Add new first clause on “Alternate notation for some conformance requirements”

5.1 Alternate notation for some conformance requirements
This standard contains more than a few cardinality assertions, each of which indicates absolute, optional, or conditional requirements. Here are some examples:

— Cardinality: Mandatory, one.
— Cardinality: Optional, one or many.
— Cardinality: Mandatory, one if {condition} is true or {feature} omitted, zero (shall be omitted) if{condition} is false.
— Cardinality: 0..1
— Cardinality: 0..*
— Cardinality: 1..1
— Cardinality: 1..*

Each of these assertions can easily be understood as to whether a feature is required, and if so, how many occurrences are required; also, whether a feature is permitted, and if so, in what number. As this is the format long familiar to the SPDX community, it has been preserved in this specification.

5 ~~2~~ Conformance

5.2 ~~2.1~~ Introduction

Profile is the term for a compliance point within the SPDX community in the Linux Foundation. The System Package Data Exchange (SPDX) specification defines the following six compliance points, defined as “Profiles”:

- Core and Software Profile (Clauses 7 & 8)
- Security Profile (Clause 9)
- Licencing Profile (Clause 10)
- Dataset Profile (Clause 11)
- AI Profile (Clause 12)
- Build Profile (Clause 13)
- Lite Profile (Clause 14)
- Extension Profile (Clause 15)

The Core and Software Profile are mandatory. All others are optional.

5.3 ~~2.2~~ Core Profile compliance point

The Core profile includes the definitions of classes properties and vocabularies usable by all SPDX profiles when producing or consuming SPDX content. Although the classes, properties and vocabularies are somewhat extensive, the required fields are rather minimal to allow maximum flexibility while meeting minimum SBOM requirements. Software that conforms to the SPDX specification at the Core Profile compliance point shall be able to import and export serialized documents that conform with one of the defined SPDX serialization formats.

Conformance to the Core Profile compliance point is mandatory for all other SPDX profiles.

This compliance point, in combination with the Software Profile compliance point, provides a baseline of functionality that facilitates interchange of the bills of materials information produced by tools supporting SPDX.

5.4 ~~2.3~~ Software Profile compliance point

The Software profile includes the definitions of classes, properties and vocabularies for refering to and conveying information about software and is usable by all SPDX profiles when producing or consuming SPDX conten Software that conforms to the SPDX specification at the Software profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats.

Conformance to the security profile compliance point does not entail support for the Licencing, Data Set, AI, Build, Lite, or Extension profiles of the SPDX.

This compliance point, in combination with the Core Profile compliance point, provides a baseline of functionality that facilitates interchange of the bills of materials information produced by tools supporting SPDX.

5.5 ~~2.4~~ Security Profile compliance point

The security profile captures security-related information when producing or consuming SPDX content.

Software that conforms to the SPDX specification at the security profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization

formats, including the properties and relationships specified in the security profile, which are in support of exchanging information about software vulnerabilities that may exist, the severity of those vulnerabilities, and a mechanism to express how a vulnerability may affect a specific software element including if a fix is available.

Conformance to the security profile compliance point does not entail support for the Licencing, Data Set, AI, Build, Lite, or Extension profiles of the SPDX.

This compliance point facilitates interchange of the security information produced by tools supporting SPDX.

~~2.5~~ 5.6 Licencing Profile compliance point

The licensing profile includes capturing details relevant to software licensing and intellectual property information when producing or consuming SPDX content. Specifically, software that conforms to the SPDX specification at the Licencing profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including the classes and fields that comprise the SPDX License Expression syntax and that relate to the SPDX License List.

Conformance to the Licencing profile compliance point does not entail support for the Software, Security, Data Set, AI, Build, Lite, or Extension profiles of the SPDX.

This compliance point facilitates interchange of the licencing documents expressing which licenses and copyright notices are determined by persons or automated tooling to apply to distributions of software that are produced by tools supporting SPDX.

~~2.6~~ 5.7 Data Set Profile compliance point

The data set profile captures the relevant information about the datasets used in an AI system or other applications when producing or consuming SPDX content.

Software that conforms to the SPDX specification at the data set profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including details such as dataset names, versions, sources, associated metadata, licensing information, and any other relevant attributes. The data set profile can covey a description or summary of a dataset, including metadata, characteristics, and statistical information about the data. The data set profile can convey insights into the structure, format, content, and properties of a dataset, helping users understand and analyze the data more effectively.

Conformance to the data set profile compliance point does not entail support for the Software, Licencing, Security, AI, Build, Lite, or Extension profiles of the SPDX.

This compliance point facilitates interchange of the information about data sets produced by tools supporting SPDX.

~~2.7~~ 5.8 AI Profile compliance point

The AI profile captures an inventory list of software components and dependencies associated with an AI system when producing or consuming SPDX content.

Software that conforms to the SPDX specification at the AI profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including the information about software components and dependencies associated with artificial intelligence and machine learning (AI/ML) models and systems. This inventory includes the software frameworks, libraries, and other components used to build or deploy the AI system, along with relevant information about their versions, licenses, and useful security references including ethical and security information.

Conformance to the ai profile compliance point does not entail support for the Software, Licencing, Security, Data Set, Build, Lite, or Extension profiles of the SPDX.

This compliance point facilitates interchange of the AI model related information produced by tools supporting SPDX.

~~2.8~~ 5.9 Build Profile compliance point

The build profile captures build-related information when producing or consuming SPDX content.

Software that conforms to the SPDX specification at the Security profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including associated definitions to help express how software is generated and transformed. This includes encoding the inputs, outputs, procedures/instructions, environments and actors from the build process along with the associated evidence.

Conformance to the Build profile compliance point does not entail support for the Software, Licencing, Securotu. Data Set, AI, Lite, or Extension profiles of the SPDX.

This compliance point facilitates interchange of the build information produced by tools supporting SPDX.

~~2.9~~ 5.10 Lite Profile compliance point

The lite profile captures the minimum set of information required for license compliance in the software supply chain for producing or consuming SPDX content.

Software that conforms to the SPDX specification at the Security profile compliance point shall be able to import and export serialized documents that conform with one of the SPDX serialization formats defined SPDX serialization formats, including creation of the SBOM, package lists with licensing and other related items, and their relationships.

Conformance to the Lite profile compliance point does not entail support for the Software, Licencing, Security, Data Set, AI, Build, or Extension profiles of the SPDX.

This compliance point facilitates interchange of minimal licencing information when produced by tools supporting SPDX.

~~2.10~~ 5.11 Extension Profile compliance point

The extension profile captures extended tailored information when producing or consuming non-standard SPDX content in three ways:

- Support profile-based extended characterization of Elements. Enables specification and expression of Element characterization extensions within any profile and namespace of SPDX without requiring changes to other profiles or namespaces and without requiring local subclassing of remote classes (which could inhibit ecosystem interoperability in some cases).
- Support extension of SPDX by adopting individuals or communities with Element characterization details uniquely specialized to their particular context. Enables adopting individuals or communities to utilize SPDX expressive capabilities along with expressing more arcane Element characterization details specific to them and not appropriate for standardization across SPDX.
- Support structured capture of expressive solutions for gaps in SPDX coverage from real-world use. Enables adopting individuals or communities to express Element characterization details they require that are not currently defined in SPDX but likely should be. Enables a practical pipeline that identifies gaps in SPDX that should be filled, expresses solutions to those gaps in a way that allows the identifying adopters to use the extended solutions with SPDX and does not conflict with current SPDX, can be clearly detected among the SPDX content exchange ecosystem, provides a clear and structured definition of gap solution that can be used as submission for revision to the SPDX standard.