ISA 21434)
- OpenChain Telco SBOM Guide

NTIA Minimum Elements as a Reference



CISA Framing: providing updates from a practical perspective

NOT REPLACE NTIA Minimum Elements

NTIA.
"Minimum Elements for a Software Bill of Materials (SBOM). July, 2021

CISA.
Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Third Edition. October, 2024

NTIA Minimum Elements	CISA Baseline Attributes
Author of SBOM Data	**SBOM Author Name**
Timestamp	**SBOM Timestamp**
	SBOM Type
Supplier Name	**Component Supplier Name**
Component Name	**Component Name**
Version of the Component	**Component Version String**
Unique Identifiers	**Component Unique Identifier**
Component Hash	**Component Cryptographic Hash**
License Information	**Component License**
Copyright Information	**Component Copyright Holder**
Dependency Relationship	**SBOM Primary Component**
	Component Relationships
External Data	

THE LINUX FOUNDATION

OPENCHAIN

[WIP] SBOM element comparison (Updating in consideration of CISA Framing Third Edition and BSI TR-03183-2 v2.0.0)
https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1667652967#gid=1667652967

Attributes Comparison (Overview)

NTIA Mnimum Elements	CISA Baseline Atrributes	BSI TR-03183-2	IMDRF/FDA	PCI-DSS/PCI-SSF	OpenChain Telco SBOM guide
		SBOM-URI			(6.5) SPDX Document Namespace
Author of SBOM Data	SBOM Author Name	Creator of the SBOM	Author name	The name of the author who designed/developed the component or service.	(6.8) Creator
Timestamp	SBOM Timestamp	Timestamp	Timestamp		(6.9) Created
Lifecycle Phase	SBOM Type (Optional: Aspiration)	(assuemed Build SBOM)			(6.10) Creator comment
Dependency Relationship	SBOM Primary Component	(primary component)	Relationship	A description of the relationship(s) between the component and service and other components/services embedded in or used by the software.	(11.1) Relationship: DESCRIBES
Component Name	Component Name	Component name	Software component name	The name of the component or service as defined by the original supplier.	(7.1) Package Name
Version of the Component	Component Version String	Component version	Software component version	The version of the component or service as defined by the original supplier to differentiate it from previous or other versions.	(7.3) Package Version
Supplier Name	Component Supplier Name	Component creator	Software component vendor (supplier)	The original source/supplier of the component or service.	(7.5) Package Supplier
Component Hash	Component Cryptographic Hash	Hash value of the executable component (Optional: Hash value of the source code of the component)	Component Hash		(7.10) Package Checksum
		Filename of the component			(NEED TO DISCUSS)
Other Unique Identifiers	Component Unique Identifier	Other unique identifiers	Unique Identifier	Any other identifiers provided by the original	(7.2) Package SPDX Identifier (6.5) SPDX Document Namespace (7.21) External Reference field
Dependency Relationship	Component Relationships	Dependencies on other components	Relationship	A description of the relationship(s) between the component and service and other components/services embedded in or used by the software.	(11.1) Relationship: CONTAINS
		-Executable property: “executable” and “non-executable” -Archive property: “archive” and “no archive” -Structured property: “structured” and “unstructured”;			(NEED TO DISCUSS)
		Source code URI URI of the deployable form of the component			(7.7) Package Download Location (7.21) External Reference field
		Associated licences			
License Information	Component License (Aspiration: Concluded)	Concluded Licences (Optional: Declared licences)	FDA: Licence		(7.13) Concluded License (7.15) Declared License
License Information(Copyright)	Component Copyright Holder	(Not mentioned clearly, but assumed)			(7.17) Copyright Text
Other Component Relationships	Component Relatuionships (Heritage or Pedigree Relationship)				(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		FDA: Software level of support		(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		- FDA: End-of-support date. - IMDRF: Life cycle of a device (e.g., a software component’s end-of-support (EOS) date)		(NEED TO DISCUSS)

[WIP] SBOM element comparison (Updating in consideration of CISA Framing Third Edition and BSI TR-03183-2 v2.0.0)
https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1667652967#gid=1667652967

Baseline Attributes Comparison

NTIA Mnimum Elements	CISA Baseline Atrributes	BSI TR-03183-2	IMDRF/FDA	PCI-DSS/PCI-SSF	OpenChain Telco SBOM guide
Author of SBOM Data	SBOM Author Name	Creator of the SBOM	(+)	(+)	(6.8) Creator
Timestamp	SBOM Timestamp	Timestamp	(+)		(6.9) Created
Lifecycle Phase	SBOM Type (Optional: Aspiration)	(assuemed Build SBOM)			(6.10) Creator comment
Dependency Relationship	SBOM Primary Component	(primary component)	(+)	(+)	(11.1) Relationship: DESCRIBES
Component Name	Component Name	Component name	(+)	(+)	(7.1) Package Name
Version of the Component	Component Version String	Component version	(+)	(+)	(7.3) Package Version
Supplier Name	Component Supplier Name	Component creator	(+)	(+)	(7.5) Package Supplier
Component Hash	Component Cryptographic Hash	Hash value of the executable component (Optional: Hash value of the source code of the component)	(+)		(7.10) Package Checksum
Other Unique Identifiers	Component Unique Identifier	Other unique identifiers	(+)	(+)	(7.2) Package SPDX Identifier (6.5) SPDX Document Namespace (7.21) External Reference field
Dependency Relationship	Component Relationships	Dependencies on other components	(+)	(+)	(11.1) Relationship: CONTAINS
License Information	Component License (Aspiration: Concluded)	Concluded Licences (Optional: Declared licences)	FDA: Licence		(7.13) Concluded License (7.15) Declared License
License Information(Copyright)	Component Copyright Holder	(Not mentioned clearly, but assumed)			(7.17) Copyright Text
Other Component Relationships	Component Relatuionships (Heritage or Pedigree Relationship)				(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		FDA: Software level of support		(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		- FDA: End-of-support date. - IMDRF: Life cycle of a device (e.g., a software component's end-of-support (EOS) date)		(NEED TO DISCUSS)

[WIP] SBOM element comparison (Updating in consideration of CISA Framing Third Edition and BSI TR-03183-2 v2.0.0)
https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1667652967#gid=1667652967

Baseline Attributes Comparison

NTIA Mnimum Elements	CISA Baseline Atrributes	BSI TR-03183-2	IMDRF/FDA	PCI-DSS/PCI-SSF	OpenChain Telco SBOM guide
Author of SBOM Data	SBOM Author Name	Creator of the SBOM	(+)	(+)	(6.8) Creator
Timestamp	SBOM Timestamp	Timestamp	(+)		
Lifecycle Phase	SBOM Type (Optional: Aspiration)	(assuemed Build SBOM)			mment
Dependency Relationship	SBOM Primary Component	(primary component)	(+)		p: DESCRIBES
Component Name	Component Name	Component name	(+)		me
Version of the Component	Component Version String	Component version	(+)		rsion
Supplier Name	Component Supplier Name	Component creator	(+)		pplier
Component Hash	Component Cryptographic Hash	Hash value of the executable cor (Op coc			hecksum
Other Unique		Oth			DX Identifier ment Namespace eference field
Dependency		Dep			p: CONTAINS
License Information	(Aspiration: Concluded)	Cor (Op			License icense
License Information(Copyright)	Component Copyright Holder	(Not mentioned clearly, but assumed)			(7.17) Copyright Text
Other Component Relationships	Component Relatuionships (Heritage or Pedigree Relationship)				(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		FDA: Software level of support		(NEED TO DISCUSS)
	Supplemental Information to Support Use Cases		- FDA: End-of-support date. - IMDRF: Life cycle of a device (e.g., a software component's end-of-support (EOS) date)		(NEED TO DISCUSS)

(11.1) Relationship: GENERATED_FROM
(11.1) Relationship: DESCENDANT_OF

One of the following comment data fields containing specific text:
1. "(6.4) Document name"; or
2. "(6.10) Creator comment"; or
3. "(6.11) Document Comment", or
4. "(7.20) Package Comment"

In SPDX-2.3:
7.27 Valid Until Date

In SPDX-2.2:
One of the following comment data fields containing specific text:
1. "(6.4) Document name"; or
2. "(6.10) Creator comment"; or
3. "(6.11) Document Comment", or
4. "(7.20) Package Comment"

[WIP] SBOM element comparison (Updating in consideration of CISA Framing Third Edition and BSI TR-03183-2 v2.0.0)
https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1667652967#gid=1667652967

BSI Only Attributes

NTIA Mnimum Elements	CISA Baseline Atrributes	BSI TR-03183-2	IMDRF/FDA	PCI-DSS/PCI-SSF	OpenChain Telco SBOM guide
		SBOM-URI			(6.5) SPDX Document Namespace
		Filename of the component			(NEED TO DISCUSS)
		-Executable property: "executable" and "non-executable" -Archive property: "archive" and "no archive" -Structured property: "structured" and "unstructured";			(NEED TO DISCUSS)
		Source code URI URI of the deployable form of the component			(7.7) Package Download Location (7.21) External Reference field
		Associated licences			(NEED TO DISCUSS)

[WIP] SBOM element comparison (Updating in consideration of CISA Framing Third Edition and BSI TR-03183-2 v2.0.0)
https://docs.google.com/spreadsheets/d/1SuGv1L3H_-Iq6dmH7DnjDgAa90LCRnoHB3DTfuWh0Jg/edit?gid=1667652967#gid=1667652967

BSI Only Attributes

(7.4) PackageFileName

NTIA Mnimum Elements	CISA Baseline Atrributes	BSI TR-03183-2	IMDRF/FDA	PCI-DSS/PCI-SSF	OpenChain Telco SBOM guide
		SBOM-URI			(6.5) SPDX Document Namespace
		Filename of the component			(NEED TO DISCUSS)
		-Executable property: “executable” and “non-executable” -Archive property: “archive” and “no archive” -Structured property: “structured” and “unstructured”.			(NEED TO DISCUSS)
		Source code URI URI of the deployable form of the component			(7.7) Package Download Location (7.21) External Reference field
		Associated licences			(NEED TO DISCUSS)

(7.20) PackageComment:

May not meet this requirement:
SPDX 2.3
(7.24)PrimaryPackagePurpose

(7.14) PackageLicenseInfoFromFiles

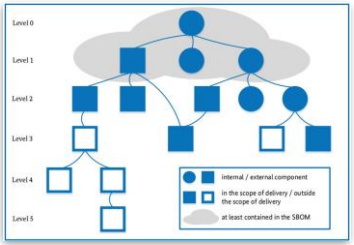
CISA. “Maturity Levels”:
Mixture of “depth and breadth (of dependencies)” and “attributes levels”

Maturity Level	2.2. Baseline Attributes
Minimum Expected	This maturity level describes the minimum data elements for documenting a Primary Component and its Included Components for SBOMs globally.
Recommended Practice	This maturity level describes the addition of Attribute data that supplements Component identification as well as practices for creating SBOMs.
Aspiration Goal	This maturity level describes areas that creators of SBOMs can consider for documenting dynamic and/or remote Dependencies (see Appendix B for descriptions) that can be uniquely and unambiguously identified in an SBOM.

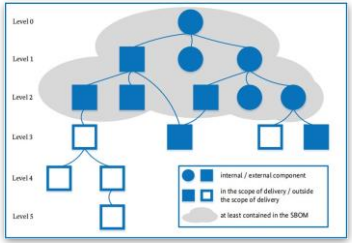
2.2 Baseline Attributes
2.2.1.1 Author Name
2.2.1.2 Timestamp
2.2.1.3 Type
2.2.1.4 Primary Component (or Root of Dependencies)
2.2.2 Component Attributes
2.2.2.1 Component Name
2.2.2.2 Version
2.2.2.3 Supplier Name
2.2.2.4 Unique Identifier
2.2.2.5 Cryptographic Hash
2.2.2.6 Relationship
2.2.2.6.1 Primary Relationship
2.2.2.6.2 “Included In” Relationship
2.2.2.6.3 Heritage or Pedigree Relationship
2.2.2.6.4 Relationship Completeness
2.2.2.7 License
2.2.2.8 Copyright Notice
2.3 Undeclared SBOM Data
2.3.1 Unknown Component Attributes
2.3.2 Redacted Components
2.3.3 Unknown Dependencies
2.4 Supplemental Information to Support Use Cases
3.6.1 Vulnerability Management and VEX
Appendix B Terminology: Attributes
Appendix B Terminology: Component
Appendix B Terminology: Dependency
Appendix B Terminology: Included Component
Appendix B Terminology: Software Bill of Materials (SBOM)

CISA. “Maturity Levels” vs. BSI. “Level of Details”

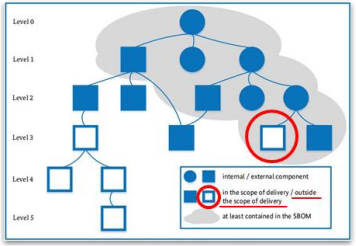
Maturity Level	2.2.2.6 Relationship
Minimum Expected	Relationships and relationship completeness declared for the Primary Component and direct Dependencies.
Recommended Practice	Relationships and relationship completeness declared for all Included Components listed in the SBOM.
Aspiration Goal	Relationships and relationship completeness to as many dynamic and remote Components as possible (e.g., loaded Components or services) are identified.



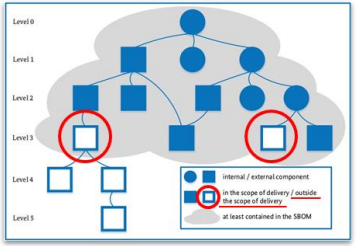
Top-level SBOM



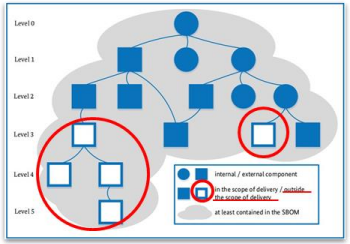
n-level SBOM



Transitive SBOM



Delivery item SBOM



Complete SBOM

THE LINUX FOUNDATION

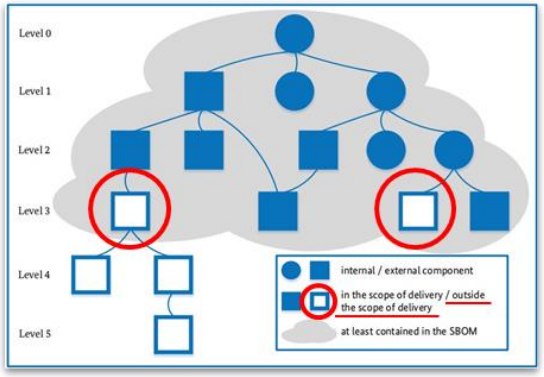
OPENCHAIN

Relationship resolution: CISA vs. BSI

Maturity Level	2.2.2.6 Relationship
Minimum Expected	Relationships and relationship completeness declared for the Primary Component and direct Dependencies.
Recommended Practice	Relationships and relationship completeness declared for all Included Components listed in the SBOM.
Aspiration Goal	Relationships and relationship completeness to as many dynamic and remote Components as possible (e.g., loaded Components or services) are identified.

BSI.
5.1 Level of detail

For an SBOM that is compliant with this Technical Guideline, recursive dependency resolution MUST be performed at least for each component included in the scope of delivery on each path downward at least up to and including the first component that is outside the scope of delivery (see Annex, section 8.2.4).



THE LINUX FOUNDATION
OPENCHAIN

SBOM Type: At least “Build SBOM” ?

CISA.
2.2.1.3 Type

The Type Attribute provides context for how and why the SBOM was created. As discussed in Section 2 (see footnote 8), different types of SBOMs can be created from different software artifacts. Documenting the SBOM Type may inform the utility and consumption of the SBOM that was created. This Attribute is optional and considered an aspirational goal.

BSI.
5.1 Level of detail

This SBOM MUST contain the same information as available during the build process or equivalent information where the build process does not exist (for details related to Build SBOM, see Annex, section 8.3.3).

8.3.3 Build SBOM
The SBOM is created as part of the build process based on e.g. source files, dependency information, already created components, volatile build process data and other SBOMs.
Notes:

- In order to enable capturing executable, binary components that already exist (i.e. precompiled code), creating a Build SBOM focuses on the linker run for translated code, not the compiler run.
- In order to let hash values unambiguously identify components, reproducible builds have to be employed.
- In the case of interpreted code, only the source code exists; each executable file has to be listed as a component. The interpreter has to be specified as a dependency, as far as reasonably possible.

SBOM Type: At least “Build SBOM” ?

CISA.
2.2.1.3 Type

The Type Attribute provides context for how and why the SBOM was created. As discussed in Section 2 (see footnote 8), different types of SBOMs can be created from different software artifacts. Documenting the SBOM Type may inform the utility and consumption of the SBOM that was created. This Attribute is optional and considered an aspirational goal.

- “Type” information is Optional for “Aspiration”
- “Aspiration” wants “remote”

“Build SBOM” is assumed

BSI.
5.1 Level of detail

This SBOM MUST contain the same information as available during the build process or equivalent information where the build process does not exist (for details related to Build SBOM, see Annex, section 8.3.3).

8.3.3 Build SBOM
The SBOM is created as part of the build process based on e.g. source files, dependency information, already created components, volatile build process data and other SBOMs.
Notes:
- In order to enable capturing executable, binary components that already exist (i.e. precompiled code), creating a Build SBOM focuses on the linker run for translated code, not the compiler run.
- In order to let hash values unambiguously identify components, reproducible builds have to be employed.
- In the case of interpreted code, only the source code exists; each executable file has to be listed as a component. The interpreter has to be specified as a dependency, as far as reasonably possible.

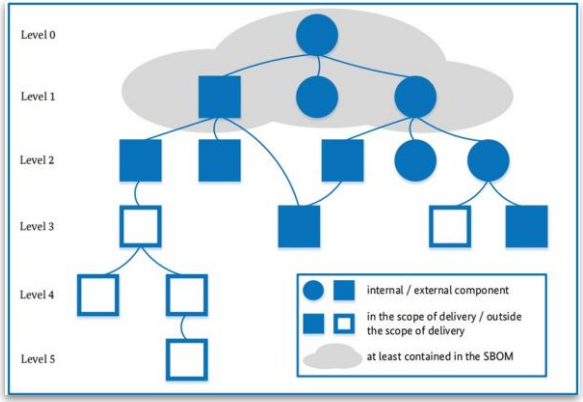
CISA. “Maturity Levels” vs. BSI. “Level of Details”

CISA. “Minimum Expected”

Relationships and relationship completeness declared for the Primary Component and direct Dependencies.

BSI. “Top-level SBOM”

In addition to the full description of the primary component, the SBOM contains the full description of all components, which the primary component directly depends on.



THE LINUX FOUNDATION
OPENCHAIN

CISA. “Maturity Levels” vs. BSI. “Level of Details”

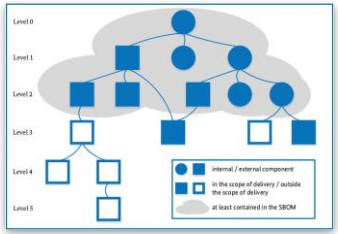
CISA. “Recommended Practice”

Relationships and relationship completeness declared for all Included Components listed in the SBOM.

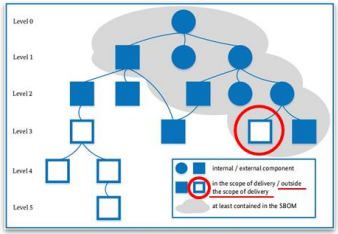
Included Component
An Included Component is any Component that is in the distributed software (e.g., masked layers within a container of an image).
cf. Appendix B Terminology

BSI.

“n-level”

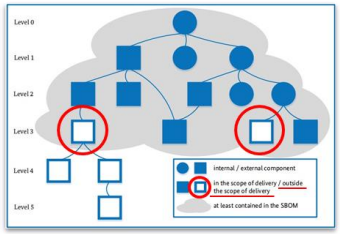


“Transitive”



at least up to and including the first external component (i.e. third-party component)

“Delivery item”



including the first component, which is outside the scope of delivery

3.2.2 External component
An “external component” is a component whose component creator differs from the component creator of the primary component.

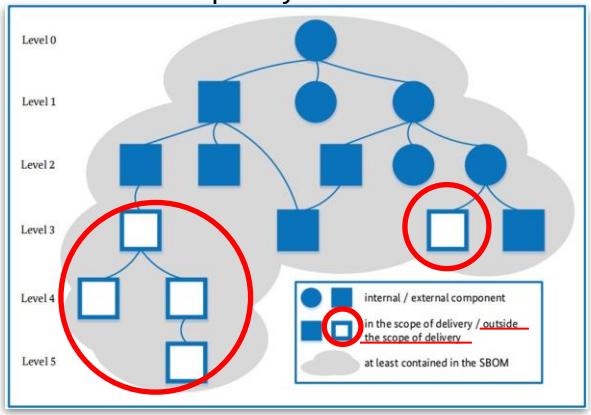
CISA. “Maturity Levels” vs. BSI. “Level of Details”

CISA. “Aspiration Goal”

Relationships and relationship completeness to as many dynamic and remote Components as possible (e.g., loaded Components or services) are identified.

BSI. “Complete SBOM”

In addition to the full description of the primary component, the SBOM contains the full description of all components, which are directly or transitively depended upon by the primary component. The full description and recursive resolution of the components and their dependencies is carried out completely.



THE LINUX FOUNDATION

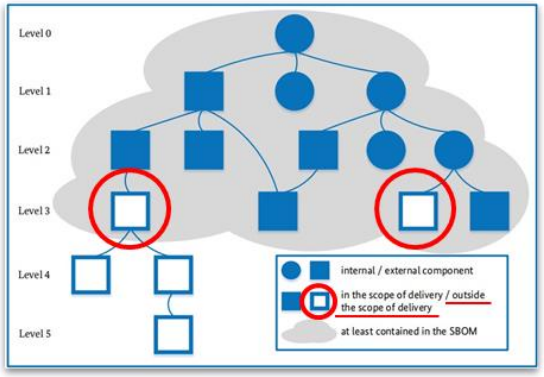
OPENCHAIN

AGAIN: Relationship resolution: CISA vs. BSI

Maturity Level	2.2.2.6 Relationship
Minimum Expected	Relationships and relationship completeness declared for the Primary Component and direct Dependencies.
Recommended Practice	Relationships and relationship completeness declared for all Included Components listed in the SBOM.
Aspiration Goal	Relationships and relationship completeness to as many dynamic and remote Components as possible (e.g., loaded Components or services) are identified.

BSI.
5.1 Level of detail

For an SBOM that is compliant with this Technical Guideline, recursive dependency resolution MUST be performed at least for each component included in the scope of delivery on each path downward at least up to and including the first component that is outside the scope of delivery (see Annex, section 8.2.4).



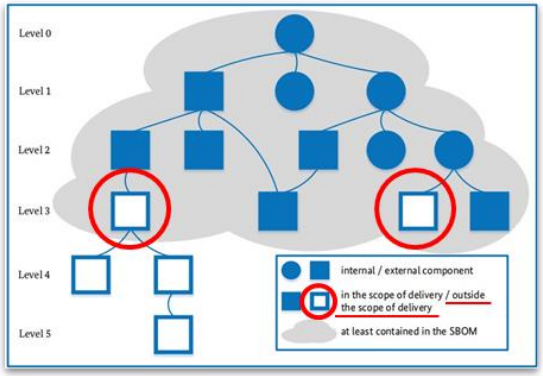
AGAIN: Relationship resolution: CISA vs. BSI

Maturity Level	2.2.2.6 Relationship
Minimum Expected	Relationships and relationship completeness declared for the Primary Component and direct Dependencies.
Recommended Practice	Relationships and relationship completeness declared for all Included Components listed in the SBOM.
Aspiration Goal	Relationships and relationship completeness to as many dynamic and remote Components as possible (e.g., loaded Components or services) are identified.

- "Aspiration" wants "remote"
- No Levels mention "outside the scope of delivery"

BSI.
5.1 Level of detail

For an SBOM that is compliant with this Technical Guideline, recursive dependency resolution MUST be performed at least for each component included in the scope of delivery on each path downward at least up to and including the first component that is outside the scope of delivery (see Annex, section 8.2.4).



- No mention about "remote"
- Outside the scope of delivery

THE LINUX FOUNDATION
OPENCHAIN

CISA “License” vs. BSI. “Associated licences” et al.

Maturity Level	2.2.2.7 License
Minimum Expected	Provide license information for the Primary Component.
Recommended Practice	Provide license information for as many Components as possible.
Aspiration Goal	Provide license information for all listed SBOM Components. Attestation of Concluded License information, i.e., license text and concluded terms and conditions, is included in the SBOM.

Concluded License
Frequently multiple licenses may be found in a Component that have different constraints. After resolving the conditions an overall license for the Component can be declared by the SBOM Supplier.

cf. Appendix B Terminology

BSI.

5.2.2 Required data fields for each component Associated licences
Associated licence(s) of the component from the perspective of the SBOM creator. For specifics see sections 6.1 and 8.1.9.

5.3.2 Additional data fields for each component Concluded licences
The licence(s) that the licensee of the component has concluded for this component. For specifics see sections 6.1 and 8.1.9

5.4.1 Optional data fields for each component Declared licences
The licence(s) that the licensor of the component has declared for this component. For specifics see sections 6.1 and 8.1.9.

Hash algorithms: SHA256 or SHA512?

Maturity Level	2.2.2.5 Cryptographic Hash
Minimum Expected	Hash algorithms accepted at this maturity level are MD5, SHA1, and SHA2 families, (including SHA256 and SHA512). Using a secure hash algorithm is recommended. Note that use of MD5 and SHA1 is no longer recommended and will be formally discontinued in 2030.
Recommended Practice	Hash algorithms accepted at this maturity level are those that are cryptographically secure SHA2 family (SHA-256 and higher) for all Components and system Dependencies listed in an SBOM. If less cryptographically secure, hashes need to be included, adding an additional cryptographically secure hash is required.
Aspiration Goal	(N/A) (SBOM-SG Note: same as Recommended Practice)

BSI.

5.2.2 Required data fields for each component
Hash value of the deployable component
Cryptographically secure checksum (hash value) of the deployed/deployable component (i.e. as a file on a mass storage device) as SHA-512; see also section 3.2.1.

SBOM and CSAF (VEX) should be used separately?

CISA.
3.6.1 Vulnerability Management and VEX

(Third paragraph)
Vulnerability management requires sources of vulnerability information (such as CVE, security advisories from Suppliers, [e.g. in CSAF, and the NVD]), mapping of vulnerabilities to Components (such as CPE as used in the NVD), and a way to convey vulnerability or exploitability status (such as VEX). While VEX was developed to address the vulnerability management use case, VEX is not limited to use with SBOMs nor expected to be included in the SBOM itself.

(Last paragraph)
Additionally, including the end-of-life date and level-of-support for the Components as supplemental to the SBOM provides the entity performing an impact assessment of a vulnerability with crucial information for mitigation options.

BSI.
1 Introduction

(Third paragraph)
SBOM information can be used to check whether a product is potentially affected by a vulnerability by comparing its component list with the components listed in a vulnerability database. However, an SBOM does not contain any statement regarding vulnerabilities or their exploitability.

8.1.10 Vulnerability information

The SBOM definition in this Technical Guideline states that vulnerability information is not contained in an SBOM. Information on vulnerabilities of a certain version of a software changes over time while the crucial information of an SBOM (e.g. on dependencies) is static. If vulnerability information is included in an SBOM, this static data is unnecessarily propagated along the software supply chain in unaltered form each time the vulnerability information is updated. Consequently, it is required not to include vulnerability information in an SBOM, even though an SBOM format specification supports that. The recommended format for distributing vulnerability information is CSAF (including also VEX as a profile).

End of X:
Just Optional

CISA.
2.4 Supplemental Information to Support Use Case

(Second paragraph)
Examples of supplemental Attributes:

- End-of-life date or level-of-support for Components.

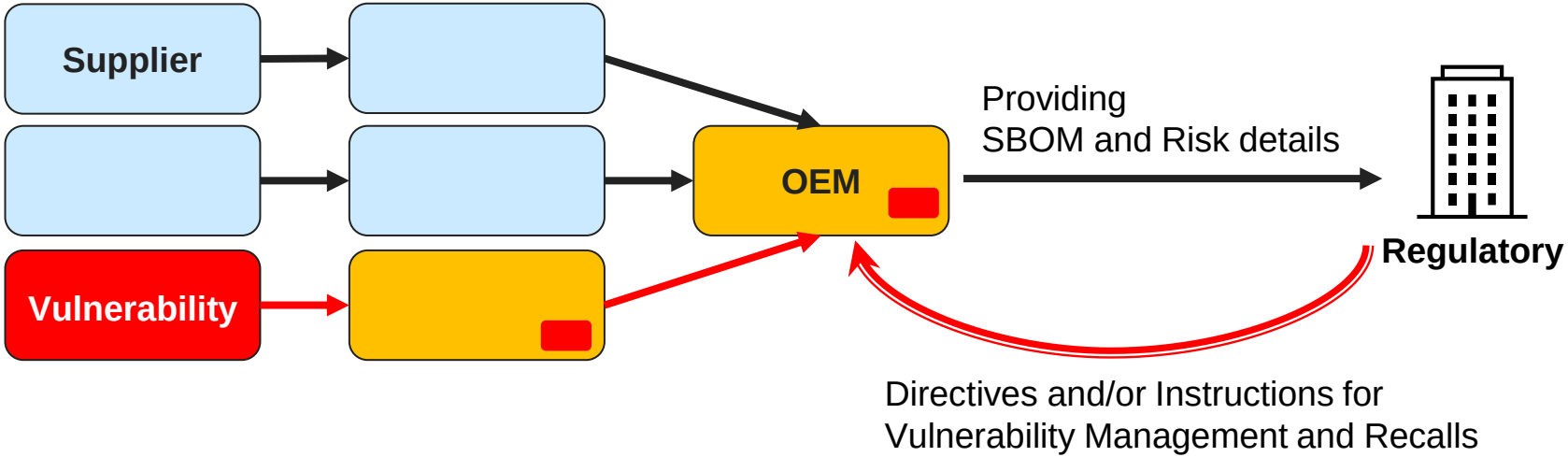
BSI.
3.2 Terms used
3.2.1 Component
In the case of interpreted code

(Second paragraph)
If the component is not part of the delivery item, the version number of the component SHOULD reflect the minimum required version as defined by the component creator. This SHOULD also take into account other factors than just the factual minimum technical requirement. This implies that the component creator SHOULD skip versions that are end-of-life or have known security vulnerabilities. The minimum required version MAY be determined by the minimum version, which was used for testing, e.g. because it was used during software development.

Note:
No descriptions of end-of-life or similar topics, other than the above.

Risk Management in Software Supply Chain

Need to consider not only B2B and B2C but also Regulatory Authorities

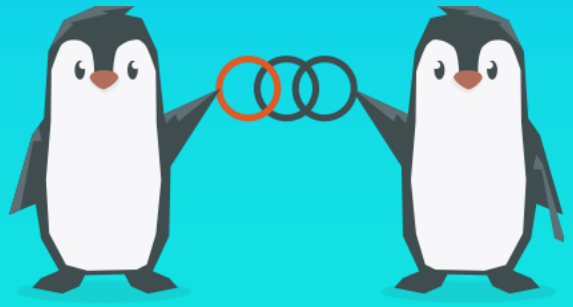


Need to Discussion

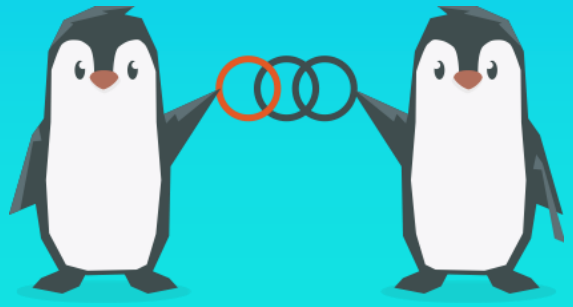
- CISA's Maturity Levels are a mixture of depth and broadness of dependency and information richness
  - SBOM Quality is likely to be a mosaic?

- Differences between CISA and BSI
  - "Maturity Levels" vs. "Level of Details"
  - What LEVEL with attributes is adequate for every stakeholder in the Software Supply chain?
  - How to express as SBOM document (both SPDX and CycloneDX)?

Thank you!



Appendix

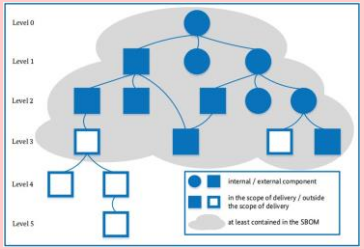


Document	URL
NTIA. Minimum Elements for Software Bill of Materials (SBOM)	https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom
CISA. Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) 3rd edition	https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024
BSI. Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2-2_0_0.html
IMDRF. Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity	https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity
FDA. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
PCI. PCI-DSS v4.0 and PCI-SSF v1.2.1	https://www.pcisecuritystandards.org/document_library/
OpenChain Project. OpenChain Telco SBOM Guide Version 1.0	https://github.com/OpenChain-Project/Reference-Material/tree/master/SBOM-Quality/Version-1

Enhance SBOM & VEX Practices Across the Supply Chain

Can we explore Practical HOW-TOs?

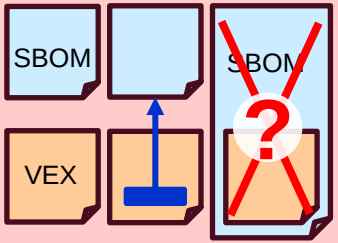
Maturity Level
Minimum Expected (Crawl)
Recommended Practice (Walk)
Aspirational Goal (Run)



Elements

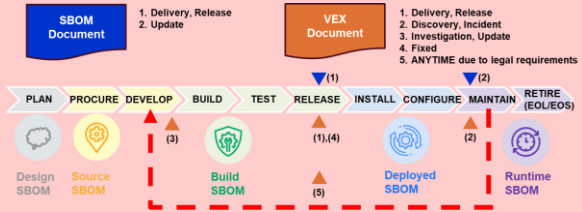
NTIA Minimum Elements	CISA Baseline Attributes	BSI TR-03183-2
Author of SBOM Data	SBOM Author Name	Creator of the SBOM
Timestamp	SBOM Timestamp	Timestamp
Lifecycle Phase	SBOM Type (Optional; Aspiration)	
Dependency Relationship	SBOM Primary Component	(primary component)
Component Name	Component Name	Component name
Version of the Component	Component Version String	Component version
Supplier Name	Component Supplier Name	Component creator
Component Hash	Component Cryptographic Hash	Hash value of the executable component (Optional: Hash value of the source code of the component)
Other Unique Identifiers	Component Unique Identifier	Other unique identifiers
Dependency Relationship	Component Relationships	Dependencies on other components
License Information	Component License (Aspiration: Concluded)	Concluded Licences (Optional: Declared licences)
License Information(Copyright)	Component Copyright Holder	(Not mentioned clearly, but assumed

SBOM & VEX



Operation

SDLC



"Delivery item SBOM" argued in: BSI. "Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0"
CISA. "When to Issue VEX Information". https://www.cisa.gov/resources-tools/resources/when-issue-vex-information
CISA. "Types of Software Bill of Materials (SBOM)". https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom